ZENworks 2017 Update 4

Remote Management Reference

January 2019

Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S.

Government rights, patent policy, and FIPS compliance, see https://www.novell.com/company/legal/.

Copyright © 2008 - 2019 Micro Focus Software Inc. All rights reserved.

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contents

About This Guide **7**

1 Overview **9**

1.1 Remote Management Terminology . . . 9
1.2 Understanding Remote Management Operations . . . 10
1.2.1 Remote Operations on a Windows Device . . . 11
1.2.2 Remote Operations on a Linux Device . . . 13
1.2.3 Remote Operations on a Macintosh Device . . . 14
1.3 Understanding Remote Management Features on a Windows Device . . . 16
1.3.1 Visible Signal . . . 16
1.3.2 Intruder Detection . . . 16
1.3.3 Session Encryption . . . 17
1.3.4 Audible Beep . . . 17
1.3.5 Keyboard and Mouse Locking . . . 17
1.3.6 Screen Blanking . . . 17
1.3.7 Abnormal Termination . . . 17
1.3.8 Overriding Screen Saver . . . 17
1.3.9 Automatic Session Termination . . . 18
1.3.10 Agent Initiated Connection . . . 18
1.3.11 Session Collaboration . . . 18
1.3.12 Remote Management Auditing . . . 18
1.3.13 Switch Display . . . 18
1.4 Understanding Remote Management Proxy . . . 19
1.5 Understanding Remote Management Join Proxy . . . 19

2 Setting Up Remote Management **21**

2.1 Setting Up Remote Management to Manage a Windows Device . . . 21
2.1.1 Configuring the Remote Management Settings on a Windows Device . . . 21
2.1.2 Creating the Remote Management Policy . . . 26
2.1.3 Configuring the Remote Operator Rights . . . 32
2.1.4 Configuring the Remote Management Agent Password on a Windows Managed Device . . . 33
2.1.5 Starting Remote Management Operations on a Windows Device . . . 35
2.1.6 Enabling the Remote Management Listener . . . 45
2.2 Setting Up Remote Management to Manage a Linux Device . . . 45
2.2.1 Configuring the Remote Management Settings on a Linux Device . . . 45
2.2.2 Configuring the Remote Management Agent Password on a Linux Managed Device . . . 49
2.2.3 Starting Remote Management Operations on a Linux Device . . . 49
2.2.4 Preparing a Linux Device for a Remote Control Session . . . 51
2.2.5 Preparing a Linux Device for a Remote Login Session . . . 52
2.3 Setting Up Remote Management to Manage a Macintosh Device . . . 55
2.3.1 Enabling Remote Management on a Macintosh Device . . . 55
2.3.2 Starting Remote Management Operations on a Macintosh Device . . . 56
2.4 Configuring and Launching Remote Management . . . 57
2.4.1 Installing ZCC Helper . . . 57
2.4.2 Installing ZCC Helper in a Terminal Server or in a Citrix XENapp Environment . . . 57

2.4.3 Options for Launching a Remote Management Operation . . . 59
2.4.4 ZENworks Remote Management Viewer Options . . . 63
2.5 Configuring Remote Management Proxy . . . 66
2.5.1 Installing a Remote Management Proxy . . . 66
2.5.2 Configuring a Remote Management Proxy . . . 68
2.6 Launching a Remote SSH Session on a Linux Device . . . 69
2.7 Requesting a Remote Management Session in the Absence of the Z-icon . . . 70

3 Managing Remote Sessions 71

3.1 Managing Remote Sessions on a Windows Device . . . 71
3.1.1 Managing a Remote Control Session . . . 71
3.1.2 Managing a Remote View Session . . . 76
3.1.3 Managing a Remote Execute Session . . . 77
3.1.4 Managing a Remote Diagnostics Session . . . 77
3.1.5 Managing a File Transfer Session . . . 78
3.1.6 Improving the Remote Management Performance on the Windows Managed Device . . . 81
3.2 Managing Remote Sessions on a Linux Device . . . 82
3.2.1 Managing a Remote Control Session . . . 82
3.2.2 Managing a Remote View Session . . . 84
3.2.3 Managing a Remote Login Session . . . 85
3.2.4 Managing a Remote SSH session . . . 86
3.2.5 Improving the Remote Management Performance on the Linux Managed Device . . . 87
3.3 Managing Remote Sessions on a Macintosh Device . . . 87
3.3.1 Managing a Remote Control Session on a Macintosh Device . . . 88
3.3.2 Managing a Remote View Session on a Macintosh Device . . . 89
3.3.3 Managing a Remote SSH Session on a Macintosh Device . . . 90
3.4 Performing Remote Control on a Macintosh device . . . 91
3.5 Managing a Remote Management Proxy Session . . . 91
3.6 Waking Up a Remote Device . . . 92
3.6.1 Prerequisites . . . 92
3.6.2 Remotely Waking Up the Managed devices . . . 92

4 Security 95

4.1 Security On Windows Devices . . . 95
4.1.1 Authentication . . . 95
4.1.2 Password Strength . . . 97
4.1.3 Ports . . . 97
4.1.4 Audit . . . 97
4.1.5 Ask Permission from the User on the Managed Device . . . 98
4.1.6 Abnormal Termination . . . 98
4.1.7 Intruder Detection . . . 99
4.1.8 Remote Operator Identification . . . 99
4.1.9 Browser Configuration . . . 100
4.1.10 Session Security . . . 100
4.2 Security On Linux Devices . . . 101
4.2.1 Authentication . . . 101
4.2.2 Password Strength . . . 101
4.2.3 Ports . . . 102
4.2.4 Ask Permission from the User on the Managed Device . . . 102

5 Remote Management Audit Events 103

5.1 Agent Events. 103
5.2 Remote Management 103
5.3 Prerequisites 104
5.4 Enabling Remote Management Agent Audit Events 104
5.5 Common Tasks 105
5.5.1 Editing or Deleting Remote Management Audit Events 106
5.5.2 Viewing Details - Generated Remote Management Audit Events 106
5.5.3 Verifying the Enabled Remote Management Audit Events 106
5.6 General 107
5.6.1 Abnormal Termination 107
5.7 Authentication 108
5.7.1 Authentication Failure 108
5.7.2 Authentication Success 110
5.8 Intruder Detection 110
5.8.1 Intruder Detection Lock 111
5.8.2 Intruder Detection Reset Audit Event 111
5.9 Session 113
5.9.1 Remote Control. 113
5.9.2 Remote View 114
5.9.3 Remote Execute 114
5.9.4 Remote Diagnostics 115
5.9.5 File Transfer 116
5.10 Others 117
5.10.1 Internal Operations 117
5.10.2 Intermediate Events 117
5.10.3 Abrupt Termination 117

6 Troubleshooting 119

6.1 Troubleshooting Windows Devices 119
6.2 Troubleshooting Linux Devices 130
6.3 Troubleshooting Macintosh Devices 132

A Cryptographic Details 135

A.1 Managed Device Key Pair Details 135
A.2 Remote Operator Key Pair Details 135
A.3 Remote Management Ticket Details 136
A.4 Session Encryption Details 136

B Best Practices 137

B.1 On a Windows Device 137
B.1.1 Closing the Remote Management Listener 137
B.1.2 Closing Applications Launched During Remote Execute Operation 138
B.1.3 Identifying the Remote Operator on the Managed Device. 138
B.1.4 Performing a Remote Control Session on a device that is already remotely connected 138
B.1.5 Determining the Management Console Name 138
B.1.6 Using the Aero Theme on Windows 8, Windows 7, Windows Server 2008, and Windows Server 2008 R2 devices 139

B.1.7 Enabling the Secure Attention Sequence (Ctrl+Alt+Del) Button when Remotely Controlling a Windows Server 2008 device 139
B.1.8 Remote Management Performance 139
B.2 On a Linux Device 139
B.2.1 Remote Management Performance 139

About This Guide

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

- Chapter 1, “Overview,” on page 9
- Chapter 2, “Setting Up Remote Management,” on page 21
- Chapter 3, “Managing Remote Sessions,” on page 71
- Chapter 4, “Security,” on page 95
- Chapter 6, “Troubleshooting,” on page 119
- Appendix A, “Cryptographic Details,” on page 135
- Appendix B, “Best Practices,” on page 137

Audience

This guide is intended for 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.

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 2017 documentation Web site.

1 Overview

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

On a Windows Device:

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

On a Linux Device:

- Remotely control a managed device
- Remotely wake up a powered-off managed device
- Remotely Log in to a managed device and start a new graphical session without disturbing the user on a managed device
- Remotely execute commands on a managed device through SSH

On a Macintosh Device:

- Remotely control a managed device

Review the following sections:

- Section 1.1, “Remote Management Terminology,” on page 9
- Section 1.2, “Understanding Remote Management Operations,” on page 10
- Section 1.3, “Understanding Remote Management Features on a Windows Device,” on page 16
- Section 1.4, “Understanding Remote Management Proxy,” on page 19
- Section 1.5, “Understanding Remote Management Join Proxy,” on page 19

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.

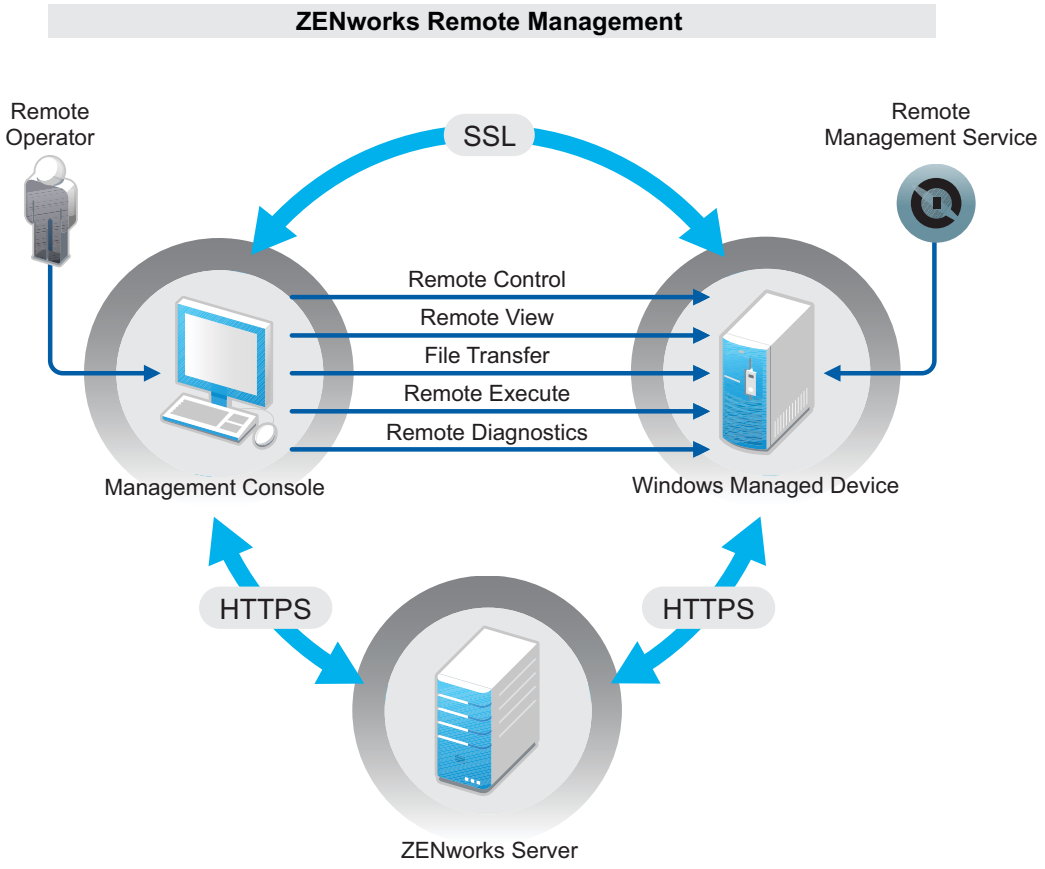
Terms	Description
Management server	A device where the ZENworks Configuration Management server is installed.
Management console	The interface for managing and administering the devices. For performing the remote operations, you must install ZCC Helper on the device. For more information on Installing ZCC Helper, see Section 2.4.1, “Installing ZCC Helper,” on page 57
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.
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 Linux 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.

- Section 1.2.1, “Remote Operations on a Windows Device,” on page 11
- Section 1.2.2, “Remote Operations on a Linux Device,” on page 13
- Section 1.2.3, “Remote Operations on a Macintosh Device,” on page 14

1.2.1 Remote Operations on a Windows Device



The following sections help you to understand the various Remote Management operations that can be performed on a Windows managed device:

- "Remote Control" on page 11
- "Remote View" on page 12
- "Remote Execute" on page 12
- "Remote Diagnostics" on page 12
- "File Transfer" on page 12
- "Remote Wake Up" on page 13

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 3.1.1, "Managing a Remote Control Session," on page 71.

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 3.1.2, “Managing a Remote View Session,” on page 76.

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 3.1.3, “Managing a Remote Execute Session,” on page 77.

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 3.1.4, “Managing a Remote Diagnostics Session,” on page 77.

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

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

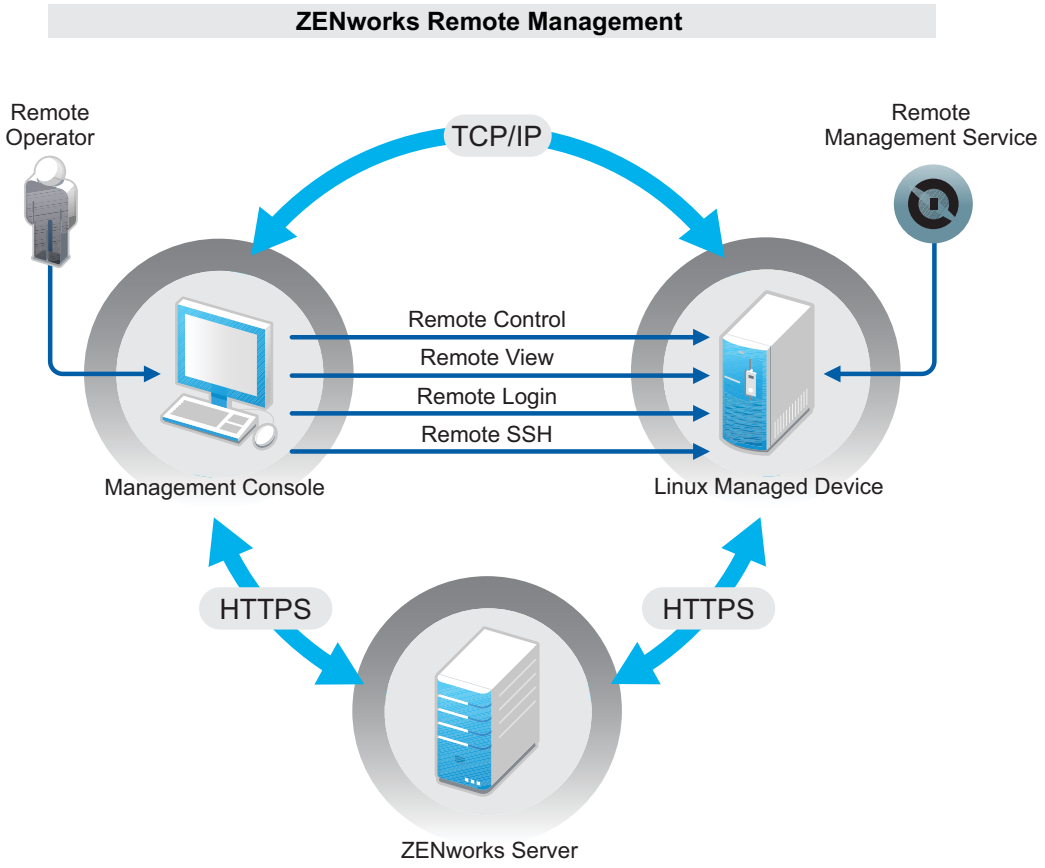
For more information, see Section 3.1.5, “Managing a File Transfer Session,” on page 78

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

Remote Wake Up

Remote Wake Up lets you remotely wake up a single node or a group of powered-down nodes in your network provided the network card on the node is enabled for Wake-on-LAN. For more information, see Section 3.6, “Waking Up a Remote Device,” on page 92

1.2.2 Remote Operations on a Linux Device



The following sections help you to understand the various Remote Management operations that can be performed on a Linux managed device:

- “Remote Control” on page 14
- “Remote View” on page 14
- “Remote Login” on page 14
- “Remote SSH” on page 14
- “Remote Wake Up” on page 14

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 3.2.1, "Managing a Remote Control Session," on page 82.

