

XIII Monitor

- Chapter 65, “Starting the Monitor Agent,” on page 903
- Chapter 66, “Configuring the Monitor Agent,” on page 909
- Chapter 67, “Using the Monitor Agent Console,” on page 927
- Chapter 68, “Configuring the Monitor Application,” on page 941
- Chapter 69, “Using the Monitor Web Console,” on page 947
- Chapter 70, “Comparing the Monitor Agent Consoles,” on page 953
- Chapter 71, “Creating a PQA File for the Monitor Web Console,” on page 955
- Chapter 72, “Using Monitor Agent Switches,” on page 957

65 Starting the Monitor Agent

Detailed instructions for installing and starting the GroupWise® Monitor Agent for the first time are provided in “Installing GroupWise Monitor” in the *GroupWise 6.5 Installation Guide*. This section presents some additional Monitor Agent startup information.

- ♦ “Starting the Linux Monitor Agent” on page 903
- ♦ “Starting the Windows Monitor Agent” on page 905

Starting the Linux Monitor Agent

- ♦ “Starting the Linux Monitor Agent Manually” on page 903
- ♦ “Starting the Linux Monitor Agent Automatically” on page 904
- ♦ “Stopping the Linux Monitor Agent” on page 904

Starting the Linux Monitor Agent Manually

You do not need to be logged in as root to start the Monitor Agent.

- 1** Make sure you are logged in as root.
- 2** Make sure you know the path to a domain directory where a domain database (`wppdomain.db`) is located or the IP address of a server where the MTA is running.

- 3** Change to the GroupWise agent bin directory.

```
cd /opt/novell/groupwise/agents/bin
```

- 4** Use one of the following commands to start the Monitor Agent:

```
./gwmon --home /domain_directory &  
./gwmon --ipa IP_address --ipp port_number &
```

A message indicates that the Monitor Agent is polling the domain you specified. The Monitor Agent does not have a `--show` switch to provide a user interface.

You can also start the Monitor Agent using its startup script (`/etc/initd/grpwise-ma`).

- 5** View the following URL to verify that the Monitor Agent is running:

```
http://localhost:8200
```

UpTime: 0 d 13 h 30 m

<input type="checkbox"/>	Status	Status Duration	Name	Type	Closed Links	Queued	Platform	Version
<input type="checkbox"/>	✔ Normal	0 d 0 h 47 m	Development.Provo1	POA	N/A	N/A	NLM	6.5a (7/10/2003)
<input type="checkbox"/>	✔ Normal	0 d 0 h 47 m	Provo1	MTA	6	0	NLM	6.5a (7/10/2003)
<input type="checkbox"/>	✔ Normal	0 d 13 h 5 m	Provo3	MTA	0	0	LINUX	6.5.1 (04/29/2004)
<input type="checkbox"/>	✘ Not Listening	0 d 13 h 30 m	Research.Provo3	POA	N/A	N/A	?	

Status information for the agents in your GroupWise system is displayed.

Starting the Linux Monitor Agent Automatically

If you selected Launch Monitor Agent on System Startup in the Monitor Agent Installation program, your system was configured so that the Monitor Agent would start automatically. The Monitor Installation program always creates a `grpwise-ma` startup script in `/etc/init.d` for starting the Monitor Agent. To enable automatic startup, the Monitor Installation program creates symbolic links named `S99grpwise-ma` in the `rc3.d` and `rc5.d` directories so that the Monitor Agent can load on startup into runlevel 3 or 5, depending on the configuration of your Linux system.

When the `grpwise-ma` script runs and starts the Monitor Agent, it reads the Monitor Agent configuration file (`monitor.xml`) in `/opt/novell/groupwise/agents/share` to check for configuration information.

Stopping the Linux Monitor Agent

NOTE: If you started the Monitor Agent as root, then you must be logged in as root in order to stop it.

When you start the Monitor Agent with the `grpwise-ma` startup script, you can also use the script to stop it.

- 1** Change to the `/etc/init.d` directory.
- 2** To stop the Monitor Agent, enter the following command:
`./grpwise-ma stop`
- 3** To confirm that the Monitor Agent has stopped, enter the following command:
`./grpwise-ma status`

When you start the Monitor Agent manually (without using the `grpwise-ma` script), use the standard Linux kill command to stop it.

- 1** Determine the process ID of the Monitor Agent.
`ps -eaf | grep gwmon`
The PIDs for all `gwmon` processes are listed.
- 2** Kill the first `gwmon` process in the list.
`kill first_process_ID`
It might take a few seconds for all `gwmon` processes to terminate.
- 3** Repeat the `ps` command to verify that the Monitor Agent stopped.

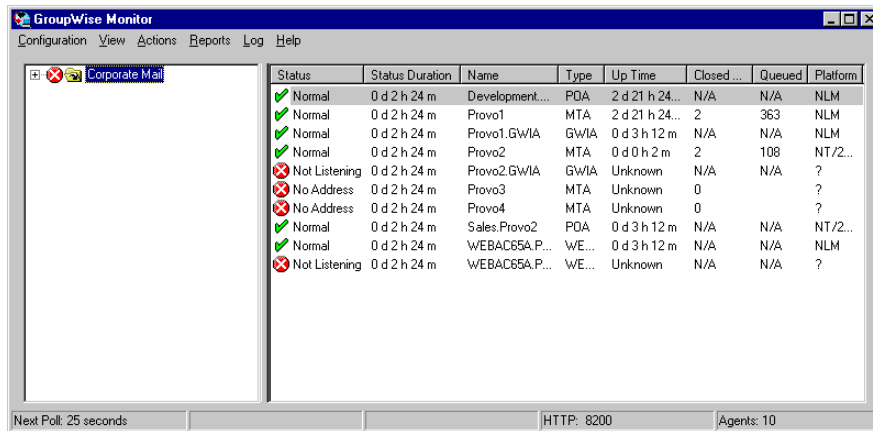
Starting the Windows Monitor Agent

- ◆ “Starting the Windows Monitor Agent Manually” on page 905
- ◆ “Starting the Windows Monitor Agent Automatically” on page 905
- ◆ “Stopping the Windows Monitor Agent” on page 906

Starting the Windows Monitor Agent Manually

In Windows, click Start > Programs > GroupWise Monitor > GroupWise Monitor. You might also want to create a desktop icon for it.

The Monitor Agent console appears.



If the Monitor Agent console does not appear, see “Monitor Agent Problems” in *GroupWise 6.5 Troubleshooting 2: Solutions to Common Problems*.

Starting the Windows Monitor Agent Automatically

To start the Monitor Agent automatically whenever you restart the Windows server, you can add the Monitor Agent program to the Windows Startup group.

- 1** In Windows NT, click Start > Settings > Taskbar > Start Menu Programs > Add.
or
In Windows 2000, click Start > Settings > Taskbar & Start Menu > Advanced > Add.
- 2** Browse to the directory where you installed the Monitor Agent.
- 3** Double-click gwmon.exe.
- 4** Click Next.
- 5** Select the Startup folder, provide a name for the shortcut, then click Finish.
- 6** If possible, restart the server to verify that the Monitor Agent starts when you log in.

Stopping the Windows Monitor Agent

At the Monitor Agent console:

- 1 Click File > Exit.

or

Close the window where the Monitor Agent is running.

Understanding the Monitor Agent Consoles

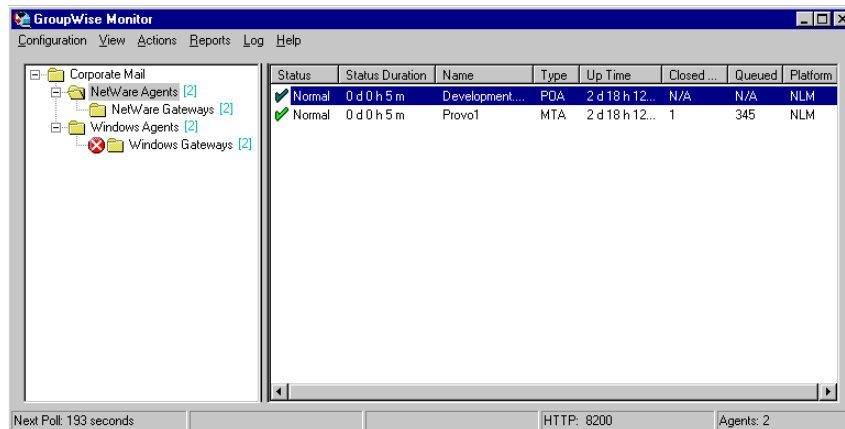
The Monitor Agent offers three consoles:

- ◆ “Monitor Agent Console” on page 906
- ◆ “Monitor Agent Web Console” on page 906
- ◆ “Monitor Web Console” on page 907

For a comparison of the capabilities of the three consoles, see [Chapter 70, “Comparing the Monitor Agent Consoles,”](#) on page 953

Monitor Agent Console

The Monitor Agent console is available for the Windows Monitor Agent but not for the Linux Monitor Agent.



All agent configuration tasks can be performed at the Monitor Agent console, but some reports are not available.

Monitor Agent Web Console

The Monitor Agent Web console is platform-independent and can be viewed at the following URL:

http://Web_server_address:8200

UpTime: 0 d 13 h 30 m

<input type="checkbox"/>	Status	Status Duration	Name	Type	Closed Links	Queued	Platform	Version
<input type="checkbox"/>	Normal	0 d 0 h 47 m	Development.Provo1	POA	N/A	N/A	NLM	6.5a (7/10/2003)
<input type="checkbox"/>	Normal	0 d 0 h 47 m	Provo1	MTA	6	0	NLM	6.5a (7/10/2003)
<input type="checkbox"/>	Normal	0 d 13 h 5 m	Provo3	MTA	0	0	LINUX	6.5.1 (04/29/2004)
<input type="checkbox"/>	Not Listening	0 d 13 h 30 m	Research.Provo3	POA	N/A	N/A	?	

To create the Monitor Agent Web console display, your Web server communicates directly with the Monitor Agent to obtain agent status information. You must be behind your firewall to use the Monitor Agent Web console. Because the Linux Monitor Agent does not have a console on the server where it runs, you use the Monitor Agent Web console in its place on Linux.

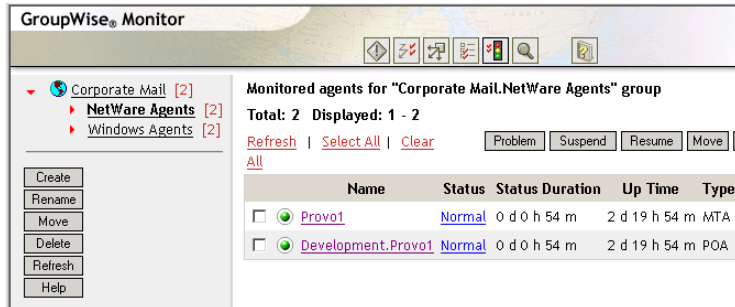
Several Monitor features are available at the Monitor Agent Web console that are not available at the Monitor Agent server console or the Monitor Web console. These are summarized in [Chapter 70, “Comparing the Monitor Agent Consoles,”](#) on page 953.

Monitor Web Console

The Monitor Web console is also platform-independent and can be viewed at the following URLs:

Linux: http://network_address/gwmon/gwmonitor

Windows: https://network_address/servlet/gwmonitor



To create the Monitor Web console display, your Web server communicates with the Monitor Application (a component of your Web server), which then communicates with the Monitor Agent to obtain agent status information. This enables the Monitor Web console to be available outside your firewall, while the Monitor Agent Web console can be used only inside your firewall.

The Monitor Web console is divided into the Agent Groups window on the left and the Agent Status window on the right. Using the Agents Groups window, you can create and manage agent groups the same as you can at the Monitor Agent server console.

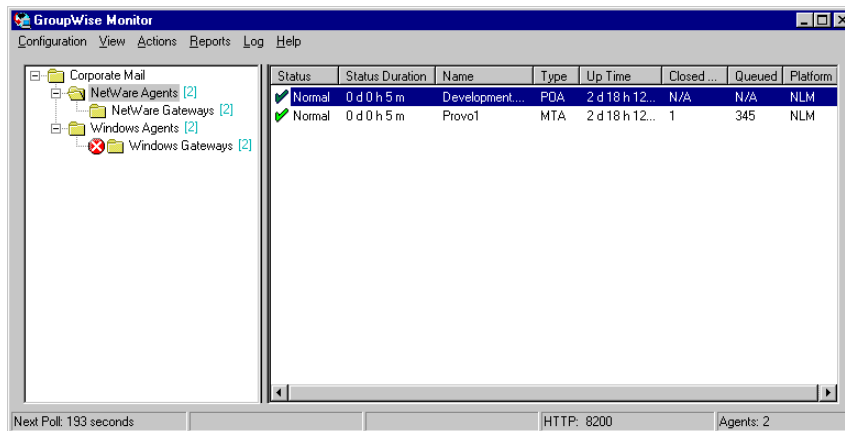
The Monitor Web console does not include some features that are available at the Monitor Agent server console and the Monitor Agent Web console. These are summarized in [Chapter 70, “Comparing the Monitor Agent Consoles,”](#) on page 953.

66

Configuring the Monitor Agent

The default configuration of the GroupWise® Monitor Agent is adequate to begin monitoring existing GroupWise agents (POAs, MTAs, Internet Agents, and WebAccess Agents). You can also customize the configuration to meet your specific monitoring needs.

On Windows, you configure the Monitor Agent at the Monitor Agent console on the Windows server where the Monitor Agent is running.



On Linux, similar functionality is available in your Web browser at <http://localhost:8200>.

[Status](#) | [Preferences](#) | [Link Trace](#) | [Link Configuration](#) | [Reports](#) | [Log](#)

[System](#) | [Problems](#)

UpTime: 0 d 13 h 30 m

<input type="checkbox"/>	Status	Status Duration	Name	Type	Closed Links	Queued	Platform	Version
<input type="checkbox"/>	✓ Normal	0 d 0 h 47 m	Development.Provo1	POA	N/A	N/A	NLM	6.5a (7/10/2003)
<input type="checkbox"/>	✓ Normal	0 d 0 h 47 m	Provo1	MTA	6	0	NLM	6.5a (7/10/2003)
<input type="checkbox"/>	✓ Normal	0 d 13 h 5 m	Provo3	MTA	0	0	LINUX	6.5.1 (04/29/2004)
<input type="checkbox"/>	✗ Not Listening	0 d 13 h 30 m	Research.Provo3	POA	N/A	N/A	?	

The following topics help you customize the Monitor Agent for your specific needs:

- ◆ [“Selecting Agents to Monitor” on page 910](#)
- ◆ [“Creating and Managing Agent Groups” on page 912](#)
- ◆ [“Configuring Monitoring Protocols” on page 914](#)
- ◆ [“Configuring Polling of Monitored Agents” on page 917](#)
- ◆ [“Configuring E-Mail Notification of Agent Problems” on page 918](#)
- ◆ [“Configuring Audible Notification of Agent Problems” on page 922](#)

- ◆ “Configuring SNMP Trap Notification of Agent Problems” on page 923
- ◆ “Configuring Authentication and Intruder Lockout for the Monitor Web Console” on page 924
- ◆ “Configuring Proxy Service Support for the Monitor Web Console” on page 925
- ◆ “Configuring Monitor Agent Log Settings” on page 925

Selecting Agents to Monitor

By default, the Monitor Agent starts monitoring all GroupWise agents (POAs, MTAs, Internet Agents, and WebAccess Agents) in your GroupWise system, based on the information from a domain database (`wpdomain.db`). You might not want to continue monitoring all agents. And as your GroupWise system grows, you might want to monitor additional agents.

