Novell
ZENworks® 10 Configuration Management

10.0.3

SYSTEM ADMINISTRATION
REFERENCE

www.novell.com

Novell®

Novell Trademarks

For Novell trademarks, see

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

This *Novell ZENworks 10 Configuration Management System Administration Reference* provides information about general administrative tasks required to manage your Novell® ZENworks® 10 Configuration Management system. The information in this guide is organized as follows:

Audience

This guide is intended for ZENworks 10 Configuration Management administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to the Novell Documentation Feedback site (http://www.novell.com/documentation/feedback.html) and enter your comments there.

Additional Documentation

ZENworks Configuration Management is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the ZENworks 10 Configuration Management documentation (http://www.novell.com/documentation/zcm10/index.html).

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux*, should use forward slashes as required by your software.

ZENworks Control Center 1

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.

The following sections provide information about using ZENworks Control Center:

1.1 Accessing ZENworks Control Center

1 Using a Web browser that meets the requirements listed in "Administration Browser Requirements" in the *ZENworks 10 Configuration Management Installation Guide*, enter the following URL:

```
https://ZENworks_Server_Address
```

Replace *ZENworks_Server_Address* with the IP address or DNS name of the ZENworks Server. 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.`

3 In the *Password* field, type the Administrator password created during installation.

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 1.2, "Changing the Default Login Disable Values," on page 12.

4 Click *Login* to display ZENworks Control Center.

1.2 Changing the Default Login Disable Values

You can change the number of login tries and the timeout length for when a login is disabled 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 of 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 adminstrator unsuccessfully attempts a login on one Primary Server, that administrator is kept from logging in to other Primary Servers in the zone. The interval that the administrator account is kept from logging in again 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\novell\zenworks\conf\datamodel\zdm.xml

Linux:
/etc/opt/novell/zenworks/datamodel/zdm.xml

2 Add the following lines into 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 the 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 Section 3.2.4, "Restarting a ZENworks Service," on page 34.

