

ZENworks 11 SP 3

Test Scenarios for *Audit*

This document contains test scenarios for ZENworks 11 SP3 Beta.

Purpose of the Test Scenarios

The purpose of these exercises is to help you become familiar with some of the new features in the *Audit* component of ZENworks 11 SP3.

Assumptions

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

Test Scenarios

1. [Enabling and Viewing the Settings Modified Audit Event](#)
2. [Enabling and Viewing the User Logged In Audit Event](#)
3. [Enabling and Viewing the Device Modified Audit Event](#)
4. [Using the Configure Audit Settings right](#)
5. [Using the View Audit Dashboard right](#)
6. [Using the View Audit Event Details right](#)
7. [Performing an Advanced Search of audit events](#)
8. [Running a Saved Ad-Hoc View From a Particular Folder](#)
9. [Creating a Crosstab Report and Saving it Under a Particular Destination Folder](#)

ZENworks Audit - Overview

The Audit feature enables administrators to record various changes or actions that occur in the zone. The recorded information can be audited later for compliance. It provides the ability to centrally monitor all the activities pertaining to Primary Servers, Satellites and Managed Devices. You also can generate reports for the ZENworks Audit events and view them either in the ZENworks Control Center Dashboard or by using the ZENworks Reporting feature.

ZENworks Audit includes two types of audit events:

Change Audit Events: These events capture any configuration changes made by the ZENworks administrators to the zone. For example, an event that records the activity of an administrator assigning a bundle to a device.

Agent Audit Events: These events capture actions that occur on the ZENworks managed devices. Hence, they are also called Device Events. For example, an audit event that records the activity of login by a ZENworks user on a managed device.

Using these test scenarios you can:

1. Configure audit events:
 - Change Events - [Enabling and Viewing the Settings Modified Audit Event](#)
 - Agent Events - [Enabling and Viewing the User Logged In Audit Event](#)
2. Override an agent event that is configured at the zone for a managed device - [Enabling and Viewing the Device Modified Audit Event](#)
3. Configure the Audit-related rights:
 - Configure Audit Settings - [Using the Configure Audit Settings Right](#)
 - View Audit Dashboard - [Using the View Audit Dashboard Right](#)
 - View Audit Events - [Using the View Audit Event Details Right](#)
4. Perform an advanced search - [Performing an Advanced Search of Audit Events](#)
5. Generate and view reports
 - Run an existing view: [Running a Saved Ad-Hoc View From a Particular Folder](#)
 - Create a Crosstab report: [Creating a Crosstab Report and Saving it Under a Particular Destination Folder](#)

Test Scenario #1: Enabling and Viewing an Audit Change Event (*Settings Modified*)

Objective

This scenario will enable you to configure a change audit event, make the relevant change, and then view the generated event. For this scenario we have used the *Settings Modified* audit event.

Procedure

Part 1

To configure the *Settings Modified* audit event:

1. In the left navigation pane of ZENworks Control Center, click *Configuration*.
2. In the *Configuration* tab, under *Management Zone Settings*, click *Audit Management*.
3. Click *Events Configuration*.
4. Under *Change Events*, click *Add* to display the *Add Change Events* dialog box.
5. Expand the Change Events tree, then select *Settings Modified*.
6. In the *Event Settings* section, set the *Event Classification* as Informational.
7. Specify the *Days to Keep* as 30.
8. Select *Send Log Message via Email* notification type.

Note: To configure the email server settings, see [E-mail Notification](#).

9. In the *From* field, specify a valid sender email address.
10. In the *To* field, specify valid recipient email addresses. More than one email address can be specified by separating them with commas.
11. Select *Send an SNMP Trap*.

Note: To configure the SNMP Trap settings, see [SNMP Traps](#).

12. Select *Send message via UDP*.

Note: To configure the UDP settings, see [UDP Forwarder](#).

13. Select *Log message to a local file*.
14. Click *OK* to add the event and close the *Add Change Events* dialog box.


Part 2

To modify a setting (for example, to add a system variable):

1. In the left navigation pane of ZENworks Control Center, click *Configuration*.
2. In the *Configuration* tab, under the *Management Zone Settings* list, click *Device Management*.
3. Click *System Variables*.
4. Click *Add*, to add a non-existent variable. For example, a variable with the name *TEST* and value *TESTVALUE*.
5. Click *OK*. The *System Variable* page is displayed.
6. Click *OK*.