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 3.2.2, "Managing a Remote View Session," on page 84.

Remote Login

Remote Login lets you log in to a managed device from the management console and start a new graphical session without disturbing the user on the managed device; however, the user on the managed device cannot view the Remote Login session.You must log into the device with a non-`root` user credentials. This operation is supported only on a Linux managed device. For more information, see Section 3.2.3, "Managing a Remote Login Session," on page 85.

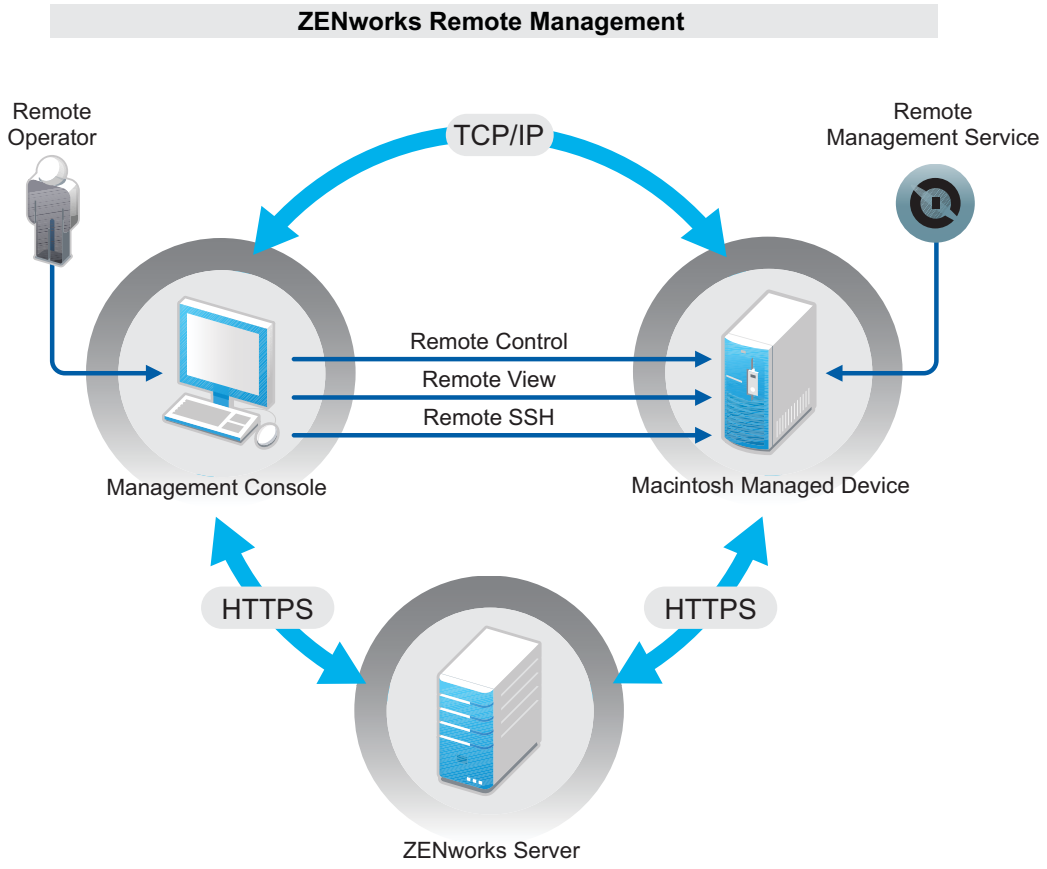
Remote SSH

Remote SSH lets you securely connect to a remote Macintosh device and safely execute commands on the device. To launch a Remote SSH session from a Management Console device, JRE version 8 or higher must be installed on the device. For more information on launching a Remote SSH session on a managed device, see Section 2.6, "Launching a Remote SSH Session on a Linux Device," on page 69.

Remote Wake Up

Remote Wake Up lets you remotely wake up a single node or a group of powered-down nodes in your network provided the network card on the node is enabled for Wake-on-LAN. For more information, see Section 3.6, "Waking Up a Remote Device," on page 92

1.2.3 Remote Operations on a Macintosh Device



The following sections help you to understand the various Remote Management operations that can be performed on a Macintosh managed device:

- "Remote Control" on page 15
- "Remote View" on page 15
- "Remote SSH" on page 16

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 3.3.1, "Managing a Remote Control Session on a Macintosh Device," on page 88.

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 3.3.2, "Managing a Remote View Session on a Macintosh Device," on page 89.

Remote SSH

Remote SSH lets you securely connect to a remote Macintosh device and safely execute commands on the device. To launch a Remote SSH session from a Management Console device, JRE version 8 or higher must be installed on the device. For more information on launching a Remote SSH session on a Macintosh device, see Section 3.3.3, “Managing a Remote SSH Session on a Macintosh Device,” on page 90.

1.3 Understanding Remote Management Features on a Windows Device

The following sections helps you to understand the various Remote Management features on a Windows managed device:

- Section 1.3.1, “Visible Signal,” on page 16
- Section 1.3.2, “Intruder Detection,” on page 16
- Section 1.3.3, “Session Encryption,” on page 17
- Section 1.3.4, “Audible Beep,” on page 17
- Section 1.3.5, “Keyboard and Mouse Locking,” on page 17
- Section 1.3.6, “Screen Blanking,” on page 17
- Section 1.3.7, “Abnormal Termination,” on page 17
- Section 1.3.8, “Overriding Screen Saver,” on page 17
- Section 1.3.9, “Automatic Session Termination,” on page 18
- Section 1.3.10, “Agent Initiated Connection,” on page 18
- Section 1.3.11, “Session Collaboration,” on page 18
- Section 1.3.12, “Remote Management Auditing,” on page 18
- Section 1.3.13, “Switch Display,” on page 18

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 (TLSv1.2 protocol). This feature is available on a Windows device only.

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. This feature is available on a Windows device only.

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.

You can disable the **Lock/Unlock keyboard and mouse** feature on managed devices with different hardware such as Windows surface Pro and Tablet PC where these features do not work or cause other side-effects. For details see "The Lock/Unlock keyboard and mouse option causes problems on some remotely managed Windows devices" on page 126.

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 blanking managed device during a remote session degrades the session performance.

Remote Management Blank Screen operation is not available on Windows 8.1 and above operating systems. You can disable the **Blank/Unblank Screen** feature on managed devices with different hardware such as Windows surface Pro and Tablet PC where these features do not work or cause other side-effects. For details see "The Blank/Unblank Screen option causes problems on some remotely managed Windows devices" on page 126.

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. This feature is available on a Windows device only.

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 available on a Windows device only.

NOTE: This feature is not available on a Windows Server 2008, Windows 7, and Windows 8 managed devices.

1.3.9 Automatic Session Termination

Automatically terminates a remote session if it has been inactive for a specified duration. This feature is available on a Windows device only.

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 "Initiating a Session from the Managed Device" on page 44.

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 "Session Collaboration" on page 74.This feature is available on a Windows device only.

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. This feature is available on a Windows device only.

1.3.13 Switch Display

The Switch Display feature enables you to switch between multiple monitors of a managed device. Click the **Switch Display** button to either view one or all the available monitors on the managed device.

NOTE: In a collaboration session, other remote operators can get access to switch display only when the master remote operator delegates the control.

In a shared session, each remote operator has access to the switch display.

1.4 Understanding Remote Management Proxy

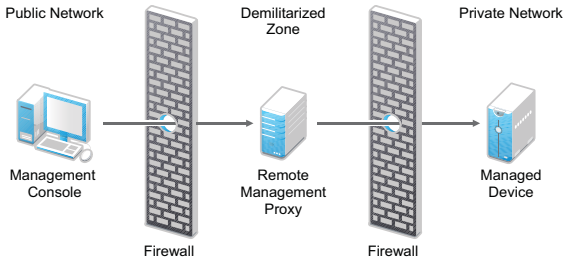
You cannot perform any remote management operation on a managed device that is on a private network or is on the other side of a firewall or router that is using NAT (Network Address Translation). This is because the NAT firewall hides the device IP address from the external network and thereby blocks 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 on a Windows device from the device context, see Route Through Proxy in "Initiating a Remote Management Session from the Device Context" on page 36.

For more information on routing the remote operation through proxy when initiating a remote session on a Windows device from the user context, see Route Through Proxy in "Initiating a Remote Management Session from the User Context" on page 39.

For more information on routing the remote operation through proxy when initiating a remote session on a Linux device, see Route Through Proxy in "Starting Remote Management Operations on a Linux Device" on page 49.

Figure 1-1 *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 2.5.1, "Installing a Remote Management Proxy," on page 66.

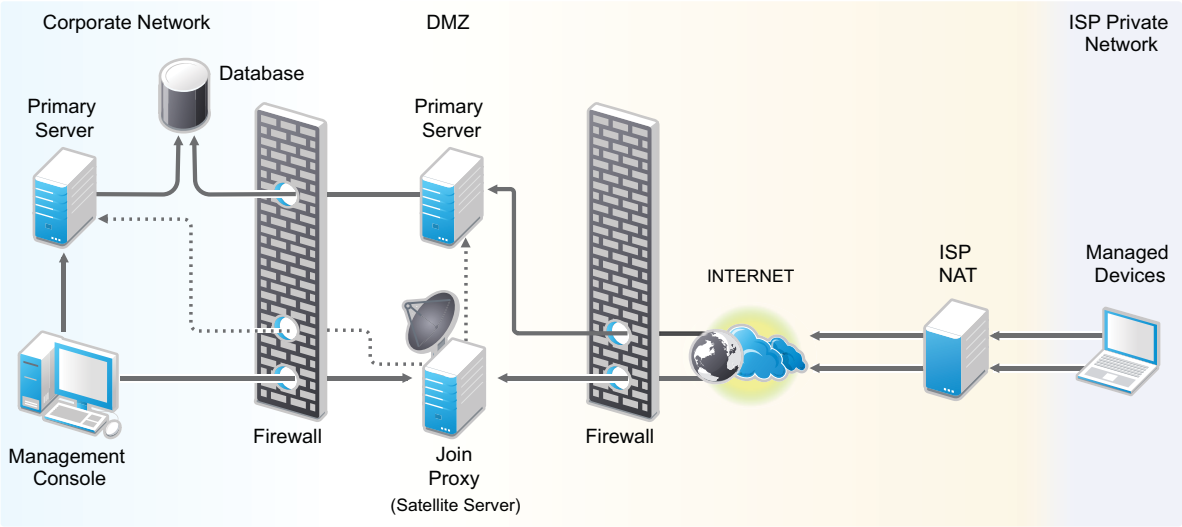
The remote management proxy listens on port 5750 by default for the incoming remote management requests from the Remote Management Viewer, and forwards the requests to the device.

1.5 Understanding Remote Management Join Proxy

Join Proxy is a Primary Server or a Satellite with the Join Proxy role that acts as a proxy by accepting and maintaining connections from Windows managed devices that are in a private network.

NOTE: For an agent initiated connection, remote management through Join Proxy is not supported.

Figure 1-2 *Remote Management Join Proxy - Satellite Server with Join Proxy role*



Join Proxy satellite server allows multiple Windows devices that are in a private network on the other side of a firewall or router that is behind NAT (Network Address Translation) to connect to it for remote management operations. Fore details, see "Join Proxy Role"in *ZENworks Primary Server and Satellite Reference*.

Join Proxy when used for remote management operations joins two connections together. The first connection being the one that the managed device maintains with the proxy server while the second one is the connection that comes from the viewer machine of the administrator.

2 Setting Up Remote Management

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

- Section 2.1, “Setting Up Remote Management to Manage a Windows Device,” on page 21
- Section 2.2, “Setting Up Remote Management to Manage a Linux Device,” on page 45
- Section 2.3, “Setting Up Remote Management to Manage a Macintosh Device,” on page 55
- Section 2.4, “Configuring and Launching Remote Management,” on page 57
- Section 2.5, “Configuring Remote Management Proxy,” on page 66
- Section 2.6, “Launching a Remote SSH Session on a Linux Device,” on page 69
- Section 2.7, “Requesting a Remote Management Session in the Absence of the Z-icon,” on page 70

2.1 Setting Up Remote Management to Manage a Windows Device

- Section 2.1.1, “Configuring the Remote Management Settings on a Windows Device,” on page 21
- Section 2.1.2, “Creating the Remote Management Policy,” on page 26
- Section 2.1.3, “Configuring the Remote Operator Rights,” on page 32
- Section 2.1.4, “Configuring the Remote Management Agent Password on a Windows Managed Device,” on page 33
- Section 2.1.5, “Starting Remote Management Operations on a Windows Device,” on page 35
- Section 2.1.6, “Enabling the Remote Management Listener,” on page 45

2.1.1 Configuring the Remote Management Settings on a Windows Device

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:

- “Configuring the Remote Management Settings at the Zone Level of a Windows Device” on page 22
- “Configuring the Remote Management Settings at the Folder Level of a Windows Device” on page 24

- "Configuring the Remote Management Settings at the Windows Device Level" on page 25
- "Exporting Remote Management Viewer settings to Managed Devices" on page 25

Configuring the Remote Management Settings at the Zone Level of a Windows Device

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. By default, this setting is enabled.

Field	Details
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. By default, this setting is enabled. **NOTE:** Remote Management Optimization Driver is not supported on Windows 10 and later versions.

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 2.5.1, "Installing a Remote Management Proxy," on page 66.

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.

Configuring the Remote Management Settings at the Folder Level of a Windows Device

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.

Configuring the Remote Management Settings at the Windows 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.

Exporting Remote Management Viewer settings to Managed Devices

While remote controlling a device, you might have changed few settings in the ZENworks Remote Management Viewer Options window and you might want to apply the same changes to other managed devices in the zone. To export remote management viewer settings, perform the following:

1. Remote control any device, and make necessary changes in the **ZENworks Remote Management Viewer Connection Options** window,
2. Click **Ok** to save and exit the remote control session.
3. Open the Registry Editor.
   - In the Start Menu, either in the Run box or in the Search box, type regedit, and then press Enter.
4. In the Registry Editor window, navigate to **HKEY_CURRENT_USER** > **Software** > **Novell** > **ZCM** > **Remote Management** > **Viewer** > **History**
5. Rename the existing device history settings registry key to Default, or create a registry key with custom settings.

   NOTE: Any run time changes will not be saved to the default registry key, instead it will be saved to the device specific registry key.

   ---
6. Export the registry key by clicking **File** menu, and then click **Export**.
7. Import the registry key to all the managed devices.

   To import registry key, you can either do it manually or create a bundle and then publish it on all the required managed devices.

Default registry key can be used for all standard settings that administrator wants to make common across the devices in the zone.

2.1.2 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 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.

Field	Details
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.

Field	Details
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.
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.

Field	Details
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.

Field	Details
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 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 (TLSv1.2 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.
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.

2.1.3 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.**

2.1.4 Configuring the Remote Management Agent Password on a Windows Managed Device

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

- "Setting Up the Remote Management Password Using ZENworks Control Center" on page 33
- "Setting Up the Remote Management Password Using ZENworks Agent" on page 34
- "Clearing the Remote Management Password Using ZENworks Control Center" on page 34
- "Clearing the Remote Management Password Using ZENworks Agent" on page 35

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 2.1.2, "Creating the Remote Management Policy," on page 26".

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.

Setting Up the Remote Management Password Using ZENworks 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 Agent** icon to display the ZENworks 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.**

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.

Clearing the Remote Management Password Using ZENworks Agent

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

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

2.1.5 Starting Remote Management Operations on a Windows Device

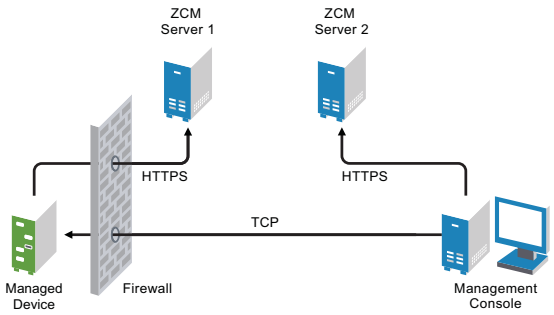
The remote operation can be initiated in the following ways:

- "Initiating a Session from the Management Console" on page 35
- "Initiating a Session from the Managed Device" on page 44

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 on a Windows Device*



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 36
- "Starting a Remote Management Operation in Standalone Mode" on page 42
- "Starting a Remote Management Operation by Using Command Line Options" on page 43

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:

Before initiating Remote Management session on Windows and Linux devices, you need to install ZCC Helper. For more information, see Section 2.4.1, "Installing ZCC Helper," on page 57

- "Initiating a Remote Management Session from the Device Context" on page 36
- "Initiating a Remote Management Session from the User Context" on page 39

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 the Remote Control, Remote View, or Remote Execute operations 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 (TLSv1.2 protocol).
Enable Logging	Logs session and debug information in the `novell-zenworks-vncviewer.txt` file. The system saves the file in the install location of the ZCC Helper.

