ZENworks 2020 Update 3
ZENworks Control Center Reference

November 2022

Legal Notice

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/.

About This Guide

This *ZENworks Control Center Reference* explains how to access, navigate, customize, and use ZENworks Control Center, the administrative console used to manage your ZENworks system. The guide includes the following sections:

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 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 Documentation Web site.

Contents

1 Accessing ZENworks Control Center

You use ZENworks Control Center to configure system settings and perform management tasks in your Management Zone.

ZENworks Control Center is installed on all ZENworks Servers in the Management Zone. You can perform all management tasks on any ZENworks Server.

1.1 Accessing ZENworks Control Center

1 Using a Web browser that meets the requirements listed in "Administration Browser Requirements", enter the following URL:

```
https://ZENworks_Server_Address:port
```

Replace *ZENworks_Server_Address* with the IP address or DNS name of the ZENworks Server. You only need to specify the *port* if you are not using one of the default ports (80 or 443). ZENworks Control Center requires an HTTPS connection; HTTP requests are redirected to HTTPS.

The login dialog box is displayed.

2 In the **Username** field, type `Administrator` (the default) or another ZENworks administrator name that you previously created in ZENworks Control Center (see the *ZENworks Administrator Accounts and Rights Reference* for more information).

To log in to ZENworks Control Center as an administrator who has been created based on users in a user source who has the same name as a previously created ZENworks administrator, specify the username as `name@usersource`.

For example, if the administrator has the name `testadmin` and belongs to the user source named `myserver`, specify the username as `testadmin@myserver`.

3 In the **Password** field, do one of the following:

- If you are logging in through the default Administrator account, specify the Administrator password that you created during installation.

- Specify the password for the administrator name that you created in ZENworks Control Center.

To prevent unauthorized users from gaining access to ZENworks Control Center, the administrator account is disabled after three unsuccessful login attempts, and a 60-second timeout is enforced before you can attempt another login. To change these default values, see Section 3.1, "Changing the Default Login Disable Values," on page 15.

4 Click **Login** to display ZENworks Control Center.

To log in again as a different administrator, click the **Logout** option in the upper right corner of the ZENworks Control Center window, then when the login dialog box is displayed, log in as a different administrator.

Performing concurrent operations in multiple sessions of ZENworks Control Center might result in an exception

If ZENworks Control Center is opened in multiple browsers and you choose to perform an operation on an object in one browser when the same object is being modified or accessed in the other browser, an exception might occur.

For example, an error might occur if you update an object in one session of ZENworks Control Center when the same object has been deleted in another session of ZENworks Control Center.

1.2 Restricting Access to ZENworks Control Center

ZENworks Control Center is available on each ZENworks Primary Server for ZENworks administration. The access to ZCC and webapps can be restricted by following a few steps. For more information on restricting access, see the ZENworks Control Center (ZCC) and Admin Services section in the ZENworks Best Practices Guide.

1.3 Accessing ZENworks Control Center through Novell iManager

ZENworks includes a Novell plug-in module (`.npm`) that you can use to access ZENworks Control Center from Novell iManager, which is a management console used by many Novell products.

The ZENworks Control Center plug-in supports iManager 2.7 only. It does not support iManager 2.6 or 2.5; it will install to these versions but does not work.

To install the ZENworks Control Center plug-in for iManager:

1 On the server where iManager is located (or on a device that has access to the iManager server), open a Web browser to the ZENworks download page:

   https://*server*/zenworks-setup

   where *server* is the DNS name or IP address of a ZENworks Server.

2 In the left navigation pane, click **Administrative Tools**.

3 Click **zcc.npm** and save the file to a location on the iManager server.

4 Follow the instructions in the *Novell iManager 2.7 Administration Guide* (http://www.novell.com/documentation/imanager27/) to install and configure the plug-in module.

5 Log into iManager.

6 Click the ZENworks icon at the top of the page.

7 Enter the ZENworks Control Center URL:

   `https://ZENworks_Server_Address:port`

   Replace *ZENworks_Server_Address* with the IP address or DNS name of the ZENworks Server. You only need to specify the *port* if the ZENworks server is not using the default port (80 or 443).

8 Click the ZENworks icon to launch ZENworks Control Center.

2 Navigating ZENworks Control Center

The following Workstations page represents a standard view in ZENworks Control Center:

Figure 2-1   *ZENworks Control Center*
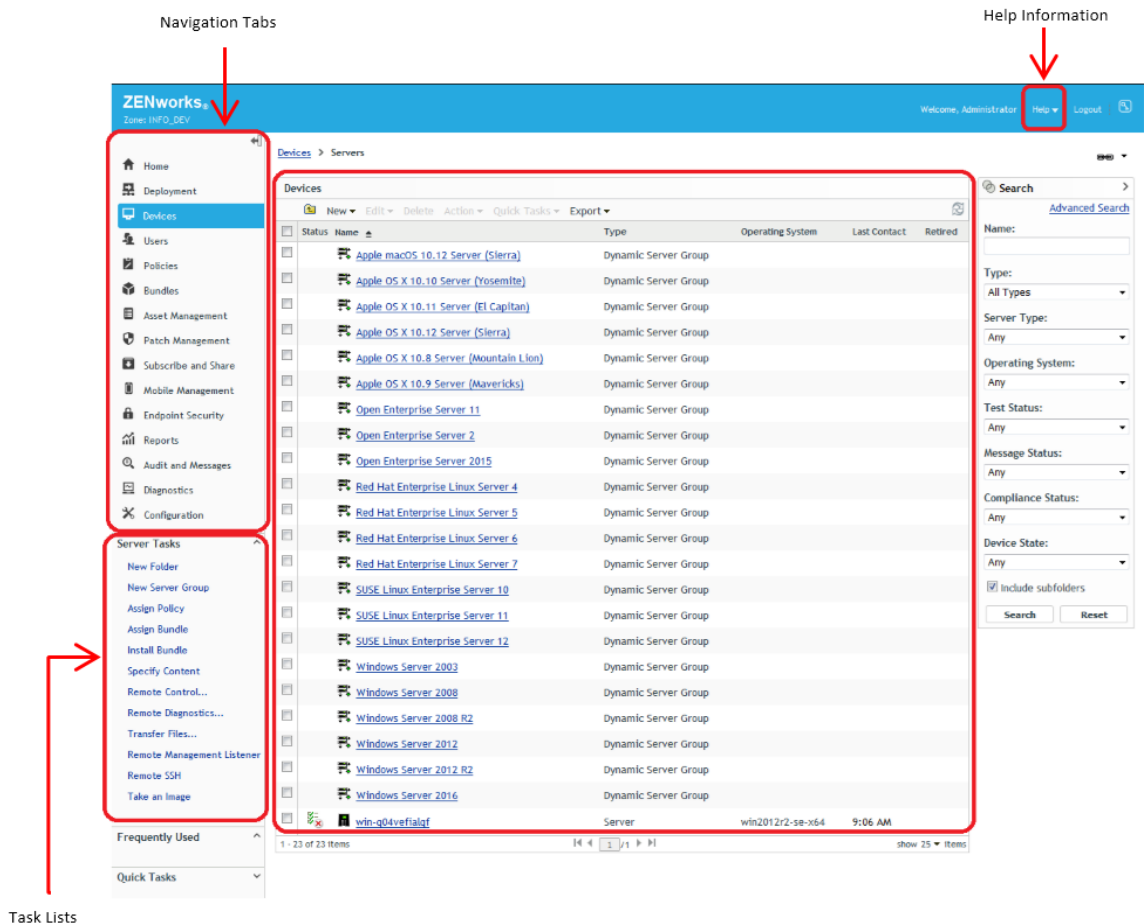
Navigation Tabs: The tabs in the left pane let you navigate among the functional areas of ZENworks. For example, the Servers page shown above lets you manage tasks associated with servers.

Task List: The task list in the left pane provides quick access to the most commonly performed tasks for the current page. The task list changes for each page. For example, the task list on the Bundles page displays bundle-related tasks and the task list on the Devices page displays device-related tasks.

Frequently Used Objects: The Frequently Used list in the left pane displays the 10 objects that you have accessed most often, from most used to least used. Clicking an object takes you directly to the details page for the object.

If required you can pin the required items using the pin icon, you can also unpin the unused items by clicking on the same pin icon. The pinned items are represented by a green pin icon and unpinned items are represented by a grey pin icon. Depending on the usage, the pinned and unpinned icons will be sorted.

Work Panel: The work panels are where you monitor and manage your ZENworks system. The panels change depending on the current page. In the above example, there are two work panels: Devices and Search. The Devices panel lists the servers, folders, server groups, and dynamic server groups that have been created; you use this panel to manage the servers. The Search panel lets you filter the Devices panel based on criteria such as a device's name, operating system, or status.

Help Information: The Help button links to Help topics that provide information about the current page. The Help button links change depending on the current page.

3 Customizing ZENworks Control Center

You can change ZENworks Control Center settings to customize behavior such as the failed login timeout and the automatic logout timeout:

3.1 Changing the Default Login Disable Values

By default, an administrator's account is disabled for 60 seconds after he or she unsuccessfully attempts to log in three times. You can change the number of login tries and the timeout length by editing a configuration file. The changes are only applied to the instance of ZENworks Control Center being run from the server where you open and modify the configuration file. To make the change applicable to all ZENworks Primary Servers, you must make the same change in each server's copy of this file.

IMPORTANT: Login attempts per administrator account are maintained in the ZENworks database, and there is only one ZENworks database per Management Zone. Therefore, if a particular administrator unsuccessfully attempts to log in to one Primary Server, that administrator is locked out of all Primary Servers in the zone. The lockout period is determined by the configuration on the server where the login attempts failed.

To modify the login tries and timeout values:

1 In a text editor, open the following file:

   Windows:

   `installation_location\microfocus\zenworks\conf\datamodel\zdm.xml`

   Linux: `/etc/opt/microfocus/zenworks/datamodel/zdm.xml`

2 Add the following lines to the file:

   `<entry key="allowedLoginAttempts">5</entry>`

   `<entry key="lockedOutTime">300</entry>`

   The 5 in this example represents the number of retries before disabling login, and 300 represents the number of seconds (the default is 60 seconds, or 1 minute).

   Keep in mind that the longer the delay before allowing a re-login after the configured number of failures (such as 5), the longer your authorized administrators must wait to access ZENworks Control Center.

> **IMPORTANT:** If you enter 0 as the login attempts value, the lockout functionality is disabled, allowing unlimited attempts at logging in.

3 Save the file, then restart the zenloader and zenserver services on the Primary Server to make the changes effective.

For instructions on restarting the services, see "Restarting the ZENworks Services" in the *ZENworks Primary Server and Satellite Reference*.

Following are the two properties which can be configured in osp-configuration.properties:

The osp-configuration.properties is available in the following location:

- On Windows: %ZENSERVER_HOME%\conf\security\osp
- On Linux: /etc/opt/microfocus/zenworks/security/osp

Account Lockout: This properties can be added in osp-configuration.properties to control the delay between invalid logging attempt and OSP response time. i.e OSP adds a random delay between min and max values specified in milliseconds before it responds when there is invalid login attempt.

- com.microfocus.zenworks.osp.security.max.delay=5000
- com.microfocus.zenworks.osp.security.min.delay=100

Access Token and Refresh Token timeout: Following properties control the access token and refresh token timeout (in millisecond)

- com.microfocus.zenworks.oauth.zcc.accessTokenTTL=86400
- com.microfocus.zenworks.oauth.zcc.refreshTokenTTL=2592000

3.2 Changing the Timeout Value for ZENworks Control Center

The purpose of the timeout is to clear memory resources. The larger the timeout value, the longer ZENworks Control Center retains the memory resources, which might have a negative impact on the long-term performance of the device from which you have launched ZENworks Control Center, including the ZENworks Server if you have it running locally on it.

You can make the ZENworks Control Center timeout value different on each ZENworks Server in the Management Zone.

To change the ZENworks Control Center timeout value on a ZENworks Server:

In ZCC, go to **Configuration** > **Infrastructure Management** > **ZCC Session Timeout Settings**.

In the ZCC Session Timeout Settings page, you can enable the ZCC session timeout. If an administrator is not active for the configured value (in minutes), then the session times out.

If the configured value is more than 5 minutes, the session timeout warning can be configured to display a pop-up before 5 mins, but this is not configured by default. By viewing the displayed prompt, the administrator can either extend the session or ignore the warning.

Configuration behavior: Following are some of the configurational behavior of the ZCC Session Timeout Settings:

- The configured value takes effect for all subsequent logins and does not apply to current sessions.
- If the configured session timeout value is set to less than 5 minutes, the session timeout pop-up is disabled, and the administrator is prompted to log in again when the session expires.
- The session timeout value can be 1 to 9999.
- If different session out values are configured in a multi-server zone in 2020 Update2, then the least of all becomes the default value after updating the server to ZENworks 2020 Update 3.

3.3 Using the custom-config.xml File to Modify ZENworks Control Center Settings

In addition to enabling you to configure the timeout value for the ZENworks Control Center (see Section 3.2, "Changing the Timeout Value for ZENworks Control Center," on page 16), the custom-config.xml file lets you control several additional configuration settings. However, the other settings are not available in the file, by default, and should be added only if its required.

1 On the ZENworks Server, open the custom-config.xml file in a text editor.
   - **Windows:** `${ZENSERVER_HOME}\services\zenserver\webapps\zenworks\WEB-INF\conf\custom-config.xml`
   - **Linux:** `/opt/microfocus/zenworks/share/tomcat/webapps/zenworks/WEB-INF/conf/custom-config.xml`

2 To add the desired setting, add `<setting id= <parameter>`.

   The following parameters should be added manually in the `custom-config.xml`

   debug.enabled: Change the value to **false** if you do not want any messages written to the ZENworks Control Center log files. The default value, **true**, causes messages to be written to the log files.

   debug.tags: These settings control debug information. You should not change them unless instructed by Technical Support.

   debug.log.viewstate: This setting controls debug information. You should not change it unless instructed by Novell Support.

   hideGettingStarted: Suppresses the Getting Started page. This setting is not functional at this time. To manually suppress the page, open the ZENworks Control Center, display the Getting Started page, then select **Do not show me this again**.

   noQuickTaskAutoRefresh: This setting disables automatic refreshing of the QuickTask status dialog box. It is used to discover issues with QuickTask status updates. You should not change this setting unless instructed by Technical Support.

3 Save the custom-config.xml file.

4 Restart the ZENworks Server service. See "Starting the ZENworks Services" in the *ZENworks Primary Server and Satellite Reference* for instructions.

4 Bookmarking ZENworks Control Center Locations

The Bookmark feature allows you to use your Web browser to manage direct access to the various locations in ZENworks Control Center, instead of performing the usual navigation clicks. You can also use this feature to bookmark hard-to-find locations.

You can create bookmarks for your Web browser to locations within the following sections of ZENworks Control Center:

- **Managed** tab on the **Devices** tab
- **Policies** tab
- **Bundles** tab
- **Management Zone Settings** on the **Configuration** tab

The locations you can bookmark include such items as lists, details of objects, and configuration settings.

Wherever the Link icon (🔗 ▾) is displayed, you can create a bookmark. The icon is located in the upper right of the page. If it is not displayed, a bookmark cannot be created for that location.

If you are logged in to ZENworks Control Center when you click a bookmark, the location is immediately displayed.

If you are not logged in to ZCC when you click a bookmark, the Login dialog box is displayed. After you enter valid credentials, the location is immediately displayed.

