VI

Remote Management

The Remote Management component of Novell® ZENworks® 6.5 Desktop Management gives you the ability to manage remote workstations from the management console. Remote Management allows you to:

- Remotely wake up a powered-off managed workstation

- Remotely control the managed workstation

- Remotely run executables found on the managed workstation with system rights, even if the logged-in user is not a member of the local Administration Group

- Transfer files between the remote management console and the managed workstation

- Display information to diagnose problems on the managed workstation

- Log audit record information about the Remote Management sessions running on the managed workstation

- Blank the managed workstation screen during a Remote Control session

- Lock the keyboard and mouse controls at the managed workstation during a Remote Control session

IMPORTANT: You can also use the Remote Management functionality on servers. For more information, see the ZENworks 6.5 Server Management documentation (http://www.novell.com/documentation/zenworks65/smadmin/data/acqbxjq.html).

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 workstation problems without visiting the user's workstation, which reduces problem resolution times and increases productivity.

The following sections will help you understand and use Remote Management:

65 Understanding Remote Management

You can use Novell® ZENworks® 6.5 Desktop Management to remotely manage Windows* 98 and Windows 2000/XP workstations from the management console.

The following sections provide information that will help you understand the functionality of Remote Management components:

- "Remote Management Terminology" on page 749
- "Understanding the Remote Management Components" on page 749

Remote Management Terminology

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

Managed workstation: A workstation that you want to remotely manage. To remotely manage a workstation, you must install the ZENworks 6.5 Remote Management Agent on it.

Management server: A server where ZENworks 6.5 Desktop Management server is installed.

Management console: A Windows machine running Novell ConsoleOne®. The management console provides the interface to manage and administer your machines.

Remote operator: A user who can remotely manages workstations from management console.

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

Remote Management Agent: A Desktop Management component that is installed on a managed workstation, which enables the remote operator to remotely manage that workstation. The Remote Management Agent starts automatically when the managed workstation boots up. It verifies whether the Remote Operator is authorized to perform operations on the workstation before the Remote Management session proceeds.

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

Registered workstation: A workstation that is registered in eDirectory and imported as an eDirectory Workstation object.

Understanding the Remote Management Components

The following sections provide information to help you understand the functionality of Remote Management components. You must install the Remote Management Agent on the managed workstation to perform the Remote Management operations.

- "Understanding Remote Control" on page 750

Understanding Remote Control

Remote Control lets you control a managed workstation from the management console to provide user assistance and to help resolve workstation problems.

Remote Control establishes a connection between the management console and the managed workstation. With remote control connections, the remote operator can go beyond viewing the managed workstation to taking control of it. For more information, see "Managing a Remote Control Session" on page 770.

Understanding Remote View

Remote View lets you connect with a managed workstation so you can view the managed workstation instead of controlling it. This helps you troubleshoot problems that the user encountered. For example, you can observe how the user at a managed workstation performs certain tasks to ensure that the user performs a task correctly. For more information, see "Managing a Remote View Session" on page 767.

Understanding Remote Execute

Remote Execute lets you run any executable on the managed workstation from the management console. An application can be remote executed by specifying its executable name in the Remote Execute window (if the program is in the path of the managed workstation) or by entering the complete path of the application (if it is not in the path of the managed workstation). For more information, see "Managing a Remote Execute Session" on page 775.

You can determine the path information from the Environment window launched from the Diagnostic feature. For more information, see "Environment Information" on page 791.

Understanding Remote Diagnostics

Remote Diagnostics helps you shorten problem resolution times and assist users without requiring a technician to physically visit the problem workstation. This increases user productivity by keeping desktops up and running. For more information, see "Viewing the Diagnostic Information" on page 789.

Diagnostics provide real-time information so the remote operator can diagnose workstation problems. Following is a list of the diagnostic information that is available on Windows 2000/XP managed workstations:

   ◆ Windows Memory

   ◆ Environment

- ◆ Network Protocols
- ◆ Name Space Provider
- ◆ Event Log
- ◆ Device Drivers
- ◆ Services

Understanding File Transfer

File Transfer lets you perform file operations between the management console and a managed workstation.

Using File Transfer, you can move or copy files between the management console and a managed workstation. You can also rename and delete files, and create directories on the management console and on the managed workstation. From the File Transfer window, you can view the properties of files and directories on the management console and the managed workstation. File Transfer also lets you open files with the associated application on the management console. For more information, see "Managing a File Transfer Session" on page 776.

IMPORTANT: The File Transfer program does not allow access to non-fixed drives on the managed workstation.

Understanding Remote Management Auditing

Remote Management Auditing generates audit records for every Remote Management session running on the managed workstation. The managed workstation where the Remote Management Agent is installed maintains this log information as an audit log. For more information, see "Managing a Remote Management Audit Session" on page 783.

Understanding the Remote Management Events using Windows Event Viewer

The Windows 2000/XP event logging mechanism allows applications running on the managed workstation to record events as log files. You can use the Event Viewer to view the event logs. The Event Viewer maintains Application, Security, and System log files. The events for Remote Management sessions are stored in the Application log file. For more information, see "Viewing the Audit Log of Remote Management Sessions Using Windows Event Viewer" on page 779.

Understanding Remote Wake Up

Remote Wake Up lets you remote power up a single node or a group of powered-down nodes in your network (provided the network card on the node is Wake on LAN enabled). This feature lets the remote operator manage nodes during off-hours to minimize the downtime users experience for system maintenance and upgrades. It also facilitates saving power while keeping systems available for maintenance. For more information, see "Managing a Remote View Session" on page 767.

66 Setting Up Remote Management

The following sections provide information on deploying the Remote Management component of Novell® ZENworks® 6.5 Desktops Management in a production environment

Remote Management Deployment Strategies

The Remote Management Agent must be installed on a managed workstation so the remote operator can remote manage that workstation.

Remote Management Agent is a Desktop Management component that is installed on a managed workstation, which enables the remote operator to remotely manage the workstation. The Remote Management Agent starts automatically when the managed workstation boots up. It verifies whether the Remote Operator is authorized to perform operations on the workstation before the Remote Management session proceeds.

Following are the modes of Remote Management authentication:

Password-Based Remote Management

In this type of Remote Management deployment, you can initiate a Remote Management session with the managed workstation whether or not the managed workstation is imported as an eDirectory Workstation object.

Password-Based Remote Management is a secured means of Remote Management authentication. As a result, the remote operator can automatically initiate Remote Management operations, without re-entering password or authentication information each time.

To deploy Password-Based Remote Management:

1 Install the Remote Management server-side components of ZENworks 6.5 Desktop Management. For more information, see the *Novell ZENworks 6.5 Desktop Management Installation Guide*.

2 During the Agent installation, choose to install the Remote Management Agent component only on the workstations that you want to remote manage.

IMPORTANT: To remote manage registered workstations, you must choose to install Workstation Manager along with the Remote Management Agent.

3 Set the Remote Management Agent password at the managed workstation.

For more information, see "Setting Up the Remote Management Agent Password" on page 758.

Usually, the Remote Management Agent password is set by the user at the managed workstation.

4 To remote manage registered workstations, configure the Remote Management policy.

For more information, see "Configuring the Remote Management Policy for the Registered Workstations" on page 754.

Directory-Based Remote Management

In this type of Remote Management deployment, for the Remote Management Agent to accept a Remote Management request, the managed workstation must be registered in eDirectory and imported as an eDirectory Workstation object.

The Remote Management Agent uses eDirectory based authentication to verify whether the remote operator requesting to remotely manage the workstation is authorized to do so. The effective policy settings based on which the remote operator performs Remote Management sessions on the managed workstation are computed from the Remote Control policy for the eDirectory Workstation object and the User object of the user logged in to the managed workstation.

To deploy Directory-Based Remote Management:

1 Register the workstation in eDirectory and import it as an eDirectory Workstation object.

For more information, see the *Novell ZENworks 6.5 Desktop Management Installation Guide*.

2 Install the ZENworks Desktop Management server-side components.

For more information, see the *Novell ZENworks 6.5 Desktop Management Installation Guide*.

3 During the Agent installation, choose to install Remote Management Agent and Workstation Manager.

4 Configure the Remote Management policy.

For more information, see "Configuring the Remote Management Policy for the Registered Workstations" on page 754

Configuring the Remote Management Policy for the Registered Workstations

The Remote Management policy is an eDirectory object in a policy package. Policy packages are eDirectory objects that contain policies grouped according to the object type. Object types can be Workstation object, Workstation Group, User object, User Group, or Container object.