Field	Details
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. **NOTE:** The Route Through Proxy option is not yet supported on Linux. 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.
Route Through Join Proxy	Enables the remote management operation of the managed device to be routed through a Join Proxy server. 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 Join Proxy server. If the managed device you are trying to remotely control is already connected to the Join Proxy, then the Route Through Join Proxy option is selected by default and the values for the Join Proxy and Join Proxy Port options are populated. **Join Proxy:** If the managed device you are trying to remote control is already connected to the Join Proxy, the DNS name or the IP address of that Join Proxy server is displayed **Join Proxy Port:** If the managed device you are trying to remote control is already connected to the Join Proxy, the port number on which the Join Proxy server is listening is displayed. When you try to remote control a managed device using Join Proxy, sometimes the configured server might not be available for Join Proxy to update the connection details in the database. In such a context, Join Proxy does not reject the connection of the managed device, but logs a message and allows you to remote control the managed device by manually entering the Join Proxy details in ZENworks Control Center. **NOTE:** If the Join Proxy IP and Port details are not available in the database for a private network device that is connected to a Join Proxy, you can manually check the **Route Through Join Proxy** option and specify the **Join Proxy IP** and **Join Proxy Port** values. On the other hand if you are trying to launch remote operation without selecting a device and have manually entered an IP address /DNS name, then you need to enter the address and port of the Join Proxy.

Field	Details
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. If the certificate contains **Enhanced Key Usage** section, then the section must contain Client Authentication (1.3.6.1.5.5.7.3.2) **NOTE:** Microsoft Certificate Services provides a number of certificate templates for issuing a certificate. Some of the certificate templates, such as Web Server, might not have the OID specified by default. If such a certificate is provided during the launch of a remote session, the SSL handshake fails. Consequently, the remote session also fails. So, if you are using Microsoft Certificate Services for issuing a certificate, ensure that the certificate template specifies Client Authentication (1.3.6.1.5.5.7.3.2) in the **Enhanced Key Usage** section. 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.

NOTE

- The **Enable Caching** and **Dynamic Bandwidth Optimization** options are available only for a ZENworks 11 SP3 managed device that is remotely managed from a ZENworks 2017 server.
- If you do not want to specify the private key and certificate, then 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, it is not recommended to use this option because it will impact the security of the device.

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 they have 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 the Remote Control, Remote View, or Remote Execute operations 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.

Field	Details
Session Encryption	Ensures that the remote session is secured by using SSL encryption (TLSv1.2 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.
Enable Logging	Logs session and debug information in the `novell-zenworks-vncviewer.txt` file. The system saves the file in the install location of the ZCC Helper.
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. **NOTE:** The Route Through Proxy option is not yet supported on Linux. 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.

Field	Details
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. If the certificate contains **Enhanced Key Usage** section, then the section must contain Client Authentication (1.3.6.1.5.5.7.3.2) **NOTE:** Microsoft Certificate Services provides a number of certificate templates for issuing a certificate. Some of the certificate templates, such as Web Server, might not have the OID specified by default. If such a certificate is provided during the launch of a remote session, the SSL handshake fails. Consequently, the remote session also fails. So, if you are using Microsoft Certificate Services for issuing a certificate, ensure that the certificate template specifies Client Authentication (1.3.6.1.5.5.7.3.2) in the **Enhanced Key Usage** section. 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.

NOTE: If you do not want to specify the private key and certificate, then 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, it is not recommended to use this option because it will impact the security of the device.

Starting a Remote Management Operation in Standalone Mode

Before starting the remote management operation in standalone mode, install ZCC Helper. For information on installing the ZCC Helper, see Section 2.4.1, “Installing ZCC Helper,” on page 57.

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 ZCC Helper. For information on installing ZCC Helper, see Section 2.4.1, "Installing ZCC Helper," on page 57.

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 "Command Line Options for Launching a Remote Operation" on page 59.

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.

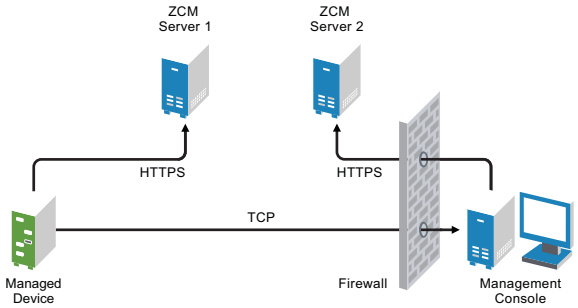
  NOTE: When you launch a remote session from ZENworks Control Center (ZCC), the certificate is automatically generated by ZCC and passed to the viewer to launch the session. The certificate is valid for only four days.

- 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.
- You cannot use a standalone `nzrViewer.exe` with rights-based authentication to remotely control the managed device. To use the standalone `nzrViewer.exe` for remote management operations, apply a Remote Management policy with password authentication enabled on the managed device.

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. Right click the ZENworks system tray icon, and select **Technician Application**. ZENworks Agent windows is displayed.
2. In the left pane of the agent, 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).

2.1.6 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.

2.2 Setting Up Remote Management to Manage a Linux Device

- Section 2.2.1, “Configuring the Remote Management Settings on a Linux Device,” on page 45
- Section 2.2.2, “Configuring the Remote Management Agent Password on a Linux Managed Device,” on page 49
- Section 2.2.3, “Starting Remote Management Operations on a Linux Device,” on page 49
- Section 2.2.4, “Preparing a Linux Device for a Remote Control Session,” on page 51
- Section 2.2.5, “Preparing a Linux Device for a Remote Login Session,” on page 52

NOTE: Remote management is not supported on Linux Devices at runlevel 3 (text-only, no X server).

2.2.1 Configuring the Remote Management Settings on a Linux Device

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.

NOTE: On Linux devices, only password based authentication is enabled for remote management and the rights based authentication is disabled by default. It is recommended to set a password for the Linux device to secure it from unauthorized access.

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

- "Configuring the Remote Management Settings at the Zone Level of a Linux Device" on page 46
- "Configuring the Remote Management Settings at the Folder Level of a Linux Device" on page 48
- "Configuring the Remote Management Settings at the Linux Device Level" on page 48

Configuring the Remote Management Settings at the Zone Level of a Linux Device

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. Click the **Linux Settings** tab.
4. 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.
5. Select one of the following options:
   - **Allow Full Control:** Enables the administrator to remotely control and also remotely view the managed device.
   - **Allow View Only:** Enables the user to remotely view the managed device.
6. Select the **Ask for permission from user on the managed device** option to request the permission from the user on the managed device before starting a Remote Control or Remote View session on the device.
7. Select the option to enable the Remote Login service. By default, the Remote Login service listens on port number 5951. You can choose to specify a different port number.
8. To configure the password policy for handling the remote sessions on the device, select one of the following:
   - **Use the Same Password Across Sessions:** This is the default option of the password policy and enables the administrator to use the same password across all the remote sessions on the device. For information on setting the password on the managed device, see "Setting Up the Remote Management Agent Password on the Managed Device" on page 49.
   - **Clear the password After Every Session:** If this option is selected, the user must set the password for every session and communicate the password to the remote operator through out-of-band means such as telephone. The password is cleared after every successful or unsuccessful attempt for a Remote Management operation. For information on setting the password on the managed device, see "Setting Up the Remote Management Agent Password on the Managed Device" on page 49

- **No Password:** If this option is selected, then Remote Control, Remote Login, and Remote View sessions are launched without asking for a password.

  This option is not recommended because it allows access to the managed device without any password.

9 (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 2.5.1, "Installing a Remote Management Proxy," on page 66.

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**.

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

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

Configuring the Remote Management Settings at the Folder Level of a Linux Device

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.

Configuring the Remote Management Settings at the Linux 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.

2.2.2 Configuring the Remote Management Agent Password on a Linux Managed Device

If the password policy for performing remote session on a Linux managed is configured to use a password to remotely connect to the device, the user on the managed device must set a Remote Management Agent password and communicate the password to the remote operator. For more information on setting the password policy for Remote Management sessions, see "Configuring the Remote Management Settings at the Zone Level of a Linux Device" on page 46.

- "Setting Up the Remote Management Agent Password on the Managed Device" on page 49
- "Clearing the Remote Management Agent Password" on page 49

Setting Up the Remote Management Agent Password on the Managed Device

The user on the managed device must create a Remote Management Agent password on the device and communicate the password to a remote operator in order to enable the remote operator to remotely manage the device.

To set the Agent password on the managed device, enter the following command at the shell prompt:

```
# /opt/novell/zenworks/sbin/zrmservice --passwd
```

The password is case-sensitive and should be between three to eight characters in length.

NOTE: You need not set the password on the device if the Password Policy is configured to **No password**.

Clearing the Remote Management Agent Password

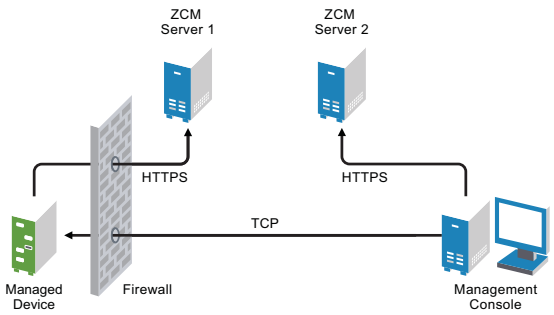
To clear the Agent password on the managed device, enter the following command at the shell prompt:

```
# /opt/novell/zenworks/sbin/zrmservice --clrpasswd
```

2.2.3 Starting Remote Management Operations on a Linux Device

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 2-3 Console-Initiated Session on a Linux Device



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.

To initiate a Remote Management session on a Linux 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 **Remote Control**.
3. In the Remote Management dialog box, select **Remote Control**, **Remote View**, or **Remote Login**.
4. 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.
Authentication	The Password-Based Authentication is the only mode of authentication.
Port	Specify the port number on which the Remote Management service is listening. By default, the port number is 5950
Enable Logging	Logs session and debug information in the `novell-zenworks-vncviewer.txt` file. The system saves the file in the install location of the ZCC Helper.
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. **NOTE:** The Route Through Proxy option is not yet supported on Linux. 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.

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

NOTE: The **Auto** mode might not work properly for SLES10 64-bit devices. You can select a scale of 25 to 150% from the remote viewer **Display** option.

2.2.4 Preparing a Linux Device for a Remote Control Session

If you want to remote control a Linux device, perform the steps mentioned based on the Linux version installed on the device.

Preparing a open-SUSE LEAP 15 Device

Gnome Display Manager

Before remote controlling a open-SUSE LEAP 15 device, ensure that the you perform the following steps:

1. Edit the `custom.conf` file located in the `etc/gdm/`, uncomment `WaylandEnable=false`.
2. Run the following command to restart Gnome Display Manager (GDM):

   ```
   Systemctl restart DisplayManager.service
   ```

2.2.5 Preparing a Linux Device for a Remote Login Session

If you choose to remotely login to a Linux device, a grey screen might appear if some settings are not configured on the device. To enable a Remote Login session to be successfully launched on a Linux managed device, you must enable the XDMCP configuration on the device and disable the firewall For more information on preparing a Linux device for a Remote Login session, review the following sections:

NOTE: Remote login is supported only on devices running Gnome Display Manager.

- "Preparing a SLES 10 / SLED 10 Device" on page 52
- "Preparing a SLES 11 / SLED 11 Device" on page 53
- "Preparing a SLES 12 / SLED 12 Device" on page 53
- "Preparing a SLES 15 Device" on page 53
- "Preparing an open-SUSE LEAP 15 Device" on page 53
- "Preparing an open-SUSE LEAP 42.3 Device" on page 54
- "Preparing a RHEL 6 Device" on page 54
- "Preparing a RHEL 7 Device" on page 54

Preparing a SLES 10 / SLED 10 Device

Gnome Display Manager

1. Run the following command to enable the Gnome Display Manager (GDM):

   ```
   sh /opt/novell/zenworks/sbin/novell-rm-fixrl.sh -dm gdm -cf /etc/opt/
   gnome/gdm/gdm.conf enable
   ```
2. Run the following command to restart the Display Manager.

   ```
   /etc/init.d/xdm restart
   ```

KDE Display Manager

1. Edit the `/etc/X11/xdm/Xaccess` file to uncomment the following line:

   ```
   *   # only local host can get a login window
   ```
2. Edit the `/opt/kde3/share/config/kdm/kdmrc` file to enable XDMCP to `true`.

3 Run the following command to restart the Display Manager.

```
/etc/init.d/xdm restart
```

Preparing a SLES 11 / SLED 11 Device

Gnome Display Manager

1 Run the following command to enable the Gnome Display Manager (GDM):

```
 sh /opt/novell/zenworks/sbin/novell-rm-fixrl.sh -dm gdm -cf /etc/dbus-1/system.d/gdm.conf enable
```

2 Run the following command to restart the Display Manager.

```
/etc/init.d/xdm restart
```

Preparing a SLES 12 / SLED 12 Device

Gnome Display Manager

1 Run the following command to enable the Gnome Display Manager (GDM):

```
sh /opt/novell/zenworks/sbin/novell-rm-fixrl.sh -dm gdm -r -cf /etc/dbus-1/system.d/gdm.conf enable
```

2 Run the following command to restart the Display Manager.

```
Systemctl restart display-manager.service
```

Preparing a SLES 15 Device

Gnome Display Manager

1 Run the following command to enable the Gnome Display Manager (GDM):

```
sh /opt/novell/zenworks/sbin/novell-rm-fixrl.sh -dm gdm -cf /etc/dbus-1/system.d/gdm.conf enable
```

2 Restart the device.

Preparing an open-SUSE LEAP 15 Device

Gnome Display Manager

1 Edit the `custom.conf` file located in the `etc/gdm/`, uncomment `WaylandEnable=false`.

2 Restart the device.

3 Run the following command to enable the Gnome Display Manager (GDM):

```
sh /opt/novell/zenworks/sbin/novell-rm-fixrl.sh -dm gdm -r -cf /etc/dbus-1/system.d/gdm.conf enable
```

Preparing an open-SUSE LEAP 42.3 Device

Gnome Display Manager

- Run the following command to enable the Gnome Display Manager (GDM):

  ```
  sh /opt/novell/zenworks/sbin/novell-rm-fixrl.sh -dm gdm -r -cf /etc/
  dbus-1/system.d/gdm.conf enable
  ```

Preparing a RHEL 6 Device

Gnome Display Manager

1. Run the following command to display a fonts directory:

   ```
   mkdir -p /usr/X11R6/lib/
   ```

2. Run the following command to link the `/usr/share/X11` directory to the newly created fonts directory:

   ```
   ln -s /usr/share/X11/ /usr/X11R6/lib/X11
   ```

3. Edit the file `/etc/gdm/custom.conf` and add the following entry:

   ```
   [xdmcp]
   Enable=true
   ```

4. Run the following command to restart the Display Manager:

   ```
   init 3
   init 5
   ```

KDE Display Manager

1. Run the following command to create a fonts directory:

   ```
   mkdir -p /usr/X11R6/lib/
   ```

2. Run the following command to link the `/usr/share/X11` directory to the newly created fonts directory:

   ```
   ln -s /usr/share/X11/ /usr/X11R6/lib/X11
   ```

3. Enable the Remote X GUI Login on the device by using XDMCP and KDM configuration. For more information on how to enable the Remote X Login, see Red Hat documentation.
4. Run the following commands as root to restart the X Server:

   ```
   init 3
   init 5
   ```

Preparing a RHEL 7 Device

Gnome Display Manager

1. Run the following command to display a fonts directory:

   ```
   mkdir -p /usr/X11R6/lib/
   ```

2 Run the following command to link the `/usr/share/X11` directory to the newly created fonts directory:

```
ln -s /usr/share/X11/ /usr/X11R6/lib/X11
```

3 Edit the file `/etc/gdm/custom.conf` and add the following entry:

```
[xdmcp]
Enable=true
```

4 Run the following command to restart the Display Manager:

```
init 3
init 5
```

2.3 Setting Up Remote Management to Manage a Macintosh Device

You can remotely connect and control your Macintosh managed device over a network or over the Internet.The Virtual Network Computing server is built into the Mac OS X managed device (10.5 or later). A VNC server allows you to control your Macintosh managed device from another computer.

