Novell ZENworks® Configuration Management

10

www.novell.com

REMOTE MANAGEMENT REFERENCE

February 22, 2008

Novell®

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

This *Novell ZENworks 10 Configuration Management Remote Management Reference* includes information about Remote Management. The information in this guide is organized as follows:

Audience

This guide is intended for Novell® ZENworks® administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to the Novell Documentation Feedback site (http://www.novell.com/documentation/feedback.html) and enter your comments there.

Additional Documentation

ZENworks Configuration Management is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the ZENworks 10 Configuration Management documentation (http://www.novell.com/documentation/zcm10/index.html).

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux*, should use forward slashes as required by your software.

Overview

1

Novell® ZENworks® Configuration Management lets you remotely manage devices from the management console. Remote Management allows you to:

- Remotely control the managed device
- Remotely run executables on the managed device
- Transfer files between the management console and the managed device
- Diagnose problems on the managed device
- Remotely wake up a powered-off managed device

Review the following sections:

- Section 1.1, “Remote Management Terminology,” on page 9
- Section 1.2, “Understanding Remote Management Operations,” on page 10
- Section 1.3, “Understanding Remote Management Features,” on page 11

1.1 Remote Management Terminology

Terms	Description
Managed device	A device that you want to remotely manage. To remotely manage a device, ensure that the Remote Management component is installed and the Remote Management service is running on the device.
Management server	A device where the ZENworks Configuration Management server is installed.
Management console	The interface for managing and administering the devices.
Administrator	A person who can configure Remote Management policies and settings, and grant Remote Management rights to remote operators.
Remote Management service	A managed device component that enables remote operators to perform remote sessions on the device.
Remote Management viewer	A management console application that enables a remote operator perform remote sessions on the managed device. It allows the remote operator to view the managed device desktop, transfer files and execute applications on the managed device. **NOTE:** Remote Management viewer is not yet supported on Linux platform.
Remote Management Listener	A management console application that enables a remote operator accept remote assistance requests from managed device users

1.2 Understanding Remote Management Operations

Remote Management gives administrators control of a device without the requirement for an on-site visit. It can save you and your organization time and money. For example, you or your organization's help desk can analyze and remotely fix the managed device problems without visiting the user's workstation, thereby reducing problem resolution times and increasing productivity.

The following sections helps you to understand the various Remote Management operations:

1.2.1 Remote Control

Remote Control lets you remotely control the managed device from the management console so that you can provide user assistance and help resolve the device problems.

Remote Control establishes a connection between the management console and the managed device. With remote control connections, you can perform all the operations that a user can perform on the device. For more information, see Section 3.1, "Managing a Remote Control Session," on page 31.

1.2.2 Remote View

Remote View lets you remotely connect with a managed device so that you can view the managed device instead of controlling it. This helps you troubleshoot problems that the user encountered. For example, you can observe how the user at a managed device performs certain tasks to ensure that the user performs the task correctly. For more information, see Section 3.2, "Managing a Remote View Session," on page 35.

1.2.3 Remote Execute

Remote Execute lets you run any executable on the managed device from the management console with system privileges. To remotely execute an application, specify the executable name in the Remote Execute window. For example, you can execute the `regedit` command to open the Registry Editor on the managed device. For more information, see Section 3.3, "Managing a Remote Execute Session," on page 36.

1.2.4 Remote Diagnostics

Remote Diagnostics lets you to remotely diagnose and analyze the problems on the managed device. This increases user productivity by keeping desktops up and running. For more information, see Section 3.4, "Managing a Remote Diagnostics Session," on page 36.

Diagnostics provide real-time information that you can use to diagnose and fix the problems on the managed device. The default diagnostics applications on the managed device include:

- System Information
- Computer Management
- Services
- Registry Editor

1.2.5 File Transfer

File Transfer lets you perform various file operations on the management console and the managed device, such as:

- Copy files between the management console and the managed device.
- Rename files or folders
- Delete files or folders
- Create directories
- View the properties of files and directories
- Open files with the associated applications on the management console

For more information, see Section 3.5, “Managing a File Transfer Session,” on page 37

IMPORTANT: The File Transfer program allows you to access the network drives on the managed device.

1.2.6 Remote Wake Up

Remote Wake Up lets you remotely wake up a single node or a group of powered-down nodes in your network provided the network card on the node is enabled for Wake-on-LAN. For more information, see Section 3.6, “Waking Up a Remote Device,” on page 40

1.3 Understanding Remote Management Features

The following sections helps you to understand the various Remote Management features:

- Section 1.3.10, “Agent Initiated Connection,” on page 13
- Section 1.3.11, “Session Collaboration,” on page 13
- Section 1.3.12, “Remote Management Auditing,” on page 13

1.3.1 Visible Signal

Lets you provide a visible indication on the managed device desktop to inform the user that the device is being remotely managed. The visible signal displays the identification of the remote operator and the session details such as type of the remote session and start time of the session. The user can terminate a particular remote session or close the signal dialog box to terminate all the remote sessions.

1.3.2 Intruder Detection

The Intruder Detection feature significantly lowers the risk of the managed device being hacked. If the remote operator fails to log in to the managed device within the specified number of attempts (the default is 5), the Remote Management service is blocked and does not accept any remote session request until it is unblocked.

1.3.3 Session Encryption

The remote sessions are secured using Secured Socket Layer (TLSv1 protocol).

1.3.4 Audible Beep

Lets you generate an audible signal on the managed device at regular time intervals as configured in the Remote Management policy when a remote session is active on the managed device.

1.3.5 Keyboard and Mouse Locking

Lets you lock the keyboard and mouse controls of the managed device during a remote session to prevent the managed device user from interrupting the session.

1.3.6 Screen Blanking

Lets you blank the screen on the managed device during a remote session to prevent the user from viewing the actions performed by the remote operator during the session. The keyboard and mouse controls of the managed device are also locked.

1.3.7 Abnormal Termination

Lets you lock the managed device or log out the user on the managed device if a remote session is abruptly disconnected.

1.3.8 Overriding Screen Saver

Lets you override any password-protected screen saver on the managed device during a remote session.

NOTE: This feature is not available on a Windows Vista* managed device.

1.3.9 Automatic Session Termination

Lets you automatically terminate a remote session if it has been inactive for a specified duration.

1.3.10 Agent Initiated Connection

Lets you enable the user on the managed device to request assistance from a remote operator. You can preconfigure the list of remote operators to be available to the user. For more information, see Section 2.6.2, “Initiating a Session from the Remote Device,” on page 28.

1.3.11 Session Collaboration

Lets a group of remote operators collaborate to jointly perform a remote session. The master remote operator can invite other remote operators to the session, delegate the remote control rights to another remote operator to solve a problem, regain control from the remote operator, and terminate a remote session. For more information, see Section 3.1.2, “Session Collaboration,” on page 33.

1.3.12 Remote Management Auditing

Lets you generate audit records for every remote session performed on the managed device. The audit log is maintained on the managed device and is viewable by the user.

Setting Up Remote Management

2

The following sections provide information on deploying the Remote Management component of Novell® ZENworks® 10 Configuration Management in a production environment:

2.1 Configuring the Remote Management Settings

The Remote Management settings are rules that determine the behavior or the execution of the Remote Management service on the managed device. The settings include configuration for the ports, session settings, and performance settings during the remote session. These settings can be applied at zone, folder, and device levels.

The following sections provide information on configuring the Remote Management settings at the different levels:

2.1.1 Configuring the Remote Management Settings at the Zone Level

By default, the Remote Management settings configured at the zone level apply to all the managed devices.

1. In ZENworks Control Center, click *Configuration*.
2. In the Management Zone Settings panel, click *Device Management*, then click *Remote Management*.
3. Select *Run Remote Management Service on Port* and specify the port to enable the Remote Management service to run on that port.

   By default, the Remote Management service listens on port number 5950.
4. Select *Look Up Viewer DNS Name at the Start of the Remote Session* to enable the Remote Management service to look up for the DNS name of the management console at the start of the remote session.

The name is saved in the audit logs and is displayed as a part of the session information during the remote sessions. If this option is not selected or the Remote Management service is unable to find the console name, then the console name is displayed as *unknown*.

If your network does not have reverse DNS lookup enabled, then we recommend that you disable this setting to prevent a significant delay in starting the remote session.

5 Select from the following options for improving the performance of a remote session:

Field	Details
Suppress Wallpaper	Suppresses the wallpaper on the managed device during a remote session. This prevents the bitmap data of wallpaper from being repeatedly sent to the Remote Management console and thereby enhances the performance of the remote session.
Enable Optimization Driver	Enables the optimization driver, which is installed by default on every managed device. If you select this option, only the changed portion of the screen on the managed device is captured and updated on the Remote Management console during the remote session, thereby enhancing the performance of the remote session.