To create bookmarks:

1 In ZENworks Control Center, navigate to a location where you want to create a bookmark.

2 Click 🔗 ▾.

This opens the following dialog box, where the URL to the current location is already selected:
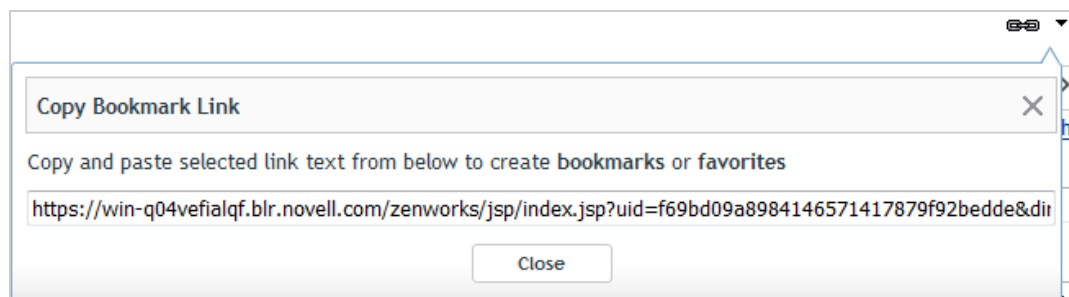
3 Press Ctrl+C to copy the URL, then click **OK** to close the dialog box.

4 Paste the URL as a new bookmark in your Web browser.

5 Naming Conventions in ZENworks Control Center

When you name an object in the ZENworks Control Center (folders, bundles, policies, groups, registration keys, and so forth), ensure that the name adheres to the following conventions:

- The name must be unique in the folder.
- Depending on the database being used for the ZENworks database, uppercase and lowercase letters might not create uniqueness for the same name. The embedded database included with ZENworks is case insensitive, so Folder 1 and FOLDER 1 are the same name and cannot be used in the same folder. If you use an external database that is case-sensitive, Folder 1 and FOLDER 1 are unique.
- If you use spaces, you must enclose the name in quotes when entering it on the command line. For example, you must enclose reg key 1 in quotes ("reg key 1") when entering it in the zman utility.
- The following characters are invalid and cannot be used: / \ * ? : " ' < > | ` % ~
- Ensure that the name of a bundle, policy, bundle folder, bundle group, policy folder, or policy group does not contain the following:
  - @Sandbox
  - @Version

6 Organizing Devices into Folders and Groups

Using ZENworks Control Center, you can manage devices by performing tasks directly on individual device objects. However, this approach is not very efficient unless you have only a few devices to manage. To optimize management of a large number of devices, ZENworks lets you organize devices into folders and groups; you can then perform tasks on a folder or group to manage its devices.

You can create folders and groups at any time. However, the best practice is to create folders and groups before you register devices in your zone. This allows you to use registration keys and rules to automatically add devices to the appropriate folders and groups when they register (see "Creating Registration Keys and Rules" in the *ZENworks Discovery, Deployment, and Retirement Reference*).

- Section 6.1, "Folders," on page 23
- Section 6.2, "Groups," on page 24
- Section 6.3, "Assignment Inheritance for Folders and Groups," on page 25

6.1 Folders

Folders are a great tool to help you organize devices in order to simplify management of those devices. You can apply configuration settings, assign content, and perform tasks on any folder. When you do so, the folder's devices inherit those settings, assignments, and tasks. You can also export the contents of a folder in the csv format by using the **Export** option.

For best results, you should place devices with similar configuration setting requirements in the same folder. If all devices in the folder require the same content or tasks, you can also make content or task assignments on the folder. However, all devices in the folder might not have the same content and task requirements. Therefore, you can organize the devices into groups and assign the appropriate content and tasks to each groups (see "Groups" on page 24 below).

For example, assume that you have workstations at three different sites. You want to apply different configuration settings to the workstations at the three sites, so you create three folders (`/Workstations/Site1`, `/Workstations/Site2`, and `/Workstations/Site3`) and place the appropriate workstations in each folder. You decide that most of the configuration settings apply to all workstations, so you configure those settings at the Management Zone. However, you want to perform a weekly collection of software and hardware inventory at Site1 and Site2 and a monthly inventory collection at Site3. You configure a weekly inventory collection at the Management Zone and then override the setting on the Site3 folder to apply a monthly schedule. Site1 and Site2 collect inventory weekly, and Site3 collects inventory monthly.

Creating a Folder

1. In ZENworks Control Center, click the **Devices** tab.
2. Click the **Workstations**, **Servers**, or **Mobile Devices** folder.
3. Click **New** > **Folder** to display the New Folder dialog box.
4. In the **Name** field, type a name for the new folder.

When you name an object in the ZENworks Control Center (folders, groups, bundles, policies, and so forth), ensure that the name adheres to the following conventions:

- The name must be unique in the folder.

- Depending on the database software being used for the ZENworks database, uppercase and lowercase letters might not create uniqueness for the same name. The embedded database included with ZENworks is case insensitive, so Folder 1 and FOLDER 1 are the same name and cannot be used in the same folder. If you use an external database that is case-sensitive, Folder 1 and FOLDER 1 are unique.

- If you use spaces, you must enclose the name in quotes when entering it on the command line. For example, you must enclose Folder 1 in quotes ("Folder 1") when entering it in the zman utility.

- The following characters are invalid and cannot be used: / \ * ? : " ' < > | ` % ~

5 Click **OK** to create the folder.

You can also use the `workstation-folder-create` and `server-folder-create` commands in the zman utility to create device folders. For more information, see "Workstation Commands" and "Server Commands" in the *ZENworks Command Line Utilities Reference*.

6.2   Groups

As you can with folders, you can also assign content and perform tasks on device groups. When you do so, the group's devices inherit those assignments and tasks. Unlike with folders, you cannot apply configuration settings to groups.

Groups provide an additional layer of flexibility for content assignments and tasks. In some cases, you might not want to assign the same content to and perform the same task on all devices in a folder. Or, you might want to assign the same content to and perform tasks on one or more devices in different folders. To do so, you can add the devices to a group (regardless of which folders contain the devices) and then assign the content to and perform the tasks on the group.

For example, let's revisit the example of the workstations at three different sites (see Section 6.1, "Folders," on page 23). Assume that some of the workstations at each site need the same accounting software. Because groups can be assigned software, you could create an Accounting group, add the target workstations to the group, and then assign the appropriate accounting software to the group. Likewise, you could use the groups to assign Windows configuration and security policies.

The advantage to making an assignment to a group is that all devices contained in that group receive the assignment, but you only need to make the assignment one time. In addition, a device can belong to any number of unique groups, and the assignments from multiple groups are additive. For example, if you assign a device to group A and B, it inherits the software assigned to both groups.

ZENworks provides both groups and dynamic groups. From the perspective of content assignments or performing tasks, groups and dynamic groups function exactly the same. The only difference between the two types of groups is the way that devices are added to the group. With a group, you must manually add devices. With a dynamic group, you define criteria that a device must meet to be a member of the group, and then devices that meet the criteria are automatically added.

ZENworks include several predefined dynamic server groups for example, Windows 2000 Servers Windows 2003 Servers and SUSE Linux Enterprise Server.

ZENworks also includes dynamic workstation groups for example, Windows XP Workstation, Windows 2000 Workstation, Windows Vista Workstations and SUSE Linux Enterprise Desktop. Devices that have these operating systems are automatically added to the appropriate dynamic group.

Creating a Group

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

2 Click the **Workstations**, **Servers**, or **Mobile Devices** folder.

3 Click **New** > **Server Group** or **New** > **Workstation Group** for workstations or **New** > **Mobile Device Group** for mobile devices to launch the Create New Group Wizard.

4 On the Basic Information page, type a name for the new group in the **Group Name** field, then click **Next**.

   The group name must follow the naming conventions.

5 On the Summary page, click **Finish** to create the group without adding members.

   or

   Click **Next** if you want to add members to the group, then continue with Step 6.

6 On the Add Group Members page, click **Add** to add devices to the group, then click **Next** when finished adding devices.

7 On the Summary page, click **Finish** to create the group.

You can also use the `workstation-group-create` and `server-group-create` commands in the zman utility to create device groups. For more information, see "Workstation Commands" and "Server Commands" in the *ZENworks Command Line Utilities Reference*.

Creating a Dynamic Group

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

2 Click the **Workstations**, **Servers**, or **Mobile Devices** folder.

3 Click **New** > **Dynamic Server Group** or **New** > **Dynamic Workstation Group** or **New** > **Dynamic Mobile Device Group** for mobile devices, to launch the Create New Group Wizard.

4 On the Basic Information page, type a name for the new group in the **Group Name** field, then click **Next**.

   The group name must follow the naming conventions.

5 On the Define Filter for Group Members page, define the criteria that a device must meet to become a member of the group, then click **Next**.

   Click the **Help** button for details about creating the criteria.

6 On the Summary page, click **Finish** to create the group.

6.3 Assignment Inheritance for Folders and Groups

This section is applicable only for ZENworks Configuration Management. When you assign content to a folder, all objects (users, devices, subfolders) except groups that are located in the folder inherit the assignment. For example, if you assign BundleA and PolicyB to DeviceFolder1, all devices within

the folder (including all devices in subfolders) inherit the two assignments. However, none of the device groups located in DeviceFolder1 inherit the assignments. Essentially, folder assignments do not flow down to groups located within the folder.

7 Using Message Logging

The Message Logger component of ZENworks lets the other ZENworks components such as zenloader, web services, ZENworks Management Daemon (ZMD), Remote Management, and Policy Enforcers log messages to different output targets. The output targets includes the system log, local log, database, SMTP, SNMP trap, and UDP.

The following sections provide additional information on the Message Logger component:

- Section 7.1, "Functionalities of Message Logger," on page 27
- Section 7.2, "Message Severity," on page 27
- Section 7.3, "Message Format," on page 28
- Section 7.4, "Configuring Message Logger Settings," on page 28
- Section 7.5, "Managing Messages," on page 33

7.1 Functionalities of Message Logger

Message Logger performs the following functions:

- Writes messages to local log files.
- Writes messages to a system log or event log.
- Writes messages to the Management console.
- Sends messages to the Management server.
- Sends messages as SMTP mail to SMTP servers from the Primary Server.
- Sends messages as SNMP traps to remote or local machines from the Primary Server.
- Sends messages as UDP packets to UDP destinations.
- Sends system message events or system messages to the Syslog server.
- Writes messages to the ZENworks database.
- Automatically purges database entries from the ZENworks database.
- Automatically acknowledges the messages in the ZENworks database.

7.2 Message Severity

A message is an event that is generated by different components and modules. These events can be exceptions such as errors, warnings, information to a user, or a debug statement to debug a module.

Messages are classified based on the following severity levels:

Error: Indicates that an action cannot be completed because of a user or system error. These messages are critical and require immediate attention from an administrator.

Warning: Indicates an exception condition. These messages might not be an error but can cause problems if not resolved. These messages do not require immediate attention from an administrator.

Information: Provides feedback about something that happened in the product or system that is important and informative for an administrator.

Debug: Provides debug information to troubleshoot and solve problems that might occur. The debug messages are stored only in the local file.

7.3 Message Format

Messages are logged in different formats depending on the output targets. For more information on message formats see, Section 7.5.1, "Understanding Message Formats," on page 34.

7.4 Configuring Message Logger Settings

The following sections provide information on configuring the settings of the Message Logger component of ZENworks.

- Section 7.4.1, "Configuring the Message Logger Settings at the Zone Level," on page 28
- Section 7.4.2, "Configuring the Message Logger Settings at the Folder Level," on page 32
- Section 7.4.3, "Configuring the Message Logger Settings at the Device Level," on page 33
- Section 7.4.4, "Turning on the Debug Messages," on page 33

7.4.1 Configuring the Message Logger Settings at the Zone Level

The following sections contain information to help you configure the settings in the Management Zone to enable message logging:

- "Local Device Logging" on page 28
- "Centralized Message Logging" on page 30

Local Device Logging

In ZENworks Control Center, the Local Device Logging page lets you configure the message logging to a local drive and the system log file of the managed device.

1. In ZENworks Control Center, click **Configuration**.
2. In the Management Zone Settings panel, click **Device Management**, then click **Local Device Logging.**
3. Configure the following options in the Local File panel:

   Log Message to a Local File if Severity Is: Choose from one of the following:

   - **Error:** Stores messages with a severity of Error.
   - **Warning and Above:** Stores messages with a severity of Warning and Error.
   - **Information and Above:** Stores messages with a severity of Information, Warning, and Error.

- **Debug and Above:** Stores messages with a severity of Debug, Information, Warning, and Error.

> **NOTE:** The **Log Message to a Local File if Severity Is** option is applicable only for the `zmd-messages`, `loader-messages` and `server-messages` logs. It is not applicable for the `zcc.log` file.

If you need to troubleshoot a ZENworks Agent issue on an individual device, you can change the severity setting so that additional information is logged. On the device, double-click the 🔗 icon in the notification area, click **Logging** in the left navigation pane, then select an option from the **Log Messages if Severity Is** drop-down list.

Rolling Based on Size: Closes the current log file and starts a new file based on the file size:

- **Limit File Size to:** Specify the maximum size of the log file, in either kilobytes (KB) or megabytes (MB). The log file is closed after the size of the file reaches the specified limit and a new file is started.
- **Number of Backup Files:** Specify the number of closed files to be backed up. The maximum number of backup files is 13.

Rolling Based on Date: Closes the current log file and starts a new file based on the following schedules:

- **Daily Pattern:** Starts a new file daily.
- **Monthly Pattern:** Starts a new file monthly.

On a Windows server, the local files include the following:

- `zcc.log` located in

  `%ZENSERVER_HOME%/logs/admin-mgmt` and `%ZENSERVER_HOME%/logs/client-mgmt`
- `loader-messages.log` located in `%zenserver_home%\logs`
- `services-messages.log` located in `%zenserver_home%\logs`

On a Windows managed device, the local files include the following:

- `zmd-messages.log` located in `%zenserver_home%\logs\LocalStore`

On a Linux server, the local files include the following:

- `zcc.log` located in

  `/var/opt/microfocus/log/zenworks/admin-mgmt` and `/var/opt/microfocus/log/zenworks/client-mgmt`
- `loader-messages.log` located in `/var/opt/microfocus/log/zenworks`
- `services-messages.log` located in `/var/opt/microfocus/log/zenworks`

On a Linux managed device, the local files include the following:

- `zmd-messages.log` located in `/var/opt/microfocus/zenworks/logs/LocalStore`

4 Configure the following options in the System Log panel.

Send Message to Local System Log and Roll Up to Collection Server if Severity Is: Allows you to select the severity of the message to be sent to the local system log and rolled up to the Collection Server. Choose from one of the following:

- **Error:** Stores messages with severity of Error.

- **Warning and Above:** Stores messages with a severity of Warning and Error.
- **Information and Above:** Stores messages with a severity of Information, Warning, and Error.

This setting lets you determine the message types that are added to the local system log. The local system log is the `\var\log\messages` directory on Linux devices and the `zenworks/logs/centralstore` directory on Windows devices.

Messages added to this system log directory are sent to the ZENworks Server for viewing in ZENworks Control Center on the **Configuration** > **System Information** page or by viewing the Summary page for the server or workstation.

Centralized Message Logging

In ZENworks Control Center, the Centralized Message Logging page lets you configure the settings related to message logging performed by the Primary Server.

1 In ZENworks Control Center, click **Configuration**.

2 In the Management Zone Settings panel, click **Event and Messaging**, then click **Centralized Message Logging.**

3 In the Automatic Message Cleanup panel, configure the settings to automatically acknowledge or remove the logged messages from the ZENworks server:

Preferred Maintenance Server: Specify the IP address of the preferred server on which the Message Cleanup actions runs to acknowledge or delete the logged messages from database.

Information: Allows you to configure the following settings for the informational messages:

- **Auto acknowledge when older than [ ] days:** Allows you to automatically acknowledge the logged informational messages that are older than the number of days you specify. For example, if you specify 30 days, then all the informational messages logged before 30 days from the current date are acknowledged when the Message Cleanup activity is scheduled to run. If you specify zero, then the informational messages dated until today are acknowledged. By default, all the informational messages older than 60 days are automatically acknowledged.