- Section 2.3.1, "Enabling Remote Management on a Macintosh Device," on page 55
- Section 2.3.2, "Starting Remote Management Operations on a Macintosh Device," on page 56

2.3.1 Enabling Remote Management on a Macintosh Device

1 Open **System Preferences**.

2 Select **Sharing Preferences**.

3 Select the **Remote Management** check box if you are using the Apple Remote Desktop (ARD), else select **Screen Sharing**.

4 Click **Computer Settings.**

5 Select the **VNC Viewers may control screen with password** check box, then set the password. You need this password to connect from the remote computer.

6 Click **OK** to save your settings.

NOTE: You might not be able to connect to the active user session through a remote control session on a Mac OS X 10.7 managed device. For more information, see "Unable to connect to the active user session when you launch a remote control session on a Mac OS X Lion 10.7 managed device" on page 133.

2.3.2 Starting Remote Management Operations on a Macintosh Device

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 inside or outside the enterprise network.

To initiate a Remote Management session on a Macintosh device:

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

   or

   In **Device Tasks** in the left pane, select **Remote Control**.
4. In the Remote Management dialog box, select **Remote Control > Remote View**.
5. Choose the relevant options in the dialog box.The following are the various options available:

   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.

   Authentication: Select the type of the remote operation you want to perform on the managed device.

   Port: Specify the port number on which the Remote Management service is listening. By default, the port number is 5900.

   Enable Logging: Logs session and debug information in the `novell-zenworks-vncviewer.txt` file. The system saves the file in the install location of the ZCC Helper.

   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.

   Indicate your preferences 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.

   ---

6. Click **OK**.

2.4 Configuring and Launching Remote Management

- Section 2.4.1, “Installing ZCC Helper,” on page 57
- Section 2.4.2, “Installing ZCC Helper in a Terminal Server or in a Citrix XENapp Environment,” on page 57
- Section 2.4.3, “Options for Launching a Remote Management Operation,” on page 59
- Section 2.4.4, “ZENworks Remote Management Viewer Options,” on page 63

2.4.1 Installing ZCC Helper

The ZCC Helper enables a remote operator to perform remote operations on the managed device from a Windows or a Linux device.

For more information on installing ZCC Helper, see Installing ZCC Helper in the ZENworks Software Distribution Reference.

Pre-requisites for Remote Management on Linux devices

The following RPM packages should be installed after installing the ZCC Helper:

You need to install the following 64-bit packages. The packages can be installed using the OS installation CD:

- `libXaw8`
- `libgnomeui`
- `libjpeg62`

After installing the RPM packages, you might need to manually create the below symbolic links:

- `libXaw8.so.8` for `libXaw8.so.8.0.0`
- `libjpeg.so.62` for `libjpeg.so.62.0.0`
- `libXmu.so.6` for `libXmu.so.6.2.0`
- `libXt.so.6` for `libXt.so.6.0.0`
- `libXpm.so.4` for `libXmu.so.6.2.0`
- `libXp.so.6` for `libXp.so.6.2.0`
- `libxcb-xlib.so.0` for `libxcb-xlib.so.0.0.0`

2.4.2 Installing ZCC Helper in a Terminal Server or in a Citrix XENapp Environment

You can copy ZCC Helper in a common location for all users in a Terminal Server or in a Citrix XENapp environment.

1. Log in to ZENworks Control Center.
2. Click **Configuration.**
3. In the left navigation pane, click **Download ZENworks Tools**.

4 Click **Administrative Tools** in the left navigation pane of the ZENworks Download page.

5 In the **Configuration** tab, click **novell-zenworks-zcc-helper-<version>.msi** to download the ZCC Helper.

6 Install ZCC Helper.

7 Manually copy ZCC Helper, Remote Management and GroupPolicy folders from `%appdata%\Novell\ZENworks` to a common location, which is accessible to all users.

   Ensure that you provide full-access to the ZENworks folder for the domain users.

8 Manually create the following registry entries:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\zcclaunch]
@="URL:zcclaunch Protocol"
"URL Protocol"=""

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\zcclaunch\shell]

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\zcclaunch\shell\open]

  [HKEY_LOCAL_MACHINE\SOFTWARE\Classes\zcclaunch\shell\open\command]
"version"="17.0.0.297" (actual version of the zcchelper.exe)
@="C:\Novell\ZENworks\ZCCHelper\bin\zcchelper.exe" "%1"

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Novell\ZCM\GroupPolicy\Helper
]
"Path"="C:\Novell\ZENworks\Policies\bin\GPTool.exe"
"version"="17.0.0.297"
```

NOTE: Where `17.0.0.297` is the actual version of `GPTool.exe`.

On 32-bit Devices:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Novell\ZCM\Remote Management\Viewer]
"Path"="C:\Novell\ZENworks\Remote Management\bin\nzrViewer.exe"
"version"="17.0.0.297"
```

On 64-bit Devices:

```
[HKEY_LOCAL_MACHINE\Software\Wow6432Node\Novell\ZCM\Remote
Management\Viewer]
"Path"="C:\Novell\ZENworks\Remote Management\bin\nzrViewer.exe"
"version"="17.0.0.297"
```

NOTE: Where `17.0.0.297` is the actual version of `nzrViewer.exe`.

If an earlier version of ZCC Helper is installed on the device, then a pop-up is displayed to download the latest ZCC Helper.

2.4.3 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 "Internal Options for Launching a Remote Operation" on page 63.

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

- "Command Line Options for Launching a Remote Operation" on page 59
- "Internal Options for Launching a Remote Operation" on page 63

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.
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.

Command Line Option	Parameter	Description
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.
skipauth31		Launches Remote operation on a Mac device. This option skips Novell authentication that is unavailable on a Mac device.
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
noemulate3		Does not emulate a three-button mouse.

Command Line Option	Parameter	Description
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.

Command Line Option	Parameter	Description
cert	*filename*	Name of the file where the certificate corresponding to the private key is stored. If the certificate contains **Enhanced Key Usage** section, then the section must contain Client Authentication (1.3.6.1.5.5.7.3.2) **NOTE:** Microsoft Certificate Services provides a number of certificate templates for issuing a certificate. Some of the certificate templates, such as Web Server, might not have the OID specified by default. If such a certificate is provided during the launch of a remote session, the SSL handshake fails. Consequently, the remote session also fails. So, if you are using Microsoft Certificate Services for issuing a certificate, ensure that the certificate template specifies Client Authentication (1.3.6.1.5.5.7.3.2) in the **Enhanced Key Usage** section. **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.
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).

Command Line Option	Parameter	Description
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.

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.

2.4.4 ZENworks Remote Management Viewer Options

You can use the various options available in the Remote Management Viewer Options dialog box to edit either connection-specific options or global settings:

- "Connection Tab" on page 63
- "Globals Tab" on page 64
- "Performance Tab" on page 65

Connection Tab

The following options are available in the **Connection** tab:

Display: Use the options under **Display to** specify the client-side display settings:

- Use the **Scale - by** option to reduce or enlarge the local copy of the remote desktop.
- Select **Full-screen mode** if you want the Viewer to show only the remote desktop and not the local desktop, toolbar, and window decorations.

Restrictions: Use the options under **Restrictions** to disable certain protocol features:

- Select **View only (input ignored)** to view the remote desktop but not control it remotely with your mouse and keyboard.

- Select **Disable clipboard transfer**, if you do not want the Viewer to propagate local clipboard changes to the server and vice-versa.
- Select **Block mouse move events** to avoid sending information about local mouse movements to the managed device. This can improve session performance.

Mouse: Use the **Mouse** options to specify the following mouse configuration details:

- Select **Emulate 3 buttons [with 2-button click]**, if you have two- button mouse but you want to emulate using the third button. If this option is enabled, pressing the left and right buttons at the same time is equivalent to pressing the middle button.
- Select **Swap mouse buttons 2 and 3** to swap the events generated by the second and third mouse buttons.The right mouse button usually generates button 2 events, and the middle mouse button is usually treated as button 3.

Globals Tab

The following options are available in the **Globals** tab:

Interface Options: Under **Interface Options**, specify how the Remote Management Viewer interface is displayed:

- Select **Show toolbars by default** to show toolbars in desktop windows.
- Select **Warn before switching to full-screen mode**, if you want the Remote Management Viewer to display a warning before switching to the full-screen mode. The warning tells users how to exit full-screen mode.
- Use th**e Connections to remember** field to specify the number of connections for the Viewer to remember.
- Click **Clear all** to remove the list of past connections from the system registry. This also removes all corresponding connection settings.

Local cursor shape: The local mouse cursor and the remote pointer might have different locations on the screen. You can choose one of the following options to customize the shape of the local cursor for improved cursor tracking:

- Select **Dot cursor** to show the local cursor position as a dot.
- Select **Small dot cursor** to show the local cursor position as a smaller dot.
- Select **Normal arrow** to show the local cursor position as an arrow cursor.
- Select **No local cursor** if you do not want to show the local cursor position.

Listening Mode: Use this option for settings specific to the listening mode that is used for reverse server-to-client connections.

Use the **Accept reverse VNC connections on TCP port** list to indicate the port number.The default port number is 5500.

Logging: Use the following logging options to customize how the Viewer logs it's activity in a text file:

- Select **Write log to a file** to enable logging.
- Select **Browse** to choose a location for the log file.

- Use the **Verbosity level** list to specify how many details to write into the log file.

  The Level 0 causes the Viewer to log only the most important events. Level 12 produces the maximum debugging output.

Performance Tab

The following options are available in the **Performance** Tab:

Format and encodings: You can specify the following **Format and Encodings** options:

- Select the appropriate graphics encoding from the **Use encoding** list.

  Encoding refers to how graphics are sent over the network. Encodings can differ depending on bandwidth and CPU usage. Use Hextile encoding on fast networks, and use Tight encoding over slow connections. Raw encoding means no compression at all.
- Select **Use 8-bit color** to minimize the amount of pixel data sent over the network.
- Select **Allow CopyRect encoding** if you want to save bandwidth when a screen area on the server changes its position.

  CopyRect sends coordinates instead of pixel arrays. You should usually select this option.
- Select **Enable caching** to cache remote desktop screen data on the local device. This improves session performance because repetitive screen information is not resent. The Viewer uses disk space on the local device to save screen information.
- Select **Update screen incrementally** to control how information is displayed when the screen is refreshed.

  When the remote desktop is rendered locally at the start of the session or when a full screen refresh is requested, this setting determines whether the screen is shown gradually or all at once.This setting is especially useful on slow links as an indication that the connection is alive.

Compression: The following options are asvailable under **Compression:**

- Select **Custom compression level** to specify a particular compression level instead of using server's default.

  The compression level ranges from level 1(Fast) to 9 (best). Higher compression levels result in greater compression ratios, but require more time to encode data. Use lower values on fast networks, and higher levels for slow connections.

  NOTE: The **Custom Compression level** is available only for Tight, Zlib, and ZlibHex encoding.

- Select **Allow JPEG compression** if you want the JPEG scheme to allow more compression for Tight encoding of full-color data. However the image quality might degrade in particular screen areas.

  The JPEG compression level ranges from poor to best. Higher JPEG quality levels result in less compression but better image quality. The Tight encoder usually tries to use JPEG only where it does not cause major quality losses, so you can safely choose low quality levels.

- Select **Enable** if you want the Viewer to enable dynamic bandwidth detection and optimize the session parameters accordingly.

- Select **Automatic** to opt for pre configured settings for the bandwidth that is detected.
- Select **Manual** to manually select the settings to be used for different bandwidth spectrums.

NOTE: The **Enable Caching** and **Dynamic Bandwidth Optimization** options are available only for a ZENworks 11 SP3 managed device that is remotely managed from a ZENworks 2017 server.

Reset to Default: Click **Reset to Default** if you want to restore user-defined settings to the defaults.

Bandwidth: Use this setting to display bandwidth information.

Encoding: Select the encoding from the **Encoding** list.

Color Depth (in bpp): Select the pixel format from the **Color Depth (in bpp)** list.

2.5 Configuring Remote Management Proxy

Remote Management proxy 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 Linux device.

Review the following sections for information on installing and configuring the proxy:

- Section 2.5.1, “Installing a Remote Management Proxy,” on page 66
- Section 2.5.2, “Configuring a Remote Management Proxy,” on page 68

2.5.1 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 Network Address Translation (NAT), the remote management operation of the device can be routed through a Remote Management proxy. The proxy can be installed on a Windows or Linux managed device. By default, the remote management proxy listens on port 5750.

For more information on the Remote Management proxy, see Section 1.4, “Understanding Remote Management Proxy,” on page 19.

For information on the system requirements that a Windows or Linux managed device must meet to enable the proxy to be installed on the device, see “Managed Device Requirements” in “ZENworks 2017 Update 4 System Requirements.”

Review the following sections for information on installing the Remote Management proxy:

- “Installing the Remote Management Proxy on a Windows Device” on page 66
- “Installing the Remote Management Proxy on a Linux Device” on page 67
- “Installing the Remote Management Proxy on an Unmanaged Linux Device” on page 67

Installing the Remote Management Proxy on a Windows Device

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

https://*server*/zenworks-setup

Replace *server* with 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".
```

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 2.5.2, "Configuring a Remote Management Proxy," on page 68.

Installing the Remote Management Proxy on a Linux Device

1 On the device, open the following ZENworks download page on a Web browser:

https://*server*/zenworks-setup

Replace *server* with 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 superuser or `root` user:

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

The Remote Management proxy is designed to run automatically on 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 2.5.2, "Configuring a Remote Management Proxy," on page 68.

Installing the Remote Management Proxy on an Unmanaged Linux Device

1 Copy the following files from a ZENworks Linux device to the proxy device:

- `/etc/opt/novell/zenworks/security/ca.cert`

  `/etc/opt/novell/zenworks/security/rm.cert`

2 (Conditional) If the Remote Management proxy has already been installed on the device, run the following command to restart the proxy:

```
/etc/init.d/nzrepeaterd restart
```

or

Install the proxy on the device. For more information on installing the proxy on the device, see "Installing the Remote Management Proxy on a Linux Device" on page 67.

2.5.2 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.

- "Remote Management Proxy Settings on a Windows Managed Device" on page 68
- "Remote Management Proxy Settings on a Linux Device" on page 68

Remote Management Proxy Settings on a Windows Managed 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. This 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 the remote operator. You should mark this setting as True because setting it to False allows unauthenticated external processes other than the Remote Management Viewer to make connections to devices in 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.

Remote Management Proxy Settings on a Linux Device

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.

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 and 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 and 1. The default value is 1, which indicates that SSL authentication is enabled.

WARNING: Disabling SSL authentication is not recommended because it allows 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 and 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. As a result, the proxy fails to connect to the server.

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

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

2.6 Launching a Remote SSH Session on a Linux Device

To launch a Remote SSH session on a Linux device:

1. In ZENworks Control Center, click the **Devices** tab.
2. Click **Servers** or **Workstations** and select a Linux device.
3. Click **Action** > Remote SSH.
4. In the Remote SSH dialog box, specify the following:
   - **Device** Specify the name or IP address of the device you want to remotely connect to. If the device is not in the same network, you must specify the IP address of the device.
   - **User Name** Specify the username used to log in to in the remote device. By default, it is `root`.
   - **Port** Specify the port number of the Remote SSH service. By default, the port number is 22.
5. Click **OK** to launch Remote SSH Java Web Start Launcher.
6. Click **Yes** to accept the certificate, then click **Run**.
7. Enter the password to connect to the managed device.

NOTE: Before launching a Remote SSH session, ensure Java 8 or a higher Runtime Environment is installed on the device.

For information on managing the Remote SSH session, see Section 3.2.4, “Managing a Remote SSH session,” on page 86.

2.7 Requesting a Remote Management Session in the Absence of the Z-icon

In the absence of the Z-icon, you can use the `zac rrs` or `zac request-remote-session` command to request a remote management session from the managed device. For details, see *ZENworks Command Line Utilities Reference*. This command is available on managed devices with 11.3.1 and later versions.

Alternatively you can enable users to request a remote management session using a bundle. To launch a Remote Management session from a bundle, do the following:

1. In ZENworks Control Center, click the **Bundles** tab.
2. Click **New** > **Bundle**.
3. In the **New Bundle Type** panel, click **Windows Bundle**, and click **Next**.
4. In the **New Bundle Category** panel, click **Empty Bundle**, and click **Next**.
5. In the **Bundle Name** box, type the name of the bundle, click **Next**, then click **Finish**.
6. In the **Actions** tab, click **Add** > **Launch Executable**.
7. In the **Add Action - Launch Executable** window, type the following details:

   General tab:

   Command: `nzrSignaller`

   Command Line Parameters: `ZRMRequestSessionEvent`

   Working Directory: `%ZENworks_Home%\bin`

   Advanced tab:

   Select **Run as secure system user (Don't allow system to interact with desktop)**.
8. Assign the bundle to a device or a user.

3 Managing Remote Sessions

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

- Section 3.1, “Managing Remote Sessions on a Windows Device,” on page 71
- Section 3.2, “Managing Remote Sessions on a Linux Device,” on page 82
- Section 3.3, “Managing Remote Sessions on a Macintosh Device,” on page 87
- Section 3.4, “Performing Remote Control on a Macintosh device,” on page 91
- Section 3.5, “Managing a Remote Management Proxy Session,” on page 91
- Section 3.6, “Waking Up a Remote Device,” on page 92

3.1 Managing Remote Sessions on a Windows Device

Review the following sections for information on managing sessions on a Windows device:

- Section 3.1.1, “Managing a Remote Control Session,” on page 71
- Section 3.1.2, “Managing a Remote View Session,” on page 76
- Section 3.1.3, “Managing a Remote Execute Session,” on page 77
- Section 3.1.4, “Managing a Remote Diagnostics Session,” on page 77
- Section 3.1.5, “Managing a File Transfer Session,” on page 78
- Section 3.1.6, “Improving the Remote Management Performance on the Windows Managed Device,” on page 81

3.1.1 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 2.1.5, “Starting Remote Management Operations on a Windows Device,” on page 35.

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.

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.
Send Ctrl-Alt-Del		Sends the Ctrl+Alt+Del keystroke to the managed device. This option is disabled for Remote View and Remote Diagnostics sessions. The Ctrl+Alt+Del keystroke is delayed in a remote session when used for the first time after rebooting the managed device. However the subsequent Ctrl+Alt+Del keystroke takes less time until you reboot the managed device again.
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.

Option	Shortcut Key	Functionality
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 3.1.5, "Managing a File Transfer Session," on page 78.
Collaboration		Launches a ZENworks Remote Management Collaboration Session on the managed device, which lets you invite multiple remote operators to join the remote management session. You can also delegate the Remote Control rights to another remote operator to help you solve a problem. For more information on Session Collaboration, see "Session Collaboration" on page 74.
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.
Switch Display		Switches the display on a managed device with multiple monitors. This option is disabled for Remote Diagnostics session. For more information, see Section 1.3.13, "Switch Display," on page 18

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 2.1.5, "Starting Remote Management Operations on a Windows Device," on page 35.

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 2.1.2, "Creating the Remote Management Policy," on page 26"

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

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.

Task	Steps	Additional Details
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.
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, IPv4: 10.0.0.0 ~~1000 and IPv6: 2001:db8::1111~~5500 3. Click **Invite.**	

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

In a Remote Control session, if you want the device IP address to be displayed instead of the DNS name, check the `Always default to IP address for all devices` box.

The values that you provide to access a device while performing a Remote Control operation are saved in the system when you click `Ok`.

During a Remote Control operation, the following values are saved for an administrator and can be accessed during the next Remote Control operation:

- Always default to IP address for all devices
- Certificate Key Pair

During a Remote Control operation, the following values are saved for a device and can be accessed during the next Remote Control operation:

- Device name
- Authentication
- Session Encryption
- Enable logging
- Route Through Proxy

3.1.2 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 2.1.5, “Starting Remote Management Operations on a Windows Device,” on page 35.

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

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.
Switch Display		Switches the display on a managed device with multiple monitors. This option is disabled for Remote Diagnostics session. For more information, see Section 1.3.13, “Switch Display,” on page 18

3.1.3 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 2.1.5, "Starting Remote Management Operations on a Windows Device," on page 35.

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.

3.1.4 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.

NOTE: After installing ZENworks agent on a Windows XP device, reboot the device to perform remote diagnostics operation.

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

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 3.1.5, "Managing a File Transfer Session," on page 78
Disconnect	Alt+F4	Closes the remote session.

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.

The following table lists the 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 2.1.1, "Configuring the Remote Management Settings on a Windows Device," on page 21.

3.1.5 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 2.1.5, "Starting Remote Management Operations on a Windows Device," on page 35.

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.

NOTE: During a remote file transfer session when you upload or download a file, ensure that the file size does not exceed 2 GB. If the file size exceeds 2 GB, then the file will be copied but some of the file attributes will not be restored.

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.

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.	

Tasks	Shortcut Keys	Steps	Additional Details
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.
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.

Tasks	Shortcut Keys	Steps	Additional Details
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.
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.	

3.1.6 Improving the Remote Management Performance on the Windows Managed Device

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:

- "On the Management Console" on page 81
- "On the Managed Device" on page 82

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.

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 1 GHz or higher processor with 1 GB or higher RAM.
- Do not set a wallpaper pattern.

3.2 Managing Remote Sessions on a Linux Device

Review the following sections for information on managing sessions on a Linux device:

- Section 3.2.1, “Managing a Remote Control Session,” on page 82
- Section 3.2.2, “Managing a Remote View Session,” on page 84
- Section 3.2.3, “Managing a Remote Login Session,” on page 85
- Section 3.2.4, “Managing a Remote SSH session,” on page 86
- Section 3.2.5, “Improving the Remote Management Performance on the Linux Managed Device,” on page 87

3.2.1 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 2.2.3, “Starting Remote Management Operations on a Linux Device,” on page 49.

Using the Toolbar Options in the Remote Management Viewer on a Linux Device

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.

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. The Ctrl+Alt+Del keystroke is delayed in a remote session when used for the first time after rebooting the managed device. However the subsequent Ctrl+Alt+Del keystroke takes less time until you reboot the managed device again.
Send Ctrl-Esc		Invokes the Start menu on the managed device. This option will not work on a SLES 12 operating system.
Send Alt Key Press / Release		Clicking this option and pressing the ALT key on the keyboard sends the Alt keystroke to the managed device. This option will not work on a SLES 12 operating system.
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.
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.

Option	Shortcut Key	Functionality
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.

3.2.2 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 2.2.3, “Starting Remote Management Operations on a Linux Device,” on page 49.

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

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.

3.2.3 Managing a Remote Login Session

Remote Login lets you log in to a managed device from the management console and start a new graphical session without disturbing the user on the managed device; however, the user on the managed device cannot view the Remote Login session.You must log into the device with a non-`root` user credentials. For information on launching a Remote Login session, see Section 2.2.3, “Starting Remote Management Operations on a Linux Device,” on page 49.

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

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.
Send Ctrl-Alt-Del		Sends the Ctrl+Alt+Del keystroke to the managed device. This option is disabled for Remote View and Remote Diagnostics sessions. The Ctrl+Alt+Del keystroke is delayed in a remote session when used for the first time after rebooting the managed device. However the subsequent Ctrl+Alt+Del keystroke takes less time until you reboot the managed device again.
Send Ctrl-Esc		Invokes the Start menu on the managed device. This option is not supported.
Send Alt Key Press / Release		Clicking this option and pressing the ALT key on the keyboard sends the Alt keystroke to the managed device. This option is not supported.
Disconnect	Alt+F4	Closes the remote session.

3.2.4 Managing a Remote SSH session

Remote SSH lets you securely connect to a remote Linux device and safely execute commands on the remote device. For information on launching a Remote SSH session, see Section 2.6, "Launching a Remote SSH Session on a Linux Device," on page 69

On launching a Remote SSH on the device, a terminal opens up on the device, which you can use to safely execute commands on the remote device.

Click **Options** to use the following options when executing the commands on the device:

- "X11 Forwarding" on page 86
- "Local Port Forwarding" on page 86
- "Remote Port Forwarding" on page 86

X11 Forwarding

Allows you to run applications such as YaST by allowing the graphical information to be displayed on the device.

X11 forwarding is supported only if the Remote SSH session is launched from a Windows device. Ensure that an instance of XServer is running on the device on which you have launched the Remote SSH Java Web Start Launcher.

In the terminal, click **Options** > **X11**. Specify the XDisplayname in the following format:

`hostname:6000`

Local Port Forwarding

Local Port Forwarding allows you to establish a secure SSH session and then tunnel TCP connections through it. The information is sent over an encrypted connection.

In the terminal, click **Options** > **Local Port.** Specify the Local port forwarding in the following format:

`port:host:hostport`

The network connections to the client device on the local port are forwarded to the remote device on the specified port.

Remote Port Forwarding

Remote Port Forwarding allows you to establish a secure SSH session and then tunnel TCP connections through it. The information is sent over an encrypted connection.

In the terminal, click **Options** > **Remote Port.** Specify the Remote port forwarding in the following format:

`port:host:hostport`

The network connections to the SSH server on the remote port are forwarded to the local device on the specified port.

3.2.5 Improving the Remote Management Performance on the Linux Managed Device

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:

- "On the Management Console" on page 87
- "On the Managed Device" on page 87
- "More Performance Tuning Tips" on page 87

On the Management Console

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

- Select the **Use Encoding value as Tight** option.
- Set the **Use 8-bit Color and Allow CopyRect encoding** to level 6.
- Adjust the Custom Compression level and Allow JPEG compression depending on the quality of image required.

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 1 GHz or higher processor with 1 GB or higher RAM.
- Disable the wallpaper.
- Configure the following settings at the managed device:
  - Reduce the screen resolution.
  - Reduce the depth of color pixels.

More Performance Tuning Tips

For additional information on performance tuning tips, refer to the following Web sites for specific components:

- www.tightvnc.com (http://www.tightvnc.com)
- www.realvnc.com (http://www.realvnc.com)

3.3 Managing Remote Sessions on a Macintosh Device

Review the following sections for information on managing sessions on a Macintosh device:

- Section 3.3.1, "Managing a Remote Control Session on a Macintosh Device," on page 88
- Section 3.3.2, "Managing a Remote View Session on a Macintosh Device," on page 89
- Section 3.3.3, "Managing a Remote SSH Session on a Macintosh Device," on page 90

3.3.1 Managing a Remote Control Session on a Macintosh Device

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 2.3.2, “Starting Remote Management Operations on a Macintosh Device,” on page 56.

Using the Toolbar Options in the Remote Management Viewer on a Macintosh Device

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.

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.
Send Ctrl-Alt-Del		Sends the Ctrl+Alt+Del keystroke to the managed device. This option is disabled for Remote View and Remote Diagnostics sessions. The Ctrl+Alt+Del keystroke is delayed in a remote session when used for the first time after rebooting the managed device. However the subsequent Ctrl+Alt+Del keystroke takes less time until you reboot the managed device again.
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.

Option	Shortcut Key	Functionality
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.
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.

3.3.2 Managing a Remote View Session on a Macintosh Device

Remote View lets you remotely connect with a managed device so that you can view the managed device desktop.

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

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.

3.3.3 Managing a Remote SSH Session on a Macintosh Device

Remote SSH lets you securely connect to a remote Macintosh device and safely execute commands on the remote device.

On launching a Remote SSH on the device, a terminal opens up on the device, which you can use to safely execute commands on the remote device.

Click **Options** to use the following options when executing the commands on the device:

- "X11 Forwarding" on page 90
- "Local Port Forwarding" on page 91
- "Remote Port Forwarding" on page 91

X11 Forwarding

Allows you to run applications such as YaST by allowing the graphical information to be displayed on the device.

X11 forwarding is supported only if the Remote SSH session is launched from a Windows device. Ensure that an instance of XServer is running on the device on which you have launched the Remote SSH Java Web Start Launcher.

In the terminal, click **Options** > **X11**. Specify the XDisplayname in the following format:

`hostname:6000`

Local Port Forwarding

Local Port Forwarding allows you to establish a secure SSH session and then tunnel TCP connections through it. The information is sent over an encrypted connection.

In the terminal, click **Options** > **Local Port.** Specify the Local port forwarding in the following format:

`port:host:hostport`

The network connections to the client device on the local port are forwarded to the remote device on the specified port.

Remote Port Forwarding

Remote Port Forwarding allows you to establish a secure SSH session and then tunnel TCP connections through it. The information is sent over an encrypted connection.

In the terminal, click **Options** > **Remote Port.** Specify the Remote port forwarding in the following format:

`port:host:hostport`

The network connections to the SSH server on the remote port are forwarded to the local device on the specified port.

3.4 Performing Remote Control on a Macintosh device

You can remote control a Macintosh device using a device from the ZENworks Control Center device list. ZENworks does not bundle Remote Management. The OEM version of Remote Management that is available with the Macintosh Operating System is leveraged by ZENworks for remote control.

To perform the Remote Control operation on a MAC device:

1. Log in to ZENworks Control Center.
2. Select a Macintosh device object.
3. Click **Actions** > **Remote Control**.
4. Launch remote control after verifying the IP address. You can also try to launch remote control using the DNS name.
5. Verify if the remote control session is launched.

3.5 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 19.

For more information on installing a Remote Management Proxy, see Section 2.5.1, “Installing a Remote Management Proxy,” on page 66.

For more information on configuring a Remote Management Proxy, see Section 2.5.2, "Configuring a Remote Management Proxy," on page 68.

3.6 Waking Up a Remote Device

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

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 WOL packet.

IMPORTANT: On a Windows 8 machine, Wake-On-LAN is supported only in sleep (S3) or hibernate (S4) mode and not in shutdown mode. For more details, see the Microsoft support page (http://support.microsoft.com/kb/2776718).

- Section 3.6.1, "Prerequisites," on page 92
- Section 3.6.2, "Remotely Waking Up the Managed devices," on page 92

3.6.1 Prerequisites

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

- Ensure that the network card on the managed device supports WOL.
- Ensure that you have enabled the WOL option in the BIOS setup of the managed device.
- Ensure that the managed device is registered with the ZENworks Management Zone.
- Ensure that the Network Interface Card is configured in Device Manager to allow it to wake up the device. For more information, read Configuring power management using the user interface (http://technet.microsoft.com/en-us/library/ee617165%28v=ws.10%29.aspx).
- Ensure that the power adapter is connected to the device.
- 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.

3.6.2 Remotely Waking Up the Managed devices

If your device supports WOL, you can remotely wake up a managed device by:

- Configuring WOL through quick task
- Configuring WOL through bundle distribution schedule

For information on steps for Assigning Existing Bundles to Devices, see "Assigning Existing Bundles to Devices" in *ZENworks Software Distribution Reference*.

Configuring Wake-on-Lan through Quick Task

To use the WOL option through quick task:

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 WOL options for the servers to send a wakeup request to the managed devices. For more information, see

---

NOTE: Any ZENworks 11.2.4 Windows and Linux managed device can act as a proxy. For 11.2.3 and earlier, only Windows agents can act as a proxy.

Configuring Wake-on-Lan Options

1. Select one of the following options to specify the servers to send a wake-up 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.
2. Select one of the following options to specify the IP address to send 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**.
3. In the **Number of Retries** option, specify the number of attempts to wake up the device. By default, it is 1.
4. In the **Time Interval between Retries option,** specify the time period between two retry attempts. By default, it is 2 minutes.
5. Click **OK**.

NOTE: 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.

---

4 Security

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

- Section 4.1, “Security On Windows Devices,” on page 95
- Section 4.2, “Security On Linux Devices,” on page 101

4.1 Security On Windows Devices

Review the following sections for the security related information on Windows Devices:

- Section 4.1.1, “Authentication,” on page 95
- Section 4.1.2, “Password Strength,” on page 97
- Section 4.1.3, “Ports,” on page 97
- Section 4.1.4, “Audit,” on page 97
- Section 4.1.5, “Ask Permission from the User on the Managed Device,” on page 98
- Section 4.1.6, “Abnormal Termination,” on page 98
- Section 4.1.7, “Intruder Detection,” on page 99
- Section 4.1.8, “Remote Operator Identification,” on page 99
- Section 4.1.9, “Browser Configuration,” on page 100
- Section 4.1.10, “Session Security,” on page 100

4.1.1 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:

- “Rights-Based Remote Management Authentication” on page 96
- “Password-Based Remote Management Authentication” on page 96

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 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.

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 "Clearing the Remote Management Password Using ZENworks Control Center" on page 34.

4.1.2 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.

4.1.3 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.

4.1.4 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.
Status	The status of the remote operation: Success, Running, or Failure. The cause of the failure is also displayed.

4.1.5 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.

4.1.6 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.

4.1.7 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.

