AUTHORIZED DOCUMENTATION

Remote Management Reference

Novell®

ZENworks 10 Configuration Management SP3

10.3

January 17, 2011

www.novell.com

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.
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 SP3 documentation (http://www.novell.com/documentation/zcm10/).

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:

1.1 Remote Management Terminology

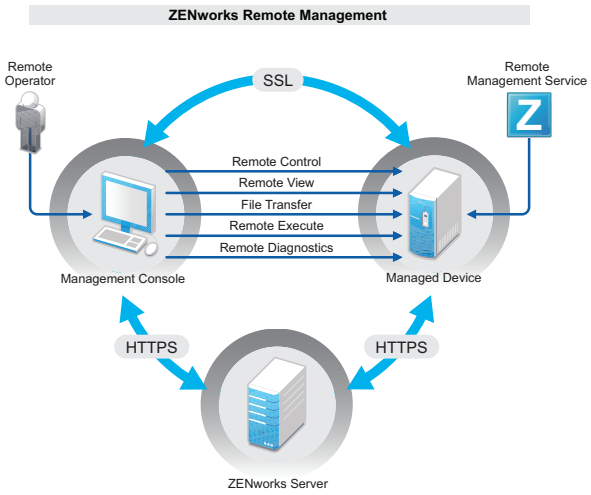
Terms	Description
Managed device	A device that you want to remotely manage. To remotely manage a device, ensure that the Remote Management component is installed and the Remote Management service is running on the device.
Management server	A device where the ZENworks Configuration Management server is installed.
Management console	The interface for managing and administering the devices. For performing the remote operations, you must install the Remote Management viewer on the console.
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 operations on the device.
Remote Management Viewer	A management console application that enables a remote operator to perform remote operations on the managed device. It allows the remote operator to view the managed device desktop, transfer files, and execute applications on the managed device.
Remote Management Listener	A management console application that enables a remote operator accept remote assistance requests from managed device users.

Terms	Description
Remote Management Proxy	A proxy server that forwards Remote Management operation requests from the Remote Management Viewer to a managed device. The proxy is useful when the viewer cannot directly access a managed device that is in a private network or on the other side of a firewall or router that is using NAT (Network Address Translation). As a prerequisite, the proxy must be installed on a Windows managed device or a Linux device (Primary server, Satellite device).

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's problems without visiting the user's workstation, thereby reducing problem resolution times and increasing productivity.

Figure 1-1 *Remote Management Operations*



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

- Section 1.2.1, "Remote Control," on page 11
- Section 1.2.2, "Remote View," on page 11
- Section 1.2.3, "Remote Execute," on page 11
- Section 1.2.4, "Remote Diagnostics," on page 11
- Section 1.2.5, "File Transfer," on page 11
- Section 1.2.6, "Remote Wake Up," on page 12

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's 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 49.

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 53.

1.2.3 Remote Execute

Remote Execute lets you run any executable with system privileges on the managed device from the management console. 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 54.

1.2.4 Remote Diagnostics

Remote Diagnostics lets you 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 54.

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 folders

- View the properties of files and folders
- Open files with the associated applications on the management console

For more information, see Section 3.5, “Managing a File Transfer Session,” on page 55

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 3.7, “Waking Up a Remote Device,” on page 58

1.3 Understanding Remote Management Features

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

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

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

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.

NOTE: On Windows Vista managed devices, mouse and keyboard locks do not function if the Aero theme is enabled.

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.

NOTE: Blanking the screen of a tablet PC managed device during a remote session degrades the session performance.

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.

This feature is not available on a Windows Vista, Windows Server 2008, and Windows 7 managed devices.

1.3.9 Automatic Session Termination

Automatically terminates 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 2.8.2, “Initiating a Session from the Managed Device,” on page 41.

NOTE: This feature is currently supported only on Windows.

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 51.

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.

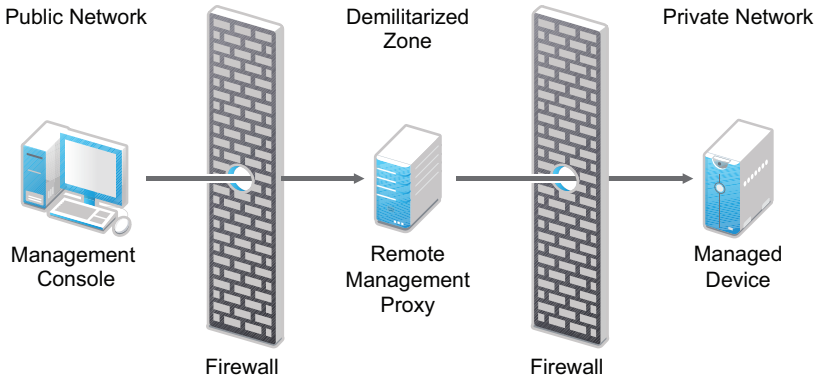
1.4 Understanding Remote Management Proxy

You cannot perform any remote management operation on a managed device that is on a private network or is on the other side of a firewall or router that is using NAT (Network Address Translation). This is because the NAT firewall hides the device IP address from the external network and thereby blocks any connection request made to the device. To remotely manage such a device, the remote operation must be routed through a Remote Management Proxy.

For more information on routing the remote operation through proxy when initiating a remote session from the Management Console, see Route Through Proxy in "Initiating a Remote Management Session from the Device Context" on page 33.

For more information on routing the remote operation through proxy when initiating a remote session from the device context, see Route Through Proxy in "Initiating a Remote Management Session from the User Context" on page 36

Figure 1-2 *Remote Management Proxy*



You must install the proxy on a device that is placed in a demilitarized zone (DMZ). The device where you install the proxy should be accessible from the public network that has the management console and must be able to access devices that are in a private network. For information on installing the remote management proxy, see Section 2.10, "Installing a Remote Management Proxy," on page 46.

The remote management proxy listens on port 5750 by default for the incoming remote management requests from the Remote Management Viewer, and forwards the requests to the device.

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 the Session Settings options:

Field	Details
Look Up Viewer DNS Name at the Start of the Remote Session	Enables 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.
Allow Remote Session when no user is logged on to the managed device	Enables a remote operator to remotely manage a device when the policy allows the remote operation but no user has logged in to the device. This option is selected by default.

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 a remote management proxy to perform remote operations on the managed device.

If the managed device is on a private network or is on the other side of a firewall or router that is using NAT (Network Address Translation), the remote management operation of the device can be routed through a remote management proxy. You must install the proxy separately. For information on installing the remote management proxy, see Section 2.10, “Installing a Remote Management Proxy,” on page 46.

Task	Details
Add a remote management proxy	1. Click *Add* to display the Add Proxy Settings dialog box. 2. Fill in the following fields: **Proxy:** Specify the IP address or DNS name of the remote management proxy. **IP Address Range:** Specify the IP addresses of the devices you want to remotely manage through the remote management proxy. You can specify the IP address range in one of the following ways: ◆ Specify the range of IP addresses using CIDR (Classless Inter-Domain Routing) notation. With CIDR, the dotted decimal portion of the IP address is interpreted as a 32-bit binary number that has been broken into four 8-bit bytes. The number following the slash (/n) is the prefix length, which is the number of shared initial bits, counting from the left side of the address. The /n number can range from 0 to 32, with 8, 16, 24, and 32 being commonly used numbers. Examples: 123.45.678.12/16: Specifies all IP addresses that start with 123.45. 123.45.678.12/24: Specifies all IP addresses that start with 123.45.678. ◆ Specify the range of IP addresses in the **From IP address** - **To IP address** format. For example: 123.45.678.12 - 123.45.678.15: Specifies all IP addresses in the range 123.45.678.12 to 123.45.678.15.
Delete a remote management proxy	1. Select the proxy you want to delete. 2. Click Delete, then click *OK*.