- **Auto delete when older than [ ] days:** Allows you to automatically delete the logged informational messages that are older than the number of days you specify. For example, if you specify 30 days, then all the informational messages logged before 30 days from the current date are deleted when the Message Cleanup activity is scheduled to run. If you specify zero, then the informational messages dated until today are deleted. By default, all the informational messages older than 60 days are automatically deleted.

If you want to specify both the auto-acknowledge and auto-delete days, then the number of auto-acknowledge days should always be less than the number for auto-delete days.

Warnings: Allows you to configure the following settings for the warning messages:

- **Auto acknowledge when older than [ ] days:** Allows you to automatically acknowledge the logged warning messages that are older than the number of days you specify. For example, if you specify 30 days, then all the warning messages logged before 30 days from the current date are acknowledged when the Message Cleanup activity is scheduled to run. If you specify zero, then the warning messages dated until today are acknowledged. By default, all the warning messages older than 60 days are automatically acknowledged.

- **Auto delete when older than [ ] days:** Allows you to automatically delete the logged warning messages that are older than the number of days you specify. For example, if you specify 30 days, then all the warning messages logged before 30 days from the current date are deleted when the Message Cleanup activity is scheduled to run. If you specify zero, then the warning messages dated until today are deleted. By default, all the warning messages older than 60 days are automatically deleted.

If you want to specify both the auto-acknowledge and auto-delete days, then the number of auto-acknowledge days should always be less than the number for auto-delete days.

Errors: Allows you to configure the following settings for the error messages:

- **Auto acknowledge when older than [ ] days:** Allows you to automatically acknowledge the logged error messages that are older than the number of days you specify. For example, if you specify 30 days, then all the error messages logged before 30 days from the current date are acknowledged when the Message Cleanup activity is scheduled to run. If you specify zero, then the error messages dated until today are acknowledged. By default, all the error messages older than 60 days are automatically acknowledged.

- **Auto delete when older than [ ] days:** Allows you to automatically delete the logged error messages that are older than the number of days you specify. For example, if you specify 30 days, then all the error messages logged before 30 days from the current date are deleted when the Message Cleanup activity is scheduled to run. If you specify zero, then error messages dated until today are deleted. By default, all the error messages older than 60 days are automatically deleted.

If you want to specify both the auto-acknowledge and auto-delete days, then the number of auto-acknowledge days should always be less than the number for auto-delete days.

Select the Days of the Week and the Time to Perform the Message Cleanup: Allows you to specify the time and the days of the week to run the Message Cleanup action. The administrator can set a daily schedule for Message Cleanup action.

Use Coordinated Universal Time: Allows you to convert the specified time to UTC (GMT) time. By default, this option is selected.

4 In the E-mail Notification panel, configure the settings to send the error messages to the administrators through e-mail:

Send Log Message via E-mail if Severity Is: Allows you to select the severity of the message to trigger sending the log messages through e-mail.

From: Specify the sender's e-mail address.

To: Specify the e-mail address of the recipients. You can specify more than one e-mail address by separating them with commas.

Subject: Specify the subject to be included while sending the e-mail from the Primary Server. You can customize the Subject field with macro values. For more information on customizing the subject field, see "E-Mail Format" on page 34.

5 In the SNMP Traps panel, configure the SNMP traps on the ZENworks Server to send log messages:

Send as SNMP Trap if Severity Is: Sends an SNMP trap if the logged message's severity is Error.

Trap Target: Specify the IP address or DNS name of the SNMP server.

Port: Specify the port number of the SNMP server configured for this operation. By default, the port number is 162.

Community String: Specify the community string of the SNMP trap that is to be sent.

6 In the UDP Forwarder panel, configure the settings to send logged messages through the UDP services. The following table contains information on the options available:

Send Message via UDP: Sends messages to the UDP destinations if the logged message's severity is Error.

UDP Destinations: You can perform the following tasks with the **Add**, **Edit**, and **Remove** options:

- ◆ **Add a Server**

    1. Click **Add** to display the Add UDP Destination Address dialog box.

    2. Specify the server name and the UDP port number configured for this operation.

    3. Click **OK**.

- ◆ **Remove a Server**

    1. Select the check box next to the server (or servers).

    2. Click **Remove**.

- ◆ **Edit Server Details**

    1. Select the check box next to the server.

    2. Click **Edit** to display the Edit UDP Destination dialog box.

    3. Modify the settings as desired, then click **OK**.

7 In the Syslog Server panel, specify the following:

1. **Syslog Server:** IP address or hostname of the Syslog server.

2. **Port:** Port number through which the system message events or system messages are shared to the Syslog server.

The Syslog Server panel enables you to configure a Syslog server for sending system message events and messages to Syslog servers such as Micro Focus ArcSight and Micro Focus Sentinel.

8 The Syslog Forwarder panel enables you to configure SIEM tools such as Archsight and Micro Focus Sentinel as Syslog servers to send audit event details and system messages.

To configure a Syslog server, specify IP address or host name of the Syslog server and port number through which the system message events and messages are shared to the Syslog server.

7.4.2 Configuring the Message Logger Settings at the Folder Level

By default, the Message Logger settings configured at the zone level are applied to all the managed devices. However, you can modify the Local Device Logging settings for all the devices within a folder:

1 In ZENworks Control Center, click **Devices**.

2 Click the **Folder (Details)** option for which you want to configure the Message Logger settings.

3 Click **Settings**, then click **Device Management > Local Device Logging**.

4 Click **Override**.

5 Edit the logging settings as required.

6 To apply the changes, click **Apply.**

or

To revert to the Local Device Logging settings configured at the zone level, click **Revert**.

7 Click **OK**.

7.4.3 Configuring the Message Logger Settings at the Device Level

By default, the Message Logger settings configured at the zone level are applied to all the managed devices. However, you can modify the Local Device Logging 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 Message Logger settings.

4 Click **Settings**, then click **Device Management > Local Device Logging**.

5 Click **Override**.

6 Edit the logging settings as required.

7 To apply the changes click **Apply.**

or

To revert to the Local Device Logging settings configured at the zone level, click **Revert**.

8 Click **OK**.

7.4.4 Turning on the Debug Messages

To turn on the logging of debug messages for all components:

1 In ZENworks Control Center, click **Configuration**.

2 In the Management Zone Settings panel, click **Device Management**, then click **Local Device Logging.**

3 In the local file panel, select the **Log message to a local file if severity is** option, then select the severity as **Debug and above**.

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

7.5 Managing Messages

The Message Logger component lets you manage the messages logged by the other components of ZENworks.

7.5.1 Understanding Message Formats

Messages are logged in different formats depending on the output targets such as local log, e-mail notification, SNMP traps, and UDP notification.

All error messages log the component name on which the error is generated. To troubleshoot the error, refer to the component's Reference Guide.

Example 1: Error related to Policy Management.

```
[DEBUG] [7/22/2007 3:42:45 PM] [] [PolicyManager] [] [Name = RM_dev, Guid =
271414163524d000190dbc6fa94272aa, Type = remote management policy, Version
= 2] [] [].
```

To troubleshoot this error, see the *ZENworks Configuration Policies Reference*.

Example 2: Error related to Remote Management.

```
[ERROR] [15-07-2007 12:44:16] [] [Remote Management]
[RemoteManagement.VNCEVENT_CANNOT_OPEN_EVENT] [Unable to open the
<ZRMUserLoginEvent> event] [] [].
```

To troubleshoot this error, see the *ZENworks Remote Management Reference*.

Local Log File Format

Messages are logged on the managed device and ZENworks Server in the following format:

```
[severity] [loggingTime] [userGUID] [componentName] [MessageID]
[MessageString] [additionalInfo] [RelatedGUID].
```

For example, `[DEBUG] [1/22/2007 12:09:15 PM] [] [ZMD] [] [refreshing QuickTaskRefresh(GeneralRefresh)] [] [].`

E-Mail Format

An e-mail message consists of the message header and the message body:

Message Header

The subject field in the e-mail can be customized as required by using keyword substitution macros:

Macro	Value
%s	Severity of the message.
%c	Name of the component.
%d	ID of the device at which the message is generated.
%t	Time of the message generation.
%a	Alias name of the device where the message is generated.

For example, if you want the subject line to display as "ERROR occurred on device Testifies at 4/1/07 5:31:01 PM", then specify "*%s* occurred on device *%a* at *%t*" in the **Subject** field.

Message Body

The message body consists of the following fields:

- **Device Alias:** Name of the device where the message is generated.
- **Device IP Address:** IP Address of the device where the message is generated.
- **Error:** [Date] Component name Message ID localized message string.
- **Additional Information:** (Optional) Any additional information.

SNMP Message Format

The SNMP messages consists of the following two parts:

- "SNMP Message Header" on page 35
- "Protocol Data Unit (PDU)" on page 35

SNMP Message Header

The following fields are contained in the header:

Version Number: Specifies the version of SNMP used. ZENworks uses SNMPv1.

Community String: Defines an access environment for a group of network-management systems (NMS).

Protocol Data Unit (PDU)

The following fields are contained in the PDU:

Enterprise: Identifies the type of managed object generating the trap. ZENworks uses 1.3.6.1.4.1.23.2.80.100.

Agent Address: Provides the IP address of the machine where the trap was generated.

GenerIc Trap Type: Contains the integer value 6. Type 6 is an enterprise-specific trap type, which has no standard interpretation in SNMP. The interpretation of the trap depends upon the value in the specific trap type field, which is defined by the Message Logger MIB.

Specific Trap Code: For enterprise-specific traps generated by ZENworks, the values in the specific trap type fields are as follows:

- For a severity level of MessageLogger.ERROR, the specific trap is 1.
- For a severity level of MessageLogger.WARN, the specific trap is 2.
- For a severity level of MessageLogger.INFO, the specific trap is 3.

Time Stamp: The time stamp indicating when the trap occurred.

Variable Bindings: Provides additional information pertaining to the trap. This field consists of the following name/value pairs:

- For trap ID 1.3.6.1.4.1.23.2.80.100.0.1, the value is the device GUID.
- For trap ID 1.3.6.1.4.1.23.2.80.100.0.2, the value is the device name.
- For trap ID 1.3.6.1.4.1.23.2.80.100.0.3, the value is the component name.
- For trap ID 1.3.6.1.4.1.23.2.80.100.0.4, the value is the time when the message was logged.
- For trap ID 1.3.6.1.4.1.23.2.80.100.0.5, the value is the message ID.
- For trap ID 1.3.6.1.4.1.23.2.80.100.0.6, the value is the probable cause.

UDP Payload Format

The payload is a byte array with null-terminated delimiters such as \0 or 0 x 00 (hexadecimal) for each element. Each element's data is presented as UTF-8 encoded strings and is explained below:

- The first element is the ZENworks version information. For example, 10.
- The second element is the value of severity of the message. The severity values are 4 for Informational, 6 for Warning, and 8 for Debug messages.
- The third element is the message date. The date is not locally specific and is represented as a UTF-8 string. For example, 09-Mar-2008 14:15:44.
- The fourth element is the user ID.
- The fifth element is the component name.
- The sixth element is the non-localized message ID.
- The seventh element is the localized message string.
- The eighth element is the additional information.
- The ninth element is the probable cause URL.
- The tenth element is the related GUID objects separated by commas.

NOTE: If the element does not have any data, it is represented as \0\0.

CEF Format

The Audit and system events, or messages in CEF format to Syslog servers. These events can be correlated in Security Information and Event Management (SIEM) tools, such as ArcSight and Sentinel, to alert administrators when specific events occur on the system.

7.5.2 Viewing the Message Status

In ZENworks Control Center, you can view the status of the logged messages in the following panels on the home page.

Message Summary

The Message Summary panel displays the number of critical, warning, and normal messages generated on the main objects in the Management Zone.

Figure 7-1 *Message Summary*

Message Summary				Advanced ⌃
	⊗	◇	⊙	Total
▊ Servers	1	0	0	1
🖳 Workstations	0	0	0	0
🔲 Mobile Devices	0	0	0	0
▨ Policies	0	0	1	1
✉ Bundles	0	0	1	1

In the Message Summary panel, you can do the following:

- Click an object type to display its root folder. For example, click **Servers** to display the Servers root folder.

- For any object type, click the number in one of its status columns (⊗◇⊙) to display a listing of all the objects that currently have that status. For example, to see the list of servers that have a normal status, click the number in the column of the **Servers**.

- For any object type, click the number in the **Total** column to display all of the objects of that type having critical, warning, or normal messages. For example, click the Total count for **Servers** to display a list of all servers having messages logged.

Device Hot List

The Device Hot List displays a list of the devices that have a noncompliant ⊠ status or have generated critical ⊗ or warning ◈ messages. The device remains in the hot list until you resolve the compliancy problem and acknowledge the messages. You can use this list as a summary of problems that need attention on the device.

To view the Device Hot List:

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

+ ⊠ This column indicates the number of bundles or policies that could not be applied to the device because an error occurred. You must review the error and warning messages to discover the compliance problem. The noncompliant status applies only to ZENworks Configuration Management. ZENworks Asset Management does not use this status.

+ ⊗ This column indicates the number or unacknowledged error messages generated for the device. An error is any action that fails so the ZENworks Agent cannot complete the action on the device.

+ ◈ This column indicates the number of unacknowledged warning messages generated for the device. A warning is any action that encounters a problem; the problem might or might not result in the ZENworks Agent completing the action on the device.

2 Click the device to display its message log.

7.5.3   Viewing the Messages

In the ZENworks Control Center, you can view the logged messages as follows:

+ "Message Log" on page 39
+ "System Message Log" on page 39

Message Log

The Message Log displays all unacknowledged messages generated for the object.

To view the message logs:

1 In ZENworks Control Center, click the **Device Hot List** on the home page, then click the device to view its message log.

You can also use the **Devices** menu to view the logs:

1 In ZENworks Control Center, click **Devices**.

2 Click **Servers** or **Workstations** to display the list of managed devices.

3 Click the name of a device, then click the **Summary** tab to display:

Status	Message	Date
⊗	The status for the MDT Deployment Action of the Bundle MDT applied to the non-registered	Dec 2
◉	The status for the MDT Deployment Action of the Bundle MDT applied to the non-registered	Dec 2
◉	The certificate presented by the server does not match the known certificate for host	Dec 1

1 - 3 of 3 items |◀ ◀   1   /1 ▶ ▶| show 5 ▾ items

Status: Displays an icon indicating the type of message:

⊗ Critical Message

◈ Warning

◉ Normal

Message: Displays a brief description of the event that occurred.

Date: Displays the date and time the event occurred.

4 To view the log messages in the advanced view, click **Advanced** on the right corner of the Memory Log panel.

You can acknowledge or delete messages from the message log. For more information on acknowledging messages, see Section 7.5.4, "Acknowledging Messages," on page 40, and for information on deleting messages, see Section 7.5.5, "Deleting Messages," on page 42.

System Message Log

The System Message Log panel displays the unacknowledged messages generated by the ZENworks Servers and managed devices in the Management Zone.

1 In ZENworks Control Center, click **Configuration**.

2 Click **System Information** to display the System Message Log.

System Message Log			Advanced
Status	Message	Date	Source
🟢	POLICYHANDLERS.PrinterPolicy.LocalPrinterAddSuccess{http://164.9	10:24 AM	🖥 blr-nrm-r5v2
🟢	POLICYHANDLERS.PrinterPolicy.LocalPrinterAddSuccess{printerlocal}	10:23 AM	🖥 blr-nrm-r5v2
🟢	Printer \\164.99.154.214\share already exists for user , hence n	10:23 AM	🖥 blr-nrm-r5v2
🔶	The action printer policy (ID:printer policy) failed, but the ac	10:23 AM	🖥 blr-nrm-r5v2:
🟢	IPrint client is already installed in the device, not reinstalli	10:23 AM	🖥 blr-nrm-r5v2

1 - 5 of 820   show 5 items

Status: Displays an icon indicating the type of message:

❌ Critical Message

🔶 Warning

🟢 Normal

Message: Displays a brief description of the event that occurred.