6 (Optional) Configure an application to be launched on the managed device during the Remote Diagnostics session by adding it to the *Diagnostics Applications* list. By default, the list includes the following applications:

- System Information
- Computer Management
- Services
- Registry Editor

The following table lists the tasks that you can perform to customize the *Diagnostics Applications* list:

Task	Details
Add an application	1. Click *Add*. 2. Specify the application name and the application path on the managed device. 3. Click *OK*.
Delete an application	1. Select the application you want to delete. 2. Click Delete, then click *OK*.
Revert to default applications	1. Click *Revert*, then click *OK*.

7 Click *Apply*, then click *OK*.

These changes are effective on the device, when the device is refreshed.

2.1.2 Configuring the Remote Management Settings at the Folder Level

By default, the Remote Management settings configured at the zone level are applied to all the managed devices. However, you can modify these settings for the devices within a folder:

1. In ZENworks Control Center, click *Devices*.
2. Click the folder (details) for which you want to configure the Remote Management settings.
3. Click *Settings*, then click *Device Management* > *Remote Management*.
4. Click *Override*.
5. Edit the Remote Management settings as required.
6. To apply the changes, click *Apply.*

   or

   To revert to the system settings configured at the zone level, click *Revert*.
7. Click *OK*.

These changes are effective on the device, when the device is refreshed.

2.1.3 Configuring the Remote Management Settings at the Device Level

By default, the Remote Management settings configured at the zone level are applied to all the managed devices. However, you can modify these settings for the managed device:

1. In ZENworks Control Center, click *Devices*.
2. Click *Servers* or *Workstations* to display the list of managed devices.
3. Click the device for which you want to configure the Remote Management settings.
4. Click *Settings*, then click *Device Management* > *Remote Management*.
5. Click *Override*.
6. Edit the Remote Management settings as required.
7. To apply the changes click *Apply.*

   or

   To revert to the system settings configured at the zone level, click *Revert*.
8. Click *Ok*.

These changes are effective on the device, when the device is refreshed.

2.2 Enabling the Remote Management Listener

To enable the Remote Management Listener to listen for connections from a managed device:

1. In ZENworks Control Center, click *Devices*.
2. In *Device Tasks* in the left pane, click Remote Management Listener.
3. In the Remote Management Listener dialog box, specify the port to listen for the remote connections. By default, the port number is 5550.

4 Click *OK*. The ZENworks Remote Management Listener icon appears in the notification area.

2.3 Configuring the Remote Management Policy

The Remote Management policy lets you configure the behavior or execution of a Remote Management session on the managed device. The policy includes properties such as Remote Management operations and security.

By default, a secure Remote Management policy is created on the managed device when the ZENworks Adaptive Agent is deployed with the Remote Management component on the device. You can use the default policy to remotely manage a device. To override the default policy, you can explicitly create a Remote Management policy for the device.

For information on configuring the Remote Management policy, see "Remote Management Policy" in the *ZENworks 10 Configuration Management Policy Management Reference*, and for more information on editing the Remote Management policy, see "Editing Policies" in the *ZENworks 10 Configuration Management Policy Management Reference*.

2.4 Configuring the Remote Operator Rights

You can assign rights to a Remote Operator to perform remote sessions on the managed device. The Remote Operator can have device-specific rights as well as user-specific rights.

1 In ZENworks Control Center, click *Configuration.*

2 In the Administrators panel, click the name of the administrator to whom you want to assign the Remote Management rights.

3 In the Assigned Rights panel, click *Add*, then click *Remote Management Rights* to display the Remote Management Rights dialog box.

4 Select the device or the user to assign the rights.

The following table contains information on the Remote Management rights:

Remote Management Rights	Details
Remote Control	Assign the remote operator the rights to remotely control devices
Remote View	Assign the remote operator the rights to remotely view devices
Remote Diagnostics	Assign the remote operator the rights to remotely diagnose devices.
Remote Execute	Assign the remote operator the rights to remotely execute applications on devices.
Transfer Files	Assign the remote operator the rights to transfer files to or from devices.
Unblock Remote Management Service	Assign the remote operator the rights to unblock the Remote Management Service that has been locked due to intruder detection.

5 Click *OK*.

2.5 Configuring the Remote Management Password

The following sections provide information on configuring the Remote Management password for the Remote Management service on the managed device:

2.5.1 Setting Up the Remote Management Password Using the ZENworks Control Center

The Administrator can set a Remote Management password in the Security Settings page while creating a Remote Management policy or after creating the policy.

If you want to set the password while creating the Remote Management policy, see "Remote Management Policy" in the *ZENworks 10 Configuration Management Policy Management Reference*. To edit the password set while creating the Remote Management policy:

1. In ZENworks Control Center, click *Policies*.
2. Click the Remote Management policy, then click the *Details* tab.
3. In the Security Settings panel, select the password and replace it with the new password.
4. Click *Apply*
5. Increment the version of this policy in the Summary page or in the Common Tasks to update the changes in the passwords on the managed device.

If you want to set the password after creating the Remote Management policy:

1. In ZENworks Control Center, click *Policies*.
2. Click the Remote Management policy, then click the *Details* tab.
3. In the Security Settings panel, select *Enable Password Based Authentication,* then select *Persistent*.
4. Click *Set Password* and specify the password. If you have already set the password while creating the Remote Management policy, then you can edit the password. To edit the password, select the password and replace it with the new password.
5. Click *Apply*
6. Increment the version of this policy in the Summary page or in the Common Tasks to update the changes in the passwords on the managed device.

2.5.2 Setting Up the Remote Management Password Using the ZENworks Adaptive Agent

The user at the managed device can set a password for the Remote Management service if the *Allow user to override default password on the managed device* option is enabled in the Remote Management policy effective on the managed device. This password has precedence over the password set in the Remote Management policy.

To set a password on the managed device:

1. Double-click the *ZENworks Adaptive Agent* icon to display the ZENworks Adaptive Agent window.
2. In the left pane, navigate to *Remote Management*, then click *Security*.
3. In the right pane, click *Set Password* to set the following passwords:
   - **ZENworks password (Recommended):** Used in ZENworks authentication. It can be up to 255 characters long.
   - **VNC password:** Used in VNC authentication for interoperability with open source VNC viewers. It can be up to 8 characters long.
4. Click *OK*.

2.5.3 Clearing the Remote Management Password Using the ZENworks Control Center

To clear the Remote Management password set using the policy:

1. In ZENworks Control Center, click *Policies*.
2. Click the Remote Management policy, then click the *Details* tab.
3. In the Security Settings panel, select *Clear Password* then click *Apply*.
4. Increment the version of this policy in the Summary page or in the Common Tasks to update the changes in the policy on the managed device.

To clear the Remote Management password set by the managed device user:

1. In ZENworks Control Center, click *Policies*.
2. Click the Remote Management policy, then click the *Details* tab.
3. In the Security Settings panel, deselect the *Allow User to Override Default Passwords on Managed Device* option, then click *Apply*.
4. Increment the version of this policy in the Summary page or in the Common Tasks to update the changes in the policy on the managed device.

2.5.4 Clearing the Remote Management Password Using the ZENworks Adaptive Agent

The user at the managed device can reset the Remote Management password set earlier by him or her.

1. Double-click the *ZENworks Adaptive Agent* icon to display the ZENworks Adaptive Agent window.

2 In the left pane, navigate to *Remote Management*, then click *Security*.

3 In the right pane, click *Clear Password* to clear the passwords.

4 Click *OK*.

The password configured in the policy shall be effective as there is no password set by the user.

2.6 Starting Remote Management Operations

The remote operation can be initiated in the following ways:

- Section 2.6.1, “Initiating a Session from the Console,” on page 21
- Section 2.6.2, “Initiating a Session from the Remote Device,” on page 28

2.6.1 Initiating a Session from the Console

In this scenario, the remote session is initiated by the administrator on the management console. The management console is typically placed within an enterprise network and the managed device can be either within or outside the enterprise network. The following illustration depicts a remote session initiated on the managed device from the management console.

Figure 2-1 *Console-Initiated Session*

The Remote Management Agent starts automatically when the managed device boots up. A default Remote Management policy is created on the managed device when the device is deployed. You can remotely manage the device without creating a new policy for the device. But, when you create a new Remote Management policy, the new policy overrides the default policy.