7 (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*.

8 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 previously configured system settings on the device, click *Revert*.

If the Remote Management settings on the device were configured at the folder level, the settings revert to the configured folder level settings; otherwise, they revert to the default zone level settings.

8 Click *Ok*.

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

2.2 Enabling the Remote Management Listener

To enable a 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 Creating 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 settings for Remote Management operations such as Remote Control, Remote View, Remote Execute, Remote Diagnostics, and File Transfer, and also allows you to control settings for 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.

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

2 In the *Policies* list, click *New*, then click *Policy* to display the Select Policy Type page.

3 Select *Remote Management Policy*, click *Next* to display the Define Details page, then fill in the fields:

Policy Name: Provide a unique name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder.

Folder: Type the name or browse to the ZENworks Control Center folder where you want the policy to reside. The default is `/policies`, but you can create additional folders to organize your policies.

Description: Provide a short description of the policy's content. This description displays in the summary page of the policy in ZENworks Control Center.

4 Click *Next* to display the Remote Management General Settings page. To accept the default settings, proceed to the next step, or use the information specified in the following table to change the default settings.

Field	Details
Allow User to Request a Remote Session	Enables the user on the managed device to request a remote operator to perform a remote session. The remote operator must ensure that the Remote Management Listener is running.
Terminate the Remote Session When Permission Is Required from a New User Logging In to the Managed Device	Terminates an ongoing remote session when permission is required from a new user who has logged into a remotely managed device.
Display Remote Session Audit Information to the User on the Managed Device	Allows the user on the managed device to view the audit information for remote sessions from the ZENworks icon.
Display Remote Management Properties in the ZENworks Icon	Allows the user on the managed device to view the properties associated with the Remote Management policy in the ZENworks icon.
Edit	To edit the message displayed to the user on the managed device before starting a remote session: 1. Click *Edit* to display the Edit Message dialog box. 2. Edit the message. 3. Click *OK*.
Restore default	To restore the default message: 1. Click *Restore default* to revert to the default message.
Add a Remote Listener	To add a Remote Listener: 1. Click *Add*. 2. In the Add Remote Listener dialog box, specify the DNS name or IP address of the management console and the port number on which the Remote Management Listener will listen for remote session requests. 3. Click *OK*.
Delete a Remote Listener	To delete a Remote Listener: 1. Select the Remote Listener you want to delete. 2. Click *Delete*.

5 Click *Next* to display the Remote Control Settings page. To accept the default settings, proceed to the next step, or use the information specified in the following table to change the default settings.

Field	Details
Allow Managed Device to be Controlled Remotely	Allows Remote Control sessions on the managed device. Selecting this option enables the subsequent options on the page. Deselecting the option disables the Remote Control operation on the device.
Ask Permission from User on Managed Device Before Starting Remote Control	Allows you to request permission from the user on the managed device before starting a Remote Control session.
Give Visible Signal to User on Managed Device During Remote Control	Displays a visible signal in the top right corner of the managed device desktop during the Remote Control session. The visible signal lets the user on the managed device know that a Remote Control session is in progress.
Give Audible Beep to User on Managed Device Every [ ] Seconds During Remote Control	Generates a beep on the managed device during a Remote Control session. The beep is generated periodically after the specified number of seconds.
Allow Managed Device Screen to be Blanked During Remote Control	Enables blanking of the screen of the managed device during a Remote Control session. Selecting this option also locks the keyboard and the mouse controls of the managed device.
Allow Managed Device Mouse and Keyboard to be Locked During Remote Control	Enables locking of the managed device mouse and keyboard during a Remote Control session.
Allow Screen Saver to be Automatically Unlocked During Remote Control	Enables the unlocking of a password-protected screen saver from the Remote Control Viewer before the start of a Remote Control session on the managed device.
Automatically Terminate Remote Control Session After Inactivity of [ ] Minutes	Terminates a Remote Control session on the managed device if it has been inactive for the specified duration.

6 Click *Next* to display the Remote View Settings page. To accept the default settings, proceed to the next step, or use the information specified in the following table to change the default settings.

Field	Details
Allow Managed Device to be Viewed Remotely	Allows Remote View sessions on the managed device. Selecting this option enables the subsequent options on the page. Deselecting the option disables the Remote View operation on the device.
Ask Permission from User on Managed Device Before starting Remote View	Allows you to request permission from the user on the managed device before starting a Remote View session.
Give Visible Signal to User on Managed Device During Remote View	Displays a visible signal in the top right corner of the managed device desktop during the Remote View session.The visible signal lets the user on the managed device know that a Remote View session is in progress.

Field	Details
Give Audible Beep to User on Managed Device Every [ ] Seconds During Remote View	Generates a beep on the managed device during the Remote View session. The beep is generated periodically after the specified number of seconds.

7 Click *Next* to display the Remote Diagnostics Settings page. To accept the default settings, proceed to the next step, or use the information specified in the following table to change the default settings.

Field	Details
Allow Managed Device to be Diagnosed Remotely	Allows Remote Diagnostics sessions on the managed device. Selecting this option enables the subsequent options on the page. Deselecting the option disables the Remote Diagnostics operation on the device.
Ask Permission from User on Managed Device Before starting Remote Diagnostics	Ensures that the remote operator requests permission from the user on the managed device before starting a Remote Diagnostics session.
Give Visible Signal to User on Managed Device During Remote Diagnostics	Displays a visible signal in the top right corner of the managed device desktop during the Remote Diagnostics session.The visible signal lets the user on the managed device know that a Remote Diagnostics session is in progress.
Give Audible Beep to User on Managed Device Every [ ] Seconds During Remote Diagnostics	Generate a beep on the managed device during the Remote Diagnostics session. The beep is generated periodically after the specified number of seconds.
Allow Managed Device Screen to be Blanked During Remote Diagnostics	Enables blanking of the screen of the managed device during a Remote Diagnostics session. The managed device keyboard and mouse are always locked during a Remote Diagnostics session. Selecting this option also disables the visible signal on the managed device.
Display Warning Message Before Reboot for [ ] Seconds	Displays a warning message on the managed device at the start of the Remote Diagnostics session, reminding the user to save all existing applications. This warning message is displayed for the specified duration to prevent the user from losing any unsaved data, because the remote operator might initiate a system reboot during the Remote Diagnostics session.
Automatically Terminate Remote Diagnostics Session After Inactivity of [ ] Minutes	Terminates the Remote Diagnostics session if it is inactive for the specified duration.

8 Click *Next* to display the Remote Execute Settings page. To accept the default settings, proceed to the next step, or use the information specified in the following table to change the default settings.

Field	Details
Allow programs to be remotely executed on the managed device	Allows programs to be executed remotely on the managed device. Selecting this option enables the subsequent options on the page. Deselecting the option disables the Remote Execute operation on the device.
Ask permission from User on Managed Device Before Starting Remote Execute	Ensures that the remote operator requests permission from the user on the managed device before starting a Remote Execute session.
Give Visible Signal to User on Managed Device During Remote Execute	Displays a visible signal in the top right corner of the managed device desktop during the Remote Execute session. The visible signal lets the user on the managed device know that a Remote Execute session is in progress.
Automatically Terminate Remote Diagnostics Session After Inactivity of [ ] Minutes	Terminates the Remote Execute session if it is inactive for the specified duration.