Date: Displays the date and time the event occurred.

3 To view the log messages in the advanced view, click **Advanced** on the right corner of the System Memory Log panel.

You can acknowledge or delete messages from the system message log. For more information on acknowledging messages, see Section 7.5.4, "Acknowledging Messages," on page 40, for information on deleting messages, see Section 7.5.5, "Deleting Messages," on page 42.

7.5.4   Acknowledging Messages

An acknowledged message is one that you have reviewed and marked as acknowledged (✔).

◆ "Acknowledging a Message" on page 40
◆ "Acknowledging Multiple Messages" on page 41
◆ "Acknowledging Messages Logged During a Specified Time" on page 41

Acknowledging a Message

1 In the Message Log panel or the System Message Log panel, click the message you want to acknowledge.

2 In the Message Detail Information dialog box, select the **Acknowledge** option, then click **OK**:
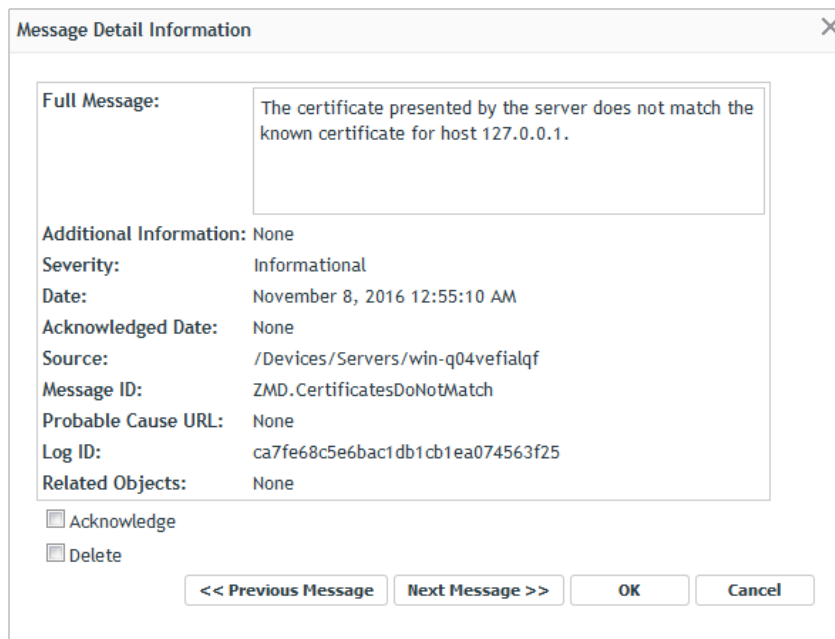
The acknowledged messages are removed from the Message Log panel or the System Message Log panel, depending on which panel you selected in Step 1.

The acknowledged messages continue to be listed in the Advanced view of these logs, marked with a check mark (✔).

Acknowledging Multiple Messages

1 In the Message Log panel or the System Message Log panel, click **Advanced** on the right corner of the panel.

2 Select the messages to acknowledge, then click **Acknowledge**:
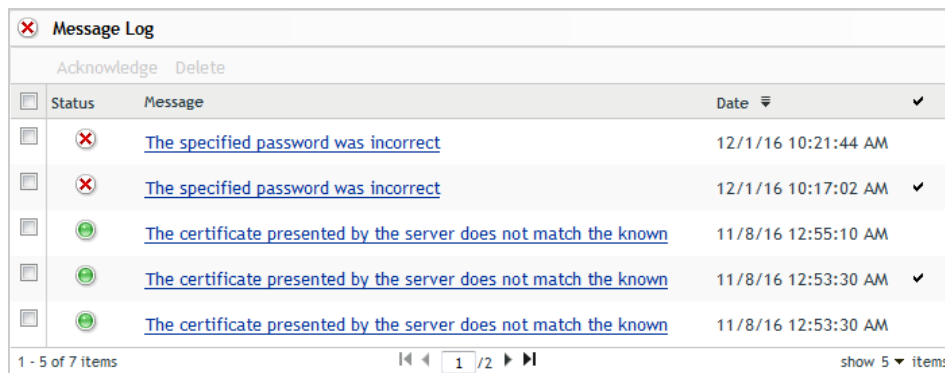
The acknowledged messages are marked with a check mark (✔).

Acknowledging Messages Logged During a Specified Time

1 In ZENworks Control Center, click **Configuration**.

2 In the **Configuration Tasks**, click **Message Cleanup** to display:
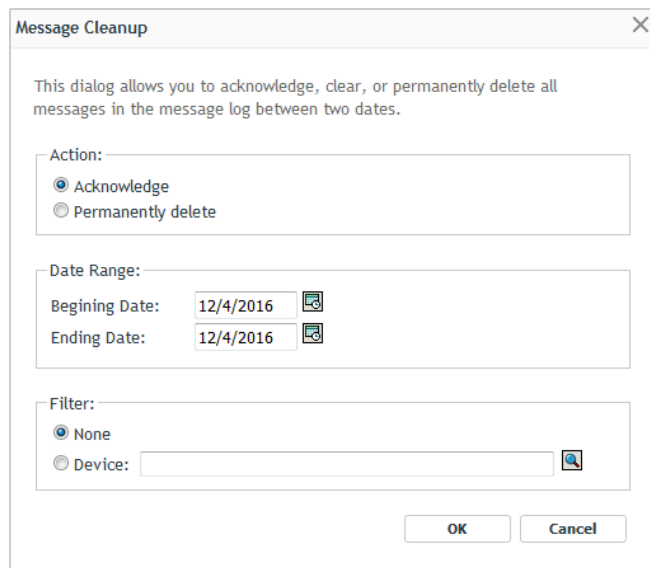
3 In the Message Cleanup dialog box, select **Acknowledge**.

4 In the **Date Range** option, select the **Beginning Date** and the **Ending Date**.

5 Select the **Filter** option:

None: Cleans up the messages in selected date range from all the devices.

Device: Cleans up the messages in selected date range from the selected device.

6 Click **OK**.

A message cleanup action is initiated and a system message is logged after the cleanup action is completed. For more information on viewing system logs, see "System Message Log" on page 39.

7.5.5 Deleting Messages

Deleting a message completely removes the message from your ZENworks system.

- ◆ "Deleting a Message" on page 43
- ◆ "Deleting Multiple Messages" on page 43
- ◆ "Deleting Messages Logged During a Specified Time" on page 43

Deleting a Message

1 In the Message Log panel or the System Message Log panel, click the message you want to delete.

2 In the Message Detail Information dialog box, select the **Delete** option, then click **OK**:
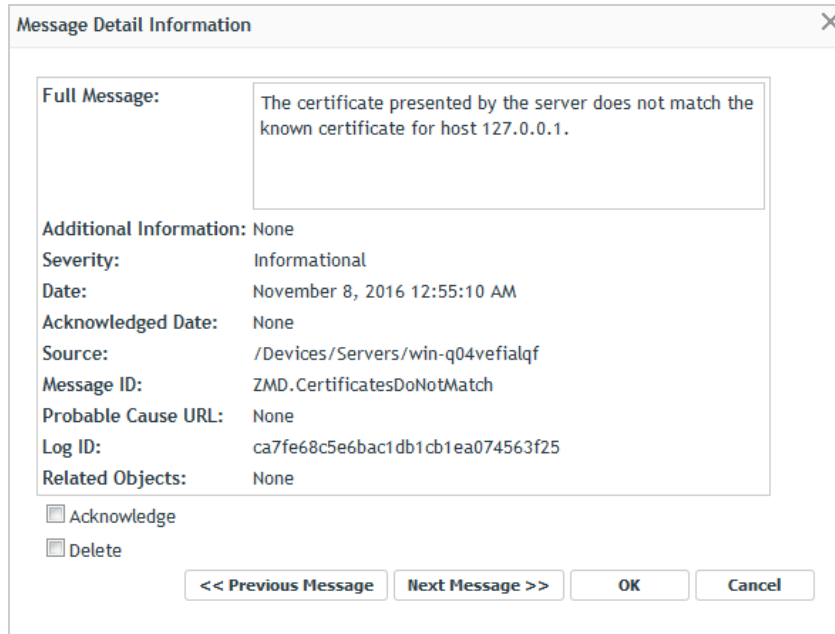
Deleting Multiple Messages

1 In the Message Log panel or the System Message Log panel, click **Advanced** on the right corner of the panel.
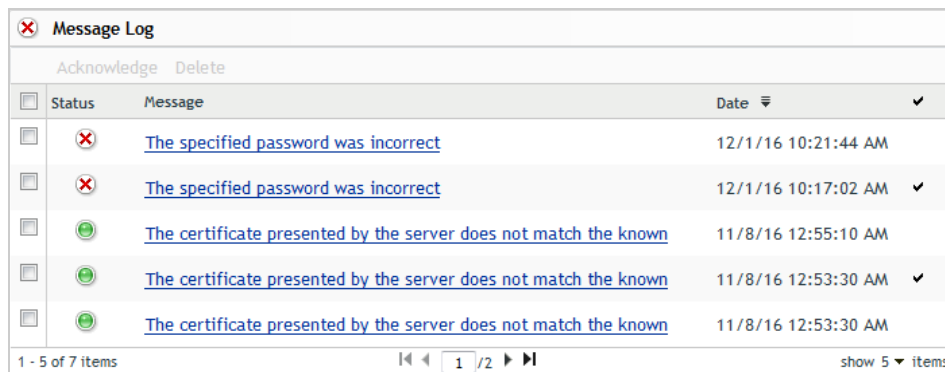
2 Select the messages to delete, then click **Delete**.

Deleting Messages Logged During a Specified Time

1 In ZENworks Control Center, click **Configuration**.

2 In the **Configuration Tasks**, click **Message Cleanup**.
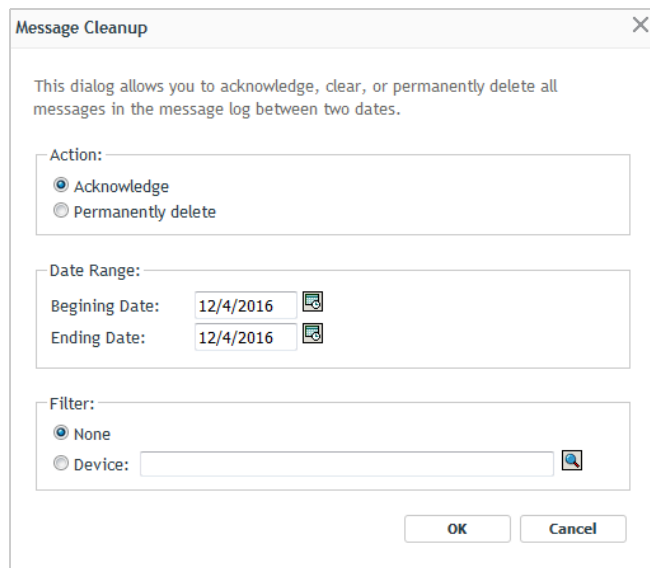
3 In the Message Cleanup dialog box, select **Permanently Delete**.

4 In the **Date Range** option, select the **Beginning Date** and the **Ending Date**.

5 Select the **Filter** option:

None: Cleans up the messages in selected date range from all the devices.

Device: Cleans up the messages in selected date range from the selected device.

6 Click **OK**.

7 In the Confirm Delete Dialog box, click **OK** to delete the message.

A system message is logged after the cleanup action is completed. For more information on viewing the system log see, "System Message Log" on page 39.

8 Customizing ZENworks News Alerts
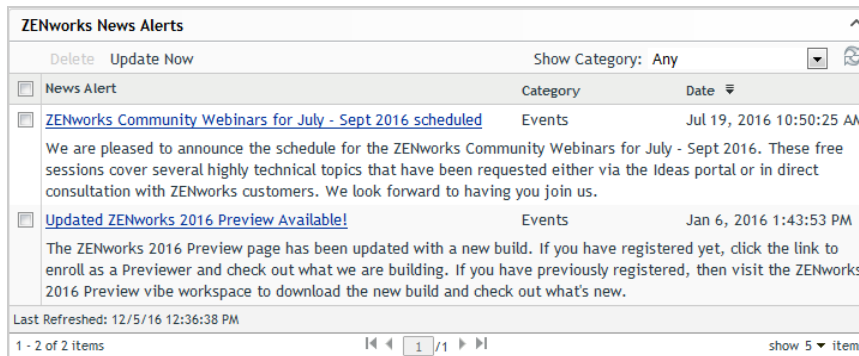
ZENworks displays information about current top issues, news updates, promotions, and so forth on the home page of the ZENworks Control Center.

The following sections provide information on deleting, updating, and sorting the news alerts, and on viewing the news. You can also configure the server and the schedule for downloading the news.

- Section 8.1, "Managing ZENworks News Alerts," on page 45
- Section 8.2, "Configuring ZENworks News Settings," on page 46

8.1 Managing ZENworks News Alerts

Figure 8-1 *ZENworks News Alerts*

Review the following sections to manage the ZENworks News Alerts:

- Section 8.1.1, "Deleting the News Alerts," on page 45
- Section 8.1.2, "Updating the News Alerts," on page 46
- Section 8.1.3, "Displaying the News Alerts Based on the Selected Category," on page 46
- Section 8.1.4, "Viewing the News," on page 46
- Section 8.1.5, "Sorting the News Alerts," on page 46

8.1.1 Deleting the News Alerts

1 In ZENworks Control Center, click **Home**.

2 In ZENworks News Alerts panel, select the check box next to the news alerts you want to delete.

3 Click **Delete**.

8.1.2 Updating the News Alerts

1 In ZENworks Control Center, click **Home**.

2 In ZENworks News Alerts panel, click **Update Now.**

The latest ZENworks news updates downloaded by the Primary Server are displayed in the ZENworks News Alerts panel. This might take some time.

8.1.3 Displaying the News Alerts Based on the Selected Category

1 In ZENworks Control Center, click **Home**.

2 In ZENworks News Alerts panel, select a category in the drop-down list next to **Show Category** to display all the news alerts based on the selected category.

8.1.4 Viewing the News

1 In ZENworks Control Center, click **Home**.

2 In ZENworks News Alerts panel, click the news alert to display the news in a new browser window.

8.1.5 Sorting the News Alerts

By default, the news alerts are sorted by the publication date. You can also sort the news alerts alphabetically by the title or category.

1 In ZENworks Control Center, click **Home**.

2 In ZENworks News Alerts panel, click **News Alert** to sort the news alerts alphabetically.

or

Click **Category** to sort the news alerts by category.

or

Click **Date** to sort the news alerts by date.

8.2 Configuring ZENworks News Settings

The ZENworks News Settings page lets you configure a dedicated news server and a schedule to download the ZENworks news. By default, the news is downloaded at midnight by the Primary Server of the Management Zone.

Review the following sections to configure the settings to download the news:

8.2.1 Dedicated News Server

By default, any available server in the Management Zone can be used to download the news updates. However, you can specify one ZENworks Server to be dedicated to handle the news downloads. The server that you select should have access to the Internet, either directly or through a proxy server.

The following sections contain more information:

- "Specifying a Dedicated News Server" on page 47
- "Clearing a Dedicated News Server" on page 47

Specifying a Dedicated News Server

1 In ZENworks Control Center, click **Configuration** in the left pane.

2 On the **Configuration** tab, expand the **Management Zone Settings** section (if necessary), click **Infrastructure Management**, then click **ZENworks News Settings** to display the News Download Schedule panel.

3 In the **Dedicated News Server** field, browse for and select a server, then click **OK**.

 The server's identification is displayed in the **Dedicated News Server** field.

4 (Conditional) If you need to revert to the last saved dedicated server setting, click **Reset**.

 This resets the dedicated server to the last saved setting, such as when you last clicked **Apply** or **OK**.