Part 3

To view the *Settings Modified* audit event:

1. After completing Part 2, wait for 5 minutes, then, in the left navigation pane of ZENworks Control Center, click *Dashboard*.
2. Under *Audit > Zone Audit*, click *Events*.
3. In the *Change Events* tree, select *Settings Modified*. The *Settings Modified* link is displayed.
4. Click *Settings Modified*. The *Event Details* information is displayed in a pane below the link.
5. In the *Event Details* pane, click . The details of the event are displayed in a new pop-out window.

Expected Results

- After adding the *Settings Modified* event from the *Add Change Events* dialog box, the event is seen in the *Events Configuration > Change Events* page.
- After adding the system variable, the *Settings Modified* event is displayed in the *Dashboard > Audit > Zone Audit > Events* page.
- In the *Event Details* pane, the name and value of the new system variable are displayed. Also, other details such as *Category*, *Classification*, *Date and Time*, *IP Address*, *Initiator*, *Session ID* and *Targets* are displayed. The *IP Address* displays the IP address of the machine from which ZENworks Control Center was launched to add the system variable.

Note: In some cases, the IP address might be of the intermediate router or proxy, depending on the network configuration.

- The event details are also found in the *AuditLog.csv* file. This file is located in the *%ZENWORKS_HOME%\logs* folder on a Windows Primary Server and in the */var/opt/novell/log/zenworks* folder on a Linux Primary Server.
- The audit event information is received by all of the configured email recipients.
- SNMP traps carrying audit event information are received by the configured SNMP trap destination.
- UDP messages carrying audit event information are received by the UDP destination system.

Logs

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

- *zcc.log*
- *services-messages.log*
- *loader-messages.log*

Log files location:

- Windows Primary Server: *%ZENWORKS_HOME%\logs*
- Linux Primary Server: */var/opt/novell/log/zenworks*

Change Events

The Change Events include the following categories and events:

Category	Event	Description
ZENworks Endpoint Security Management	Endpoint Security Policy Modified	Generates an event when an Endpoint Security Policy is modified. For more information on this ZESM Audit event, see the <i>ZENworks Endpoint Security Policy</i> scenarios in the ZENworks 11 SP3 Scenarios.zip file.
ZENworks System	Settings	Generates an event when any settings are modified.
	User Source	Generates an event when user sources and user source connections are added, removed or modified.
	Administration	Generates an event when

Category	Event	Description
		changes are made to the ZENworks Control Center, Administrator, Credential Vault, Roles and Registration components.
	Location	Generates an event when Locations, Network Environments are created, modified or deleted.
	System Update	Generates an event when system updates are downloaded, deployed and canceled.
	Licensing	Generates an event when product licenses are activated or deactivated.
	Devices	Generates an event when changes are made to Devices, Device Folders, Device Groups, satellite Servers or Device Quick Tasks.
	Bundles	Generates an event when changes are made to Bundles, Bundle Sandboxes, Bundle Folders and Bundle Groups.
	Policies	Generates an event when changes are made to Policies, Policy Folders and Policy Groups.
	Discovery Task	Generates an event when Discovery Tasks are created, modified, deleted, launched or aborted.
	Deployments Tasks	Generates an event when Deployment Tasks are created, modified, deleted, launched or aborted.
	Subscriptions	Generates an event when any changes are made to the Subscriptions component.
	Zone Sharing	Generates an event when Zone Sharing is suspended, added, modified or removed.
	Patch	Generates an event when Patches are enabled or disabled

Category	Event	Description
		and when Patch Policies are created or modified.
Full Disk Encryption	Full Disk Encryption Policy Modified	<p>Generates an event when a Full Disk Encryption policy is modified.</p> <p>For more information on this audit event, see the Full Disk Encryption Beta Scenarios in the ZENworks 11 SP3 Beta Scenarios.zip file.</p>

Test Scenario #2: Enabling and Viewing an Audit Agent Event (*User Logged In*)

Objective

This scenario will enable you to enable you to configure an agent audit event, and to view the generated event after it has been performed on the device. For this scenario, we have used the *User Logged In* event.

