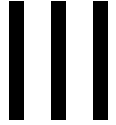


Remote Management



The Remote Management component of Novell® ZENworks® 7 Server Management gives you the ability to manage remote servers from the management console. You can use ZENworks 7 Server Management to remotely manage Novell NetWare® 5.1/6/6.5 or Windows® 2000/2003 servers.

Remote Management can save you and your organization time and money. For example, you or your organization's help desk can analyze and remote fix server problems without having to visit the server, which reduces problem resolution times and increases productivity.

This documentation contains following sections:

- ♦ [Chapter 19, “Remote Management for NetWare Servers,” on page 795](#)
- ♦ [Chapter 20, “Remote Management for Windows Servers,” on page 805](#)
- ♦ [Appendix P, “Documentation Updates,” on page 829](#)

Remote Management for NetWare Servers

19

The Java*-based remote console utility (RConsoleJ) for Novell® ZENWorks® 7 Server Management lets you control a Novell NetWare® server and perform the following tasks:

- ♦ Use console commands as you would at the server console
- ♦ Use NLM™ programs as you would at the server console (for example, `edit.nlm` to edit files)
- ♦ Send console commands in the server's native language from the RConsoleJ Client using Buffer Input
- ♦ Control the server from another server that is using RConsoleJ
- ♦ Upgrade a NetWare server (text-based UI only)
- ♦ Secure Socket Layer (SSL) based secure session

This section contains the following topics:

- ♦ [Section 19.1, “Overview of RConsoleJ Components,” on page 795](#)
- ♦ [Section 19.2, “Setting Up RConsoleJ,” on page 796](#)
- ♦ [Section 19.3, “RConsoleJ,” on page 797](#)
- ♦ [Section 19.4, “Loading Agents at Startup,” on page 802](#)
- ♦ [Section 19.5, “Setting Up Security for RConsoleJ,” on page 802](#)
- ♦ [Section 19.6, “Managing Remote NetWare Servers,” on page 803](#)

19.1 Overview of RConsoleJ Components

RConsoleJ has the following components. These components interact with each other during the remote control session of a NetWare server.

- ♦ [Section 19.1.1, “RConsoleJ Client,” on page 795](#)
- ♦ [Section 19.1.2, “RConsoleJ Agent,” on page 795](#)
- ♦ [Section 19.1.3, “RConsoleJ Proxy Agent,” on page 796](#)

19.1.1 RConsoleJ Client

The RConsoleJ Client is a Java-based utility running on the workstation. From the RConsoleJ Client, you can remote control and monitor all NetWare console operations.

19.1.2 RConsoleJ Agent

The RConsoleJ Agent (`rconag6.nlm`) is a utility running on the target NetWare server. The target NetWare server can be connected over IP, IPX™, or IP/IPX running the RConsoleJ Agent. The RConsoleJ Agent services all RConsoleJ Client requests.

The RConsoleJ Agent advertises its services using the Service Location Protocol (SLP) on a NetWare 5.x and later.

19.1.3 RConsoleJ Proxy Agent

The RConsoleJ Proxy Agent (`rconprxy.nlm`) is a utility running on a NetWare server (supported only on Netware 5.x and up). It routes all IP packets to IPX, and vice versa.

The RConsoleJ Proxy Agent advertises its services using the Service Location Protocol (SLP).

IMPORTANT: If the target NetWare server uses only IPX, the NetWare server (loaded with the RConsoleJ Proxy Agent) must have both IP and IPX stacks installed.

19.2 Setting Up RConsoleJ

To set up RConsoleJ, complete the following sections:

- ♦ [Section 19.2.1, “Loading the RConsoleJ Agent,” on page 796](#)
- ♦ [Section 19.2.2, “Running the RConsoleJ Client,” on page 796](#)
- ♦ [Section 19.2.3, “Loading the RConsoleJ Proxy Agent on a Proxy Server,” on page 797](#)

19.2.1 Loading the RConsoleJ Agent

- 1 At the server console prompt, enter:

```
rconag6
```

- 2 Enter the password you want network administrators to use when accessing the target NetWare server using RConsoleJ.

- 3 Enter the TCP port number.

The default value is 2034.

If the server communicates using IPX only, enter -1 to disable TCP listening.

To enable listening over a dynamically assigned port, enter 0.

- 4 Enter the SPX™ port number on which RCONAG6 will listen for a proxy server.

The default is 16800.

If the server communicates using IP only, enter -1 to disable SPX listening.

To enable listening over a dynamically assigned port, enter 0.

NOTE: /DEV/TCP and /DEV/TCPSSL fail if you are using a pure IPX server.

To enable RConsoleJ across the firewall, you need to keep the following ports open: 2034, 2035, and 2036.

19.2.2 Running the RConsoleJ Client

You can run the RConsoleJ client from a workstation or a NetWare server.

- ♦ [“Running the RConsoleJ Client from a Workstation” on page 797](#)
- ♦ [“Running the RConsoleJ Client on a NetWare Server” on page 797](#)

Running the RConsoleJ Client from a Workstation

You can run the RConsoleJ Client on a workstation using any of the following methods:

- ♦ From a Windows* 2000/XP workstation, browse to *ConsoleOne_installation_directory\1.2*, and run *rconj.exe*.
- ♦ In ConsoleOne, right-click the NetWare server object that you want to remotely control, then click *Remote Management*.
- ♦ In ConsoleOne, select the NetWare server object and then from the Tools menu, click *ZENworks Remote Management > Remote Console > NetWare*.
- ♦ In ConsoleOne, right-click a Subscriber or Distributor object, then click *Remote Management*.
- ♦ If you have installed ZENworks 7 Management and Monitoring Services, select the NetWare server in the *Atlas Namespace*, then click *Remote Management*.

Running the RConsoleJ Client on a NetWare Server

You can run the RConsoleJ Client on a NetWare server using any of the following methods:

- ♦ In ConsoleOne, right-click the NetWare server object that you want to remote control and click *Remote Management*, or click the NetWare server object and then from the Tools option click *ZENworks Remote Management > Remote Console > NetWare*.
- ♦ From the server console prompt, enter *rconj.ncf*.
- ♦ From the server GUI, click *Novell > Programs > RConsoleJ*.

19.2.3 Loading the RConsoleJ Proxy Agent on a Proxy Server

The NetWare server loaded with the RConsoleJ Proxy Agent should have an IP/IPX stack loaded.

- 1 At the server console prompt, enter the following command:
rconprxy
- 2 Enter the TCP port number on which RCONPRXY listens for RConsoleJ.
The default is 2035.

To enable listening over a dynamically assigned port, enter 0.

When the NetWare server is running the RConsoleJ Proxy Agent, the RConsoleJ Client can communicate through it with the target NetWare server that uses only IPX to communicate.

19.3 RConsoleJ

This section will help you initiate RConsoleJ in the following scenarios:

- ♦ [Section 19.3.1, “Scenario 1: An IP Client Controlling an IP NetWare Server,” on page 797](#)
- ♦ [Section 19.3.2, “Scenario 2: An IP Client Controlling an IPX NetWare Server,” on page 800](#)

19.3.1 Scenario 1: An IP Client Controlling an IP NetWare Server

- ♦ [“Prerequisites” on page 798](#)
- ♦ [“Setting Up a Secured IP Connection” on page 798](#)

- ♦ “Setting Up an Unsecure IP Connection” on page 799

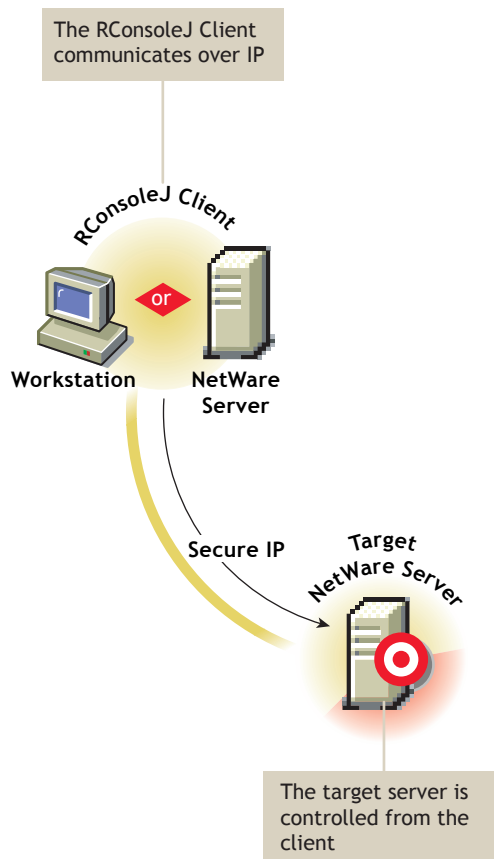
Prerequisites

- ♦ “Loading the RConsoleJ Agent” on page 796
- ♦ “Running the RConsoleJ Client” on page 796

Setting Up a Secured IP Connection

Figure 19-1 illustrates how the RConsoleJ Client communicates directly with the RConsoleJ Agent using TCP/IP.