9 Click *Next* to display the File Transfer Settings page. To accept the default settings, proceed to the next step, or use the information specified in the following table to change the default security settings.

Field	Details
Allow Transferring Files on Managed Device	Enables transfer of files between the management console and the managed device. Selecting this option enables the subsequent options on the page. Deselecting the option disables the File Transfer operation on the device
Ask permission from User on Managed Device Before Starting File Transfer	Ensures that the remote operator requests permission from the user on the managed device before starting a File Transfer session.
Give Visible Signal to User on Managed Device During File Transfer	Displays a visible signal in the top right corner of the managed device desktop during the File Transfer session. The visible signal lets the user on the managed device know that a File Transfer session is in progress.
Allow Files to be Downloaded from Managed Device	Allows a remote operator to open files on the managed device and transfer them to the management console. If this option is not selected, the remote operator can only transfer files from the management console to the managed device.
File Transfer Root Directory	Specify the managed device directory to be seen by the remote operator during a File Transfer session. The remote operator can only transfer files to and from this directory and its subdirectories. The default directory is My Computer, which means that the remote operator can see and transfer files in the entire file system of the managed device.

10 Click *Next* to display the Security Settings page. To accept the default settings, proceed to the next step, or use the information specified in the following table to change the default security settings.

Password Authentication

Field	Details
Enable Password Based Authentication	Allows the remote operator to use a password to authenticate to the managed device. Select this option to configure the password type settings.
Minimum Password Length	Allows you to specify the minimum length for the password. By default, it is 6 characters.
Session Password	Select this option to prompt the user on the managed device to set a password before the start of a new remote session. This option is recommended because the password is not stored on the managed device and is valid only for the current session.
Persistent Password	Select this option to set the ZENworks and VNC passwords. Setting the ZENworks Password is recommended because it is safer and more secure than the VNC Password. This password can be set by the administrator through the Remote Management policy or by the managed device user from the ZENworks icon. Selecting this option enables the subsequent options. To enable the user to set the password through the ZENworks icon, select the *Allow user to override default passwords on managed device* option.
ZENworks Password	To clear the ZENworks password: 1. Click *Clear Password*. 2. Click *Apply*, then click *OK*. To set the ZENworks password: 1. Click *Set Password*. 2. Enter the password. The maximum length of the password is 255 characters. 3. Click *Apply*, then click *OK*.
VNC Password	To clear the VNC password: 1. Click *Clear Password*. 2. Click *Apply*, then click *OK*. To set the VNC password: 1. Click *Set Password*. 2. Enter the password. The maximum length of the password is 8 characters. 3. Click *Apply*, then click *OK*.

Intruder Detection

Field	Details
Enable Intruder Detection	Select this option to enable the detection of invalid or unauthorized attempts to launch a remote session on the managed device. Selecting this option enables the subsequent options in the Intruder Detection section.
Suspend Accepting Connections After [ ] Successive Invalid Attempts	Specify the maximum number of consecutive invalid attempts a remote operator can make before the Remote Management service on the managed device is blocked. By default, it is five attempts.
Automatically Start Accepting Connections After [ ] Minutes	Specify the time in minutes after which the Remote Management Agent automatically accepts a connection to the managed device. To manually unblock the Remote Management service, double-click the ZENworks Adaptive Agent icon, click *Security Settings*, then click *Enable Accepting Connections if Currently Blocked Due to Intruder Detection.* By default, it is 10 minutes.

Session Security

Field	Details
Enable Session Encryption	Enables session encryption using SSL encryption (TLSv1 protocol). Selecting this option enables the subsequent options in the Session Security section.
Allow Connection When Remote Management Console Does Not Have SSL Certificate	When a remote session is launched from the ZENworks Control Center, a certificate is automatically generated for a remote operator. This certificate is used during authentication. Select this option to allow connections from a Remote Management console launched outside ZENworks Control Center that might not have an SSL certificate.
Allow up to [ ] levels in Viewer certificate chain	The Novell rights-based and password-based authentication schemes are played over an SSL encrypted channel. The establishment of this channel requires the viewer to present a certificate. This certificate can be signed by an intermediate or a root certificate authority, thereby creating a certificate chain. This property defines the maximum number of levels that are allowed in the viewer's certificate chain. When the ZENworks internal certificate authority is employed (it is installed by default), a two-level viewer certificate chain is automatically created while launching a remote session from ZENworks Control Center.

Abnormal Termination

Field	Details
Lock Device	Locks the managed device when the remote session is terminated abnormally.

Field	Details
Log Off User	Logs off the user on the managed device when the remote session is terminated abnormally.

11 Click *Next* to display the Summary page.

12 Click *Finish* to create the policy now, or select *Define Additional Properties* to specify additional information, such as policy assignment, enforcement, status, and which group the policy is a member of.

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.

NOTE: The Remote Management rights are applicable only for Rights based authentication. However, the remote operator can perform the Remote Management operation using Password based authentication if the Remote Management policy allows.

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 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 "Section 2.3, "Creating the Remote Management Policy," on page 21".

To edit the password set in the Remote Management policy:

1. In ZENworks Control Center, click *Policies*.
2. Click the Remote Management policy, then click the *Settings* 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 *Settings* 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 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 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 *Settings* 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 *Settings* 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 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 will be effective as there is no password set by the user.

2.6 Installing the Remote Management Viewer

The Remote Management Viewer is a management console application that enables a remote operator to perform remote operations on the managed device. It allows the remote operator to view the managed device desktop, transfer files, and execute applications on the managed device.

To install the Remote Management Viewer, click the *Install Remote Management Viewer* link that is displayed in ZENworks Control Center when you are performing a remote management operation on the managed device. This link is displayed only if you are performing a remote management operation on the device for the first time and if the viewer is not already installed on the device.

If an earlier version of the Remote Management Viewer is already installed on the device, then the *Upgrade Remote Management Viewer* link is displayed. Click this link to upgrade the version of the viewer installed on the device.

Installing Remote Management Viewer on a SUSE Linux Enterprise Server 11 (SLES 11) or SUSE Linux Enterprise Desktop 11 (SLED 11) requires dependent glitz package. You must install the appropriate glitz package from the openSUSE Web site (http://software.opensuse.org/112/en).

On Windows:

1. In ZENworks Control Center, click *Configuration*.
2. In the left navigation pane, click *Download ZENworks Tools*.
3. In the left navigation pane of the ZENworks Download page, click *Administrative Tools*.
4. Click `novell-zenworks-rm-viewer-<version>.msi`.
5. (Conditional) If you have launched ZENworks Control Center by using Internet Explorer, do one of the following:
   - Click *Run* to install the viewer.
   - Click *Save* to save the file to a temporary location. Double-click the file to install the viewer.
6. (Conditional) If you have launched ZENworks Control Center by using Firefox, click *Save File* to save the file to a temporary location, then double-click the file to install the viewer

On Linux:

1. In ZENworks Control Center, click *Configuration*.
2. In the left navigation pane, click *Download ZENworks Tools*.
3. In the left navigation pane of the ZENworks Download page, click *Administrative Tools*.
4. Click `novell-zenworks-rm-viewer-<version>.noarch.rpm`.
5. Decide whether to immediately install the viewer or save the viewer RPM file to install it later.
   - To immediately install the viewer, click *Open With* to open the Remote Management Viewer with zen-installer, specify the root password, then click *OK*.

