

# **ZENworks 11 SP3**

## **Test Scenarios for *Remote Management***

This document contains test scenarios for ZENworks 11 SP3 Beta.

### **Purpose of the Test Scenarios**

The purpose of this exercise is to help you become familiar with some of the new features added in the *Remote Management* component of ZENworks 11SP3.

### **Assumptions**

- We assume that you have followed the instructions for installing ZENworks 11 SP3 by using the *ZENworks 11SP3 Installation Guide* (<http://www.novell.com/documentation/zenworks113>).

### **Test Scenarios**

1. [Launching Remote Operations through Join Proxy](#)
2. [Identifying a Remote Operator in an External Certificate Authority Environment](#)
3. [Generating an Abnormal Termination Detected Audit Event](#)
4. [Generating an Authentication Failure Audit Event](#)
5. [Generating an Authentication Success Audit Event](#)
6. [Generating an Intruder Detection Lock Audit Event](#)
7. [Generating Intruder Detection Reset Audit Event](#)
8. [Generating Remote Control Audit Event](#)
9. [Generating a Remote View Audit Event](#)
10. [Generating a Remote Execute Audit Event](#)
11. [Generating Remote Diagnostics Audit Event](#)
12. [Generating a File Transfer Audit Event](#)

## Test Scenario #1: Launching Remote Operations through Join Proxy

### Objective

This scenario will enable you to:

- Learn about the Join Proxy Satellite Server, which allows multiple devices to connect to it for remote management operations. The devices connect to the Join Proxy based on the locations configured for them.
- Remotely manage a device through Join Proxy when you cannot reach the device directly.

### Procedure

Before you start remote managing a device through Join Proxy, you need to first promote a device with the Join Proxy role to make it function as a Join Proxy server.

To promote a device to the Join Proxy role from the Device view:

1. In ZENworks Control Center, click *Devices > Managed*, then click either *Servers* or *Workstations*.
2. In the Servers or Workstations panel, identify the ZENworks 11 SP3 Windows or Linux managed device in the demilitarized zone (DMZ). Select the check box for the Satellite that you want to configure, click *Action*, then click *Configure Satellite Server*.
3. Click the *General* tab, select the check box next to *Join Proxy*, then click *Configure*. The Join Proxy Role Settings dialog box is displayed.
4. In the Join Proxy Role Settings dialog box, specify the *port* on which the Join Proxy listens for connection. The default port number is 7019.
5. Specify the *maximum number of devices* to be allowed to connect to the Join Proxy. The default value is 1000, but you can change it to any value up to 10000.
6. Specify the frequency interval at which the Join Proxy should check to see if the devices are still connected to it. The default value is one minute.

To launch a remote management operation through Join Proxy:

1. Configure the locations which define the NATed environment with one or more of the nearest Join Proxy servers in the zone.

**Note:** Any Primary Server with default configuration, or any device which is promoted to the Join Proxy Satellite role can be added as a Join Proxy server to the Closet Server Rule (CSR). For details about promotion, see the previous set of steps.

2. Select any device which is in the NATed environment from the device list in ZENworks Control Center.
3. Launch a remote management operation on the device. For example, Remote Control, Remote Execute, and so forth.
4. Click *More Options* in the specific remote operation dialog box, verify that the *Route through Join Proxy* check box is selected and that the values for Join Proxy and Join Proxy Port options are populated (host name/IP and port) by default.

**Note:** 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 Join Proxy and Join Proxy Port options are populated. These default values are not populated if the following conditions exist:

- The managed device is not in the configured location
  - The Closest Server list has not flown down to the managed device
  - The Join Proxy server is down
5. Verify the Join Proxy status from ZENworks icon on the target managed device. If Join Proxy configuration details are not updated on the managed device, refresh the ZENworks Configuration Management Agent manually. The Closest Server list and location are updated.
  6. If the Join Proxy IP and Port details are not updated 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.
  7. Click *OK* to launch the remote management operation after selecting the required options.
  8. Enter a password for the remote session if you are using the password mode.

### ***Expected Results***

The remote management operation is successful through Join Proxy even if the managed device is not reachable directly.

### ***Logs***

If you have difficulty in performing the procedure, send us the following files:

- *zcc.log* (From the server from which ZENworks Control Center is launched to initiate a remote management operation.)
- *zmd-messages.log*, *WinVNC.log* and *WinVNCAApp.log* (For Vista and above, from the managed device.)

- `zen-join-proxy.log`  
From the machine that is promoted as a Join Proxy server.