Figure 19-1 *RConsoleJ Client Communicates with the Target NetWare Server Over Secure IP*



To setup a Secured IP connection, complete the following:

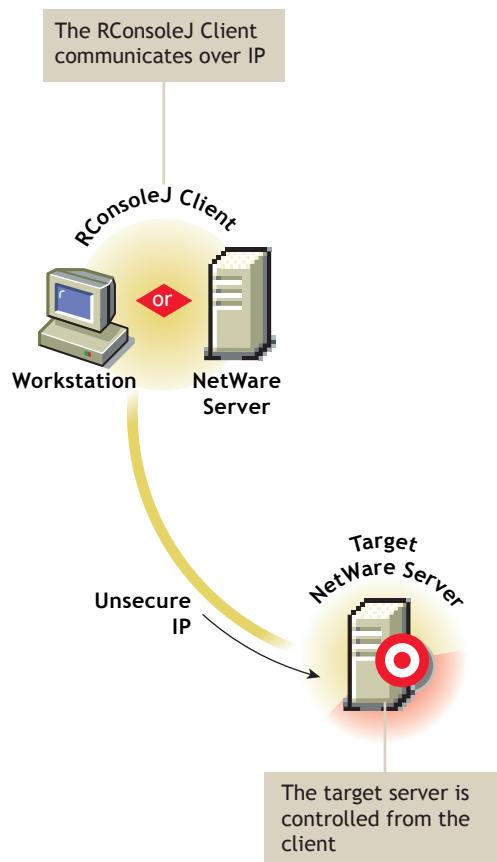
- 1 In the RConsoleJ Connection dialog box, select *Secure IP*.
- 2 Enter the IP address of the target NetWare server, or click the *Remote Servers* icon and then select the target NetWare server from the list.
- 3 Enter the password provided during loading of the RConsoleJ Agent on the target server.
- 4 Enter the port number.
The default is 2036.
- 5 Click *Connect*.

- 6 To ensure server authentication, read the Untrusted Certificate Verification server certificate issued by the target server and click *OK* to accept.

Setting Up an Unsecure IP Connection

Figure 19-2 illustrates how the RConsoleJ Client communicates directly with the RConsoleJ Agent using TCP/IP.

Figure 19-2 *RConsoleJ Communicates with the Target NetWare Server Over IP*



When you run the RConsoleJ client from ConsoleOne, the Novell RConsoleJ dialog box is displayed with the Netware Server IP address. To run the RConsoleJ client, see [“Running the RConsoleJ Client”](#) on page 796.

To start an IP connection:

- 1 Enter the password specified during loading the RConsoleJ Agent.
- 2 Enter the port number.
The default is 2034.
- 3 Click *Connect*.

19.3.2 Scenario 2: An IP Client Controlling an IPX NetWare Server

- ♦ “Prerequisites” on page 800
- ♦ “Starting an IPX Connection” on page 800

Prerequisites

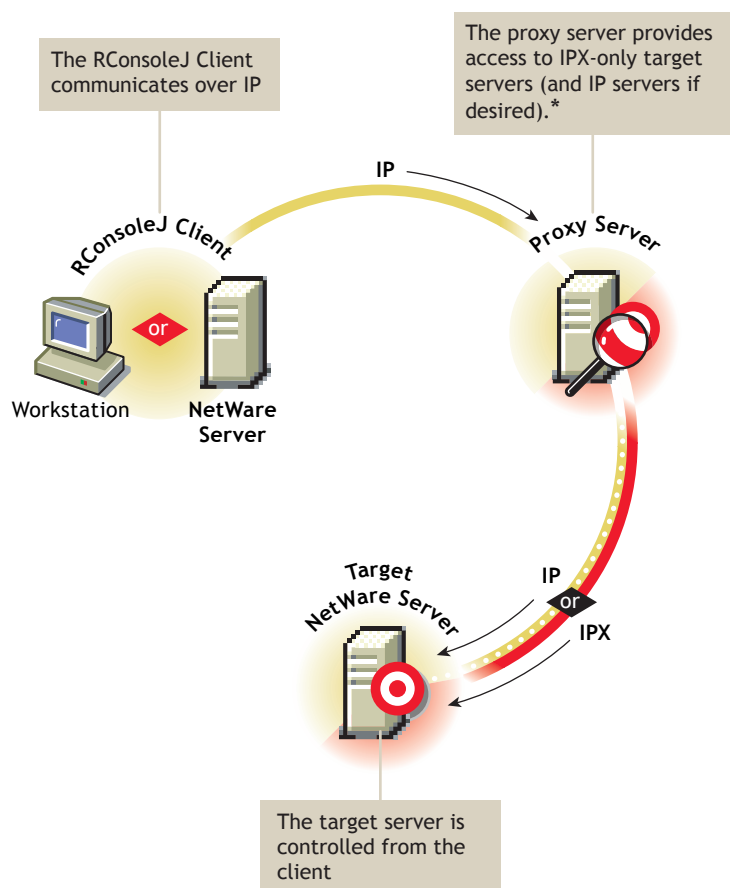
- ♦ “Loading the RConsoleJ Agent” on page 796
- ♦ “Running the RConsoleJ Client” on page 796
- ♦ “Loading the RConsoleJ Proxy Agent on a Proxy Server” on page 797

Starting an IPX Connection

The RConsoleJ Client communicates with the RConsoleJ Agent through the RConsoleJ Proxy Agent because the target NetWare server is based only on IPX.

The RConsoleJ Proxy Agent is loaded on a NetWare server (proxy server) that has both IP and IPX stacks loaded. The RConsoleJ Proxy Agent receives all the IP requests from the RConsoleJ Client, converts them to IPX requests, and then sends them to the RConsoleJ Agent and vice-versa. **Figure 19-3** illustrates this.

Figure 19-3 The RConsoleJ Client Communicates with the Target NetWare Server through the Proxy Server



*If the target server uses IPX, the proxy server must have both IP and IPX stacks loaded.

When you run the RConsoleJ client from ConsoleOne, the Novell RConsoleJ dialog box is displayed with the Netware Server IP address. To run the RConsoleJ client, see [“Running the RConsoleJ Client” on page 796](#).

To start an IPX connection:

- 1 From the Connect Type drop-down list, select *Connect through Proxy*. Select *SPX* to get the IPX address and *TCP* to get the IP address.

The default port is be selected when you make the above change.

The default is 16800 for IPX address and 2034 for IP address.

- 2 Enter the IP address of the proxy server, or click the *Remote Servers* icon and then select a proxy server from the list.
- 3 Enter the port number specified during loading the RConsoleJ Proxy Agent.
The RConsoleJ Client communicates with the RConsoleJ Proxy Agent on this port.
The default is 2035.
- 4 Click *Connect*.

19.4 Loading Agents at Startup

You can load the RConsoleJ Agent and the RConsoleJ Proxy Agent at the startup.

- [Section 19.4.1, “Loading RConsoleJ Agent at Startup,” on page 802](#)
- [Section 19.4.2, “Loading RConsoleJ Proxy Agent at Startup,” on page 802](#)

19.4.1 Loading RConsoleJ Agent at Startup

You can load RConsoleJ Agent (`rconag6.nlm`) at startup using either of the following methods:

- [“Using Encrypted Password \(Recommended\)” on page 802](#)
- [“Using Plain Text Password” on page 802](#)

Using Encrypted Password (Recommended)

- 1 Prepare the `ldrconag.ncf` script file.
 - 1a At the console prompt, enter `rconag6 encrypt`.
 - 1b In the RConsoleJ Agent server screen, enter the password and port numbers.
 - 1c Enter `Y`.
- 2 Prepare the `autoexec.ncf` file to run the `ldrconag.ncf` script file at startup.
 - 2a Comment out the following line:

```
load rconag6 user_defined_password_here 2034 16800 2036
```
 - 2b Enter the following line:

```
ldrconag
```

NOTE: The ZENworks 7 Server Management Remote Management Agent install automatically executes the above steps if you specified a password for the managed server in the installation wizard.