- To save the viewer RPM file to the default download directory so that you can install it later, click *Save to Disk*. To install the RPM, do one of the following:
  - Click the viewer RPM file, specify the root password, then click *OK*.
  - Run the following command as a super user or root user:

    ```
    rpm -ivh novell-zenworks-rm-viewer-<version>.noarch.rpm
    ```

2.7 Upgrading the Remote Management Viewer

If you are performing a remote management operation on a Windows managed device on which an earlier version of the Remote Management Viewer is already installed, the *Upgrade Remote Management Viewer* link is displayed in ZENworks Control Center. Click this link to upgrade the version of the viewer installed on the device.

To upgrade the Remote Management viewer on a Linux device from Novell ZENworks 10 Configuration Management SP2 (10.2) to Novell ZENworks 10 Configuration Management SP3 (10.3) or later, run the following command as a super user or root user:

```
rpm -Uvh --nopostun novell-zenworks-rm-viewer-<version>.noarch.rpm
```

Alternatively, uninstall the old version `novell-zenworks-rm-viewer-10.x.x.rpm`, and install the new version. For more information on installing the viewer, see Section 2.6, “Installing the Remote Management Viewer,” on page 31.

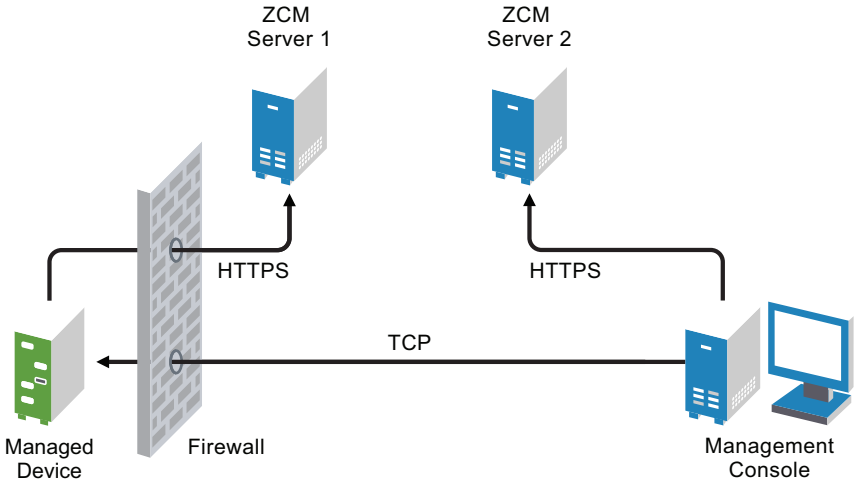
2.8 Starting Remote Management Operations

The remote operation can be initiated in the following ways:

2.8.1 Initiating a Session from the Management 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 using this default policy in rights-based authentication mode only. If you create a new Remote Management policy, the new policy overrides the default policy.

If the ZENworks Management Zone setup is spread across two or more NAT-enabled private networks that are interconnected by a public network, you must deploy DNS_ALG on the gateways of these private networks. DNS_ALG ensures that the DNS lookup queries initiated by the ZENworks components return the correct private address mapped hostname and enables the communication between the management console and the managed devices. For more information on DNS_ALG, refer to DNS ALG RFC - 2694 (http://www.ietf.org/rfc/rfc2694).

If you want to remotely manage a device by using its DNS name, ensure that Dynamic DNS service is deployed in the network.

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

- “Starting a Remote Management Operation in ZENworks Control Center” on page 33
- “Starting a Remote Management Operation in Standalone Mode” on page 39
- “Starting a Remote Management Operation by Using Command Line Options” on page 40

Starting a Remote Management Operation in ZENworks Control Center

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 33
- “Initiating a Remote Management Session from the User Context” on page 36

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 option is available only in the Remote Management dialog box.
Application	Select the application you want to launch on the device to remotely diagnose. This option 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. This mode is selected by default for the Remote Control operation. 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. **NOTE:** The collaborate mode is not yet supported on Linux. ◆ **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 mode is selected by default for the Remote View operation. This option 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 Caching	Enables caching of the remote management session data to enhance performance. This option is available for Remote Control, Remote View, and Remote Diagnostics operations. This option is currently supported only on Windows.
Enable Dynamic Bandwidth Optimization	Enables detection of the available network bandwidth and accordingly adjusts the session settings to enhance performance. This option is available for Remote Control, Remote View, and Remote Diagnostics operations.

Field	Details
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.
Route Through Proxy	Enables the remote management operation of the managed device to be routed through a remote management proxy. If the managed device is on a private network or is on the other side of a firewall or router that is using NAT (Network Address Translation), the remote management operation of the device can be routed through a remote management proxy. Fill in the following fields: **Proxy:** Specify the DNS name or the IP address of the remote management proxy. By default, the proxy configured in the Proxy Settings panel to perform the remote operation on the device is populated in this field. You can specify a different proxy. **Proxy Port:** Specify the port number on which the remote management proxy is listening. By default, the port is 5750. **NOTE:** The Remote Management Audit displays the IP Address of the device that is running the remote management proxy and not the IP address of the management console.
Use the Following Key Pair for Identification	If an internal certificate authority (CA) is deployed, the following options are not displayed. If an external CA is deployed, fill in the following fields: **Private Key:** Click *Browse* to browse to and select the private key of the remote operator. **Certificate:** Click *Browse* to browse to and select the certificate corresponding to the private key. This certificate must be chained to the certificate authority configured for the zone. The supported formats for the key and the certificate are DER, PEM, and PFX. If the PFX format is used, both the key and the certificate must be available in the same file. You should provide this file as an input for both the key and the certificate. **Enable Cache Path:** Enables the primary key and the certificate paths to be cached on the management console. This option is currently supported only on Windows.

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	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 option is available only in the Remote Management dialog box.
Application	Select the application you want to launch on the device to remotely diagnose. This option 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. This mode is selected by default for the Remote Control operation. 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. **NOTE:** The collaborate mode is not yet supported on Linux. ◆ **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 mode is selected by default for the Remote View operation. This option 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 Caching	Enables caching of the remote management session data to enhance performance. This option is available for Remote Control, Remote View, and Remote Diagnostics operations. This option is currently supported only on Windows.
Enable Dynamic Bandwidth Optimization	Enables detection of the available network bandwidth and accordingly adjusts the session settings to enhance performance. This option is available for Remote Control, Remote View, and Remote Diagnostics operations.