The Remote Management policy enables the administrator to specify security settings for various Remote Management sessions. The administrator can use the ZENworks Policy Wizard to create a policy package or use an existing Remote Management policy for an object. The policy packages are categorized into Workstation Policy Packages and User Policy Packages. The Workstation Policy Package and the User Policy Package are further categorized based on the operating system of the workstation or the operating system that the user is logged in to. Each policy package has a set of default policies that you can use. By default, the Remote Management policy is available from all the listed User and Workstation policy packages provided by Desktop Management, including:

- General

- Windows 9x

- Windows NT-2000-XP

- Windows NT

- Windows 2000

- Windows XP

The default values are provided for parameters in each page of the Remote Management policy. You can change the default values to suit your requirements.

To change the default values:

1 In Novell ConsoleOne®, create a Workstation policy package.

For more information about how to create the policy packages, see the *Novell ZENworks 6.5 Desktop Management Installation Guide*.

2 Right-click the Workstation policy package, click Properties and select the Policies tab.

3 Select the check box under the Enabled column for the Remote Control Policy.

4 Click the Properties button > Remote Management.

5 Click the remote session tab for which you want to change settings, then select the options that you want to use.

The following table provides a description of options available in the Remote Management policy:

Tab	Options	Description
General	Enable Diagnostics	Allows the remote operator to diagnose the managed workstation.
	Enable Password-Based Remote Management	Allows the remote operator to establish Remote Management session with the managed workstation using password mode of authentication after the workstation was imported.

Tab	Options	Description
	Enable Session Encryption	If this option is enabled, the Remote Control and Remote View sessions will be encrypted. The Remote Operator will not be able to change this to an unencrypted mode. When the option is disabled, the remote sessions will be unencrypted by default. In this case, the Remote Operator will have an option to switch over to the encrypted mode from the Console. An encrypted session will slightly impact the performance of remote sessions over fast links. **IMPORTANT:** This option will not work with Novell ZENworks for Desktops 4.*x* and older versions of Agent.
	Allow User to Request Remote Session	If this option is enabled, the user at the managed workstation can request the Remote Operator on the management console to perform a remote session. **IMPORTANT:** This option will not work for ZENworks for Desktops 4.*x* and older versions of the agent.
	Terminate Session When Workstation User Logs In Requires To Be Prompted for Permission	Terminates any ongoing Remote Management session when a new eDirectory user, whose permission for initiating any Remote Management operation is required, logs into the managed workstation.
	Accept Connections across NAT/Proxy	Enables the Remote Management Agent to accept connection with the management console across NAT or Proxy. This is applicable for connections initiated through the Directory-based authentication only.
	Prompt User for Permission to Accept Connections across NAT/Proxy	Allows the user at the managed workstation to accept or reject connections across NAT or Proxy. This is applicable for connections initiated through the Directory-based authentication only.
	Display Remote Management Agent Icon to Users	Displays the Remote Management Agent icon in the taskbar of the Windows* 98 and Windows 2000/XP managed workstation on which the Remote Management Agent is running.
Control	Enable Remote Control	Allows the remote operator to remote control the managed workstation.
	Prompt User for Permission to Remote Control	Allows the user at the managed workstation 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 workstation every time the remote operator remote controls the managed workstation. You can modify the time interval as to when the audible signal should be generated.
	Give User Visible Signal when Remote Controlled	Displays a visible signal with the name of the remote operator on the managed workstation every time the remote operator remote controls the managed workstation. You can modify the time interval as to when the name should be displayed.

Tab	Options	Description
	Allow Blanking User's Screen	Allows the remote operator to blank the screen of the managed workstation during a remote control session and also lock the mouse and the keyboard controls.
	Allow Locking User's Keyboard Mouse	Allows the remote operator to lock the mouse and keyboard controls of the managed workstation during a remote control session.
View	Enable Remote View	Allows the remote operator to remote view the desktop of the managed workstation.
	Prompt User for Permission to Remote View	Allows the user at the managed workstation to either accept or reject the Remote View session initiated by the remote operator.
	Give User Audible Signal when Remote Viewed	Enables the management console to send an audible signal to the managed workstation every time the remote operator remote views the managed workstation.
	Give User Visible Signal when Remote Viewed	Enables the management console to send a visible signal to the managed workstation every time the remote operator remote views the managed workstation.
File Transfer	Enable File Transfer	Allows the remote operator to transfer files between the management console and the managed workstation.
	Prompt User for Permission to Transfer Files	Allows the user at the managed workstation to either accept or reject the File Transfer session initiated by the remote operator.
Remote Execute	Enable Remote Execute	Allows the remote operator to execute applications or files on the managed workstation.
	Prompt User for Permission to Remote Execute	Allows the user at the managed workstation to either accept or reject the Remote Execute session initiated by the remote operator.

The administrator can change the default settings on any page of the Remote Management policy. If you change the Remote Management Agent icon setting, you must restart the Remote Management Agent for the changes to take effect. The new settings are applied for all subsequent Remote Management sessions.

NOTE: To traverse the options of the Remote Operations button, press Ctrl+Up or Ctrl+Down.

6 Click the Associations tab > Add.

7 Browse to and select the container object where the workstations are registered > click OK.

8 Click Apply > Close.

Configuring the Remote Management Policy for Non-Registered Workstations

You can change the security settings on the non-registered managed workstations by modifying the [Remote Management Policy] section in the *ZENworks_agent_directory*\remotemanagement\rmagent\rmcfg.ini file.

Setting Up the Remote Management Agent Password

The user at the managed workstation must set a password for the Remote Management Agent and communicate the password to the remote operator.

To set the agent password at the managed workstation:

1 Right-click the Remote Management Agent icon.

2 Click Security > Set Password

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

NOTE: The password is stored in an encrypted form in *HKLM\software\novell\zenworks\remote management\rmagent, password.* It is encrypted in the registry with a non-machine specific hash. This means you can use NAL to distribute a standard password.

Assigning Rights to the Remote Operator

You can use the Manage Remote Operators wizard to set up the required rights for a management console user or a set of users to manage a workstation. Alternatively, you can use the Remote Operators tab in the properties of a workstation to add a user as a remote operator while providing the appropriate Remote Management rights.

Assigning Rights Using the Remote Operator Wizard

The Remote Operator wizard is a utility that runs on the NDS® namespace.

To assign the required rights using the Remote Operator wizard:

1 In ConsoleOne, select an eDirectory tree in the NDS namespace.

2 Click Tools > Manage Remote Operator.

3 Click Add to browse and select the container or the workstation you want to manage from the list of containers and workstations.

NOTE: If you want to remove any of the container or the workstation, select the container or the workstation, then click Remove.

4 Select the check box to inherit the properties for the workstations that you want to import into the container.

NOTE: If you choose to select the check box, the properties will also be inherited to workstations that you add later to the container.

5 Click Next.

6 In the Remote Management Operations list, you must assign at least one rights options. By default all the operations are indicated by ✔.

To assign Remote Management operation rights, click the button until the symbol is ✔.

To remove Remote Management operation rights, click the button until the symbol is ✘.

7 Click Next.

8 Click Add to browse and select the container or the user to whom you want to assign the rights.

NOTE: To disassociate a container or a user, select the container or the user, then click Remove.

9 Click Next.

10 The summary of the selected container or workstation, remote management rights that are assigned, or removed, and names of the affected remote operators are displayed.

Click Finish.

Assigning Rights Using the Remote Operators Tab

1 In ConsoleOne, right-click the workstation object.

2 Click Properties > Remote Operators tab > Add.

3 In the Select Objects dialog box, do the following:

3a Select an object type from the Object Type drop-down list.

3b To list the contents of a higher container, select the container from the Look in drop-down list.

3c Select an object, then click OK.

4 Click Apply > OK.

NOTE: To remove an object from the list of remote operators select the object and click the Remove button.

Operating with Windows XP Service Pack 2

Windows XP Service Pack 2 (SP2) comes with a firewall enabled by default. As a result, the Remote Management Agent and Remote Control Listener running on Windows XP SP2 will not be able to receive connections initiated by the Remote Management Console and the Remote Management Agent, respectively.