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.

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.**

4.1.8 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.

4.1.9 Browser Configuration

If you use Internet Explorer to remotely manage devices, then turn off the Protected mode in the security settings of the browser (**Tools > Internet Options > Security**).

Ensure that the ZENworks Control Center server is added to the list of trusted sites.

4.1.10 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.

SSL Handshake

When the ZENworks 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.

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.

4.2 Security On Linux Devices

Review the following sections:

- Section 4.2.1, “Authentication,” on page 101
- Section 4.2.2, “Password Strength,” on page 101
- Section 4.2.3, “Ports,” on page 102
- Section 4.2.4, “Ask Permission from the User on the Managed Device,” on page 102

4.2.1 Authentication

Remote Management on a Linux device is controlled by `xinetd` super service daemon on the device. This service is automatically started on the device during the device boot up.

When a remote operator initiates a remote session to the device, the `xinetd` launches a Remote Management service to start the Remote Management X-Server depending on the type of the remote operation to be performed on the device:

- For Remote Control or Remote View, the `x11vnc` service is started
- For Remote Login, the `xvnc` service is started

To prevent unauthorized access to the managed device, the Remote Management service on the managed device uses Password-Based Remote Management Authentication. This is the traditional VNC password authentication scheme, where in the remote operator is prompted to enter a password to launch the remote session on the managed device.

4.2.2 Password Strength

Use secure passwords. Keep the following guidelines in mind:

- **Length:** The minimum recommended length is 6 characters.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.

- **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.

4.2.3 Ports

By default, the Remote Management service for Remote Control and Remote View runs on port 5950 and the Remote Management service for Remote Login runs on port 5951. The Remote device should be configured to allow the ports 5950 and 5951 through the firewall.

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

4.2.4 Ask Permission from the User on the Managed Device

When user is logged on to a Linux managed device and a remote operator initiates a Remote Control or Remote View session to the device, the user on the managed device is asked permission before the Remote Control or Remote View session starts on the device.

5 Remote Management Audit Events

The Audit feature enables administrators to record various changes or actions that occur in the zone.The recorded information can be audited for compliance. It provides the ability to centrally monitor activities related to Primary Servers, Satellites, and Managed Devices. ZENworks Audit includes two types of audit events that can be configured using the Events Configuration page. They are:

- Change Events
- Agent Events

For more information, see *ZENworks Audit Management Reference*.

- Section 5.1, “Agent Events,” on page 103
- Section 5.2, “Remote Management,” on page 103
- Section 5.3, “Prerequisites,” on page 104
- Section 5.4, “Enabling Remote Management Agent Audit Events,” on page 104
- Section 5.5, “Common Tasks,” on page 105
- Section 5.6, “General,” on page 107
- Section 5.7, “Authentication,” on page 108
- Section 5.8, “Intruder Detection,” on page 110
- Section 5.9, “Session,” on page 113
- Section 5.10, “Others,” on page 117

5.1 Agent Events

Agent events log information about the actions performed on the ZENworks managed devices. For example, an audit event that records the login activity of a ZENworks user on a managed device.

5.2 Remote Management

Remote Management is one of the categories for which agent events are generated. Remote management events performed on a device are logged and audit information for the same is available in the Dashboard.

NOTE: The Remote management audit logs are generated only for Windows managed devices.

5.3 Prerequisites

The following prerequisites are required to configure and view remote management audit events:

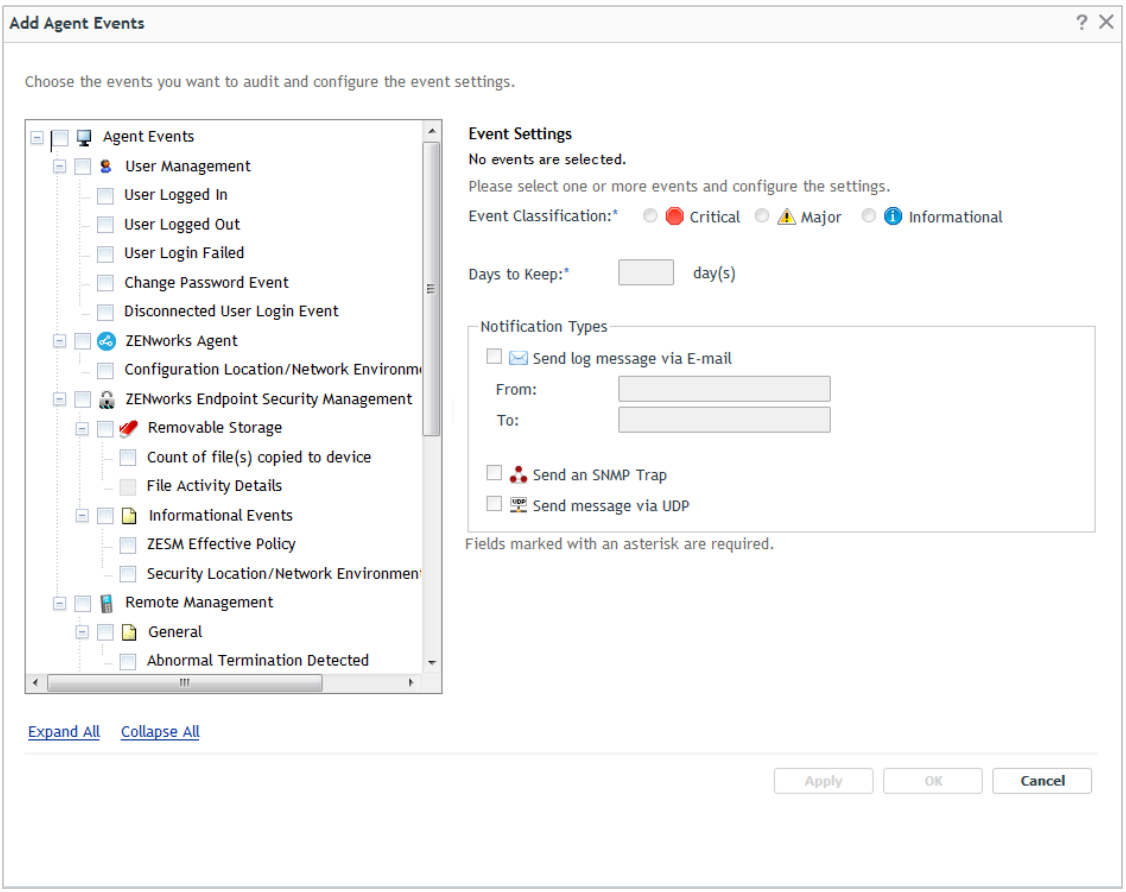
- The agent should be registered with the ZENworks server.
- The ZENworks super administrator should have the following rights:
  - Remote Management Rights
  - Policy Rights
  - Device Rights
  - Zone Rights
  - User Rights

NOTE: The non-super administrator has limited rights and can only view the audit events but cannot edit.

5.4 Enabling Remote Management Agent Audit Events

If you want remote event details to be generated and logged in the audit database, you need to first enable or configure the remote management audit events in ZENworks Control Center.

1. Log in to ZENworks Control Center
2. Click **Configuration** >**Audit Management** >**Events Configuration.**
3. Click the **Agent Events** tab, then click **Add**.



4 Select any of the remote audit events available under the Remote Management category.

5 Select the attributes such as **Event Classification Type**, **Days to Keep**, and **Notification Types** etc for each event either separately or combined.

6 Click **OK**.

5.5 Common Tasks

The tasks that are common with similar steps for all the remote management audit events include:

- Section 5.5.1, “Editing or Deleting Remote Management Audit Events,” on page 106
- Section 5.5.2, “Viewing Details - Generated Remote Management Audit Events,” on page 106
- Section 5.5.3, “Verifying the Enabled Remote Management Audit Events,” on page 106

5.5.1 Editing or Deleting Remote Management Audit Events

To edit or delete the enabled events, select and click on edit or delete on the same page. For example, to edit or delete the enabled abnormal termination detected audit event:

1. Click **Abnormal Termination Detected** on the Event Configuration page under the Agent Events tab.
2. Click **Edit** to display the edit properties dialog box and make the required changes.
3. Click **OK**.

5.5.2 Viewing Details - Generated Remote Management Audit Events

After enabling a remote management audit event on a device or zone, you can view details of the generated remote management audit events.

For example,

To view event details of the generated abnormal termination detected audit event on a device:

1. In ZENworks Control Center, click **Devices**> **Workstations**.
2. Click any device, then click the **Audit** tab.
3. Click **Agent Events**, then click the plus sign to expand the tree view structure of Agent Events.
4. Click the plus sign next to **Remote Management** to view the **Authentication Failure** audit event listed under **Authentication**, if enabled.

To view event details of the generated abnormal termination detected audit event on a zone:

1. In ZENworks Control Center, click **Audit and Messages**> **Audit** > **Events** > **Agent Events**. In the Agent Events Summary, events are categorized as Critical, Major, or Informational based on severity.
2. Click **Agent Events**, then click the plus sign to expand the tree view structure of Agent Events.
3. Click the plus sign next to Remote Management to view the Authentication Success audit event listed under Authentication, if enabled. Click any device, click the **Audit** tab.
4. Click **Authentication Success**. The Authentication Success events logged in that zone are displayed.

5.5.3 Verifying the Enabled Remote Management Audit Events

If for some reason the details of the enabled remote management audit event for a zone or a device are not displayed in ZENworks control center, you can verify if that remote management audit event is enabled on the device. For example, to verify if the abnormal termination detected audit event is enabled on the device:

1. On the device, open the following file:

   `ZENWORKS_HOME\conf\audit\events\daudit.remote.abnormal.termn.detect.xml`
2. Verify that the event is enabled (**Enable = true**). If it is not enabled, repeat the steps listed under Enabling an Abnormal Termination Detected Audit Event (page 107).

5.6 General

The event that logs basic, general information related to the sudden termination of a remote session is grouped under the general category.

- Section 5.6.1, “Abnormal Termination,” on page 107

5.6.1 Abnormal Termination

The Abnormal Termination Detected audit event is logged when a remote management session is terminated suddenly and abnormally. This occurs when either the network is disconnected or when vnc viewer process is killed. This event logs an audit event with basic information of an abnormally terminated remote session.

- “Enabling an Abnormal Termination Detected Audit Event” on page 107
- “Generating an Abnormal Termination Detected Audit Event” on page 107

Enabling an Abnormal Termination Detected Audit Event

To enable an Abnormal Termination Detected audit event during the Remote Control operation on a device:

1. Log in to ZENworks Control Center on a server that has Windows devices.
2. Click **Configuration** > **Audit Management** > **Events Configuration**.
3. In the Events Configuration page, click **Agent Events** > **Add**.
4. In the Add Agent Events dialog box, select the **Abnormal Termination Detected** check box under **Remote Management** > **General**.
5. Configure the event settings such as **Event classification**, **Days to keep**, **Notification Types**, and so forth, for the Abnormal Termination Detected event, then click **Apply**.
6. Click **OK** to add the Abnormal Termination Detected event and close the Add Agent Events dialog box.

Generating an Abnormal Termination Detected Audit Event

1. In ZENworks Control Center, click **Devices** > **Workstations**
2. Select a Windows device, then click **Remote Control** to remotely manage that device.
3. When the Remote Control operation is in progress, do the following on the management console:
   - **3a** Press **Ctrl+Alt+Del** to invoke the Task Manager.
   - **3b** Click the **Processes** tab, then select `nzrViewer.exe` from the list.
   - **3c** Click **End** to kill the `nzrViewer.exe` process. The managed device will either be locked or logged off which indicates that the Abnormal Termination is detected and the Abnormal Termination Detected event is logged.

NOTE: In a remote management operation that is performed through Join Proxy, when the viewer crashes, and the session is closed, the abnormal termination event is not generated.

5.7 Authentication

The events that log information related to the user credentials are grouped under the authentication category. You can configure the following:

- Section 5.7.1, “Authentication Failure,” on page 108
- Section 5.7.2, “Authentication Success,” on page 110

5.7.1 Authentication Failure

This event is generated when authentication is unsuccessful for the remote operator due to several reasons. The failure could be due to wrong password, lack of permission, or cancellation of certification.

- “Enabling an Authentication Failure Audit Event” on page 108
- “Generating an Authentication Failure Audit Event” on page 108
- “Authentication Failure Reasons” on page 109

Enabling an Authentication Failure Audit Event

To enable an Authentication Failure audit event during a remote session:

1. Log in to ZENworks Control Center on a server that has Windows devices.
2. Click **Configuration**> **Audit Management** >**Events Configuration**.
3. In the Events Configuration page, Click the **Agent Events** tab >**Add**.
4. In the Add Agent Events dialog box, select the **Authentication Failure** check box under **Remote Management** >**Authentication**.
5. Configure the event settings such as **Event classification**, **Days to keep**, **Notification Types**, and so forth, for the Authentication Failure audit event, then click **Apply**.
6. Click **OK** to add Authentication Failure event and close the Add Agent Events dialog box.

Generating an Authentication Failure Audit Event

1. In ZENworks Control Center, click **Devices** >**Workstations**
2. Select a Windows device, then execute one of the remote management operations on the device in password mode.
3. Enter a wrong password when you are prompted for a password. The Authentication Failure event is logged and the password is requested again.

In a remote session if authentication fails at a stage when the identity of the remote operator is not verified yet, then the information about the initiator of the event on the managed device is recorded as unknown in the audit log. For example, initiator information is not logged for certificate related failures, because the failure occurs even before the remote operator information is passed on to the managed device.

Authentication Failure Reasons

In the event log you might find some of the authentication failure reasons listed with error codes.

Event Details

Initiator :	Administrator	**Category :**	Remote Management/Authentication
Classification :	Major	**Device :**	/devices/servers/epm-cld-167183
Message :	Remote operator authentication failed	**Date and Time :**	22 Nov, 2013 11:38:07 PM

Session ID:	1385143684
Operation:	Remote Control
Agent Initiated Connection:	No
Asked User Permission:	No
Authentication Mode:	Password
Password Mode:	ZENworks Persistent Password
Console Device:	blr-d-rdarshan.blr.novell.com
ZENworks User:	Not Available
Local User:	EPM-CLD-167183\Administrator
Failure Reason:	Authentication failed with an error code : 2.

The following are the error codes with their description:

- 2: Failed while reading from or writing to the socket on the managed device.
- 4: Failed abruptly while verifying Novell password on the managed device.
- 7: Failed while verifying version compatibility for the session on the managed device
- 9: Failed while enabling encryption for session on the managed device.
- 10: Failed while verifying operation for the session on the managed device
- 16: Failed as the managed device received an unknown Novell authentication scheme
- 17: Failed as the managed device received invalid security type.
- 18: Failed as the managed device received incorrect security type.
- 22: Failed while allocating memory using malloc on the managed device.
- 23: Failed as managed device received unexpected size for client proof or client parameter
- 32: Failed as the managed device encountered an error while attempting to retrieve the Remote Management policy

5.7.2 Authentication Success

Authentication Success audit event is generated when authentication is successful during a Remote Management session, either in password or in rights mode. This is a high priority event in that it alerts the administrator about the initiation of a remote session on a specific device.

The following basic information about the remote session is also logged during the Authentication Success event:

- Session ID
- Operation
- Authentication Mode

This section included information on the following:

- "Enabling an Authentication Success Audit Event" on page 110
- "Generating an Authentication Success Audit Event" on page 110

Enabling an Authentication Success Audit Event

1. Log in to ZENworks Control Center on a server that has Windows devices.
2. Click **Configuration** >**Audit Management** >**Events Configuration**.
3. In the **Events Configuration** page, Click the **Agent Events** tab > **Add**.
4. In the **Add Agent Events** dialog box, select the **Authentication Success** check box under **Remote Managemen**t >**Authentication**.
5. Configure the event settings such as **Event classification**, **Days to keep**, **Notification Types**, and so forth, for the Authentication Success audit event, then click **Apply**.
6. Click **OK** to add the Authentication Success event and close the Add Agent Events dialog box.

Generating an Authentication Success Audit Event

1. In ZENworks Control Center, click **Devices** >**Workstations.**
2. Select a Windows device, then execute one of the remote management operations on the device in password or rights mode.
3. When authentication is successful, the Authentication Success audit event is logged.

5.8 Intruder Detection

This section includes information on the following:

- Section 5.8.1, "Intruder Detection Lock," on page 111
- Section 5.8.2, "Intruder Detection Reset Audit Event," on page 111

5.8.1 Intruder Detection Lock

Intruder Detection Lock audit event is logged when an intruder is detected after successive authentication failures and the device stops accepting remote session requests. This is possible when a remote operator enters the wrong credentials several times during a remote session and if those invalid attempts cross the limit specified in the Remote Management Policy settings.

- "Enabling an Intruder Detection Lock Audit Event" on page 111
- "Generating an Intruder Detection Lock Audit Event" on page 111

Enabling an Intruder Detection Lock Audit Event

1. Log in to ZENworks Control Center on a server that has Windows devices.
2. Click **Configuration** > **Audit Management** > **Events Configuration**.
3. In the Events Configuration page, click **Agent Events** > **Add**.
4. In the **Add Agent Events** dialog box, select the **Intruder Detection Lock** check box under Remote Management > **Intruder Detection**.
5. Configure the event settings such as **Event classification**, **Days to keep**, **Notification Types**, and so forth, for the Intruder Detection Lock event, then click **Apply**.
6. Click **OK** to add the Intruder Detection Lock event and close the Add Agent Events dialog box.

Generating an Intruder Detection Lock Audit Event

1. Apply a remote management policy that enables Persistent password mode and set the password. Set the value of Intruder Detection Lock to Suspend accepting connections after 2 successive invalid attempts.
2. In ZENworks Control Center, click **Devices** > **Workstations**.
3. Select a Windows device and click **Remote Control** in password mode, to remotely manage that device.
4. Enter a wrong password when prompted. This invalid attempt logs an Authentication Failure event and then the password is requested again. Enter a wrong password for the second time.

   Based on the settings configured for Intruder Detection in the security settings of the remote management policy, the device is locked for remote management operations and the Intruder Detection Lock audit event is logged.

After the specified time in Audit Settings, the generated Intruder Detection Lock event is uploaded to the server and displayed in ZENworks Control Center. You can view the Intruder Detect Lock audit events logged on a device and also on a zone.

5.8.2 Intruder Detection Reset Audit Event

The Intruder Detection Reset audit event is logged when you unblock a device to accept remote session requests. You can trigger this event by quick task, local user or policy settings which is logged as initiator.

Enabling an Intruder Detection Reset Audit Event

1. Log in to ZENworks Control Center on a server that has Windows devices.
2. Click **Configuration** > **Audit Management** > **Events Configuration**.
3. In the Events Configuration page, Click the **Agent Events** tab >**Add**.
4. In the Add Agent Events dialog box, select the **Intruder Detection Reset** check box under **Remote Management** > **Intruder Detection**.
5. Configure the event settings such as **Event classification**, **Days to keep**, **Notification Types**, and so forth, for the Intruder Detection Reset event, then click **Apply**.
6. Click **OK** to add the Intruder Detection Reset event and close the Add Agent Events dialog box.

Generating an Intruder Detection Reset Audit Event

1. Perform the steps listed for Generating an Intruder Detection Lock Audit Event.
2. To perform remote operations again on the device that is locked, unlock the device by using one of the following options:

   2a In ZENworks Control Center, select the device > click **Unblock Remote Management** quick task. If the Intruder Detection Rest is performed through quick task, the information about ZENworks administrator who initiated the quick task is not recorded in the audit log.

   Or

   2b Increase the value of **Suspend accepting connections after X successive invalid attempts** in the Remote Management Policy settings.

   Or

   2c Perform the remote management operation only after the time specified in **Automatically start accepting connections after Y minutes** under Intruder Detection is over in the Remote Management Policy Settings

   Or

   2d On the Z-Icon page of the managed device,

   2d1 Click **Remote Management** > click **Security**, then click **Enable accepting connections if currently blocked due to intruder detection**.

   2d2 Click **Ok** in the pop-up that displays **The device is enabled to accept remote management connections**.

After unlocking the device if you perform remote operations through one of the above listed methods, the device starts accepting connections and the Intruder Detection Reset audit event is logged.

5.9 Session

There are five different remote sessions that are grouped under the session category. These session events require more time for completion as apposed to the non-session events which are instant. For remote sessions, audit events are logged after the session is terminated or when the maximum limit is reached for audit log size.

- Section 5.9.1, “Remote Control,” on page 113
- Section 5.9.2, “Remote View,” on page 114
- Section 5.9.3, “Remote Execute,” on page 114
- Section 5.9.4, “Remote Diagnostics,” on page 115
- Section 5.9.5, “File Transfer,” on page 116

5.9.1 Remote Control

Remote Control audit event is logged when a remote operator launches Remote Control session on a Windows managed device.

- “Enabling a Remote Control Audit Event” on page 113
- “Generating a Remote Control Audit Event” on page 113

Enabling a Remote Control Audit Event

1. Log in to ZENworks Control Center on a server that has Windows devices.
2. Click **Configuration** > **Audit Management** >**Events Configuration**.
3. In the Events Configuration page, Click the **Agent Events** tab >**Add**.
4. In the Add Agent Events dialog box, select the **Remote Control** check box under **Remote Management** > **Session**.
5. Configure the event settings such as **Event classification**, **Days to keep**, **Notification Types**, and so forth, for the Remote Control audit event, then click **Apply**.
6. Click **OK** to add the Remote Control audit event and close the Add Agent Events dialog box.

Generating a Remote Control Audit Event

1. In ZENworks Control Center, click **Devices** > **Workstations**
2. Select a Windows device and click **Remote Control** to remotely manage that device.
3. Close the Remote Control session. The Remote Control audit event is logged on the device.

If you launch Remote Execute and File Transfer through remote control, then the session ID is common to all three sessions.

On the other hand if you launch Remote View and Remote Control in collaborate mode, then the collaborate id is common to both of these events.

Thus remote control audit event logs basic session information such as session ID, session start time, session end time and specific information such as collaborate ID in case of collaboration. If both session ID and collaborate ID are same then the session is master collaborate session.

Files transferred or commands executed in the Remote Control session are logged as respective file transfer and remote execute events with same session ID as remote control audit event.

NOTE: Abnormal Termination Detected event is possible only in Remote Control session.

5.9.2 Remote View

Remote View audit event is logged when a remote operator launches a Remote View session to view the desktop of a Windows managed device. This event logs basic session information such as session ID, session start time, session end time and also specific information such as collaborate ID in case of collaboration.

- "Enabling a Remote View Audit Event" on page 114
- "Generating a Remote View Audit Event:" on page 114

Enabling a Remote View Audit Event

Enable a Remote View audit event while remotely managing a device:

1. Log in to ZENworks Control Center on a server that has Windows devices.
2. Click **Configuration** >**Audit Management** >**Events Configuration**.
3. In the Events Configuration page, click the **Agent Events** tab > **Add**.
4. In the Add Agent Events dialog box, select the **Remote View** check box under **Remote Management** > **Session.**
5. Configure the event settings such as **Event classification**, **Days to keep**, **Notification Types**, and so forth, for the Remote View audit event, then click **Apply**.
6. Click **OK** to add the Remote View audit event and close the Add Agent Events dialog box.

Generating a Remote View Audit Event:

1. In ZENworks Control Center, click **Devices** > **Workstations**.
2. Select a Windows device, then click **Remote Control**.
3. In the **Operation** list, select **Remote View** to launch a Remote View session.
4. Close the Remote View session. The Remote View audit event is logged on the device.

5.9.3 Remote Execute