- ◆ “Filtering the Agent List” on page 910
- ◆ “Adding All Agents on a Server” on page 911
- ◆ “Adding All Agents on a Subnet” on page 911
- ◆ “Adding an Individual Agent” on page 911
- ◆ “Removing Added Agents” on page 912

Filtering the Agent List

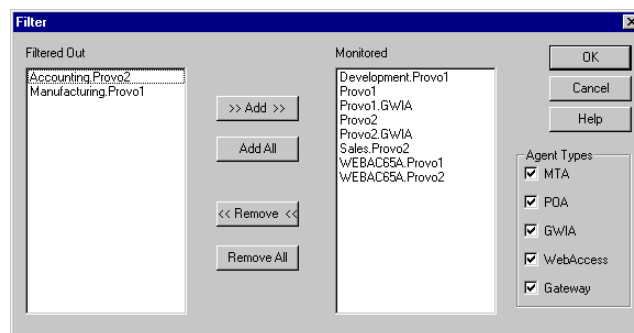
You can configure the Monitor Agent to stop and start monitoring selected agents as needed.

At the Windows Monitor Agent console:

- 1 Click Configuration > Filter.

or

On Linux, click Preferences > Filter.



The Filtered Out list displays all agents that are not currently being monitored.

- 2 Select one or more agents in the Monitored list, then click Remove to move them to the Filtered Out list.
- 3 Click OK.

Agents in the Filtered Out list are not monitored and do not appear at the Monitor Agent console nor at the Monitor Web console. To start monitoring a filtered-out agent, move it back to the Monitored list.

Adding All Agents on a Server

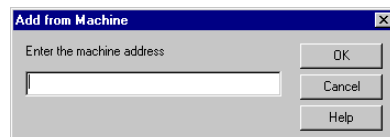
If you add a new server to your GroupWise system or want to monitor agents in a different GroupWise system, you can easily start monitoring all the agents running on that server.

At the Windows Monitor Agent console:

- 1 Click Configuration > Add from Server.

or

On Linux, click Preferences > Add Agents.



- 2 Type the IP address of the new server, then click OK.

All GroupWise agents on the new server are added to the list of monitored agents.

If the server is part of your local GroupWise system, you can simply restart the Monitor Agent and it picks up all new agents in your system.

Adding All Agents on a Subnet

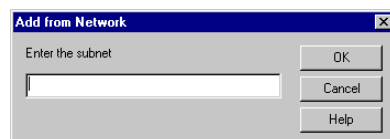
If you add several new servers to your GroupWise system or want to monitor agents in a different GroupWise system, you can easily start monitoring all the agents running on the same subnet.

At the Windows Monitor Agent console:

- 1 Click Configuration > Add from Network.

or

On Linux, click Preferences > Add Agents.



- 2 Type the subnet portion of the IP addresses of the new servers, then click OK.

All GroupWise agents on the subnet are added to the list of monitored agents.

If the servers are part of your local GroupWise system, you can simply restart the Monitor Agent and it picks up all new agents in your system.

Adding an Individual Agent

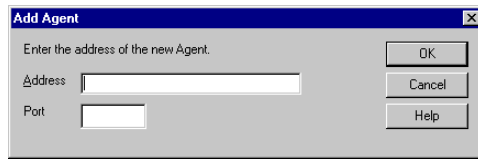
You can start monitoring an individual agent anywhere in your GroupWise system or another GroupWise system.

At the Windows Monitor Agent console:

- 1 Click Configuration > Add Agent.

or

On Linux, click Preferences > Add Agents.



- 2 Type the IP address of the server where the agent runs.
- 3 Type the port number the agent listens on.
- 4 Click OK.

The agent is added to the list of monitored agents.

Removing Added Agents

To stop monitoring agents that you have manually added to the Monitor Agent's configuration:

At the Windows Monitor Agent console:

- 1 Click Configuration > Remove Agents.

or

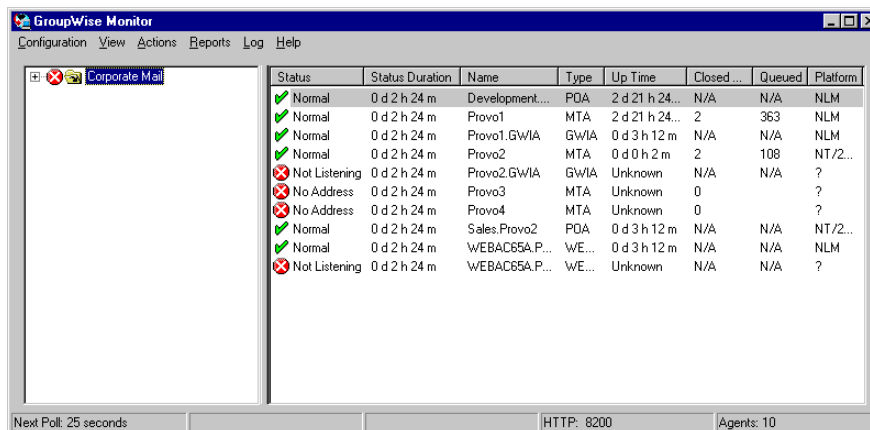
On Linux, click Preferences > Remove Agents.

- 2 Select the agents you want to remove, then click Remove.
- 3 Click OK.

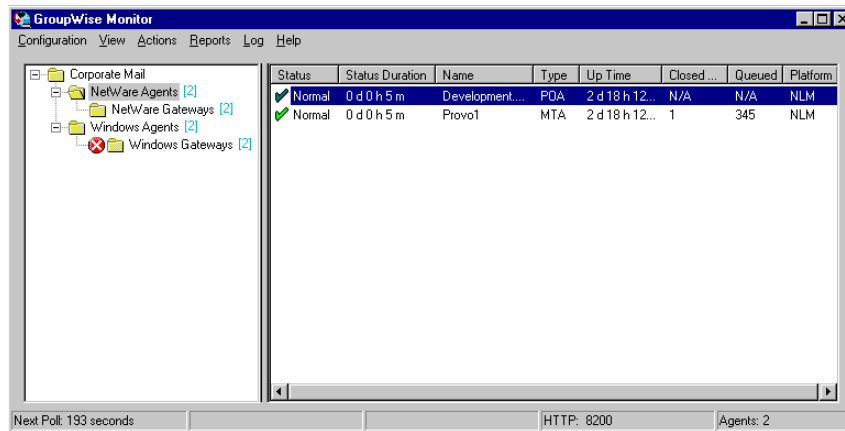
Creating and Managing Agent Groups

You might find it convenient to group related agents together for monitoring purposes. Initially, all agents are in a single group with the same name as your GroupWise system.

Agent groups are displayed on the left side of the Monitor Agent console. When you select an agent group, the monitored agents in the group and their status information are listed on the right side of the Monitor Agent console.



You can create additional groups and subgroups as needed to make monitoring similar agents easier. You might want to create agent groups based on geographical areas, on administrative responsibilities, or on agent configuration similarities. The number of agents in the group is displayed to the right of the group name in the agent groups window.



In addition, by creating agent groups, you can provide configuration settings for monitoring just once for all agents in each group, rather than having to provide them individually for each agent in your GroupWise system.

- ◆ [“Creating an Agent Group” on page 913](#)
- ◆ [“Managing Agent Groups” on page 913](#)
- ◆ [“Viewing Your Agent Group Hierarchy” on page 914](#)
- ◆ [“Configuring an Agent Group” on page 914](#)

NOTE: On Linux, perform these tasks in the Monitor Web console.

Creating an Agent Group

At the Windows Monitor Agent console:

- 1** Right-click the folder where you want to create the agent group, then click Create.
- 2** Type a name for the group, then click OK to create a new folder for the agent group.
The group name must be unique within its parent group.
- 3** Click a folder containing agents that you want to add to the new group.
- 4** Drag and drop agents into the new group as needed.
- 5** Click the new group to view its contents.

You can nest groups within groups as needed.

Managing Agent Groups

Managing agent groups is easy:

- ◆ To rename an agent group, right-click the agent group, click Rename, type the new name, then press Enter.
- ◆ To move an agent group, drag and drop it to its new location.

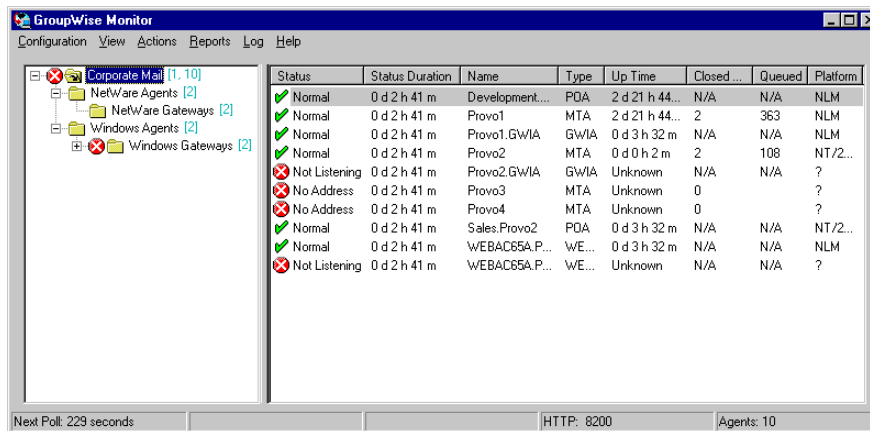
- ◆ To delete an agent group, right-click the agent group, then click Delete. A group must be empty before you can delete it.

Viewing Your Agent Group Hierarchy

When you create nested groups, you can choose how much of the hierarchy you want displayed:

- ◆ You can open and close groups manually by clicking the plus and minus icons beside each folder.
- ◆ To expand your entire group hierarchy, click View > Expand Tree.
- ◆ To collapse your entire group hierarchy, click View > Collapse Tree.

You can also decide, when viewing the agents in a group, whether you want to view just the agents in the currently selected group or the agents in subgroups as well. By default, only the agents in the selected folder are listed in the agent window. Right-click an agent group, then click Show Subgroup Agents to display the contents of nested groups along with the selected group.



Numbers in brackets beside each group indicate the number of agents in the selected group and the total number displayed

Configuring an Agent Group

Configuration settings for monitoring can be set for each monitored agent individually, for each agent group, or for all monitored agents collectively. You can establish default configuration settings for all agents by setting them on the root agent group that is named the same as your GroupWise system. Those default settings can be inherited by each subgroup that you create thereafter if you select Apply Options to Subgroups. Those default settings can be overridden by establishing different settings for an agent group or for an individual agent if you deselect Use Parent Options.

Configuring Monitoring Protocols

By default, the Monitor Agent uses HTTP to communicate with the agents it monitors, whenever HTTP is available. If HTTP is not available, the Monitor Agent changes automatically to SNMP.

GroupWise 6.x agents and gateways as well as the GroupWise agents provided with the GroupWise 5.5 Enhancement Pack can be monitored using HTTP. Agents dating from GroupWise 5.5 and earlier, as well as 5.5-level GroupWise gateways, must be monitored using SNMP.

- ◆ “Configuring the Monitor Agent for HTTP” on page 915
- ◆ “Configuring the Monitor Agent for SNMP” on page 916

Configuring the Monitor Agent for HTTP

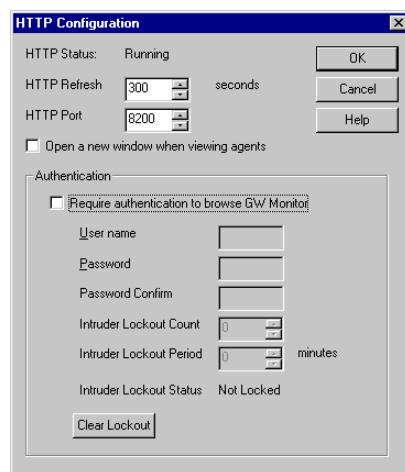
You can customize how the Monitor Agent communicates with your Web browser.

At the Windows Monitor Agent console:

- 1 Click Configuration > HTTP.

or

On Linux, click Preferences > Setup, then scroll down to the HTTP Settings section.



- 2 Modify the HTTP settings as needed:

HTTP Refresh: Specify the number of seconds after which the Monitor Agent sends updated information to the Monitor Web console. The default is 300 seconds (5 minutes).

HTTP Port: Specify the port number for the Monitor Agent to listen on for requests for information from the Web console. The default port number is 8200.

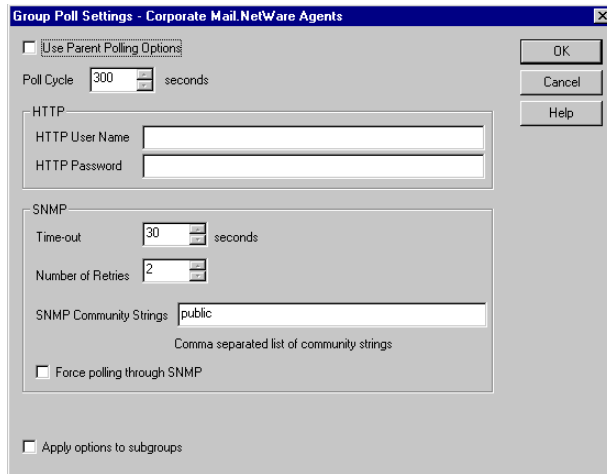
Open a New Window When Viewing Agents: Select this option to open a new Web browser window whenever you display an agent Web console. This enables you to view the Monitor Web console and an agent Web console at the same time, or to view two agent Web consoles at the same time for comparison.

- 3 Click OK to put the new HTTP settings into effect.

- 4 Click Configuration > Poll Settings.

or

On Linux, click Preferences > Setup, then scroll down to the HTTP Settings section.



5 Fill in the following fields:

Poll Cycle: Specify the number of seconds after which the Monitor Agent polls all monitored GroupWise agents for updated information.

By default, the Monitor Agent starts 20 threads to poll monitored agents. You can use the `/pollthreads` startup switch to adjust the number of threads.

By default, the Monitor Agent communicates with other GroupWise agents by way of XML. However, if XML is unavailable, the Monitor Agent automatically uses SNMP instead. Prior to the GroupWise 5.5 Enhancement Pack, GroupWise agents did not support XML, so the Monitor Agent must use SNMP to monitor these older agents. If you need to monitor older agents, see [“Configuring the Monitor Agent for SNMP” on page 916](#).

If all monitored agents in the group require the same username and password in order to communicate with the Monitor Agent, you can provide that information as part of the Monitor Agent’s configuration.

HTTP User Name: Provide the username for the Monitor Agent to use when contacting monitored agents in the group for status information.

HTTP Password: Provide the password, if any, associated with the username specified in the field above.

NOTE: On Linux, the HTTP User Name and HTTP Password fields are not available. However, you can use the `--httpagentuser` and `--httpagentpassword` startup switches on the command line when you start the Monitor Agent to achieve the same functionality.