You will have to configure the firewall settings to allow the Remote Management Agent and the Remote Control Listener to receive connections.

By default, Remote Management Agent and the Remote Control Listener bind to TCP ports 1761 and 1762. In order to change the ports, refer to .

Starting Remote Management Operations Using ConsoleOne

The Remote Management Agent starts automatically when the managed workstation boots up. The remote operator can initiate a Remote Management session in any of the following ways:

Initiating Directory-Based Remote Management Session

NOTE: The selected user must have logged in to at least one managed workstation before Directory-Based Remote Management is initiated.

You can initiate directory-based Remote Management using either of the following methods:

From the Workstation Object

The following table lists the directions for initiating a Remote Management session.

Remote Management Session	To Initiate
Remote Control	Right-click the managed workstation, then click Actions > Remote Control.
Remote View	Right-click the managed workstation, then click Actions > Remote View.
File Transfer	Right-click the managed workstation, then click Actions > File Transfer.
Remote Execute	Right-click the managed workstation, then click Actions > Remote Execute.
Diagnostics	Right-click the managed workstation, then click Actions > Diagnostics.
Remote Wake Up	Right-click the managed workstation, then click Actions > Remote Wake Up.
Remote Audit	Right-click the managed workstation, then click Actions > Remote Audit.

From the User Object

1 In ConsoleOne, right-click a user object.

The selected user must have logged in to at least one managed workstation before Directory-Based Remote Management is initiated.

2 Click Remote Management.

3 In the Remote Management dialog box:

3a Select the IP address of the managed workstation which you want to Remotely Manage.

TIP: If the user has logged into the eDirectory through the Middle Tier, the list of IP address will contain the IP address of the Middle Tier. To filter this address, in the *console_one_installation_directory*\1.2\bin\drishtitype.ini file, add the XTierServerAddresses property and specify the Middle Tier IP addresses. For example, XTierServerAddresses = *Middle_Tier_IP_address1,* Middle_Tier_IP_address2, ...

3b Select a Remote Management operation which you want to perform on the selected managed workstation.

3c Select Directory-Based > OK.

Initiating Password-Based Remote Management Session

NOTE: The selected user must have logged in to at least one managed workstation before Directory-Based Remote Management is initiated.

Before initiating the Password-based Remote Management, ensure that the following prerequisites are met:

Is the managed workstation registered in eDirectory and imported as an eDirectory workstation object?	Has an eDirectory user logged at the managed workstation?	To initiate Password-Based Remote Management Session
Yes	Yes	◆ The Enable Password-Based Remote Management option in the Remote Control policy of the managed workstation object should be enabled.
		◆ The Enable Password-Based Remote Management option in the user object's Remote Management property page should be enabled.
		◆ The workstation user must have set a password on the managed workstation.
Yes	No	◆ The Enable Password-Based Remote Management option in the Remote Control policy of the managed workstation object should be enabled.
		◆ The workstation user must have set a password on the managed workstation.
No	Yes	◆ The workstation user must have set a password on the managed workstation.
No	No	◆ The workstation user must have set a password on the managed workstation.

You can initiate Password-Based Remote Management using either of the following methods:

- ◆ "From the ConsoleOne Menu" on page 761
- ◆ "From the User Object" on page 761

From the ConsoleOne Menu

1 In ConsoleOne, click Tools > Remote Management > Windows.

2 In the Remote Management dialog box:

2a Enter or select the IP address or DNS name of the managed workstation with which you wish to initiate a Remote Management session.

2b Enter the password set by the workstation user on the managed workstation.

2c Select a Remote Management operation which you want to perform on the selected managed workstation.

From the User Object

1 In ConsoleOne, right-click a user object.

The selected user must have logged in to at least one managed workstation before Password-Based Remote Management is initiated.

2 Click Remote Management.

3 In the Remote Management dialog box:

3a Select the IP address of the managed workstation which you want to remotely manage.

> **TIP:** If the user has logged into the eDirectory through the Middle Tier, the list of IP address will contain the IP address of the Middle Tier. To filter this address, in the *console_one_installation_directory*\1.2\bin\drishtitype.ini file, add the XTierServerAddresses property and specify the Middle Tier IP addresses. For example, XTierServerAddresses = *Middle_Tier_IP_address1,* Middle_Tier_IP_address2, ...

3b Select a Remote Management operation which you want to perform on the selected managed workstation.

3c Click Password.

3d Enter the password set by the workstation user on the managed workstation.

3e Click OK.

Initiating Remote Management Session from the Remote Management Agent

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

1 The user at the managed workstation 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.

To request for a session, the user at the managed workstation 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 Select the Directory option for directory-based authentication.

or

Select the Password option for password-based authentication.

2b If the password-based authentication is selected, enter the password for authentication.

2c Click OK.

Operating in Terminal Server environment

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

Starting Remote Management Operations Without Using ConsoleOne

The desktop4.exe application that ships with ZENworks 6.5 Desktop Management allows you to start the following Remote Management operations without using ConsoleOne: Remote Control, Remote View, Remote Execute, File Transfer, Remote Wake Up, and Remote Diagnostics.

You can install desktop4.exe using either of the following methods:

- Install the ZENworks 6.5 Desktop Management ConsoleOne snap-ins. This automatically installs desktop4.exe. Desktop4.exe is located in the *consoleone_installation_directory\consoleone_version*\bin directory.

- From the \desktop directory in the *ZENworks 6.5 Companion 2* CD, extract desktop.zip to a temporary directory on your machine. Copy the contents of *temporary_directory*\desktop to the *\consoleone_installation_location* directory.

Before you can run desktop4.exe, you must perform the following tasks.

1 For Password-Based Remote Management, enter the following details in the *consoleone_installation_directory*\bin\remagent.ini file:

Agent IP address: IP address of the managed workstation.

Agent Password: Remote Management Agent password.

Authentication Mode: `PASSWORD`.

Protocol: Enter `TCPIP`.

A sample remagent.ini file is as follows:

```
# Novell Inc.

AGENT_IPADDRESS=164.99.149.37

AGENT_PASSWORD=novell

AUTHENTICATION_MODE=PASSWORD

PROTOCOL=TCPIP
```

2 If you want to perform the Remote Management operation using Directory mode of authentication, you must log into the eDirectory tree to which the Managed workstation is imported. For Directory-Based Remote Management, ensure that the AUTHENTICATION_MODE in *consoleone_installation_directory*\bin\remagent.ini file is DS.

3 You can run desktop4.exe from the MS-DOS prompt or by using a .bat file. You must specify valid values for the following parameters

- **-w:** Fully qualified Distinguished Name (DN) of the managed workstation

- **-n:** eDirectory tree name

- **-c:** Remote Management operation to be performed on the managed workstation.

    To perform File Transfer, enter `-c"File Transfer"`
    To perform Diagnostics, enter `-c"Diagnostics"`
    To perform Remote Control, enter `-c"RemoteControl"`
    To perform Remote View, enter `-c"RemoteView"`
    To perform Remote Execute, enter `-c"Remote Execute"`

To perform Remote Wake-up, enter `-c"Remote Wakeup"`

For example, you can perform Remote control using either of the following methods:

- At the MS-DOS prompt, enter the following command:

```
Desktop4 -w"CN=WINXP-R1B164_99_151_48.OU=WsProm.O=novell" -n"INDYPROM-
TREE" -c"RemoteControl"
```

where Desktop4 is the name of the application; "CN=WINXP-R1B164_99_151_48.OU=WsProm.O=novell" is the DN of the managed workstation; "INDYPROM-TREE" is the eDirectory tree name; and "Remote Control" is the Remote Management operation to be performed on the managed workstation.

NOTE: You need to ensure that the remagent.ini file is updated with the specific details before you execute the desktop4.exe at the MS-DOS prompt.

- Using a .bat file.

1 Create a .bat file in the same directory as desktop4.exe with the following contents:

```
Desktop4 -w"CN=WINXP-R1B164_99_151_48.OU=WsProm.O=novell" -n"INDYPROM-
TREE" -c"RemoteControl"
```

where Desktop4 is the name of the application; "CN=WINXP-R1B164_99_151_48.OU=WsProm.O=novell" is the DN of the managed workstation; "INDYPROM-TREE" is the tree name; and "RemoteControl" is the Remote Management operation to be performed on the managed workstation.