## Test Scenario #2: Identifying a Remote Operator in an External Certificate Authority Environment

### Objective

This scenario will enable you to identify a remote operator when a remote management operation is launched from ZENworks Control Center, in an external Certificate Authority environment with no certificate details.

### Procedure

1. Setup a ZENworks Configuration Management Zone in an external CA environment with at least one Windows device.
2. Apply a remote management policy on the Windows device by selecting *Allow connection when Remote Management Console does not have SSL certificate option* in the security settings of the Remote Management Policy.
3. In ZENworks Control Center, click the *Devices* tab.
4. Click *Servers* or *Workstations* and select a Windows device to which you have applied the above mentioned remote management policy setting.
5. Click *Action*, then select the Remote Management operation you want to perform.  
**Note:** Remote operation is successful even without the certificate information.
6. Click *OK*.
7. Once the connection is established, click the *Visible Signal* on the Windows managed device. The ZENworks Remote Management Remote Operators dialog box is displayed. The name of the remote operator is recorded and displayed even when you do not provide details about the private key and the Certificate corresponding to the private key.

### Expected Results

In an external CA environment, when you launch remote operation on a Windows managed device through ZENworks Control Center:

- The name of the ZENworks Control Center administrator will be displayed instead of *An Unknown User* in the remote operator field.
- The Windows managed device connects to a Primary Server to verify the identity token that is introduced to identify the remote operator on the managed device. When the mode of authentication is *Password* and the managed device fails to connect to a Primary Server, the name of the remote operator is recorded and displayed as *Unknown User*.

**Note:** In such contexts, if you want to make verification of identity token mandatory for the authentication to be successful for security considerations, create the following registry key:

Key: HKLM\Software\Novell\ZCM\Remote Management\Agent

Value: IdentityVerification  
Type: DWORD  
Data: Non-zero number

## **Logs**

If you are unable to successfully perform the procedure, send us the following files:

- *zcc.log* (From the server from which ZENworks Control Center is launched to initiate a remote management operation.)
- *zmd-messages.log*, *WinVNC.log* and *WinVNCAApp.log* (For Vista and above, from the managed device.)

## Test Scenario #3: Generating an Abnormal Termination Detected Audit Event

### Objective

This scenario will enable you to:

- Learn about the Abnormal Termination Detected audit event that is logged when a remote management session is terminated suddenly and abnormally.
- Enable and generate an abnormal termination audit event while remote controlling a device.

### Procedure

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

To edit or delete the Abnormal Termination Detected 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*.

To generate an Abnormal Termination Detected audit event:

1. In ZENworks Control Center, click *Devices > Workstations*
2. Select a Windows XP device, then click *Remote Control* to remotely manage that device.

**Note:** Abnormal termination is detected only in Remote Control operation on Windows XP machines. On Vista Plus machines, Abnormal Termination will not be detected.

3. When the Remote Control operation is in progress, do the following on the management console:
  1. Press *Ctrl+Alt+Del* to invoke the Task Manager.
  2. Click the *Processes* tab, then select `nzrViewer.exe` from the list.
  3. 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.

To view the generated Abnormal Termination Detected audit event details:

### **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 *Abnormal Termination Detected* audit event listed under the *General* category, if enabled.

### **On a Zone**

1. In ZENworks Control Center, click *Dashboard > Events > Agent Events*. In the *Agent Events Summary*, events are categorized as Critical, Major, or Informational based on severity.
2. Perform Steps 3 and 4 listed in the previous section [On a Device](#).
3. Click *Abnormal Termination Detected*. The *Abnormal Termination* events logged in that zone are displayed.

If the Abnormal Termination Detect event is not displayed in ZENworks Control Center, verify that the event is enabled on the device:

1. On the device, open the following file:  
`ZENWORKS_HOME\conf\audit\events\daudit.remote.abnormal.termination.detect.xml`
2. Verify that the event is enabled (`Enable = true`). If it is not enabled, repeat the scenario steps.

### **Expected Results**

After the specified time in *Audit Settings*, the generated abnormal termination detected event is uploaded to the server and displayed in ZENworks Control Center. You can view the abnormal termination detected events logged on a device and also on a zone.



## **Test Scenario #4: Generating an Authentication Failure Audit Event**

### **Objective**

This scenario will enable you to:

- Learn about the Authentication Failure event that 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.
- Learn how to enable and generate an Authentication Failure audit event during a remote session.

### **Procedure**

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.

To edit or delete the *Authentication Failure* event:

1. Click *Authentication Failure* 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*.

To generate 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.

To view the generated Authentication Failure audit event details:

### **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.

### **On a Zone**

1. In ZENworks Control Center, click *Dashboard > 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 Failure* audit event listed under *Authentication*, if enabled.
4. Click any device, then click the *Audit* tab.
5. Click *Authenticator Failure*. The *Authenticator Failure* events logged in that zone will be displayed.