If you want to allow connections to be made from a public network into a private network, deploy the DNS Application Level Gateway (DNS_ALG). For more information on DNS_ALG, refer to RFC 2694 (http://www.ietf.org/rfc/rfc2694).

The remote operator can initiate a session in any of the following ways:

- “Starting a Remote Management Operation in ZENworks Control Center” on page 22
- “Starting a Remote Management Operation in Standalone Mode” on page 24
- “Starting a Remote Management Operation by Using Command Line Options” on page 25

Starting a Remote Management Operation in ZENworks Control Center

ZENworks Control Center is the comprehensive web-based interface for ZENworks Configuration Management. It provides an intuitive and task-driven console to manage various ZENworks components, including Remote Management.

You can initiate the various Remote Management operations from the device context or the user context:

- "Initiating a Remote Management Session from the Device Context" on page 22
- "Initiating a Remote Management Session from the User Context" on page 23

Initiating a Remote Management Session from the Device Context

To initiate a Remote Management session on a device

1. In ZENworks Control Center, click the *Devices* tab.
2. Click *Servers* or *Workstations* and select the device you want to remotely manage. Click *Action*, then select the Remote Management operation you want to perform.

   or

   In *Device Tasks* in the left pane, select the Remote Management operation you want to perform.

   The available remote operations are:

   - **Remote Control:** Displays the Remote Management dialog box, which lets you perform a Remote Control, Remote View, or Remote Execute operation on the managed device.
   - **Remote Diagnostics:** Displays the Remote Diagnostics dialog box, which lets you perform a Remote Diagnostics operation on the managed device.
   - **Transfer Files:** Displays the File Transfer dialog box, which lets you perform a file transfer operation on the managed device.
3. Fill in the options in the dialog box that displays. The following table contains information on the various options available:

Field	Details
Device	Specify the host name or the IP address of the device you want to remotely manage.
Operation	Select the type of the remote operation you want to perform on the managed device. This field is available only in the Remote Management dialog box.
Application	Select the application you want to launch on the device to remotely diagnose. This field is available only in the Remote Diagnostics dialog box.
Authentication	Select the mode you want to use to authenticate to the managed device. The authentication modes are: ◆ Rights-Based Authentication ◆ Password-Based Authentication
Port	Specify the port number on which the Remote Management service is listening. By default, the port number is 5950

Field	Details
Session Mode	Select one of the following modes for the session: ◆ **Collaborate:** Allows you to launch a Remote Control session and a Remote View session in collaboration mode. If you launch the Remote Control session on the managed device first, then you get the privileges of a master remote operator, which include: ◆ Inviting other remote operators to join the remote session. ◆ Delegating Remote Control rights to a remote operator. ◆ Regaining control from the remote operator. ◆ Terminating a Remote Session. The consecutive sessions launched are Remote View sessions. ◆ **Shared:** Allows more than one remote operator to simultaneously control the managed device. ◆ **Exclusive:** Allows you to have an exclusive remote session on the managed device. No other remote session can be initiated on the managed device after a session has been launched in exclusive mode. This field is available only in the Remote Management dialog box.
Session Encryption	Ensures that the remote session is secured by using SSL encryption (TLSv1 protocol).
Enable Logging	Logs session and debug information in the `novell-zenworks-vncviewer.txt` file. The file is saved by default on the desktop if you launch ZENworks Control Center (ZCC) through Internet Explorer and in the mozilla installed directory if you launch ZCC through Mozilla* FireFox*.

4 Click *OK* to launch the selected remote operation.

Initiating a Remote Management Session from the User Context

If you want to assist a user by performing a remote session on the managed device where he or she has logged in:

1 In ZENworks Control Center, click the *Users* tab.

2 Click the *User Source*.

3 Select the user to remotely manage the device where he or she is logged in.

4 Click *Action*, then select the Remote Management operation you want to perform.

The available operations are:

- **Remote Control:** Displays the Remote Management dialog box, which lets you perform a Remote Control, Remote View, or Remote Execute operation on the managed device.
- **Remote Diagnostics:** Displays the Remote Diagnostics dialog box, which lets you perform a Remote Diagnostics operation on the managed device.
- **Transfer Files:** Displays the File Transfer dialog box, which lets you perform a file transfer operation on the managed device.

5 Fill in the options in the dialog box that displays. The following table contains information on the various options available:

Field	Details
Device	Displays the host name or the IP address of the device the user has logged in. If the user has not logged in to any device, then you can specify the name or the IP address of the device you want to remotely manage.
Operation	Select the type of the remote operation you want to perform on the managed device. This field is available only in the Remote Management dialog box.
Application	Select the application you want to launch on the device to remotely diagnose. This field is available only in the Remote Diagnostics dialog box.
Authentication	Select the mode you want to use to authenticate to the managed device. The authentication modes are: ◆ Rights-Based Authentication ◆ Password-Based Authentication
Port	Specify the port number on which the Remote Management service is listening. By default, the port number is 5950
Session Mode	Select one of the following modes for the session: ◆ **Collaborate:** Allows you to launch a Remote Control session and a Remote View session in collaboration mode. If you launch the Remote Control session on the managed device first, then you get the privileges of a master remote operator, which include: ◆ Inviting other remote operators to join the remote session. ◆ Delegating Remote Control rights to a remote operator. ◆ Regaining control from the remote operator. ◆ Terminating a Remote Session. ◆ **Shared:** Allows more than one remote operator to simultaneously control the managed device. ◆ **Exclusive:** Allows you to have an exclusive remote session on the managed device. No other remote session can be initiated on the managed device after a session has been launched in exclusive mode. This field is available only in the Remote Management dialog box.
Session Encryption	Ensures that the remote session is secured by using SSL encryption (TLSv1 protocol).
Enable Logging	Logs session and debug information in the `novell-zenworks-vncviewer.txt` file. The file is saved by default on the desktop if you launch ZENworks Control Center (ZCC) through Internet Explorer and in the mozilla installed directory if you launch ZCC through Mozilla* FireFox*.

6 Click *OK* to launch the selected remote operation.

Starting a Remote Management Operation in Standalone Mode

Before you launch a Remote Management operation in standalone mode, ensure that the *Allow connection when Remote Management Console does not have SSL certificate* option in the security settings of the Remote Management policy is enabled.

To start the Remote Management Operation in standalone mode:

1. Install the latest version of the ZENworks Remote Management viewer by downloading the `novell-zenworks-rm-viewer.msi` file from `https://` *`ZENworks_server_IPaddress`*`/zenworks-remote-management/.`

   The file is automatically installed in the `C:\Document And Settings\` *`username`*`\ApplicationData\Novell\Zenworks\Remote Management\bin` directory.
2. Double-click the `nzrViewer.exe` file to launch the ZENworks Remote Management Client.
3. In the New ZENworks Remote Management Connection window that displays, specify the DNS name or the IP address of the managed device and the port number in the format *IP address~~Port*. For example 10.0.0.0~~1000.
4. Click *Connect.*

   On successful authentication, the remote session starts. By default, a Remote Control session is launched.

Starting a Remote Management Operation by Using Command Line Options

Before you launch a Remote Management operation from the command line, ensure that the *Allow connection when Remote Management Console does not have SSL certificate* option in the security settings of the Remote Management policy is enabled.

To start the Remote Management operation by using the command line options:

1. Install the latest version of the ZENworks Remote Management viewer by downloading the `novell-zenworks-rm-viewer.msi` file from `https://` *`ZENworks_server_IPaddress`*`/zenworks-remote-management/.`

   The file is automatically installed in the `C:\ Document And Settings\` *`username`*`\ApplicationData\Novell\Zenworks\Remote Management\bin` directory.
2. At the command prompt, change to the directory where the `novell-zenworks-rm-viewer.msi` file is installed.
3. Execute the following command:

   `nzrViewer [`*`/options <parameters if any>`*`][`*`IP address of the managed device`*`] [~~`*`port`*`].`

   The default port is 5950.

   The following table lists the command line options and the parameters available:

Command Line Option	Parameter	Description
listen	*port*	Enables the listener to listen to the remote session requests on the port specified. By default, the port is 5550.
restricted		Hides the toolbar and system menu.
viewonly		Launches a Remote View operation on the managed device.
remotecontrol		Launches a Remote Control operation on the managed device.