Procedure

Part 1

To configure the *User Logged In* audit event:

1. In the left navigation pane of ZENworks Control Center, click *Configuration*.
2. In the *Configuration* tab, from the *Management Zone Settings* list, click *Audit Management*.
3. Click *Event Configuration*.
4. Click the *Agent Events* tab, then click *Add* to display the *Add Agent Events* dialog box.
5. Expand the Agent Events tree, then select the *User Logged In* event.
6. In the *Event Settings* section, select Major as the *Event Classification*.
7. Specify *Days to Keep* as 60.
8. Select *Send Log Message via Email* notification type.
Note: To configure the email server settings, see [E-mail Notification](#).
9. In the *From* field, specify a valid sender email address.
10. In the *To* field, specify valid recipient email addresses. More than one email address can be specified by separating them with commas.
11. Select *Send an SNMP Trap*.
Note: To configure the SNMP Trap settings, see [SNMP Traps](#).
12. Select *Send message via UDP*.
Note: To configure the UDP settings, see [UDP Forwarder](#).
13. Select *Log message to a local file*.
14. Click *OK* to add the event and close the *Add Agent Events* dialog box.

Part 2


To generate the *User Logged In* event on a Windows managed device:

1. Add a User Source to the zone.

Note: To configure a User Source, see [Adding User Sources](#).
2. Refresh the Windows managed device, by selecting the chosen device from the *Devices* panel and by using the *Refresh Device* quick task.
3. Log in to the chosen Windows managed device.
4. Right click on the *ZENworks Icon* in the Windows system tray, then select *Login*.
5. In the *Login* dialog box, type a valid user name (exists in the configured User Source), the correct password, then click *OK*.

Part 3

To view the *User Logged In* audit event:

1. After completing Part 2, wait for an hour, and open the device summary for the device on which the user login action was performed.
2. Click the *Audit* tab.
3. In the *Agent Events* tree, select the *User Logged In* event.
4. If a *User Logged In* row is visible, click *User logged in successfully*.
5. In the *Event Details* section displayed below the link, click  .

Expected Results

- After you add the *User Logged In* event from the *Add Agent Events* dialog box, the event is displayed in the *Events Configuration > Agent Events* page.
- After the user (from the user source) has successfully logged in, the *User Logged In* event is displayed in the *Audit > Agent Events* page for the given managed device.
- In the *Event Details* section, the name of the user who logged in is displayed as the *Initiator*. Also, details such as *Category*, *Classification*, *Date and Time*, *Device*, and *Message* are also displayed.
- The same event is also seen in the *Dashboard > Audit > Zone Audit > Events > Agent Events* page.

Logs

If you are unable to successfully perform the scenario, send us the following files.

- `%ZENWORKS_HOME%\logs\LocalStore\zmd-messages.log` (from the Windows managed device on which the action was performed).
- `%ZENWORKS_HOME%\conf\audit\events` folder (from the Windows managed device where the action was performed).
- `services-messages.log` (Primary Server)
- `loader-messages.log` (Primary Server)

Log files location:

- Windows Primary Server: `%ZENWORKS_HOME%\logs`
- Linux Primary Server: `/var/opt/novell/log/zenworks`

Agent Events

The Agent Events include the following categories and events:

Category	Event	Description
User Management	<ul style="list-style-type: none">• User Logged In• User Logged out• User Login Failed• Change Password Event• Disconnected User Login Event	Generates events for changes associated with a user login or logout.
Remote Management	General	Generates an event when an abnormal termination is detected. For more information on the Remote Management Audit events, see the <i>Remote Management</i> scenarios in the ZENworks 11 SP3 Beta Scenarios.zip file.
	Authentication	Generates an event when the authentication succeeds or fails.
	Intruder Detection	Generates events when the Intruder Detection is locked or reset.
	Session	Generates an event when changes are made related to remote sessions and file transfer.
ZENworks Endpoint Security	Removal Storage	Generates events for changes

Category	Event	Description
Management		related to removal storage. For example, count of files copied to the removal storage.
	Licensing	Generates events when product licenses are activated or deactivated.
	Informational Events	Generates events when changes a policy is activated or when security changes are made to Locations or Network Environments.
ZENworks Adaptive Agent	Configuration Location/Network Environment	Generates an event when configuration changes are made to a Location or Network Environment.