5 Click **Apply** to make the changes effective.

6 Either click **OK** to close the page, or continue with configuring the schedule type.

 If you did not click **Apply** to make your changes effective, clicking **OK** does so. Clicking **Cancel** also closes the page, but loses your unapplied changes.

Clearing a Dedicated News Server

Clearing a dedicated update server causes the news updates to be retrieved randomly from any server in the Management Zone.

1 In ZENworks Control Center, click **Configuration** in the left pane.

2 On the **Configuration** tab, expand the **Management Zone Settings** section (if necessary), click **Infrastructure Management**, then click **ZENworks News Settings** to display the News Download Schedule panel.

3 Click ✖ to remove the dedicated server from the **Dedicated News Server** field.

4 (Conditional) If you need to revert to the last saved dedicated server setting, click **Reset**.

 This resets the dedicated server to the last saved setting, such as when you last clicked **Apply** or **OK**.

5 Click **Apply** to make the change effective.

8.2.2 Schedule Type

You can configure the schedule for downloading the news:

1 In ZENworks Control Center, click **Configuration** in the left pane, then click the **Configuration** tab.

2 Click **Management Zone Settings** to expand its options, click **Infrastructure Management** to expand its options, then select **ZENworks News Settings**.

3 (Conditional) To exclude scheduled checking for news updates, click the down-arrow in the **Schedule Type** field, select **No Schedule**, click **Apply** to save the schedule change, then skip to Step 6.

With this option selected, you must download the news updates manually. For more information, see "Updating the News Alerts" on page 46.

4 (Conditional) To set a recurring schedule for checking for the news updates, click the down-arrow in the **Schedule Type** field, then select **Recurring**.

5 Fill in the fields:

   5a Select one or more check boxes for the days of the week when you want to check for news updates.

   5b Use the **Start Time** box to specify the time of day for checking to occur.

   5c (Optional) Click **More Options**, then select the following options as necessary:

   ◆ **Process Immediately if Device Unable to Execute on Schedule:** Causes checking for news updates to occur as soon as possible if the checking cannot be done according to schedule. For example, if a server is down at the scheduled time, checking for news updates occurs immediately after the server comes back online.

   ◆ **Use Coordinated Universal Time:** Causes the schedule to interpret the times you specify as UTC instead of local time.

   ◆ **Start at a Random Time Between Start and End Times:** Allows checking for news updates to occur at a random time between the time you specify here and the time you specified in Step 5b. Fill in the **End Time** fields.

   ◆ **Restrict Schedule Execution to the Following Date Range:** In addition to the other options, you can specify a date range to check for the news updates.

   5d (Conditional) If you need to revert to the last saved schedule, click **Reset** at the bottom of the page.

This resets all data to the last saved state, such as when you last clicked **Apply** or **OK**.

   5e When you have finished configuring the recurring schedule, click **Apply** to save the schedule change.

6 To exit this page, click **OK** when you are finished configuring the schedule.

If you did not click **Apply** to make your changes effective, clicking **OK** does so. Clicking **Cancel** also closes the page, but loses your unapplied changes.

9 Using the Credential Vault

The Credential Vault stores the credentials used by ZENworks actions and tasks that require authentication to access a particular resource.

For example, if you want to create a third-party Imaging bundle by using the image files stored in a shared-network image repository that requires authentication, you can add a credential that includes the login name and password for the repository in the credential vault. During the creation of the third-party Imaging bundle, you can specify the credential name to access the repository.

ZENworks features like Third-party imaging, Intel AMT provisioning, Subscriptions download, and actions such as Copy Directory uses credentials that are stored in the credential vault.

You can use ZENworks Control Center or the zman command line utility to manage credentials. The procedures in this section explain how to manage credentials by using ZENworks Control Center. If you prefer the zman command line utility, see "Credential Commands" in the *ZENworks Command Line Utilities Reference*.

The following sections contain information to help you manage credentials:

- Section 9.1, "Adding a Credential," on page 49
- Section 9.2, "Creating a Folder for Credentials," on page 50
- Section 9.3, "Assigning Credential Rights," on page 50
- Section 9.4, "Editing a Credential," on page 50
- Section 9.5, "Renaming a Credential," on page 51
- Section 9.6, "Moving a Credential to Another Folder," on page 51
- Section 9.7, "Removing a Credential," on page 51

9.1 Adding a Credential

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

2 In the **Credential Vault** panel, click **New** > **Credential** to display the Add Credential dialog box.

3 Fill in the following fields.

- **Credential Name:** Specify the name of the credential. When an action or task that requires authentication is executed, ZENworks uses this name to access the credential vault to obtain the resource's credentials.
- **Description:** Provide an optional description of the credential.
- **Login Name** Specify the login name for the resource. For example, to access a resource on a network that requires authentication do one of the following:
  - **For Basic Authentication:** Specify the `username`.
  - **For Domain Authentication:** Specify the `domain\username`.
  - **For eDirectory Authentication:** Specify the Fully Qualified Distinguished Name in the following format:

```
.username.ou.o
```

For example: `.jsmith.provo.novell`

However, the format `cn=jsmith,ou=provo,o=novell` is not supported.

- ◆ **Password** Specify the password for the resource's login name that you specified in the **Login Name** field.
- ◆ **Reenter Password** Re-enter the password for the resource's login name.

9.2 Creating a Folder for Credentials

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

2 In the Credential Vault panel, click **New** > **Folder** to display the New Folder dialog box.

3 In the **Name** field, specify a unique name for the folder.

   The folder cannot have the same name as any folders or credentials that already exist in the folder where you are creating it.

4 In the **Folder** field, click ⌕ to browse for and select the folder where you want the new folder created.

5 Type a description for the new folder, if desired.

6 Click **OK** to create the folder.

9.3 Assigning Credential Rights

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

2 In the **Administrators** section, click the underlined link for the administrator for which you want to change rights.

3 Click the **Rights** tab.

4 In the **Assigned Rights** section, click **Add** > **Credential Rights**.

5 Click **Add** to select folders containing credentials, then modify the rights associated with those folders.

   If you need help, click the **Help** button.

9.4 Editing a Credential

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

2 In the Credential Vault panel, select the check box next to the credential.

3 Click **Edit**.

4 Edit the following fields.

- ◆ **Credential Name:** Specify the name of the credential. When an action or task that requires authentication is executed, ZENworks uses this name to access the credential vault to obtain the resource's credentials.
- ◆ **Description:** Provide an optional description of the credential.

- **Login Name** Specify the login name for the resource. For example, to access a resource on a network that requires authentication do one of the following:

  - **For Basic Authentication:** Specify the `username`.

  - **For Domain Authentication:** Specify the `domain\username`.

  - **For eDirectory Authentication:** Specify the Fully Qualified Distinguished Name in the following format:

    `.username.ou.o`

    For example: `.jsmith.provo.novell`

    However, the format `cn=jsmith,ou=provo,o=novell` is not supported.

- **Password** Specify the password for the resource's login name that you specified in the **Login Name** field.

- **Reenter Password** Re-enter the password for the resource's login name.

5 Click **OK**.

9.5 Renaming a Credential

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

2 In the Credential Vault panel, select the check box next to the credential.

3 Click **Edit** > **Rename**.

4 Type the new name for the credential.

5 Click **OK**.

9.6 Moving a Credential to Another Folder

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

2 In the Credential Vault panel, select the check box next to the credential.

3 Click **Edit** > **Move**.

4 In the **Folder** field, click to browse for and select the folder where you want the credential moved.

5 Click **OK**.

9.7 Removing a Credential

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

2 In the Credential Vault panel, select the check box next to the credential.

3 Click **Delete**.

10 Using Quick Tasks

Quick Tasks are the tasks that you can quickly perform on one or more devices through ZENworks Control Center.

10.1 Quick Tasks Types

There are various quick tasks that you can perform on devices. Not all tasks are available for all objects (device, device group, device folder); unavailable tasks are dimmed in the ZENworks Control Center.

After the quick task is invoked, you are prompted to specify the Primary Server to send the quick task notification and to specify the quick task notification and expiry options. The status of the quick task is also displayed. For more information on initiating the quick task options and viewing the quick task status, see Section 10.2, "Initiating a Quick Task," on page 56.

NOTE: The quick task options are not available for the Wake Up and Intel AMT Power Management quick task types.

The following list provides descriptions of the Quick Tasks you can perform:

* **Refresh Device:** Updates all information, such as configuration settings and registration on the selected devices. In ZENworks Configuration, it also updates the bundles and policies.

    NOTE: A Refresh Device quick task cannot be created for a device when another Refresh Device quick task is already active on the device. A Refresh Device quick task that is created for a group of devices is not assigned to the devices within the group that already have a Refresh Device quick task active on them.

---

* **Refresh Policies:** Updates policy information on the selected devices. This quick task is applicable for ZENworks Endpoint Security Management and ZENworks Configuration Management.

* **Clear ZESM User Defined Password:** Clears the user-defined secondary decryption password and the user-defined encryption/decryption password for removable storage devices. This quick task is applicable only for ZENworks Endpoint Security Management.

* **Clear ZESM Local Client Self Defense Settings:** Resets the Endpoint Security Agent to use the Client Self Defense settings contained within the device's effective Security Settings policy. This overrides any local changes made to the settings. This quick task is applicable only for ZENworks Endpoint Security Management.

- **Clear ZESM Local Firewall Registration Settings:** Resets the Endpoint Security Agent to use the firewall registration settings contained within the device's effective Firewall policy. This overrides any local changes made to the settings. This quick task is applicable only for ZENworks Endpoint Security Management.

- **FDE - Decommission Full Disk Encryption:** Prevents access to a device's encrypted data by decommissioning the device disk. You can temporarily decommission the drive, in which case encrypted data is recoverable with a HelpDesk file or Emergency Recovery Disk, or you can permanently decommission the disk by erasing it. This quick task is applicable only for ZENworks Full Disk Encryption.

- **FDE - Enable Additive User Capturing:** Enables one-time user capturing. After the device receives this task, the user capture occurs at the next reboot. Whichever user logs in at that reboot is added to the PBA. To avoid possible security breaches and ensure the correct user capture, coordinate with the intended user when initiating this task. This quick task is applicable only for ZENworks Full Disk Encryption.

- **FDE - Force Device to Send ERI File to Server:** Instructs the device to send its Emergency Recovery Information (ERI) file to the ZENworks Server. This file is required to recover any temporarily decommissioned disk. This quick task is applicable only for ZENworks Full Disk Encryption.

- **FDE - Update PBA Password Settings:** Updates an existing user's PBA password or adds a new user (and password) to the PBA. This quick task is applicable only for ZENworks Full Disk Encryption.

- **Inventory Scan:** Initiates an inventory scan on the selected devices. Inventory scan collects inventory data such as updated list of discovered product and latest usage data. The latest inventory data will be uploaded as per the upload schedule set by the administrator.

  For each device, the inventory scan uses the Scan Now settings defined for the device (*device* view > **Settings** tab > **Inventory**) to determine what information the scan collects.

- **Inventory Wizard:** Sends the inventory data collection form to the selected devices. For each device, the Inventory Collection Wizard uses the data collection form defined for the device (*device* view > **Settings** tab > **Inventory**).

- **Install Bundle:** Installs one or more bundles on the selected devices. This quick task is applicable only for ZENworks Configuration Management.

- **Launch Bundle:** Launches one or more bundles on the selected devices. This quick task is applicable only for ZENworks Configuration Management.

  NOTE: If a bundle is installed or launched with a quick task, or with the Now device assignment distribution schedule (which also triggers a quick task for the assigned devices), the bundle actions defined to run as a logged-in user are performed in the system space.

  The related quick task triggers a bundle execution and a device refresh at approximately the same time. Because the user session is still busy refreshing, it does not update the list of assigned bundles, and the ZENworks agent falls back to process the bundles in the device session. After a subsequent refresh, the bundle actions defined to run as a logged-in user are executed correctly.

- **Uninstall Bundle:** Uninstalls one or more bundles on the selected devices. This quick task is applicable only for ZENworks Configuration Management.

- **Wake Up:** Uses Wake on LAN (WOL) technology to start a device that is shut down. The device must support WOL.

+ **Intel AMT Power Management:** Allows you to change the power state of a device.

+ **Reboot/Shutdown Devices:** Depending on your choice, shuts down or reboots the selected devices. You can include a warning message to be displayed on the devices. You can also specify a delay period for the reboot or shutdown.

+ **Launch Application:** Launches an executable on the selected devices. The executable must be available to the devices either locally or in an accessible network location.

+ **Run Script:** Runs a script on the selected devices. You can run a script that resides on the devices, on your local drive, or on a drive that you intend to create. The script engine must be available to the devices either locally or in an accessible network location.

+ **Launch Java Application:** Runs a Java application on the selected devices.

+ **Reset Agent:** Triggers a reset action on the Agent device. This quick task will stop the agent service, delete the cache, and then restart the agent service.

+ **Verify Last Update:** Runs the last successful update on the selected device. Your device might reboot as a result of this action.

NOTE: The Reset Agent and Verify Last Update quick tasks are applicable only to Windows devices. These quick tasks cannot be applied on device groups or folders.

+ **Retire Device Now:** Immediately retires the selected device from your ZENworks system. To retire a device at its next refresh, use the Retire Device action. Retiring a device is different from deleting a device. When you retire a device, its GUID is retained (as opposed to when you delete a device, which also deletes its GUID). As a result, all inventory information is retained and is assessable. In ZENworks Configuration Management, all policy and bundle assignments are also removed. If you unretire the device in the future, its assignments are restored.

+ **Unretire Device Now:** Immediately reactivates the selected device. In ZENworks Configuration Management, it reapplies all policy and bundle assignments that the device previously had. To unretire a device at its next refresh, use the Unretire Device action.

+ **Device Wipe:** You can remotely wipe 1709 and later versions of Windows 10 devices using this quick task. This action resets the device operating system to its factory settings and removes all non-OS files and applications from the device. You can multi-select devices, but devices with non-supported operating systems will be ignored.

+ **Lock Device:** Applicable for mobile devices only. You can remotely lock a lost or a stolen device from ZENworks Control Center by using the Lock Device quick task. If passcode restriction is already enabled on the device, then the user can unlock the device by only entering the set passcode.This quick task is applicable for Android and iOS devices that are enrolled as fully managed devices in the management zone.

+ **Unlock Device:** Applicable for mobile devices only. The Unlock Device quick task removes the passcode restriction on an iOS device. For an Android device, the passcode restriction is not removed. However, on Android devices a new passcode can be set that should be compliant with the existing Mobile Security policy assigned to the Android device, if any. This task can be performed on only a single device at any given point in time. This quick task is applicable for Android and iOS devices that are enrolled as fully managed devices in the management zone.

+ **Unenroll Device:** Applicable for mobile devices only. Unenrolls the device so that it is no longer managed. You can delete the device from the zone or retire it (remains in the zone but is inactive). You can also choose to fully wipe the device by resetting it to factory settings, or to selectively wipe the device by removing only corporate data and email.

◆ **Send Message:** Applicable for mobile devices only. Sends a text message to the device. The message can contain a subject and body (140 character limit). This quick task is applicable for Android devices only. If this quick task notification is initiated for any device other than an Android device, then the status of the quick task is displayed as ignored.

10.2 Initiating a Quick Task

Quick Tasks are available for the Devices, Bundles, and Policies lists in ZENworks Control Center. The following procedure provides an example of how to initiate a Quick Task from the Device list. The procedures for applying a Quick Task from the Bundles or Policies list is similar.

1 In ZENworks Control Center, click **Devices**, then locate the device to which you want to apply a Quick Task.

2 Select the check box next to the device, click **Quick Tasks**, then click **Refresh Policies** (or if you want to initiate a different Quick Task, click that task).

In the Quick Task dialog, click the Edit link to rename the quick task. The name is applicable only for that instance of the quick task.