Command Line Option	Parameter	Description
ftponly		Launches a File Transfer operation on the managed device.
remoteexecute		Launches a Remote Execute operation on the managed device.
diagnostics	*appname*	Launches a Remote Diagnostics operation on the managed device. If the appname parameter is specified, then that application is launched on the managed device.
filecompressionlevel	*level*	Provides means of optimizing the file compression process for better speed or better compression during a file transfer operation. The compression level can vary from 0 to 9: ◆ 0 indicates no compression ◆ 1 indicates best speed ◆ 9 indicates best compression If the compression level is not specified, the default compression level, which is optimized for both speed and compression, is used.
noencrypt		Launches the remote session in an unencrypted mode.
fullscreen		Launches a remote operation in the full screen mode on the managed device.
notoolbar		Hides the toolbar of the viewing window.
exclusive		Launches the remote session in an exclusive mode.
8bit		Specifies the color depth to be used to render the session data.
shared		Enables a shared connection, allowing you to share the desktop with other clients already using it. This option is True by default.
collaborate		Launches the remote session in a collaborative mode.
noshared		Enables an unshared connection, which disconnects other connected clients or refuses your connection, depending on the server configuration.
swapmouse		Swaps the mouse buttons.
nocursor		Displays only the managed device mouse pointer. The local mouse pointer is not displayed.
dotcursor		Displays the local mouse pointer as a dot. This option is true by default.
smalldotcursor		Displays the local mouse pointer as a small dot.
normalcursor		Displays the local mouse pointer in the default shape.
belldeiconify		Allows the transmission of a bell character, causing a beep at the viewer. This option also causes a minimized vncviewer to be maximized when the bell character is received.

Command Line Option	Parameter	Description
emulate3		Users with a two-button mouse can emulate a middle button by pressing both buttons at once. This option is True by default
noemulate3		Does not emulate a three-button mouse.
nojpeg		Disables lossy JPEG compression. This is not recommended because the efficiency of the encoder might reduce. You might want to use this option if it is absolutely necessary to achieve a perfect image quality.
nocursorshape		Disables the cursor shape updates to handle remote cursor movements. Using the cursor shape updates decreases the delays with remote cursor movements, and can improve bandwidth usage dramatically.
noremotecursor		Does not show the remote cursor.
fitwindow		Hides the scroll bar of the viewing window.
scale	*percentage*	Zooms the viewing window to the percentage of scaling specified.
emulate3timeout	*ms*	Specifies the time-out for emulating a three-button mouse.
disableclipboard		Disables the copying of data into the clipboard.
delay		Renders a display area and waits for the specified time before retrieving the next update.
loglevel	*n*	Specifies the levels of information logging.
console		Logs information in a console window.
logfile	*filename*	Name of the log file where information is to be logged.
config	*filename*	Name of the configuration file to be used for loading predefined configuration settings.
key	*filename*	Name of the file where private key is stored. This key is used during an SSL handshake with the managed device. **IMPORTANT:** The key and the cert options must be used together. If you use these options along with the `nzrViewer` command, then for security reasons you must disable the *Allow connection when Remote Management Console does not have SSL certificate* option in the security settings of the Remote Management policy.
cert	*filename*	Name of the file where the certificate corresponding to the private key is stored. **IMPORTANT:** The key and the cert options must be used together. If you use these options along with the `nzrViewer` command, then for security reasons you must disable the *Allow connection when Remote Management Console does not have SSL certificate* option in the security settings of the Remote Management policy.

Command Line Option	Parameter	Description
CAcert	*filename*	Name of the file where the root certificate is stored. This certificate is used to verify the managed device certificate during an SSL handshake.
encoding	*encname*	Specifies the desired encoding to be used for the session. The different types of encoding are Raw, CopyRect, RRE, CoRRE, Hextile, Zlib, and Tight.
compresslevel	*n*	Specifies the compression level from 0 to 9. Level 1 uses a minimum of CPU time and achieves weak compression ratios, and level 9 offers best compression but is slow in terms of CPU time consumption on the server side. Use high levels with very slow network connections, and low levels when working over high-speed LANs. We recommend that you do not use compression level 0.
quality	*n*	Specifies the JPEG quality level from 0 to 9. Quality level 0 denotes poor image quality but very impressive compression ratios, and level 9 offers very good image quality at lower compression ratios.
zenrights		Specifies that the authentication scheme to be used is ZENworks Rights Authentication.
zenpasswd		Specifies that the authentication scheme to be used is ZENworks Password Authentication.
locale		Specifies the locale in which the resources are to be displayed. By default, English is used. The values for this option are: English, French, German, Spanish, Portuguese, Japanese, Italian, Chinese(Simplified), and Chinese(Traditional).

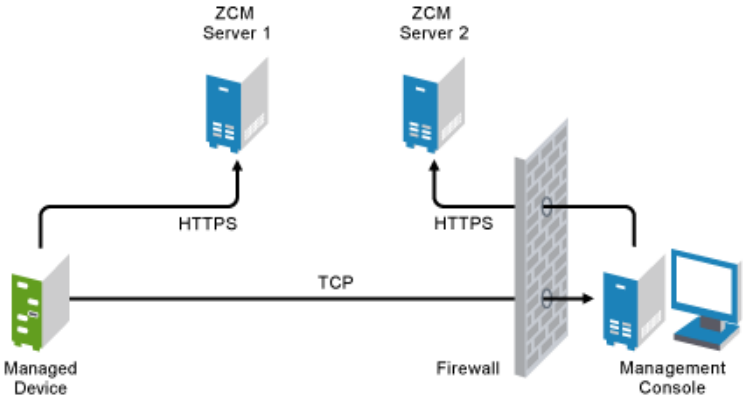
4 Click *Connect.*

On successful authentication, the remote session starts. If you have not specified the type of remote operation in the command line, a Remote Control session is launched by default.

2.6.2 Initiating a Session from the Remote Device

In this scenario, the remote session is initiated by the user on the managed device. This is useful if the management console cannot connect to the managed device. The following illustration depicts a remote session initiated by the user at the managed device.

Figure 2-2 *Agent-Initiated Session*



The user at the managed device can request a remote operator to perform a remote session on the device if:

- The remote operator has launched the Remote Management listener to listen to the remote session requests from the user.
- The port at which the Remote Management listener listens for the remote connections must be opened in the management console firewall. The default port is 5550.

To request a session:

1. Double-click the ZENworks icon in the notification area.
2. In the left pane, navigate to *Remote Management*, then click *General*.
3. Click *Request Remote Management Session* to display the Request Session dialog box.

   The ability to request a Remote Management session is controlled by your administrator, which means the option might be disabled, particularly if your company or department does not have dedicated help desk personnel to serve as on-call remote operators. If the *Request Remote Management Session* option is not displayed as linked text, the option is disabled.
4. In the *Listening Remote Operators* list, select the remote operator you want to open the remote session with.

   or

   If the remote operator is not listed, provide the operator's connection information in the *Request Connection* fields.
5. In the *Operation* field, select the type of operation (Remote Control, Remote View, Remote Diagnostics, File Transfer, or Remote Execute) you want to open.

   For information about each operation, see Section 1.2, "Understanding Remote Management Operations," on page 10.
6. Click *Request* to launch the session.

If you want to allow connections to be made from a public network into a private network, deploy the DNS Application Level Gateway (DNS_ALG). For more information on DNS_ALG, refer to RFC 2694 (http://www.ietf.org/rfc/rfc2694).

Managing Remote Sessions

3

The following sections provide information to help you effectively manage the remote sessions of Novell® ZENworks® 10 Configuration Management:

3.1 Managing a Remote Control Session

Remote Management lets you remotely control a managed device. With remote control connections, the remote operator can go beyond viewing the managed device to taking control of it, which helps to provide user assistance and resolve problems on the managed device. For information on launching a Remote Control session, see Section 2.6, “Starting Remote Management Operations,” on page 21.

3.1.1 Using the Toolbar Options in the Remote Management Viewer

The following table describes the various toolbar options available in the Remote Management viewer during a Remote Control session. It also lists the shortcut keys if they are available.

Table 3-1 *Toolbar Options in the Remote Management Viewer*

Option	Shortcut Key	Functionality
Connection Options 	Ctrl+Alt+Shift+P	Allows you to configure various session parameters such as format and encoding for enhancing the session performance, logging, and local and remote cursor handling.
Connection Info 	Ctrl+Alt+Shift+I	Provides the hostname, port, screen resolution, and protocol version of the managed device.
Full Screen 	Ctrl+Alt+Shift+F	Allows you to toggle between full screen and normal mode.