If the monitored agents use different usernames and passwords, you are prompted to supply them when the Monitor Agent needs to communicate with the monitored agents.

6 Click Apply Options to Subgroups if you want subgroups to inherit these settings.

7 Click OK to put the specified poll cycle into effect.

Configuring the Monitor Agent for SNMP

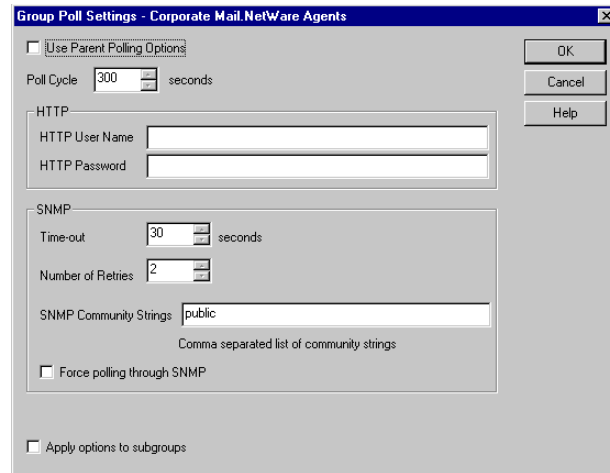
The Monitor Agent must use SNMP to communicate with GroupWise agents that date from earlier than the GroupWise 5.5 Enhancement Pack. You can customize how the Monitor Agent communicates with such older agents and how it communicates with SNMP monitoring and management programs.

At the Windows Monitor Agent console:

1 Click Configuration > Polling.

or

On Linux, click Preferences > Setup, then scroll down to the SNMP Settings section.



2 Specify the number of seconds after which the Monitor Agent polls all monitored GroupWise agents for updated information using SNMP.

3 In the SNMP box, modify the SNMP settings as needed:

Time Out: Specify the number of seconds the Monitor Agent should wait for a response from servers where GroupWise agents run.

Number of Retries: Specify how often the Monitor Agent should try to contact the servers where GroupWise agents run.

SNMP Community Strings: Provide a comma-delimited list of community strings required to access the servers where GroupWise agents run.

Force Polling through SNMP: Select this option to use SNMP polling instead of the default of XML polling when contacting servers where agents in the group run.

4 Click Apply Options to Subgroups if you want subgroups to inherit these settings.

5 Click OK to put the new SNMP settings into effect.

6 Make sure the GroupWise agents you want to monitor using SNMP are enabled for SNMP. See [“Setting Up SNMP Services for the POA” on page 499](#) and [“Setting Up SNMP Services for the MTA” on page 627](#). The same instructions can be followed for all GroupWise 5.x and 6.x agents.

Configuring Polling of Monitored Agents

By default, the Monitor Agent polls all monitored agents every five minutes. You can adjust the poll cycle as needed.

At the Windows Monitor Agent console:

1 Select the root agent group to set the poll cycle default for all monitored agents.

or

Select any agent group to set the poll cycle for the agents in the selected group.

or

Select any agent to set the poll cycle for that individual agent.

- 2 Click Configuration > Poll Settings.

or

On Linux, click Preferences > Setup, then scroll down to the HTTP Settings section.

The screenshot shows a dialog box titled "Group Poll Settings - Corporate Mail NetWare Agents". It features a "Use Parent Polling Options" checkbox at the top left. Below it is a "Poll Cycle" spinner set to 300 seconds. The "HTTP" section includes "HTTP User Name" and "HTTP Password" text boxes. The "SNMP" section includes "Time-out" (30 seconds), "Number of Retries" (2), and "SNMP Community Strings" (public) text boxes. There is also a "Force polling through SNMP" checkbox. At the bottom left is an "Apply options to subgroups" checkbox. On the right side, there are "OK", "Cancel", and "Help" buttons.

Unless you selected the root agent group, Use Parent Notification Options is selected and all options are dimmed. Deselect Use Parent Notification Options to set up e-mail notification for an agent group.

- 3 Increase or decrease the poll cycle as needed, then click OK.

Configuring E-Mail Notification of Agent Problems

The Monitor Agent can notify you by e-mail when agent problems arise.

- ♦ [“Configuring E-Mail Notification” on page 918](#)
- ♦ [“Customizing Notification Thresholds” on page 920](#)

Configuring E-Mail Notification

You can configure the Monitor Agent to notify one or more users by e-mail if an agent goes down. You can also receive e-mail confirmation messages showing that the Monitor Agent itself is still running normally.

At the Windows Monitor Agent console:

- 1 Select the root agent group to set up e-mail notification defaults for all monitored agents.

or

Select any agent group to set up e-mail notification for the agents in the selected group.

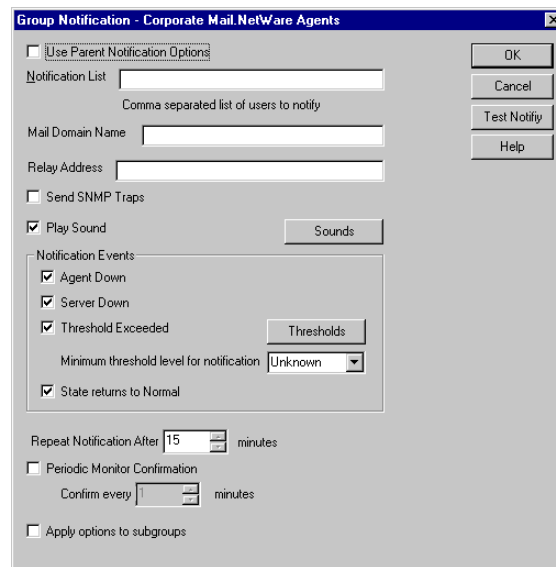
or

Select any agent to set up e-mail notification for that individual agent.

- 2 Click Configuration > Notification.

or

On Linux, click Preferences > Setup to display the Notify settings.



Unless you selected the root agent group, Use Parent Notification Options is selected and all options are dimmed. Deselect Use Parent Notification Options to set up e-mail notification for an agent group or an individual agent.

- 3** Specify one or more e-mail addresses or pager addresses to send notifications to.
- 4** Specify the Internet domain name of your GroupWise system.
- 5** If the mail system to which e-mail notification is being sent performs reverse DNS lookups, specify the IP address or hostname of a server to relay the notification messages through.

The Monitor Agent should relay e-mail notifications through a server that has a published DNS address.

- 6** Click Test Notify to determine if the Monitor Agent can successfully send to the addresses specified in the Notification List field.

A message informs you of the results of the test. If the test is successful, a test message arrives shortly at each address. If the test is unsuccessful, double-check the information you provided in the Notification List, Mail Domain Name, and Relay Address fields.

- 7** Select the events that you want to trigger e-mail notification messages.

- ◆ Agent down
- ◆ Server down
- ◆ Threshold exceeded
- ◆ State returns to normal

If you want to be notified of more specific states, see [“Customizing Notification Thresholds” on page 920](#).

- 8** Select the amount of time that you want to elapse before repeat e-mail notifications are sent.

- 9 To monitor the Monitor Agent and assure it is functioning normally, select Periodic Monitor Confirmation, select the number of minutes between Monitor Agent e-mail confirmation messages.
- 10 Click OK to save the e-mail notification settings.

Customizing Notification Thresholds

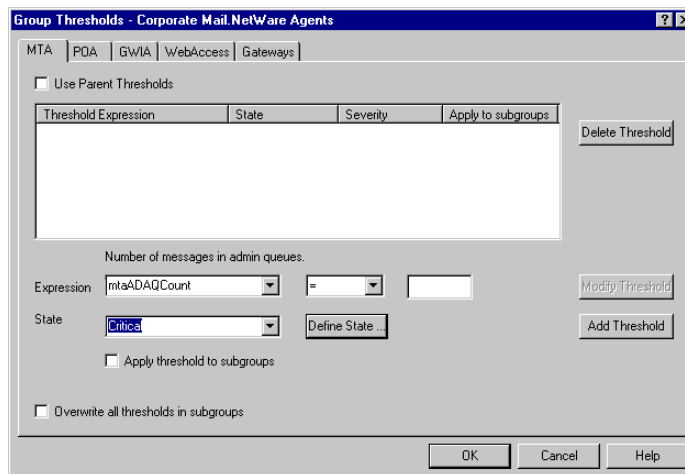
To refine the types of events that trigger e-mail notification messages, you can create your own thresholds that describe very specific states. Using thresholds, you can configure the Monitor Agent to notify you of problem situations peculiar to your GroupWise system.

At the Windows Monitor Agent console:

- 1 Click Configuration > Notification.
- 2 Make sure that notification has been properly set up as described in “Configuring E-Mail Notification” on page 918.
- 3 Click Thresholds.

or

On Linux, click Preferences > Thresholds.











The tabs at the top of the dialog box enable you to create a separate threshold for each type of GroupWise agent.

- 4 Select the type of agent to create a threshold for.
- 5 In the Expression field, select a MIB variable.

GroupWise agent MIB files are located in the `\agents\snmp` directory of your GroupWise software distribution directory or *GroupWise 6.5 Administrator* CD. The MIB files list the meanings of the MIB variables and what type of values they represent. The meaning of the MIB variable selected in the Expression field is displayed above the field.

- 6 Select an operator from the drop-down list.
- 7 Type the value to test for.
- 8 In the State field, select an existing state.

Icon	State
	Unknown
	Normal
	Informational
	Marginal
	Warning
	Minor
	Major
	Critical

or

Create a new state:

8a Click Define State

or

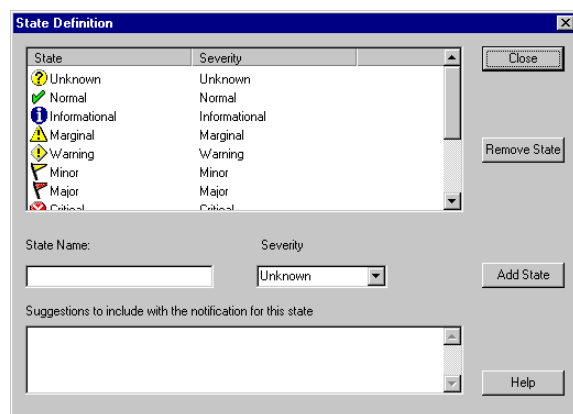
On Linux, click Preferences > States.

8b Type a name for the new state.

8c Select a severity level.

8d Provide instructions about how to handle the new state.

8e Click Close to save the new state.



9 Click OK to create the new threshold.

10 Repeat **Step 3** through **Step 9** for each type of agent that you want to create a customized state for.

11 Make sure Threshold Exceeded is selected in the Notification Events box.

12 Click OK to save the new notification settings.

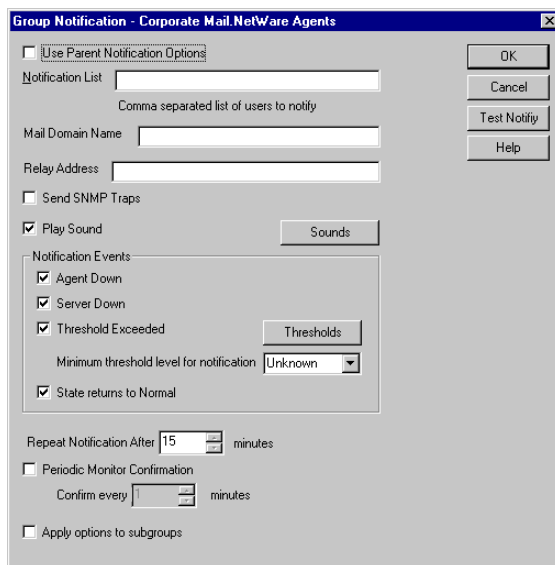
Configuring Audible Notification of Agent Problems

If the server where the Monitor Agent runs is located where someone can respond immediately to a GroupWise agent problem, you can configure the Monitor Agent to produce a different sound according to the nature of the problem.

NOTE: Audible notification is not available on Linux.

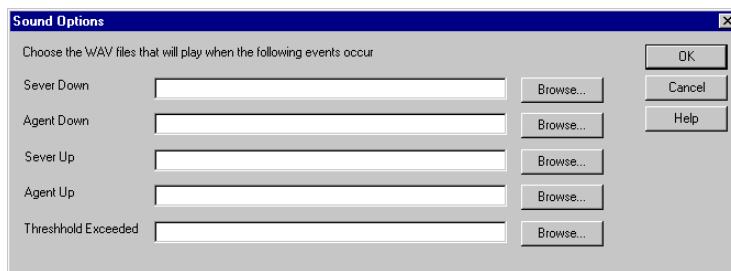
At the Windows Monitor Agent console:

- 1 Select the root agent group to set up audible notification defaults for all monitored agents.
or
Select any agent group to set up audible notification for the agents in the selected group.
or
Select any agent to set up audible notification for that individual agent.
- 2 Click Configuration > Notification.



Unless you selected the root agent group, Use Parent Notification Options is selected and all options are dimmed. Deselect Use Parent Notification Options to set up notification for an agent group or individual agent.

- 3 Select Play Sound, then click Sounds.



- 4 For each event, browse to and select a sound file to provide auditory notification for each type of event for the selected agent group.

The Monitor Agent launches the default media player for whatever type of sound file you select. Basic sound files are available in the c:\winnt\media directory.

- 5 Click OK to return to the Notification dialog box.
- 6 Select notification events and other notification settings as described in [“Configuring E-Mail Notification of Agent Problems” on page 918](#).
- 7 Click OK to save the audible notification settings.

Configuring SNMP Trap Notification of Agent Problems

The Monitor Agent can throw SNMP traps for use by the Management and Monitoring component of Novell® ZENworks® for Servers, ManageWise®, or any other SNMP management and monitoring program.

At the Windows Monitor Agent console:

- 1 Select the root agent group to set up SNMP trap notification defaults for all monitored agents.
or
Select any agent group to set up SNMP trap notification for the agents in the selected group.
or
Select any agent to set up SNMP trap notification for that individual agent.
- 2 Click Configuration > Notification.
or
On Linux, click Preferences > Setup to display the Notify settings.

The screenshot shows a dialog box titled "Group Notification - Corporate Mail NetWare Agents". It contains several sections for configuring notification settings:

- Use Parent Notification Options (dimmed)
- Notification List: [Text field]
- Comma separated list of users to notify
- Mail Domain Name: [Text field]
- Relay Address: [Text field]
- Send SNMP Traps
- Play Sound (with Sounds button)
- Notification Events:
 - Agent Down
 - Server Down
 - Threshold Exceeded (with Thresholds button)
 - Minimum threshold level for notification: [Unknown dropdown]
 - State returns to Normal
- Repeat Notification After: [15] minutes
- Periodic Monitor Confirmation
- Confirm every: [1] minutes
- Apply options to subgroups

Buttons on the right side include OK, Cancel, Test Notify, and Help.

Unless you selected the root agent group, Use Parent Notification Options is selected and all options are dimmed. Deselect Use Parent Notification Options to set up notification for an agent group or individual agent.

- 3 Select Send SNMP Traps, then click OK.
- 4 Make sure that the Monitor Agent is properly configured for SNMP, as described in “Configuring the Monitor Agent for SNMP” on page 916.