Remote Execute audit event is logged when a remote operator launches a Remote Execute session to run an executable with system privileges on a Windows managed device. The specific details that are audited for this event include commands executed, time of execution and result of the operation.

Enabling a Remote Execute Audit Event

Enable a Remote Execute audit event while remotely managing a device:

1. Log in to ZENworks Control Center on a server that has Windows devices.
2. Click **Configuration** > **Audit Management** >**Events Configuration**.
3. In the Events Configuration page, Click the **Agent Events** tab > **Add**.
4. In the Add Agent Events dialog box, under **Remote Management** > **Session**, select the **Remote Execute** check box.
5. Configure the event settings such as **Event classification**, **Days to keep**, **Notification Types**, and so forth for the Remote Execute audit event, then click **Apply**.
6. Click **OK** to add the Remote Execute audit event and close the Add Agent Events dialog box.

Generating a Remote Execute Audit Event

1. In ZENworks Control Center, click **Devices** > **Workstations**
2. Select a Windows device, then click **Remote Control**.
3. In the **Operation** list, select **Remote Execute** to launch a Remote Execute session.
4. Execute at least one command and then close the Remote Execute session. The Remote Execute audit event is logged on the device.

It is also possible to generate a remote execute event when you launch a Remote Execute session through a Remote Control session.

5.9.4 Remote Diagnostics

Remote Diagnostics audit event is logged when a remote operator launches a Remote Diagnostics session to remotely diagnose and analyze the problems on a Windows managed device. This audit event gives more information regarding the applications launched, path of the application and launch time of the session.

- "Enabling a Remote Diagnostics Audit Event" on page 115
- "Generating a Remote Diagnostics Audit Event" on page 116

Enabling a Remote Diagnostics Audit Event

Enable Remote Diagnostics audit event while remotely managing a device

1. Log in to ZENworks Control Center on a server that has Windows devices.
2. Click **Configuration** > **Audit Management** >**Events Configuration**.
3. In the Events Configuration page, Click the **Agent Events** tab > **Add**.
4. In the Add Agent Events dialog box, select the **Remote Diagnostics** check box under **Remote Management** > **Session**.
5. Configure the event settings such as **Event classification**, **Days to keep**, **Notification Types**, and so forth, for the **Remote Diagnostics** audit event, then click **Apply**.
6. Click **OK** to add the Remote Diagnostics audit event and close the Add Agent Events dialog box.

Generating a Remote Diagnostics Audit Event

1. In ZENworks Control Center, click **Devices** > **Workstations**
2. Select a Windows device, then click **Remote Diagnostics** to launch a Remote Diagnostics session.
3. Close the Remote Diagnostics session. The Remote Diagnostics audit event is logged on the device.

5.9.5 File Transfer

File Transfer audit event is logged when a remote operator launches a File Transfer session to transfer files between the management console and the Windows managed device.

Enabling a File Transfer Audit Event

1. Log in to ZENworks Control Center on a server that has Windows devices
2. Click **Configuration** > **Audit Management** >**Events Configuration**.
3. In the Events Configuration page, click the **Agent Events** tab > **Add.**
4. In the Add Agent Events dialog box, under **Remote Management** > **Session**, select the **File Transfer** check box.
5. Configure the event settings such as **Event classification**, **Days to keep**, **Notification Types**, and so forth, for the File Transfer audit event, then click **Apply**.
6. Click **OK** to add the File Transfer audit event and close the Add Agent Events dialog box.

Generating a File Transfer Audit Event

1. In ZENworks Control Center, click **Devices** > **Workstations**.
2. Select a Windows device, then click **File Transfer** to launch a File Transfer session.
3. Launch at least one file operation, then Close the File Transfer session. The File Transfer audit event is logged on the device.

NOTE: An empty file transfer event is logged with no extra information of files transferred, if File Transfer is launched as an internal operation either from Remote Control or Remote Diagnostics session. This helps to indicate that the file transfer is initiated in the parent session and the session might take long time before logging a file transfer event.

In a File Transfer session when you are in the process of downloading files from the managed device on to a local device and the session fails with the access denied to create file error, then the failure of file downloads is not recorded in the File Transfer audit log. As failure occurs even before the data is requested from the managed device, there is no communication to the managed device about the failure of file download.

NOTE: You cannot transfer or copy internal operating system files which are not visible in Windows Explorer or in remote management File Transfer dialog, though the folder size indicates the existence of system files in this folder.

5.10 Others

There are certain other helpful details related to the audit events logged for remote management events. Some of them are explained in the following sections:

5.10.1 Internal Operations

Operations which are launched in another session (not independently) are termed as internal operations.

For example, File Transfer can be launched internally in a Remote Control or a Remote Diagnostics session. Remote Execute event is logged when launched as single operation where only commands can be executed. Remote Execute event is also logged when it is launched in a Remote Control session

You can launch and exit these internal operations any time without affecting actual remote session. But irrespective of how many times you launch these internal operations, an audit event is logged only at the end of the actual remote session.

5.10.2 Intermediate Events

An intermediate event is launched for events such as remote execute, remote diagnostics and file transfer when the commands executed, applications launched and files transferred are huge and exceed the limit of audit log file size. An intermediate event will have only start time and the status displayed for this event is **In-Progress**.

For example in a single File transfer session there can be thousands of files that can be transferred. As per the limitation on each audit log file size, you cannot log additional data (files transferred info) which has size exceeding 200KB. This comes to around 250 files transferred. Due to this limitation approximately for every 250 files transferred there is an intermediate file transfer audit log event. Similarly for remote execute and remote diagnostics events.

For events that are generated at the end of a session both start and end time information is available.

5.10.3 Abrupt Termination

In a remote session that is in progress, if there is abrupt termination due to force reboot or power failure, the audit information is not lost and will be logged once the system comes back. Every time remote management service is initialized, it checks for the pending audit events to be logged and logs it with reason for termination as abrupt. The end time will not be accurate but will have maximum of a minute deviation. When system is down, the last updated time available on disk will be used as end time for the pending events to be logged.

6 Troubleshooting

The following sections explain the scenarios that you might encounter while using the Remote Management component of Novell ZENworks:

- Section 6.1, “Troubleshooting Windows Devices,” on page 119
- Section 6.2, “Troubleshooting Linux Devices,” on page 130
- Section 6.3, “Troubleshooting Macintosh Devices,” on page 132

6.1 Troubleshooting Windows Devices

- “When you configure a ZENworks zone with an external CA and remote control a device an error message is displayed” on page 120
- “Unable to override the screen saver on the managed device” on page 121
- “Unable to launch a remote session on the managed device that is running on a very low color quality” on page 121
- “Unable to launch the Remote Management viewer” on page 122
- “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.” on page 122
- “Troubleshooting error messages encountered while using the Remote Management component” on page 122
- “How do I enable Remote Management debug log on the device launching the ZENworks Control Center” on page 122
- “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” on page 123
- “Blank screen option might fail to work while remote controlling a Windows device” on page 123
- “Unable to use the Ctrl-Alt-Del icon while remotely controlling a Windows 8, Windows 7, Windows Server 2008, or Windows Server 2008 R2 device” on page 123
- “The default session mode is not selected in the Remote Management snap-in” on page 124
- “The Remote Management viewer fails to launch on a Windows device” on page 124
- “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 124
- “The desktop of a device might not be visible when you remotely control or remotely view the device” on page 124
- “Unable to remotely transfer files to restricted folders on a Windows device” on page 125
- “Unable to remotely control Remote Desktop Protocol session on a Windows device” on page 125

- "Unable to remotely manage a Windows device after changing the network configuration" on page 126
- "The Lock/Unlock keyboard and mouse option causes problems on some remotely managed Windows devices" on page 126
- "The Blank/Unblank Screen option causes problems on some remotely managed Windows devices" on page 126
- "A remote session might get disconnected on an attempt to switch a user logged on to a Windows managed device with wireless network connection" on page 127
- "On a Windows managed device that has IE 10 or 11, Remote Management prompts for adding the IP of the ZENworks Primary Server to the trusted zone" on page 127
- "The File Transfer Window Crashes When You Repeatedly Scroll, Sort the List View, or Check the File Size" on page 127
- "On a managed device that is remotely managed from ZENworks Control Center, Wallpaper might not be restored if the remote operator disconnects on the login screen" on page 128
- "The ZENworks RM Viewer appears tilted if you remote control a tablet device which is tilted" on page 128
- "Unable to launch connection to a ZENworks managed device through some of the third-party viewers" on page 128
- "The visible signal might not appear on a remote controlled managed device that includes Windows 8.1 operating system" on page 128
- "The status entry of an uninstalled Mirror driver is not automatically removed from the Device Manager" on page 129
- "Unable to perform remote operations on a Tablet device after clicking the blank screen menu option" on page 129
- "Unable to perform remote operations on a linux managed device because the device's RM port is not added as a firewall exception" on page 129
- "Applications installed beyond a specific limit are not visible in the RM diagnostics applications toolbar" on page 130

When you configure a ZENworks zone with an external CA and remote control a device an error message is displayed

Source: ZENworks 2017

Explanation: When you configure a ZENworks zone with an external Certificate Authority and launch the remote management operation on a managed device without providing a certificate or by providing an invalid certificate, you might get the following error message: *The managed device was unable to initialize Novell encryption scheme for the session.*

Action: Provide a valid Private Key and certificate, or enable **Allow Connection When Remote Management Console Does Not Have SSL Certificate** in the Remote Management policy.

NOTE: If you do not want to specify the Private Key and certificate, then 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, it is not recommended to use this option because it will impact the security of the device.

Unable to override the screen saver on the managed device

Source: ZENworks; ZENworks 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 Windows 7, Windows Server 2008, or Windows Server 2008 R2 device, and Windows 8.

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.

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

Source: ZENworks; ZENworks 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; ZENworks 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: Install the latest version of ZCC Helper from the Administrative Tools tab in the setup page (`https://<ZENworks_server_IPaddress>/zenworks-setup`).

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; ZENworks 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; ZENworks 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 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 DebugLevel, and set the hexadecimal value to a (decimal value equals 10).
4. 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; ZENworks Configuration Management; Remote Management.

Action: To enable the logs, see TID 3418069 (http://www.novell.com/support/search.do?usemicrosite=true&searchString=3418069)

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; ZENworks 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.

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

Source: ZENworks; ZENworks 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.

Unable to use the Ctrl-Alt-Del icon while remotely controlling a Windows 8, Windows 7, Windows Server 2008, or Windows Server 2008 R2 device

Source: ZENworks; ZENworks Configuration Management; Remote Management.

Explanation: If you launch a Remote Control operation on a Windows 8, 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; ZENworks 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 Remote Management viewer fails to launch on a Windows device

Source: ZENworks; ZENworks Configuration Management; Remote Management.

Explanation: On a Windows 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 in Internet Explorer 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; ZENworks 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; ZENworks Configuration Management; Remote Management.

Explanation: If you remotely control or remotely view a Windows XP or Windows 2003 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 device

Source: ZENworks; ZENworks Configuration Management; Remote Management.

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

Action: Do any of the following to turn off User Account Control (UAC) on Windows 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.

OR

1. Press **Windows Key +R**, type `regedit`
2. Locate `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA`
3. Update the EnableLUA value to 0
4. Restart the device.

Unable to remotely control Remote Desktop Protocol session on a Windows device

Source: ZENworks; ZENworks Configuration Management; Remote Management

Explanation: You cannot remotely control an RDP session on a Windows device.

Possible Cause: The Windows architecture on these devices prevents desktop capture when an RDP session is active.

Action: There is no workaround for this issue.

Unable to remotely manage a Windows device after changing the network configuration

Source: ZENworks; ZENworks Configuration Management; Remote Management.

Explanation: When you install the ZENworks Configuration Management Agent on Windows devices, the Firewall exception for Remote Management is added by default to the network profile that is configured to the network connection during the Agent installation.

If you change the current network profile, you might not be able to remotely control the device.

Possible Cause: Firewall exceptions are added only for the current network profile and not for all profiles.

Action: Manually add the Firewall exception for Remote Management for the new network profile.

The Lock/Unlock keyboard and mouse option causes problems on some remotely managed Windows devices

Source: ZENworks; ZENworks Configuration Management; Remote Management.

Explanation: The **Lock/Unlock keyboard and mouse** menu bar option does not work on some of the remotely managed Windows devices.

Action: Disable this feature on problematic devices to prevent the remote operator from using this operation:

1. Create the `DisableLockKeyboardMouse` DWORD and set it's value to more than zero in the following location:

   `HKLM\Software\Novell\ZCM\Remote Management\Agent`

2. Restart the Remote Management service.

The Blank/Unblank Screen option causes problems on some remotely managed Windows devices

Source: ZENworks; ZENworks Configuration Management; Remote Management.

Explanation: The **Blank/Unblank Screen** menu bar option does not work on some of the remotely managed Windows devices. This option might lead to side-effects such as high CPU utilization, abrupt system shutdown on some devices. This is caused by underlying hardware.

Action: Disable this feature on problematic devices to prevent the remote operator from using this operation:

1. Create the `DisableBlankScreen` DWORD and set it's value to more than zero in the following location:

   `HKLM\Software\Novell\ZCM\Remote Management\Agent`

2. Restart the Remote Management service.

A remote session might get disconnected on an attempt to switch a user logged on to a Windows managed device with wireless network connection

Source: ZENworks; ZENworks Configuration Management; Remote Management.

Explanation: On a Windows managed device with wireless network connection, when you try switching to Switch User screen, Windows disconnects the wireless network in the background. This in turn causes an ongoing remote session to be disconnected.

Action: There is no workaround.

On a Windows managed device that has IE 10 or 11, Remote Management prompts for adding the IP of the ZENworks Primary Server to the trusted zone

Source: ZENworks; ZENworks Configuration Management; Remote Management.

Explanation: Remote management on a Windows managed device that has Internet Explorer 10 or 11 prompts you to add the IP address of the ZENworks Primary Server to the trusted zone.

Possible Cause: The IP address of the ZEnworks Primary Server is not added to the trusted zone.

Action: Add the IP address of the ZENworks Primary Server to the list of trusted sites to avoid the prompt each time.

1. Open Internet Explorer10 or 11
2. On the **Tools** menu, select **Internet Options**> **Security**
3. Click the **Trusted Sites** icon > **Sites**
4. In the Trusted Sites dialog, enter the IP address of the ZENworks Primary Server
5. Click **Add** > **Close**.

The File Transfer Window Crashes When You Repeatedly Scroll, Sort the List View, or Check the File Size

Source: ZENworks; ZENworks Configuration Management; Remote Management.

Explanation: During the remote file transfer session, the File Transfer window crashes if you perform the following actions repeatedly:

- Sort the files
- Scroll the list of files
- Check the size of files

Action: Relaunch the File Transfer window.

On a managed device that is remotely managed from ZENworks Control Center, Wallpaper might not be restored if the remote operator disconnects on the login screen

Source: ZENworks; ZENworks Configuration Management; Remote Management.

Explanation: When you remote control a managed device from ZENworks Control Center, the wallpaper on the managed device's desktop might not be displayed during the subsequent login, if you disconnect the remote session on the login screen.

After you logoff and end the remote session, the wallpaper should be visible during the next login.

Action: Logout and login from the user session until the Wallpaper is restored.

If users on the managed device are able to access ZENWORKS_HOME, they can execute the `ZENWORKS_HOME\bin\nzrWallpaper.exe` file to restore the wallpaper.

The ZENworks RM Viewer appears tilted if you remote control a tablet device which is tilted

Source: ZENworks; ZENworks Configuration Management; Remote Management.

Explanation: If you launch a remote control session from ZENworks Control Center to a tablet device when it is tilted, the ZENworks RM Viewer is also tilted. As a result, you cannot view the screen properly.

Action: Ensure that the screen of the tablet device is not tilted during the remote session.

Unable to launch connection to a ZENworks managed device through some of the third-party viewers

Source: ZENworks; ZENworks Configuration Management; Remote Management.

Explanation: If you try to launch connection to a ZENworks managed device through some of the third-party viewers, the connection fails.

Workaround: Use one of the following:

- Standalone ZENworks remote management viewer
- TightVNC or UltraVNC third-party viewer

The visible signal might not appear on a remote controlled managed device that includes Windows 8.1 operating system

Source: ZENworks; ZENworks Configuration Management; Remote Management

Explanation: When you remote control a managed device on which Windows 8.1 is installed, you might not see the visible signal in the top right-hand corner.

Action: Restart either the Remote Management Service or the managed device.

The status entry of an uninstalled Mirror driver is not automatically removed from the Device Manager

Source: ZENworks; ZENworks Configuration Management; Remote Management

Explanation: On 64-bit Windows devices, the Mirror driver entry created in Device Manager during installation is not removed automatically when you uninstall a Mirror driver.

If you try to reinstall a mirror driver at a later time, you will find multiple entries created in the Device Manager; some with the status as **Working** while the others with the status as **Not working**. Next time when you try to install a Mirror driver, multiple entries with the status as working or not working are created in Device Manager. The Mirror driver icon appears corrupted.

Action: During the Mirror driver uninstall, manually delete the **Not working** status entries in the Device Manager.

Unable to perform remote operations on a Tablet device after clicking the blank screen menu option

Source: ZENworks; ZENworks Configuration Management; Remote Management.

Explanation: After launching a remote connection to a Tablet device if you click the Blank screen menu option on the remote management viewer, you might not be able to perform remote operations further. The tablet device is sometimes not restored to the original state even after clicking the Unblank screen menu option.

Workaround: None

Action: It is recommended that you reboot the Tablet device to restore it to the original state.

Unable to perform remote operations on a linux managed device because the device's RM port is not added as a firewall exception

Source: ZENworks; ZENworks Configuration Management; Remote Management.

Explanation: You cannot remote control a managed device on which Linux is installed, if the devices's remote management port is not added as an exception in the firewall settings of the Linux managed device.

Action: Do one of the following:

- To allow remote connection through a configured port, manually add an exception for the port in the firewall settings of the managed device
- For multiple devices, create a bundle with a script, which adds the port as an exception in the firewall settings. Assign the bundle to the devices.

Applications installed beyond a specific limit are not visible in the RM diagnostics applications toolbar

Source: ZENworks; ZENworks Configuration Management; Remote Management.

Explanation: By default, four applications are listed in the RM Diagnostics Applications toolbar. When a ZENworks user adds more than 20 Applications, only the Applications in the first row of the toolbar are visible. The icons of the remaining Applications are not displayed in the RM Diagnostics toolbar.

Action: It is recommended that you install upto10-15 applications only. However, the display of Application icons also depends on the configured resolution of the session.

6.2 Troubleshooting Linux Devices

- "Unable to launch a remote session on a SUSE Linux Enterprise Server 11 device through Mozilla Firefox" on page 130
- "Installing the Remote Management Proxy on a SUSE Linux Enterprise Server 11 device displays an error message" on page 130
- "The Remote Management Viewer hangs when a Remote Control Session is launched on a Linux device" on page 131
- "Unable to launch a Remote SSH session on a SLES 10 device that has on older version of the JRE installed" on page 131
- "Unable to launch a Remote Control session on a Linux device that has an X session running on a display port other than the default display port" on page 131

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

Source: ZENworks; ZENworks 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.

Installing the Remote Management Proxy on a SUSE Linux Enterprise Server 11 device displays an error message

Source: ZENworks; ZENworks Configuration Management; Remote Management.

Explanation: If you choose to install the Remote Management proxy on a SLES 11 device, you might encounter the following error message:

```
insserv: Script jexec is broken: incomplete LSB comment.
```

```
insserv: missing `Required-Stop:' entry: please add even if
empty.
```

This error occurs because of the version of the jexec script installed on the device. However, the Remote Management proxy is successfully installed on the device.

Action: Ignore the error message.

The Remote Management Viewer hangs when a Remote Control Session is launched on a Linux device

Source: ZENworks; ZENworks Configuration Management; Remote Management.

Explanation: If you launch a Remote Control session on a Linux device and then resize or move a terminal that is open on the device, the Remote Management Viewer on the management console device hangs.

Action: Click the on the Remote Management Viewer to refresh the device.

Unable to launch a Remote SSH session on a SLES 10 device that has on older version of the JRE installed

Source: ZENworks; ZENworks Configuration Management; Remote Management.

Explanation: If you launch a Remote SSH session on a SLES 10 device that has an older version of the JRE installed, the latest available version of the JRE is automatically downloaded and installed on the device. If the installation of the JRE fails, the Remote SSH session also fails on the device.

Action: Perform the following steps:

1. Manually install JRE version 1.5 or later on the device.
2. Launch the Remote SSH session on the device.
3. In the Remote SSH Java Web Start Launcher, browse to and select the latest version of the Java Web Start executable file that is installed on the device.

Unable to launch a Remote Control session on a Linux device that has an X session running on a display port other than the default display port

Source: ZENworks; ZENworks Configuration Management; Remote Management.

Explanation: If you launch a Remote Control session on a Linux device that has an X session running on a display port other than the default display port (:0), the Remote Control session fails with the following error:

```
RemoteManagement.X_AUTH_FAILURE{30246}
```

Action: Restart the device X session to run on the default display port (:0).

6.3 Troubleshooting Macintosh Devices

- "Unable to launch X11 application on Mac devices" on page 132
- "Unable to perform a Custom Remote Control operation on a Mac device" on page 132
- "Unable to perform a Remote Control Operation on a Mac device" on page 132
- "Unable to connect to the active user session when you launch a remote control session on a Mac OS X Lion 10.7 managed device" on page 133

Unable to launch X11 application on Mac devices

Source: ZENworks; ZENworks Configuration Management; Remote Management.

Explanation: If you launch a X11 application from a Remote SSH session on a Mac device, the Remote Control session fails with the following error:

```
Can't open display.
```

Action: In the `/etc/ssh_config` file, set the `X11Forwarding` value to `Yes`.

Unable to perform a Custom Remote Control operation on a Mac device

Source: ZENworks; ZENworks Configuration Management; Remote Management.

Explanation: If you want to perform a Remote Control operation on a Mac device from the Common Tasks panel, without selecting the device in the ZENworks Control Center, you may encounter the following error:

```
Unable to identify the version of Remote Management service
on the managed device. It is likely that some other
application is running on the specified port.
```

Possible Cause: The Remote Management Viewer is unable to identify that the managed device is a Mac device, and proceeds with the unsupported authentication mode.

Action: Select the Mac managed device in the ZENworks Control Center and launch the Remote Control operation.

Unable to perform a Remote Control Operation on a Mac device

Source: ZENworks; ZENworks Configuration Management; Remote Management.

Explanation: If you attempt to perform a Remote Control operation on a Mac device, after selecting the device from the ZENworks Control Center, you may encounter the following error:

```
Server did not offer supported security type!
```

Possible Cause: No password is set on the Mac device.

Action: Set a password on the Mac device and retry.

Unable to connect to the active user session when you launch a remote control session on a Mac OS X Lion 10.7 managed device

Source: ZENworks; ZENworks Configuration Management; Remote Management.

Explanation: When you launch a remote control session on a Mac OS X 10.7 managed device, you are not connected to the active user session. Instead, you are prompted for the login credentials in the default login screen.

Possible Cause: The default OEM VNC server in Mac OS X 10.7 supports several remote control sessions in parallel (similar to Windows terminal sessions), so support for connecting to the active user session on a Mac OS X 10.7 managed device is discontinued.

Action: To launch a remote control session on the Mac OS X 10.7 managed device and to connect to the active user session without sharing the login credentials:

1. Disable the default screen sharing option on the Mac OS X 10.7 managed device:
   - **1a** Click **System Preferences** icon.
   - **1b** Select the **Sharing** preferences.
   - **1c** Uncheck **Screen Sharing** checkbox within the **Service** list.
2. Download and install Vine Server 4.0 (currently in beta) from the Vine VNC TestPlant (http://www.testplant.com/support/downloads/vine/).
3. Set the VNC password in the **System Preferences** tab of the Vine Server window.
4. Run Vine Server 4.0.

NOTE: Launching of remote control session on a Mac OS X 10.7 managed device with Vine Server installed has not been fully tested and is not supported.

A Cryptographic Details

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

- Section A.1, “Managed Device Key Pair Details,” on page 135
- Section A.2, “Remote Operator Key Pair Details,” on page 135
- Section A.3, “Remote Management Ticket Details,” on page 136
- Section A.4, “Session Encryption Details,” on page 136

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 (TLSv1.2)
Session Cipher: AES256-SHA
SSL Authentication Mode: Mutual/Server

B Best Practices

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

- Section B.1, “On a Windows Device,” on page 137
- Section B.2, “On a Linux Device,” on page 139

B.1 On a Windows Device

Review the followings sections:

- Section B.1.1, “Closing the Remote Management Listener,” on page 137
- Section B.1.2, “Closing Applications Launched During Remote Execute Operation,” on page 138
- Section B.1.3, “Identifying the Remote Operator on the Managed Device,” on page 138
- Section B.1.4, “Performing a Remote Control Session on a device that is already remotely connected,” on page 138
- Section B.1.5, “Determining the Management Console Name,” on page 138
- Section B.1.6, “Using the Aero Theme on Windows 8, Windows 7, Windows Server 2008, and Windows Server 2008 R2 devices,” on page 139
- Section B.1.7, “Enabling the Secure Attention Sequence (Ctrl+Alt+Del) Button when Remotely Controlling a Windows Server 2008 device,” on page 139
- Section B.1.8, “Remote Management Performance,” on page 139

B.1.1 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.1.2 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.1.3 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 2.1.5, "Starting Remote Management Operations on a Windows Device," on page 35.

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.1.4 Performing a Remote Control Session on a device that is already remotely connected

While remote controlling a device which is already in a remote session:

- You will be prompted for a windows login.
- Log into the managed device to terminate the remote desktop session.

B.1.5 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.1.6 Using the Aero Theme on Windows 8, 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 of a Windows Device.

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

B.1.7 Enabling the Secure Attention Sequence (Ctrl+Alt+Del) Button when Remotely Controlling a Windows Server 2008 device

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

B.1.8 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 3.1.6, “Improving the Remote Management Performance on the Windows Managed Device,” on page 81.

B.2 On a Linux Device

Review the following section:

- Section B.2.1, “Remote Management Performance,” on page 139

B.2.1 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 3.2.5, “Improving the Remote Management Performance on the Linux Managed Device,” on page 87.