Using Plain Text Password

Enter the following line in `autoexec.ncf`:

```
load rconag6 your_password 2034 16800 2036
```

19.4.2 Loading RConsoleJ Proxy Agent at Startup

To load the RConsoleJ Proxy Agent (`rconprxy.nlm`) at the startup, enter the following line in `autoexec.ncf`:

```
load rconprxy 2035
```

19.5 Setting Up Security for RConsoleJ

You can change the agent password to ensure that RConsoleJ sessions are secure.

To change the agent password for a remotely managed NetWare server:

- 1 At the NetWare Console prompt, enter `unload rconag6` to unload `rconag6.nlm`.

2 Enter `rconag6 encrypt`.

3 Enter a new password.

4 Enter the TCP port number.

The default is 2034.

5 Enter the SPX port number.

The default is 16800.

6 Enter `y` when prompted to save the following command line in the `ldrconag.ncf` file.

If you enter `n`, the `ldrconag.ncf` file is not updated. The new password is valid only for the current session. If you load RCONAG6 from the `ldrconag.ncf` file later, the previously saved password is used.

The new password is in effect when the agent is loaded from the LDRCONAG script file after you reboot the server.

Alternatively, you can change the password using the following commands:

- ♦ For Netware 4.x and 5.x:

```
LOAD RCONAG6 - E encrypted_password TCP_port_number  
SPX_port_number
```

- ♦ For Netware 6.x:

```
LOAD RCONAG6 - E encrypted_password TCP_port_number  
SPX_port_number Secure_port_number
```

19.6 Managing Remote NetWare Servers

After RConsoleJ establishes connection with the NetWare server, you can view and manage the target NetWare server from your desktop.

The following sections explain the tasks you can perform to effectively manage a remote NetWare Server:

- ♦ [Section 19.6.1, “Sending Console Commands in the Server's Native Language,” on page 803](#)
- ♦ [Section 19.6.2, “Synchronizing RConsoleJ Client and Target NetWare Screens,” on page 804](#)

19.6.1 Sending Console Commands in the Server's Native Language

You can send console commands in the server's native language from the RConsoleJ Client using the *Buffer Input* field as shown in [Figure 19-4](#). The buffer stores a list of ten history commands.

Figure 19-4 Send Console Commands in Japanese using Buffer Input



To send console commands, do the following:

- 1 From the Novell RConsoleJ Client window, enter the command that you want to run at the target server in the *Buffer Input* field.
- 2 Click *Send*.

19.6.2 Synchronizing RConsoleJ Client and Target NetWare Screens

You can synchronize the screen displayed on the target NetWare server and the screen displayed on the RConsoleJ Client with each other. Switching the screen in the RConsoleJ Client switches the screen at the target server console, and vice versa.

To synchronize the screens, from the Novell RConsoleJ window, click *Sync*.

To switch the screen on the server console to the currently activated screen on the RConsoleJ Client, click *Activate*.

Remote Management for Windows Servers

20

The Remote Management component of Novell® ZENworks® 7 Server Management allows you to remotely manage Windows* 2000/2003 servers from your computer.

This chapter contains the following topics:

- ♦ [Section 20.1, “Remote Management Terminology,” on page 805](#)
- ♦ [Section 20.2, “Understanding Remote Management for Windows Servers,” on page 805](#)
- ♦ [Section 20.3, “Setting Up Security for Remote Management,” on page 807](#)
- ♦ [Section 20.4, “Managing Remote Windows Servers,” on page 810](#)

20.1 Remote Management Terminology

The following brief glossary provides basic definitions of Remote Management terms:

Managed server: A Windows server that you want to remotely manage. You must install the ZENworks 7 Remote Management Agent on it. If you manage the server through the Server Remote Management Policy, you must install the ZENworks 7 Subscriber component also.

Management console: A Windows 2000/XP workstation or 2000/2003 server running Novell ConsoleOne® with the ZENworks 7 Remote Management ConsoleOne snap-ins installed. The management console provides the interface where you manage and administer your network.

Management server: A server with Novell eDirectory™ and the ZENworks 7 Distributor components. The eDirectory and Distributor components must be installed if you want to manage servers through the Server Remote Management Policy. Your management server can be a managed server.

Remote operator: A user who can remotely manage servers.

Administrator: A person who has the rights to install Remote Management components. All administrators are remote operators but all remote operators are not administrators.

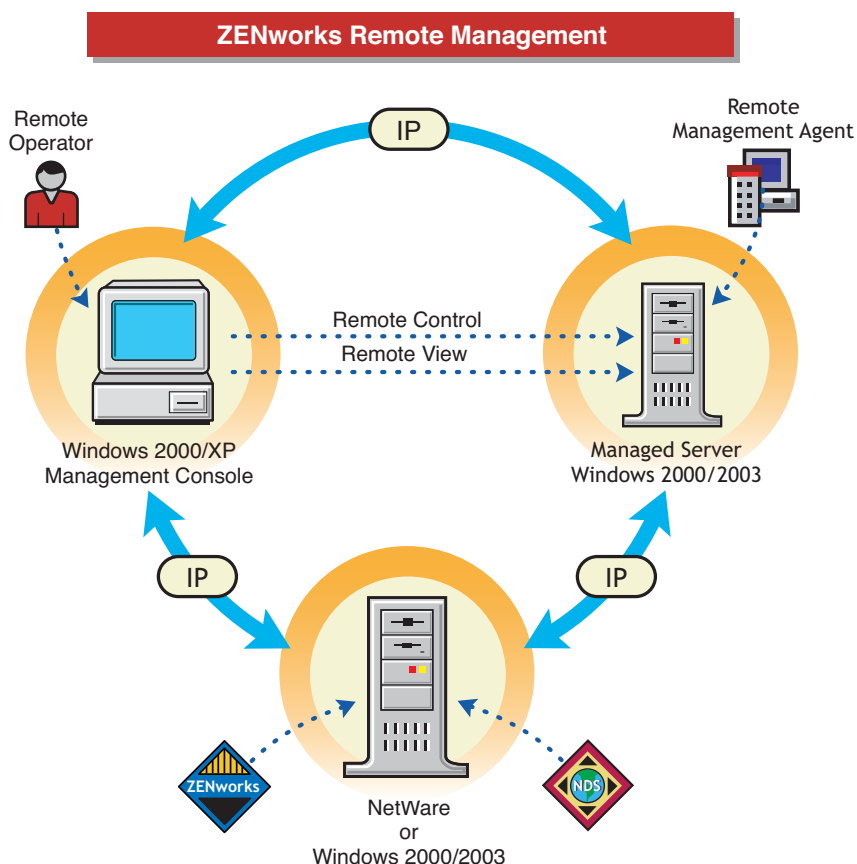
Remote Management Agent: A Server Management component that is installed on a managed server so the remote operator can remotely manage that server. The Remote Management Agent starts automatically when the managed server boots up and authenticates the remote operator when the remote session is initiated.

Viewing window: A representation of the managed server desktop. It is displayed on the management console when the remote operator initiates a Remote Management session.

20.2 Understanding Remote Management for Windows Servers

Figure 20-1 depicts the functionality of the ZENworks 7 Remote Management, which is explained below:

Figure 20-1 Remote Management Functionality



To remotely manage a server, the ZENworks 7 Remote Management Agent component must be installed on that server. For more information, see [“Policy-Enabled Server Management Installation”](#) in the *Novell ZENworks 7 Server Management Installation Guide*.

The Remote Management Agent starts automatically when the managed server boots up. The agent password can be set either by the administrator during the Remote Management installation or by the user at the managed server after the installation. The remote operator would be required to enter the password when he or she initiates a Remote Management session with a managed server. On successful verification, the Remote Management session proceeds and the Viewing window is displayed on the management console.

The user at the managed server can change the agent password. In such a case, the new password will have to be communicated to the remote operator. It is recommended that the password be changed frequently to prevent it from being compromised. For more details on how to set up a new agent password or change the existing agent password, see [“Setting Up the Agent Password at the Managed Server”](#) on page 810.