Test Scenario #3: Enabling and Viewing the *Device Modified* Audit Event

Objective

This scenario will enable you to configure a typical audit event, override its settings for a particular managed device and then view the event after the changes have been made on that device. The *Device Modified* event has been used as the example for this scenario.

Procedure

Part 1

To enable the *Device Modified* audit event:

1. In the left navigation pane of ZENworks Control Center, click *Configuration*.
2. In the *Configuration* tab, from the *Management Zone Settings* list, click *Audit Management*.
3. Click *Event Configuration*.
4. In the *Change Events* tab, click *Add* to display the *Add Change Events* dialog box.
5. Expand the *Change Events* tree, then select the *Device Modified* event.
6. In the *Event Settings* section, select *Informational* as the *Event Classification*.
7. Specify the *Days to Keep* as 30.
8. Click *OK* to add the event, then close the *Add Change Events* dialog box.

Part 2

To override the configuration of the *Device Modified* event for a given device folder:

1. In the left navigation pane of ZENworks Control Center, click *Devices*.
2. Click *Workstation Details*.
3. Click on the *Settings* tab.
4. Click *Audit Management*, then click *Events Configuration*.
5. Select the italicized *Device Modified* event under *Change Events*, then click *Action>Override*. The *Edit Properties* dialog box is displayed.
6. Select *Major* as the *Event Classification*.
7. Specify *Days to Keep* as 60.
8. Click *OK* to add the event and then close the *Edit Properties* dialog box.


Part 3

To mark a device as *Test* under the *Workstations* folder:

1. In the left navigation pane of ZENworks Control Center, click *Devices*.
2. Click the *Workstations* folder.
3. Click an existing managed device to open the device *Summary*.
4. In the device *Summary* page, click the *Set* option next to *Test Device*.

Part 4

To view the *Device Modified* audit event:

1. After completing Part 3, wait for a few minutes (minimum 5), then open the device *Summary* page for the device that was marked as a Test device.
2. Click the *Audit* tab.
3. In the *Change Events* tree, select the *Device Modified* event.
4. If a *Device Modified* link is displayed, click on it. The *Event Details* are displayed in the lower part of the screen.
5. In the *Event Details* pane, click .

Expected Results

- After you add the *Device Modified* event from the *Add Change Events* dialog box, it is displayed in the *Events Configuration > Change Events* page.
- After you mark the device as *Test*, the event *Device Modified* is displayed in the *Audit > Change Events* page.
- In the *Event Details* screen, the message *Device set as Test Device* is displayed and the *Classification* is displayed as *Major*. Also, other details such as *Category*, *Date and Time*, *IP Address*, *Initiator*, *Session ID* and *Targets* are also displayed. The *IP Address* will display the IP address of the machine where ZENworks Control Center was launched to add the system variable. In some scenarios, the IP address might be of the intermediate router or proxy, depending on the network configuration.
- The same event is also seen in the *Dashboard > Audit > Zone Audit > Events* page.

Logs

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

- zcc.log*

- services-messages.log*

- loader-messages.log*

Log files location:

- Windows Primary Server: *%ZENWORKS_HOME%\logs*

- Linux Primary Server: */var/opt/novell/log/zenworks*

Test Scenario #4: Using the *Configure Audit Settings* Right

Objective

This scenario will enable you to set the *Configure Audit Settings* right at the zone or device level.

Procedure

Part 1

To enable the *Configure Audit Settings* right:

1. In the left navigation pane of ZENworks Control Center, click *Configuration*.
2. In the *Configuration* tab, under *Administrators*, click *New>Administrator*.
3. Create an Administrator named *zoneAdmin*.
4. Click the *zoneAdmin* link.
5. Click the *Rights* tab.
6. Under the *Assigned Rights* section, click *Add>Zone Rights*.
7. Allow the *Configure Audit Settings* right.
8. Click *OK*.
9. Click *Apply*.
10. Repeat Steps 2 and 3 to create another administrator named *deviceAdmin*.
11. Click the *Rights* tab.
12. Under the *Assigned Rights* section, click *Add Device Rights*.
13. Add the context as *Devices*, and allow the *Configure Audit Settings* right.
14. Click *OK*.
15. Click *Apply*.