1.3 Accessing ZENworks Control Center through Novell iManager

ZENworks 10 Configuration Management 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 a number of other 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 will 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/imanager_admin_27/data/b8qrsg0.html) 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
```

Replace *ZENworks_Server_Address* with the IP address or DNS name of the ZENworks Server.

8 Click the ZENworks icon to launch ZENworks Control Center.

1.4 Navigating ZENworks Control Center

The following Bundles page represents a standard view in ZENworks Control Center.

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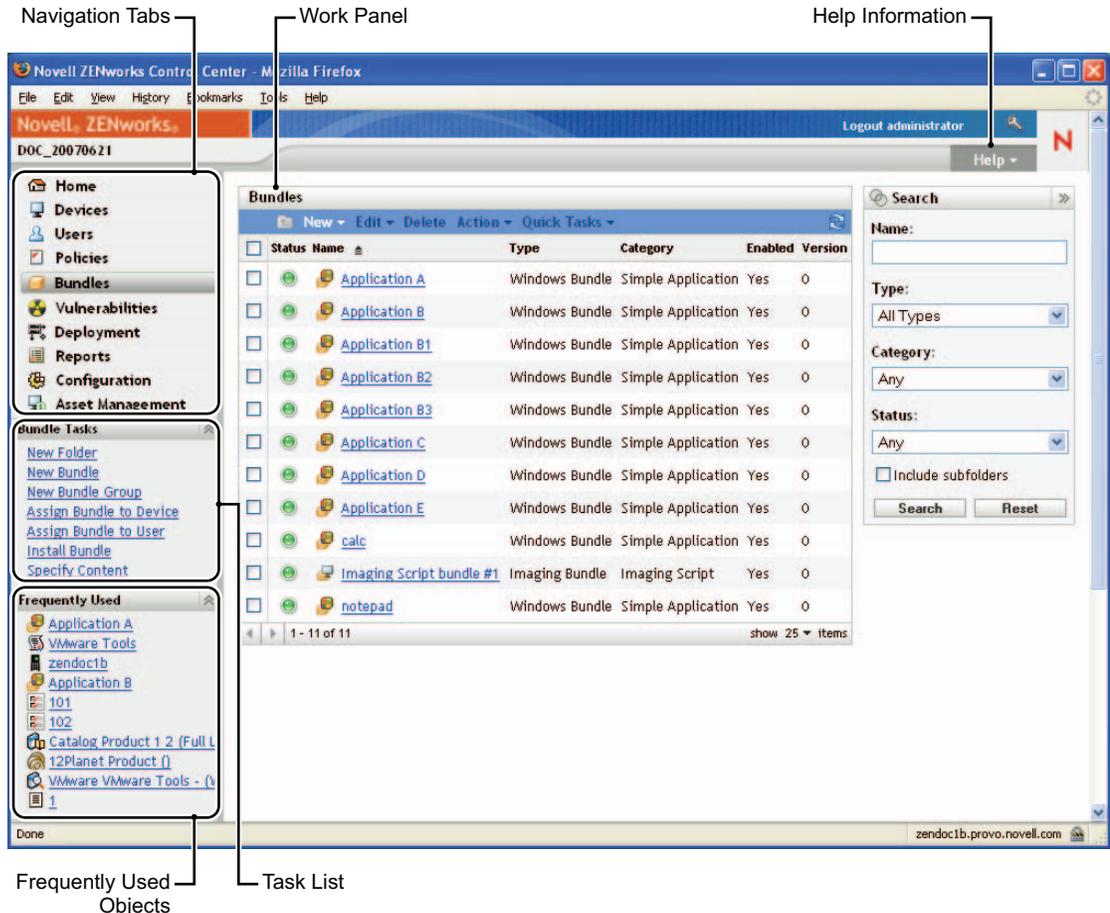
Navigation Tabs: The tabs in the left pane let you navigate among the functional areas of ZENworks. For example, the Bundles page shown above lets you manage tasks associated with software distribution and imaging.

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.

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: Bundles and Search. The Bundles panel lists the software and imaging bundles that have been created; you use this panel to manage the bundles. The Search panel lets you filter the Bundles panel based on criteria such as a bundle's name, type, category, 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.

1.5 Changing the Timeout Value for ZENworks Control Center

By default, ZENworks Control Center has a 30-minute timeout value, so if you leave ZENworks Control Center idle on your computer for more than 30 minutes, you are prompted to log in again to continue.

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.

To increase or decrease the timeout value, you modify two XML files on the ZENworks Server. The change applies only to that server's ZENworks Control Center. Therefore, any devices that launch ZENworks Control Center from that server experience the same timeout value.

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:

1 On the ZENworks Server, open the `web.xml` file in a text editor.

 ◆ **Windows:** `\Novell\ZENworks\share\tomcat\webapps\ zenworks\WEB-INF\web.xml`

 ◆ **Linux:** `/opt/novell/zenworks/share/tomcat/webapps/zenworks/ WEB-INF/web.xml`

2 Locate the `<session-timeout>` entry.

3 Increase or decrease the timeout value, as needed.

 Specify the timeout value in minutes.

4 Save the `web.xml` file.

5 Open the `config.xml` file in a text editor.

 The `config.xml` file is located in the same directory as the `web.xml` file:

 ◆ **Windows:** `\Novell\ZENworks\share\tomcat\webapps\ zenworks\WEB-INF\config.xml`

 ◆ **Linux:** `/opt/novell/zenworks/share/tomcat/webapps/zenworks/ WEB-INF/config.xml`

6 Locate the `<setting id="timeout">` entry.

7 Set the timeout value to the same number as you entered in the `web.xml` file.

8 Save the `config.xml` file.

9 Restart the ZENworks Server by restarting the zen-server service.

 For instructions, see Chapter 3, "ZENworks Server," on page 31.

1.6 Using the 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 1.5, "Changing the Timeout Value for ZENworks Control Center," on page 15), the `config.xml` file lets you control several additional configuration settings. However, with the exception of the timout value, you should not need to modify the `config.xml` settings. In some cases, you should not modify a setting unless instructed by Novell Technical Services.

1 On the ZENworks Server, open the `config.xml` file in a text editor.

- Windows server path: `\Novell\ZENworks\share\tomcat\webapps\zenworks\WEB-INF\config.xml`

- Linux server path: `opt/novell/zenworks/share/tomcat/webapps/zenworks/WEB-INF/config.xml`

2 Modify the desired setting. All settings begin with `<setting id=`.

timeout: Specify the timeout value in minutes. 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 where you have launched ZENworks Control Center. If you change this value, you must also change the <session-timeout> entry in the web.xml file. See Section 1.5, "Changing the Timeout Value for ZENworks Control Center," on page 15).

debug.enabled: Change the value to *false* if you do not want any messages written to the ZCC 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 Novell Technical Services.

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

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 the *Do not show me this again* option.

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

3 Save the `config.xml` file.

4 Restart the ZENworks Server by restarting the zen-server service. See Chapter 3, "ZENworks Server," on page 31 for instructions if necessary.

Administrators 2

During installation of Novell® ZENworks® 10 Configuration Management, a default ZENworks administrator account (named Administrator) is created. This account provides rights to administer all of your Management Zone.

You can create additional administrator accounts that provide various levels of access to the Management Zone. For example, you could create an administrator account that enables the administrator to assign bundles to devices, but doesn't allow the administrator to create bundles. Or, you could create an administrator account that allows access to all management tasks, except those pertaining to your Management Zone configuration (user sources, registration, configuration settings, and so forth).

You can use ZENworks Control Center (ZCC) or the zman command line utility to create and modify administrator accounts. The following procedures explain how to perform these tasks by using ZCC. If you prefer the zman command line utility, see "Administrator Commands" in the *ZENworks 10 Configuration Management Command Line Utilities Reference*.

2.1 Managing Administrator Accounts

The following sections help you create and manage administrator accounts:

2.1.1 Creating Administrators

To create an administrator account:

1 In ZCC, click the *Configuration* tab.

Configuration	Registration	System Information	Asset Inventory	System Updates	Asset Management

Management Zone Settings ⪡

Server Hierarchy ⪡

Administrators ⪢

New Edit ▾ Delete

☐ Name ⬘ Full Name Username in User Source

No items available.

User Sources ⪡

Licenses ⪡
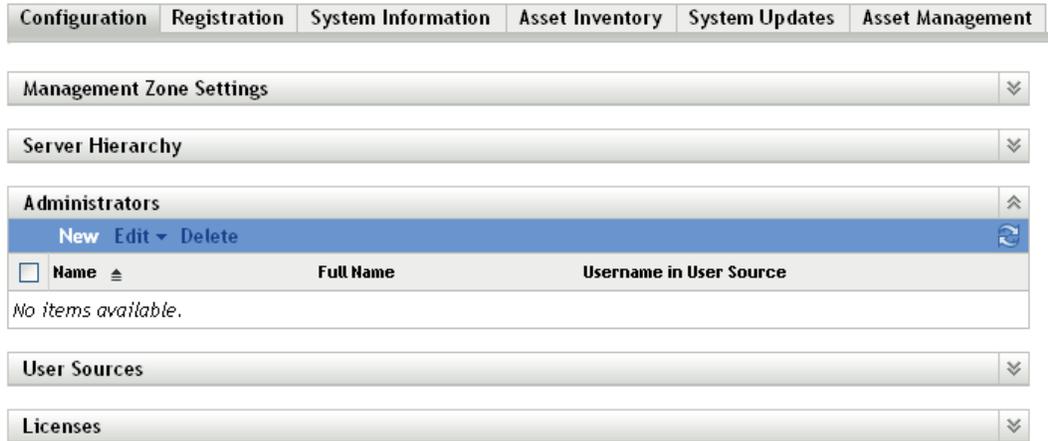
2 In the Administrators panel, click *New* to display the Add New Administrator dialog box.

Add new Administrator ? ✕

There are two ways to create an Administrator:

◉ Create a new Administrator providing name and password.

Administrator Name:

[   ] *

Full Name:

[   ]

Password:

[   ] *

Retype Password:

[   ] *

○ Based on user(s) in a user source
will use the same credential defined in Authoritative source.

Add Remove

☐ Name In Folder

No items selected, click add to select items

☐ Give this Administrator the same rights as I have.
Fields marked with an asterisk are required.

[OK]   [Cancel]

The Add New Administrator dialog box lets you create a new administrator account by providing a name and password, or you can create a new administrator based on an existing

user in the user source. Optionally, you can give the new administrator the same rights that the logged-in administrator has.

3 Fill in the fields.

Create a New Administrator by Providing Name, Password: Select this option if you want to create a new administrator account by manually specifying the name and password.

Administrator login names with Unicode* characters are case-sensitive. Make sure that you use the correct case for each character in the login name when it contains Unicode characters.

The new administrator can change the password the first time he or she logs in by clicking the key icon located next to the *Logout* link in the upper right corner of ZENworks Control Center.

Based on User(s) in a User Source: Select this option if you want to create a new administrator account based on information from your user source. To do so, click *Add*, then browse for and select the user you want.

The newly created administrator account is granted View rights to all objects in the Management Zone. To grant additional rights, or to limit the administrator's rights to specific folders only, you need to modify the rights.

Give this Administrator the Same Rights as I Have: Select this option if you want to assign the new administrator the same rights that you have as the currently-logged in administrator.

4 When you have finished filling in the fields, click *OK* to add the new administrator.

You can also use the `admin-create` command in zman to create an administrator account. For more information, see "Administrator Commands" in the *ZENworks 10 Configuration Management Command Line Utilities Reference*.

2.1.2 Deleting Administrators

1 In ZCC, click the *Configuration* tab.

2 In the Administrators panel, select the check box in front of the administrator's name, then click *Delete*.

You can also use the `admin-delete` command in zman to delete an administrator account. For more information, see "Administrator Commands" in the *ZENworks 10 Configuration Management Command Line Utilities Reference*.

2.1.3 Renaming Administrators

1 In ZCC, click the *Configuration* tab.

2 In the Administrators panel, select the check box in front of the administrator's name, click *Edit*, then click *Rename*.

3 Specify the new name, then click *OK*.

You can also use the `admin-rename` command in zman to rename an administrator account. For more information, see "Administrator Commands" in the *ZENworks 10 Configuration Management Command Line Utilities Reference*.

2.1.4 Changing Administrator Passwords

1 In ZCC, click the *Configuration* tab.

2 In the Administrators panel, select the check box in front of the administrator, click *Edit*, then click *Set Password* to display the Change Administrator Password Dialog box.

3 Fill in the fields, then click *OK*.

2.2 Managing Administrator Rights

The following sections help you manage existing administrator accounts and their assigned rights:

* Section 2.2.1, "Assigning Super Administrator Rights," on page 20
* Section 2.2.2, "Assigning Additional Rights," on page 20
* Section 2.2.3, "Modifying Assigned Rights," on page 20
* Section 2.2.4, "Removing Assigned Rights," on page 21

2.2.1 Assigning Super Administrator Rights

A Super Administrator has all right to perform all actions in ZCC. For more information about all of the rights that a Super Administrator has, see Section 2.3, "Rights Descriptions," on page 21. If you grant an administrator Super Administrator rights, any assigned rights that have been allowed, denied, or not set are overridden.

1 In ZCC, click the *Configuration* tab.

2 Click the administrator in the *Name* column of the Administrators panel.

3 Select the *Super Administrator* check box.

4 Click *OK*.

2.2.2 Assigning Additional Rights

1 In ZCC, click the *Configuration* tab.

2 Click the administrator in the *Name* column of the Administrators panel.

3 Click *Add*, then click an item from the drop-down list.

4 Fill in the fields.

For more information, see Section 2.3, "Rights Descriptions," on page 21.

5 Click *OK*.

You can also use the `admin-rights-set` command in zman to assign additional rights for an administrator account. For more information, see "Administrator Commands" in the *ZENworks 10 Configuration Management Command Line Utilities Reference*.

2.2.3 Modifying Assigned Rights

1 In ZCC, click the *Configuration* tab.

2 Click the administrator in the *Name* column of the Administrators panel.

3 Select the check box in front of the assigned right.

4 Click *Edit*, then modify the settings.

For more information, see Section 2.3, "Rights Descriptions," on page 21.

5 Click *OK*.

2.2.4 Removing Assigned Rights

1 In ZCC, click the *Configuration* tab.