Field	Details
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.
Route Through Proxy	Enables the remote management operation of the managed device to be routed through a remote management proxy. If the managed device is on a private network or is on the other side of a firewall or router that is using NAT (Network Address Translation), the remote management operation of the device can be routed through a remote management proxy. Fill in the following fields: **Proxy:** Specify the DNS name or the IP address of the remote management proxy. By default, the proxy configured in the Proxy Settings panel to perform the remote operation on the device is populated in this field. You can specify a different proxy. **Proxy Port:** Specify the port number on which the remote management proxy is listening. By default, the port is 5750. **NOTE:** The Remote Management Audit displays the IP Address of the device that is running the remote management proxy and not the IP address of the management console.
Use the Following Key Pair for Identification	If an internal certificate authority (CA) is deployed, the following options are not displayed. If an external CA is deployed, fill in the following fields: **Private Key:** Click *Browse* to browse to and select the private key of the remote operator. **Certificate:** Click *Browse* to browse to and select the certificate corresponding to the private key. This certificate must be chained to the certificate authority configured for the zone. The supported formats for the key and the certificate are DER, PEM, and PFX. If the PFX format is used, both the key and the certificate must be available in the same file. You should provide this file as an input for both the key and the certificate. **Enable Cache Path:** Enables the primary key and the certificate paths to be cached on the management console. This option is currently supported only on Windows.

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

Starting a Remote Management Operation in Standalone Mode

Before starting the remote management operation in standalone mode, install the Remote Management viewer. For information on installing the viewer, see Section 2.6, “Installing the Remote Management Viewer,” on page 31.

To start the Remote Management Operation in standalone mode:

1 Double-click the `nzrViewer.exe` file to launch the ZENworks Remote Management Client.

2 In the 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.

3 Specify the DNS name or the IP address of the remote management proxy and the port number in one of the following formats:

- *IP address~~Port*. For example 10.0.0.0~~5750.
- *IP address~Port*. For example 10.0.0.0~50.

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, install the Remote Management viewer. For information on installing the viewer, see Section 2.6, "Installing the Remote Management Viewer," on page 31.

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

1 At the command prompt, change to the directory where the viewer is installed. The viewer is by default installed to the `<User_Application_Data_Folder>\Novell\ZENworks\Remote Management\bin` directory.

2 Execute the following command:

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

The default port for the managed device is 5950.

For information on the available command line options, see Section 2.9.1, "Command Line Options for Launching a Remote Operation," on page 42.

3 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.

However, starting a Remote Management operation by using the command line options has the following limitations:

- If you do not want to specify the `key`, `cert`, and `CAcert` command line options in the `nzrViewer` command for SSL authentication, 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. However, this is not recommended because the security of the device is reduced.
- If the managed device is a part of the Management Zone, ensure that the certificate presented by the viewer is valid, signed, and chained to the CA, or the SSL authentication fails.

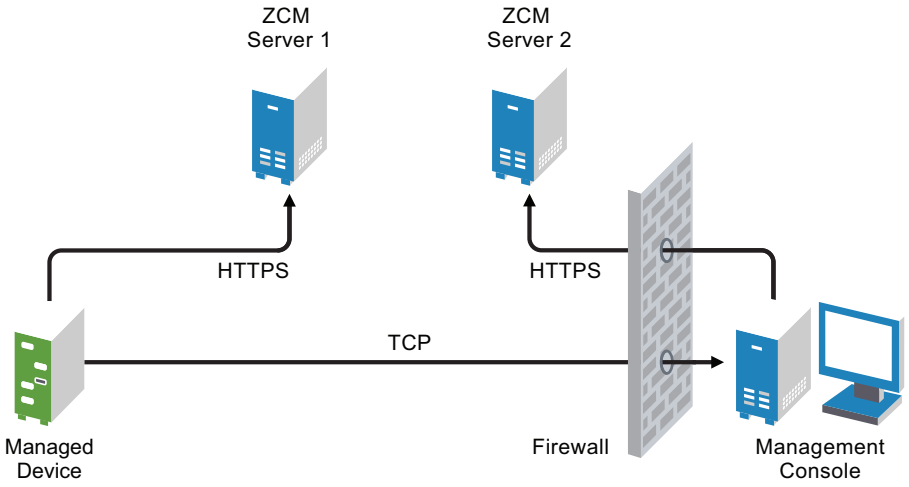
NOTE: When you launch a remote session from ZENworks Control Center (ZCC), the certificate is automatically generated by ZCC and passed on to the viewer to launch the session. The validity of the certificate is only four days.

- The managed device uses the certificate provided by the viewer to identify the remote operator. If the viewer does not provide a certificate, the user is not identified and is recorded as *unknown* in the permission message, visible signal, and audit logs.

2.8.2 Initiating a Session from the Managed 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 *Allow user to request a remote session* option is enabled in the Remote Management policy.
- 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).

2.9 Options for Launching a Remote Management Operation

When you launch a remote management operation from the command line, you can specify options to control the behavior of the remote session. For example, specifying the `remotecontrol` option launches a Remote Control operation on the device and specifying the `notoolbar` option hides the toolbar of the viewing window.

Remote Management uses certain options internally when you launch a remote management operation on a device. For example, the `zenrights` option specifies that the authentication scheme is ZENworks Rights Authentication. You must not specify these internal options when you use the command line to launch a remote management operation on a device. For more information on the options that are internally used, see Section 2.9.2, "Internal Options for Launching a Remote Operation," on page 45.

Review the following sections for more information on the remote management options:

- Section 2.9.1, "Command Line Options for Launching a Remote Operation," on page 42
- Section 2.9.2, "Internal Options for Launching a Remote Operation," on page 45

2.9.1 Command Line Options for Launching a Remote Operation

Use the following command line options to control a remote operation:

Table 2-1 *Command Line Options for Launching a Remote Operation*

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.

Command Line Option	Parameter	Description
remotecontrol		Launches a Remote Control operation on the managed device.
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 of 6, 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. This option is not yet supported on Linux.
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.
emulate3		Users with a two-button mouse can emulate a middle button by pressing both buttons at once. This option is True by default

Command Line Option	Parameter	Description
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.
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.

Command Line Option	Parameter	Description
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 to compress the remote session data 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.
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).
proxy	proxy_server	Specifies the DNS name or the IP address of the remote management proxy and the port number in one of the following formats: ◆ *IP address~~Port*. For example 10.0.0.0~~5750. ◆ *IP address~Port*. For example 10.0.0.0~50. The default port for the proxy is 5750. This option is not yet supported on Linux.

2.9.2 Internal Options for Launching a Remote Operation

The following table lists the options that Remote Management uses internally. These options should not be used when you launch a remote management operation from the command line.

Table 2-2 *Internal Options for Launching a Remote Operation*

Option	Description
zenrights	Specifies ZENworks Rights Authentication as the authentication scheme.
pipe	Specifies authentication information.

2.10 Installing a Remote Management Proxy

If a managed device is on a private network or is on the other side of a firewall or router that is using NAT (Network Address Translation), the remote management operation of the device can be routed through a remote management proxy. The proxy can be installed on a Windows managed device or a Linux device (Primary Server or Satellite Server). By default, the remote management proxy listens on port 5750.

For more information on Remote Management Proxy, see Section 1.4, "Understanding Remote Management Proxy," on page 14.

For information on the system requirements that a Windows managed device or a Linux device must meet to enable the proxy to be installed on the device, see "System Requirements" in the *ZENworks 10 Configuration Management Installation Guide*.