Part 2

To configure the audit settings:

1. Log into ZENworks Control Center as *zoneAdmin*.
2. In the left navigation pane of ZENworks Control Center, click *Configuration*.
3. In the *Configuration* tab, under the *Management Zone Settings* list, click *Audit Management*.

4. Click *Event Configuration*.
5. Under *Change Audit Events*, click *Add* to display the *Add Change Events* dialog box.
6. Click the *Settings* tab.
7. Click *Audit Management*, then click *Events Configuration*.
8. Select any event(s).
9. Select Major as the *Event Classification*.
10. Specify *Days to Keep* as 60.
11. Click *OK* to add the event, then close the *Edit Properties* dialog box.
12. In left navigation pane of ZENworks Control Center, click *Devices*.
13. Navigate to any device or folder.
14. Click the device or folder *Details*.
15. Click the *Settings* tab.
16. Click *Audit Management*, then click *Events Configuration*.
17. Verify that the page is disabled and that the administrator cannot configure events.

Part 3

To configure the audit settings at the Device level:

1. Log into ZENworks Control Center as *deviceAdmin*.
2. In the left navigation pane of ZENworks Control Center, click *Devices*.
3. Navigate to a device or folder and view its details.
4. In the *Settings* tab, click *Audit Management*.
5. Click *Event Configuration*.
6. Under *Change Audit Events*, click *Add* to display the *Add Change Events* dialog box.
7. Select any event(s).
8. Select Major as the *Event Classification*.
9. Specify *Days to Keep* as 60.

10. Click *OK* to add the event, then close the *Edit Properties* dialog box.
11. In the left navigation pane of ZENworks Control Center, click *Configuration*.
12. Under the *Management Zone Settings* list, click Audit management.
13. Click *Events Configuration*.
14. Verify that the page is disabled and that the administrator cannot configure events.

Expected Results

- After configuring the *Configure Audit Settings* right at the zone level, the administrator (zoneAdmin) is able to configure the audit events. However, the same administrator is not able to configure the events at a device level.
- After configuring the *Configure Audit Settings* right at the device level, the administrator (deviceAdmin) is able to configure the audit events at the device level. However, the same administrator is not able to configure the events at the zone level.

Logs

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

- zcc.log*
- services-messages.log*
- loader-messages.log*

Log files location:

- Windows Primary Server: %ZENWORKS_HOME%\logs
- Linux Primary Server: /var/opt/novell/log/zenworks

Test Scenario #5: Using the *View Audit Dashboard* Right

Objective

This scenario will enable you to grant the *View Audit Dashboard* right at the zone level and grant the *View Audit Log* right at the Device level.

Procedure

Part 1

To enable the *View Audit Dashboard* right:

1. In the left navigation pane of ZENworks Control Center, click *Configuration*.
2. In the *Configuration* tab, under *Administrators*, click *New> Administrator*.
3. Create an administrator named *zoneAdmin*. *ZoneAdmin* is listed below the Administrator section.
4. Click *zoneAdmin*. The *zoneAdmin* details page is displayed.
5. Click the *Rights* tab.
6. Below the *Assigned Rights* section, click *Add>Zone Rights*.
7. Allow the *View Audit Dashboard* right.
8. Click *OK*.
9. Click *Apply*.
10. Repeat Steps 2 and 3 to create another administrator named *deviceAdmin*.
11. Click the *Rights* tab.
12. Below the *Assigned Rights* section, click *Add Device Rights*.
13. Add the context as *Devices*, and allow the *View Audit Log* right.
14. Click *OK*.
15. Click *Apply*.

Part 2

To view the Audit Dashboard:

1. Log in to ZENworks Control Center as *zoneAdmin*.
2. In the left navigation pane of ZENworks Control Center, click *Dashboard*.

3. Click any event. The *Events* tab is displayed, listing the events related to the selected event.
4. Navigate to any device or folder.
5. Click the device or folder details.
6. Verify that you can view a tab called *Audit*.

Part 3

To view the Audit Log at the Device level:

1. Log in to ZENworks Control Center as *deviceAdmin*.
2. In the left navigation pane of ZENworks Control Center, click *Devices*.
3. Navigate to a device or folder and view its details.
4. Click the *Audit* tab. Check if you can click on the events in the events tree in the left side panel and see the related events.
5. In the left navigation pane of ZENworks Control Center, click *Dashboard*.
6. Verify that you can view the *Audit* tab.