20.3 Setting Up Security for Remote Management

The information in the following sections help you in setting up security for the Remote Management sessions:

- ♦ [Section 20.3.1, “Configuring the Remote Management Policies,” on page 807](#)
- ♦ [Section 20.3.2, “Setting Up the Agent Password at the Managed Server,” on page 810](#)

20.3.1 Configuring the Remote Management Policies

To configure the Remote Management policies, you must perform the following tasks:

- ♦ [“Creating the Policy Packages” on page 807](#)
- ♦ [“Creating and Configuring the Tiered Electronic Distribution Objects” on page 808](#)
- ♦ [“Configuring the Server Remote Management Policy” on page 808](#)
- ♦ [“Configuring the Distribution Object for Remote Management” on page 810](#)
- ♦ [“Configuring the Distributor and the Subscriber Objects” on page 810](#)

You can also change the security settings on the managed servers by modifying the [Remote Management Policy] section in the

`ZENworks_agent_directory\rmagent\zfsrpol.ini` file.

Creating the Policy Packages

ZENworks 7 requires policy packages in the eDirectory tree that can hold the server policies. You can later configure and enable the server policies.

Policy packages are eDirectory objects that contain collections of policies grouped according to the object types. You should create an Organizational Unit (OU) for holding the policy packages. Consider the following when determining where to place this OU:

- ♦ Whether you have partitions in your tree
- ♦ The 256-character limit in eDirectory for the full distinguished name
- ♦ How you will use the Search policy to locate the policy package

If you install ZENworks 7 Desktop Management to your tree, you may want to keep the ZENworks Server Management and Desktop Management policies in separate containers, such as `Server_Policies` and `Desktop_Policies`.

For Remote Management, create two containers, one for Tiered Electronic Distribution objects and the other for the Remote Management policy package.

To create a container:

- 1 In ConsoleOne, right-click the container where you want the container for the policy packages placed.
- 2 Click *New > Object > Organizational Unit > OK*.
- 3 Name the container, for example, `Server_Policies`, then click *OK*.

IMPORTANT: If you have partitions that are accessed across a WAN, make sure that the Policy Package objects are in the same partition as the Server object so that the Policy/Package Agents are loaded. Also make sure that the Search policy does not require searching outside the partition where the Server object exists.

For Remote Management, you must create the Distributed Server package. The Distributed Server package is required to distribute the Remote Management policies among the managed servers for enforcement.

To create the Distributed Server package:

- 1 In ConsoleOne, right-click the policy package's container, then click *New > Policy Package*.
The Policy Package Wizard is displayed.
- 2 In the *Policy Packages* list, select *Distributed Server Package*, then click *Next*.
- 3 Enter a name for the Distributed Server Package, then click *Next*, then click *Finish*.

Creating and Configuring the Tiered Electronic Distribution Objects

For Remote Management, you must create and configure the following Tiered Electronic Distribution objects:

- ♦ TED Distribution
- ♦ TED Channel

To create and configure the Tiered Electronic Distribution objects, see [Chapter 3, “Tiered Electronic Distribution,” on page 85](#).

Configuring the Server Remote Management Policy

The Server Remote Management Policy defines the behavior of the Remote Management Agent. This policy is distributed to the specified Windows managed servers using the Tiered Electronic Distribution, which helps the remote operator to associate the Remote Management policy to a group of Windows managed servers from the management console.

To configure the Server Remote Management Policy:

- 1 In ConsoleOne, right-click the Distribute Server Package object, then click *Properties*.
- 2 Click the *Policies* tab and select the *Windows* sub-option.
- 3 Select the check box under the *Enabled* column for the Server Remote Management Policy.
- 4 Click the *Properties* button > the *Remote Management* tab.
- 5 Click the *General* tab, then select the any of following options:
 - ♦ **Enable Session Encryption:** Encrypts the Remote Control and Remote View sessions. The Remote Operator cannot change this to an unencrypted mode. If you do not select this check box, the remote sessions are unencrypted by default. In this case, the Remote Operator has an option to switch over to the encrypted mode from the Console. An encrypted session slightly impacts the performance of remote sessions over fast links.

IMPORTANT: This option does not work for ZENworks for Servers 3.x and earlier versions of the Remote Management Agent.

- ♦ **Allow User to Request Remote Session:** Enables the user at the managed server to request the Remote Operator on the management console to perform a remote session.

IMPORTANT: This option does not work for ZENworks for Servers 3.x and earlier versions of the Remote Management Agent.

- ♦ **Display Remote Management Agent Icon To Users:** Displays the *Remote Management Agent* icon in the system tray of the Windows 2000 or Windows 2003 managed servers on which the Remote Management Agent is running.

6 Click the *Remote Control* tab, then select the any of following options:

- ♦ **Prompt User for Permission to Remote Control:** Allows the user at the managed server to either accept or reject the Remote Control session initiated by the remote operator.
- ♦ **Give User Audible Signal when Remote Controlled:** Generates an audible signal on the managed server every time the remote operator remote controls the managed server. You can modify the time interval as to when you want the audible signal should be generated.
- ♦ **Give User Visible Signal when Remote Controlled:** Displays a visible signal with the name of the remote operator and console machine on the managed server every time the remote operator remote controls the managed server. You can modify the time interval as to when the name should be displayed.
- ♦ **Allow Blanking User's Screen:** Allows the remote operator to blank the screen of the managed server during a remote control session and also locks the mouse and keyboard controls.
- ♦ **Allow Locking User's Keyboard and Mouse:** Allows the remote operator to lock the keyboard and mouse controls of the managed server during a remote control session.

7 Click the *Remote View* tab, then select the any of following options:

- ♦ **Prompt User for Permission to Remote View:** Allows the user at the managed server to either accept or reject the Remote View session initiated by the remote operator.
- ♦ **Give User Audible Signal when Remote Viewed:** Generates an audible signal on the managed server every time the remote operator remotely views the managed server. You can modify the time interval as to when you want the audible signal should be generated.
- ♦ **Give User Visible Signal when Remote Viewed:** Displays a visible signal with the name of the remote operator and console machine on the managed server every time the remote operator remotely views the managed server. You can modify the time interval as to when the name should be displayed.

8 Click *Apply*, then click *Close*.

9 Right-click the Server Remote Management Policy, then select *Edit Schedule*.

10 Modify the schedule.

11 Click *Apply*, then click *Close*.

12 To associate the Server Remote Management Policy with a managed server, click the *Distribution* tab.

13 Click *Add*.

14 Browse for and select the Distribution object, then click *OK*.

15 Click *Apply*, then click *Close*.

Configuring the Distribution Object for Remote Management

You must configure the Distribution object for distributing the Remote Management policies.

To configure the Distribution object:

- 1 In ConsoleOne, right-click the Distribution object, then click *Properties*.
- 2 Click the *Type* tab.
- 3 Select Policy Package from the *Select Type* drop-down list.
- 4 Click *Add*, then select the Distributed Server package that has the Server Remote Management Policy.
- 5 Click the *Schedule* tab.
- 6 Modify the schedule.
- 7 Click *Apply*, then click *Close*.

Configuring the Distributor and the Subscriber Objects

To configure the Distributor and the Subscriber objects, see [Chapter 3, “Tiered Electronic Distribution,” on page 85](#).

If the managed servers are residing on a different eDirectory tree or the Windows 2000/2003 server does not have the eDirectory installed, you must create and configure an External Subscriber object for sending Distributions to Subscribers residing on managed servers in other trees. For more information on External Subscribers, see [Section 3.8, “External Subscribers,” on page 158](#).

20.3.2 Setting Up the Agent Password at the Managed Server

The user at the managed server can change the password of the Remote Management Agent to make sure that the Remote Management sessions are secure.

To change the agent password:

- 1 Right-click the *Remote Management Agent* icon from the system tray of the Windows 2000/2003 managed server.
- 2 Click *Security > Set Password*.
Use a password of ten or fewer ASCII (non-extended) characters. The password is case-sensitive and cannot be blank.

The new password must be communicated to the remote operator each time it is changed.