2 Run the .bat file.

Depending upon the operation that you have specified, the Remote Management session starts.

Desktop4.exe is a back-end utility that can be leveraged by developing user-friendly interface to launch desktop4.exe.

Using desktop4.exe, you can also view Inventory information of the inventoried workstations. For more information, see "Viewing Inventory Information Without Using ConsoleOne" on page 1072.

Launching User-Based Remote Management using Desktop4.exe

You can launch Remote Management from desktop4.exe in both Password based or Directory Based authentication mode.

To launch Remote Management from desktop4.exe:

1 Run the desktop.exe and specify `-w`.

2 Populate the IP address of the managed workstation in which the user has logged in the *consoleone_installation_directory*\bin\remagent.ini file.

Configuring Remote Management Ports

The Remote Management Agent and Remote Control Listener bind to TCP ports 1761 and 1762, respectively. In case there is a conflict of port numbers with some application, you can change the port numbers to which they bind as follows:

- "Configuring the Remote Management Agent Port" on page 765
- "Configuring the Remote Control Listener Port" on page 765

Configuring the 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\remotemanagement\rmagent*\rmcfg.ini file.

2 Under the Remote Management Agent Port section, set the DefaultCommPort to the desired port number.

3 Restart the Novell ZfD Remote Management service.

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

1 Open the *ConsoleOne_directory\1.2\bin\rmports.ini.* file

2 Under the Remote Management Agent Ports section, add the port number.

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

Configuring the 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 ConsoleOne_directory\1.2\bin\rmports.ini file.

2 Under 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 workstations:

1 Open the *ZENworks_agent_directory*\remotemanagement\rmagent\rmcfg.ini file.

2 Under 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 under the Remote Control Listener Ports section.

67 Managing Remote Workstations

The following sections provide information that will help you effectively manage the Remote Management sessions of Novell® ZENworks® 6.5 Desktop Management:

Managing a Remote View Session

You can use ZENworks 6.5 to remote view the managed workstation.

The following sections explain the tasks you can perform to effectively manage a Remote View session:

Controlling the Display of the Viewing Window

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
Enable High Quality Scaling	Enhances the quality of images in the Scale To Fit Mode.
Enable Accelerator Keys	Allows you to enable or disable the default accelerator keys sequences.
Enable Encryption	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. 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.
Hide Wallpaper	Suppresses any wallpaper displayed on the managed workstation. This option is enabled by default. If you want to display the wallpaper on the managed workstation during a Remote View session, disable this option.
Color Quality	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: ◆ 16 Colors: Forces the use of 16-color palette on the managed workstation 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 workstation 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 workstation during a Remote Management session.
Network Type	if the managed workstation is connected by a LAN, select the Fast Links option to enhance the Remote Management performance. if he managed workstation is connected over a dial-up link or by WAN, select the Slow Links option to enhance the Remote Management performance.

3 To save the Control Parameter settings, click 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 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 770.

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.

The following table explains the Accelerator Key options you can use during the Remote View session:

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

Defining a Custom Accelerator Key Sequence

Default keystrokes assigned to the accelerator key option 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.

Managing a Remote Control Session

Remote Management lets you remote control a managed workstation. You can use Remote Control to provide user assistance and to help resolve workstation problems. With remote control connections, the remote operator can go beyond viewing the managed workstation to taking control of it.

You can effectively manage a Remote Control session by performing the following tasks:

- "Controlling the Display of the Viewing Window" on page 770
- "Using the Viewing Window Accelerator Keys" on page 772
- "Using the Toolbar Buttons on the Viewing Window" on page 773
- "Enabling the Wallpaper on the Managed Workstation" on page 774
- "Obtaining Information About Remote Management Sessions" on page 774

Controlling the Display of the Viewing Window

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

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
Blocks Mouse Movements to Agent	To reduce network bandwidth consumption, blocks all the mouse movements to the Agent.
Enable High Quality Scaling	Enhances the quality of images in the Scale To Fit mode.
Enable Accelerator Keys	Enables the accelerator keys on the management console so that you can change the default accelerator key sequences during the remote session.
Enable Encryption	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. 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.
System Key Pass	Passes Alt-key sequences from the management console to the managed workstation. **NOTE:** During a Remote View session, the System Key Pass-Through option is not enabled.
Hide Wallpaper	Suppresses any wallpaper displayed on the managed workstation. This option is enabled by default. If you want to display the wallpaper on the managed workstation during a Remote Control or Remote View session, disable this option.
Color Quality	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: ◆ **16 Colors:** Forces the use of 16-color palette on the managed workstation 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 workstation 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 workstation during a Remote Management session.
Network Type	If the managed workstation is connected by a LAN, select the Fast Links option to enhance the Remote Management performance. If the managed workstation is connected over a dial-up link or by WAN, select the Slow Links option to enhance the Remote Management performance.

4 To save the Control Parameter settings, click 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 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 770.

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.

The following table explains the Accelerator Key options you can use to control the display of the Viewing window:

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

Option	Default Keystroke	Description
Mouse/Keyboard Lock	Ctrl+L	Locks the keyboard and mouse controls at the managed workstation.
Blank Screen	Ctrl+Alt+B	Blanks the screen at the managed workstation.
Reboot	Ctrl+Alt+D	Sends the Ctrl+Alt+Del keystroke to the managed workstation.
		Invokes the Security window on Windows 2000/XP managed workstation. Invokes the reboot confirmation dialog on Windows 98 managed workstation.
Start	Alt+R	Invokes the start menu on the managed workstation.
Switch Applications	Ctrl+T	Switches applications on managed workstations.

Using the Toolbar Buttons on the Viewing Window

The following table describes the toolbar options in the Viewing window:

Button	Default Keystroke	Key Function
Screen Blanking	Ctrl+Alt+B	Enabled only if the Allow Blanking User's Screen option is enabled in the effective Remote Control policy of the managed workstation.
		Blanks the screen at the managed workstation. When the remote operator selects this option, the screen of the managed workstation is blacked out and the operations performed by the remote operator on the managed workstation are not visible to the user at the managed workstation.
		Not supported over certain display adapters. Refer to the ZENworks 6.5 Desktop Management Readme for the list of display adapters that do not support this feature.
Mouse and Keyboard Lock	Ctrl+L	Locks the keyboard and mouse controls at the managed workstation. When the remote operator selects this option, the user at the managed workstation will not be able to use the keyboard and mouse controls of the managed workstation.
System Start	Alt+R	Invokes the start menu on the managed workstations.
Application Switcher	Ctrl+T	Sends the Alt-tab key sequences to the managed workstation.
		Switches applications on managed workstations. If you use the toolbar button, you must click it continuously to traverse through the applications and then press Tab to select the desired application. If you use the Ctrl+Taccelerator key, you would have to use it as you would use the Alt+Tab sequence to switch between applications.
System Key Pass Through	Ctrl+Alt+S	Sets the system key pass to On or Off.
		Passes Alt-key sequences on the management console to the managed workstation.
Reboot	Ctrl+Alt+D	Sends the Ctrl+Alt+Del keystroke to the managed workstation.
		Displays the Security window on Windows 2000/XP managed workstation. Displays the reboot confirmation dialog on Windows 98 managed workstation.

Button	Default Keystroke	Key Function
Refresh	Ctrl+Alt+R	Refreshes the viewing window.
Full Screen Polling	Alt+L	Scans and renders the information of the entire screen of the managed workstation continuously.
Scale To Fit	Ctrl+Alt+G	Hides the scroll bars and scales the Remote Management window to fit your screen.
Session Encryption		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.

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. |

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 770.

Enabling the Wallpaper on the Managed Workstation

When the remote operator initiates a Remote Control session, any wallpaper displayed on the desktop of the managed workstation is suppressed. This feature reduces the response time from the managed workstation 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 workstation. When you terminate the Remote Control session, the suppressed wallpaper is restored.

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

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

2 Deselect the Hide Wallpaper option.

Obtaining Information About Remote Management Sessions

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

To view information about remote sessions:

1 Right-click the Remote Management Agent icon located in the system tray of the managed workstation.

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

The following table explains the general information you can obtain about Remote Management sessions from the Information window:

Parameter	Description
RM Operation	Lists the ongoing Remote Management sessions.
RM Information > Initiator	Displays the name of the remote operator.
RM Information > Protocol	Displays the protocol that the Remote Management Agent uses to communicate with the management console during a remote session.
Optimization Status > RC/RV Optimization	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 following categories of remote sessions:

 ◆ Remote Control

 ◆ Remote View

 ◆ File Transfer

 ◆ Remote Execute

 ◆ Others

Managing a Remote Execute Session

You can remotely run executables found on the managed workstation with system rights, even if the logged-in user is not a member of the local Administrator Group.