3 Configure the Quick Task options:

Option	Steps
Select the Primary Server to send the Quick Task notification	Depending on the Primary Server that you want to send the quick task notification to, do one of the following: ◆ **Current primary server:** Select this option to enable the Primary Server of the ZENworks Control Center that you are accessing to send the quick task notification. ◆ **Any primary server:** Select this option to enable any Primary Server in the Management Zone to send the quick task notification. For example, you might want to use this option when the current Primary Server is busy performing other tasks. ◆ **Select one or more primary servers:** Select this option to choose one or more Primary Servers in the Management Zone to send the quick task notification. For example, if you choose to use a single Primary Server to send the quick task notification to many devices, the workload on the server might increase because it must send the notification to all the devices. You can select multiple Primary Servers so that the load of notifying many devices is distributed among the servers. Click **Add** to select and add the Primary Servers. Click **Remove** to remove any previously added Primary Server.

Option	Steps
QuickTask Notification Options	Select one of the following:
	◆ **Notify all the devices immediately:** Select this option to send the quick task notification to all the devices immediately.
	For example, you might want to select this option when the quick task notification is sent to a smaller number of devices and the Primary Server can handle all the quick task requests from all the devices at the same time.
	◆ **Notify all the devices within _ mins:** Select this option to send the quick task notification to all the devices within the specified time. By default, the notification time is set to 5 minutes. You can choose to specify the notification time according to your requirements.
	For example, you might want to select this option when the quick task notification is sent to a larger number of devices and the Primary Server might not be able to handle all the quick task requests from all the devices at the same time.
QuickTask Expiry Option	Select one of the following:
	◆ **Expires immediately when failed to notify the device:** Select this option to immediately expire the quick task when the quick task notification to the devices fails.
	For example, you might want to select this option to send a **Reboot/Shut Down Devices** quick task for rebooting or shutting down a device. If the device is already shut down, you don't want to execute the quick task on the device when the device restarts.
	NOTE: This option is not applicable for iOS bundles.
	◆ **Never Expires:** Select this option if you never want the quick task to expire.
	For example, you might want to select this option when you send an **Install Bundle** quick task to install an application on a device that might not be running at that time.
	◆ **Expires after _ mins of the quick task creation:** Select this option to expire the quick task a certain amount of time after it is created. By default, the expiration time is set to 5 minutes. You can choose to specify the expiration time according to your requirement.
	For example, you might want to select this option when you need to launch an application on multiple devices that are either in the process of booting up or are likely to be started within the stipulated time.

4 Click **Start** to initiate the notification of the quick task.

5 Click the QuickTask Status tab to monitor the status of the task.

Status	Description
New	The Primary Server has not started the process of notifying the device.
Connecting	The Primary Server is attempting to connect to the device.
Connected	The Primary Server is connected to the device.
Connection Failed	The Primary Server is unable to connect to the device.
Connection Failed (Expired)	The Primary Server is unable to connect to the device, and the quick task assignment has expired.
Stopped	The quick task notification was stopped before it was sent to the device. You can do this only if the quick task has not yet been assigned to the device.
Assigned	The quick task has been assigned to the device.
Initiated	The quick task notification has been sent to the device.
Install Requested	The device has requested for installation of the bundle.
Notification Failed	Sending of the quick task notification failed.
Ignored	The quick task notification was ignored because it is not applicable to the device.
Ignored by App	This quick task notifications status is specific to mobile devices. The quick task notification was ignored as the ZENworks app installed on the mobile device is outdated.
Done	The quick task has been executed on the device.

10.3 Cancelling, Stopping, or Hiding a Quick Task

 - To stop the quick task on a managed device, select the device on which you want to stop the quick task and click **Stop**. You can do this only if the quick task has not yet been assigned to the device.

 - To hide the quick task dialog box, click **Hide**. The quick task is listed in the Quick Tasks list in the left navigation pane; you can click the quick task to check the status again.

 - To cancel the quick task, click **Cancel**.

11 Using System Variables

System variables let you define variables that can be used to replace paths, names, and so forth as you enter information in ZENworks Control Center.

You can define system variables at three levels:

- **Management Zone:** The system variables are inherited by all device folders, devices, and bundles.
- **Device Folder:** The system variables are inherited by all devices contained within the folder or its subfolders.
- **Device or Bundle:** The system variables apply only to the device or bundle for which they are configured.

The following sections contain more information:

11.1 Understanding System Variables

The following examples illustrate some uses of system variables:

- **Specifying Paths and Filenames in Actions:** When you create an Edit INI File action, for example, you specify a `.ini` file and configure the changes to be performed on that file. During the creation process, you can specify the full path to the file (for example, `C:\Program Files\OpenOffice.org 2.0\program\setup.ini`).

  Instead of specifying the entire path and filename, you can create a system variable. For example, the name of the variable can be OpenOffice INI and the value can be the full path to the file. Now, instead of specifying the full path and filename when you create the action, you can type `${OpenOffice INI}` in the **Filename** field.

  An advantage of using a system variable rather than typing the full path and filename is that you can specify this particular `.ini` file in many different types of actions. Suppose that the location of the `.ini` file changes. Instead of editing the path in each action, you can edit the path in the system variable and all the actions still point to the correct path.

  You can generalize the path even more by creating a system variable named ProgramFiles with the value of `C:\program files`. In the future, when you specify a path, you can type `${ProgramFiles}` and then specify the remaining path to the specific file. For example,

${ProgramFiles}\OpenOffice 2.0\program\setup.ini. Again, if the path to the C:\program files directory changes in the future, you only need to change the path in the system variable, rather than in each bundle that uses that location in a path.

 ◆ **Overriding Inherited Settings:** When configuring system variables for a folder, device, or bundle, you can override an inherited variable by defining a new variable with the same name but a different value. For example, if `ProgramFiles=C:\` is defined at the Management Zone, you can override it by defining `ProgramFiles=D:\` at the device folder level or at the device or bundle.

You can use a system variable when creating a bundle. Depending on the location of the targeted device object in the folder hierarchy, the value can be different.

For example, suppose that all of your applications are installed in `C:\program files` except for specific applications used by the accounting department, which are installed in `D:\program files`. You define the ProgramFiles variable at the Management Zone level to point to `C:\program files`. For the accounting applications, you create a device folder called `Accounting Department` to contain the devices in the accounting department. You can set the value for the ProgramFiles variable to `D:\program files` on the Accounting Department device folder level. When the same bundle is applied to devices, the path to the program files directory is on the `C:\` drive for all targeted devices except for those contained in the Accounting Department device folder. For those devices, the program files directory points to the `D:\` drive.

11.2   Adding System Variables

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

2 In the Management Zone Settings list, click **Device Management**.

3 Click **System Variables**.

4 Click **Add**, provide the name and value for the variable, then click **OK**.

When configuring system variables for a folder, device, or bundle, you can override an inherited variable by defining a new variable with the same name but a different value. For example, if `Var1=c:\` is inherited, you can override it by defining `Var1=d:\`.

Variable names cannot include spaces and must be unique at the level where they are defined. For example, you cannot have two variables named Var1 defined at the device level (unless one is inherited, in which case the device-level variable overrides the inherited variable).

Variable values cannot include the characters & and <.

5 Click **Apply**.

11.3   Removing System Variables

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

2 In the **Management Zone Settings** list, click **Device Management**.

3 Click **System Variables**.

4 Select the check box next to the variable (or variables).

5 Click **Remove**.

6 Click **Apply**.

11.4   Editing System Variables

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

2 In the **Management Zone Settings** list, click **Device Management**.

3 Click **System Variables**.

4 Select the check box next to the variable, then click **Edit**.

5 Modify the **Name** and **Value** fields as desired, then click **OK**.

6 Click **Apply**.

11.5   Using System Variables

1 Use the following syntax:

`${VAR_NAME}`

`%VAR_NAME%`

`%*VAR_NAME%`

Replace `VAR_NAME` with the name of the variable.

2 When you perform an action on the agent, you might sometimes need to put the name of a macro into the registry, or a file, rather than the value itself. Use the following syntax in such a case:

`%%username%%`

The variable is written as it is and is not replaced with a value.

12 Using Special System Variables

The following sections contain information on the special system variables supported in ZENworks Configuration Management:

12.1 Windows Special System Variables

A Windows special system variable is one that defines the Windows directories. The typical paths listed below are based on default installations and might not match your specific setup.

Suppose that you have installed Windows to drive D: (for example, `D:\WINDOWS`). However, an application installation expects Windows to be on drive C: (for example, `C:\WINDOWS`). You can use the WinDisk system variable to substitute drive D: for the files that require it.

NOTE: For compatibility with traditional ZENworks, the system variable can also be specified in one of the following formats:

- %*system_variable*%

  For example, %ProgramFiles%
- %**system_variable*%

  For example, %*ProgramFiles%
- ${*system_variable*}

  For example, ${ProgramFiles}

Table 12-1   *Windows System Variables*

Macro	Description
${AdminTools}	File system directory that contains the adminstrative tools that appear in the Control Panel when a specific user logs on to the device.
	On a Windows Server 2003 or Windows XP device, it is typically `C:\Documents and Settings\`*`Username`*`\Start Menu\Programs\Administrative Tools`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `C:\Users\`*`Username`*`\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools`.
${AllUsersProfile}	File system directory that contains common profile for all the users.
	On a Windows Server 2003 or Windows XP device, it is typically `C:\Documents and Settings\All Users`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `C:\ProgramData`.
${AppData}	File system directory that serves as a common repository for application-specific data.
	On a Windows Server 2003 or Windows XP device, it is typically `C:\Documents and Settings\`*`Username`*`\Application Data`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `C:\Users\`*`Username`*`\AppData\Roaming`.
${CommonDesktop}	File system directory that contains files and folders that appear on the desktop for all users.
	On a Windows Server 2003 or Windows XP device, it is typically: `C:\Documents and Settings\All Users\Desktop`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `C:\Users\Public\Desktop`.
${CommonPrograms}	File system directory that contains the directories for the common program groups that appear on the Start menu for all users.
	On a Windows Server 2003 or Windows XP device, it is typically `C:\Documents and Settings\All Users\Start Menu\Programs`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `C:\ProgramData\Microsoft\Windows\Start Menu\Programs`.
${CommonStartMenu}	File system directory that contains the programs and folders that appear on the Start menu for all users.
	On a Windows Server 2003 or Windows XP device, it is typically: `C:\Documents and Settings\All Users\Start Menu`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically: `C:\ProgramData\Microsoft\Windows\Start Menu`.

Macro	Description
${CommonStartup}	File system directory that contains the programs that appear in the Startup folder for all users. The system starts these programs whenever any user logs on.
	On a Windows Server 2003 or Windows XP device, typically this directory is `C:\Documents and Settings\All Users\Start Menu\Programs\Startup`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, typically this directory is `C:\ProgramData\Microsoft\Windows\Start Menu\Programs/`**Startup**.
${CommonAdminTools}	File system directory that contains the administrative tools that appear in the Control Panel for all users who logs in to the device.
	On a Windows Server 2003 or Windows XP device, it is typically `C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools`.
${CommonAppData}	File system directory that contains the application-specific data for all users who logs in to the device.
	On a Windows Server 2003 or Windows XP device, it is typically `C:\Documents and Settings\All Users\Application Data`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `C:\ProgramData`.
${CommonDocuments}	File system directory that contains the documents shared by all users who log in to the device.
	On a Windows Server 2003 or Windows XP device, it is typically: `C:\Documents and Settings\All Users\Documents`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically: `C:\Users\Public\Documents`.
${CommonProgramFiles}	File system directory that contains the program files shared by multiple applications.
	On a Windows Server 2008, Windows XP, Windows Vista, or Windows 7 device, it is typically `C:\Program Files\Common Files`.
${CommonTemplates}	File system directory that contains the document templates shared by all users who log in to the device.
	On a Windows Server 2003 or Windows XP device, it is typically: `C:\Documents and Settings\All Users\Templates`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `C:\ProgramData\Microsoft\Windows\Templates`.

Macro	Description
${Cookies}	Files system directory that contains the user's cookies.
	On a Windows Server 2003 or Windows XP device, it is typically `C:\Documents and Settings\`*`Username`*`\Cookies`.
	On a Windows Server 2008, Windows Vista, it is typically: `C:\Users\`*`Username`*`\AppData\Roaming\Microsoft\Windows\Cookies`.
${Desktop}	File system directory used to physically store file objects on the desktop (not the desktop folder itself).
	On a Windows Server 2003, typically this directory is `C:\Documents and Settings\`*`Username`*`\Desktop`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, typically this directory is `C:\Users\`*`Username`*`\Desktop`.
${Favorites}	File system directory that serves as a common repository for the user's favorite items.
	On a Windows Server 2003, typically this directory is `C:\Documents and Settings\`*`Username`*`\Favorites`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, typically this directory is `C:\Users\`*`Username`*`\Favorites`.
${Fonts}	Virtual folder containing fonts. Typically `C:\Windows\Fonts`.
${History}	File system directory that contains the user's history of visited Internet addresses.
	On a Windows Server 2003, it is typically, `C:\Documents and Settings\`*`Username`*`\Local Settings\History`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `C:\Users\`*`Username`*`\AppData\Local\Microsoft\Windows\History`.
${LocalAppData}	File system directory that serves as a common repository for application-specific data.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically, `C:\Users\`*`Username`*`\AppData\Local`.
${MyPictures}	File system directory that contains a specific user's graphics files.
	On a Windows Server 2003, it is typically `c:\Documents and Settings\`*`Username`*`\My Documents\My Pictures`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `c:\Users\`*`Username`*`\Pictures`.

Macro	Description
${NetHood}	File system directory containing objects that appear in the network neighborhood.
	On a Windows Server 2003, it is typically `C:\Documents and Settings\`*Username*`\NetHood`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `C:\Users\`*Username*`\Roaming\Microsoft\Windows\Network Shortcuts`.
${Personal}	File system directory that serves as a common repository for documents.
	On a Windows Server 2003, it is typically: `C:\Documents and Settings\`*Username*`\My Documents`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `C:\Users\`*Username*`\Documents`.
${PrintHood}	File system directory that serves as a common repository for printer links.
	On a Windows Server 2003, it is typically `C:\Documents and Settings\`*Username*`\PrintHood`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `C:\Users\`*Username*`\AppData\Roaming\Microsoft\Windows\Printer Shortcuts`.
${Programs}	File system directory that contains the user's program groups, which are also file system directories.
	On a Windows Server 2003, it is typically `C:\Documents and Settings\`*Username*`\Start Menu\Programs`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `C:\Users\`*Username*`\AppData\Roaming\Microsoft\Windows\Start Menu\Programs`.
	◆ For a Windows 7 device, when the action is configured for logged-in user or dynamic administrator, it is typically: `C:\Users\Username\AppData\Roaming\Microsoft\Windows\Start Menu\Programs`
	◆ This variable is not resolved for the system user.