Option	Shortcut Key	Functionality
Request Screen Refresh 	Ctrl+Alt+Shift+H	Refreshes the viewing window.
Send Ctrl-Alt-Del 		Sends the Ctrl+Alt+Del keystroke to the managed device.
Send Ctrl-Esc 		Invokes the Start menu on the managed device.
Send Alt Key Press / Release 		Clicking this option and pressing the ALT key on the keyboard sends the Alt keystroke to the managed device.
Blank / Unblank Screen	Ctrl+Alt+Shift+B	Blanks or displays the screen on the managed device. When the screen of the device is blanked, the operations performed by the remote operator on the device are not visible to the user at the device. The keyboard and the mouse controls on the managed device also gets locked. This option is enabled only if the *Allow managed device screen to be blanked* option is enabled in the Remote Management policy effective on the managed device.
Lock / Unlock Keyboard and Mouse 	Ctrl+Alt+Shift+L	Locks or unlocks the keyboard and mouse controls for the managed device. When the mouse and keyboard controls of the device are locked, the user at the managed device cannot use these controls. This option is enabled only if the *Allow managed device mouse and keyboard to be locked* option is enabled in the Remote Management policy effective on the managed device.
Transfer Files 	Ctrl+Alt+Shift+T	Launches a session to transfer files to and from the managed device. This option is enabled only if the *Allow transferring files on the managed device* option is enabled in the Remote Management policy effective on the managed device. For more information on File Transfer, see Section 3.5, “Managing a File Transfer Session,” on page 37.
Collaboration 		Launches a ZENworks Remote Management Collaboration Session on the managed device, which lets you invite multiple remote operators to join the remote management session. You can also delegate the Remote Control rights to another remote operator to help you solve a problem. For more information on Session Collaboration, see Section 3.1.2, “Session Collaboration,” on page 33.

Option	Shortcut Key	Functionality
Remote Execute 	Ctrl+Alt+Shift+U	Launches a Remote Execute session on the managed device, which enables you to remotely launch any executable on the managed device. This option is enabled only if the *Allow programs to be remotely executed on the managed device* option is enabled in the Remote Management policy effective on the managed device.
Override Screensaver 	Ctrl+Alt+Shift+O	Overrides any password-protected screen saver on the managed device during the remote session. This option is enabled only if the *Allow screen saver to be automatically unlocked during Remote Control* option is enabled in the Remote Management policy effective on the managed device.
Disconnect 	Alt+F4	Closes the remote session.

3.1.2 Session Collaboration

The Session Collaboration feature lets you invite multiple remote operators to join the Remote Management session if the remote operators have launched the Remote Management listener to listen to the remote session requests. You can also delegate the Remote Control rights to a remote operator to help you solve a problem and then regain control back from the remote operator.

If you launch the Remote Control session on the managed device first, then you gain the privileges of the master remote operator. You can use Session Collaboration to:

- Invite multiple remote operators to join the Remote Control session.
- Delegate the remote control rights to a remote operator to help you solve a problem and then regain control back from him or her.
- Terminate a remote session.

To launch Session Collaboration:

1. Launch the Remote Control session on the managed device in the collaborate mode.

   For information on launching a Remote Control session, see Section 2.6, “Starting Remote Management Operations,” on page 21.
2. On the Remote Management viewer toolbar, click  to display the Session Collaboration window.

The Session Collaboration window lists the remote operators added in the Remote Management policy effective on the device. Each remote operator is listed as a separate entry preceded by a colored circle:

- A gray circle indicates that the remote operator has not joined the session.
- A red circle indicates that the remote operator has joined the session and is in the Remote View mode.

- A green circle indicates that the remote operator has joined the session and has been delegated Remote Control rights in the session.

For more information on Adding the Remote Operators, see "Remote Management Policy"

The following table lists the actions that you as a master remote operator can perform during session collaboration:

Table 3-2 *Session Collaboration Window Options*

Task	Steps	Additional Details
Invite a remote operator to join a remote session	1. Select a remote operator listed in the session collaboration window. 2. Click *Invite.*	If the remote operator accepts the request and joins the session, the gray circle for the remote operator changes to red. By default, the new session starts in the Remote View mode.
Delegate Remote Control rights to the remote operator	1. Select the remote operator you want to delegate the Remote Control rights. 2. Click *Delegate.*	The selected remote operator is now in Remote Control mode and the red circle for the remote operator changes to green. The master remote operator automatically switches to the Remote View mode.
Regain Remote Control rights from the remote operator	1. Click *Regain Control.*	The remote operator switches into Remote View mode and the green circle for the remote operator changes to red. The master remote operator automatically switches to the Remote Control mode.
Terminate the Remote Session	1. Select the remote operator you want to terminate from the Remote Session. 2. Click *Terminate.*	If the selected remote operator is in Remote Control mode, then you will regain the Remote Control rights. The remote operator's session terminates and the color of the circle for the remote operator changes to gray.

Task	Steps	Additional Details
Invite an external remote operator	1. Click *Invite External* to invite remote operators not listed in the Session Collaboration window to join the remote session. 2. Specify the DNS name or the IP address of the remote operator's device and the port number. For example, 10.0.0.0 ~~1000. 3. Click *Invite*.	

If the master remote operator disconnects the remote session, then all the remote operators are terminated from the session.

3.2 Managing a Remote View Session

Remote View lets you remotely connect with a managed device so that you can view the managed device desktop. For information on launching a Remote View session, see Section 2.6, "Starting Remote Management Operations," on page 21.

The following table describes the various toolbar options available in the Remote Management viewer during a Remote View session.

Table 3-3 *Toolbar Options in the Remote Management Viewer*

Option	Shortcut Key	Functionality
Connection Options 	Ctrl+Alt+Shift+P	Allows you to configure various session parameters such as format and encoding for enhancing the session performance, logging, and local and remote cursor handling.
Connection Info 	Ctrl+Alt+Shift+I	Provides the hostname, port, screen resolution, and protocol version of the managed device.
Full Screen 	Ctrl+Alt+Shift+F	Allows you to toggle between full screen and normal mode.
Request Screen Refresh 	Ctrl+Alt+Shift+H	Refreshes the viewing window.
Disconnect 	Alt+F4	Closes the remote session.

3.3 Managing a Remote Execute Session

Remote Execute lets you remotely run executables with system privileges on the managed device. To execute an application on the managed device, launch the Remote Execute session.

If you launch Remote Execute session in a standalone mode, ensure that you have the privileges to execute the application.

1. Launch the Remote Execute session.

   For information on launching a Remote Execute session, see Section 2.6, "Starting Remote Management Operations," on page 21.

2. Specify the executable name.

   If the application is not in the system path of the managed device, then specify the complete path of the application. If you do not specify the extension of the file you want to execute at the managed device, Remote Execute appends the `.exe` extension.

3. Click *Execute*.

The remote execution of the specified application might fail if the application is not available on the managed device in the defined path.

WARNING: By default, the Remote Management module runs as a service with system privileges on the managed device. Hence, all the applications launched during the Remote Execute session also run with system privileges. For security reasons, we strongly recommend that you close the application after use.

3.4 Managing a Remote Diagnostics Session

Remote Management lets you to remotely diagnose and analyze the problems on the managed device. This helps you to shorten problem resolution times and assist users without requiring a technician to physically visit the problem device. This increases user productivity by keeping desktops up and running.

When you launch a Remote Diagnostics session on the managed device, you can access only the diagnostics applications configured for the device in the Remote Management settings for diagnosing and fixing the problems on the device. During the session, the diagnostics applications are displayed as icons in a toolbar. By default, the following diagnostics applications are configured in the Remote Management Settings:

Table 3-4 *Toolbar Options in the Remote Management Viewer*

Option	Shortcut Key	Functionality
Connection Options 	Ctrl+Alt+Shift+P	Allows you to configure various session parameters such as format and encoding for enhancing the session performance, logging, and local and remote cursor handling.
Connection Info 	Ctrl+Alt+Shift+I	Provides the hostname, port, screen resolution, and protocol version of the managed device.

Option	Shortcut Key	Functionality
Full Screen 	Ctrl+Alt+Shift+F	Allows you to toggle between full screen and normal mode.
Request Screen Refresh 	Ctrl+Alt+Shift+H	Refreshes the viewing window.
Transfer Files 	Ctrl+Alt+Shift+T	Launches a session to transfer files to and from the managed device. This option is enabled only if the *Allow transferring files on the managed device* option is enabled in the Remote Management policy effective on the managed device. For more information on File Transfer, see Section 3.5, "Managing a File Transfer Session," on page 37
Disconnect 	Alt+F4	Closes the remote session.

Table 3-5 *Remote Diagnostics Applications*

Icon	Application
	*System information*
	*Computer Management*
	*Services*
	*Registry Editor*

You can configure the applications to be launched on the managed device during the Remote Diagnostics session. For more information on configuring the diagnostics applications, see Section 2.1, "Configuring the Remote Management Settings," on page 15.