If the Authentication Failure audit event is not displayed in ZENworks Control Center, verify that the event is enabled on the device:

1. On the device, open the following file:  
ZENWORKS\_HOME\conf\audit\events\daudit.remote.auth.fail.xml  
file
2. Verify that the event is enabled (`Enable = true`). If it is not enabled, repeat the scenario steps.

### **Expected Results**

After the specified time in *Audit Settings*, the generated Authentication Failure event is uploaded to the server and displayed in ZENworks Control Center.

**Note:** Some of the reasons displayed as part of Authentication Failure event include:

- Rejection of the certificate of the managed device
- Insufficient rights
- Operation not allowed in policy settings, and so forth

## Test Scenario #5: Generating an Authentication Success Audit Event

### Objective

This scenario will enable you to:

- Learn about the Authentication Success audit event that is generated when authentication is successful during a Remote Management session, either in password or in rights mode.
- Learn how to enable and generate an Authentication Success audit event during a remote session.

**Note:** This is a critical remote audit event that alerts the administrator about the initiation of a remote session on a specific device. In addition, the following basic information about the remote session is also logged during the Authentication Success event:

- Session ID
- Operation
- Authentication Mode

### Procedure

To enable an Authentication Success 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 Success* 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 Success audit event, then click *Apply*.
6. Click *OK* to add the Authentication Success event and close the Add Agent Events dialog box.

To edit or delete an Authentication Success event:

1. Click *Authentication Success* 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*.

To generate 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.

To view the generated Authentication Success audit event details:

### **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 *Authentication Success* audit event listed under the *Authentication* category, if enabled.

### **On a Zone**

1. In ZENworks Control Center, click *Dashboard > 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.

If the Authentication Success event is not displayed in ZENworks Control Center, verify that the event is enabled on the device:

1. On the device, open the following file:  
  
`ZENWORKS_HOME\conf\audit\events\daudit.remote.auth.success.xml`
2. Verify that the event is enabled (`Enable = true`). If it is not enabled, repeat the scenario steps.

***Expected Results***

After the specified time in *Audit Settings*, the generated Authentication Success event is uploaded to the server and displayed in ZENworks Control Center.

## Test Scenario #6: Generating an Intruder Detection Lock Audit Event

### Objective

This scenario will enable you to:

- Learn about the Intruder Detection Lock audit event that is logged 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 Policy settings.
- Learn how to enable and generate an Intruder Detection Lock audit event while remote controlling a device.

### Procedure

To enable an Intruder Detection Lock audit event during 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 *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

To edit or delete the *Intruder Detection Lock* event:

1. Click the *Intruder Detection Lock* event 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*.

To generate an *Intruder Detection* 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.

### **Expected Results**

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.

To view the generated Intruder Detection Lock audit event details:

#### **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 Intruder Detection Lock audit event listed under *Intruder Detection*, if enabled.

#### **On a Zone**

1. In ZENworks Control Center, click *Dashboard > Events > Agent Events*.  
In the *Agent Events Summary*, events are categorized as Critical, Major, or Informational based on severity.
2. Click the plus sign next to *Remote Management* to view the Intruder Detection Lock audit event listed under Intruder Detection, if enabled. Click any device, click *Audit* tab.
3. Click *Intruder Detection Lock*. The Intruder Detection Lock events logged in that zone are displayed.

If the Intruder Detection Lock event is not displayed in ZENworks Control Center, verify that the event is enabled on the device:

1. On the device, open the following file:  
`ZENWORKS_HOME\conf\audit\events\daudit.remote.intruderDet.lock.xml`
2. Verify that the event is enabled (`Enable = true`). If it is not enabled, repeat the scenario steps.

## Test Scenario #7: Generating Intruder Detection Reset Audit Event

### Objective

This scenario will enable you to:

- Learn about the Intruder Detection Reset audit event that is logged when you unblock a device to accept remote management session requests.
- Learn how to enable and generate an Intruder Detection Reset audit event while remote controlling a device.

### Procedure

To enable an Intruder Detection Reset audit event during 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 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.

To edit or delete the Intruder Detection Reset event:

1. Click *Intruder Detection Reset* 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*.

To generate an Intruder Detection Reset audit event:

1. Perform the steps listed in scenario 4 for generating Intruder Detection Lock event.
2. To perform remote operations again on the device that is locked, unlock the device by using one of the following options :
  - Increase the value of *Suspend accepting connections after X successive invalid attempts* in the Remote Management Policy settings.