Expected Results

- After configuring the *View Audit Dashboard* right at the zone level, the administrator (zoneAdmin) is able to view the *Audit* tab and view the events. However, the same administrator is not able to view the *Audit* tab at a device level.
- After configuring the *View Audit Log* at the Device level, the admin (deviceAdmin) is able to view the audit events at the Device level. But the same admin is not able to view the Audit tab at the Dashboard level.

Logs

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

- zcc.log*
- services-messages.log*
- loader-messages.log*

Log files location:

- Windows Primary Server: *%ZENWORKS_HOME%\logs*
- Linux Primary Server: */var/opt/novell/log/zenworks*

Test Scenario #6: Using the *View Audit Event Details* Right

Objective

This scenario will enable you to use the *View Audit Events* right at the zone or device level.

Procedure

Part 1

To enable the *View Audit Events* rights:

1. In the left navigation pane of ZENworks Control Center, click *Configuration*.
2. In the *Configuration* tab, under *Administrators*, click *New> Administrator*.
3. Create an administrator named *zoneAdmin*. *ZoneAdmin* is listed below the *Administrator* section.
4. Click *zoneAdmin*. The *zoneAdmin* details page is displayed.
5. Click the *Rights* tab.
6. Below the *Assigned Rights* section, click *Add>Zone Rights*. The *Zone Rights* dialog box is displayed.
7. Allow the *View Audit Events* Right.
Note: The *View Audit Dashboard* right is automatically granted.
8. Click *OK*.
9. Click *Apply*.
10. Repeat Steps 2 and 3 to create another administrator named *deviceAdmin*.
11. Click the *Rights* tab.
12. Below the *Assigned Rights* section, click *Add Device Rights*.
13. Add the context as *Devices*, and allow the *View Audit Events* right.
Note: The *View Audit Log* right is automatically granted.
14. Click *OK*.
15. Click *Apply*.

Part 2

To view the Audit Event Details at the zone level:

1. Log in to ZENworks Control Center *as zoneAdmin*.
2. In the left navigation pane of ZENworks Control Center, click *Dashboard*. The Audit Dashboard is displayed.
3. Select any event. The Events tab is displayed listing the events related to the clicked event.

Note: The events are displayed as links.

4. Click any event link. The *Event Details* section is displayed in the lower part of the screen.

Part 3

To view the Audit Log at the Device level:

1. Log in to ZENworks Control Center as the *deviceAdmin*.
2. In the left navigation pane of ZENworks Control Center, click *Devices*.
3. Navigate to a device or folder and view its details.
4. Click the *Audit* tab.
5. In the left panel, verify that you can select events in the Events Trees and that you can view the related events.
6. Verify that the listed events are all links.
7. Click any event. The details of the event are displayed in the *Event Details* section, in the lower part of the screen.

Expected Results

- After configuring the *View Audit Events* right at the zone level, the administrator (zoneAdmin) is able to view the *Audit* tab and the events details for the selected events.
- After configuring the *View Audit Events* right at the device level, the admin deviceAdmin is able to see the audit events at the Devices level and view the event details for the events.

Logs

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

- *zcc.log*
- *services-messages.log*
- *loader-messages.log*

Log files location:

- Windows Primary Server: *%ZENWORKS_HOME%\logs*
- Linux Primary Server: */var/opt/novell/log/zenworks*

Test Scenario #7: Performing an Advanced Search of Audit Events

Objective

This scenario will enable you to use the advanced search option to find the relevant audit events more easily.

Procedure

1. Log in to ZENworks Control Center.
2. In the left navigation pane of ZENworks Control Center, click *Dashboard*. The Audit Dashboard is displayed.
3. Click the *Events* tab. The audit events tree is displayed.
4. Click any category that has events. Choose an event category rather than individual events, in order to search more data. The view will list all events related to the selected event or category in the tree.
5. Click the drop-down option next to the search box at the top of the events table.
6. Select *Advanced Search*. The Advanced Search dialog box is displayed.
7. Enter the relevant search criteria.
8. Select the *Save Search as* option and provide a name for this search.
9. Click *Search*.