To execute an application program on a managed workstation, launch Remote Execute Window:

1 Enter the command line in the Remote Execute window.

Specify the complete path of the application if the application is not in the path of the managed workstation.

If you do not specify the extension of the file you want to execute at the managed workstation, Remote Execute will append the .exe extension.

2 Click Execute.

Enter the name of the application or the parameter within double quotes if the application or parameter has a space character. Following are a few examples:

```
"My Wordpad"

"C:\Program Files\Accessories\My Wordpad"

"C:\Program Files\Accessories\My Wordpad" "C:\myfile.txt"

"C:\Program Files\Accessories\My Wordpad" C:\myfile.txt

"Wordpad"
```

Managing a File Transfer Session

ZENworks 6.5 Desktop Management enables you to transfer files between the management console and a managed workstation. Right-click the file or folder to view the list of available menu options.

NOTE: Transferring larger files (by launching file transfer from ConsoleOne) may block the usage of ConsoleOne. In this case, launch the file transfer from desktop4.exe.

The following section explains how you can use File Transfer and the options that are available for working with files from the File Transfer window.

Using File Transfer Window Controls

The left pane of the File Transfer window shows the files in the current folder on the management console and the right pane shows the files on the managed workstation. The following table explains the function of the File Transfer controls:

Menu Option	Toolbar Option	Description
File > Open		Opens the selected file in its associated application at the management console.
		Opens the folder with the list of files at the management console.
File > Open with		Opens a dialog box that lists the applications, which are installed on the managed workstation. You can choose the application in which the file must open.
File > New Folder		Creates the folder with the specified name.
File > Delete		Deletes the selected files.
		Deletes the folder if the folder selected from the management console is empty.
File > Rename		Renames the selected file.
File > Properties		Displays the properties of a selected file or folder, such as size of the file and the date and time of last modification.
File > Upload		Moves files from the management console to the managed workstation.

Menu Option	Toolbar Option	Description
File > Download		Moves files from the managed workstation to the management console.
File > Exit		Closes the File Transfer window.
Edit > Cut		Transfers the selected files to the Clipboard.
Edit > Copy		Copies the selected files to the Clipboard.
Edit > Paste		Pastes the selected files from the Clipboard to the current location.
Edit > Select All		Selects all the files in the current pane.
Edit > Cancel All		Deselects all the files in the current pane.
View Refresh		Updates the display in the Operator Station pane and Target Station pane
Help		Displays help for this window.
Up One Level Folder button		Moves one level up in the directory tree.
		Right-click the file or folder to view the list of available menu options.
Operator Station Pane		The left pane of the File Transfer window shows the files in the current folder on the management console.
Target Station Pane		The right pane of the File Transfer window shows the files in the current folder on the managed workstation.

Managing a Remote Wake Up Session

The Remote Wake Up feature supports Magic Packet* technology. When a powered off node that is enabled for Wake on LAN receives the magic packet, the system will boot up.

This section provides information on the following topics:

Prerequisites

Before waking up the managed workstations, the following requirements must be fulfilled:

❑ Make sure that the managed workstation has a network card that supports Wake on LAN. Additionally, ensure that you have enabled the Wake on LAN option in the BIOS setup of the managed workstation.

❑ Make sure that the managed workstation is registered to Novell eDirectory™.

❑ Make sure that the remote node is in a soft-off power state. In the soft-off state, the CPU is powered off and a minimal amount of power is utilized by its network interface card. Unlike the hard-off state, in the soft-off state the power connection to the machine remains switched on when the machine is shut down.

❑ Make sure that the routers connecting the management console and the remote node are configured to forward subnet-oriented broadcasts

Remotely Waking Up the Managed Workstations

You can perform Remote Wake Up without configuring the Wake-on-LAN policy and service. To perform a Remote Wake Up:

1 In Novell ConsoleOne®, right-click a managed workstation, a group of managed workstations, a container, or a group of containers.

2 Click Actions > Remote Wake Up.

Setting Up a Scheduled Remote Wake Up Using the Wake-on-LAN Policy

Remote Management Wake-on-LAN service allows you to wake up a managed workstation or a set of managed workstations automatically by configuring the Wake-on-LAN policy.

To schedule the wake up of a managed workstation or a set of managed workstations automatically through the Wake-on-LAN service, you have to perform the following tasks in the order listed:

◆ "Configuring the Wake-on-LAN Service Object" on page 778

◆ "Configuring the Server Package for the Wake-on-LAN Service" on page 778

Configuring the Wake-on-LAN Service Object

1 In ConsoleOne, right-click the Wake-on-LAN service object (WOLService_*servername*), then click Properties > Look Up Schedule.

2 Modify the schedule to read the Wake-on-LAN policy.

3 Click OK.

IMPORTANT: If you modify the Wake-on-LAN schedule after starting the Wake-on-LAN service, you need to restart the Wake-on-LAN service. For more information, see "Starting the Wake-on-LAN Service" on page 779.

Configuring the Server Package for the Wake-on-LAN Service

1 In the ConsoleOne, right-click the Server package, then click Properties > Policies > General.

2 Click the Add button.

3 Select the Wake-on-LAN policy type and enter a name for the Wake-on-LAN policy.

4 Select the check box under the Enabled column for the Wake-on-LAN policy, then click Properties > Target List tab.

5 Click Add.

6 Select the workstations or the workstation container, then click OK.

7 Click the Policy Schedule tab.

8 Modify the policy schedule.

9 Click Apply > Close.

10 Click the Associations tab.

11 Browse to select the server object or the container where ZENworks 6.5 Desktop Management is installed, then click OK twice.

NOTE: You can create different policies for different target lists.

Starting and Stopping the Wake-on-LAN Service

   ◆ "Starting the Wake-on-LAN Service" on page 779

   ◆ "Stopping the Wake-on-LAN Service" on page 779

Starting the Wake-on-LAN Service

To load the Wake-on-LAN service on NetWare server, enter `startwol` at the console prompt.

To start the Wake-on-LAN service on Windows server,

1 From the Control Panel, double-click Administrative Tools.

2 Double-click Services.

3 Select Novell ZfD Wake-on-LAN Service.

4 Click Start.

Stopping the Wake-on-LAN Service

To stop the Wake-on-LAN service on NetWare server, enter `stopwol` at the console prompt.

To stop the Wake-on-LAN service on Windows server,

1 From the Control Panel, double-click Administrative Tools.

2 Double-click Services.

3 Select Novell ZfD Wake-on-LAN Service.

4 Click Stop.

You can also obtain the information about the Wake-on-LAN operations from the wolstatus.log file in the sys:\ directory on NetWare servers or *zenworks_installation_path*\remmgmt\server\bin\ directory on Windows servers.

Viewing the Audit Log of Remote Management Sessions Using Windows Event Viewer

ZENworks 6.5 Desktop Management records log information on a Windows 2000/XP managed workstation.

To view the audit log of 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.

NOTE: 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.

Desktop Management provides remote diagnostics of workstations. Remote diagnostics displays the event log information of Windows 2000/XP managed workstations. You can also view the audit log for Remote Management using the Event Log window. For more information, see "Event Log Information" on page 791.

Understanding the Audit Log

The Windows 2000/XP event logging mechanism allows applications running on the managed workstation to record events as log files. You can use the Event Viewer to view the event logs. The Event Viewer maintains Application, Security, and System log files. The events for Remote Management sessions are stored in the Application log file. The managed workstation where the Remote Management Agent is installed maintains this log information as an audit log. For more information, see "Viewing the Audit Log of Remote Management Sessions Using Windows Event Viewer" on page 779.