3.5 Managing a File Transfer Session

Remote Management enables you to transfer files between the management console and the managed device. For information on launching a File Transfer session, see Section 2.6, "Starting Remote Management Operations," on page 21.

In the File Transfer window, the Local Computer pane displays all the files and the folders on the management console, and the Remote Computer pane displays all the files and the folders in the directory specified in the *File Transfer Root Directory* option in the Remote Management policy. If the *File Transfer Root Directory* is not specified in the policy or if the managed device does not have

any policy associated with it, you can perform file transfer operations on the complete file system of the remote device.

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

Table 3-6 *File Transfer Window Options*

Tasks	Shortcut Keys	Steps	Additional Details
Create New Local Folder	Alt+L	1. Click *Actions* > *New Local Folder*. or Click  in the Local Compute pane. 2. Follow the on-screen prompts.	
Create New Remote Folder	Alt+W	1. Click *Actions* > *New Remote Folder*. or Click  in the Remote Computer pane. 2. Follow the on-screen prompts.	
Open a File		1. Double-click the file to open it in its associated application.	
Rename Files or Folders	Alt+N	1. Select the file or folder to rename. 2. Click *Actions* > *Rename.* or Click  . 3. Follow the on-screen prompts.	
Delete Files or Folders	Alt+D	1. Select the files or folders to delete. 2. Click *Actions* > *Delete.* or Click  3. Follow the on-screen prompts.	You can use the Shift or Ctrl keys to select multiple files.

Tasks	Shortcut Keys	Steps	Additional Details
Refresh Local Folder	Alt+E	1. Click *Actions* > *Refresh Local Folder*. or Click in the Local Computer pane.	
Refresh Remote Folder	Alt+M	1. Click *Actions* > *Refresh Remote Folder*. or Click in the Remote Computer pane.	
Sort Local Files		1. Click *Actions* > *Local Sort*. 2. Select the sort type. You can sort the files by name, size, or date.	You can also sort the files by clicking the respective column headers.
Sort Remote Files		1. Click *Actions* > *Remote Sort*. 2. Select the sort type. You can sort the files by name, size, or date	You can also sort the files by clicking the respective column headers.
Upload Files / Folders		1. Select the files to upload to the remote computer. 2. Select the destination folder in the remote computer pane. 3. Click *Actions* > *Upload*. or Click	The *Action* > *Upload option* is available only when the focus is on the local computer. You can use Shift or Ctrl keys to select multiple files.
Download Files / Folders	Alt+O	1. Select the files to download to the local computer. 2. Select the destination folder in the local computer pane 3. Click *Actions* > *Download*. or Click	The *Action* > *Download option is* available only when the focus is on the remote computer. You can use Shift or Ctrl keys to select multiple files. .
Cancel File Transfer	Alt+C	1. Click *Actions* > *Cancel File Transfer*	You can also cancel the file transfer operation by clicking the cancel button.

Tasks	Shortcut Keys	Steps	Additional Details
Display File Properties	Alt+P	1. Select the files. 2. Click *Actions* > *Properties.* or Click 	You can use Shift or Ctrl keys to select multiple files. Displays the cumulative size of the selected files and folders.
Move to Parent Folder		1. Click  to move to the parent folder.	

3.6 Waking Up a Remote Device

Remote Wake Up lets you remotely wake up a single node or a group of powered-down nodes in your network if the network card on the node is enabled for Wake-on-LAN.

- Section 3.6.1, “Prerequisites,” on page 40
- Section 3.6.2, “Remotely Waking Up the Managed devices,” on page 40

3.6.1 Prerequisites

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

- Ensure that the network card on the managed device supports Wake-on-LAN. Additionally, ensure that you have enabled the Wake-on-LAN option in the BIOS setup of the managed device.
- Ensure that the managed device is registered with the ZENworks Management Zone.
- Ensure that the remote node is in a soft- power off state. In the soft-power 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.
- Ensure that the routers connecting the management server and the remote device are configured to forward subnet-oriented broadcasts.

3.6.2 Remotely Waking Up the Managed devices

To perform a Remote Wake Up:

1. In ZENworks Control Center, click *Devices*.
2. Click *Servers* or *Workstations* to display the list of managed devices.
3. Select the device to wake up.
4. Click *Quick Tasks* > *Wake Up* to display the Wake Up dialog box.
5. Select the name or the IP address of the Primary Server to be used to send a wake-up request to a managed device that is powered off.

   If you do not select the Primary Server, then ZENworks automatically contacts the Primary Server closest to the managed device.
6. (Optional) Specify the IP address to be used by the Primary Server for sending the wake-up broadcast.

7 Click *OK*.

3.7 Improving the Remote Management Performance

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

- Section 3.7.1, “On the Management Console,” on page 41
- Section 3.7.2, “On the Managed Device,” on page 41

3.7.1 On the Management Console

In the ZENworks Remote Management Connection window at the console, click *Options* and set the following values:

- To maximize the Remote Management performance over slow link:
  - Select the *Use 8-bit color* option.
  - Set the *Custom compression level* to level 6.
- Select the *Block Mouse Move Events* option.
- Enable the *Suppress Wallpaper* option in the Remote Management Settings.

3.7.2 On the Managed Device

- The speed of the Remote Management session depends upon the processing power of the managed device. We recommend that you use Pentium* III, 700 MHz (or later) with 256 MB RAM or higher.
- Do not set a wallpaper pattern.

Security

4

The following sections provide security related information that you should be aware of while using the Remote Management component of Novell® ZENworks® 10 Configuration Management:

4.1 Authentication

The Remote Management service must be installed on a device for the remote operator to remotely manage the device. The service automatically starts when the managed device boots up. When a remote operator initiates a remote session on the managed device, the service starts the remote session only if the remote operator is authorized to perform remote operations on the managed device.

To prevent unauthorized access to the managed device, the Remote Management service on the managed device uses the following modes of authentication:

4.1.1 Rights-Based Remote Management Authentication

In rights-based authentication, rights are assigned to the remote operator to launch a remote session on the managed device. By default, the ZENworks administrator and the super administrator have rights to perform remote operations on all the managed devices regardless of whether the local user or the ZENworks user is logged in to the device.

The remote operator does not need any exclusive rights to perform a remote session on the managed device if no user has logged in to the managed device or if a user has logged in to the managed device but not in to ZENworks. However, the remote operator needs exclusive Remote Management rights to perform the remote operation on the managed device when a ZENworks user has logged in to the device. We strongly recommend that you use the rights-based authentication because it is safe and secure.

4.1.2 Password-Based Remote Management Authentication

In password-based authentication, the remote operator is prompted to enter a password to launch the remote session on the managed device.

The two types of password authentication schemes used are:

- **ZENworks Password:** This scheme is based on the Secure Remote Password (SRP) protocol (version 6a). The maximum length of a ZENworks password is 255 characters.
- **VNC Password:** This is the traditional VNC password authentication scheme. The maximum length of a VNC password is 8 characters. This password scheme is inherently weak and is provided only for interoperability with the open source components.

If you use password-based authentication, we strongly recommend that you use ZENworks Password scheme because it is safer and more secure than the VNC Password scheme.

The password schemes operate in the following modes:

- **Session Mode:** The password set in this mode is valid only for the current session. The user on the managed device must set a password at the start of the remote session and communicate the password to the remote operator through out-of-band means. When initializing a remote session with the managed device, the remote operator must enter the correct password in the session password dialog box that displays. If the remote operator fails to enter the correct password within two minutes after the dialog box is displayed, then the session closes for security reasons. If you use password-based authentication, we strongly recommend that you use this mode of authentication because the password is valid only for the current session and is not saved on the managed device.
- **Persistent Mode:** In this mode, the password can be set by the administrator through the Remote Management policy or by the managed device user through the ZENworks icon if the *Allow user to override default passwords on managed device* option is selected in the security settings of the Remote Management policy.

  If the password is set both by the managed device user and in the policy, the password set by the user takes precedence over the password configured in the policy.

  The administrator can prevent the managed device user from setting the password and can even reset the password set by the user to ensure that the password configured in the policy is always enforced during authentication. For more information on resetting the password set by the managed device user, see Section 2.5.3, “Clearing the Remote Management Password Using the ZENworks Control Center,” on page 20.