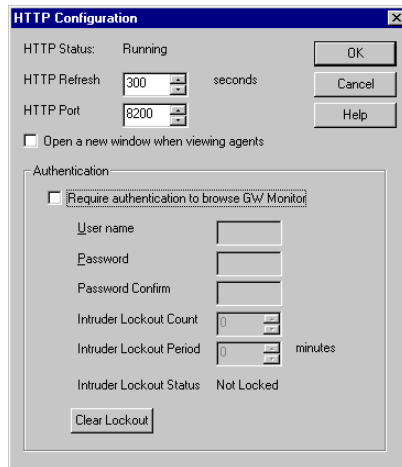
Configuring Authentication and Intruder Lockout for the Monitor Web Console

Accessing GroupWise agent status information from your Web browser is very convenient. However, you might want to limit access to that information. You can configure the Monitor Agent to request a username and password before allowing users to access the Monitor Web console. In addition, you can configure the Monitor Agent to detect break-in attempts in the form of repeated unsuccessful logins.

NOTE: To limit access on Linux, use the `--httpmonuser` and `--httpmonpassword` startup switches on the command line when you start the Monitor Agent. The intruder lockout functionality is not available on Linux.

At the Windows Monitor Agent console:

- 1 Click Configuration > HTTP.



- 2 In the Authentication box, select Require Authentication to browse GW Monitor.
- 3 Fill in the fields:

User Name: Provide a username for the Monitor Agent to prompt for when a user attempts to access the Monitor Web console.

Password: Provide a password for the Monitor Agent to prompt for when a user attempts access. Repeat the password in the Password Confirm field.

To provide additional security for the Monitor Web console, use the `/httpsll` and `/httpcertfile` startup switches when starting the Monitor Agent.

Intruder Lockout Count: Specify the number of failed attempts the Monitor Agent should allow before it stops prompting the potentially unauthorized user for a valid username and password.

Intruder Lockout Period: Specify the number of minutes that must elapse before the user can again attempt to access the Monitor Web console.

If a valid user gets locked out of the Monitor Web console, you can use Clear Lockout to grant access before the intruder lockout period has elapsed.

- 4 Click OK to put the authentication settings into effect.

Configuring Proxy Service Support for the Monitor Web Console

By default, the Monitor Agent and Monitor Web console are not configured to support browser-based access to the Monitor Agent through a firewall. If you require this functionality, you need to enable the Monitor Agent and Monitor Web console to support proxy service.

- 1 In a text editor, open the Monitor Application configuration file (`gwmonitor.cfg`)

On Linux, the default location is `/opt/novell/groupwise/agents/gwmonitor`. On Windows, the default location is `c:\novell\gwmonitor`

- 2 Locate the following line:

```
Provider.GWMP.Agent.Http.level=basic
```

- 3 Change it to:

```
Provider.GWMP.Agent.Http.level=full
```

The BASIC setting restricts use of the Monitor Web console to within a firewall, while the FULL setting allows use of the Web console both inside and outside a firewall. A third setting, NONE, disables use of the Web console.

- 4 Save and exit the Monitor Application configuration file.

- 5 Start the Monitor Agent with the `/proxy` startup switch.

The `/proxy` switch must be used on the command line or in a script or batch file. The Monitor Agent does not use a startup file for switches.

Without proxy service support enabled, the Monitor Web console, after it gets a GroupWise agent's address from the Monitor Agent, communicates directly with the GroupWise agent. This process, however, does not work when communicating through a firewall.

With proxy service support enabled, all communication is routed through the Monitor Agent and Monitor Application (on the Web server). As long as the Web server can be accessed through the firewall, the Monitor Web console can receive information about all GroupWise agents that the Monitor Agent knows about.

Configuring Monitor Agent Log Settings

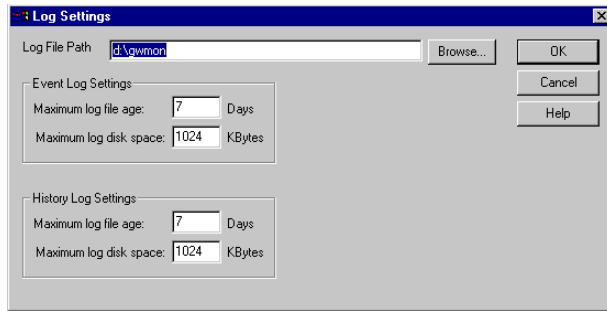
The Monitor Agent writes to two different types of log files. Event log files record error messages, status messages, and other types of event-related messages. History log files record dumps of all MIB values gathered during each poll cycle. Log files can provide a wealth of information for resolving problems with Monitor Agent functioning or agent monitoring.

At the Windows Monitor Agent console:

- 1 Click Log > Log Settings.

or

On Linux, click Log.



2 Fill in the fields:

Log File Path: Specify the full path of the directory where the Monitor Agent writes its log files. On Linux, the default directory is `/var/log/novell/groupwise/gwmon`. On Windows, the default is the GroupWise Monitor installation directory (typically `c:\gwmon`).

Maximum Event Log File Age: Specify the number of days you want Monitor Agent event log files to remain on disk before being automatically deleted. The default event log file age is 7 days.

Maximum Event Log Disk Space: Specify the maximum amount of disk space for all Monitor event log files. When the specified disk space is used, the Monitor Agent overwrites existing Monitor Agent event log files, starting with the oldest. The default is 1024 KB of disk space for all Monitor Agent event log files.

Maximum History Log File Age: Specify the number of days you want Monitor Agent history log files to remain on disk before being automatically deleted. The default history log file age is 7 days.

Maximum History Log Disk Space: Specify the maximum amount of disk space for all Monitor history log files. When the specified disk space is used, the Monitor Agent overwrites existing Monitor Agent history log files, starting with the oldest. The default is 1024 KB of disk space for all Monitor Agent history log files.

- 3** Click OK to put the new log settings into effect.
- 4** To view existing event logs, click View > View Log Files.
- 5** To view existing history log files, click Log > View History Files.

67

Using the Monitor Agent Console

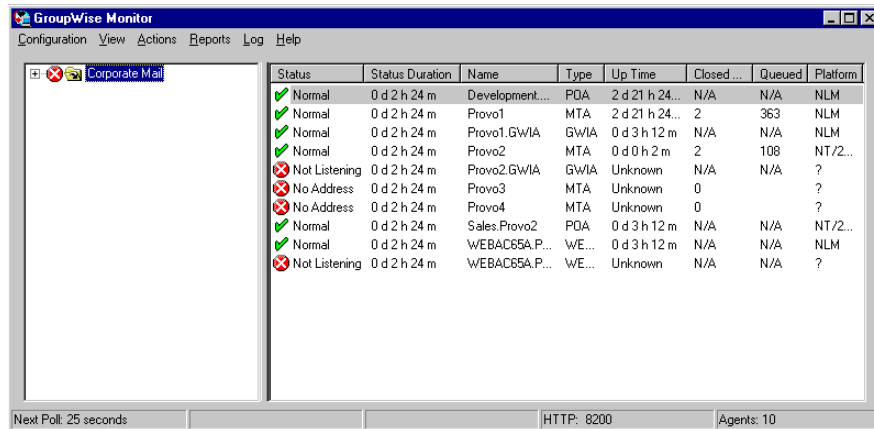
The GroupWise® Windows Monitor Agent console displays GroupWise agent status on the server where the Monitor Agent runs. On Linux, similar information can be displayed in a Web browser.

- ♦ “Monitoring Agents at the Monitor Agent Console” on page 927
- ♦ “Generating Reports” on page 931
- ♦ “Measuring Agent Performance” on page 935

Monitoring Agents at the Monitor Agent Console

Initially, the Monitor Agent console lists all monitored GroupWise agents, along with their statuses.

NOTE: On Windows, agents and agent groups are displayed at the Monitor Agent console. On Linux, agents groups are displayed only at the Monitor Web console.

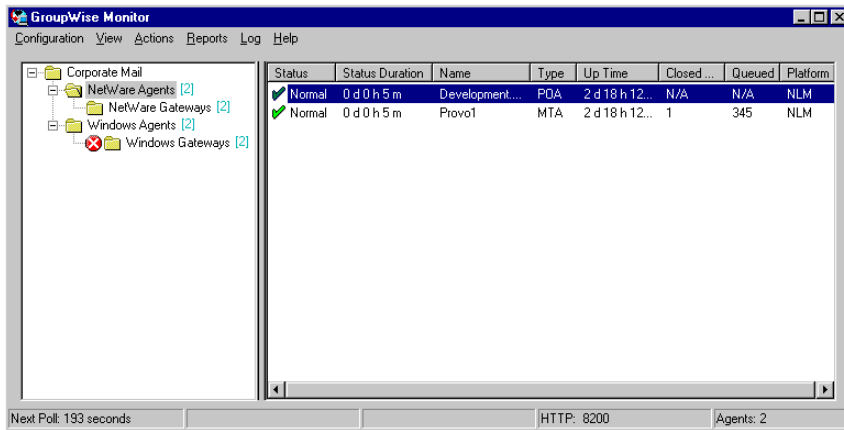


The screenshot shows the GroupWise Monitor application window. The title bar reads "GroupWise Monitor" and the menu bar includes "Configuration", "View", "Actions", "Reports", "Log", and "Help". On the left, there is a tree view with "Corporate Mail" selected. The main area displays a table of agents with the following columns: Status, Status Duration, Name, Type, Up Time, Closed..., Queued, and Platform.

Status	Status Duration	Name	Type	Up Time	Closed...	Queued	Platform
✓ Normal	0 d 2 h 24 m	Development...	POA	2 d 21 h 24...	N/A	N/A	NLM
✓ Normal	0 d 2 h 24 m	Provo1	MTA	2 d 21 h 24...	2	363	NLM
✓ Normal	0 d 2 h 24 m	Provo1.GWIA	GWIA	0 d 3 h 12 m	N/A	N/A	NLM
✓ Normal	0 d 2 h 24 m	Provo2	MTA	0 d 0 h 2 m	2	108	NT/2...
✗ Not Listening	0 d 2 h 24 m	Provo2.GWIA	GWIA	Unknown	N/A	N/A	?
✗ No Address	0 d 2 h 24 m	Provo3	MTA	Unknown	0	?	?
✗ No Address	0 d 2 h 24 m	Provo4	MTA	Unknown	0	?	?
✓ Normal	0 d 2 h 24 m	Sales.Provo2	POA	0 d 3 h 12 m	N/A	N/A	NT/2...
✓ Normal	0 d 2 h 24 m	WEBAC65A.P...	WE...	0 d 3 h 12 m	N/A	N/A	NLM
✗ Not Listening	0 d 2 h 24 m	WEBAC65A.P...	WE...	Unknown	N/A	N/A	?

At the bottom of the window, there are three status indicators: "Next Poll: 25 seconds", "HTTP: 8200", and "Agents: 10".

After you create agent groups, as described in “Creating and Managing Agent Groups” on page 912, the agents in each group are displayed when you select a group.



You can display many types of monitoring information at the Monitor Agent console.

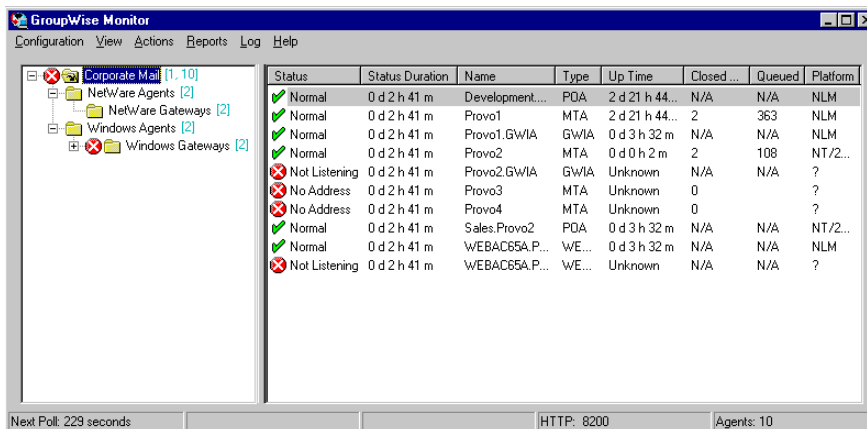
- ◆ “Viewing All Agents” on page 928
- ◆ “Viewing Problem Agents” on page 928
- ◆ “Viewing an Agent Console” on page 929
- ◆ “Viewing an Agent Web Console” on page 930
- ◆ “Polling the Agents for Updated Status Information” on page 930

Viewing All Agents

After you have separated your agents into groups, you can still view all agents in your GroupWise system in a single list.

At the Windows Monitor Agent console:

- 1 Right-click the root agent group, then click Show Agent Subgroups.



You can use the Show Agent Subgroups feature on any group that contains nested subgroups.

Viewing Problem Agents

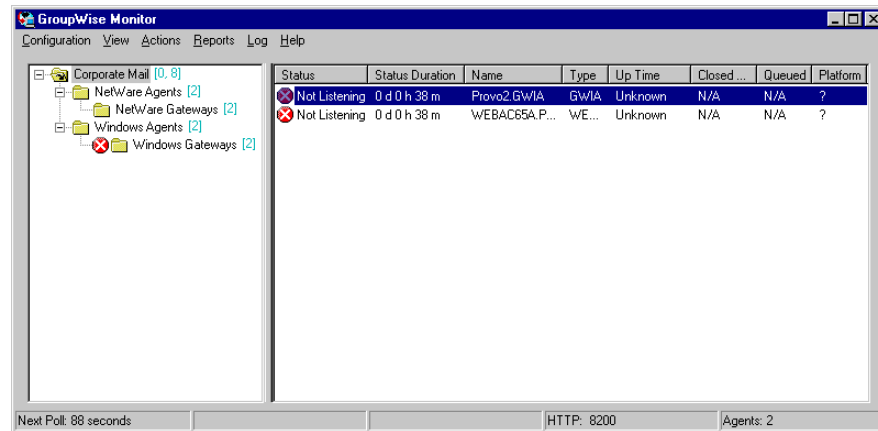
In a single agent group or in a group with subgroups shown, you can filter the list to show only those agents whose status is not Normal.

At the Windows Monitor Agent console:

- 1 Click View > Problem Agents.

or

On Linux, click Problems.



Only problem agents are now displayed. If you leave the Monitor Agent with only problem agents displayed, many groups might appear empty because all agents have a status of Normal.

- 2 To view all monitored agents again, click View > All Agents.

or

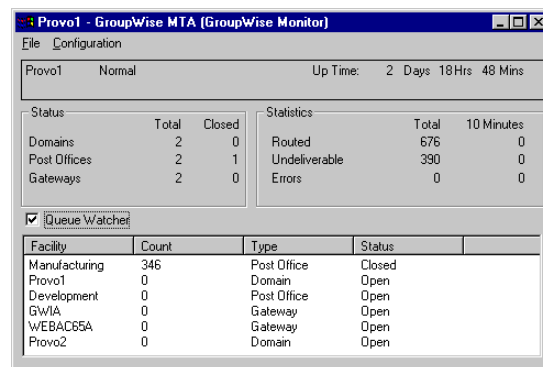
On Linux, click System.

Viewing an Agent Console

An active agent console displays on each server where a GroupWise agent is running. You can display a similar agent console from the Windows Monitor Agent console.