- Perform the remote management operation only after the time specified in *Automatically start accepting connections after Y minutes* under Intruder Detection in the Remote Management Policy Settings, is over.
  - On the Z-Icon page of the managed device, Click *Remote Management* > click the *Security* tab, then click *Enable accepting connections if currently blocked due to intruder detection*. Click *Ok* in the pop-up that displays *The device is enabled to accept remote management connections*.
3. After you unlock the device and perform remote operations through one of the above listed methods, the device starts accepting connections and the Intruder Detection Reset audit event is logged.

To view the generated Intruder Detection Reset audit event details:

### **On a Device**

1. In ZENworks Control Center, click *Devices* > *Workstations*.
2. Click any device, 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 Intruder Detection Reset audit event listed under *Intruder Detection*, if enabled.

### **On a Zone**

1. In ZENworks Control Center, click *Dashboard* > *Events* > *Agent Events*. In the *Agent Events Summary*, events are categorized as Critical, Major, or Informational based on severity.
2. Click the plus sign next to *Remote Management* to view the Intruder Detection Reset audit event listed under Intruder Detection, if enabled. Click any device, then click the *Audit* tab.
3. Click *Intruder Detection Reset*. The Intruder Detection Reset events logged in that zone will be displayed.

If the Intruder Detection Reset audit event is not displayed in ZENworks Control Center, verify that the event is enabled on the device:

1. On the device, open the following file:  
ZENWORKS\_HOME\conf\audit\events\daudit.remote.intruderDet.reset.xml
2. Verify that the event is enabled (`Enable = true`). If it is not enabled, repeat the scenario steps.

### ***Expected Results***

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

## Test Scenario #8: Generating Remote Control Audit Event

### Objective

This scenario will enable you to:

- Learn about the Remote Control audit event that is logged when a remote operator launches Remote Control Operation on a Windows managed device.
- Learn how to enable and generate Remote Control audit event while remote controlling a device.

**Note:** You can launch Abnormal Termination and Remote Execute audit events only through Remote Control.

### Procedure

To enable a Remote Control 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 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

To edit or delete a *Remote Control* audit event:

1. Click *Remote Control* 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*.

To generate 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.

**Note:** If you launch *Remote Execute* and *File Transfer* through remote control, then the session id is common to both. 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.

To view details of the Remote Control audit event that is generated :

### **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 Remote Control audit event listed under *Session*, if enabled.

### **On a Zone**

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

If the Remote Control audit event is not displayed in ZENworks Control Center, verify that the event is enabled on the device:

1. On the device, open the following file:  
`ZENWORKS_HOME\conf\audit\events\daudit.remote.session.control.xml`
2. Verify that the event is enabled (`Enable = true`). If it is not enabled, repeat the scenario steps.

### **Expected Results**

After the specified time in *Audit Settings*, the generated Remote Control event is uploaded to the server and displayed in ZENworks Control Center. You can view the Remote Control audit events logged on a device and also on a zone. Files transferred or commands executed in the Remote Control session are also displayed in the log.

## Test Scenario #9: Generating a Remote View Audit Event

### Objective

This scenario will enable you to:

- Learn about the Remote View audit event that is logged when a remote operator launches a Remote View session to view the desktop of a Windows managed device.
- Learn how to enable and generate Remote View audit event while remote controlling a device.

### Procedure

To 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.

To edit or delete the *Remote View* audit event:

1. Click *Remote View* 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*.

To generate a *Remote View* audit event:

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

**Note:** You can launch a Remote View audit event through a Remote Control session.

To view details of the Remote View audit event that is generated:

### ***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 on the plus sign to expand the tree view structure of Agent Events.
4. Click the plus sign next to *Remote Management* to view the *Remote View* audit event listed under *Session*, if enabled.

### ***On a Zone***

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

If the Remote View audit event is not displayed in ZENworks Control Center, verify that the event is enabled on the device:

1. On the device, open the following file:  
`ZENWORKS_HOME\conf\audit\events\daudit.remote.session.view.xml`
2. Verify that the event is enabled (`Enable = true`). If it is not enabled, repeat the scenario steps.

### ***Expected Results***

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

## Test Scenario #10: Generating a Remote Execute Audit Event

### Objective

This scenario will enable you to:

- Learn about the Remote Execute audit event that is logged when a remote operator launches a Remote Execute session to run an executable with system privileges on a Windows managed device.
- Learn how to enable and generate Remote Execute audit event while remote controlling a device.

### Procedure

To 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, select the *Remote Execute* 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 Execute* audit event and close the Add Agent Events dialog box.