2 Click the administrator in the *Name* column of the Administrators pane.

3 Select the check box in front of the assigned right.

4 Click *Delete*.

You can also use the `admin-rights-delete` command in zman to delete assigned rights for an administrator account. For more information, see "Administrator Commands" in the *ZENworks 10 Configuration Management Command Line Utilities Reference*.

2.3 Rights Descriptions

When you create additional administrator accounts you can provide full access to your zone or you can create accounts with limited rights. For example, you could create an administrator account that enables the administrator to assign bundles to devices but doesn't allow the administrator to create bundles. Or, you could create an administrator account that allows access to all management tasks except those pertaining to Management Zone configuration (user sources, registration, configuration settings, and so forth). For information about creating additional administrators, see "Creating Administrators" on page 17.

You can also add, modify, or remove the assigned rights for an existing administrator. For more information, see Section 2.2.2, "Assigning Additional Rights," on page 20, Section 2.2.3, "Modifying Assigned Rights," on page 20, or Section 2.2.4, "Removing Assigned Rights," on page 21.

The following sections contain additional information about the various rights that you can assign:

- Section 2.3.1, "Administrator Rights," on page 22
- Section 2.3.2, "Bundle Rights," on page 22
- Section 2.3.3, "Contract Management Rights," on page 22
- Section 2.3.4, "Device Rights," on page 23
- Section 2.3.5, "Document Rights," on page 24
- Section 2.3.6, "Inventoried Device Rights," on page 24
- Section 2.3.7, "License Management Rights," on page 25
- Section 2.3.8, "Policy Rights," on page 25
- Section 2.3.9, "Quick Task Rights," on page 26
- Section 2.3.10, "Remote Management Rights," on page 27
- Section 2.3.11, "Reporting Rights," on page 27
- Section 2.3.12, "User Rights," on page 27
- Section 2.3.13, "ZENworks User Group Rights," on page 28
- Section 2.3.14, "Zone Rights," on page 28

2.3.1 Administrator Rights

The Administrator Rights dialog box lets you allow the selected administrator to grant rights to other administrators and to create or delete administrator accounts for your Management Zone.

The following rights are available:

- ◆ **Grant Rights:** Allow or deny the administrator the rights necessary to grant rights to other administrators.
- ◆ **Create/Delete:** Allow or deny the administrator the rights necessary to create or delete administrator accounts.

2.3.2 Bundle Rights

The Bundle Rights dialog box lets you select folders containing bundles, then modify the rights associated with those folders.

Bundles

To select the folder that contains the bundles for which you want to assign rights, click *Add* to display the Subjects dialog box, then browse for and select the folders for which you want to assign rights.

Bundle Rights

The *Privileges* section lets you grant the selected administrator rights to create or modify bundles, create or modify groups, and create or modify folders.

The following rights are available:

- ◆ **Modify:** Allow or deny the administrator the rights necessary to modify existing bundles.
- ◆ **Create/Delete:** Allow or deny the administrator the rights necessary to create or delete bundles.
- ◆ **Modify Groups:** Allow or deny the administrator the rights necessary to modify existing groups.
- ◆ **Create/Delete Groups:** Allow or deny the administrator the rights necessary to create or delete groups.
- ◆ **Modify Group Membership:** Allow or deny the administrator the rights necessary to modify the list of bundles contained in bundle groups.
- ◆ **Modify Folder:** Allow or deny the administrator the rights necessary to modify folders.
- ◆ **Create/Delete Folders:** Allow or deny the administrator the rights necessary to create or delete folders.

2.3.3 Contract Management Rights

The Contract Management Rights dialog box lets you select folders containing contracts, then modify the rights associated with contracts and folders.

Contract Management

To select the folder that contains the contracts for which you want to assign rights, click *Add* to display the Subjects dialog box, then browse for and select the folders for which you want to assign rights.

Privileges

- ◆ **Modify:** Allow or deny the administrator the rights necessary to modify the existing contracts.
- ◆ **Create/Delete:** Allow or deny the administrator the rights necessary to create or delete contracts.
- ◆ **Modify Folder:** Allow or deny the administrator the rights necessary to modify folders.
- ◆ **Create/Delete Folders:** Allow or deny the administrator the rights necessary to create or delete folders.

2.3.4 Device Rights

The Device Rights dialog box lets you select folders containing devices, then modify the rights associated with those folders.

Devices

To select the folder that contains the devices for which you want to assign rights, click *Add* to display the Subjects dialog box, then browse for and select the folders for which you want to assign rights.

Device Rights

The *Privileges* section lets you grant the selected administrator rights to work with devices, including device groups and folders, allowing the administrator to assign policies and bundles to devices.

The following rights are available:

- ◆ **Modify:** Allow or deny the administrator the rights necessary to modify the existing device objects.
- ◆ **Create/Delete:** Allow or deny the administrator the rights necessary to create or delete device objects.
- ◆ **Modify Groups:** Allow or deny the administrator the rights necessary to modify existing groups.
- ◆ **Create/Delete Groups:** Allow or deny the administrator the rights necessary to create or delete groups.
- ◆ **Modify Group Membership:** Allow or deny the administrator the rights necessary to modify the list of devices contained in device groups.
- ◆ **Modify Folder:** Allow or deny the administrator the rights necessary to modify folders.
- ◆ **Create/Delete Folders:** Allow or deny the administrator the rights necessary to create or delete folders.
- ◆ **Modify Settings:** Allow or deny the administrator the rights necessary to modify device settings.

- **Assign Policies:** Allow or deny the administrator the rights necessary to assign policies to devices.
- **Assign Bundles:** Allow or deny the administrator the rights necessary to assign bundles to devices.

2.3.5 Document Rights

The Document Rights dialog box lets you select folders containing documents, then modify the rights associated with documents and folders.

Documents

To select the folder that contains the documents for which you want to assign rights, click *Add* to display the Subjects dialog box, then browse for and select the folders for which you want to assign rights.

Privileges

- **Modify:** Allow or deny the administrator the rights necessary to reassign existing documents.
- **Create/Delete:** Allow or deny the administrator the rights necessary to import or delete documents.
- **Modify Folder:** Allow or deny the administrator the rights necessary to modify folders.
- **Create/Delete Folders:** Allow or deny the administrator the rights necessary to create or delete folders.

2.3.6 Inventoried Device Rights

The Inventoried Device Rights dialog box lets you select folders containing devices, then modify the rights associated with those folders.

Devices

To select the folder that contains the inventoried devices for which you want to assign rights, click *Add* to display the Subjects dialog box, then browse for and select the folders for which you want to assign rights.

Inventoried Device Rights

The *Privileges* section lets you grant the selected administrator rights to work with inventoried devices, including device groups and folders.

The following rights are available:

- **Modify:** Allow or deny the administrator the rights necessary to modify existing inventoried device objects.
- **Create/Delete:** Allow or deny the administrator the rights necessary to create or delete inventoried device objects.
- **Modify Groups:** Allow or deny the administrator the rights necessary to modify existing groups.

- ◆ **Create/Delete Groups:** Allow or deny the administrator the rights necessary to create or delete groups.
- ◆ **Modify Group Membership:** Allow or deny the administrator the rights necessary to modify the list of devices contained in device groups.
- ◆ **Modify Folder:** Allow or deny the administrator the rights necessary to modify folders.
- ◆ **Create/Delete Folders:** Allow or deny the administrator the rights necessary to create or delete folders.
- ◆ **Modify Settings:** Allow or deny the administrator the rights necessary to modify inventoried device settings.

2.3.7 License Management Rights

The License Management Rights dialog box lets you select folders containing licenses, then modify the rights associated with licenses and folders.

License Management

To select the folder that contains the licenses for which you want to assign rights, click *Add* to display the Subjects dialog box, then browse for and select the folders for which you want to assign rights.

Privileges

- ◆ **Modify:** Allow or deny the administrator the rights necessary to modify the existing licenses.
- ◆ **Create/Delete:** Allow or deny the administrator the rights necessary to create or delete licenses.
- ◆ **Modify Folder:** Allow or deny the administrator the rights necessary to modify folders.
- ◆ **Create/Delete Folders:** Allow or deny the administrator the rights necessary to create or delete folders.

2.3.8 Policy Rights

The Policy Rights dialog box lets you select folders containing policies, then modify the rights associated with those folders.

Policies

To select the folder that contains the policies for which you want to assign rights, click *Add* to display the Subjects dialog box, then browse for and select the folders for which you want to assign rights.

Policy Rights

The *Privileges* section lets you grant the selected administrator rights to work with policies, including device groups and folders.

The following rights are available:

- ◆ **Modify:** Allow or deny the administrator the rights necessary to modify the existing policies.

- **Create/Delete:** Allow or deny the administrator the rights necessary to create or delete policies.
- **Modify Groups:** Allow or deny the administrator the rights necessary to modify existing groups.
- **Create/Delete Groups:** Allow or deny the administrator the rights necessary to create or delete groups.
- **Modify Group Membership:** Allow or deny the administrator the rights necessary to modify the list of policies contained in policy groups.
- **Modify Folders:** Allow or deny the administrator the rights necessary to modify folders.
- **Create/Delete Folders:** Allow or deny the administrator the rights necessary to create or delete folders.

2.3.9 Quick Task Rights

The Quick Tasks Rights dialog box lets you select folders containing devices, then modify the Quick Task rights associated with those folders.

Quick Tasks are tasks that appear in ZCC task lists (for example, Server Tasks, Workstation Tasks, Bundles Tasks, and so forth). When you click a task, either a wizard launches to step you through the task or a dialog box appears in which you enter information to complete the task.

You can use the Quick Tasks Rights dialog box to allow or deny the selected administrator the rights to perform certain tasks using Quick Tasks.

Devices

To select the folder that contains the device for which you want to assign rights, click *Add* to display the Subjects dialog box, then browse for and select the folders for which you want to assign rights.