20.4 Managing Remote Windows Servers

The following sections provide information that will help you effectively manage Remote Management sessions on Windows 2000/2003 servers:

- ♦ [Section 20.4.1, “Initiating Remote Management Sessions,” on page 811](#)
- ♦ [Section 20.4.2, “Operating with Windows XP SP2,” on page 813](#)
- ♦ [Section 20.4.3, “Configuring Remote Management Ports,” on page 813](#)
- ♦ [Section 20.4.4, “Customizing the Permission Message,” on page 814](#)

- ♦ Section 20.4.5, “Managing a Remote View Session,” on page 815
- ♦ Section 20.4.6, “Managing a Remote Control Session,” on page 817
- ♦ Section 20.4.7, “Remote Operator Identification Display,” on page 825
- ♦ Section 20.4.8, “Viewing the Audit Log for Remote Management Sessions,” on page 825
- ♦ Section 20.4.9, “Improving the Remote Management Performance,” on page 825
- ♦ Section 20.4.10, “Shutting Down and Restarting the Remote Management Agent,” on page 826

20.4.1 Initiating Remote Management Sessions

You have several options for initiating a Remote Management session from ConsoleOne. They include the following:

- ♦ “Initiating Remote Management Session from the ConsoleOne Tools Menu” on page 811
- ♦ “Initiating Remote Management Session from the eDirectory/NDS Namespace” on page 811
- ♦ “Initiating Remote Management Session from the Atlas Namespace” on page 812
- ♦ “Initiating Remote Management Session from the Remote Management Agent” on page 812

Initiating Remote Management Session from the ConsoleOne Tools Menu

- 1 In ConsoleOne, click *Tools > ZENworks Remote Management > Remote Console > Windows*.
- 2 In the Remote Management dialog box, enter the IP address or the DNS name of the managed server.
- 3 Enter the agent password.
- 4 Select the Remote Management operation that you want to initiate with the managed server.
- 5 Click *OK*.

Initiating Remote Management Session from the eDirectory/NDS Namespace

You can start a Remote Management session from the eDirectory (NDS) namespace (in ConsoleOne) using one of the following methods:

- 1 In ConsoleOne, select a managed server.
- 2 Click *Tools > ZENworks Remote Management > Remote Console > Windows*.
- 3 In the Remote Management dialog box, select the IP address of the managed server from the *Agent* drop-down list.
The IP address of the selected managed server is automatically populated to the *Agent* drop-down list.
- 4 Enter the agent password.
- 5 Select the Remote Management operation that you want to initiate with the managed server.
- 6 Click *OK*.

You can also use the following procedure:

- 1 In ConsoleOne, right-click a managed server.
- 2 Click *Remote Management*.

- 3 In the Remote Management dialog box, select the IP address of the managed server from the *Agent* drop-down list.
The IP address of the selected managed server is automatically populated to the *Agent* drop-down list.
- 4 Enter the agent password.
- 5 Select the Remote Management operation that you want to initiate with the managed server.
- 6 Click *OK*.

Initiating Remote Management Session from the Atlas Namespace

Before initiating a Remote Management session from the Atlas namespace (in ConsoleOne), make sure that the NetWare[®] Management Agent[™] (NMA) is installed and the Discovery discovers the network topology.

To initiate the Remote Management session:

- 1 In ConsoleOne, right-click a managed server.
- 2 Click *Actions > Remote Control* or *Remote View*.
- 3 Select the IP address and enter the agent password.
The IP address of the selected managed server is automatically populated to the *Agent* drop-down list.
- 4 Click *OK*.

Initiating Remote Management Session from the Remote Management Agent

If the managed server is configured behind dynamic NAT, the managed server cannot be accessed from the management console but the management console can be accessed from the managed server. To resolve this problem:

- 1 The user at the managed server must initiate a request for a Remote Management session to the remote operator by using the Request Session option.

IMPORTANT: Before initiating a Remote Management session from the Remote Management Agent, the remote operator must ensure that ConsoleOne is running on the management console.

NOTE: The first instance of ConsoleOne receives the request when a session request is initiated from a Remote Management Agent to the management console running on a terminal server. None of the ConsoleOne instances receive the session request until all ConsoleOne instances are closed on the session where ConsoleOne was launched for the first time. To receive the session request, ConsoleOne must be launched again on any terminal session.

To request for a session, the user at the managed server must do the following:

- 1a Right-click the *Remote Management Agent* icon.
- 1b Select *Request Session*.
- 1c Enter the IP address or the DNS name of the management console.
- 1d Select the *Remote Control* or *Remote View* operation from the drop-down list.

- 1e** Click *OK*.
- 2** The Remote Management Listener listens to the request and notifies the remote operator about it. The remote operator must accept the request and provide the following credentials for the request in the Select Authentication Mode dialog box:
 - 2a** Enter the password for authentication.
 - 2b** Click *OK*.

20.4.2 Operating with Windows XP SP2

Windows XP SP2 comes with a firewall enabled by default. As a result, the Remote Control Listener running on Windows XP SP2 cannot receive connections initiated by the Remote Management Agent.

You need to configure the firewall settings to allow the Remote Control Listener to receive connections.

The Remote Control Listener binds to TCP port 1762 by default. In order to change the ports, refer to [“Configuring Remote Control Listener Port” on page 814](#).

20.4.3 Configuring Remote Management Ports

This section provides information on the following topics:

- ♦ [“Configuring Remote Management Agent Port” on page 813](#)
- ♦ [“Configuring Remote Control Listener Port” on page 814](#)

Configuring Remote Management Agent Port

The Remote Management Agent port binds to TCP port 1761 by default. You may configure it to run on a different TCP port by following the steps mentioned below:

- 1** Open *ZENworks_agent_directory\rmagent\rmcfg.ini* file.
- 2** In the *Remote Management Agent Port* section, set the *DefaultCommPort* to the desired port number.
- 3** Restart the Novell ZENworks Remote Management Agent service.

To initiate a remote session to a managed server where the Remote Management Agent is running on any port other than 1761, do the following modifications on the management console:

- 1** Open the *ConsoleOne_directory\1.2\bin\rmports.ini* file.
- 2** In the *Remote Management Agent Ports* section, add the port number.

NOTE: If the Remote Management Agents are running on different ports on different managed servers, you may mention the port numbers one below the other under the Remote Management Agent Ports section.

Configuring Remote Control Listener Port

The Remote Control Listener port binds to TCP port 1762 by default when ConsoleOne is started. You may configure it to run on a different TCP port by following the steps mentioned below:

- 1 Open the *ConsoleOne_directory\1.2\bin\rmports.ini* file.
- 2 In the *Remote Control Listener Port* section, set the *DefaultCommPort* to the desired port number.
- 3 Restart ConsoleOne.

To initiate a remote session request to a management console, where the Remote Control Listener is running on any port other than 1762, the following modifications need to be done on the managed servers:

- 1 Open the *ZENworks_agent_directory\rmagent\rmcfg.ini* file.
- 2 In the *Remote Control Listener Ports* section, add the port number.

NOTE: If the Remote Control Listeners are running on different ports on different management consoles, you may mention the port numbers one below the other in the *Remote Control Listener Ports* section.

20.4.4 Customizing the Permission Message

If the *Ask for user permission* option is selected in the Remote Management policy, the Request for Permission dialog box is displayed with the following default message:

Do you want to allow console user to perform remote management operation?

ZENworks 7 with Support Pack 1 allows you to customize the default message displayed in the Request for Permission dialog box.

To customize the default message, do the following on the managed server:

- 1 Open the Registry Editor.
- 2 Traverse to HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\RemoteManagement\RMAgent and create a registry string in the name "PermissionMessage".
- 3 Enter the message that should be displayed in the Request for Permission dialog box as the value of the registry string created in the previous step.
- 4 (Optional) In the registry string value, you can use the following parameters that will be dynamically replaced by valid information in the message:

Table 20-1 Parameters Used to Customize the Message of the Request for Permission dialog box

Parameter	Information Displayed
%a or %A	Displays the Remote console user name.
%i or %I	Displays the IP address of the management console.
%r or %R	Displays the Remote Management operation initiated by Remote Operator.

A sample registry string with parameters is as follows:

Do you want to allow %a to %r from the remote machine, %i?

The registry string is displayed as the following message in the Request for Permission dialog box:

Do you want to allow admin.novell to Remote Control from the remote machine, 10.0.0.0?

20.4.5 Managing a Remote View Session

After you have initiated a Remote Management session and selected Remote View as the operation, you have several options to help you view the managed server.

- ♦ [“Controlling the Display of the Viewing Window” on page 815](#)
- ♦ [“Using the Viewing Window Accelerator Keys” on page 816](#)
- ♦ [“Defining a Custom Accelerator Key Sequence” on page 817](#)

Controlling the Display of the Viewing Window

You can regulate the display of the Viewing window through using the control options.