NOTE: This feature is not available on Linux.

- 1 Right-click an agent, then click Agent Console.



You cannot control the agent from the Monitor Agent like you can at the actual agent console, but you can gather status information about the monitored agent.

Viewing an Agent Web Console

An agent Web console can be displayed anywhere you have access to a Web browser and the Internet. You can launch an agent Web console from the Windows Monitor Agent console.

- 1 Right-click an agent, then click Agent Web Console.

or

On Linux, click the domain or post office link.

GroupWise 6 POA - SALES.PROVO2		
Status Configuration Environment Log Files Scheduled Events MTP Status		
GroupWise Post Office Agent		
Up Time: 0 Days 8 Hours 22 Minutes		
	Total	
C/S Users	0	
User Connections	0	
Physical Connections	0	
Priority Queues	0	
Normal Queues	0	
GWCheck Auto Queues	0	
GWCheck Scheduled Queues	0	
Thread Status		
	Total	Busy
C/S Handler Threads	6	0
Message Worker Threads	6	0
GWCheck Worker Threads	0	0
Message Transfer Status	Open	
Statistics		
	Total	
C/S Requests	6	
C/S Requests Pending	0	
Users Timed Out	0	
Rules Executed	0	
Users Delivered	0	
Messages Files Processed	70	
Messages Undelivered	0	
Problem Messages	0	
Users Deleted	0	
Statuses Processed	0	

For information about the agent Web consoles, see the GroupWise agent documentation:

- ◆ [“Using the POA Web Console” on page 489](#)
- ◆ [“Using the MTA Web Console” on page 617](#)
- ◆ [“Monitoring the Internet Agent through the Web Console” on page 742](#)
- ◆ [“Monitoring the WebAccess Agent through the Web Console” on page 879](#)


Polling the Agents for Updated Status Information

By default, the Monitor Agent polls the monitored agents every five minutes. You can change the default poll cycle, as described in [“Configuring Polling of Monitored Agents” on page 917](#). The time remaining until the next poll cycle is displayed in the lower left corner of the Monitor Agent console.

You can also manually poll monitored agents:

- ◆ To poll all agents, click Action > Poll All Agents.
- or
- On Linux, click Poll.
- ◆ To poll a specific agent, right-click the agent, then click Poll Agent.

- ◆ To stop polling a specific agent (for example, because the server it runs on is awaiting repairs), right-click the agent, then click Suspend Polling. You can specify a time interval for the agent to be suspended, after which polling resumes automatically. By suspending polling, you prevent repeat notifications for a problem that is already being addressed.

The suspended agent's status is listed as Suspended, accompanied by the same icon used for the Unknown status .

- ◆ To restart regular polling of an agent for which polling was suspended, right-click the agent, then click Resume Polling.

Generating Reports

You can generate reports on demand at the Monitor Agent console to help you manage message flow throughout your GroupWise system.

- ◆ [“Link Trace Report” on page 931](#)
- ◆ [“Link Configuration Report” on page 932](#)
- ◆ [“Environment Report” on page 933](#)
- ◆ [“User Traffic Report” on page 933](#)
- ◆ [“Link Traffic Report” on page 934](#)
- ◆ [“Message Tracking Report” on page 934](#)
- ◆ [“Performance Tracking Report” on page 935](#)

Link Trace Report

A link trace report enables you to follow the path a message would take between two GroupWise domains. A link trace report includes a list of all the domains through which a message would need to pass, along with their current status, link type, address, and number of messages currently queued in each domain. If any domain along the link path is closed, an error message is displayed.

If a message fails to arrive at its destination, this report can help you pinpoint its current location, so you can resolve the problem and get messages flowing smoothly again.

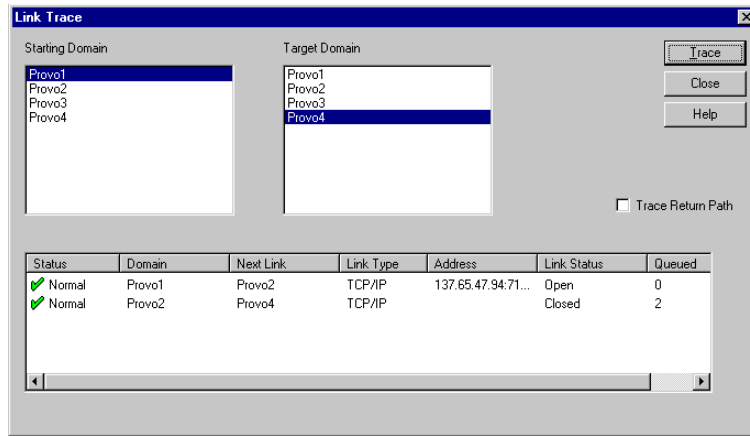
At the Windows Monitor Agent console:

- 1** Click Reports > Link Trace.

or

On Linux, click Link Trace.

- 2** Select a starting domain and a target domain.
- 3** If you want to trace the path back, which is the route status messages will take, select Trace Return Path.
- 4** Click Trace.



If any domain in the path is closed, an error message displays so you know where the problem is occurring.

- 5 When you are finished tracing links, click Close.

Link Configuration Report

A link configuration report enables you to list the links from one or more GroupWise domains to all other domains in your GroupWise system. This helps you identify inefficient link paths, loops, and unreachable domains. All domains must be open to obtain an accurate link map of your GroupWise system.

At the Windows Monitor Agent console:

- 1 Make sure all domains in your GroupWise system are open.

You cannot obtain an accurate link map of your GroupWise system if any domains are closed. For assistance with closed domains, see *“Message Transfer Agent Problems”* in *GroupWise 6.5 Troubleshooting 2: Solutions to Common Problems*.

- 2 Click Reports > Link Configuration

or

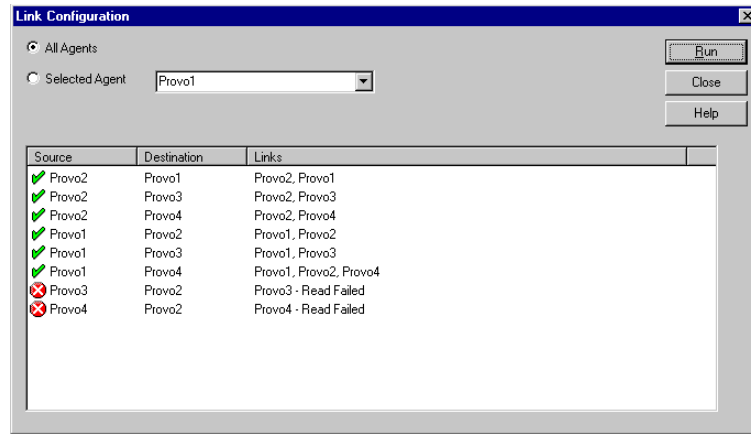
On Linux, click Link Configuration

- 3 Select All Agents

or

Select a specific agent from the drop-down list.

- 4 Click Run



The list shows what domains a message would pass through to travel from the domain in the Source column to the domain in the Destination column. If a domain displays as closed, it means that the Monitor Agent could not contact the MTA for the domain or that a loop was detected in the link configuration.

- 5 When you are finished checking links, click Close.

Environment Report

An environment report lists all monitored agents, along with each agent's location, version, IP address, port number, and operating system information. For NetWare[®] agents, the server name, CLIB version, TCP/IP version, Novell eDirectory[™] version, and the number of packet receive buffers are also listed.

At the Monitor Agent console:

- 1 Click Reports > Environment.
- 2 Scroll through the displayed information for your own use.

or

Click Send, type your e-mail address, type one or more e-mail addresses to send the environment report to, then click Send.

- 3 Click OK to close the Environment Report dialog box.

User Traffic Report

A user traffic report enables you to determine how many messages a user has sent outside his or her post office. The user traffic report lists all messages sent by a specified user during a specified date/time range, along with date, time, and size information for each message. You can also generate a user traffic report for all users whose messages pass through a selected domain.

In order for the information to be available to generate a user traffic report, you must configure the MTA to perform message logging. See [“Enabling MTA Message Logging” on page 603](#).

At the Monitor Agent console:

- 1 Click Reports > User Traffic.
- 2 Select the user's domain or the domain you want to generate a user traffic report for.
- 3 Type the GroupWise user ID that you want to create a report for.

or

Leave the field blank to create a report for all users whose messages pass through the selected domain.

- 4** If you want to restrict the report to a particular time interval, specify start and end dates and times.
- 5** Click Run.
- 6** After the results are displayed, click Save, provide a filename for the report, select the format for the report, then click OK.

Reports can be saved in comma-separated or tab-separated format to meet the needs of the program you plan to use to display and print the report. For example, you could bring the data into a spreadsheet program. If needed, you can include column headings to create an initial line in the output file that labels the contents of each column.

- 7** When you are finished generating user traffic reports, click Close.

Link Traffic Report

A link traffic report enables you to determine how many messages are passing from a selected GroupWise domain across a specified link. The link traffic report lists the total number and total size of all messages passing through the link during each hour or half hour of operation.

In order for the information to be available to generate a link traffic report, you must configure the MTA to perform message logging. See [“Enabling MTA Message Logging” on page 603](#).

At the Monitor Agent console:

- 1** Click Reports > Link Traffic.
- 2** Select the source domain of the link.

The list includes all domains that the Monitor Agent uses XML to communicate with. If the Monitor Agent must use SNMP to communicate with a domain, that domain is not included in the list.
- 3** Select the other end of the link, which could be another domain, a post office, or a gateway.
- 4** If you want to restrict the report to a particular time interval, specify start and end dates and times.
- 5** Click Run.
- 6** After the results are displayed, click Save, provide a file name for the report, select the format for the report, then click OK.

Reports can be saved in comma-separated or tab-separated format to meet the needs of the program you plan to use to display and print the report. For example, you could bring the data into a spreadsheet program. If needed, you can include column headings to create an initial line in the output file that labels the contents of each column.

- 7** When you are finished generating link traffic reports, click Close.

Message Tracking Report

A message tracking report enables you to track an individual message through your GroupWise system. The message tracking report provides information about when a message was sent, what

queues the message has passed through, and how long it spent in each message queue. If the message has not been delivered, the message tracking report shows where it is.

In order for the information to be available to generate a message tracking report, you must configure the MTAs in your GroupWise system to perform message logging. See [“Enabling MTA Message Logging” on page 603](#).

In addition, you need to determine the message ID of the message. Have the sender check the Sent Item Properties of the message in the GroupWise client. The Mail Envelope Properties field displays the message ID of the message; for example, 3AD5EDEB.31D : 3 : 12763.

At the Monitor Agent console:

- 1** Click Reports > Message Tracking.
- 2** Type the message ID of the message to track.
You can obtain the message file ID in the GroupWise client. Open the Sent Items folder, right-click the message, click Properties, then check the Mail Envelope Properties field for the message file ID; for example, 3A75BAB9.FF1 : 8 : 31642.
- 3** Select the domain where you want to start tracking.
- 4** Click Track.
- 5** When you are finished generating message tracking reports, click Close.

Performance Tracking Report

Before you can run a performance tracking report, you must configuration the Monitor Agent for performance tracking. See [“Measuring Agent Performance” on page 935](#).

Measuring Agent Performance

To test the performance of the agents in your GroupWise system, you can send performance test messages from a specially configured Monitor domain to target domains anywhere in your GroupWise system. The Monitor Agent measures the amount of time it takes for replies to return from the target domains, which lets you ascertain the speed at which messages flow through your GroupWise system.

Perform the following steps to set up agent performance testing:

- ◆ [“Setting Up an External Monitor Domain” on page 935](#)
- ◆ [“Selecting an MTA to Communicate with the Monitor Agent” on page 936](#)
- ◆ [“Configuring the Monitor Agent for Agent Performance Testing” on page 937](#)
- ◆ [“Viewing Agent Performance Data” on page 938](#)
- ◆ [“Viewing an Agent Performance Report” on page 938](#)
- ◆ [“Receiving Notification of Agent Performance Problems” on page 938](#)

Setting Up an External Monitor Domain

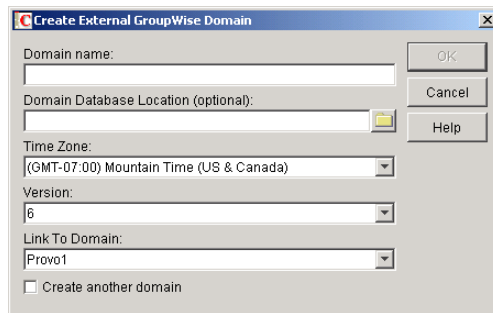
Before you can use the GroupWise Performance Testing dialog box to configure and enable GroupWise performance testing, you must create a specially configured Monitor domain and

select an MTA to receive performance test messages from the Monitor Agent. The Monitor Agent uses an external GroupWise domain as part of measuring performance.

In ConsoleOne®:

- 1 Create an external GroupWise domain.

For information about external GroupWise domains, see “[Creating an External Domain](#)” in “[Connecting to GroupWise 5.x and 6.x Systems](#)” in the *GroupWise 6.5 Multi-System Administration Guide*. By creating an external domain, you enable the Monitor Agent to approximate the round-trip time for e-mail messages to travel to recipients and for status messages to travel back to senders.



- 2 Name the external domain to reflect its role in your GroupWise system.

For example, you could name it GW Performance Tester. It does not matter which domain you link the external domain to.

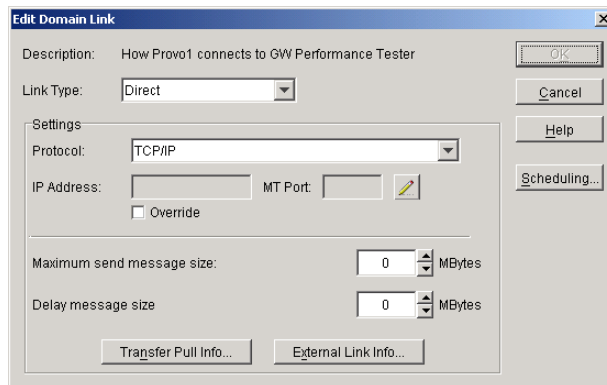
- 3 Continue with “[Selecting an MTA to Communicate with the Monitor Agent](#)” on page 936.

Selecting an MTA to Communicate with the Monitor Agent

The Monitor Agent needs to send its performance testing messages to a specific MTA in your GroupWise system. It does not matter which MTA you decide to use. It could be the MTA for the domain to which the external Monitor domain is linked.

In the Link Configuration Tool in ConsoleOne:

- 1 Configure the outbound link from the selected MTA to the external Monitor domain to be a TCP/IP link.



- 2 Click the pencil icon to provide the IP address of the server where the Monitor Agent runs.

- 3 Specify a unique port number for the MTA to use to communicate with the Monitor Agent. Click OK twice to finish modifying the link.
- 4 Exit the Link Configuration Tool to save the new link configuration information.
- 5 Continue with “[Configuring the Monitor Agent for Agent Performance Testing](#)” on page 937.