Quick Task Rights

The following rights are available:

- **Shutdown/Reboot/Wake Up Devices:** Specify whether the administrator can shut down, reboot, or wake up the devices in the folders you selected in the list.
- **Execute Processes:** Allow or deny the administrator the rights necessary to execute processes on the devices.
- **Refresh ZENworks Adaptive Agent:** Allow or deny the administrator the rights necessary to refresh the ZENworks Adaptive Agent on devices.
- **Install/Launch Bundles:** Allow or deny the administrator the rights necessary to install or launch bundles. The administrator must also have Assign Bundles rights for devices to install or launch bundles using Quick Task options.
- **Apply Image:** Allow or deny the administrator the rights necessary to apply an image to devices.
- **Take Image:** Allow or deny the administrator the rights necessary to take an image of a device.
- **Inventory:** Allow or deny the administrator the rights necessary to inventory devices.

2.3.10 Remote Management Rights

The Remote Management Rights dialog box lets you select folders containing devices and users, then modify the Remote Management rights associated with those folders. Granting Remote Execute rights allows the administrator to execute processes in the system space.

Devices/Users

To select the folder that contains the devices and users for which you want to assign rights, click *Add* to display the Subjects dialog box, then browse for and select the folders for which you want to assign rights.

Remote Management Rights

The following rights are available:

- **Remote View:** Allow or deny the administrator the rights necessary to remotely view devices.
- **Remote Diagnostics:** Allow or deny the administrator the rights necessary to perform remote diagnostic procedures on devices.
- **Remote Execute:** Allow or deny the administrator the rights necessary to remotely execute processes on devices.
- **Transfer files:** Allow or deny the administrator the rights necessary to transfer files to or from devices.
- **Remote Control:** Allow or deny the administrator the rights necessary to remotely control devices.

2.3.11 Reporting Rights

The Reporting Rights dialog box lets you allow or deny the administrator the rights to create, delete, execute, or publish reports.

2.3.12 User Rights

The User Rights dialog box lets you select folders containing users, then modify the rights associated with those folders.

Users

To select the folder that contains the users for which you want to assign rights, click *Add* to display the Subjects dialog box, then browse for and select the folders for which you want to assign rights.

User Rights

The *Privileges* section lets you grant the selected administrator rights to work with devices, including device groups and folders, allowing the administrator to assign policies and bundles to devices.

The following rights are available:

Modify ZENworks Group Membership: Allow or deny the rights necessary to modify ZENworks group membership. If you select this option, you must also grant rights to *Modify ZENworks Group Membership* under *ZENworks User Group Rights*.

Assign Policies: Allow or deny the administrator the rights necessary to assign policies to users.

Assign Bundles: Allow or deny the administrator the rights necessary to assign bundles to users.

2.3.13 ZENworks User Group Rights

The ZENworks User Group Rights dialog box lets you allow or deny the administrator the rights to create, delete, or modify groups and to modify group membership.

The following rights are available:

* **Modify Groups:** Allow or deny the administrator the rights necessary to modify existing groups.
* **Create/Delete Groups:** Allow or deny the administrator the rights necessary to create or delete groups.
* **Modify ZENworks Group Membership:** Allow or deny the administrator the rights necessary to modify the ZENworks group membership. If you select this option, you must also grant rights to *Modify ZENworks Group Membership* under *User Rights*.
* **Assign Policies:** Allow or deny the administrator the rights necessary to modify the list of policies contained in policy groups.
* **Assign Bundles:** Allow or deny the administrator the rights necessary to modify the list of bundles contained in policy groups.

2.3.14 Zone Rights

The Zone Rights dialog box lets you modify the administrator's rights to administer settings in your ZENworks Management Zone.

* **Modify User Sources:** Allow or deny the administrator the rights necessary to modify user sources.

  A user source is an LDAP directory that contains the users to whom you want to distribute ZENworks content. When you define a user source, you also define the source containers from which you want to read users and user groups.

  Modifying user sources includes adding, removing, or renaming user sources and assigning policies or bundles to user sources.
* **Create/Delete User Sources:** Allow or deny the administrator the rights necessary to create or delete user sources.
* **Modify Settings:** Allow or deny the administrator the rights necessary to modify your Management Zone settings.

  The Management Zone settings let you manage the global configuration settings for your Management Zone. These global configuration settings are inherited by other objects (devices, users, and folders) within your Management Zone and remain in effect unless they are overridden on those objects.

- **Modify Zone Infrastructure:** Allow or deny the administrator the rights necessary to modify Zone infrastructure.

- **Configure Registration:** Allow or deny the administrator the rights necessary to configure device registration.

  Registration lets you manage the various configuration settings for registering devices as managed devices in the Management Zone. Registration lets you create registration keys or registration rules to help you register devices. A registration key lets you apply group and folder assignments to devices as they register. A registration rule lets you apply group and folder assignments to folders if the device meets the rule criteria.

- **Discovery:** Allow or deny the administrator the rights necessary to manage discovery tasks.

- **Approve Updates:** Allow or deny the administrator the rights necessary to approve updates.

- **Apply Updates:** Allow or deny the administrator the rights necessary to apply updates.

- **Deployment:** Allow or deny the administrator the rights necessary to perform deployment operations.

  Deployment lets you discover network devices and deploy the ZENworks Adaptive Agent to them so that they become managed devices in your Management Zone.

ZENworks Server

<div style="text-align: right; font-size: xx-large;">3</div>

The ZENworks® Server is the backbone of the ZENworks system. It communicates with the ZENworks Adaptive Agent on managed devices to deliver software, apply policies, collect inventory, and perform other management tasks. It stores content to be delivered to devices and images to be used for imaging devices. It communicates with other ZENworks Servers to replicate content throughout the servers and distribution points in the system.

The following sections provide additional information about the ZENworks Server:

3.1 ZENworks Services on a Windows Server

When running on a Windows* server, a ZENworks Server includes the following services:

Table 3-1 *ZENworks Services on Windows*

Service	Service Name	Description
Proxy DHCP Service	novell-proxydhcp	Used with a standard DHCP server to inform PXE-enabled devices of the IP address of the Novell® TFTP server.
TFTP Service	novell-tftp	Used by PXE-enabled devices to request files that are needed to perform imaging tasks.
ZENworks Agent Service	zenworkswindowsservice novell-zmd	Used to enable the server as a managed device.
ZENworks Datastore	dbsrv10	Embedded database used for storing ZENworks objects and resources.
ZENworks Loader	zenloader	Used for loading and controlling the Java* services that perform ZENworks Server tasks.
ZENworks Preboot Policy Service	novell-zmgprebootpolicy	Used by PXE-enabled devices to check for assigned preboot policies and work.
ZENworks Preboot Service	novell-pbserv	Used to provide imaging services to a device. This includes sending and receiving image files, discovering assigned Preboot bundles, acting as session master for multicast imaging, and so forth.

Service	Service Name	Description
ZENworks Remote Management	nzrwinvnc	Used to enable remote management of the server.
ZENworks Server	zenserver	Used for communicating with the ZENworks Agent.
ZENworks Services Monitor	zenwatch	Used to monitor the status of the ZENworks services.
ZENworks Imaging Agent	ziswin	Used to save and restore image-safe data on the server (as a managed device). Only runs when launched by the ZENworks Agent.

The services reside in the `\novell\zenworks\bin` directory on a ZENworks Server. Refer to the following sections for instructions to help you control the ZENworks services:

- Section 3.1.1, "Checking the Status of a ZENworks Service," on page 32
- Section 3.1.2, "Starting a ZENworks Service," on page 32
- Section 3.1.3, "Stopping a ZENworks Service," on page 32

3.1.1 Checking the Status of a ZENworks Service

1 On the server, click *Start*, select *Administrative Tools > Services*, then review the status of the services listed in Table 3-1 on page 31.

3.1.2 Starting a ZENworks Service

1 On the server, click *Start*, select *Administrative Tools > Services*.

2 Select the service you want to start (see Table 3-1 on page 31), then click *Start the service.*

3.1.3 Stopping a ZENworks Service

1 On the server, click *Start*, select *Administrative Tools > Services*.

2 Select the service you want to stop (see Table 3-1 on page 31), then click *Stop the service.*

3.2 ZENworks Services on a Linux Server

The ZENworks Server includes the following services:

Table 3-2 *ZENworks Services on Linux*

Service	Service Name	Description
Proxy DHCP Service	novell-proxydhcp	Used with a standard DHCP server to inform PXE-enabled devices of the IP address of the Novell TFTP server.

Service	Service Name	Description
TFTP Service	novell-tftp	Used by PXE-enabled devices to request files that are needed to perform imaging tasks.
ZENworks Agent Service	novell-zmd	Used to enable the server as a managed device.
ZENworks Datastore	sybase-asa	Used to run the embedded SQL Anywhere database.
ZENworks Loader	novell-zenloader	Used for loading and controlling the Java services that perform ZENworks Server tasks.
ZENworks Preboot Policy Service	novell-zmgprebootpolicy	Used by PXE-enabled devices to check for assigned preboot policies and work.
ZENworks Preboot Service	novell-pbserv	Used to provide imaging services to a device. This includes sending and receiving image files, discovering assigned Preboot bundles, acting as session master for multicast imaging, and so forth.
ZENworks Server	novell-zenserver	Used for communicating with the ZENworks Agent.
ZENworks Services Monitor	novell-zenmntr	Used to monitor the status of the ZENworks services.
ZENworks Imaging Agent	novell-zenagent	Used to save and restore image-safe data on the server (as a managed device). Only runs when launched by the ZENworks Agent.

The services reside in the `/etc/init.d` directory. Refer to the following sections for instructions to help you control the ZENworks services:

- Section 3.2.1, "Checking the Status of a ZENworks Service," on page 33
- Section 3.2.2, "Starting a ZENworks Service," on page 33
- Section 3.2.3, "Stopping a ZENworks Service," on page 34
- Section 3.2.4, "Restarting a ZENworks Service," on page 34

3.2.1 Checking the Status of a ZENworks Service

1 At the server command prompt, enter the following command:

```
/etc/init.d/servicename status
```

Replace *servicename* with the name of the service as listed in Table 3-2 on page 32.

3.2.2 Starting a ZENworks Service

1 At the server command prompt, enter the following command:

```
/etc/init.d/servicename start
```

Replace *servicename* with the name of the service as listed in .

2 To start all services, use the following command:

```
/opt/novell/zenworks/bin/novell-zenworks-configure Start
```

3.2.3 Stopping a ZENworks Service

To stop a service, use the following command:

```
/etc/init.d/servicename stop
```

Replace *servicename* with the name of the service as listed in .

3.2.4 Restarting a ZENworks Service

To restart a service that is already running, use the following command:

```
/etc/init.d/servicename restart
```

Replace *servicename* with the name of the service as listed in .

3.3 Configuring Additional Access to a ZENworks Server

If you have managed devices that are unable to authenticate to the IP address or DNS name of a ZENworks Server, such as devices outside the firewall or devices using a proxy server, you can specify additional IP addresses or DNS names for the ZENworks Server that can be used by the devices for access to the server.

-
-

3.3.1 Addressing Non-Detectable IP Address Conditions

The Non-Detectable IP Addresses panel lets you specify the addresses that can be used to access the ZENworks Server when the server's IP address cannot be found by a device.

For example, assume that you've configured a proxy server to handle traffic for the ZENworks Server and the devices that need to access the ZENworks Server cannot detect the ZENworks Server's IP address. To ensure that the devices can access the ZENworks Server through the proxy server, you enter the IP address of the proxy server.

1 In ZENworks Control Center, click *Devices* in the left pane, in the Devices panel select *Servers*, select a server object, click the *Settings* tab, click *Infrastructure Management*, then select *Non-detectable IP Addresses*.

2 Fill in the following fields:

IP Address: Standard dotted-decimal notation. For example, `123.45.167.100.`

Optional CIDR Subnet Mask: Use this field if you want to specify multiple addresses based on standard CIDR (Classless Inter-Domain Routing) notation. With CIDR, the dotted decimal

portion of the IP address (in the *IP Address* field) is interpreted as a 32-bit binary number that has been broken into four 8-bit bytes. You can use this field to enter the prefix length, which is the number of shared initial bits, counting from the left side of the address. The prefix length can range from 0 to 32, with 8, 16, 24, and 32 being commonly used numbers. For example, `123.45.167.100` with an optional CIDR submask (or prefix length) of 24 matches all IP addresses that start with `123.45.167`.

3 Click *Add* to add the address to the list.

4 Repeat the above steps to add additional IP addresses.

5 If necessary, use the *Move Up* and *Move Down* buttons to reorder the list.

The IP addresses are used in the order listed, from top to bottom.

6 When you are finished adding addresses, click *Apply* or *OK* to save the addresses.

3.3.2 Addressing Non-Detectable DNS Name Conditions

The Additional DNS Names panel lets you specify additional names that can be used to access the ZENworks Server when the server's DNS name cannot be found by a device.

For example, assume that you've configured a proxy server to handle traffic for the ZENworks Server and the devices cannot detect the ZENworks Server by its DNS name. To ensure that the devices can access the ZENworks Server through the proxy server, you enter the DNS name of the proxy server.

The DNS names added in this panel are distributed to all managed devices for them to use in connecting to the server.

To add a DNS name:

1 In ZENworks Control Center, click *Devices* in the left pane, in the Devices panel select *Servers*, select a server object, click the *Settings* tab, click *Infrastructure Management*, then select *Additional DNS Names*.

2 In the *List of Server DNS Names* field, specify the DNS name for the IP address of the server (such as a proxy server) that the devices can access.

3 Click *Add* to add the DNS name to the list.

IMPORTANT: Do not add the main DNS name of ZENworks Server, nor the DNS name of any of the devices that need to access the ZENworks Server. Only add DNS names of the intermediary devices that are used by managed devices to connect to the ZENworks Server.

4 If necessary, use the *Move Up* and *Move Down* buttons to reorder the list.

The DNS names are used in the order listed, from top to bottom.

5 When you are finished adding addresses, click *Apply* or *OK* to save the addresses.

3.4 Uninstalling a ZENworks Server

Instructions for uninstalling a ZENworks Server are provided in "Uninstalling ZENworks 10 Configuration Management" in the *ZENworks 10 Configuration Management Installation Guide*.

Server Hierarchy

4

Your Management Zone's server hierarchy determines the relationships among the ZENworks® Primary Servers and Content Distribution Points. These relationships control the flow of content and information within the zone. Proper configuration can help you to *minimize* network traffic between network segments connected by slow links.

4.1 Understanding Server Hierarchy Relationships

The following sections provide information to help you understand these relationships:

4.1.1 Primary Servers: Peer Versus Parent/Child Relationships

By default, each Primary Server that you add to the system is created as a peer to all other Primary Servers. Being in a peer relationship enables a Primary Server to:

- Have direct write access to the ZENworks database so that it can add information (inventory, messages, and status).
- Retrieve device configuration information directly from the database.
- Pull content (bundles and policies) from any Primary Server.

Direct write access to the ZENworks database requires a JDBC*/ODBC connection. If a Primary Server is located on the network such that it cannot effectively access the ZENworks database via a JDBC/ODBC connection, you can configure the Primary Server as a child of another Primary Server that does have direct write access to the database. Being in a child relationship requires a Primary Server to:

- Use HTTP to roll up inventory, message, and status information to its parent Primary Server, which then writes the information to the database.
- Retrieve device configuration information through its parent Primary Server.

In general, you should try to maintain peer relationships between your Primary Servers unless your network connections do not allow it. However, you can add Content Distribution Points to aid in minimizing network traffic.

Any managed device (server or workstation) in the Management Zone other than a Primary Server can be a Content Distribution Point.

4.1.2 Content Distribution Point Relationships

A Content Distribution Point is a managed device that is able to distribute content (bundles and policies) to other devices. When you set up a device to function as a Content Distribution Point, you must specify a Primary Server as its parent. The Content Distribution Point device receives all content from its parent Primary Server.

4.1.3 Changing the Parent-Child Relationships of Primary Servers

You can move a Primary Server to be a peer or child of other Primary Servers:

Making a Primary Server a Child

You can place a Primary Server as a child of another Primary Server. In doing so, this child Primary Server no longer writes directly to the ZENworks database; instead, it passes its information on to its parent Primary Server who does so.

You cannot change the level or location of a Content Distribution Point using the *Move* option.

To make a Primary Server a child of another server:

1 In ZENworks Control Center, click the *Configuration* tab.
2 In the Server Hierarchy panel, select the check box in front of the Primary Server you want to make a child.
3 Click *Move* to display the *Move Device* dialog box.
4 Select the Primary Server that you want to be its parent server.
5 Click *OK*.

Making a Primary Server a Peer

This places the Primary Server back to the first level of the hierarchy, or up to be a child of another Primary Server if it is nested more than one level deep.

When you move a Primary Server back up to the first level, it now writes directly to the ZENworks database.

To make a child Primary Server a peer to your other servers, or to change its parent server:

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

2 In the Server Hierarchy panel, select the check box in front of the Primary Server you want to make a peer.

3 Click *Move* to display the *Move Device* dialog box.

4 Do one of the following:

- ◆ Select *None* to move it up to the first level of servers in the listing.
- ◆ Select another Primary Server that is listed to make it a child of that server.

5 Click *OK*.

4.2 Managing Content Distribution Points

For information on managing Content Distribution Points, see Chapter 9, "Content Distribution Point," on page 75.

4.3 Changing the Primary Server Roll-Up Schedules

Typically, each Primary Server gathers information from the devices that use it as a collection server, then adds the information to the ZENworks database so that it can be viewed in ZENworks Control Center. However, if a Primary Server has been demoted to a child of another Primary Server, it no longer has access to the ZENworks database. Its parent instead completes the roll-up of information to the database.

To edit the various roll-up schedules for the Primary Server devices in the Server Hierarchy that are children of other Primary Servers:

- ◆ Section 4.3.1, "Changing the Inventory Roll-Up Schedule," on page 39
- ◆ Section 4.3.2, "Changing the Message Roll-Up Schedule," on page 40
- ◆ Section 4.3.3, "Changing the Status Roll-Up Schedule," on page 40

4.3.1 Changing the Inventory Roll-Up Schedule

The inventory roll-up schedule determines how often a child Primary Server sends collected inventory information to its parent Primary Server. The parent then includes the information in the ZENworks database.

The default inventory roll-up schedule is every 5 minutes. To change the schedule:

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

2 In the Server Hierarchy panel, select the check box in front of the child Primary Server whose inventory roll-up schedule you want to change.

3 Click *Action > Edit Inventory Roll-Up Schedule*.

4 Use the *Days*, *Hours*, and *Minutes* fields to specify how often you want the inventory rolled up.

Typically, this length of time should be longer than the time specified for the schedules of the Collection role that are children of this Primary Server.

5 Click *OK*.

4.3.2 Changing the Message Roll-Up Schedule

The message roll-up schedule determines how often a child Primary Server sends collected messages (errors, warning, informational, and so forth) to its parent Primary Server. The parent then includes the messages in the ZENworks database.

The default message roll-up schedule is every 5 minutes. To change the schedule:

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

2 In the Server Hierarchy panel, select the check box in front of the child Primary Server whose message roll-up schedule you want to change.

3 Click *Action > Edit Message Roll-Up Schedule*.

4 Use the *Days*, *Hours*, and *Minutes* fields to specify how often you want the messages rolled up.

Typically, this length of time should be longer than the time specified for the schedules of the Collection role that are children of this Primary Server.

5 Click *OK*.

4.3.3 Changing the Status Roll-Up Schedule

The status roll-up schedule determines how often a child Primary Server sends policy and bundle status information to its parent Primary Server. The parent then includes the information in the ZENworks database.

The default status roll-up schedule is every 5 minutes. To change the schedule:

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

2 In the Server Hierarchy panel, select the check box in front of the child Primary Server whose status roll-up schedule you want to change.

3 Click *Action > Edit Status Roll-Up Schedule*.

4 Use the *Days*, *Hours*, and *Minutes* fields to specify how often you want the status information rolled up.

Typically, this length of time should be longer than the time specified for the schedules of the Collection role that are children of this Primary Server.

5 Click *OK*.

4.4 Managing the Content Distribution Point's Port

You can change the default port number that a Content Distribution Point uses.

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

2 In the Server Hierarchy panel, select the check box in front of the Content Distribution Point whose port number you want to change.

You can only select one device at a time for changing the port number.

3 Click *Action > Edit Port*.

4 Change the port number, then click *OK*.

4.5 Deleting a Primary Server Object from the Listing

This option allows you to clean up the Server Hierarchy listing by removing unusable server objects. It only removes the Primary Server object from the listing; it does not uninstall the ZENworks software from the server.

The purpose if this option is to remove an unusable Primary Server from the Server Hierarchy listing when that server can no longer be used in the Management Zone. For example, if you uninstall ZENworks from a server, but the object isn't for some reason removed from the Server Hierarchy listing, or a server has a hardware malfunction that makes it unusable in the zone, you can use this option to remove the object from the Server Hierarchy list.

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

2 In the Server Hierarchy panel, select the check box in front of the Primary Server that you want to remove from the zone.

3 Click *Action > Delete ZENworks Server*.

4 Confirm the removal, then click *OK*.

4.6 Changing the Primary Server Roll-Up Schedules

Typically, each Primary Server gathers information from the devices that use it as a collection server, then adds the information to the ZENworks database so that it can be viewed in ZENworks Control Center. However, if a Primary Server has been demoted to a child of another Primary Server, it no longer has access to the ZENworks database. Its parent instead completes the roll-up of information to the database.

To edit the various roll-up schedules for the Primary Server devices in the Server Hierarchy that are children of other Primary Servers:

- Section 4.6.1, "Changing the Inventory Roll-Up Schedule," on page 41
- Section 4.6.2, "Changing the Message Roll-Up Schedule," on page 42
- Section 4.6.3, "Changing the Status Roll-Up Schedule," on page 42

4.6.1 Changing the Inventory Roll-Up Schedule

The inventory roll-up schedule determines how often a child Primary Server sends collected inventory information to its parent Primary Server. The parent then includes the information in the ZENworks database.

The default inventory roll-up schedule is every 5 minutes. To change the schedule:

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

2 In the Server Hierarchy panel, select the check box in front of the child Primary Server whose inventory roll-up schedule you want to change.

3 Click *Action > Edit Inventory Roll-Up Schedule*.

4 Use the *Days*, *Hours*, and *Minutes* fields to specify how often you want the inventory rolled up.

Typically, this length of time should be longer than the time specified for the schedules of the Collection role that are children of this Primary Server.

5 Click *OK*.

4.6.2 Changing the Message Roll-Up Schedule

The message roll-up schedule determines how often a child Primary Server sends collected messages (errors, warning, informational, and so forth) to its parent Primary Server. The parent then includes the messages in the ZENworks database.

The default message roll-up schedule is every 5 minutes. To change the schedule:

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

2 In the Server Hierarchy panel, select the check box in front of the child Primary Server whose message roll-up schedule you want to change.

3 Click *Action > Edit Message Roll-Up Schedule*.

4 Use the *Days*, *Hours*, and *Minutes* fields to specify how often you want the messages rolled up.

Typically, this length of time should be longer than the time specified for the schedules of the Collection role that are children of this Primary Server.

5 Click *OK*.

4.6.3 Changing the Status Roll-Up Schedule

The status roll-up schedule determines how often a child Primary Server sends policy and bundle status information to its parent Primary Server. The parent then includes the information in the ZENworks database.

The default status roll-up schedule is every 5 minutes. To change the schedule:

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

2 In the Server Hierarchy panel, select the check box in front of the child Primary Server whose status roll-up schedule you want to change.

3 Click *Action > Edit Status Roll-Up Schedule*.

4 Use the *Days*, *Hours*, and *Minutes* fields to specify how often you want the status information rolled up.

Typically, this length of time should be longer than the time specified for the schedules of the Collection role that are children of this Primary Server.

5 Click *OK*.

4.7 Managing the Content Distribution Point's Port

You can change the default port number that a Content Distribution Point uses.

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

2 In the Server Hierarchy panel, select the check box in front of the Content Distribution Point whose port number you want to change.

You can only select one device at a time for changing the port number.

3 Click *Action > Edit Port*.

4 Change the port number, then click *OK*.

4.8 Deleting a Primary Server Object from the Listing

This option allows you to clean up the Server Hierarchy listing by removing unusable server objects. It only removes the Primary Server object from the listing; it does not uninstall the ZENworks software from the server.

The purpose if this option is to remove an unusable Primary Server from the Server Hierarchy listing when that server can no longer be used in the Management Zone. For example, if you uninstall ZENworks from a server, but the object isn't for some reason removed from the Server Hierarchy listing, or a server has a hardware malfunction that makes it unusable in the zone, you can use this option to remove the object from the Server Hierarchy list.

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

2 In the Server Hierarchy panel, select the check box in front of the Primary Server that you want to remove from the zone.

3 Click *Action > Delete ZENworks Server*.

4 Confirm the removal, then click *OK*.

ZENworks Adaptive Agent

5

The ZENworks® Adaptive Agent is part of the Novell® ZENworks 10 Configuration Management software that lets a ZENworks administrator manage devices over the network. The ZENworks Adaptive Agent, commonly referred to as the Adaptive Agent, provides services that help an administrator do the following without visiting individual devices:

- Deliver software, patches, and other files to devices.
- Manage policies that determine the behavior of devices.
- Take inventory of device hardware and software.
- Access devices from a remote location to troubleshoot and fix problems with hardware and software.

Each of these services is provided through the use of modules that plug in to the Adaptive Agent. The default modules included with the Adaptive Agent are the Bundles module, Policies module, Inventory module, Remote Management module, and Distribution Point module. Depending on the services implemented by the administrator, one or more of these modules might not be active on devices. For example, if an administrator does not intend to remotely access workstations, the Remote Management module might not be installed.

You can use ZENworks Control Center to configure the ZENworks Adaptive Agent's settings.

The following sections contain more information:

5.1 Configuring ZENworks Adaptive Agent Settings

You can choose whether or not to let users uninstall the Adaptive Agent, configure the Agent's cache, set retry settings, and enable or disable the Remote Management agent.

You can configure settings at three levels:

- **Management Zone:** The setting applies to all devices in the Management Zone.
- **Device Folder:** The setting applies to all devices contained within the folder or its subfolders. Overrides the Management Zone setting.
- **Device:** The setting applies only to the device for which it is configured. Overrides the settings established at the Management Zone and folder levels.

The following sections contain more information:

5.1.1 Configuring Agent Settings on the Management Zone Level

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

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

3 Click *ZENworks Agent*.

4 Fill in the fields. For more information, see Section 5.1.4, "ZENworks Agent Settings," on page 49.

5 Click *OK* to apply the changes.

5.1.2 Configuring Agent Settings on the Device Folder Level

1 In ZENworks Control Center, click the *Devices* tab.
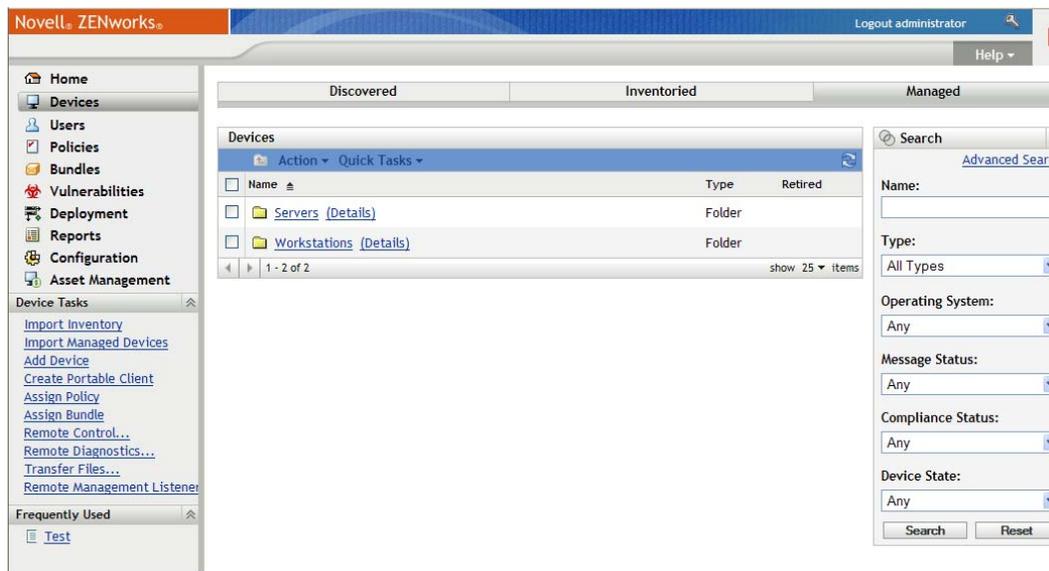
2 Click the *Servers* or *Workstations* folder.

3 Click *Details* next the folder for which you want to configure settings.

4 Click the *Settings* tab, click *Device Management*, then click *ZENworks Agent*.
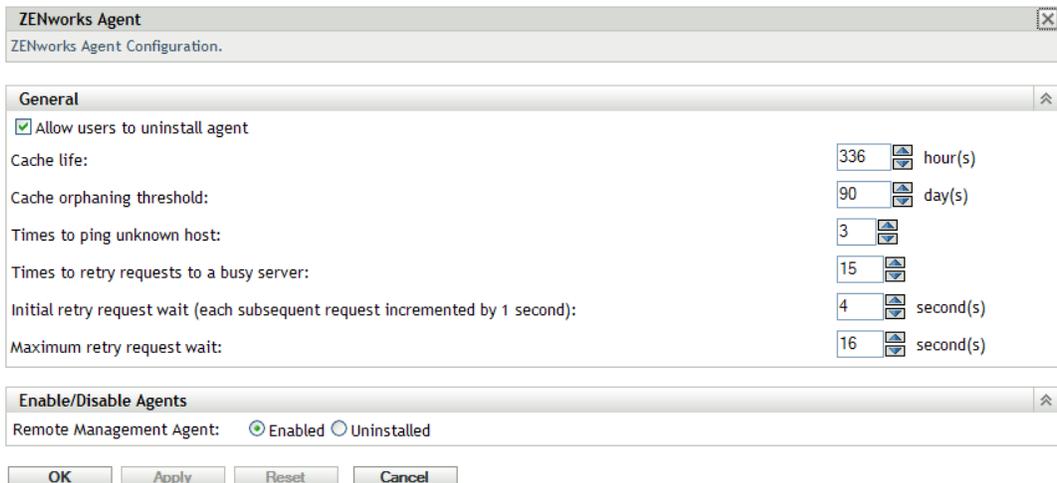
5 Fill in the fields. For more information, see Section 5.1.4, "ZENworks Agent Settings," on page 49.

6 Click *OK* to apply the changes.

5.1.3 Configuring Agent Settings on the Device Level

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

2 Click the *Servers* or *Workstations* folder.

3 Click the device for which you want to configure settings.

4 Click the *Settings* tab, click *Device Management*, then click *ZENworks Agent*.