To install the proxy, perform the following steps:

On Windows:

1. On the device, open a Web browser to the ZENworks download page:

   https://*server*/zenworks-setup

   where *server* is the DNS name or IP address of a ZENworks Server.
2. In the left navigation pane, click *Administrative Tools*.
3. Click `novell-zenworks-rm-repeater-<version>.msi` and save the file to a temporary location.

   version is the version of the ZENworks product.
4. Install the proxy application by executing the following command:

```
msiexec /i novell-zenworks-rm-repeater-<version>.msi
TARGETDIR="ZENworks_Installation_directory".
```

On Linux:

1. On the device, open a Web browser to the ZENworks download page:

   https://*server*/zenworks-setup

   where *server* is the DNS name or IP address of a ZENworks Server.
2. In the left navigation pane, click *Administrative Tools*.
3. Click `novell-zenworks-rm-repeater-<version>.noarch.rpm`.
4. Decide whether to immediately install the proxy or save the proxy RPM file to install it later.
   - To immediately install the proxy, click *Open With* to open the Remote Management Proxy with zen-installer, specify the root password, then click *OK*.
   - To save the proxy RPM file to the default download directory so that you can install it later, click *Save to Disk*. To install the RPM, do one of the following:
     - Click the proxy RPM file, specify the root password, then click *OK*.
     - Run the following command as a super user or root user:

```
rpm -ivh novell-zenworks-rm-repeater-<version>.noarch.rpm
```

The Remote Management Proxy is designed to run automatically upon installation. You can choose to customize its behavior by modifying the default settings for the device. For more information on the Remote Management Proxy settings, see Section 2.11, “Configuring a Remote Management Proxy,” on page 47.

2.11 Configuring a Remote Management Proxy

When you install a Remote Management Proxy on a device, certain settings are configured on the device, by default. You can choose to edit the settings.

2.11.1 Remote Management Proxy Settings on a Windows Device

On a Windows device, the registry settings for the Remote Management proxy are available at `HKLM\SOFTWARE\Novell\ZCM\Remote Management\Proxy`.

ClientPort: Specifies the port number that the proxy uses to listen for any remote session requests from the Remote Management Viewer. The default value is 5750.

SessionEncryption: Specifies whether the initial flow of data between the proxy and the Remote Management Viewer is encrypted. The default value is True. The setting is not applicable after the proxy establishes a connection with the managed device. The session encryption is then governed by the Remote Management policy and the preferences of remote operator. You should leave this setting as True because setting it to False allows unauthenticated external processes other than the Remote Management Viewer to make connections to devices inside the private network.

SSLClientAuthentication: Specifies whether the proxy should accept connection requests from a viewer that does not have a valid certificate. The possible values are True and False. The default value is True.

2.11.2 Remote Management Proxy Settings on a Linux Primary Server or Satellite Server

On a Linux Primary Server or Satellite Server, the settings for the Remote Management proxy are available in the `/etc/opt/novell/zenworks/repeater/nzrepeater.ini` file. Some of the settings are:

viewerport: Specifies the port number that the Remote Management proxy uses to listen for any remote session requests from the Remote Management Viewer. The default value is 5750.

runasuser: Specifies the user that the proxy should impersonate. The Remote Management Proxy requires only user privileges to perform remote operations. The default value is zenworks. However, you can specify a different user.

strictimpersonation: Specifies if the remote session should continue as `root` when the user specified as the runasuser does not exist. The possible values are true or false. The default value is false, which indicates that the remote session continues as `root` when the user specified as the runasuser does not exist.

sslauth: Specifies whether SSL authentication is enabled or disabled. The possible values are 0 or 1. The default value is 1, which indicates that SSL authentication is enabled.

WARNING: Disabling SSL authentication is not recommended because it allows the external processes to access the network devices without any authentication.

---

verifyViewerCert: Specifies if the Remote Management Viewer certificates needs to be verified. This setting is applicable only when SSL authentication is enabled. The possible values are 0 or 1. The default value is 1, which indicates that the Remote Management Viewer certificates must be verified When a session is initiated from a stand-alone viewer, the remote operator might not have the required certificates that are chained to the root Certificate Authority. If this is a case, the proxy fails to connect to the server.

loggingenabled: Specifies whether the messages should be logged on the device. The possible values are true or false. The default value is true.

For information on other registry settings, see the `/etc/opt/novell/zenworks/repeater/nzrepeater.ini` file.

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 2.8, “Starting Remote Management Operations,” on page 32.

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 get 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 55.
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. This option is currently supported only on Windows. For more information on Session Collaboration, see Section 3.1.2, “Session Collaboration,” on page 51.

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. This option is currently supported only on Windows.

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 collaborate mode.

   For information on launching a Remote Control session, see Section 2.8, “Starting Remote Management Operations,” on page 32.
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 "Section 2.3, "Creating the Remote Management Policy," on page 21"

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 to whom 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 2.8, "Starting Remote Management Operations," on page 32.

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.

1. Launch the Remote Execute session.

   For information on launching a Remote Execute session, see Section 2.8, "Starting Remote Management Operations," on page 32.

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.
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.
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 55
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 17.

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 2.8, “Starting Remote Management Operations,” on page 32.

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 the File Transfer controls and the options that are available for working with files from the File Transfer window. The *Actions* menu option is not yet supported on Linux. However, you can perform the operation by clicking the appropriate icon on the toolbar.

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 Managing a Remote Management Proxy Session

A Remote Management Proxy enables you to perform a Remote Management operation on a managed device that is on a private network or is on the other side of a firewall or router that is using NAT (Network Address Translation).

For more information on a Remote Management Proxy, see Section 1.4, “Understanding Remote Management Proxy,” on page 14.

For more information on installing a Remote Management Proxy, see Section 2.10, “Installing a Remote Management Proxy,” on page 46.

For more information on configuring a Remote Management Proxy, see Section 2.11, “Configuring a Remote Management Proxy,” on page 47.

3.7 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.

Waking up a device that has multiple NICs (Network Interface Cards) is successful only if one or more of the NICs is configured for a subnet that contains the device that is broadcasting the Wake-on-LAN packet.

3.7.1 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.

3.7.2 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 one of the following options to specify the servers to send a wakeup request to the managed devices:
   - **Automatically detect the server:** ZENworks automatically detects the Primary Server closest to the managed device. If the server and the remote device are in different subnets, ensure that the router connecting them is configured to forward subnet-oriented broadcasts on UDP port 1761.
   - **Use the following devices:** Click *Add* to select a proxy device that exists in the same subnet as the device you want to wake up.

     If the router is configured to forward subnet-oriented broadcasts on UDP port 1761, a proxy is not required.
6. (Optional) Select one of the following options to specify the IP address to be used for sending the wake-up broadcast:
   - **Automatically detect the IP address:** ZENworks automatically detects the default broadcast address of the subnet to send the wakeup broadcast to the managed device.
   - **Use the following IP address:** Specify the IP address to send the wakeup broadcast to the managed device, then click *Add*.
7. In the *Number of Retries* option, specify the number of attempts to wake up the device. By default, it is 1.
8. In the *Time Interval between Retries option,* specify the time period between two retry attempts. By default, it is 2 minutes.
9. Click *OK*.

The default values for the *Number of Retries* and the Time Interval between Retries options are configured at the zone level. You can override these values at the device level.

3.8 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 3.8.1, “On the Management Console,” on page 60
- Section 3.8.2, “On the Managed Device,” on page 60

3.8.1 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.

3.8.2 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.

Using rights-based authentication requires the ZENworks Adaptive Agent to be installed on the device. Installing only the Remote Management service on the device is not sufficient.

This mode of authentication is not supported when launching remote management operation in the standalone mode or from the command line.

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 the 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 such as telephone. 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 ZENworks Control Center,” on page 30.

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 the Remote Management Listener.

By default, the remote management proxy listens on port 5750.

