Installing the GroupWise Agents

The updated GroupWise®agents in the GroupWise 5.5 Enhancement Pack provide significant new functionality, including running the NT agents as NT services, starting the NLM™ agents in protected mode on NetWare® 5, monitoring the agents from your web browser, and improving performance and security for Remote client users.

SYSTEM REQUIREMENTS

You should already be running the GroupWise 5.5 agents before you install and run the updated agents provided in the Enhancement Pack. The system requirements for the updated agents are the same as for the standard 5.5 agents, as described in the *GroupWise 5.5 Agent Configuration Guide* at:

http://www.novell.com/groupwise/administration/gw55/us/gwagents.html

BASIC AGENT INSTALLATION

To install the updated GroupWise agents,

1. Run SETUP.EXE at the root of the Enhancement Pack CD > click Install Products > GroupWise Agents.
2. Follow the standard agent installation instructions provided in the *GroupWise 5.5 Agent Configuration Guide* cited above.

This *Quick Start* card provides additional instructions for agent features that are new in the Enhancement Pack.

INSTALLING THE NT AGENTS AS SERVICES

To install the GroupWise agents for Windows NT* as NT services,

1. Run SETUP.EXE at the root of the Enhancement Pack CD > click Install Products > click GroupWise Agents.
2. Follow the on-screen instructions, paying special attention to the dialog boxes pertaining to the NT agents as services, as described in Steps 3 through 7 below.
3. In the Install/Uninstall dialog box, note that Install is selected by default > click Next.

   The Uninstall option is new with the Enhancement Pack. If you want to remove the NT agents as services from an NT server, you must rerun the agent installation program and

select Uninstall. Simply deleting the agent software from the NT server will not properly uninstall the NT agents if they have been installed as services.

4. In the Installation Path dialog box, browse to and select the agent installation path > select Install as NT Services > click Next.

5. In the Domains / Post Offices dialog box, add the information for the domain and/or post office to be serviced by the NT agents > click OK when finished.

    This information helps the agent installation program create customized startup files for the agents. Even if startup files have already been created for existing agents, you must still select the domain and/or post office to be serviced in order to install the updated agents as NT services.

6. In the NT Service Information dialog box, set the NT service configuration options as needed for the NT agents > click OK.

    For an optimal installation, the NT agents should run on the same NT server where the domain and/or post office is located. Accept the default of Use Local System Account. If you want the standard GroupWise agent operation screen to appear on the NT desktop of the server, select Allow Service to Interact with Desktop.

    If you plan to run the NT agents as services on a server other than where the domain and/or post office is located, specify the NT user account and password the NT agents can use to log in to the server where the domain and/or post office is located. If the domain and/or post office is located on a NetWare server, the NT user must also be an NDS™ user so it can authenticate to the server where the domain and/or post office is located. Installing agents on servers other than where the domain and/or post office is located is not recommended because it increases network traffic and slows down agent performance.

    If you select Automatic as the startup type, you must still start the agents manually the first time.

7. In the Installation Complete dialog box, click Finish.

    The agent installation program automatically establishes NT service names for the agents and records the names in the agent startup files using the /NTServiceName switch. Do not modify the service name or remove this switch from the startup files.

8. To start the GroupWise NT agents as services for the first time, from the NT desktop click Start > Settings > Control Panel > Services > select the agent service > click Start.

9. Manage the GroupWise NT agents just as you would any other NT services.

    For example, you can change the service configuration settings for the agents. From the NT desktop, click Start > Settings > Control Panel > Services > select the agent service > click Startup > modify the settings as needed > click OK.

INSTALLING THE NLM AGENTS TO START IN PROTECTED MODE

To install the NLM agents so they start in protected mode,

1. Run SETUP.EXE at the root of the Enhancement Pack CD > click Install Products > click GroupWise Agents.
2. Follow the on-screen instructions, paying special attention to the dialog boxes pertaining to running the agents in protected mode, as described in Steps 3 and 4 below.
3. In the Installation Path dialog box, browse to and select any directory on the NetWare server where sufficient disk space is available.

   For easiest agent startup, add the selected directory to the server search path.

4. In the Installation Complete dialog box, select Launch GroupWise Agents Now > select Launch in Protected Mode > click Finish.

   To ensure that the agents always start in protected mode, edit the AUTOEXEC.NCF file so that the agents are started with the following command:

   ```
   protect grpwise.ncf
   ```

SETTING UP THE AGENT WEB CONSOLE

To install the GroupWise agents so they can be monitored from your web browser,

1. Run SETUP.EXE at the root of the Enhancement Pack CD > click Install Products > click GroupWise Agents.
2. Follow the on-screen instructions, paying special attention to the dialog boxes pertaining to the agent web console, as described in Steps 3 and 4 below.
3. In the Web Console Information dialog box, notice that Enable Web Console is selected by default. To prevent unauthorized viewing of agent status, provide a unique user name and password > click Next.