The audit log maintains the list of events for each Remote Management session and stores the following details:

- The success or failure of the authentication process
- The start time or end time of Remote Management sessions
- The name of the user attempting to remote manage the workstation
- The domain name and address of the management console accessing the managed workstation
- The remote operation performed on the managed workstation
- The name of the user logged in to the managed workstation
- The event success or failure status, and details for the failure

The following sections contain additional information:

- "Details of Events in the Audit Log" on page 780
- "Event Log Messages for Remote Management Sessions" on page 781

Details of Events in the Audit Log

The following table explains the information stored by each event during a Remote Management session:

Parameter	Description
Date	Date of the event occurrence.
Time	Time stamp of the event occurrence.
Computer	Name of the computer on which the event occurred.
Event ID	Unique ID assigned to the event.
Source	The source name for the Remote Management audit log is Remote Management Agent.
Type	The type of the event indicates if the particular event was a success, failure, information, warning, or error.

Parameter	Description
Category	The category lists the different events for the application. The details of an event are in the detailed message for the event. The events for Remote Management Agent are: • Authentication Event • Session Start Event • Session Terminate Event
Operation	The various operations that a management console user can perform on the managed workstation are: • Remote Control • Remote View • Remote Diagnostics • File Transfer • Remote Execute All events record the domain name of the remote operator who is remote accessing the managed workstation.
Console Address	IP address of the workstation that the remote operator uses to remote access the managed workstation.
Console DN	Domain name of the workstation that the remote operator uses to remote access the managed workstation.
Local User	Domain name of the user logged in to the managed workstation.
Event Message	The message for the event.

Event Log Messages for Remote Management Sessions

Informational and error messages are recorded for the following events during a Remote Management session:

-
-
-

You can view the details of events that occurred during a Remote Management session from the Description box in the Event Detail window. For more information about event details, see .

Authentication Event

The Authentication event records whether the Remote Management Agent could authenticate the remote user for that operation. The following table describes the Authentication Event messages:

Type	Message
Success	◆ Authentication was successful.
	◆ The password is successfully set for this workstation.
	◆ The password is successfully reset for this workstation.
Failure	◆ Authentication failed.

Session Start Event

The Session Start event records the time when a particular session was started. The following table describes the Session Start Event messages:

Type	Message
Information	Session started.

Session Terminate Event

The Session Terminate event details the time when the session was disconnected, and the reason for terminating the session. The following table describes the Session Terminate Event messages:

Type	Message
Information	Session terminated normally.

Remote Operator Identification Display

The Remote Management Agent displays the identification of the remote operator in the following dialog boxes on the managed workstation:

- ◆ Permission dialog box
- ◆ Visible signal dialog box

The information displayed can be one of the following (listed in the order):

1 If the managed workstation is imported to a ZENworks tree, and the remote operator has logged in to the ZENworks tree:

    1a If the Fullname attribute of the remote operator's user object has been populated, then the full name of the remote operator is displayed, for example, "Network Administrator." If it has not been populated, then the typeless name of the object is displayed. For example, "user.novell."

    1b If the Fullname attribute of the remote operator's user object has not been populated, then the typeless name of the remote operator's user object is displayed. For example, user.novell

2 If the managed workstation is not imported to a ZENworks tree, then the *Console_machine_name\console_windows_username* is displayed.

Managing a Remote Management Audit Session

The Remote Management Auditing mechanism allows you to store information about the Remote Management sessions running on the managed workstations as log files.

The Remote Management Audit session is launched automatically as soon as the management console initiates a Remote Management session with the managed workstation.

The Remote Management sessions are logged as audit records. The managed workstation where the Remote Management Agent is installed logs the audit records into the auditlog.txt file. The auditlog.txt file is created and updated only when there are no Remote Management sessions in progress. The audit session information is recorded from the fourth line in the auditlog.txt file. You can find the auditlog.txt file in the system directory of the managed workstation:

The following table explains the information stored by each event during a Remote Management session:

Parameter	Description
Start Time	Start time of the event occurrence.
Duration	Duration of the Remote Management session.
Console DN	Distinguished name of the workstation that the remote operator uses to remote access the managed workstation.
Console user DN	Distinguished name of the remote operator.
Operation Code	The various operations that a management console user can perform on the managed workstation are: ◆ Remote Control, indicated by 1 ◆ Remote View, indicated by 2 ◆ File Transfer, indicated by 3 ◆ Remote Execute, indicated by 5 ◆ Remote Diagnostics, indicated by 6
Operation Status	The status of the event indicates if the particular event was a success or failure. 1 indicates that the Remote Management operation was successful and 0 indicates that the Remote Management operation was unsuccessful.

A sample entry is as follows:

```
1005572546000 1000 rajwin2ktestpc admin.novell 1 0
```

All the parameters in an audit record are separated by spaces. Each record is logged in a new line. The auditlog.txt file can store a maximum of one hundred records and is saved in the system directory.

Viewing the Audit Logs from a Centralized Database

You can store the audit records of all the managed workstations in a database in a centralized location. To store the auditlog.txt files in a database, you have to install the Workstation Inventory Agent on every managed workstation. For information on installing the Workstation Inventory Agent, see the Novell ZENworks 6.5 Desktop Management Installation Guide.

The Inventory Scanner collects the audit records and store them as scan data files in the scan directory at the Inventory server. The Inventory Storer stores the files in the Inventory database.

NOTE: If the Inventory Server rolls up scan data across servers, the audit records are not rolled up after the data stored for the first time.

You can configure the number of audit records per workstation that can be stored in the Inventory database using the RM Audit property page.

To configure the RM Audit property page:

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

2 Click the RM Audit tab.

3 Specify the maximum number of records per workstation that can be stored in the Inventory database.

4 Specify the life span of the audit records.

If the Inventory database has enough space to store new records, the audit records are not deleted from the auditlog.txt file even after their expiry time. But if the Inventory database doesn't have enough space to store new records, the oldest audit records are deleted even before their expiry time.

Generating Remote Management Report

You can run reports to gather Remote Management information from the Inventory database.

The Remote Management information is taken from the Inventory database you configure.

You can print or export the report as desired. Remember that any reports you generate will be empty if you have not configured ZENworks 6.5 Desktop Management to start populating the Inventory database with the data you want.

This section covers the following sections:

- "Prerequisites for Generating Remote Management Reports" on page 784
- "Generating a Remote Management Report" on page 785
- "Printing a Remote Management Report" on page 785
- "Exporting a Remote Management Report to a File" on page 785

Prerequisites for Generating Remote Management Reports

Before running the inventory reports you must perform the following tasks:

- Configure the Inventory database. For more information, see "Configuring the Inventory Database" on page 1036.

  The Remote Management reports always use the Inventory database you configured as the data source for your reports unless you change it later as described in "Configuring the Inventory Database" on page 1036.

- Before running the inventory reports you must make sure that the appropriate ODBC client for Sybase, Oracle, or MS SQL is installed on the machine running ConsoleOne. The ODBC driver is automatically configured on the machine when you invoke the Inventory report. For more information on how to configure the ODBC client, see "Installing the ODBC Drivers" in the *Novell ZENworks 6.5 Desktop Management Installation Guide*.

Generating a Remote Management Report

1 In ConsoleOne, configure database through Tools > ZENworks Inventory > Configure DB...

2 Click Tools > ZENworks Reports.

3 From the Available Reports list, double-click RM Audit Reports, then click Remote Management Report.

The description for the report is displayed on the right side of the screen.

4 Specify the selection criteria.

Date of Operation: Enter a date when the Remote Management operation occurred. All the records of the Remote Management operation subsequent to the specified date are listed.

Console DN: Enter the Distinguished Name (DN) of the workstation that the remote operator uses to remote access the managed workstation.

Console User DN: Enter the DN of the remote operator.

Target Workstation DN: Enter the DN of the managed workstation.

Operation: Select the Remote Management operation for which you want to generate the report.

Operation Status: Select the status of the selected Remote Management operation.

In the Reporting dialog box, you can use wildcards: an asterisk (*). The wildcard character can be used for character data only.

The following table lists examples of wildcards.

Example	Specifies to Include
*	All items
wNT*	All items starting with "wNT"
wNTcpq.xcorp	The single named item, in this case a workstation

5 Click Run Selected Report.

A status box appears displaying the progress of the report generation. When the report is generated, it appears in the viewer. Use the buttons on the toolbar to page through, print, or export the report.

Printing a Remote Management Report

1 Generate and view the report.

2 To change the default settings of the Printer, click the Printer Setup icon and modify the settings.

3 Click the printer icon.

Exporting a Remote Management Report to a File

1 Generate and view the report.

2 On the toolbar, click the Export Report icon.

3 In the dialog box, specify the location and file format, then click OK.

4 Browse for and select the directory where you want to save the exported file.

5 Click OK.

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 workstation in the Control Parameters dialog box.