Configuring the Monitor Agent for Agent Performance Testing

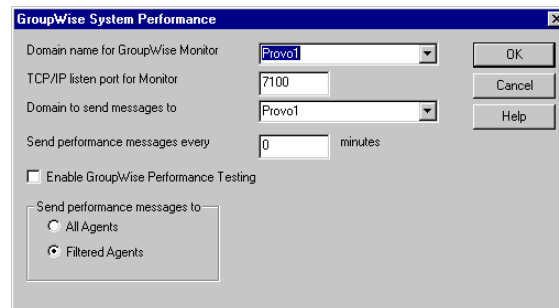
After you have created an external Monitor domain and configured a link from it to an MTA, you are ready to configure the Monitor Agent for performance testing.

At the Windows Monitor Agent console:

- 1 Click Configuration > Performance Testing.

or

On Linux, click Preferences > Setup, then scroll down to the Performance Testing section.



- 2 Fill in the fields:

Domain Name for GroupWise Monitor: Select the external Monitor domain that you configured for system performance testing.

You might need to restart the Monitor Agent in order to see the new Monitor domain in the drop-down list.

TCP/IP Listen Port for Monitor: Specify the port number where you configured the MTA to communicate with the Monitor Agent.

Domain to Send Messages To: Select the domain where the specially configured MTA is running.

The Monitor Agent directs all performance test messages to the selected domain. From there, the MTA transfers the performance test messages to the agents whose performance is being measured.

Send Performance Messages Every: Specify in minutes the time interval for the Monitor Agent to send performance test messages.

Enable GroupWise Performance Testing: Select this option to turn on performance testing. Deselect this option when you have finished your performance testing.

Send Performance Messages To: Select All Agents to send performance test messages to all domains in your GroupWise system. Select Filtered Agents to send performance test messages only to the agents currently listed at the Monitor Agent console.

- 3 Click OK to put the performance testing settings into effect.

4 Continue with [“Viewing Agent Performance Data” on page 938](#).

or

Continue with [“Receiving Notification of Agent Performance Problems” on page 938](#).

Viewing Agent Performance Data

The information gathered by the Monitor Agent through performance test messages is recorded in the Monitor history log.

At the Monitor Agent console:

- 1** Click Log > View History Files.
- 2** Select a history log file > click View.

Viewing an Agent Performance Report

A performance testing report enables you to measure how long it takes messages to travel through your GroupWise system. The performance testing report lists each domain that a performance test message was sent to, when it was sent by the Monitor Agent, and the number of seconds between when it was sent and when the Monitor Agent received a response from the tested agent.

At the Monitor Agent Console:

- 1** Click Reports > Performance Testing.
- 2** Select All Domains to generate a performance testing report for all domains in your GroupWise system.
or
Select one domain to generate a performance testing report for it.
- 3** Click Run to generate the performance testing report.

Receiving Notification of Agent Performance Problems

If you want the Monitor Agent to notify you if system performance drops to an unacceptable level, you can create a threshold to check the `mtaLastResponseTime` and `mtaAvgResponseTime` MIB variables. The average response time is a daily average that is reset at midnight. See [“Customizing Notification Thresholds” on page 920](#) for setup instructions.

Assigning Responsibility for Specific Agents

If multiple GroupWise administrators manage the agents throughout your GroupWise system, you can assign a contact for each agent. Or, in a helpdesk environment, a person can be assigned to an agent when a problem occurs. The person assigned to the agent can record notes about the functioning of the agent which are then available to other administrators.

At the Windows Monitor Agent console:

- 1** Right-click an agent in the agent status window, then click Agent Details.
or
On Linux, click the agent status link.

The screenshot shows a dialog box titled "Development.Provo1 Details". It contains the following information:

- Name: Development.Provo1
- Type: POA
- Address: 133.45.67.99
- Port: 1677
- State: Normal
- Poll Type: XML

On the right side of the dialog, there are four buttons: OK, Cancel, MIB Values, and Help. Below the main information, there are four sections:

- Thresholds:** A large empty text area.
- Suggestions:** A large empty text area.
- Assigned to:** A text input field.
- Notes:** A text area with a vertical scrollbar.

- 2** In the Assign To field, type the name of the GroupWise administrator who is responsible for this agent.

The name is displayed to the right of the agent status in the status window of the Monitor Agent console and the Monitor Web console.

- 3** In the Notes box, type any comments you might have about the agent.

If a problem with the agent occurs, the Thresholds box and the Suggestions box displays helpful information about the problem if you have set up customized thresholds, as described in [“Customizing Notification Thresholds” on page 920](#).

- 4** Click OK to save the information about who is assigned to the agent.

68

Configuring the Monitor Application

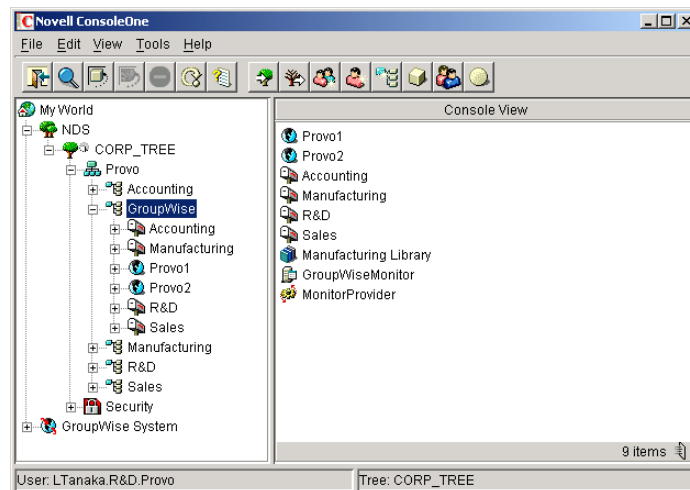
During installation, the GroupWise® Monitor Application is set up with a default configuration. However, you can use the information in the following sections to optimize the Monitor Application configuration:

- ◆ “Modifying Monitor Application Environment Settings” on page 941
- ◆ “Modifying Monitor Application Log Settings” on page 942
- ◆ “Adding or Removing Service Providers” on page 944
- ◆ “Modifying Monitor Application Template Settings” on page 945

Modifying Monitor Application Environment Settings

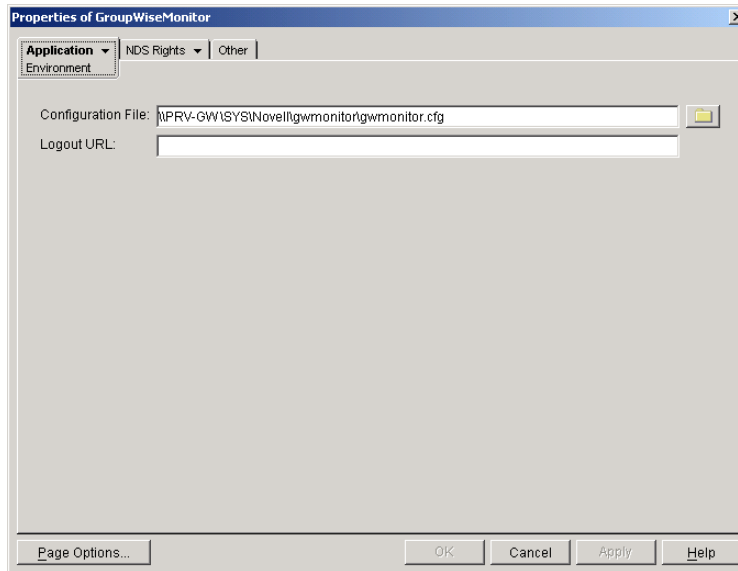
Using ConsoleOne®, you can modify the Monitor Application’s environment settings. The environment settings determine such things as the location where ConsoleOne stores the Monitor Application’s configuration file and how long the Monitor Application maintains an open session with an inactive user.

- 1 In ConsoleOne, use the Console View to browse to the Monitor Application object (named GroupWiseMonitor).



The Monitor Application object is not available in the GroupWise View.

- 2 Right-click the Monitor Application object, then click Properties to display the Environment page.



3 Modify the fields as needed:

Configuration File: The Monitor Application does not have access to Novell® eDirectory® or the GroupWise domain database (**wpdomain.db**). Therefore, ConsoleOne writes the application's configuration information to the file specified in this field. By default, this is the gwmonitor.cfg file located in the Monitor Application's home directory (**novell\gwmonitor** at the root of the Web server). On Linux, the gwmonitor.cfg file is located in the **/opt/novell/groupwise/gwmonitor** directory.

In general, you should avoid changing the location of the file. If you do change the location of the file, you need to make sure to modify the gwmonitor.cfg path in the servlets.properties file, located in the novell\servletgateway\servlets directory on a Windows server or the Java servlet directory on a NetWare® or UNIX server. If you do not, the Monitor Application continues to look for its configuration information in the old location. On Linux, do not change the location of the gwmonitor.cfg file.

Logout URL: By default, if users are required to log in to the Monitor Web console, they are returned to the login page when they log out. If desired, you can enter the URL for a different page.

4 Click OK to save the changes.

Modifying Monitor Application Log Settings

The Monitor Application logs information to log files on disk. You can control the following logging features:

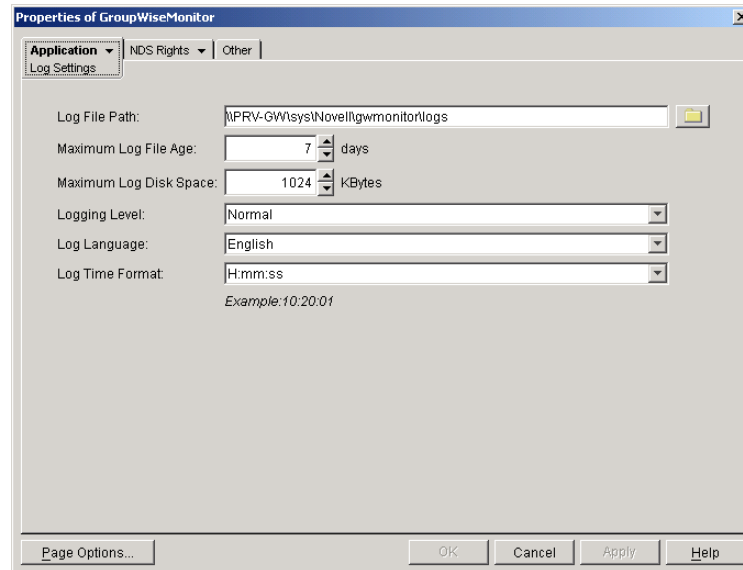
- ◆ The type of information to log
- ◆ How long to retain log files
- ◆ The maximum amount of disk space to use for log files
- ◆ Where to store log files

The Monitor Application creates a new log file each day and each time it is restarted (as part of the Web server startup). The log file is named *mmddmon.nnn*, where *mm* is the month, *dd* is the year,

and *mmn* is a sequenced log file number (001 for the first log file of the day, 002 for the second, and so forth).

To modify the log settings:

- 1 In ConsoleOne, browse to and right-click the Monitor Application object (named GroupWiseMonitor), then click Properties.
- 2 Click Application > Log Settings.



- 3 Modify the log settings as needed:

Log File Path: Specify the path to the directory where you want to store the log files.

By default, the log files are stored in the `novell\gwmonitor\logs` directory at the root of the Web server. On Linux, the log files are stored in the `/var/log/novell/groupwise/gwmon` directory.

Maximum Log File Age: Specify the number of days you want to retain the log files. The Monitor Application retains the log file for the specified number of days unless the maximum disk space for the log files is exceeded. The default age is 7 days.

Maximum Log Disk Space: Specify the maximum amount of disk space you want to use for the log files. If the disk space limit is exceeded, the Monitor Application deletes log files, beginning with the oldest file, until the limit is no longer exceeded. The default disk space is 1024 KB.

Logging Level: There are four logging levels: None, Normal, Verbose, and Diagnostic. None turns logging off; Normal displays warnings and errors; Verbose displays Normal logging plus information messages and user requests; and Diagnostic displays all possible information. The default is Normal logging. Use Diagnostic only if you are troubleshooting a problem with Monitor.

The verbose and diagnostic logging levels do not degrade Monitor Agent performance, but log files saved to disk consume more disk space when verbose or diagnostic logging is in use.

Log Language: Select the language in which you want information written to the log files. The list contains many languages, some of which the Monitor Application might not support. If you select an unsupported language, the information is written in English.

Log Time Format: Choose from the following formats to use when the Monitor Application records dates and times in the log files: *HH:mm:ss:SS*, *MM/dd: H:mm:ss.SS*, or *dd/MM: H:mm:ss.SS*. *H* and *HH* represent hours, *mm* represents minutes, *ss* and *SS* represent seconds, *MM* represents months, and *dd* represents days.

- 4 Click OK to save the log settings.

Adding or Removing Service Providers

The Monitor Application receives requests from Monitor Web console users and then passes the requests to the appropriate service provider. The service provider fills the requests and returns the required information to the Monitor Application. The Monitor Application merges the information into the appropriate template and displays it to the user.

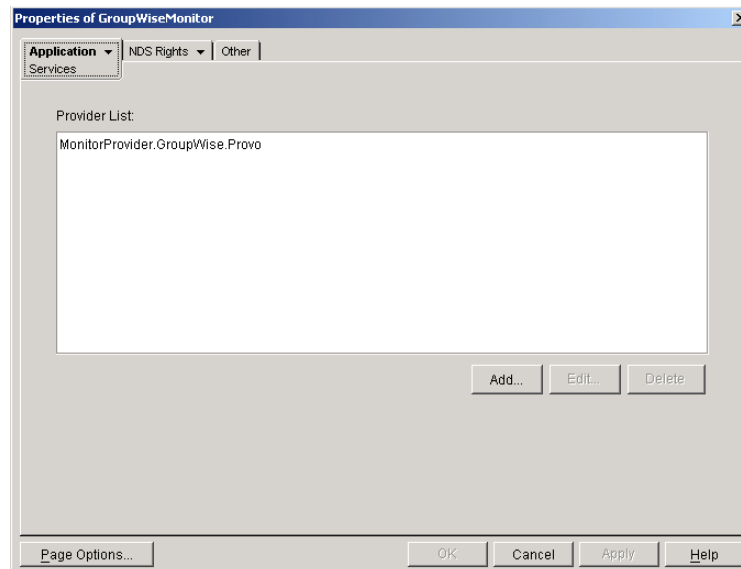
To function properly, the Monitor Application must know which service providers are available. The Monitor service provider communicates with the Monitor Agent to fill Monitor Web console requests. The Monitor service provider is installed and configured at the same time as the Monitor Application.

You can disable the Monitor service by removing the Monitor service provider. If you've created new service providers to expose additional services through GroupWise Monitor, you must define those service providers so that the Monitor Application knows about them.

To define service providers:

- 1 In ConsoleOne, right-click the Monitor Application object (named GroupWiseMonitor), then click Properties.
- 2 Click Application > Services.

The Provider List displays all service providers that the Monitor Application is configured to use.



- 3 Choose from the following options:

Add: To add a service provider to the list, click Add, browse to and select the service provider's object, then click OK.

Edit: To edit a service provider's information, select the provider in the list, then click Edit.