To enable the control options:

- 1 Click the *Remote Management Agent* icon, located at the top left corner of the Viewing window.
- 2 Click *Configure*.

Option	Description
<i>Enable High Quality Scaling</i>	Enhances the quality of images in the Scale To Fit Mode.
<i>Enable Accelerator Keys</i>	Enables the accelerator keys on the management console so that you can change the default accelerator key sequences during the remote session.
<i>Enable Encryption</i>	<p>Encryption is an optional feature and will be effective per session. If the saved configuration has enabled encryption, the session will be encrypted from the start of the session.</p> <p>Encrypting a whole session provides greater security as the data transferred over the wire will be encrypted and it will be difficult to decipher anything meaningful even after the data over the wire is captured. However, it impacts performance slightly and is recommended when the security requirement is very stringent.</p>
<i>Hide Wallpaper</i>	Suppresses any wallpaper displayed on the managed server. This option is enabled by default. If you want to display the wallpaper on the managed server during a Remote View session, disable this option.

Option	Description
<i>Color Quality</i>	<p>By default, on a fast Link, the color quality is set to Normal and on a slow link the color quality is set to 256 colors. You can change the color quality of the slow link or the fast link to one of the following:</p> <ul style="list-style-type: none"> ♦ 16 Colors: Forces the use of 16-color palette on the managed server during a Remote Management session. This enhances the Remote Management performance particularly over a slow-link. ♦ 256 Colors: Forces the use of 256-color palette on the managed server during a Remote Management session. This enhances the Remote Management performance over a slow-link. ♦ Normal: The color is not altered and the setting is the same on the managed server during a Remote Management session.
<i>Network Type</i>	<p>if the managed server is connected by a LAN, select the <i>Fast Links</i> option to enhance the Remote Management performance.</p> <p>if the managed server is connected over a dial-up link or by WAN, select the <i>Slow Links</i> option to enhance the Remote Management performance.</p>

- 3 To save the *Control Parameter* settings, select the *Save on Exit* check box.
The saved settings are implemented in the next Remote View session.
- 4 Click *OK*.

Using the Viewing Window Accelerator Keys

You can use accelerator keys to assign the shortcut keys to the control options and also to control the display of the Viewing window. Default accelerator key sequences are assigned to each accelerator key option. The Accelerator Keys dialog box displays the default key sequence in the edit field of each accelerator key option. You can define a custom accelerator key sequence to change the default sequence. For more information, see [“Defining a Custom Accelerator Key Sequence” on page 817](#).

To enable the Accelerator Keys option:

- 1 Click the *Remote Management Agent* icon, located at the top left corner of the Viewing window.
- 2 Click *Configure*.
- 3 Select *Enable Accelerator Keys*.
- 4 Click *OK*.

To open the Accelerator Keys dialog box:

- 1 Click the *Remote Management Agent* icon, located at the top left corner of the Viewing window.
- 2 Click *Accelerator Keys*.

[Table 20-2](#) explains the Accelerator Key options you can during the Remote View session:

Table 20-2 Accelerator Key Options for Remote View Session

Option	Default Keystroke	Description
<i>Toggle Full Screen</i>	Ctrl+Alt+M	Applicable only if the color resolution settings on the management console and managed server are same. Sizes the Viewing window to the size of your screen without window borders.
<i>Refresh Screen</i>	Ctrl+Alt+R	Refreshes the Viewing window.
<i>Restart Session</i>	Ctrl+Alt+T	Re-establishes the connection with the managed server.
<i>Enable Accelerator Keys</i>	Ctrl+Alt+A	Allows you to enable or disable the default accelerator key sequences.
<i>Stop Viewing</i>	Left-Shift+Esc	Closes the Viewing window.
<i>Configure Dialog</i>	Alt+M	Opens the Control Parameters dialog box.
<i>Accelerator Keys Dialog</i>	Alt+A	Opens the Accelerator Keys dialog box.
<i>Poll Full Screen</i>	Alt + L	Scans and renders the information of the entire screen of the managed server.
<i>Scale To Fit</i>	Ctrl+Alt+G	Hides the scroll bars and scale the Remote Management window to fit your screen.

Defining a Custom Accelerator Key Sequence

The default keystrokes assigned to the accelerator key options are displayed in the edit field to the right of each accelerator key option in the Accelerator Keys dialog box. You can change the accelerator key sequence and define a custom accelerator key sequence if you do not want to use the default keystroke.

To define a custom accelerator key sequence:

- 1 Click the *Remote Management Agent* icon, located at the top-left corner of the Viewing window.
- 2 Click *Accelerator Keys*.
- 3 Click the *Edit* field of the accelerator key option where you want to define a custom accelerator key sequence.
- 4 Press the new accelerator key sequence.
- 5 Click *OK*.

IMPORTANT: The shift keys are left-right sensitive, and are indicated in the Control Options dialog box as LShift and RShift. Avoid the use of standard key sequences like Ctrl+C, Ctrl+V, Shift+Del, etc.

20.4.6 Managing a Remote Control Session

After you have initiated a Remote Management session and selected Remote Control as the operation, you can control the managed server from the management console to provide user

assistance and to help resolve server problems. With remote control connections, the remote operator can go beyond viewing the managed server to taking control of it.

You can effectively manage a Remote Control session by performing the following tasks with the Viewing window control options, the Viewing window toolbar buttons, and the Remote Management Agent icon options:

- ♦ “Controlling the Display of the Viewing Window” on page 818
- ♦ “Using the Viewing Window Accelerator Keys” on page 819
- ♦ “Using the Toolbar Buttons on the Viewing Window” on page 821
- ♦ “Enabling the Wallpaper on the Managed Server” on page 822
- ♦ “Using the Remote Management Agent Icon” on page 823
- ♦ “Setting Up a Password for the Managed Server” on page 823
- ♦ “Obtaining Information About Remote Management Sessions” on page 824
- ♦ “Obtaining General Information” on page 824
- ♦ “Obtaining Security Information” on page 824

Controlling the Display of the Viewing Window

You can control the display of the managed server by using the Viewing window control options.

To enable control options:

- 1 Click the *Remote Management Agent* icon, located at the top left corner of the Viewing window.
- 2 Click *Configure*.
- 3 Select the control options you want to enable for the remote session.

The following table explains the options you can use to control the display of the Viewing window.

Option	Description
<i>Block Mouse Movements to Agent</i>	To reduce network bandwidth consumption, blocks all the mouse movements to the Agent.
<i>Enable High Quality Scaling</i>	Enhances the quality of images in the Scale To Fit mode.
<i>Enable Accelerator Keys</i>	Enables the accelerator keys on the management console so that you can change the default accelerator key sequences during the remote session.
<i>Enable Encryption</i>	<p>Encryption is an optional feature and will be effective per session. If the saved configuration has enabled encryption, the session will be encrypted from the start of the session.</p> <p>Encrypting a whole session provides greater security as the data transferred over the wire will be encrypted and it will be difficult to decipher anything meaningful even after the data over the wire is captured. However, it impacts performance slightly and is recommended when the security requirement is very stringent.</p>

Option	Description
<i>System Key Pass</i>	<p>Passes Alt-key sequences on the management console to the managed server.</p> <hr/> <p>NOTE: During a Remote View session, the <i>System Key pass Through</i> option is not enabled.</p>
<i>Hide Wallpaper</i>	<p>Suppresses any wallpaper displayed on the managed server. This option is enabled by default. If you want to display the wallpaper on the managed server during a Remote Control or Remote View session, disable this option.</p>
<i>Enable Encryption</i>	<p>Encryption is an optional feature and will be effective per session. If the saved configuration has enabled encryption, the session will be encrypted from the start of the session.</p> <p>Encrypting a whole session provides greater security as the data transferred over the wire will be encrypted and it will be difficult to decipher anything meaningful even after the data over the wire is captured. However, it impacts performance slightly and is recommended when the security requirement is very stringent.</p>
<i>Color Quality</i>	<p>By default, on a fast Link, the color quality is set to <i>Normal</i> and on a slow link the color quality is set to <i>256 colors</i>. You can change the color quality of the slow link or the fast link to one of the following:</p> <ul style="list-style-type: none"> ♦ 16 Colors: Forces the use of 16-color palette on the managed server during a Remote Management session. This enhances the Remote Management performance particularly over a slow-link. ♦ 256 Colors: Forces the use of 256-color palette on the managed server during a Remote Management session. This enhances the Remote Management performance over a slow-link. ♦ Normal: The color is not altered and the setting is the same on the managed server during a Remote Management session.
<i>Network Type</i>	<p>If the managed server is connected by a LAN, select the <i>Fast Links</i> option to enhance the Remote Management performance.</p> <p>If the managed server is connected over a dial-up link or by WAN, select the <i>Slow Links</i> option to enhance the Remote Management performance.</p>

- 4 To save the *Control Parameter* settings, select the *Save on Exit* check box.