Expected Results

- The search results are displayed and the name of the search being displayed is shown at the top, adjacent to the search box. The *Clear* option is displayed next to the search name that will allow you to clear the search results.
- The search has been saved and will be available to you anytime. This search will now be listed in the drop-down. You can click on a saved search entry in this drop-down to list the results.

Logs

If you are unable to successfully perform the scenario, send us the following file:

- zcc.log

Log files location:

- Windows Primary Server: %ZENWORKS_HOME%\logs
- Linux Primary Server: /var/opt/novell/log/zenworks

Note:

- A saved search can be edited, renamed or deleted when required.
- Pre-saved (canned) searches are available (example, *Critical Events*). These are not editable.
- You can perform an advanced search and choose not to save it.

Test Scenario #8: Running a Saved Ad-Hoc View From a Particular Folder

Objective

This scenario will enable you to run a saved Ad-Hoc view from a particular folder.

Procedure

1. Using a Web browser navigate to the `https://<ip address:non-sslport>/jasperserver-pro` site.

Note: The recommended browsers are:

- Mozilla Firefox 4.0 or higher
 - Microsoft Internet Explorer 7 (certified), 8 (certified), 9.0 (certified), 10.0 (v5.1)
 - Google Chrome 6.0 or higher
2. Replace the IP address with the IP of your ZENworks Reporting Server.
 3. In the Login screen specify values for the *Organization*, *User ID* and *Password* fields.
 4. In the Home screen click *View>Repository*.
 5. In the left pane, under *root*, expand the tree and navigate to *Organizations>Organization>Reports>ZENworks>Audit>Predefined Reports*. The available predefined reports are displayed in the right pane.
 6. Click *Failed login attempts for managed devices_view*. This view displays the following objects: *Event Name*, *Event Created On*, *Failure Reason* as Columns, and the *User Name as Group* and *Failure Reason* as Filters.

This provides information about all the user management events with their event name, date on which the events were created and what was the reason for failure.
 7. Verify the *Failure Reason* for all the failed events and also verify the other views under *Predefined Reports*.

Expected Results

- You can access all the views saved under the given location.

Test Scenario #9: Creating a Crosstab Report and Saving it Under a Particular Destination Folder

Objective

This scenario will enable you to create a report in Crosstab and to save it in a particular folder.

Procedure

1. Using a Web browser navigate to the `https://<ip address>:non-sslport/<jasperserver-pro>` site.

Note: The recommended browsers are:
 - Mozilla Firefox 4.0 or higher
 - Microsoft Internet Explorer 7 (certified), 8 (certified), 9.0 (certified), 10.0 (v5.1)
 - Google Chrome 6.0 or higher
2. Replace the IP address with the actual IP of your ZENworks Reporting Server.
3. In the *Login* screen, specify values for the *Organization*, *User ID* and *Password* fields.
4. In the Home screen click *Create Ad Hoc View*.
5. In the *Data Chooser* screen click *Domains*.
6. Expand the tree by clicking *Organizations>Organization>Domains>ZENworks Audit Domain*.
7. Click *Choose Data...*
8. From the *Source* panel on the left ,click *ZENworks Change Summary* and drag and drop it in the *Selected Fields* pane on the right.
9. Click *Table*.
10. From the left pane drag and drop the *Event Name*, *Device Name*, *Event created On*, and the *Event Initiator Name* into the *Columns* field.
11. In the drop-down menu that lists *Table* as the default value, select *Crosstab*. This view displays the count of all the objects which have been selected.
12. To save the report, click the *Save* icon, then select *Save Ad Hoc View and Create Report*.
13. Specify an appropriate *Data View Name*.
14. Specify an appropriate *Report Name* (for example, *Change Summary Count Report*).
15. To save the report navigate to *root>Organizations>Organization>Reports* (or any other location where you want to save the report) and click *Save*.

16. To view the saved report click *View>Repository*.
17. On the left pane navigate to the path (in this scenario *Organizations>Organization>Reports*) to view the saved report in the right pane. Click to open the report.

Note: Similarly you can create your own customized reports and views in the cross tab and save them in required folders.

Expected Results

- You can create and save reports and views in a particular location.