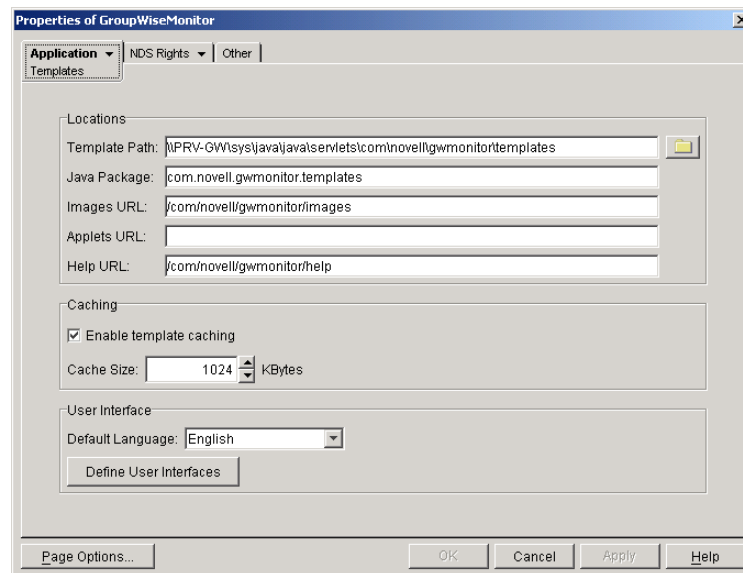
Delete: To remove a service provider from the list, select the provider, then click Delete.

- 4 Click OK to save the changes.

Modifying Monitor Application Template Settings

When the Monitor Application receives information from a service provider, it merges the information into the appropriate Monitor template before displaying the information to the Monitor Web console user. Using ConsoleOne, you can modify the Monitor Application's template settings. The template settings determine such things as the location of the templates, the maximum amount of server memory to use for caching the templates, and the default template language.

- 1 In ConsoleOne, browse to and right-click the Monitor Application object (named GroupWiseMonitor), then click Properties.
- 2 Click Applications > Templates to display the Templates page.



- 3 Modify the fields as needed:

Template Path: Select the location of the template base directory. The template base directory contains the subdirectories (simple, frames, hdml, and wml) for each of the templates provided with GroupWise Monitor. If you create your own templates, you need to place the templates in a new subdirectory in the template base directory.

On a NetWare[®] server with the Novell Servlet Gateway, the default installation directory is `java\servlets\com\novell\gwmonitor\templates`.

On a Windows server with the Novell Servlet Gateway, the default installation directory is `novell\java\servlets\com\novell\gwmonitor\templates`.

On a NetWare or Windows server with Tomcat, the default installation directory is `tomcat_dir\webapps\ROOT\web-inf\classes\com\novell\gwmonitor\templates`.

On a Linux server with Tomcat, the default installation directory is `/var/opt/novell/tomcat/webapps/gw/WEB-INF/classes/com/novell/gwmonitor/templates`.

Java Package: Specify the Java package that contains the template resources used by the Monitor Application. The default package is `com.novell.gwmonitor.templates`.

Images URL: Specify the URL for the GroupWise Monitor image files. These images are merged into the templates along with the GroupWise information. This URL must be relative to the Web server's document root directory. On NetWare and Windows, the default relative URL is `com\novell\gwmonitor\images`. On Linux, the default relative URL is `/gw/com/novell/gwmonitor/images`.

Applets URL: The Monitor Application does not currently use applets.

Help URL: Specify the URL for the GroupWise Monitor Help files. The default installation directory is the `com\novell\gwmonitor\help` directory under the Web server's document root directory.

Enable Template Caching: To speed up access to the template files, the Monitor Application can cache the files in memory. Select this option to turn on template caching.

Cache Size: Select the maximum amount of memory, in kilobytes, you want to use when caching the templates. The default cache size, 1024 KB, is sufficient to cache all templates shipped with GroupWise Monitor. If you modify or add templates, you can turn on Verbose logging on the Monitor Application object Log Settings page to view the size of the template files. Using this information, you can then change the cache size appropriately.

Default Language: Select the language to use when displaying the initial Monitor Web console page.

Define User Interfaces: GroupWise Monitor supports Web browsers on many different devices (for example, computers and wireless telephones). Each device supports specific content types such as HTML, HDML, and WML. When returning information to a device's Web browser, the Monitor Application must merge the information into a set of templates to create an interface that supports the content type required by the Web browser.

GroupWise Monitor ships with several predefined user interfaces. These interfaces support Web browsers that require HTML, HDML, and WML content types. Click the User Interface button to view, add, modify, or delete user interfaces.

- 4 Click OK to save the new template settings.

69

Using the Monitor Web Console

The Monitor Web console displays GroupWise® agent status anywhere a browser and a connection to the Internet are available.

- ◆ “Displaying the Monitor Web Console” on page 947
- ◆ “Monitoring Agents at the Monitor Web Console” on page 947
- ◆ “Managing Links” on page 950
- ◆ “Searching for Agents” on page 951

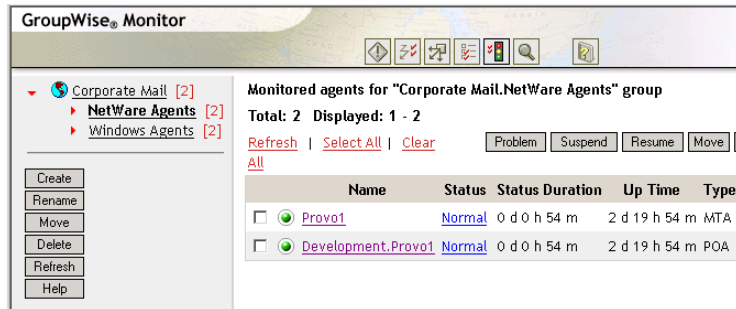
Displaying the Monitor Web Console

- 1 Make sure that your Web server is running.
- 2 To display the Monitor Web console, enter the Monitor URL in your Web browser:

Linux: `http://network_address/gwmon/gwmonitor`

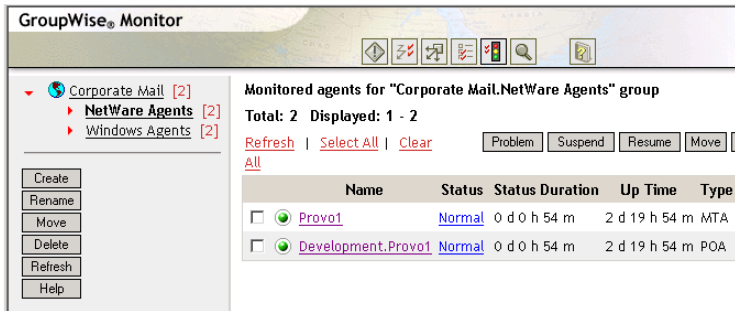
Windows: `https://network_address/servlet/gwmonitor`

where *network_address* represents the IP address or hostname of the server where the Monitor Agent is running.









Monitoring Agents at the Monitor Web Console

The Monitor Web console lists all GroupWise agents that the Monitor agent is polling for status information.



Features of the Monitor Web console are available on buttons at the top of the Monitor page.

Button	Feature
	Problems
	Link Trace
	Link Configuration
	Global Options
	States
	Search

Click an agent group to display all monitored agents in the group. Click the Problem button to display only those agents whose status is other than Normal in the agent group. Click the Problems icon to display all agents in your GroupWise system whose status is other than Normal.

Click the status of an agent to display agent status details.

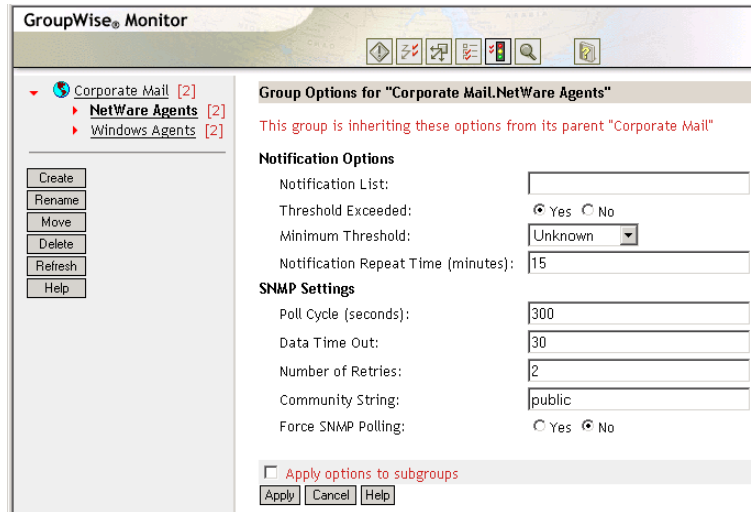
Click an agent in the list to open its agent Web console. For information about the agent Web consoles, see [“Viewing an Agent Web Console” on page 930](#).

Click Refresh to update the agent status information. To modify the default poll cycle, see [“Configuring Polling of Monitored Agents” on page 917](#).

Changing Monitor Agent Configuration Settings at the Monitor Web Console

Some Monitor Agent configuration settings can be changed at the Monitor Web console.

- 1 To change settings that apply to a particular agent group, click the agent group, then click Options.

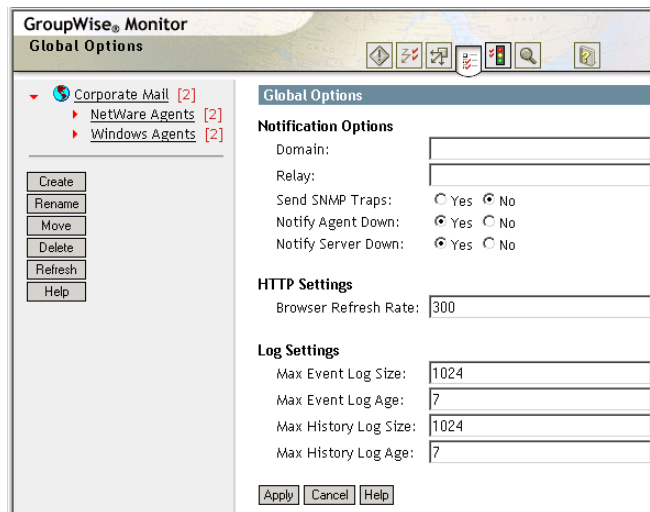


2 Set the options as needed, then click Apply.

For information about the options, see the following sections that describe this functionality for the Windows Monitor Agent console:

- ◆ [“Configuring E-Mail Notification of Agent Problems” on page 918](#)
- ◆ [“Configuring Polling of Monitored Agents” on page 917](#)
- ◆ [“Configuring the Monitor Agent for SNMP” on page 916](#)

3 To change settings that apply to the Monitor Agent itself, rather than to a group of monitored agents, click the Global Options icon.



4 Set the global options as needed, then click Apply.

For information about the options, see the following sections that describe this functionality for the Windows Monitor Agent console:

- ◆ [“Configuring E-Mail Notification of Agent Problems” on page 918](#)
- ◆ [“Configuring SNMP Trap Notification of Agent Problems” on page 923](#)
- ◆ [“Configuring the Monitor Agent for HTTP” on page 915](#)
- ◆ [“Configuring Monitor Agent Log Settings” on page 925](#)

Managing Links

The Monitor Web console can help you manage links throughout your GroupWise system.

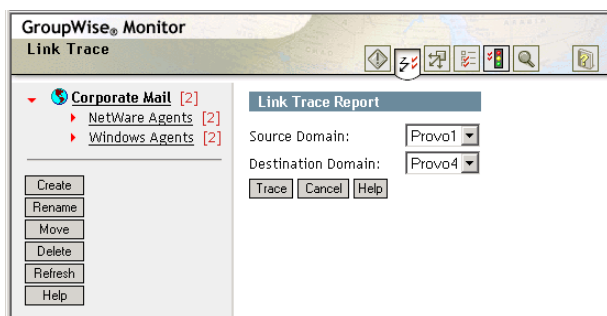
- ◆ “Tracing a Link at the Monitor Web Console” on page 950
- ◆ “Checking Links Configuration at the Monitor Web Console” on page 950

Tracing a Link at the Monitor Web Console

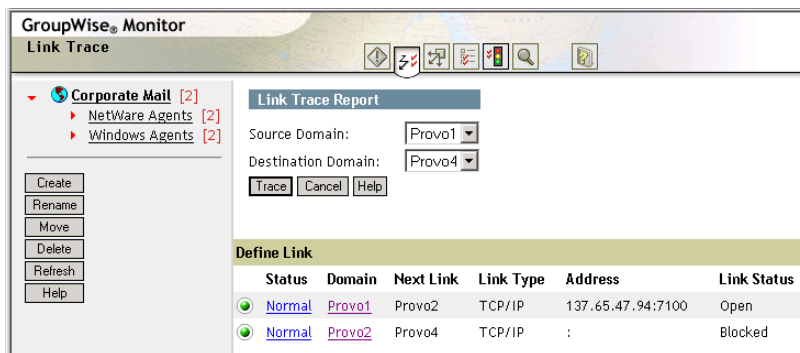
When you trace a link, you follow the path a message would take when travelling between two GroupWise domains. If a message fails to arrive at its destination, this feature helps you pinpoint its current location, so you can resolve the problem and get messages flowing again.

At the Monitor Web console:

- 1 Click the Link Trace icon.



- 2 Select a source domain, select a destination domain, then click Trace.



If any domain in the path is closed, the link trace shows where the problem is occurring.

Checking Links Configuration at the Monitor Web Console

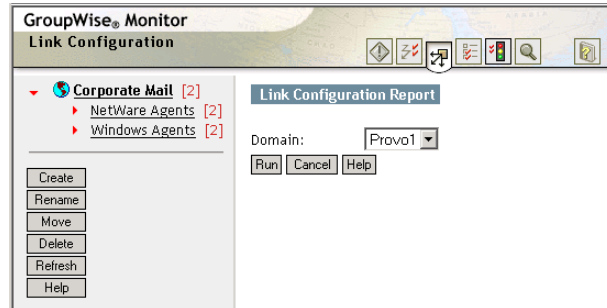
When you check link configuration, you list the links from a GroupWise domain to all other domains in your GroupWise system. This helps you identify inefficient link paths, loops, and unreachable domains.

At the Monitor Web console:

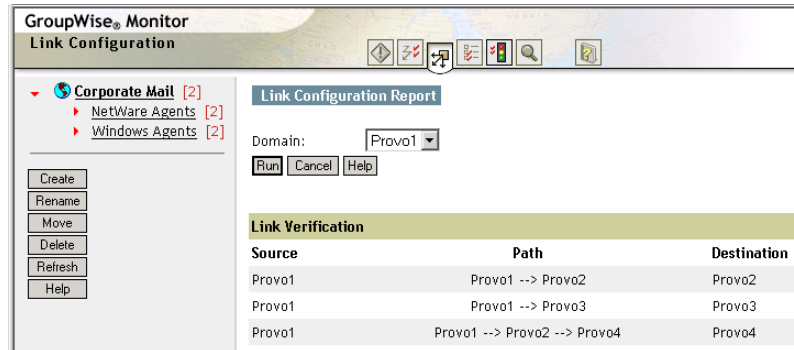
- 1 Make sure all domains in your GroupWise system are open.

You cannot obtain an accurate link map of your GroupWise system if any domains are closed. For assistance with closed domains, see “[Message Transfer Agent Problems](#)” in *GroupWise 6.5 Troubleshooting 2: Solutions to Common Problems*.