   The agent will prompt for the specified user name and password before allowing status information to be displayed in a web browser. The user name and password are recorded in the agent startup file using the /HTTPUser and /HTTPPassword switches. Do not use an NDS user name and password because the information passes over the insecure connection between the agent and your browser.

4. In the Domains / Post Offices dialog box, add the information for each domain and/or post office > specify a unique HTTP port for each agent > click OK when finished.

   This information helps the agent installation program create customized startup files for the agents, including a customized /HTTPPort switch for each agent.

5. In the Installation Complete dialog box, select Launch GroupWise Agents Now > click Finish.

6. To monitor an agent from your web browser, view the URL where the agent is located by supplying the IP address and port number. For example,

```
http://123.456.78.90:1677
http://123.456.78.90:7100
http://123.456.78.90:2800
```

When viewing an agent, you can specify either its standard TCP port or the HTTP port you specified during installation.

To change the rate at which an agent refreshes the status information, set the /HTTPRefresh switch in the agent startup file. Specify the number of seconds between refreshes. The default is 60 seconds.

GETTING THE MOST FROM THE AGENT WEB CONSOLE

The agent web console displays all information presented in the standard agent operation screens, plus significant new information and functionality. From the agent web console, you can:

- Identify closed links

- Review agent configuration settings

- Check server configuration

- Search and filter agent log files

- Monitor message queues (MTA only)

- Track messages (MTA only)

- List scheduled events (POA only)

- List client/server user connections (POA only)

To easily monitor many agents from a single location, use the GroupWise Monitor provided in the Enhancement Pack. The help provided with GroupWise Monitor explains in more detail how to use the new agent monitoring features available in the agent web console. To view the *GroupWise Monitor Quick Start* card, run SETUP.EXE from the root of the CD > click Install Products > click GroupWise Monitor > click View Quick Start Card.

IMPROVING PERFORMANCE FOR REMOTE CLIENT USERS

The MTA provided in the Enhancement Pack has the capability of re-directing GroupWise Remote client requests to other MTAs and POAs. The GroupWise client provided in the Enhancement Pack can establish a client/server connection to an MTA across the Internet, eliminating the queuing and polling process used by the standard 5.5 Remote client. The result

is significantly improved performance for Remote client users, similar to a live network connection.

To configure the MTA for this new Live Remote feature, add the following switches to the MTA startup file:

/liveremote-unique_TCP_port_number

This switch turns on re-direction of Remote client requests and provides the TCP port on which the MTA listens for Remote client requests.

/lrconn-maximum_connections

This switch specifies the maximum number of simultaneously connected Remote client users the MTA can accept. The default is 25.

In order for Live Remote to work throughout your GroupWise system, all links between the Remote client user and his or her post office must be TCP/IP links.

In order for Remote client users to use Live Remote feature, you must provide them with the IP address and TCP port of the MTA to connect to so they can modify the Remote connection. In the Remote client, users need to click Accounts > Account Options > select the Remote account > click Properties > Connection > Connect To > New > select TCP/IP > click OK > provide a name for the new Remote connection, along with the IP address and TCP port for the MTA that is providing the live remote functionality > click OK.

IMPROVING SECURITY FOR CLIENT USERS

The POA provided in the Enhancement Pack has the capability of detecting system break-in attempts in the form of repeated unsuccessful logins. This can be especially helpful when allowing Remote client users to establish client/server connections to MTAs in your system. To enable this security feature, add the following switches to the POA startup file.

/intruderlockout

This switch turns on intruder lockout processing, using defaults that can be overridden by the additional switches detailed below.

/incorrectloginattempts-number

This switch sets the number of unsuccessful attempts after which lockout will occur. The default is 5 attempts; valid values range from 3 to 10.

/attemptsresetinterval-minutes

This switch sets the length of time during which unsuccessful attempts are counted, leading to lockout. The default is 30 minutes; valid values range from 15 to 60.

/lockoutresetinterval-*minutes*

This switch sets the length of time the user login is disabled. The default is 30 minutes; the minimum setting is 15; there is no maximum setting. The login can also be manually re-enabled in NetWare Administrator in the GroupWise Account page of the User object. If the /lockoutresetinterval is set to 0 (zero), the login can only be re-enabled manually through NetWare Administrator.

LEGAL INFORMATION