- Assign color settings on the management console higher than the managed workstation or assign the same color settings for the management console and the managed workstation.

- 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 Workstation

- 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 workstation, 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 it or close it.

- Make sure that the scrolling texts (such as the debug windows) and animations are not active on the managed workstation.

- Make sure to minimize or close the dialog boxes that are not in use.

- To perform any operations at the managed workstation, 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 workstation:

  - Set the color mode of the managed workstation to 16 color.

  - Select the Slow Link Option.

Using the Remote Management Agents

You can access and remote control the managed workstations if you have installed the Remote Management Agent on the managed workstations.

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

- "Shutting Down the Remote Management Agent" on page 787
- "Restarting the Remote Management Agent" on page 787
- "Using the Remote Management Agent icon" on page 788

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 reload the Remote Management Agent. For more information, see "Restarting the Remote Management Agent" on page 787.

To shut down the Remote Management Agent on a Windows* 2000/XP managed workstation:

1 From the Control Panel, double-click Administrative Tools.

2 Double-click Services.

3 Select Novell ZfD Remote Management service.

4 Click Stop.

To shut down the Remote Management Agent on a Windows 98 managed workstation:

1 Right-click the Remote Management Agent icon in the system tray.

2 Click Shutdown Agent.

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

Restarting the Remote Management Agent

During the ZENworks 6.5 Desktop Management installation, the Remote Management Agent is installed on the managed workstation and started automatically when the managed workstation 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 workstation.

To restart the Remote Management Agent on a Windows 2000/XP managed workstation:

1 From the Control Panel, double-click Administrative Tools.

2 Double-click Services.

3 Select Novell ZfD Remote Management service.

4 Click Start.

To restart the Remote Management Agent on a Windows 98 managed workstation:

1 Go to the *ZENworks_agent_installation_directory*\remotemanagement\rmagent directory.

2 Double-click Zenrem32.exe.

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

Using the Remote Management Agent icon

By default, the Remote Management Agent icon is displayed in the system tray of the managed workstations. This icon indicates that the Remote Management Agent is loaded on the managed workstation.

If the Remote Management Agent is loaded and the Remote Management Agent icon is not displayed in the system tray, it indicates that you have disabled the display option in the Remote Control Policy settings.

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

Option	Description
Terminate RC/RV Session	Disconnects and closes the remote session on the managed workstation and displays a message on the management console indicating that the remote session is closed.
Security	Allows the user at the managed workstation to set or clear the password for the workstation
Information	Displays information such as who is accessing the managed workstation for the remote session, security settings, and the protocol in use for the remote session. For details, see "Obtaining Information About Remote Management Sessions" on page 774. You can right-click or double-click the Remote Management Agent icon to view the Information window.
Shutdown Agent	Allows the user logged into the Windows 98 managed workstation to shutdown the Remote Management Agent. This option is not applicable for Windows 2000/XP managed workstations. To shutdown the Remote Management Agent on Windows 2000/XP managed workstations, the user must go to the Service Control Panel and stop the "Novell ZfD Remote Management" service.
Request Session	Enables the user at the managed workstation to request a remote operator to perform remote session.
Help	Displays the Remote Management Agent help.

68 Viewing the Diagnostic Information

You can diagnose the managed workstation and obtain information that will help you analyze problems at the managed workstation.

You can view real-time managed workstation diagnostic information from the management console. For more information, see "Viewing Diagnostic Information for a Managed Workstation" on page 789.

Before you begin to obtain the diagnostic information, ensure that the Remote Management Agent is installed on the managed workstation. During the Remote Management Agent installation, the Diagnostic Agent is also installed on the managed workstation, which runs automatically when the managed workstation boots up. When the management console user requests diagnostic information from the managed workstation, the Diagnostic Agent on the managed workstation procures the requested information and provides it to the Remote Management Agent, which then makes it available to the management console.

Viewing Diagnostic Information for a Managed Workstation

You can view diagnostic information that will help you analyze problems at the managed workstation.

IMPORTANT: If you have not installed the Novell® Client™ on the managed workstation, you cannot view the information about NetWare Connections, Novell Client, Network Drives, Network Open files, and Print Capture.

To view diagnostic information:

1 Right-click the managed workstation from the management console.

2 Click Actions > Diagnostics.

2a To view the Windows Memory window, expand the Diagnostics folder > Operating System folder > Memory folder, then click Windows Memory.

For more information, see "Windows Memory Information" on page 790.

2b To view the Environment window, expand the Diagnostics folder > Operating System folder, then click Environment.

For more information, see "Environment Information" on page 791.

2c To view the Event Log window, expand the Diagnostics folder > Operating System folder, then click Event Log > Security, System, or Application.

Click an event row in the Event Log table to view a description of the event.

For more information, see "Event Log Information" on page 791.

2d To view the Device Drivers window, expand the Diagnostics folder > Operating System folder, then click Device Drivers.

For more information, see "Device Drivers Information" on page 792.

2e To view the Services window, expand the Diagnostics folder > Operating System folder, then click Services.

For more information, see "Services Information" on page 792.

2f To view the Services window, expand the Diagnostics folder > Operating System folder, then click WIN32 Processes.

For more information, see "WIN32 Process Information" on page 793.

2g To view the Services window, expand the Diagnostics folder > Operating System folder, then click WIN32 Modules.

For more information, see "WIN32 Modules Information" on page 793.

2h To view the NetWare Connections window, expand the Diagnostics folder > Network folder, then click NetWare Connections.

For more information, see "NetWare Connections Information" on page 793.

2i To view the Novell Client window, expand the Diagnostics folder > Network folder, then click Novell Client.

For more information, see "Novell Client Information" on page 794.

2j To view the Network Protocols window, expand the Diagnostics folder > Network folder, then click Network Protocols.

For more information, see "Network Protocols Information" on page 794.

2k To view the Name Space Providers window, expand the Diagnostics folder > Network folder, then click Name Space Providers.

For more information, see "Name Space Providers Information" on page 795.

2l To view the Network Drives window, expand the Diagnostics folder > Network folder, then click Network Drives.

For more information, see "Network Drives Information" on page 795.

2m To view the Network Open Files window, expand the Diagnostics folder > Network folder, then click Network Open Files.

For more information, see "Network Open Files Information" on page 797

2n To view the Print Capture window, expand the Diagnostics folder > Network folder, then click Print Capture.

For more information, see "Print Capture Information" on page 797.

You can use the Edit menu options to copy all or selected diagnostic information from the diagnostics window to a text editor for later analysis.

Windows Memory Information

On Windows 2000/XP managed workstations, the Windows Memory window displays the percentage of memory in use, physical memory, paging details, and free space details.

The following table describes the fields in the Windows Memory window:

Field	Description
Memory Load (%)	Percentage of memory utilization. Zero percentage memory indicates memory usage is nil; 100% indicates that all the available memory is in use.
Total Physical Memory (MB)	Total physical memory in MB.
Free Physical Memory (MB)	Amount of available physical memory in MB.
Total Paging File Size (MB)	Total number of MB that can be stored in the paging file. This number does not indicate the actual physical size of the paging file on the managed workstation.
Free Space in Paging File (MB)	Number of MB available in the paging file.
Total Address Space (MB)	Total number of MB described in the user mode portion of the virtual address space of the calling process.
Free User Bytes (MB)	Number of MB in unreserved and uncommitted memory of the user address space of the calling process.

Environment Information

The Environment window displays the variables set at the managed workstation. You can view the Environment information on Windows 2000/XP managed workstations.

The following table describes the fields in the Environment window:

Field	Description
Variables	Environment variable name.
Value	Value of the variable or the path.

Event Log Information

Event logging in Windows 2000/XP provides a standard, centralized way for applications and the operating system to record important software and hardware events. Event logging provides a means to merge events from various sources into a single informative story. The event log diagnostics help the remote operator view the System, Security, and Application event logs. You can view the Event Log Information on Windows 2000/XP managed workstations.

The following table describes the fields in the Event Log window:

Field	Description
Event Generated Date	Date when the entry was submitted (MM/DD/YYYY).
Event Generated Time	Time when the entry was submitted (HH:MM:SS).
Event ID	Identifies the event specific to the source that generated the event log entry.