- 2 Click the Link Configuration icon.



- 3 Select a domain from the drop-down list.
- 4 Click Run.



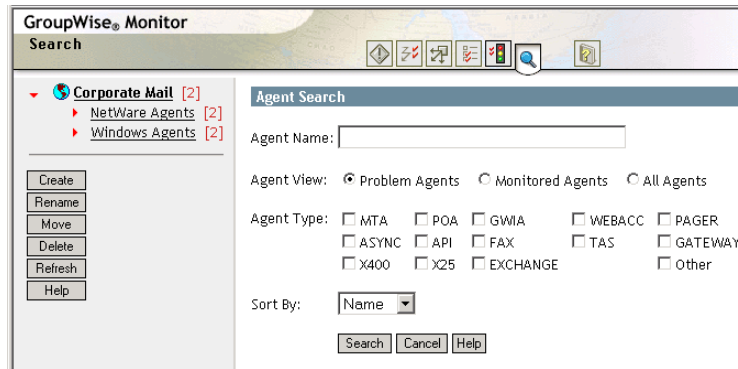
The list shows what domains a message would pass through to travel from the domain in the Source column to the domain in the Destination column.

Searching for Agents

If you monitor a large number of agents, the list displayed in the Monitor Web console can become very long. You can easily search for an individual agent or for a group of related agents.

At the Monitor Web console:

- 1 Click the Search icon.



2 Type the name of an agent.

or

Select Problems to list all agents whose status is other than Normal.

or

Select one or more types of agent to list.

3 Select the number of instances you want listed at one time.

4 Click Search.

The results display on the Search page with the same functionality as is available on the regular Monitor Web console pages.

70

Comparing the Monitor Agent Consoles

Many aspects of agent monitoring are available in one or more of the Monitor Agent consoles. The table below summarizes agent monitoring features and where they are available.

Task	Windows Monitor Agent Console	Monitor Agent Web Console	Monitor Web Console
Selecting Agents to Monitor	Yes	Yes	No
Creating and Managing Agent Groups	Yes	No	Yes
Viewing All Agents	Yes	Yes	Yes if not in groups
Viewing Problem Agents	Yes	Yes	Yes
Viewing an Agent Console	Yes	No	No
Viewing an Agent Web Console	Yes	Yes	Yes
Searching for Agents	No	No	Yes
Assigning Responsibility for Specific Agents	Yes	Yes	Yes
Configuring the Monitor Agent for HTTP	Yes	Yes	Yes
Configuring the Monitor Agent for SNMP	Yes	Yes	Yes
Configuring Polling of Monitored Agents	Yes	Yes	Yes
Configuring E-Mail Notification of Agent Problems	Yes	Yes	Yes
Configuring Audible Notification of Agent Problems	Yes	No	No
Configuring SNMP Trap Notification of Agent Problems	Yes	Yes	Yes
Configuring Authentication and Intruder Lockout for the Monitor Web Console	Yes	Authentication: Yes Intruder Lockout: No	No
Configuring Monitor Agent Log Settings	Yes	Yes	Yes
Generating Reports	Yes	Yes	Yes
Link Trace Report	Yes	Yes	Yes
Link Configuration Report	Yes	Yes	Yes

Environment Report	Yes	Yes	No
User Traffic Report	Yes	Yes	No
Link Traffic Report	Yes	Yes	No
Message Tracking Report	Yes	Yes	No
Performance Tracking Report	Yes	Yes	No

71

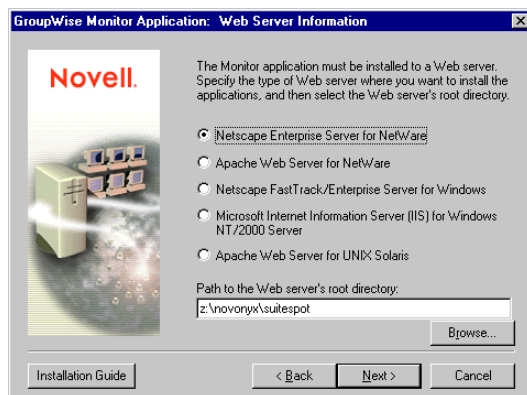
Creating a PQA File for the Monitor Web Console

You can use the GroupWise® Monitor Installation program on Windows to create a Web Clipping Application (PQA), also referred to as a Palm Query Application, to enable Palm OS device users to log in to the Monitor Web console.

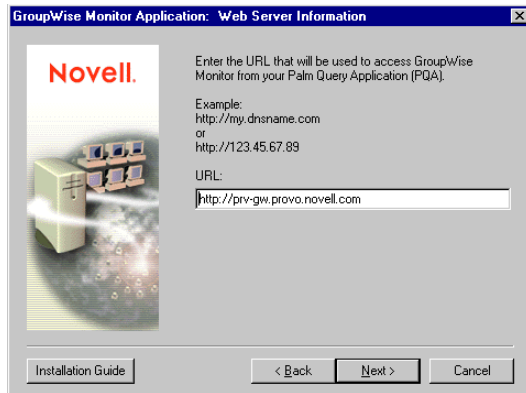
The Web Clipping Application, named gwmon.pqa, includes the URL required to connect to your GroupWise Monitor installation, a Login page, an About Novell GroupWise page, and the images used when displaying the Monitor Web console on the Palm OS device.

To create a gwmon.pqa file:

- 1 If you've already created another gwmon.pqa file that you want to keep, make sure it is not in the Web server's *doc_root_directory*\com\novell\gwmonitor\palm\en directory. The Installation program overwrites any gwmon.pqa file in the directory.
- 2 At a Windows workstation, run setup.exe /pqa from the *\admin\monitor* directory on the *GroupWise 6.5 Administrator* CD or the GroupWise software distribution directory
- 3 Select the language for the Installation program, then accept the License Agreement to display the following dialog box.



- 4 Select the type of Web server where the Monitor Web console is installed, make sure the path to the Web server's root directory is correct, then click Next.



5 Specify the URL you want included in the .pqa file. For example:

```
http://groupwise.novell.com
```

The Installation program automatically appends /servlet/gwmon to the URL so that users are directed to the Monitor Web console login page. For example, using the URL above, the Installation program would create the following URL in the gwmon.pqa file:

```
http://grouppwise.novell.com/servlet/gwmon
```

As you determine the URL, keep in mind the following:

- ◆ If the Web server uses SSL, you should change http to https.
- ◆ If you are using a proxy server, you need to enter the proxy server's address.
- ◆ The Web clipping proxy server (gateway) does not currently support challenge and response authentication. Therefore, you need to ensure that the Web server is not configured to require basic challenge and response authentication, or at least is configured not to require this authentication for the URL defined in the gwmon.pqa file.

6 Click Next to create the .pqa file, then click Finish.

The gwmon.pqa file is created in the Web server's `doc_root_directory\com\novell\gwmonitor\palm\en` directory. You can distribute it to your Palm OS device users just as you would any other .pqa file.

72 Using Monitor Agent Switches

GroupWise® Monitor Agent startup switches must be used on the command line when you start the Monitor Agent, or in a script or batch file created to start the Monitor Agent. The Monitor Agent does not have a startup file for switches.

Linux Monitor Agent	Windows Monitor Agent
--help	/help
--home	/home
--httpagentpassword	/httpagentpassword
--httpagentuser	/httpagentuser
--httpcertfile	/httpcertfile
--httpmonpassword	/httpmonpassword
--httpmonuser	/httpmonuser
--httpport	/httpport
--httpssl	/httpssl
--ipa	/ipa
--ipp	/ipp
--lang	/lang
--log	/log
--pollthreads	/pollthreads
--proxy	/proxy

/help

Displays the Monitor Agent startup switch Help information. When this switch is used, the Monitor Agent does not start.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--help	/help

/home

Specifies a domain directory, where the Monitor Agent can access a domain database ([wpdomain.db](#)). From the domain database, the Monitor Agent can determine which agents to monitor, what usernames and passwords are necessary to access them, and so on.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	<code>--home /directory</code>	<code>/home-[svr^][vol:]\dir</code> <code>/home-\\svr^vo\dir</code> <code>/home-[drive:]\dir</code> <code>/home-\\svr\sharename\dir</code>
Example:	<code>--home /gwsystem/provo2</code>	<code>/home-\provo2</code> <code>/home-mail:\provo2</code> <code>/home-server2\mail:\provo2</code> <code>/home-\\server2\mail\provo2</code> <code>/home-\provo2</code> <code>/home-m:\provo2</code> <code>/home-\\server2\c\mail\provo2</code>

See also [/ipa](#) and [/ipp](#).

/httpagentpassword

Specifies the password for the Monitor Web console to prompt for before allowing GroupWise agent status information to be displayed in your Web browser. Do not use an existing Novell eDirectory password because the information passes over the insecure connection between your Web browser and the Monitor Agent. See “[Configuring Authentication and Intruder Lockout for the Monitor Web Console](#)” on page 924.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	<code>--httpagentpassword <i>unique_password</i></code>	<code>/httpagentpassword-<i>unique_password</i></code>
Example:	<code>--httpagentpassword AgentWatch</code>	<code>/httpagentpassword-AgentWatch</code>

See also [/httpagentuser](#).

/httpagentuser

Specifies the username for the Monitor Web console to prompt for before allowing GroupWise agent status information to be displayed in your Web browser. Providing a username is optional. Do not use an existing eDirectory username because the information passes over the insecure connection between your Web browser and the Monitor Agent. See “[Configuring Authentication and Intruder Lockout for the Monitor Web Console](#)” on page 924.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--httpagentuser <i>unique_username</i>	/httpagentuser- <i>unique_username</i>
Example:	--httpagentuser MonWebConsole	/httpagentuser-MonWebConsole

See also [/httpagentpassword](#).

/httpcertfile

Specifies the full path to the public certificate file used to provide secure SSL communication between the Monitor Agent and the Monitor Web console displayed in your Web browser. See “[Configuring Authentication and Intruder Lockout for the Monitor Web Console](#)” on page 924.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--httpcertfile <i>/dir/file</i>	/httpcertfile-[<i>drive:</i>] <i>dir\file</i> /httpcertfile-\\ <i>svr\sharename\dir\file</i>
Example:	--httpcertfile /certs/gw.crt	/httpcertfile- <i>lssl\gw.crt</i> /httpcertfile- <i>m:\ssl\gw.crt</i> /httpcertfile-\\ <i>server2\c\ssl\gw.crt</i>

See also [/httpssl](#).

/httpmonpassword

Specifies the password for the Monitor Web console to prompt for before allowing a user to display the Monitor Web console. Do not use an existing Novell® eDirectory™ password because the information passes over the insecure connection between your Web browser and the Monitor Agent. See “[Configuring Authentication and Intruder Lockout for the Monitor Web Console](#)” on page 924.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--httpmonpassword <i>unique_password</i>	/httpmonpassword- <i>unique_password</i>
Example:	--httpmonpassword WatchIt	/httpmonpassword-WatchIt

See also [/httpmonuser](#).

/httpmonuser

Specifies the username for the Monitor Web console to prompt for before allowing a user to display the Monitor Web console. Providing a username is optional. Do not use an existing eDirectory username because the information passes over the insecure connection between your

Web browser and the Monitor Agent. See “[Configuring Authentication and Intruder Lockout for the Monitor Web Console](#)” on page 924.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--httpmonuser <i>unique_username</i>	/httpmonuser- <i>unique_username</i>
Example:	--httpmonuser MonAdmin	/httpmonuser-MonAdmin

See also [/httpmonpassword](#).

/httpport

Sets the HTTP port number used for the Monitor Agent to communicate with your Web browser. The default is 8200; the setting must be unique. See “[Configuring the Monitor Agent for HTTP](#)” on page 915.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--httpport <i>port_number</i>	/httpport- <i>port_number</i>
Example:	--httpport 8201	/httpport-9200

/https

Sets the availability of secure SSL communication between the Monitor Agent and the Monitor Web console displayed in your Web browser. Valid values are enabled and disabled. See “[Configuring Authentication and Intruder Lockout for the Monitor Web Console](#)” on page 924.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--https <i>setting</i>	/https- <i>setting</i>
Example:	--https enabled	/https-enabled

See also [/httpcertfile](#).

/ipa

Specifies the network address (IP address or DNS hostname) of a server where an MTA is running. The Monitor Agent can communicate with the MTA to obtain information about agents to monitor.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--ipa <i>network_address</i>	/ipa- <i>network_address</i>

	Linux Monitor Agent	Windows Monitor Agent
Example:	--ipa 172.16.5.19 --ipa server2	/ipa-172.16.5.20 /ipa-server3

See also [/ipp](#).

/ipp

Specifies the TCP port number associated with the network address of an MTA with which the Monitor Agent can communicate to obtain information about agents to monitor. Typically, the MTA listens for service requests on port 7100.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--ipp <i>port_number</i>	/ipp- <i>port_number</i>
Example:	--ipp 7110	/ipp-7111

See also [/ipa](#).

/lang

Specifies the language to run the Monitor Agent in, using a two-letter language code as listed below. You must install the Monitor Agent in the selected language in order for the Monitor Agent to display in the selected language.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--lang <i>code</i>	/lang- <i>code</i>
Example:	--lang de	/lang-fr

The table below lists the valid language codes. Contact your local Novell sales office for information about language availability.

Language	Language Code	Language	Language Code
Arabic	AR	Hungarian	MA
Czechoslovakian	CS	Italian	IT
Chinese-Simplified	CS	Japanese	NI
Chinese-Traditional	CT	Korean	KR
Danish	DK	Norwegian	NO
Dutch	NL	Polish	PL

Language	Language Code	Language	Language Code
English-United States	US	Portuguese-Brazil	BR
Finnish	SU	Russian	RU
French-France	FR	Spanish	ES
German-Germany	DE	Swedish	SV
Hebrew	HE	Turkish	TR

/log

Specifies the full path of the directory where the Monitor Agent writes its log files. On Linux, the default directory is `/var/log/novell/groupwise/gwmon`. On Windows, the default is the GroupWise Monitor installation directory (typically `c:\gwmon`). See “[Configuring Monitor Agent Log Settings](#)” on page 925.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	<code>--log /dir/file</code>	<code>/log-[drive:]dir/file</code> <code>/log-\\svr\sharename\dir/file</code>
Example:	<code>--log /opt/novell/groupwise/agents/logs</code>	<code>/log-gw\logs</code> <code>/log-m:\gw\logs</code> <code>/log-\\server2\c\gw\logs</code>

/pollthreads

Specifies the number of threads that the Monitor Agent uses for polling the agents for status information. Valid values range from 1 to 32. The default is 20. See “[Configuring Polling of Monitored Agents](#)” on page 917.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	<code>--pollthreads number</code>	<code>/pollthreads-number</code>
Example:	<code>--pollthreads 10</code>	<code>/pollthreads-32</code>

/proxy

Routes all communication through the Monitor Agent and the Monitor Application (on the Web server). As long as the Web server can be accessed through the firewall, the Monitor Web console can receive information about all GroupWise agents that the Monitor Agent knows about. Without `/proxy`, the Monitor Web console cannot communicate with the GroupWise agents through a firewall. See “[Configuring Proxy Service Support for the Monitor Web Console](#)” on page 925.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	<code>--help</code>	<code>/help</code>