Macro	Description
${ProgramData}	File system directory that contains the user's program groups, which are also file system directories. On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `C:\ProgramData.`
${ProgramFiles}	File system directory that contains the user's program files on a 32-bit device or the user's 64-bit program files on a 64-bit device. Typically `C:\Program Files.`
${ProgramFiles32}	File system directory that contains the user's 32-bit program files on a 64-bit device. This file resolves to (typically) `C:\Program Files` on a 32-bit machine and resolves to `C:\Program Files (x86)` on a 64-bit machine. On 32-bit devices, this file system directory returns the same as ${ProgramFiles}, so that you can use it to point to 32-bit programs irrespective of the platform. For example: On a device that has the 32 bit Office application installed, you can use the following path to refer Excel.exe: `${ProgramFiles32}\Microsoft Office\Office14\EXCEL.exe` The above path works on both 64 and 32-bit devices.
${ProgramFilesCommon}	File system directory that contains the program files shared by multiple applications. Typically `C:\Program Files\Common Files.`
${Public}	File system directory that has public access to all the users on the network. On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `C:\Users\Public.`
${Recent}	File system directory that contains the user's most recently used documents. On a Windows Server 2003, it is typically `C:\Documents and Settings\`*Username*`\Recent.` On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `C:\Users\`*Username*`\AppData\Roaming\Microsoft\Windows\Recent`

Macro	Description
${SendTo}	File system directory that contains Send To menu items.
	On a Windows Server 2003, it is typically `C:\Documents and Settings\`*`Username`*`\SendTo`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `C:\Users\`*`username`*`\AppData\Roaming\Microsoft\Windows\SendTo`
${StartMenu}	File system directory containing **Start** menu items.
	On a Windows Server 2003, it is typically `C:\Documents and Settings\`*`Username`*`\Start Menu`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `C:\Users\`*`Username`*`\AppData\Roaming\Microsoft\Windows\Start Menu`.
${Startup}	File system directory that corresponds to the user's Startup program group.
	On a Windows Server 2003, it is typically `C:\Documents and Settings\`*`Username`*`\Start Menu\Programs\Startup`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `C:\Users\`*`Username`*`\AppData\Roaming\Microsoft\Windows\Startup`.
${TempDir}	Windows temporary directory.
	On a Windows Server 2003, it is typically `C:\Documents and Settings\`*`Username`*`\Local Settings\Temp`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `C:\Users\`*`Username`*`\AppData\Local\Temp`.
${Templates}	File system directory that serves as a common repository for document templates.
	On a Windows Server 2003 or Windows XP device, it is typically `C:\Documents and Settings\`*`Username`*`\Templates`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `C:\Users\`*`Username`*`\AppData\Roaming\Microsoft\Windows\Templates`.

Macro	Description
${UserProfile}	File system directory that contains the logged-in user's profile.
	On a Windows Server 2003 or Windows XP device, it is typically `C:\Documents and Settings\Username`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `C:\Users\Username`.
${WinDesktop}	Windows desktop directory
	On a Windows Server 2003, it is typically `C:\Documents and Settings\Username\Desktop`.
	On a Windows Server 2008, Windows Vista, or Windows 7 device, it is typically `C:\Users\Username\Desktop`.
${WinDir}	Windows directory. Typically `C:\WINDOWS`.
${WinDisk}	Drive letter (plus colon) for the Windows directory. Typically `C:`.
${WinSysDir}	Windows system directory. Typically `C:\WINDOWS\system32`.
${WinSysDisk}	Drive letter (plus colon) for the Windows system directory. Typically `C:`.

NOTE: The values of PATH variable alone will be appended from both the user environment and the system variable. If values of variables other than PATH are defined in volatile, user environment and system variable, then the values in the volatile environment takes precedence over that of the system variable and the user variable.

If values of variables other than PATH are not defined in volatile environment variable, the values in the user environment variable take precedence over that of the system variable.

12.2 Login Script Special System Variables

NOTE: For compatibility with traditional ZENworks, the system variable can also be specified in one of the following formats:

- *%system_variable%*

  For example, %MONTH%
- *%*system_variable%*

  For example, %*MONTH%
- *${system_variable}*

  For example, ${MONTH}

The following table lists the supported login script special system variables:

Table 12-2 *Supported Login Script Special System Variables*

Macro	Description
${COMPUTER_NAME}	The name of the computer. For example: work_pc.
${DAY}	Numeric day of the month. For example: 01, 10, 15.
${HOUR24}	Time of the day according to a 24-hour clock. For example: 02, 05, 14, 22.
${HOUR}	Hour of the day. For example: 0 = 12, 13 = 1.
${LAST_NAME}	Last name of the current user (also known as the user's eDirectory Surname attribute). For example: Jones.
${MINUTE}	Current minute. For example: 02, 59.
${MONTH}	Current month number. For example: 01 for January.
${NDAY_OF_WEEK}	Numeric day of the week. For example: 1 for Sunday, 2 for Monday.
${NETWORK}	Workstation network address. For example: 101.10.101.101
${OS_VERSION}	Version of the OS. For example: v5.00.
${OS}	OS type. For example: MSDOS, WIN98, WINNT, WIN2000, WINXP.
${PLATFORM}	Platform running. For example: WIN32NT.
${PHYSICAL_STATION}	MAC address. For example: 0000C04FD92ECA.
${SECOND}	Number of seconds. For example: 03, 54.
${SHORT_YEAR}	Short year number. For example: 97, 00.
${WINVER}	Windows version. For example: v3.11, v4.00.
${YEAR}	Full year number. For example: 2008.

12.3 Novell eDirectory Attribute Special System Variables

The ZENworks Application Window supports system variables that pull information from the attributes of the currently logged-in user.

The following sections explain the system variable syntax and provide examples:

- Section 12.3.1, "Syntax," on page 71
- Section 12.3.2, "Examples," on page 72
- Section 12.3.3, "Configuring the eDirectory Attribute Special System Variables," on page 73

12.3.1 Syntax

eDirectory attribute system variables use the following syntax:

```
%eDirectory_attribute%
```

Table 12-3 *Special System Variable Syntax*

Element	Description
%	Flags the text as a system variable. The entire system variable must be enclosed in% characters.
eDirectory_attribute	Defines the attribute to be read.
	You can use the ConsoleOne Schema Manager (available from the Tools menu) to view an eDirectory object's available attributes.

NOTE: For compatibility with traditional ZENworks, the special system variables can also be specified in one of the following formats:

◆ %system_variable%

   For example, %CN%

◆ %*system_variable*%

   For example, %*CN%

12.3.2   Examples

The following table provides examples of eDirectory attribute system variables.

Table 12-4 *Special System Variable Examples*

Macro	Description
%CN%	Returns the common name of the currently logged-in user.
%DN%	Returns the distinguished name of the currently logged-in user.
%Full Name%	Returns the full name of the currently logged-in user. This is the name defined in User object > General tab > Identification page > Full Name field.
%Given Name%	Returns the first name of the currently logged-in user. This is the name defined in User object > General tab > Identification page > Given Name field.
%Surname%	Returns the last name of the currently logged-in user. This is the name defined in the User object > General tab > Identification page > Last Name field.

The remaining system variables that are predefined by ZENworks are available in the following locations:

◆ **On Windows:** *ZENworks_Home*/microfocus/zenworks/datamodel/authsource/
   edirectory-users.zls.xml

◆ **On Linux:** /etc/opt/microfocus/zenworks/datamodel/authsource/edirectory-
   users.zls.xml

12.3.3 Configuring the eDirectory Attribute Special System Variables

To use eDirectory attributes as a reference in the bundle system variables, use the following procedures:

On the eDirectory Server

Define a name mapping between LDAP attribute types and eDirectory attribute definitions. You can log in to Novell iManager and click **Attribute Map** to do the mapping. For example, you can choose to map an eDirectory attribute named `GWMailID`, which stores the user e-mail id, to a Primary LDAP Attribute named `Mail`.

Only User attributes are supported.

For information on mapping the LDAP attribute types and eDirectory attribute, see Novell eDirectory Administration guide at the Documentation Website (http://www.novell.com/documentation/).

On the ZENworks Server

1 Edit the sample file to create a file that contains the attribute that you want to use with ZENworks:

2 Add an entry for the attribute that you want to use with ZENworks. For example:

```
<attribute name="ZEN" ldapName="Mail"
builder="com.novell.zenworks.datamodel.session.jndi.builder.StringAttr
ibuteBuilder" />
```

Replace `ZEN` with the attribute that you want to use with ZENworks and replace `Mail` with the Primary LDAP Attribute that you mapped with the eDirectory attribute named `GWMailID`.

You must use the right builder, depending on whether the syntax is a string, integer, or Boolean. The `edirectory-users-additional.zls.xml.sample` file lists the different type of builders.

3 Save the sample file as `edirectory-users-additional.zls.xml`.

4 Replace the `edirectory-users-additional.zls.xml` file on all the Primary Servers in the Management Zone.

5 Restart the zenserver service.

Sample Scenario

Create a bundle with an action that references the macro and that runs in the user impersonation mode. For example:

1. Create a bundle with a Run Script action that references the special system variable, `${ZEN}` and has the executable security level set to `Run as logged in user`.

2. Perform the bundle assignment.

    When the action is executed on the managed device, the value of the LDAP attribute is substituted for the special system variable.

In the example, the email id stored in the `GWMailID` attribute is substituted for the special system variable, `${ZEN}`. Consequently, when the action is executed on the managed device, the e-mail ID stored in the `GWMailID` attribute is displayed on the device.

12.4 Microsoft Active Directory Attribute Special System Variables

The ZENworks Application Window supports special system variables that pull information from the attributes of the currently logged-in user.

The following sections explain the system variable syntax and provide examples:

12.4.1 Syntax

Active Directory attribute special system variables use the following syntax:

```
%active-directory_attribute%
```

Table 12-5   *Special System Variable Syntax*

Element	Description
%	Flags the text as a system variable. The entire system variable must be enclosed in% characters.
active-directory_attribute	Defines the attribute to be read.

NOTE: For compatibility with traditional ZENworks, the special system variables can also be specified in one of the following formats:

- %system_variable%

  For example, %Street%
- %*system_variable*%

  For example, %*Street%

12.4.2 Examples

The following table provides examples of Active Directory attribute system variables.

Table 12-6 *Special System Variable Examples*

Special System Variables	Description
`%CN%`	Returns the common name of the currently logged-in user.
`%OU%`	Returns the organizational unit name for the currently logged-in user.
`%Full Name%`	Returns the full name of the currently logged-in user.
`%Surname%`	Returns the last name of the currently logged-in user.
`%Street%`	Returns the street address of the currently logged-in user.

The remaining special system variables that are predefined by ZENworks are available in the following locations:

12.4.3   Configuring the Active Directory Attribute Special System Variables

To use Active Directory attributes as a reference in the special system variables, use the following procedures:

On the Active Directory Server

To map existing or new attributes defined in the Active Directory schema, see the Microsoft TechNet Library (http://technet.microsoft.com/en-us/library/cc961581.aspx).

On the ZENworks Server

1 Edit the sample file to create a file that contains the attribute that you want to use with ZENworks:

2 Add an entry for the attribute that you want to use with ZENworks. For example:

```
<attribute name="ZEN" ldapName="employeeID"
builder="com.novell.zenworks.datamodel.session.jndi.builder.StringAttr
ibuteBuilder" />
```

Replace `ZEN` with the attribute that you want to use with ZENworks and replace `EmployeeID` with the LDAP Display Name in Active Directory. If the Active Directory common name for this attribute is defined as `Employee-ID`, `ZEN` now maps to the attribute `Employee-ID`.

You must use the right builder, depending on whether the syntax is a string, integer, or Boolean. The `active-directory-users-additional.zls.xml.sample` file lists the different type of builders.

3 Save the sample file as `active-directory-users-additional.zls.xml`.

4 Replace the `active-directory-users-additional.zls.xml` file on all the Primary Servers in the Management Zone.

5 Restart the zenserver service.

Sample Scenario

Create a bundle with an action that references the special system variable and that runs in the user impersonation mode. For example:

1. Create a bundle with a Run Script action that references the special system variable `${ZEN}` and has the executable security level set to `Run as logged in user`.

2. Perform the bundle assignment.

   When the action is executed on the managed device, the value of the LDAP attribute is substituted for the special system variable.

In the example, the employee id stored in the `Employee-ID` attribute is substituted for the special system variable, `${ZEN}`. Consequently, when the action is executed on the managed device, the employee ID stored in the `Employee-ID` attribute is displayed on the device.

12.5 Language Variable Special System Variables

To minimize the number of Application objects required to distribute the same application in different languages, you can use language variables to represent language-related information in MSI Application objects.

NOTE: For compatibility with traditional ZENworks, the special system variables can also be specified in one of the following formats:

- %system_variable%

  For example, %LOCALE_USER_LANG%

- %*system_variable%

  For example, %*LOCALE_USER_LANG%

The following table describes the available language variables:

Table 12-7 *Language Variable Special System Variables*

Language Variable	Description
`%LOCALE_SYS_DEFAULT_ANSI_CP%`	Retrieves the American National Standards Institute (ANSI) code page associated with the system locale. If the locale does not use an ANSI code page, the value is 0. Example: 1252
`%LOCALE_SYS_DEFAULT_OEM_CP%`	Retrieves the original equipment manufacturer (OEM) code page associated with the system locale. If the locale does not use an OEM code page, the value is 1. Example: 437

Language Variable	Description
`%LOCALE_SYS_LANGID%`	Retrieves the language identifier for the system locale. The language identifier is a standard international numeric abbreviation for the language in a country or geographical region.

Example: 0409 |
| `%LOCALE_SYS_ABBR_LANG%` | Specifies the abbreviated name of the system language. In most cases, it is created by taking the two-letter language abbreviation from the International Organization for Standardization (ISO) Standard 639 and adding a third letter, as appropriate, to indicate the sub language.

Example: ENU |
| `%LOCALE_SYS_ENG_LANG%` | Specifies the full English name of the system language from ISO Standard 639. This is always restricted to characters that can be mapped into the ASCII 127-character subset.

Example: English |
| `%LOCALE_SYS_LANG%` | Specifies the full localized name of the system language. This name is based on the localization of the product and might vary for each localized version.

Example: English (United States) |
| `%LOCALE_SYS_ISO639_LANG%` | Specifies the abbreviated name of the system language based only on ISO Standard 639.

Example: en |
| `%LOCALE_SYS_NATIVE_LANG%` | Specifies the native name of the system language.

Example: English |
| `%LOCALE_USER_DEFAULT_ANSI_CP%` | Retrieves the American National Standards Institute (ANSI) code page associated with the user locale. If the locale does not use an ANSI code page, the value is 0.

Example: 1252 |
| `%LOCALE_USER_DEFAULT_OEM_CP%` | Retrieves the original equipment manufacturer (OEM) code page associated with the user locale. If the locale does not use an OEM code page, the value is 1.

Example: 850 |
| `%LOCALE_USER_LANGID%` | Retrieves the language identifier for the user locale. The language identifier is a standard international numeric abbreviation for the language in a country or geographical region.

Example: 0c09 |

Language Variable	Description
`%LOCALE_USER_ENG_LANG%`	Specifies the full English name of the user language from ISO Standard 639. This is always restricted to characters that can be mapped into the ASCII 127-character subset.
	Example: English
`%LOCALE_USER_LANG%`	Specifies the full localized name of the user language. This name is based on the localization of the product and might vary for each localized version.
	Example: English (Australia)
`%LOCALE_USER_ISO639_LANG%`	Specifies the abbreviated name of the user language based only on ISO Standard 639.
	Example: en
`%LOCALE_USER_NATIVE_LANG%`	Specifies the native name of the user language.
	Example: English

12.6 ZENworks System Variables

12.6.1 MAX_WAIT_FOR_WIS

During bundle MSI action, if one MSI is already running on the Windows device, the Bundle MSI action fails. To address this issue, a new zone level system variable "MAX_WAIT_FOR_WIS" is introduced. By enabling the system variable, the Bundle MSI action waits for the specified time for other MSI to complete, and then fails the bundle MSI action.

For example: If the value of MAX_WAIT_FOR_WIS variable is set to 5, the Bundle MSI action waits for a maximum of 5 minutes before failing the action. If the MSI installer is available between 0 to 5 minutes, then bundle MSI action will start the installation.

12.6.2 Content_Download_Failure_Log_Level

Using this system variable, on Windows or Linux Satellite Servers, you can either prevent the logging of error messages for content replication on Satellite Servers or you can log them as warnings or error messages. The values for these actions are NoLogging, Error and Warning respectively. If no value is defined for this variable, the error messages are logged as errors.