Field	Description
Event Generated Type	Classification of the type as Error, Warning, Information, Success, or Failure.
Event Generated Category	Subcategory for the event. This subcategory is source specific.
	NOTE: Every application registering for Windows Event log needs to specify message resource file for Event Category.
	Event Category is application specific and is defined in message file. Diagnostics reads this information from HKLM\system\CurrentControlSet\Services\EventLog\<application>, maps the category to message and fetches the category.
	Some applications do not specify message resource file for Event Description and Event Category. In this case, Windows assigns arbitrary numbers for event category. Also, there is no way to get this arbitrary number (as it is not stored in registry). The Diagnostics reports it as None.
Source Name	Name of the source (application, service, driver, subsystem) that generated the entry.
Description	Details of the event.
Computer Name	Name of the computer that generated the event.

Device Drivers Information

The Device Drivers window displays information about the device drivers installed on Windows 2000/XP managed workstations. You can use the information in this window to determine whether the workstation has the required drivers loaded and their status.

The following table describes the fields in the Device Driver window for Windows 2000/XP managed workstations:

Field	Description
Name	Name of the device driver.
State	Indicates if the device driver is Stopped or Running.

Services Information

The Services window indicates which services are available on Windows 2000/XP managed workstations, and lists the state of each service.

The following table describes the fields in the Services window:

Item	Description
Service Name	List of services available on the workstation.
State	Indicates if the service is Stopped or Running.

WIN32 Process Information

Diagnostic information about processes is available on Windows 98 managed workstations.

To view the WIN32 modules associated for a particular Windows 32-bit process, double-click the row entry in the WIN32 Processes window.

The following table describes the fields in the WIN32 Processes window:

Field	Description
Path	Path and filename of the executable file for the process.
PID	Processor identifier.
PPID	Parent processor identifier.
No. of threads	Number of execution threads started by the process.
Usage Count	Number of references to the process. A process exists as long as its usage count is non-zero. When the usage count becomes zero, the process terminates.

WIN32 Modules Information

The WIN32 Modules window displays the list of modules associated with a specified process on Windows 98 managed workstations.

The following table describes the fields in the WIN32 Modules window:

Field	Description
Module ID	Module identifier in the context of the owning process.
Global Usage Count	Global usage count on the module.
Process Usage Count	Module usage count in the context of the owning process.
Module Path	Location of the module.
Module Size (KB)	Size of the module in KB.

NetWare Connections Information

The NetWare Connections window displays information about all current connections for the Novell Client. It also indicates the current server and current tree.

The following table describes the fields in NetWare Connections window:

Field	Description
Server Name	Names of the servers and trees the workstation is connected to.
User Name	Username for each connection.
Connection Number	User's connection number on the server.

Field	Description
Authentication State	Connections are either NDS® or bindery connection.
NDS Tree	NDS Directory tree for each connection to a server that is running NetWare®4 or later.
Transport Type	The transit protocol in use between the server and the workstation.
Address	The internal address of the server.
Resource Type	Identifies the primary server.

Novell Client Information

The Novell Client window displays the information about the installed Novell Client and its settings.

The following table describes the fields in the Novell Client window:

Field	Description
Preferred Server	NetWare server that is used for NDS authentication of the user when the Novell Client for Windows workstation software is started.
Preferred Tree	Directory tree that the client first attaches to when the Novell Client for Windows software is started.
Name Context	The current position or context in the NDS tree structure. This setting is applicable only to client workstations connecting to a NetWare 4 or NetWare 5 network.
First Network Drive	Network drive that is selected when you connect to a NetWare server.
Client Version	Novell Client32 ™ version number.

Network Protocols Information

The Network Protocols window displays the information about the active network protocols on a managed workstation using WinSock. The WinSock architecture also allows for simultaneous access to multiple transport protocols. WinSock contains the Windows Open System Architecture (WOSA) compliant architecture, which allows applications to access protocols including TCP/IP.

The following table describes the fields in the Network Protocols window:

Field	Description
Properties	Specifies characteristics of the protocol.
Address Family	Defines the structure of protocol addresses that are in use by the protocol.

Field	Description
Socket Type	Represents the different socket types for the BSD socket interface. It can have the following values: ◆ Stream ◆ Datagram ◆ Raw Socket ◆ Seq. Packet ◆ RDM Socket ◆ Unknown
Protocol ID	Protocols identifier.
Message Size (Bytes)	Specifies the maximum message size (in bytes) supported by the protocol. This is the maximum size of a message that can be sent from or received by the host. For protocols that do not support message framing, the actual maximum size of a message that can be sent to a given address might be less than this value. If the protocol is stream-oriented, the concept of message size is not relevant. If the protocol is message-oriented, there is no maximum message size.
Protocol Name	Name of the protocol that is supported, such as TCP/IP, UDP/IP, or IPX™.

Name Space Providers Information

The Name Space Providers window displays information about the Name Space Provider registered with WinSock Name Resolution and Registration APIs. WinSock 2 includes a new set of API functions that standardize how the applications access and use the various network naming services. This information is not displayed for workstations with WinSock 1.1.

The following table describes the fields in the Name Space Providers Information window:

Field	Description
Name space	Specifies the name space (SAP, DNS, SLP).
Connected	Displays whether the Name Space Provider is enabled on the workstation.
Version	The name space version identifier.
Service Provider	Displays the string for the name space provider.

Network Drives Information

The Network Drives window displays information about mapped drives, drive capacity, volume label, file system information, sector size, and cluster size. The following table describes the fields in the Network Drives window:

Field	Description
Drive Letter	Mapped drive letter.
Path	NetWare path of the volume or directory to which the drive is mapped. For example, if the directory zenworks on sys: volume of server zen_kyoto is mapped to drive Q, the path displays zen_kyoto\sys:zenworks.
File System	File system type for the mapped NetWare directory or volume.
Effective Rights	- Read For a folder, grants the right to open files in the folder and read the contents or run the programs. For a file, grants the right to open and read the file. - Write For a folder, grants the right to open and change the contents of files in the folder. For a file, grants the right to open and write to the file. - Create For a folder, grants the right to create new files and folders in the folder. For a file, grants the right to create a file and to salvage a file after it has been deleted. - Delete Grants the right to delete the folder or file. - Modify Grants the right to change the attributes or name of the folder or file, but does not grant the right to change its contents. Changing the contents requires the Write right. - File Scan Grants the rights to see the folder or file with the DIR or NDIR command. - Ownership Grants the ownership rights of the file, folder, or volume. If the corresponding rights are not given to the user, Effective Rights displays a hyphen (-).
Long Name Size (Bytes)	Maximum length in characters of a filename component supported by the specified file system. For example, for a FAT file system supporting long names, the value is 255. The value for a DOS file system is 11.
Sector Size (Bytes)	Sector size in bytes.
Sectors Per Cluster	Number of sectors per cluster.
Total Clusters	Size of the volume in clusters.
Free Clusters	Number of clusters currently free for allocation. This number includes the space that is reclaimed from the sub-allocation file system and also clusters freed from deleted files.

Network Open Files Information

The Open Files window displays the names of files open on a NetWare server corresponding to the connection ID from the mapped drives of managed workstation.

The following table describes the fields in the Network Open Files window:

Field	Description
File Name	Name of the file.
Volume Name	Name of the volume.
Server Name	Name of the file server.
User	The NetWare name under which the user's workstation is logged in to the file server.
Connection ID	Connection ID on which the file is opened.

Print Capture Information

The Print Capture window displays information about the captured queues, print options for each parallel port on the managed workstation, and current status of each port.

The following table describes the fields in the Print Capture window:

Field	Description
Printer Device Name	LPT device. Number of LPT ports for which captures can be managed.
Port State	Specifies whether the LPT device is captured.
Captured Queues	Captured print queue name.

Documentation Updates

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® 6.5 Desktop 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 dates:

February 11, 2005 (Support Pack 1)

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

Location	Change
"Operating in Terminal Server environment" on page 762.	Added this section to "Starting Remote Management Operations Using ConsoleOne" on page 759 as part of the Support Pack 1 update.
"Starting Remote Management Operations Without Using ConsoleOne" on page 763.	Clarified the content in the second bullet point describing how to install desktop4.exe.

July 23, 2004

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

Location	Change
"Remote Operator Identification Display" on page 782.	Updated Step 1 on page 782.