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 an administrator who is a member of the administrators group of the managed device. 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 was 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.
	NOTE: If the remote management operation of the device is routed through a Remote Management proxy, the IP address of the device that is running the proxy is displayed.
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.

Field	Description
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 about 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

When the ZENworks Adaptive Agent is installed on a 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.

- "During the Remote Control session, clicking the Ctrl+Alt+Del icon in the Remote Management viewer might display the Secure Attention Sequence window without any controls" on page 73
- "The desktop of a device might not be visible when you remotely control or remotely view the device" on page 74
- "Unable to remotely transfer files to restricted folders on a Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 device" on page 74
- "Unable to launch a remote session on a SUSE Linux Enterprise Server 11 device through Mozilla Firefox" on page 74
- "The Upgrade Remote Management Viewer link is not displayed if you launch the ZENworks Control Center through Internet Explorer 8" on page 75

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 a Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 device.

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 that 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 a Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 managed device

Source: ZENworks 10 Configuration Management; Remote Management.

Explanation: During a remote session, if the user disables the network connection on a Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 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 following log files to Novell Support (http://support.novell.com):

- `WinVNCApp.log` and `WinVNC.log` files for Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 device
- `WinVNC.log` file for other managed devices

To access the log file:

1. Open the Registry Editor.
2. Go to `HKLM\Software\Novell\ZCM\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. Restart the Remote Management Service.

The following Remote Management log files are created under *`ZENworks_installation_directory`*`\logs`:

- `WinVNC.log`
- `WinVNCApp.log`

How do I enable Remote Management debug log on the device launching the ZENworks Control Center

Source: ZENworks 10 Configuration Management; Remote Management.

Action: To enable the logs, see TID 3418069 in the Novell Support Knowledgebase (http://support.novell.com/search/kb_index.jsp).

Install a new version of the Mirror driver

Source: ZENworks 10 Configuration Management; Remote Management.

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

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

Action: Ignore this message.

Possible Cause: If you remotely control a device which is already connected using Remote Desktop Connection (RDP), the message `Install new version of the Mirror 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.

Possible Cause: The managed device has been upgraded or registered and this information might not be updated in the registry of the managed device.

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\ZCM

   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.

Possible Cause: The managed device has been moved to a new Management Zone.

Action: Manage the device from the new Management Zone.

Applications such as 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.

Blank screen option might fail to work while remote controlling a Windows device

Source: ZENworks 10 Configuration Management; Remote Management.

Possible Cause: The legacy drivers of Windows do not allow blank screen power option.

Action: You must install the system-specific graphics driver.

On launching a remote management session on a Windows 2000 Professional managed device, the device reboots

Source: ZENworks 10 Configuration Management; Remote Management.

Possible Cause: The video driver is not installed on the device.

Action: You must install the system-specific video driver.

Multiple instances of the Remote Management viewer are launched on the device that has the Internet Explorer 7 browser

Source: ZENworks 10 Configuration Management; Remote Management.

Possible Cause: If you launch a Remote Management operation on a device that has the Internet Explorer 7 browser, multiple instances of the viewer are launched on the device if download accelerator software such as FlashGet is installed on the management console.

Action: Temporarily disable the add-ons for the download accelerators:

1. Launch the Internet Explorer 7 browser.
2. Click *Tools > Manage Add-ons*.
3. Click *Enable or Disable Add-ons*, then disable the add-on for the download accelerator.
4. Launch the Remote Management operation.

Action: Try using the Firefox browser to perform the operation.

Unable to use the Ctrl-Alt-Del icon while remotely controlling a Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 device

Source: ZENworks 10 Configuration Management; Remote Management.

Explanation: If you launch a Remote Control operation on a Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 device that has User Account Control (UAC) disabled, the *Ctrl-Alt-Del* icon is dimmed.

Action: Either enable the UAC or perform the following steps to edit the Windows Group Policy settings:

1. Click *Start > Run*.
2. In the Run dialog box, specify gpedit.msc and click *OK*.
3. In the Group Policy Editor, double-click *Computer Configuration > Administrative Templates > Windows Components > Windows Logon Options > Disable or enable software Secure Attention Sequence*.
4. In the *Disable or enable software Secure Attention Sequence* Window, click *Enabled*.
5. In the *Set which software is allowed to generate the Secure Attention Sequence* option, select *Services and Ease of Access applications*.
6. Click *OK*.

The default session mode is not selected in the Remote Management snap-in

Source: ZENworks 10 Configuration Management; Remote Management.

Explanation: If you use Internet Explorer to open ZENworks Control Center and perform a Remote Management operation on a device, the default session mode is not selected in the Remote Management snap-in. However, if you do not select any session mode, the Remote Control operation is launched in the default collaborate mode and the Remote View operation is launched in the default exclusive mode.

Action: Select the session mode to perform the Remote operation.

The Install Remote Management Viewer link remains active on a Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 device that has the Internet Explorer 7 browser

Source: ZENworks 10 Configuration Management; Remote Management.

Explanation: On a Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 device that has the Internet Explorer 7 browser, the *Remote Management Viewer* might fail to install if the ActiveX control is not activated.

Action: Do the following to turn on User Account Control (UAC) on the Vista device:

1. Click *Start* > *Settings* > *Control Panel* > *User Accounts* > *User Accounts* > *Turn User Account Control On or Off*.
2. Select *Use User Account Control (UAC) to help protect your computer*.
3. Click *OK*.

Action: If you do not want to turn on the UAC on the Windows Vista device, you should upgrade to Windows Vista SP1.

Installation of the Remote Management viewer might fail

Source: ZENworks 10 Configuration Management; Remote Management.

Explanation: The Remote Management viewer installation might fail. This error is inherent to the MSI framework.

Action: Perform either of the following steps:

- Uninstall the Remote Management viewer by using Add/Remove Programs, then reinstall it
- Use the Microsoft Windows Installer Cleanup Utility to clean up the application, then reinstall it. This utility can be downloaded from Microsoft Support (http://support.microsoft.com/kb/290301)

The Remote Management viewer fails to launch on a Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 device

Source: ZENworks 10 Configuration Management; Remote Management.

Explanation: On Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 device, the Remote Management viewer fails even though the security prompt is successfully completed.

Action: Add the server running ZENworks Control Center to the list of trusted sites and retry.

During the Remote Control session, clicking the Ctrl+Alt+Del icon in the Remote Management viewer might display the Secure Attention Sequence window without any controls

Source: ZENworks 10 Configuration Management; Remote Management.

Action: Click the *Ctrl+Alt+Del* icon in the Remote Management viewer, then press the Esc key to exit the Secure Attention Sequence (SAS) window. Then, click the *Ctrl+Alt+Del* icon again in the Remote Management viewer.

The desktop of a device might not be visible when you remotely control or remotely view the device

Source: ZENworks 10 Configuration Management; Remote Management.

Explanation: If you remotely control or remotely view a device on which an RDP session was performed, you might see a black screen rather than the desktop of the device.

Action: To view the desktop of the device:

1. Manually unlock the desktop.
2. Reinitiate an RDP session on the console session of the device by running the following command:

   ```
   mstsc /console
   ```

Unable to remotely transfer files to restricted folders on a Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 device

Source: ZENworks 10 Configuration Management; Remote Management.

Explanation: If you launch a File Transfer operation to remotely transfer files to restricted folders on a Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 device that has User Account Control (UAC) enabled, the operation fails.