The saved settings are implemented in the next Remote Control session.

Using the Viewing Window Accelerator Keys

You can use accelerator keys to assign shortcut keys to the control options and also to control the display of the Viewing window. Default accelerator key sequences are assigned to each accelerator key option. The Accelerator Keys dialog box displays the default key sequence in the edit field of each accelerator key option. You can define a custom accelerator key sequence to change the default sequence. For more information, see [“Defining a Custom Accelerator Key Sequence” on page 817](#).

To enable the Accelerator Keys option:

- 1 Click the *Remote Management Agent* icon, located at the top left corner of the Viewing window.

- 2 Click *Configure*.
- 3 Select *Enable Accelerator Keys*.

To open the Accelerator Keys dialog box:

- 1 Click the *Remote Management Agent* icon, located at the top left corner of the Viewing window.
- 2 Click *Accelerator Keys*.

Table 20-3 explains the Accelerator Key options you can use to control the display of the Viewing window:

Table 20-3 *Accelerator Key Options for Remote Control Session*





Option	Default Keystroke	Description
<i>Toggle Full Screen</i>	Ctrl+Alt+M	Applicable only if the color resolution settings on the management console and managed server are similar. Sizes the Viewing window to the size of your screen without window borders.
<i>Refresh Screen</i>	Ctrl+Alt+R	Refreshes the Viewing window.
<i>Restart Session</i>	Ctrl+Alt+T	Re-establishes the connection with the managed server.
<i>Enable Accelerator Keys</i>	Ctrl+Alt+A	Enables you to change the default accelerator key sequences.
<i>Stop Viewing</i>	Left-Shift+Esc	Closes the Viewing window.
<i>Configure Dialog</i>	Alt+M	Opens the Control Parameters dialog box.
<i>Accelerator Keys Dialog</i>	Alt+A	Opens the Accelerator Keys dialog box.
<i>Poll Full Screen</i>	Alt + L	Scans and renders the information of the entire screen.
<i>Scale To Fit</i>	Ctrl+Alt+G	Hides the scroll bars and scale the Remote Management window to fit your screen.
<i>System Key Pass</i>	Ctrl+Alt+S	Passes Alt-key sequences on the management console to the managed server.
<i>Mouse/Keyboard Lock</i>	Ctrl+L	Locks the keyboard and mouse controls at the managed server. This option is available only if the Allow Locking User's Keyboard and Mouse option is enabled in the Server Remote Management Policy .
<i>Blank Screen</i>	Ctrl+Alt+B	Blanks the screen at the managed server. This option is available only if the <i>Allow Blanking User's Screen</i> option is enabled in the Server Remote Management Policy .
<i>Reboot</i>	Ctrl+Alt+D	Sends the Ctrl+Alt+Del keystroke to the managed server. Display the Security window on the managed server.







Option	Default Keystroke	Description
<i>Start</i>	Alt+R	Invokes the <i>Start</i> menu on Windows server.
<i>Switch Applications</i>	Ctrl+T	Switches applications on managed servers.

Using the Toolbar Buttons on the Viewing Window

Table 20-4 describes the toolbar options in the Viewing window:

Table 20-4 Viewing Window Toolbar Buttons

Button	Default Keystroke	Key Function
<i>Screen Blanking</i> 	Ctrl+L	<p>Enabled only if the <i>Allow Blanking User's Screen</i> option is enabled in the effective Remote Control policy of the managed server.</p> <p>Blanks the screen at the managed server. When the remote operator selects this option, the screen of the managed server is be blacked out and the operations performed by the remote operator on the managed server are not visible to the user at the managed server.</p> <p>Not supported over certain display adapters. Refer to the ZENworks 7 Server Management Readme (http://www.novell.com/documentation/zenworks7) for the list of display adapters that do not support this feature.</p>
<i>Mouse and Keyboard Lock</i> 	Ctrl+Alt+B	<p>Locks the keyboard and mouse controls at the managed server. When the remote operator selects this option, the user at the managed server will not be able to use the keyboard and mouse controls of the managed server.</p>
<i>System Start</i> 	Alt+R	<p>Invokes the <i>Start</i> menu on the managed server.</p>
<i>Application Switcher</i> 	Ctrl+T	<p>Sends the Alt-tab key sequences to the managed server.</p> <p>Switches applications on managed servers.</p> <p>To switch the applications,</p> <ol style="list-style-type: none"> 1. In the Viewing window, click the <i>Application Switcher</i> icon or press the Application Switcher shortcut key. 2. To traverse to the application use the <i>Application Switcher</i> icon. 3. To view the application, press Tab.

Button	Default Keystroke	Key Function
System Key Pass Through 	Ctrl+Alt+S	<p>Sets the system key pass to On or Off.</p> <p>Passes Alt-key sequences from the management console to the managed server.</p> <p>Certain key sequences such as Ctrl+Esc, Alt+Tab, Ctrl+Alt+Del, and Alt+PrintScreen are not allowed even when the System Key Pass-Through is set to On. However, you can use the toolbar buttons on the Viewing window for the Ctrl+Esc, Alt+Tab, and Ctrl+Alt+Del keystrokes.</p>
Reboot 	Ctrl+Alt+D	<p>Sends the Ctrl+Alt+Del keystroke to the managed server.</p> <p>Displays the Security window on the managed server.</p>
Refresh Screen 	Ctrl+Alt+R	Refreshes the viewing window.
Full Screen Polling 	Alt+L	Scans and renders the information of the entire screen of the managed server continuously.
Scale To Fit 	Ctrl+Alt+G	Hides the scroll bars and scales the Remote Management window to fit your screen.
Session Encryption 		<p>Encryption is an optional feature and will be effective per session. If the saved configuration has the option enabled, the session will be encrypted from the start of the session.</p> <p>Encrypting a whole session provides greater security as the data transferred over the wire will be encrypted and it will be difficult to decipher anything meaningful even after the data over the wire is captured. However, it impacts performance slightly and is recommended when the security requirement is very stringent.</p>

You can define a custom key sequence if you do not want to use the default key sequence. For more information, see [“Defining a Custom Accelerator Key Sequence” on page 817](#).

Enabling the Wallpaper on the Managed Server

When the remote operator initiates a Remote Control session, any wallpaper displayed on the desktop of the managed server is suppressed. This feature reduces the response time from the managed server for requests from the management console because less traffic is generated over the network while the wallpaper is suppressed.

You can configure the control parameter for this option to change the default settings and enable the display of the wallpaper on the managed server. When you terminate the Remote Control session, the suppressed wallpaper will be restored.

To enable the display of suppressed wallpaper on the managed server:

- 1 Click the *Remote Management Agent* icon, located at the top left corner, then click *Configure*.
- 2 Deselect the *Hide Wallpaper* option.

Using the Remote Management Agent Icon

By default, the *Remote Management Agent* icon is displayed in the system tray of the Windows servers. This icon indicates that the Remote Management Agent is loaded on the managed server.

The user at the managed server can right-click the *Remote Management Agent* icon and choose from the following options:

Table 20-5 *Remote Management Icon Options*

Option	Description
<i>Terminate RC/RV Session</i>	Disconnects and closes the remote session on the managed server and displays a message on the management console indicating that the remote session is closed.
<i>Security</i>	Allows the user at the managed server to set or clear the password for the server.
<i>Information</i>	<p>Displays information such as who is accessing the managed server for the remote session, security settings, and the protocol in use for the remote session.</p> <p>For details, see “Obtaining Information About Remote Management Sessions” on page 824.</p> <p>You can right-click or double-click the <i>Remote Management Agent</i> icon to view the Information window.</p>
<i>Shutdown Agent</i>	This option is always dimmed on managed servers. To shut down the Remote Management Agent on managed servers, you must go to the Service Control Panel and stop the “Novell ZENworks Remote Management Agent” service.
<i>Request Session</i>	Enables the user at the managed server to request a remote operator to perform remote session.
<i>Help</i>	Displays the Remote Management Agent help.