To edit or delete the *Remote View* audit event:

1. Click *Remote Execute* 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*.

To generate a *Remote View* audit event:

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

**Note:** You can generate a Remote Execute audit event even when you launch a Remote Execute event through a Remote Control session.

To view details of the Remote Execute audit event that is generated:

### **On a Device**

1. In ZENworks Control Center, click *Devices > Workstations*.
2. Click any device, then click *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 *Remote Execute* audit event listed under *Session*, if enabled.

### **On a Zone**

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

**Note:** If multiple commands are executed in a Remote Execute session, an intermediate remote execute audit event is logged with no information on the end time, indicating that the Remote Execute session is still in progress. This is mainly due to the limited size of the audit log.

If the Remote Execute audit event is not displayed in ZENworks Control Center, verify that the event is enabled on the device:

1. On the device, open the following file:  
ZENWORKS\_HOME\conf\audit\events\daudit.remote.session.execute.xml
2. Verify that the event is enabled (`Enable = true`). If it is not enabled, repeat the scenario steps.

### **Expected Results**

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



## Test Scenario #11: Generating Remote Diagnostics Audit Event

### Objective

This scenario will enable you to:

- Learn about the Remote Diagnostics audit event that is logged when a remote operator launches a Remote Diagnostics session to remotely diagnose and analyze the problems on a Windows managed device.
- Learn how to enable and generate Remote Diagnostics audit event while remote controlling a device.

### Procedure

To 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.

To edit or delete the *Remote Diagnostics* audit event:

1. Click *Remote Diagnostics* 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*.

To generate 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.

To view details of the Remote Diagnostics audit event that is generated:

### **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 *Remote Diagnostics* audit event listed under *Session*, if enabled.

### **On a Zone**

1. In ZENworks Control Center, click *Dashboard* > *Events* > *Agent Events*. In the *Agent Events Summary*, events are categorized as Critical, Major, or Informational based on severity.
2. Click the plus sign next to *Remote Management* to view the *Remote Diagnostics* audit event listed under *Session*, if enabled. Click any device, click the *Audit* tab.
3. Click *Remote Diagnostics*. The Remote Diagnostics audit events logged in that zone are displayed.

**Note:** If multiple applications are launched in a Remote Diagnostics session, an intermediate Remote Diagnostics audit event is logged with no information about the end time, indicating that the Remote Diagnostics session is still in progress. This is mainly due to the limited size of the audit log.

If the Remote Diagnostics audit event is not displayed in ZENworks Control Center, verify that the event is enabled on the device:

1. On the device, open the following file:  
ZENWORKS\_HOME\conf\audit\events\daudit.remote.session.diagnostics.xml
2. Verify that the event is enabled (`Enable = true`). If it is not enabled, repeat the scenario steps.

### **Expected Results**

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

## Test Scenario #12: Generating a File Transfer Audit Event

### Objective

This scenario will enable you to:

- Learn about the File Transfer audit event that is logged when a remote operator launches a File Transfer session to transfer files between the management console and the Windows managed device.
- Learn how to enable and generate a File Transfer audit event while remote controlling a device.

### Procedure

To enable a File Transfer 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 *File Transfer > 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 *File Transfer* audit event and close the Add Agent Events dialog box.

To edit or delete the *File Transfer* audit event:

1. Click *File Transfer* 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*.

To generate 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:** You can generate a File Transfer audit event even when you launch it either through a Remote Control or Remote Diagnostics session.

To view details of the File Transfer audit event that is generated:

### **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 *File Transfer* audit event listed under *Session*, if enabled.

### **On a Zone**

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

**Note:** If multiple file operations are executed in a File Transfer session, an intermediate File Transfer audit event is logged with no information about the end time, indicating that the File Transfer session is still in progress. This is mainly due to the limited size of the audit log.

If the File Transfer audit event is not displayed in ZENworks Control Center, verify that the event is enabled on the device:

1. On the device, open the following file:  
`ZENWORKS_HOME\conf\audit\events\daudit.remote.session.fileTransfer.xmlfile`
2. Verify that the event is enabled (`Enable = true`).  
If it is not enabled, repeat the scenario steps.

If you are unable to successfully perform any of the above scenarios, send us the following logs:

1. `zcc.log` from the server from which ZENworks Control Center is launched to initiate a remote management operation.
2. `zmd-messages.log`, `WinVNC.log` and `WinVNCAApp.log` (for Vista and above) from the managed device.

### **Expected Results**

After the specified time in *Audit Settings*, the generated Remote Control event is uploaded to the server and displayed in ZENworks Control Center. You can view the File Transfer audit events logged on a device and also on a zone.