Action: Do the following to turn off User Account Control (UAC) on the Windows Vista device:

1. Click *Start* > *Settings* > *Control Panel* > *User Accounts* > *User Accounts* > *Turn User Account Control On or Off*.
2. Deselect *Use User Account Control (UAC) to help protect your computer*.
3. Click *OK*.

Action: Do the following to turn off User Account Control (UAC) on the Windows 7 device:

1. Click *Start* > *Control Panel* > *User Accounts* > *Change User Account Control Settings*.
2. Slide the slider bar to the lowest value (towards *Never Notify*) with description displaying Never notify me.
3. Click *OK*.
4. Restart the device.

Unable to launch a remote session on a SUSE Linux Enterprise Server 11 device through Mozilla Firefox

Source: ZENworks 10 Configuration Management; Remote Management.

Explanation: Remote Management plug-in for Firefox is installed in the `/usr/lib/firefox` directory, which is also the default Firefox installation directory. If you have installed Firefox in a different directory on the SLES 11 device, then launching a remote session through Firefox fails on the device.

Action: Copy the `nsZenworksPluginSample.so` file from the `/usr/lib/firefox/plugins` directory to the Firefox plug-ins directory.

The Upgrade Remote Management Viewer link is not displayed if you launch the ZENworks Control Center through Internet Explorer 8

Source: ZENworks 10 Configuration Management; Remote Management.

Explanation: If you upgrade to ZENworks Configuration Management SP3 from ZENworks Configuration Management SP2 and launch ZENworks Control Center through Internet Explorer 8, the *Upgrade Remote Management Viewer* link is not displayed in ZENworks Control Center.

Action: To view the U*pgrade Remote Management Viewer* link, perform the following steps:

1. Launch the Internet Explorer 8 browser.
2. Click *Tools* > *Internet Options* to display the Internet Options dialog box.
3. Click the *Security* tab.
4. Click the *Custom level* option.
5. Ensure that the following settings are enabled:
   - *Run ActiveX controls and plug-ins*
   - *Initialize and script ActiveX controls not marked as safe for scripting*
6. Restart the browser.

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 Closing the 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 the *ZENworks Remote Management Listener* icon in the notification area, then click *Close listening daemon*.

B.2 Closing Applications Launched During Remote Execute Operation

By default, the Remote Management module runs as a service with system privileges on the managed device. Consequently, 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 Identifying the Remote Operator on the Managed Device

When a remote operator launches a remote session on a managed device through ZENworks Control Center, a certificate that helps the managed device to identify the remote operator is automatically generated by ZENworks if an internal CA is used. However, if an external CA is used, the remote operator needs to manually provide the certificate that is chained to the deployed external CA and is certified for SSL Client Authentication. For more information on using the external CA, see *Use the Following Key Pair for Identification* in Section 2.8, "Starting Remote Management Operations," on page 32.

If a remote operator launches a remote operation on a managed device without providing a certificate, the name of the remote operator is recorded as *An Unknown User* in the audit logs, the Visible Signal and the Ask User Permission dialog box. To ensure that the remote operator provides the certificate, deselect *Allow Connection When Remote Management Console Does Not Have SSL Certificate* in the Remote Management policy.

B.4 Performing a Remote Control Session on a Device That Is Already Connected through a Remote Desktop Connection

To remotely control a device that is already connected using Remote Desktop Connection (RDP), ensure one of the following:

- The RDP session is in progress on the managed device
- The managed device was manually unlocked after the termination of the RDP session on the device.

B.5 Determining the Management Console Name

If the *Look up viewer DNS name at the start of the remote session* option is enabled in the Remote Management policy, the managed device attempts to determine the management console name at the start of a remote session. This might cause a significant delay in starting the remote session if the network does not have reverse DNS lookup enabled. To prevent the delay, disable *Look up viewer DNS name at the start of the remote session* in the policy.

B.6 Using the Aero Theme on Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2 devices

To enhance the performance of a remote session, Remote Management uses a mirror driver to detect the changes on the screen. If the mirror driver is not compatible with the Aero desktop theme, an attempt to load the mirror driver on a device that has the Aero theme enabled switches the device to the default desktop theme. This might affect the user experience, so it is not recommended to use Aero theme on a device that you want to remotely manage.

If you would like to retain the Aero theme during the remote session of the managed device, then disable the mirror driver on the device. To disable the mirror driver, deselect the *Enable Optimization Driver*setting on the device. For more information on the Enable Optimization Driver setting, see Configuring the Remote Management Settings at the Zone Level.

However, enabling the Aero theme on the managed device might degrade the performance of the remote session on the device.

B.7 Enabling the Secure Attention Sequence (Ctrl+Alt+Del) Button when Remotely Controlling a Windows Vista or Windows Server 2008 device

To enable the  (Ctrl+Alt+Del) icon in the Remote Management viewer toolbar when remotely controlling a Windows Vista or Windows Server 2008 device, ensure that the User Account Control (UAC) is enabled on the managed device.

B.8 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, see Section 3.8, “Improving the Remote Management Performance,” on page 59.

Documentation Updates

C

This section contains information on documentation content changes that were made in this *ZENworks Remote Management Reference* for Novell ZENworks10 Configuration Management SP3. The information can help you to keep current on updates to the documentation.

The documentation for this product is provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the changes listed in this section.

If you need to know whether a copy of the PDF documentation that you are using is the most recent, the PDF document includes a publication date on the title page.

The following updates were made to the document:

C.1 January 17, 2011: Update for ZENworks 10 Configuration Management SP3 (10.3.2)

Updates were made to the following changes sections:

Location	Change
Chapter 5, "Troubleshooting," on page 67	Updated the following scenario: "Unable to use the Ctrl-Alt-Del icon while remotely controlling a Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 device" on page 72.

C.2 July 27, 2010: Update for ZENworks 10 Configuration Management SP3 (10.3.1)

Updates were made to the following changes sections:

Location	Change
"Unable to use the Ctrl-Alt-Del icon while remotely controlling a Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 device" on page 72	This scenario is applicable for a Windows 7 device also.

C.3 March 30, 2010: SP3 (10.3)

Updates were made to the following changes sections:

Location	Change
"Remote Management Proxy" on page 10	Updated the section.
Section 1.3, "Understanding Remote Management Features," on page 12	Updated the section.
Section 2.5, "Configuring the Remote Management Password," on page 29	Updated the section.
Section 2.9, "Options for Launching a Remote Management Operation," on page 42	Added the section.
Section 2.10, "Installing a Remote Management Proxy," on page 46	Updated the section to add the support for installing Remote Management proxy on Linux.
Section 2.11, "Configuring a Remote Management Proxy," on page 47	Added the section.
Section 3.7, "Waking Up a Remote Device," on page 58	Updated the section to add information on waking up a device that has multiple NICs.
Section 3.6, "Managing a Remote Management Proxy Session," on page 58	Added the section.
Chapter 5, "Troubleshooting," on page 67	Added the following scenarios: ◆ "Unable to launch a remote session on a SUSE Linux Enterprise Server 11 device through Mozilla Firefox" on page 74 ◆ "The Upgrade Remote Management Viewer link is not displayed if you launch the ZENworks Control Center through Internet Explorer 8" on page 75
Chapter 5, "Troubleshooting," on page 67	Added the following scenario: Unable to remotely transfer files to restricted folders on a Windows Vista or Windows 7 device
Section B.6, "Using the Aero Theme on Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2 devices," on page 80	Updated the section.