4.2 Password Strength

Use secure passwords. Keep the following guidelines in mind:

- **Length:** The minimum recommended length is 6 characters. A secure password is at least 8 characters; longer passwords are better. The maximum length is 255 characters for a ZENworks password and 8 characters for a VNC password.
- **Complexity:** A secure password contains a mix of letters and numbers. It should contain both uppercase and lowercase letters and at least one numeric character. Adding numbers to passwords, especially when they are added to the middle and not just at the beginning or the end, can enhance password strength. Special characters such as &, *, $, and > can greatly improve the strength of a password. Do not use recognizable words such as proper names or

words from a dictionary, and do not use personal information such as phone numbers, birth dates, anniversary dates, addresses, or ZIP codes.

4.3 Ports

By default, the Remote Management service runs on port 5950 and the Remote Management Listener runs on port 5550. The firewall is configured to allow any port used by the Remote Management service, but you need to configure the firewall to allow the port used by Remote Management Listener.

4.4 Audit

ZENworks Configuration Management maintains a log of all the remote sessions performed on the managed device. This log is maintained on the managed device and can be viewed by the user and the administrator. The administrator can view the logs of all the remote sessions performed on the device. The user can view the logs of all the remote sessions performed on the device when he or she has logged in.

To view the audit log:

1. Double-click the ZENworks icon in the notification area of the managed device.
2. In the left pane, navigate to *Remote Management*, then click *Security*.
3. Click *Display Audit Information* to display the audit information of the remote operations performed on the device.

Field	Description
ZENworks User	Name of the ZENworks user logged in to the managed device at the start of the remote session.
Remote Operator	Name of the remote operator who performed the operation.
Console Machine	Host name of the device from which the remote operation was performed.
Console IP	IP address of the device from which the remote operation was performed.
Operation	The type of operation performed: Remote Control, Remote Execute, Remote View, Remote Diagnostics, File Transfer.
Start Time	The time when the remote operation started.
End Time	The time when the remote operation completed.
Status	The status of the remote operation: Success, Running, or Failure. The cause of the failure is also displayed.

4.5 Ask Permission from the User on the Managed Device

The administrator can configure the Remote Management policy to enable the remote operators to request permission from the user on the managed device before starting a remote operation on the device.

When the remote operator initiates a remote session on the managed device, the Remote Management service checks if the *Ask permission from user on managed device* option for that remote operation is enabled in the policy effective on the device. If the option is enabled and no user has logged in the device, the remote session proceeds. But, if the option is enabled and a user has logged in the managed device, then a message configured in the Remote Management policy is displayed to the user requesting permission to launch a remote session on the device. The session starts only if the user grants permission.

4.6 Abnormal Termination

When a remote session is abruptly disconnected, the abnormal termination feature lets you lock the managed device or log out the user on the managed device, depending on the configuration in the security settings of the Remote Management policy. The remote session terminates abnormally under the following circumstances:

- The networks fails and the Remote Management viewer and the Remote Management service are unable to communicate
- The Remote Management viewer is closed abruptly through the task manager.
- The network is disabled either on the managed device or on the management console.

Under some circumstances, the Remote Management service might take up to one minute to determine the abnormal termination of the session.

4.7 Intruder Detection

The Intruder Detection feature significantly lowers the risk of the managed device being hacked. If the remote operator fails to log in to the managed device within the specified number of attempts (the default is 5), the Remote Management service is blocked and does not accept any remote session request until it is unblocked. The administrator can unblock the Remote Management service either manually or automatically.

4.7.1 Automatically Unblocking the Remote Management Service

The Remote Management service is automatically unblocked after the duration of the time specified in the *Automatically start accepting connections after [] minutes* option in the Remote Management policy. The default time is10 minutes. You can change the default time in the security settings of the Remote Management policy.

4.7.2 Manually Unblocking the Remote Management Service

You can manually unblock the Remote Management service from the managed device or from ZENworks Control Center.

To unblock the Remote Management service from ZENworks Control Center, the remote operator must have Unblock Remote Management Service rights over the managed device.

1. In ZENworks Control Center, click *Devices*.
2. Click *Servers* or *Workstations* to display the list of managed devices.
3. Select the device to unlock.

4 Click *Action*, then click *Unblock Remote Management*.

5 Click *OK*.

To unblock the Remote Management service from the managed device:

1 Double-click the ZENworks icon in the notification area of the managed device.

2 In the left pane, navigate to the *Remote Management*, then click *Security*.

3 Click *Enable Accepting Connections if Currently blocked due to Intruder Detection.*

4.8 Remote Operator Identification

When a remote operator launches a remote session from ZENworks Control Center, a certificate that helps the managed device to identify the remote operator is automatically generated. However, if the remote operator launches the session in a standalone mode, the certificate is not generated and the remote operator is recorded as *An Unknown User* in the audit logs, the Visible Signal and the Ask User Permission dialog box. The Remote Management service retrieves the identity of the remote operator by using the certificate provided by the management console during the Secure Socket Layer (SSL) handshake. The SSL handshake happens for all the types of authentication except for the VNC password authentication.

The Remote Management service on the device displays the details of the remote operator in the visible signal dialog box, if the *Give Visible Signal to the User on the Managed Device* option is enabled in the policy effective on the device. It also logs the information of the remote operator in the Remote Management Audit logs.

4.9 Browser Configuration

If you use Internet Explorer to launch ZENworks Control Center on Windows Vista devices, then turn off the protected mode in the security settings of the browser (*Tools* > *Internet Options* > *Security*) and restart the browser.

4.10 Session Security

ZENworks Configuration Management uses Secure Socket Layer (SSL) to secure remote sessions. However, the remote sessions launched using the VNC password-based authentication are not secured. The authentication process happens over a secure channel as the SSL handshake takes place regardless of whether session encryption is configured in the Remote Management policy or not.

After the authentication is complete, the remote session switches to an insecure mode if the *Enable Session Encryption* option is disabled in the Remote Management policy and if the *Session Encryption* option is disabled by the remote operator while initiating a remote session on the managed device. However, we recommend that you continue the session in a secure mode because there is no major impact on the performance of the session.

4.10.1 SSL Handshake

While installing ZENworks Adaptive Agent on the managed device, the Remote Management service generates a self-signed certificate that is valid for 10 years.

When a remote operator initiates a remote session on the managed device, the Remote Management viewer prompts the remote operator to verify the managed device certificate. The certificate displays

details such as name of the managed device, certificate issuing authority, the validity of the certificate, and the fingerprint. For security reasons, the remote operator must verify the credentials of the managed device by matching the fingerprint of the certificate against the fingerprint communicated by the managed device user through out-of-band means. Then, the remote operator can do one of the following:

- **Accept the certificate permanently:** If a user who has logged in to the management console accepts the certificate permanently, then the certificate is not displayed in the subsequent remote sessions initiated by the users logged in that console.
- **Accept the certificate temporarily:** If a user who has logged in to the management console accepts the certificate temporarily, the certificate is accepted only for the current session. The user is prompted to verify the certificate the next time a connection is initiated to the managed device.
- **Reject the certificate:** If a user who has logged in to the management console rejects the certificate, the remote session terminates.

4.10.2 Certificate Regeneration

The managed device regenerates a new self-signed certificate if:

- The name of the managed device has changed
- The certificate is postdated and is not currently valid
- The certificate has expired
- The certificate is about to expire
- The certificate is missing

By default, the certificate is regenerated once in every 10 years.

Troubleshooting

5

The following sections explains the scenarios that you might encounter while using the Remote Management component of Novell® ZENworks® 10 Configuration Management.

Unable to override the screen saver on the managed device

Source: ZENworks 10 Configuration Management; Remote Management.

Explanation: When a password-protected screen saver is activated on the managed device prior to the start of a Remote Control session, the Remote Management service attempts to override the screen saver to enable the remote operator to view the user desktop. The remote operator can also override the screen saver during the remote session by clicking the *Override Screen Saver* icon on the Remote Management viewer toolbar.

Possible Cause: If the screen saver activates because of the inactivity of the remote session.

Action: Click the *Override Screen Saver* icon on the Remote Management viewer toolbar. You might have to click the icon a few times till it overrides.

Possible Cause: Overriding the Screen Saver feature is not supported on the Windows Vista Platform.

Action: None.

Possible Cause: The screen saver might be interrupted if any mouse movements are sent to the managed device.

Action: Select the *Block mouse move events* option in the ZENworks Remote Management viewer options window to prevent the mouse movements from being sent to the managed device.

Possible Cause: The graphical identification and authentication (GINA) on the managed device is activated because of the interruption of the screen saver on the managed device.

Action: Log in to the managed device again.

During a Remote management session, if you log off and then log in to the Windows 2000 professional machine, the wallpaper set on the machine might not be restored.