13 Installing ZCC Helper

ZENworks ZCC Helper is a standalone application which provides a browser independent way to perform various actions such as:

- **On Windows:**
  - Icon Extractor
  - Remote Management
  - Uploading Imaging Files
  - Windows Group Policy
  - File and Directory Upload
- **On Linux:**
  - Remote Management
  - File and Directory Upload

To install ZCC Helper:

1 In ZENworks Control Center, click **Configuration**.

2 In the left navigation pane, click **Download ZENworks Tools**.

3 In the left navigation pane of the ZENworks Download page, click **Administrative Tools**.

4 Click the **Configuration** tab.

5 Depending on the device architecture (32-bit or 64-bit), download the appropriate RPM or MSI.

   novell-zenworks-zcc-helper-<version>.msi for Windows devices

   novell-zenworks-zcc-helper-<version>.rpm for Linux devices

   The above mentioned MSI and RPM is for a per-user installation. To download ZCC Helper in a common location for all users such as in a Terminal Server or in a Citrix XENapp environment, download the all users version of the MSI:

   novell-zenworks-zcc-helper-all-users-<version>.msi

   NOTE: If ZCC Helper is not installed on your Windows device and on performing any one of the actions listed above such as remote management or file upload, by default the per user MSI (novell-zenworks-zcc-helper-<version>.msi) is downloaded.

6 Save and install the ZCC Helper.

NOTE

- **All Users**
  - The all user MSI is by default installed on C drive. However, if C drive does not have sufficient space, then it is installed on a drive that has maximum free space.

    To install the MSI in a specific path, in the command line specify the destination directory (TargetDir) parameter.

For example: If `msiexec /i novell-zenworks-zcc-helper-all-users-20.0.0.3138.x86_64.msi TargetDir="%custompath%\ZCCHelper` is the custom path, then set the *ZCC_JAVA_HOME* environment variable to point to the same location provided for TargetDir.

If the `%custompath%` is `C:\ZENworks\Tools`, in the **ZCC_JAVA_HOME** variable specify the value as `C:\ZENworks\Tools\ZCCHelper`

It is recommended that you do not specify the *%ProgramFiles%* folder as the destination directory. Moreover, if the device is a **managed device**, **then it is mandatory that you do not specify *%ProgramFiles%* as the destination directory**.

  ◆ For a non-managed device, if ZCC Helper is installed in the *%ProgramFiles%* directory, then ensure that the user has sufficient rights to access the directory.

  ◆ If you are installing the all user MSI for the first time, ensure that you remove all previous installations of ZCC helper.

◆ **Windows (Per-user and All Users):**

  ◆ For 64-bit operating system, no need to install the JRE, as JRE is included with ZCC Helper.

  ◆ For 32-bit operating system, the 3rd party JRE (8.x or higher version) should be manually installed, and then set the `ZCC_JAVA_HOME` environment variable to point to where the JRE software is located. For example, in the PATH variable specify *C:\Program Files\Java\jre1.8.0_211\bin*.

◆ **Linux (Per-user):**

  ◆ On Linux device, Remote Management operations are supported on SLES 12.x, SLED 12.x devices running the GNOME display manager.

  ◆ If `novell-zenworks-rm-viewer` package is installed on the device, ensure it is uninstalled before installing ZCC Helper.

  ◆ Remote Control operations from RHEL devices are not supported.

  ◆ For Linux devices ensure that you copy the `ZENworks11-gpg-pubkey.asc` key on to the device and execute the `rpm --import ZENworks11-gpg-pubkey.asc` command to avoid any errors while installing ZCC Helper. The `ZENworks11-gpg-pubkey.asc` key is available in the ZENworks ISO.

  ◆ For 64-bit operating system, no need to install the JRE, as JRE is included with ZCC Helper. However, on 64-bit SLES 11 devices, the 3rd party JRE (8.x or higher version) should be installed and then set the `ZCC_JAVA_HOME` environment variable to point to where the JRE software is located. For example, in the PATH variable specify *C:\Program Files\Java\jre1.8.0_211\bin*.

  ◆ For 32-bit operating system, the 3rd party JRE (8.x or higher version) should be manually installed, and then set the `ZCC_JAVA_HOME` environment variable to point to where the JRE software is located. For example, in the PATH variable specify *C:\Program Files\Java\jre1.8.0_211\bin*.

13.1   Troubleshooting ZCC Helper

  ◆ While installing ZCC Helper on Linux devices, if any of the following error message is displayed, then perform the steps mentioned in the Workaround section:

```
Error setting value: Client failed to connect to the D-BUS daemon:
Did not receive a reply. Possible causes include: the remote
application did not send a reply, the message bus security policy
blocked the reply, the reply timeout expired, or the network connection
was broken.

Error setting value: Client failed to connect to the D-BUS daemon:
Did not receive a reply. Possible causes include: the remote
application did not send a reply, the message bus security policy
blocked the reply, the reply timeout expired, or the network connection
was broken.

Error setting value: Client failed to connect to the D-BUS daemon:
Did not receive a reply. Possible causes include: the remote
application did not send a reply, the message bus security policy
blocked the reply, the reply timeout expired, or the network connection
was broken.
```

Workaround: Run the following commands:

```
/usr/bin/gconftool-2 -s /desktop/gnome/url-handlers/zcclaunch/command
'/opt/novell/zenworks/zcchelper/bin/zcchelper "%s"' -t string

/usr/bin/gconftool-2 -s /desktop/gnome/url-handlers/zcclaunch/
needs_terminal false -t bool

/usr/bin/gconftool-2 -s /desktop/gnome/url-handlers/zcclaunch/enabled
true -t bool

/usr/bin/gconftool-rebuild
```

* While installing ZCC Helper on Linux devices, if any of the following error message is displayed, then perform the steps mentioned in the Workaround section:

```
/usr/bin/xdg-mime: line 545: /root/.local/share/applications/
defaults.list.new: No such file or directory

grep: /root/.local/share/applications/defaults.list.new: No such file
or directory

/usr/bin/xdg-mime: line 547: /root/.local/share/applications/
defaults.list.new: No such file or directory

/usr/bin/xdg-mime: line 549: /root/.local/share/applications/
defaults.list.new: No such file or directory

mv: cannot stat `/root/.local/share/applications/defaults.list.new': No
such file or directory
```

Workaround: Run the following commands:

```
mkdir .local/share/applications

xdg-mime default zcchelper.desktop x-scheme-handler/zcclaunch || true

update-desktop-database
```

- After installing ZCC Helper on 64-bit SLES 11 devices, ZCC Helper might not launch.

  Workaround: Install 3rd party JRE (8.x or higher version) manually, and then set the ZCC_JAVA_HOME path variable.
- If you are using wayland display manager, ZCC Helper might not launch.

  Workaround: Logout and log into the device using the x11 display manager.

13.1.1 ZCC Helper fails to work with the L4 Switch

If the ZENworks Management Zone is configured with an L4 switch, then ZCC Helper might not work as expected.

Workaround: If the ZENworks Management Zone is configured with an L4 switch, then perform the following steps manually on all ZCC servers in the zone:

1. The ZCC servers should be directly reachable from the management console.

   Append the following setting to the existing settings in the custom-config.xml file:

   ```
   <setting id="changezcclaunchServer">
           <value>true</value>
       </setting>
   ```

   The custom-config.xml file location:
   - **On Windows:** ${ZENWORKS_HOME} \services\zenserver\webapps\zenworks\WEB-INF\conf\
   - **On Linux:** /opt/microfocus/zenworks/share/tomcat/webapps/zenworks/WEB-INF/conf/
2. Restart ZENworks server services.

   After configuring the settings, ZCC Helper contacts the Primary Server behind the L4 switch that generated the zcclaunch custom protocol token, instead of contacting the L4 switch.

14 Troubleshooting ZENworks Control Center

An error is displayed while logging into ZENworks Control Center

Source: ZENworks 2020 Update 3, ZENworks Control Center

Explanation and Possible Cause:After updating to ZENworks 2020 Update 3, unable to access ZENworks Control Center, and the following error message is displayed:

> *Unable to Complete request at this time. Please contact your system administrator.*

> The error message is displayed only when your browser language is not one of the languages supported by ZENworks.

Action: Switch the browser language to English and log into ZCC again.

Unable to login message is displayed consistently

Explanation: Unable to login message is displayed consistently even after providing the correct credentials.

Possible Cause: This might be due any of the following reasons:

- Invalid credentials
- Database Server or User Source is not accessible.

Action: Ensure that the database or user source is accessible.

Unable to Pick a Date from the Calendar Dropdown in Chrome and Firefox browsers

Source: ZENworks

Explanation: In ZENworks Control Center, when you click to pick a date, the calendar dropdown is not displayed.

This issue might be observed in the following sections:

- While selecting a date range in the Zone Audit Dashboard and the Zone Audit Events page.
- While selecting a date during certificate management (Change CA, Remint CA or Remint Certificate in the **Configuration** > **Certificates** section).

Action: To select the date, use the Internet Explorer browser.

An HTTP request is not redirected to HTTPS if IIS is running on the Primary Server

Source: ZENworks; ZENworks Control Center.

Explanation: During installation, the setup checks to see if the default HTTP port (80) and HTTPS port (443) are in use. If the ports are in use by another application (such as IIS), you are prompted to use alternative ports. In this case, you must access ZENworks Control Center via the port it is using and not access IIS.

Action: Although http://*Primary_Server_IP_address* works if ZENworks Control Center is using port 80, http://*Primary_Server_IP_address*:### (where ### is the port Tomcat is using) always works.

ZENworks Control Center throws a java.lang.NoClassDefFoundError Exception

Source: ZENworks; ZENworks Control Center.

Explanation: When you use ZENworks Control Center to perform an operation, you might encounter a `java.lang.NoClassDefFoundError` exception.

Action: Restart the Novell ZENworks Server service:

On Windows: Do the following:

1. On the Windows desktop, click **Start** > **Settings** > **Control Panel**.
2. Double-click **Administrative Tools** > **Services**.
3. Restart **Novell ZENworks Server**.

On Linux: At the console prompt, enter `/etc/init.d/novell-zenserver restart`.

Opening links in a new tab or new window of ZENworks Control Center might fail to display the page

Source: ZENworks; ZENworks Control Center.

Explanation: While browsing ZENworks Control Center, if you choose to open a link in a new tab or a new window, the page might fail to display.

Action: Open the link in the same window.

Logging in to ZENworks Control Center or navigating within ZENworks Control Center by using Firefox 3.*x* might display a blank page

Source: ZENworks; ZENworks Control Center.

Explanation: If you are accessing ZENworks Control Center across the network by using Firefox 3.*x*, you might see a blank page when you log in to ZENworks Control Center or navigate within ZENworks Control Center.

Action: Do one of the following:

⬧ Use the Firefox Web browser to open `about:config`, then change the value of **browser.cache.memory.enable** to **False**.

⬧ Refresh the Web browser to reload the ZENworks Control Center page every time ZCC displays a blank page.

⬧ Use any other ZENworks supported Web browser to access ZENworks Control Center.

For more information about the supported Web browsers, see *Administrator Browser Requirements* in the *ZENworks Server Installation*.

ZENworks Control Center displays a warning message indicating that some of the ZENworks features might behave incorrectly

Source: ZENworks; ZENworks Control Center.

Explanation: When you deploy ZENworks with an external database, if the Primary Server time is not synchronized with the ZENworks database server time, you might see the following warning message on the ZENworks Control Center Login page:

```
Some of the ZENworks features might behave incorrectly
because the time of the current Primary Server and the time
of the ZENworks database server are not in sync.
```

Action: Synchronize the Primary Server time with that of the Database Server.

The Nessus scan report for ZENworks Control Center shows that the site is vulnerable to cross-site scripting attacks

Source: ZENworks; ZENworks Control Center.

Explanation: If you run a Nessus scan for the ZENworks Control Center, the report shows that the site is vulnerable to cross-site scripting attacks. This issue is addressed by the ZENworks Control Center and there is no actual vulnerability.

Action: Ignore this message. For more information, see "User Source Authentication" in the ZENworks User Source and Authentication Reference.

Unable to manage reports without Super Administrator rights

Source: ZENworks; ZENworks Control Center.

Explanation: Without super administrator rights, you are not able to create, edit or delete workstation reports.

NOTE: For more information see TID 7008889 (http://www.novell.com/support/kb/doc.php?id=7008889), in the Novell Support Knowledgebase.

Action: The relevant rights have to be configured using ZENworks Control Center.

1 Log into ZENworks Control Center as an administrator.

2 Click the **Configuration** tab.

3 In the **Administrators** panel, select the name of the user who requires rights to the reports.

4 Click the **Rights** tab.

5 In **Administrator Tasks** section, in the left pane of ZENworks Control Center, click **Inventory Report Rights**. The Inventory Report Rights are displayed.

6 Select the folders to which the user requires the rights.

7 From the **Edit** drop-down menu, select **Assign Full Rights**.

For more information about configuring Inventory Report rights, see "Inventory Report Rights" in the *ZENworks Asset Inventory Reference*.

8 Repeat steps 2 through 4 and in the **Administrator Tasks** section, in the left pane of ZENworks Control Center, click **Asset Management Report Rights**. The Asset Management Report Rights are displayed.

9 Select the folders to which the user requires the rights.

10 From the **Edit** drop-down menu, select **Assign Full Rights**.

For more information about configuring Asset Management Report rights, see "Configuring Report Rights" in the *ZENworks Asset Management Reference*.

Unable to login in to ZENworks Control Center in Internet Explorer 8 on Windows 8 machine

Source: ZENworks; ZENworks Control Center

Explanation: When you launch ZENworks Control Center url on Internet Explorer 8 on Windows 8 machine and try logging in, an error message is displayed in the browser status bar.

Possible Cause: Security option **Allow websites to prompt for information using scripted windows** is enabled.

Action: Disable security option **Allow websites to prompt for information using scripted windows**.

Email notifications with SSL to the SMTP Server fail

Source: ZENworks; ZENworks Control Center

Possible Cause: The certificate from the SMTP Server may not be authenticated.

Action: To be able to send emails, import the certificate for authentication as follows:

1 Navigate to the OpenSSL directory and execute the following command:

```
openssl s_client -showcerts -starttls smtp -connect
[SMTP SERVER IP]: 25
```

2 Copy the contents of the certificate displayed in the console from "----BEGIN CERTIFICATE----" to "----END CERTIFICATE----" including the "----" lines.

3 Save this to a text file. For example, `smtpcert.txt`. For more information on how to generate or import GroupWise certificate, see:.

   ◆ Server Certificates and SSL Encryption
   ◆ Securing GWIA Connections with SSL

4 Import the certificate authority into the Java trusted CA keystore file.

On Windows Primary Server: If ZENworks is installed in the `C:\Program Files x(86)` folder, then in the command prompt, go to `C:\Program Files x(86)\Novell\ZENworks\share\java\jre\bin>` and run the following command:

```
.keytool -importcert -trustcacerts -alias smtpcert -file
<saved text file name with full path> -keystore
"C:\Program
Files\x(86)\Novell\ZENworks\share\java\jre\lib\security
\cacerts" -storepass changeit
```

On Linux Primary Server: Run the following command from the Java installed path:

```
/usr/java/jdk1.6.0_24/jre/bin/keytool -importcert -
trustcacerts -alias smtpcert -file "<saved text filename
with full path>" -keystore /usr/java/jdk1.6.0_24/jre/
lib/security/cacerts -storepass changeit
```

ZENworks Control Center is vulnerable to SQL injection attacks

Source: ZENworks; ZENworks Control Center

Explanation: SQL injection is an attack which injects an SQL query through the input data from the client to the application. This injection exploit can read sensitive data from the database, modify data, and execute administrative operations on the database such as database shutdown and so forth.

Action: In order to prevent or minimize the impact of SQL injection attacks on ZCC, you can do the following:

- As ZENworks has a strong implementation of the access control layer through its Roles and Rights, by properly configuring these for the users, you can ensure that they have access only to the information they are entitled to. To configure roles and rights through ZCC, see ZENworks Administrator Accounts and Rights Reference.

- Restrict the access to ZCC servers only to authorized persons. You may restrict ZCC access from a network subnet or IP range, so that unauthorized access to ZCC is prevented. For more information, see Securing DMZ Servers.