Setting Up a Password for the Managed Server

The user at the managed server can set an agent password. This password overrides the password set by the administrator during the ZENworks 7 Remote Management installation.

To set the agent password:

- 1 From the managed server, right-click the *Remote Management Agent* icon.
- 2 Click *Security > Set Password*.

Use a password of ten or fewer alphanumeric characters. The password is case sensitive and cannot be blank.

After the completion of the Remote Management session, you can clear the agent password. If you clear the agent password, the remote operator cannot perform the Remote Management operations.

To clear the agent password:

- 1 On the managed server, right-click the *Remote Management Agent* icon.
- 2 Click *Security > Clear Password*.

Obtaining Information About Remote Management Sessions

Using the Information window, the user at the managed server can view details about the session, such as the name of the remote operator how is remotely managing the server, the security settings, and the protocol in use for the remote session.

To view information about remote sessions:

- 1 On the managed server, right-click the *Remote Management Agent* icon.
- 2 Click *Information*.
- 3 Click the *General* tab to view the general information and the *Security* tab to view the security information.

See the following sections for details:

- ♦ “Obtaining General Information” on page 824
- ♦ “Obtaining Security Information” on page 824

Obtaining General Information

Table 20-6 explains the general information you can obtain about Remote Management sessions from the Information window:

Table 20-6 Remote Management Session General Information

Option	Description
<i>RM Operation</i>	Lists the ongoing Remote Management sessions.
<i>RM Information > Initiator</i>	Displays the name of the remote operator.
<i>RM Information > Protocol</i>	Displays the protocol that the Remote Management Agent uses to communicate with the management console during a remote session.
<i>Optimization Status > RC/RV Optimization</i>	Displays if the optimization driver is enabled or disabled for the Remote Management session. The remote session performance is enhanced if the optimization driver is enabled.

Obtaining Security Information

The Security Information dialog box displays information based on the Remote Control and Remote View sessions.

Table 20-7 Remote Control and Remote View Session Security Information

Options	Description
<i>Permission Required</i>	Indicates if the remote operator should obtain permission from the user at the managed server each time the he wants to perform the remote management session on the managed server.
<i>Audible Signal Required</i>	Indicates if an audible signal should be sent to the managed server every time the remote operator accesses the managed server.

Options	Description
<i>Beep Every</i>	Indicates the time interval based on which the audible signal is periodically sent to the managed server.
<i>Visual Signal Required</i>	Indicates if a visible signal should be sent to the managed server every time the remote operator accesses the managed server.
<i>Session Encryption Enabled</i>	Indicates whether a remote session will be encrypted or not. Session Encryption Enabled is applicable for Remote Control and Remote View.
<i>Display Name Every</i>	Indicates the time interval based on which the visual signal is periodically sent to the managed server.
<i>Screen Blanking Allowed</i>	Indicates if the remote operator is allowed to blank the managed server screen. Screen Blanking Allowed is applicable for Remote Control only.
<i>Locking Control Allowed</i>	Indicates if the remote operator is allowed to lock the keyboard and mouse controls of the managed server. Locking Control Allowed is applicable for Remote Control only.

20.4.7 Remote Operator Identification Display

The Remote Management Agent will display the identification of the remote operator in the following dialog boxes on the managed server:

- ♦ Permission dialog box
- ♦ Visible signal dialog box

The information displayed is *console_machine_name\console_windows_username*.

20.4.8 Viewing the Audit Log for Remote Management Sessions

ZENworks Server Management records log information on a Windows managed server.

To view the audit log for Remote Management sessions:

- 1 Click *Start > Programs > Administrative Tools > Event Viewer*.
- 2 Click *Log > Application*.
- 3 Double-click the event associated with the source Remote Management Agent.

To view only the events pertinent to the Remote Management Agent, choose *Remote Management Agent* from the *Source* drop-down list in the Filter dialog box.

20.4.9 Improving the Remote Management Performance

The Remote Management performance, especially over a slow link, has been enhanced through using improved compression.

The performance during a Remote Management session over a slow link or a fast link varies depending on the network traffic. For better response time, try one or more of the following strategies:

On the Management Console

- ♦ Select the *Hide Wallpaper* option on the managed server in the Control Parameters dialog box.
- ♦ Assign color settings on the management console higher than the managed server or assign the same color settings for the management console and the managed server.
- ♦ Select *16 Colors* or *256 Colors* mode in the Control Parameters dialog box to enhance the Remote Management performance.
- ♦ The speed of the management console depends upon the processing power of the client machine. We recommended that you to use single-processor client with a Pentium* III, 500MHz (or later).

On the Managed Server

- ♦ Deselect the *Enable Pointer Shadow* option before starting the Remote Control or Remote View session.

To disable Enable Pointer Shadow:

1. From the Windows desktop, click *Start > Settings > Control Panel > double-click Mouse*.
2. Click *Pointers*.
3. Deselect *Enable Pointer Shadow*.
4. Click *Apply > OK*.

- ♦ At the managed server, use a plain background. Do not set a wallpaper pattern.
- ♦ If the Task manager is opened at the target machine, it is recommended to minimize or close it.
- ♦ Make sure that the scrolling texts (such as the debug windows) and animations are not active on the managed server.
- ♦ Make sure to minimize or close the dialog boxes that are not in use.
- ♦ To perform any operations at the managed server, if possible, use the toolbar options instead of menu options.
- ♦ To maximize the Remote Management performance over WAN, configure the following settings in the Control Parameters dialog box at the managed server:
 - ♦ Set the color mode of the managed server to *16 Colors*.
 - ♦ Select the *Slow Link* option.

20.4.10 Shutting Down and Restarting the Remote Management Agent

The following sections explain how you can use the Remote Management Agent during remote sessions:

- ♦ [“Shutting Down the Remote Management Agent” on page 826](#)
- ♦ [“Restarting the Remote Management Agent” on page 827](#)

Shutting Down the Remote Management Agent

You can shut down the Remote Management Agent during a remote session. When you shut down the Remote Management Agent, the remote session stops. To start another remote session, you need

to restart the Remote Management Agent. For more information, see “[Restarting the Remote Management Agent](#)” on page 827.

To shut down the Remote Management Agent on a Windows 2000/2003 managed server:

- 1 From the Control Panel, double-click *Administrative Tools*.
- 2 Double-click *Services*.
- 3 Click *Novell ZENworks Remote Management Agent* > *Stop*.

IMPORTANT: You can stop the Remote Management Agent on Windows 2000/2003 server only if you have the rights to stop the Windows service.

Restarting the Remote Management Agent

During ZENworks Server Management installation, the Remote Management Agent is installed on the managed server and started automatically when the managed server starts up. If you shut down the Remote Management Agent during a remote session, the remote session stops. To start another remote session, you need to restart the Remote Management Agent on the managed server.

To restart the Remote Management Agent on Windows 2000/2003 managed server:

- 1 From the Control Panel, double-click *Administrative Tools*.
- 2 Double-click *Services*.
- 3 Click *Novell ZENworks Remote Management Agent* > *Start*.

IMPORTANT: You can start the Remote Management Agent on Windows 2000/2003 server only if you have the rights to start the Windows service.

Documentation Updates

P

This section contains information on documentation content changes that have been made in the *Administration* guide for Remote Management since the initial release of Novell® ZENworks® 7 Server Management. The information will help you to keep current on updates to the documentation.

All changes that are noted in this section were also made in the documentation. The documentation is provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the documentation changes listed in this section.

The documentation update information is grouped according to the date the changes were published. Within a dated section, the changes are alphabetically listed by the names of the main table of contents sections for Remote Management.

If you need to know whether a copy of the PDF documentation you are using is the most recent, the PDF document contains the date it was published on the front title page or in the Legal Notices section immediately following the title page.

The documentation was updated on the following date:

- ♦ Section P.1, “July 14, 2006 (Support Pack 1),” on page 829
- ♦ Section P.2, “December 9, 2005,” on page 829

P.1 July 14, 2006 (Support Pack 1)

Updates were made to the following sections. The changes are explained below.

Location	Change
Section 20.4.4, “Customizing the Permission Message,” on page 814	This section has been newly added.

P.2 December 9, 2005

Page design is reformatted to comply with revised Novell documentation standards.