Source: ZENworks 10 Configuration Management; Remote Management.

Action: None.

Unable to launch a remote session on the managed device, which is running on a very low color quality

Source: ZENworks 10 Configuration Management; Remote Management.

Explanation: You might not be able to launch Remote control, Remote View, or Remote Diagnostics session on a managed device that is running on a very low color quality (less than 8 bits per pixel (bpp)).

Action: Increase the color quality of the device to 16 bpp or higher by using the following procedure:

1. Right-click the desktop.
2. Click *Properties*.
3. In the Display Properties window, click *Settings*.
4. Select the appropriate color quality, then click *OK*.

Unable to launch the Remote Management viewer

Source: ZENworks 10 Configuration Management; Remote Management.

Possible Cause: The Remote Management viewer might not be launched if the Remote Management viewer executable file is deleted or renamed.

Action: Reinstall the Remote Management viewer by downloading the latest version of `novell-zenworks-rm-viewer.msi` from `https://` *`ZENworks_server_IPaddress`*`/zenworks-remote-management`.

Abnormal Session Termination might fail on the Windows Vista managed device

Source: ZENworks 10 Configuration Management; Remote Management.

Explanation: During a remote session, if the user disables the network connection on Windows Vista managed device, ZENworks might not detect it as an abnormal termination and might not lock the device or log out the user on the managed device.

Action: None.

The Remote Management Listener fails to accept the remote session requests from the managed device, if the port at which the listener binds is not opened in the management console firewall.

Source: ZENworks 10 Configuration Management; Remote Management.

Action: In the management console firewall, open the listener port.

Troubleshooting error messages encountered while using the Remote Management component

Source: ZENworks 10 Configuration Management; Remote Management.

Action: To troubleshoot the error messages encountered while using the Remote Management component, send the `WinVNCApp.log` and `WinVNC.log` file for Windows Vista device or `WinVNC.log` file for other managed devices to Novell Support (http://support.novell.com).

To access the log file:

1. Open the Registry Editor.
2. Go to `HKLM\Software\Novell\ZENworks\Remote Management\Agent`.
3. Create a DWORD called DebugMode, and set value to 2.
4. Create a DWORD called DebugLevel, and set the hexadecimal value to `a` (decimal value equals 10).
5. The following Remote Management log files are created under *`ZENworks_installation_directory`*`\logs`:
   - `WinVNC.log`
   - `WinVNCApp.log` (Windows Vista only)

Install new version of the Mirage driver

Source: ZENworks 10 Configuration Management; Remote Management.

Explanation: When you install the ZENworks Adaptive Agent on a Windows 2003 64-bit managed device, the Mirage driver is not installed on the device. The message `Install new version of the Mirage driver` is logged in ZENworks Control Center.

You can perform remote sessions on the device, but the performance slows down.

Action: Ignore this message.

The managed device was unable to initialize Novell encryption scheme for the session. Ensure that the managed device is UTC time synchronized with this system. If the problem persists, contact Novell Technical Services

Source: ZENworks 10 Configuration Management; Remote Management

Action: When the managed device is upgraded or registered, do the following:

1. Update the domain name of the new CA certificate in the registry with the new details:

Key: HKLM\Software\Novell\ZENworks

Value: CASubject

2. Import the CA certificate of the new zone to the trusted root certificate store.
3. Remove the CA certificate of the old zone from the trusted root certificate store.

Applications such Regedit when launched on 64-bit managed device through Remote Execute will not have access to certain registry keys

Source: ZENworks 10 Configuration Management; Remote Management.

Possible Cause: Applications launched on 64-bit managed device using Remote Execute runs in Windows On Windows (WOW) environment.

Action: Launch the applications using Remote Diagnostics.

Cryptographic Details

A

The following sections contain the details of the various certificates generated while using the Remote Management component of Novell® ZENworks® 10 Configuration Management.

A.1 Managed Device Key Pair Details

Certificate Generated By: Remote Management service
Certificate Generated Using: OpenSSL v0.9.8e (Novell version)
Certificate Signed By: Self-signed
Certificate Signed Using: OpenSSL v0.9.8e (Novell version)
Certificate Verified By: Remote Management viewer
Certificate Verified Using: OpenSSL v0.9.8e (Novell version)
Used By: Remote Management Service
Used For: Establishing a secure session with the Remote Management viewer
Private Key Type: RSA
Key Strength: 1024 bits
Signature Algorithm: RSA-SHA256
Validity: 10 years

A.2 Remote Operator Key Pair Details

This certificate is valid only when Internal CA is deployed.

Certificate Generated By: ZENworks Server hosting ZENworks Control Center
Certificate Generated Using: Bouncy Castle library (`bcprov-jdk15-134.jar`)
Certificate Signed By: ZENworks Server hosting ZENworks Control Center
Certificate Signed Using: Bouncy Castle library (`bcprov-jdk15-134.jar`)
Certificate Verified By: Remote Management Service
Certificate Verified Using: OpenSSL v0.9.8e (Novell version)
Used By: The Remote Management viewer and the Remote Management service
Used For: Establishing secure session and identifying the remote operator
Private Key type: RSA
Key Strength: 1024 bits
Signature Algorithm: RSA-SHA1
Validity: 4 days

A.3 Remote Management Ticket Details

This certificate is valid for Rights Authentication Only.

Ticket Generated By: ZENworks Server hosting ZENworks Control Center
Ticket Generated Using: Bouncy Castle library (`bcprov-jdk15-134.jar`)
Certificate Signed By: ZENworks Server hosting ZENworks Control Center
Ticket Signed Using: Bouncy Castle library (`bcprov-jdk15-134.jar`)
Certificate Verified By: Remote Management Web Service (on the ZENworks server)
Certificate Verified Using: Bouncy Castle library (`bcprov-jdk15-134.jar`)
Used By: The Remote Management viewer and the Remote Management Web service
Used For: Authenticating the remote operator and verifying the rights to perform an operation
Signature Algorithm: RSA-SHA1
Validity: 2 minutes

A.4 Session Encryption Details

Session Established Between: Remote Management Service and Remote Management viewer
Encryption Protocol: SSL (TLSv1)
Session Cipher: AES256-SHA
SSL Authentication Mode: Mutual/Server

Best Practices

B

The following sections explain the best practices to follow while using the Remote Management component of Novell® ZENworks® 10 Configuration Management.

B.1 Remote Management Listener

When a remote operator launches the Remote Management Listener to listen to the remote session requests from the managed device user, ZENworks issues a ticket to enable the remote operator to authenticate to the managed device. The lifetime of this ticket is two days.

The Remote Management Listener continues to run even after the remote operator logs out or closes the ZENworks Control Center. If the ticket is still valid, any other remote operator might use the listener to listen to the remote session requests from the managed device users. For security purposes, you must close the Remote Management Listener before logging out or closing the browser.

To close the Remote Management Listener, right-click *ZENworks Remote Management Listener* icon in the notification area, then click *Close listening daemon*.

B.2 Remote Execute Operation

By default, the Remote Management module runs as a service with system privileges on the managed device. Hence, all the applications launched during the Remote Execute session also run with system privileges. For security reasons, we strongly recommend that you close the applications after use

B.3 Remote Management Policy

Before performing a remote operation on a device, you must create a Remote Management policy and assign it to the device.

Documentation Updates

C

This section contains information on documentation content changes that were made in this *Administration Guide* after the initial release of Novell® ZENworks® 10 Configuration Management. The information can help you to keep current on updates to the documentation.

All changes that are noted in this section are 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 are published. Within a dated section, the changes are alphabetically listed by the names of the main table of contents sections in the guide.

If you need to know whether a copy of the PDF documentation you are using is the most recent, the PDF document contains its publish date on the front title page.

The documentation was updated on the following dates:

C.1 December 04, 2007

The following changes were made:

Location	Change
Section 2.4, "Configuring the Remote Operator Rights," on page 18	1. Added Unblock Remote Management Service in the Remote Management Rights table.
Section 4.7.2, "Manually Unblocking the Remote Management Service," on page 46	1. To Unblock Remote Management Service you must have Unblock Remote Management Service rights.

C.2 November 7, 2007

The following changes were made:

Location	Change
Section 2.6, "Starting Remote Management Operations," on page 21	1. Removed the section Agent-initiated Connection from the Chapter 3, "Managing Remote Sessions," on page 31. 2. Added Section 2.6.2, "Initiating a Session from the Remote Device," on page 28 in Chapter 2, "Setting Up Remote Management," on page 15. 3. Added network diagrams for Agent-Initiated sessions and Console-Initiated sessions.