```
┌─────────────────────────────────────────────────────────────────────────┐
│ ZENworks Agent                                                      [X]   │
│ ZENworks Agent Configuration.                                            │
├─────────────────────────────────────────────────────────────────────────┤
│ General                                                              ⌃    │
│ ☑ Allow users to uninstall agent                                         │
│ Cache life:                                        336 [▲▼] hour(s)       │
│ Cache orphaning threshold:                          90 [▲▼] day(s)        │
│ Times to ping unknown host:                          3 [▲▼]              │
│ Times to retry requests to a busy server:           15 [▲▼]              │
│ Initial retry request wait (each subsequent request incremented by 1 second):  4 [▲▼] second(s) │
│ Maximum retry request wait:                         16 [▲▼] second(s)     │
├─────────────────────────────────────────────────────────────────────────┤
│ Enable/Disable Agents                                                ⌃    │
│ Remote Management Agent:     ⦿ Enabled ○ Uninstalled                     │
│  [ OK ]   [ Apply ]   [ Reset ]   [ Cancel ]                             │
└─────────────────────────────────────────────────────────────────────────┘
```
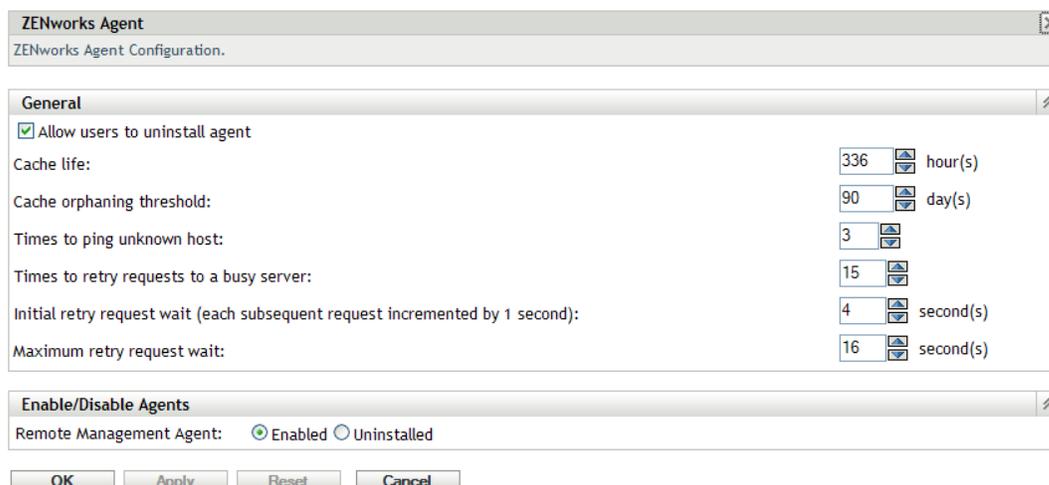
5 Fill in the fields. For more information, see Section 5.1.4, "ZENworks Agent Settings," on page 49.

6 Click *OK* to apply the changes.

5.1.4 ZENworks Agent Settings

The following sections contain more information:

-
-

General

You can configure the ZENworks Adaptive Agent's cache, whether or not users can uninstall the Adaptive Agent, and set retry settings.

You can configure the following settings on the ZENworks Agent General panel:

- **Allow Users to Uninstall Agent:** Enable this option if you want users to be able to uninstall the ZENworks Adaptive Agent.

- **Cache Hours to Live** The ZENworks Adaptive Agent's cache directory contains content data used by the agent. Each piece of data, referred to as a cache entry, is stored in the cache database.

  When a cache entry is added to the cache database, it is assigned a creation time and an expiration time. The creation time is simply the time it was added to the database. The expiration time is the creation time plus the number of hours specified by the *Cache Hours to Live* setting (by default, 336 hours or 14 days). Take, for example, a cache entry that is added on June 10 at 3:00 p.m. Using the default*Cache Hours to Live* setting, the expiration time is set to June 24 at 3:00 p.m.

  The agent does not attempt to update a cache entry until after the entry's expiration time. At that point, the agent updates the cache entry the next time it contacts the ZENworks Server to refresh its information.

  NOTE: Updates to expired cache entries occur only for cache entries that are content-related (bundles, policies, configuration settings, registration settings, and so forth). Updates to cache

entries that are event-related (remote management, inventory, reporting, and so forth) only occur at the time the event takes place on the device.

A higher*Cache Hours to Live* setting reduces the traffic load on your network because cache entries are refreshed less frequently. A lower setting provides newer information but increases the traffic load.

It is important to note that this setting affects only how often the agent requests updates to a cache entry. Cache entries can also be updated before their expiration time if information is changed in ZENworks Control Center that causes the information to be pushed from the ZENworks Server to the agent.

- **Cache Orphaning Days Threshold:** Over a period of time, it is possible for entries to be inserted in the cache database but not removed. This can cause the cache to grow unnecessarily.

An orphan is an entry that is inserted into the cache but not accessed within the number of days specified by the *Cache Orphaning Days Threshold* setting. Take, for example, a cache entry that is accessed on July 1 at 10:00 a.m. Using the default *Cache Orphaning Days Threshold* setting (30 days), the entry becomes an orphan if it is not accessed again before July 31 at 10:00 a.m.

A higher *Cache Orphaning Days Threshold* setting ensures that infrequently accessed information is not removed from the cache database. A lower setting can reduce the cache size.

Enable/Disable Agents

The ZENworks Adaptive Agent uses several modules to perform policy, bundle, remote management, and inventory functions on a device. By default, all modules are installed on a device.

You can cause the Remote Management module to not be installed with the Adaptive Agent. The other modules (Bundle, Policy, and Inventory) cannot be disabled; they are always installed.

IMPORTANT: Changing this option does not uninstall the Remote Management module from currently managed devices. It only causes it to not be installed to new devices.

On the *Enable/Disable Agents* panel, click *Enabled* (the default) to have the module installed with the Adaptive Agent, or click *Uninstalled* to not have it installed.

To disable the module on a selected folder or device, click *Override Settings* on the *Enable/Disable Agents* panel.

To enable the module on a selected folder or device and return the settings to the Management Zone level, click *Revert*.

5.2 Configuring ZENworks Explorer

You can configure common settings for the ZENworks Explorer component of the ZENworks Adaptive Agent.

You can define the settings at three levels:

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

The following sections contain more information:

5.2.1 Configuring ZENworks Explorer Settings on the Management Zone Level

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

2 Click the *Content* tab.
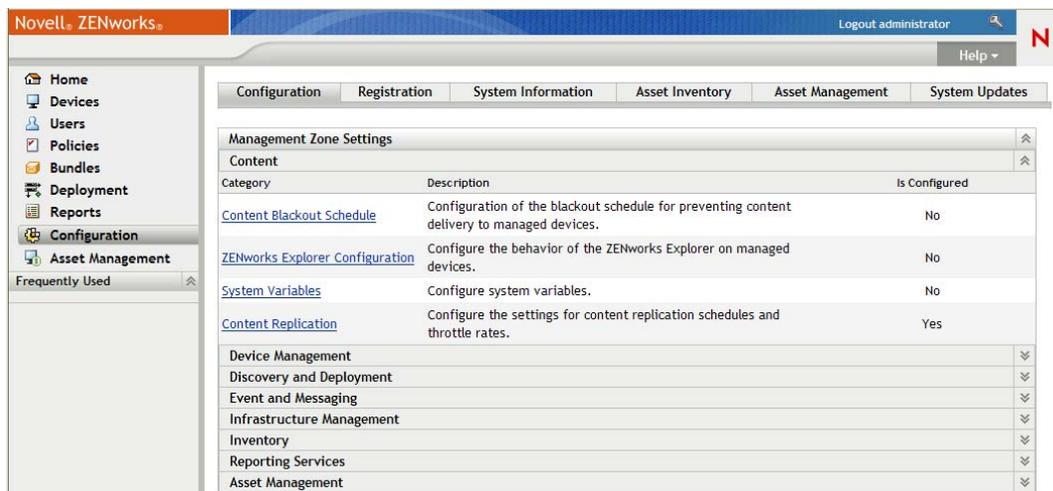
3 Click *ZENworks Explorer Configuration*.
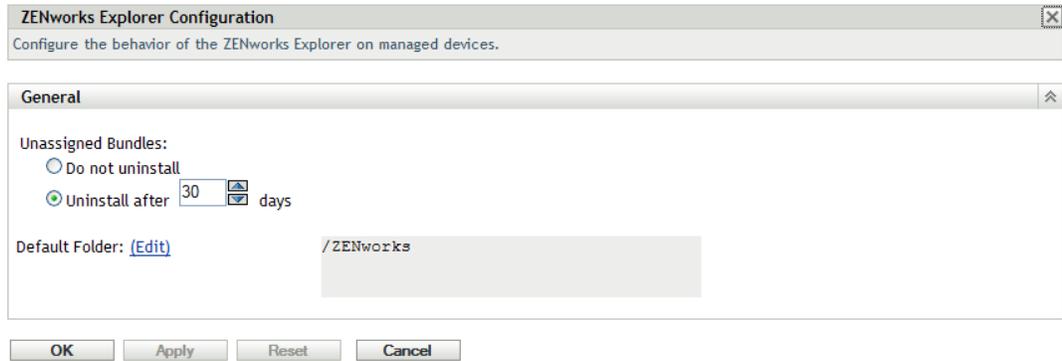
4 Fill in the fields. For more information, see Section 5.2.4, "ZENworks Explorer General Settings," on page 54.

5 Click *OK* to apply the changes.

5.2.2 Configuring ZENworks Explorer Settings on the Device Folder Level

1 In ZENworks Control Center, click the *Devices* tab.
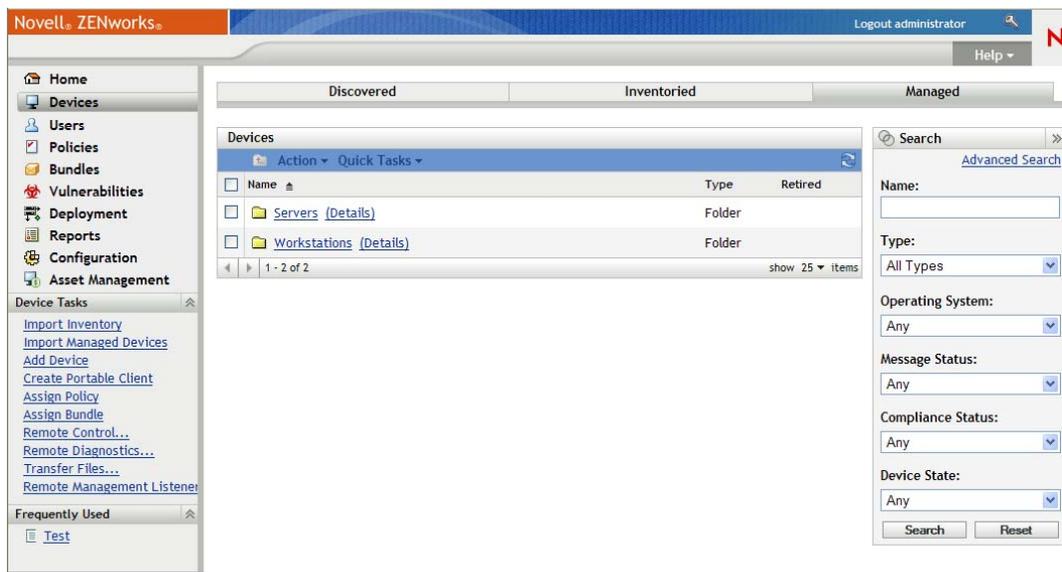
2 Click the *Servers* or *Workstations* folder.

3 Click *Details* next the folder for which you want to configure settings.

4 Click the *Settings* tab, click *Content*, then click *ZENworks Explorer Configuration*.
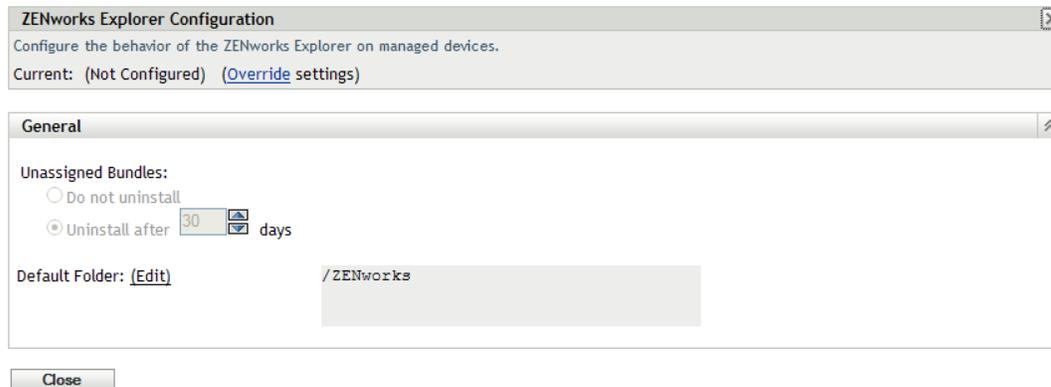
5 Click *Override Settings*.

If you are configuring the settings on a device folder or a device, you need to click *Override Settings* before you can select any of the settings.

6 Fill in the fields. For more information, see Section 5.2.4, "ZENworks Explorer General Settings," on page 54.

7 Click *OK* to apply the changes.

5.2.3 Configuring ZENworks Explorer Settings on the Device Level

1 In ZENworks Control Center, click the *Devices* tab.
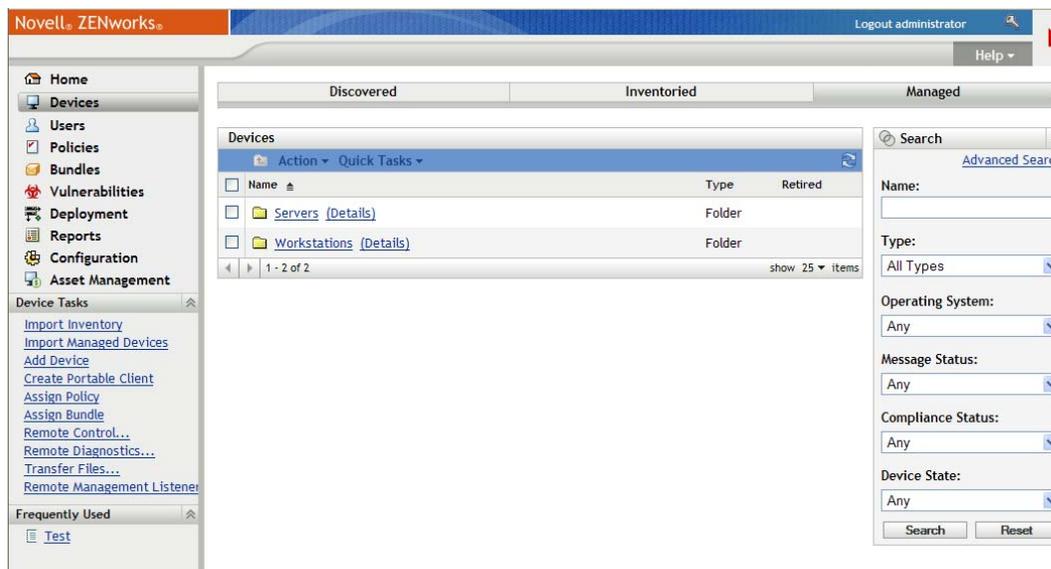
2 Click the *Servers* or *Workstations* folder.

3 Click the device for which you want to configure settings.

4 Click the *Settings* tab, click the *Content* tab, then click *ZENworks Explorer Configuration*.
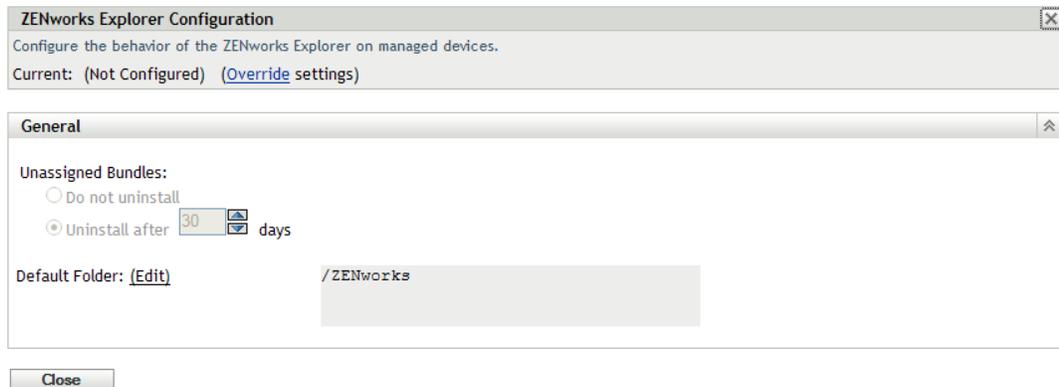
5 Click *Override Settings*.

If you are configuring the settings on a device folder or a device, you need to click *Override Settings* before you can select any of the settings.

6 Fill in the fields. For more information, see Section 5.2.4, "ZENworks Explorer General Settings," on page 54.

7 Click *OK* to apply the changes.

5.2.4 ZENworks Explorer General Settings

You can configure ZENworks Explorer to uninstall a bundle that is no longer assigned to the device, specify the number of days to wait before uninstalling the bundle, and specify the default folder that ZENworks Explorer uses.

You can configure the following settings on the ZENworks Explorer General panel:

Unassigned Bundles: Select whether or not you want a bundle to be uninstalled after it is no longer assigned to a device or the device's user.

If you choose to uninstall the bundle, select the number of days to wait before uninstalling the application. Specify 0 if you want the application to be uninstalled as soon as it is no longer assigned to the device or user.

Default Folder: ZENworks Explorer displays a default folder (ZENworks) in Windows Explorer, on the Windows Start menu and in the ZENworks Window. Bundles are placed in the default folder unless you override the default folder by specifying a folder on a bundle's Summary page.

The default folder can be renamed to meet the needs of your organization. Click *Edit* to change the folder name.

Content Repository

<div align="right">6</div>

Each ZENworks® Server contains a content repository. The content repository stores all bundle and policy content that has been replicated to the server and any images that have been captured and stored to the server.

The content repository is self-maintaining. Whenever you add a bundle or policy, the bundle or policy content is added to the appropriate content repositories based upon the replication settings. Whenever you remove a bundle or policy or change which servers host its content, the bundle or policy content is also removed from the appropriate servers.

If necessary, you can move the content repository to a different location. The following sections provide instructions:

6.1 Changing the Location of the Content Repository on a Windows Server

The content repository is found in the following location on a Windows server:

installation_path\zenworks\work\content-repo

You can specify a different disk drive to be your content repository. This is done by "mounting" the drive, rather than simply providing a mapped drive letter, which does not work to create a new location. Mounting is simply pointing an existing path to a hard drive partition without the use of mapped drive letters.

In the following steps, you will perform a Windows mounting of the default content repository location to a disk drive partition, which becomes the new content repository. These steps include the necessary preparations in order to make this work.

To change the default content repository location to a different disk drive partition:

1 Make sure that the disk drive you want to use is attached to the server and is properly formatted (NTFS).

Specifying a drive letter is unnecessary. However, the hardware must be recognized by the server. In Step 4, you will select the disk drive partition.

2 Because an empty content-repo directory must exist in the default location (*installation_path*\zenworks\work\content-repo) to be the pointer to the new content repository location, to make sure that there is no content in the default location, do one of the following:

- If you need to save the content that is now in this directory, rename the existing directory and create a new directory named content-repo.

  You can later copy the content from this renamed directory to the new content repository location (see Step 9).

- If you do not need any of the content in the existing `content-repo` directory, delete the directory and re-create it.
- If the `content-repo` directory is not present in the path given above, create the path and directory.

3 Click *Start*, right-click the *My Computer* icon, then select *Manage*.

You can also click *Start*, then enter `compmgmt.msc` at the *Run* command line.

4 Select *Disk Management* under the *Storage* section in the left pane.

The disk drive you selected in Step 1 should be displayed in the right pane.

5 Right-click the partition of the disk drive that you want to use as your content repository, then select *Change Driver Letter and Paths*.

This is the disk drive that in Step 7 you will mount to the `content-repo` directory.

6 Click *Add*.

This displays the Add Drive Letter or Path dialog box.

7 Select *Mount in the Following Empty NTFS Folder*, then browse for and select the default `content-repo` directory:

installation_path`\zenworks\work\content-repo`

This mounts the default path to the hard drive partition that you selected in Step 5.

8 Click *OK* as necessary to exit and save the configuration change.

9 If necessary (see Step 2), copy the files from the old renamed `content-repo` directory to the new `content-repo` directory.

This copies the files to the hard drive that you selected for your new content repository.

From this point on, all ZENworks 10 Configuration Management data is written directly to the new content repository location on the selected hard drive partition.

6.2 Changing the Location of the Content Repository on a Linux Server

You can store your data on a network share such as NFS, SMB, or CIFS and mount the share in your `content-repo` directory to access your data.

6.2.1 Mounting a Share

After configuring a share on a remote machine, you can mount it from `/var/opt/novell/zenworks/content-repo` using the following command:

```
mount -t cifs -o username=username //example.machine.com/share_name
/var/opt/novell/zenworks/content-repo
```

In the command, *//example.machine.com/share-name* is the share to mount and `/var/opt/novell/zenworks/content-repo` is the mount point.

If you only need to store the data from part of your content repository on another share, you can also do that. For example, if you to store your ZENworks image files on another share, you could use the following command:

```
mount -t cifs -o username=username //example.machine.com/share_name
/var/opt/novell/zenworks/content-repo/images
```

Or, to store bundle and policy content on another share, you could use the following command:

```
mount -t cifs -o username=username //example.machine.com/share_name
/var/opt/novell/zenworks/content-repo/content
```

6.2.2 Unmounting a Share

This mount is temporary; the share is unmounted when the operating system is shut down or rebooted. You can also use the following command to manually unmount the share:

```
umount /var/opt/novell/zenworks/content-repo
```

6.2.3 Creating a Permanent Mount

To ensure that the mount occurs each time the Linux server starts, you must add an entry to your `/etc/fstab` configuration file using the following command:

```
//example.machine.com/share_name /var/opt/novell/zenworks/content-
repo cifs credentials=path_to_credentials_file 0 0
```

The credentials file contains a username and password. For more information, see the `mount.cifs(8)` man page. The format of the file is:

```
username=value
```

```
password=value
```

A symbolic link can also be created on your local hard drive if you want to store your data elsewhere on your local device. See the `ln(1)` man page for more information about how to symbolically link directories.

6.2.4 Moving Existing Content to the New Repository

After you change the location of a content repository by mounting a new share, any content in the old location is no longer available. To make it available, you must move it to the new repository.

Content Replication

7

When you add a bundle or policy that contains files, the files are uploaded to the content repository on the ZENworks® Server. In addition, the ZENworks database is updated to reflect the addition of the bundle or policy and its content.

ZENworks Servers and Distribution Points, collectively referred to as content servers, periodically read the ZENworks database to discover new bundles and policies. Each content server that does not have the bundle or policy content retrieves it from the content server where it resides.

There are a variety of settings you can use to control how content is replicated among content servers in your zone. You can:

- Specify whether content is replicated to new content servers by default.
- Manually include content on or exclude content from content servers.
- Schedule how often replication occurs.
- Set a limit, or throttle, on the maximum amount of content that is replicated per second from one content server to another.

For information about performing these tasks, see the following sections:

7.1 Replicating Content to New Content Servers

By default, when a new content server (ZENworks Server or Distribution Point) is added to the zone, all bundle and policy content is replicated to that content server. You can, however, choose not to replicate a specific bundle or content policy.

For example, assume that you have a bundle for Microsoft* Office. You've included it on specific content servers and don't want it replicated to additional servers. To keep this from happening, you would modify the Microsoft Office bundle's replication settings to exclude replication to new content servers.

1 In ZENworks Control Center, go to the details page for the bundle or policy whose replication setting you want to modify.

2 Click the *Content Servers* tab.

The Replication Settings panel displays whether new content servers are included (receive the content) or excluded (don't receive the content).

3 In the Replication Settings panel, click *Edit* to display the Include/Exclude New Servers dialog box.

4 Select *Included* to include new servers in replication of the content.

or

Select *Excluded* to exclude new servers.

5 Click *OK* to save the changes.

7.2 Including or Excluding Content

The default replication setting determines whether content is automatically replicated to new content servers (see Section 7.1, "Replicating Content to New Content Servers," on page 59). You configure the setting for each bundle or policy. If you choose to include a bundle's or policy's content on new content servers, it is replicated to all new servers; likewise, if you choose to exclude the content, it is not replicated to any new servers.

In some cases, the default replication settings might not give you the desired replication scope for your content, or the scope might change. If this occurs, you can manually include content on or exclude it from specific content servers. There are three ways to do this:

- Section 7.2.1, "Managing a Single Piece of Content on Multiple Content Servers," on page 60
- Section 7.2.2, "Managing Multiple Pieces of Content on a Single Content Server," on page 61
- Section 7.2.3, "Managing Multiple Pieces of Content on Multiple Content Servers," on page 61

7.2.1 Managing a Single Piece of Content on Multiple Content Servers

This section provides instructions for managing the replication of a single bundle's or policy's content to multiple content servers. If you want to manage the replication of the content for multiple bundles or policies to a single content server, see Section 7.2.2, "Managing Multiple Pieces of Content on a Single Content Server," on page 61.

1 In ZENworks Control Center, go to the details page for the bundle or policy whose content replication you want to manage.

2 Click the *Content Servers* tab.

The Replication Status panel displays all content servers in the zone. If the bundle or policy content is included on a content server, the *Included* column displays a ✔ icon.

3 To change the replication status for a content server, select the check box in front of the server, then click *Include* to include the content on the server or click *Exclude* to exclude the content from the server.

As you include or exclude content servers, you should be aware of the following replication rules:

- If a ZENworks Server is the parent server for one or more Distribution Points, you can't exclude the content from the ZENworks Server without first excluding it from the Distribution Points.
- If you only have one ZENworks Server in your Management Zone, you can't exclude the content from it.
- You can't include a Distribution Point without first including the Distribution Point's parent ZENworks Server.

7.2.2 Managing Multiple Pieces of Content on a Single Content Server

This section provides instructions for managing the replication of the content for multiple bundles or policies to a single content servers If you want to manage the replication of a single bundle's or policy's content to multiple content servers, see Section 7.2.1, "Managing a Single Piece of Content on Multiple Content Servers," on page 60.

1 In ZENworks Control Center, go to the details page for the content server whose content replication you want to manage.

2 Click the *Content* tab.

The Replication Settings panel displays all bundles and policies in the zone. If the bundle or policy content is included on the content server, the Included column displays a ✔ icon.

3 To change the replication status for a bundle or policy, select the check box in front of the bundle or policy, then click *Include* to include its content on the server or click *Exclude* to exclude its content from the server.

As you include or exclude content from the server, you should be aware of the following replication rules:

- If a ZENworks Server is the parent server for one or more Distribution Points, you can't exclude the content from the ZENworks Server without first excluding it from the Distribution Points.

- If you only have one ZENworks Server in your Management Zone, you can't exclude the content from it.

- You can't include a Distribution Point without first including the Distribution Point's parent ZENworks Server.

7.2.3 Managing Multiple Pieces of Content on Multiple Content Servers

You can use the Specify Content Wizard to include or exclude multiple pieces of content on multiple content servers. For example, you might have four bundles that you want included on only two of your four content servers. Rather than managing the replication for the individual bundles (see Section 7.2.1, "Managing a Single Piece of Content on Multiple Content Servers," on page 60) or the individual content servers (see Section 7.2.2, "Managing Multiple Pieces of Content on a Single Content Server," on page 61), you can use the wizard to manage the replication for all four bundles and content servers at one time.

1 In ZENworks Control Center, click the *Devices* tab, then click the *Servers* folder to open it.

2 In the *Server Tasks* list in the left navigation pane, click *Specify Content* to launch the wizard.

3 Follow the prompts to complete the wizard.

If you need more information about a wizard page, click the *Help* button or refer to the following table.

Wizard Page	Details
Include or Exclude Content Servers/Distribution Points	Move the content servers on which you want to include the content to the *Included* list. Move the content servers on which you want to exclude the content to the *Excluded* list.
	As you include or exclude content servers you should be aware of the following replication rules:
	◆ If a ZENworks Server is the parent server for one or more Distribution Points, you can't exclude content from the ZENworks Server without also excluding it from the Distribution Points.
	◆ If you only have one ZENworks Server in your Management Zone, you can't exclude the content from it.
	◆ You can't include a Distribution Point without also including the Distribution Point's parent ZENworks Server.
New Servers Added to the System page	Select whether the content is included on or excluded from content servers added in the future.
Select Content to Update page	Identify the content you want affected by moving it from the *Available Content* list to the *Selected Content* list.

You can also launch the Specify Content Wizard from the following locations:

- ◆ Bundles page
- ◆ Policies page
- ◆ Configuration page > Server Hierarchy panel

7.3 Modifying the Replication Schedule

By default, a ZENworks Server checks for new or removed content every 5 minutes. If you do not add or remove bundles and policies very often, you might want to decrease the frequency of the schedule.

A ZENworks Server uses up to five threads to update the content in its repository during a replication cycle. If the current replication cycle does not complete before the next scheduled cycle, the schedule is ignored and replication automatically continues into the next cycle.

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

2 In the Management Zone Settings panel, click *Content > Content Replication*.

3 For the *Primary Server Recurring Content Replication Schedule*, use the *Days*, *Hours*, and *Minutes* fields to set the schedule.

You can use any combination of the fields. For example, to specify every 30 hours, you can enter 30 hours or 1 day, 6 hours.

4 Click *Apply* or *OK* to save the schedule.

7.4 Throttling the Content Replication Rate

The content replication throttling rate determines the maximum amount of content (in kilobytes per second) that a ZENworks Server transfers when replicating content to other content servers or when distributing content to managed devices.

By default, no throttling rate is imposed, which means that a ZENworks Server uses all available bandwidth. To set a throttling rate:

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

2 In the Management Zone Settings panel, click *Content > Content Replication*.

3 In the *Primary Server Output Throttling in KB/Sec* list, select the throttling rate you want.

   This rate applies to all ZENworks Servers in your zone. You cannot set individual throttling rates.

4 Click *Apply* or *OK* to save the changes.

Content Delivery

<div style="text-align: right; font-size: large;">8</div>

Content delivery, or distribution, refers to the process of transferring bundle and policy content from a content server (ZENworks® Primary Server or Content Distribution Point) to a managed device.

There are a variety of settings you can use to determine how content is delivered to managed devices, such as setting up Closest Server rules, setting delivery blackout dates for when content can't be downloaded, and setting how often you want managed devices to look for new content to download.

For information about performing these tasks, see the following sections:

8.1 Setting Up Closest Server Rules

When you have multiple content servers, you can use the Closest Server rules to determine which content server a managed device uses to download content. The Closest Server rules let you map devices to content servers based on network addresses (DNS names and IP addresses).

For example, you can create a rule that maps all devices to ContentServer1 that fall within the IP address range of 123.45.678.1 to 123.45.678.100.

The following sections provide information and instructions for setting up Closest Server rules:

8.1.1 Understanding Closest Server Rules

When your ZENworks Management Zone includes more than one server (Primary Servers, Collection Roll-Up Points, and Content Distribution Points), devices need to know which server to contact. The Closest Server Rules panel lets you create rules that are used to determine which servers a device contacts for the collection, content, and configuration functions.

The following sections provide information you should understand before you start creating Closest Server rules:

Collection, Content, and Configuration Servers

There are three basic functions for which devices contact a server:

- **Collection:** Inventory and message log information is collected from each device to be viewed in ZENworks Control Center and output to reports. Each ZENworks Primary Server and Collection Roll-Up Point can act as a collection server.

- **Content:** Provides content to the managed devices. Each ZENworks Primary Server and Collection Roll-Up Point can act as a content server.

- **Configuration:** Configuration settings and registration information must be applied to devices. Only ZENworks Primary Servers can act as a configuration server.

A device can contact the same server for all three functions, or it can contact different servers for each function.

Mapping Devices to Collection, Content, and Configuration Servers

A Closest Server rule maps devices with specific network addresses to three lists: a *Collection Server* list, a *Content Server* list, and a *Configuration Server* list.

For example, assume that you want to create a rule for devices that fall within the IP address range of 123.45.678.1 to 123.45.678.100. You specify the IP address range and then create the following three lists:

Collection Server List	Content Server List	Configuration Server List
Server 1	Server 3	Server 1
Server 2	Server 1	Server 3
Server 3		Server 2

Based on the three lists, any device whose IP address falls within the range will contact Server 1 for collection, Server 3 for content, and Server 1 for configuration. If any of these servers are unavailable, the device contacts the next server in the list.

Effective Rules

You can configure Closest Server rules at three levels:

- **Management Zone:** The rules are inherited by all device folders and devices.
- **Device Folder:** The rules are inherited by all devices contained within the folder or its subfolders. Overrides the Management Zone settings.
- **Device:** The rules apply only to the device for which they are configured. Overrides the settings set at the Management Zone and folder levels.

Each device can have only one Closest Server rule applied to it. A device's effective rule is determined as follows:

1. **Device Settings:** Evaluate all rules that are set on the device. If the device meets a rule's criteria, that rule becomes the device's effective rule.

2. **Folder settings:** If no device rule applies, evaluate all rules that are set on the device's parent folder. If the device meets a rule's criteria, that rule becomes the device's effective rule. If not, evaluate the rules on the next folder up in the hierarchy.

3. **Management Zone:** If no folder rule applies, evaluate all rules that are set in the Management Zone. If the device meets a rule's criteria, that rule becomes the device's effective rule. If not, apply the default rule to the device.

4. **Default Rule:** If no device, folder, or Management Zone rule applies, apply the default rule to the device. The default rule is simply a listing of all content servers in the order you want devices to contact them.

8.1.2 Configuring the Closest Server Default Rule

The Closest Server Default rule lets you define the rule that is used by a device to determine the closest collection, content, and configuration servers when no Closest Server rules have been defined or when none apply. This rule is simply a listing of the servers in the order you want devices to contact them. You cannot add or remove servers from the lists.

By default, all ZENworks Servers function as collection, content, and configuration servers and are therefore displayed in the Collection Servers, Content Servers, and Configuration Servers lists. In addition, any devices that are defined as Content Distribution Points are also displayed in the Content Servers list, and any devices that are defined as Collection Roll-Up Points are also displayed in the Collection Servers list.

To configure a Closest Server Default rule:

1 In ZENworks Control Center, click the *Configuration* tab, then click *Infrastructure Management* (in the Management Zone Settings panel) > *Closest Server Default Rule*.

The Content Servers section includes all ZENworks Primary Servers and Content Distribution Points in your zone. You cannot add or remove servers from the list. However, you can reorder the list to reflect the order in which you want the servers contacted by devices.

2 Use the *Move Up* and *Move Down* buttons to determine the order devices should use to contact the servers for their content.

3 When you are finished reordering the servers, click *OK* or *Apply* to save the changes.

8.1.3 Creating Closest Server Rules

1 Launch ZENworks Control Center.

2 Do one of the following:

 - To create a Closest Server rule for your Management Zone, click the *Configuration* tab, then click *Infrastructure Management* (in the Management Zone Settings panel) > *Closest Server Rules*.

 - To create a Closest Server rule for a device folder, open the folder's details page, then click *Settings* > *Infrastructure Management* (in the Settings panel) > *Closest Server Rules*.

 - To create a Closest Server rule for a device, open the device's details page, then click *Settings* > *Infrastructure Management* (in the Settings panel) > *Closest Server Rules*.
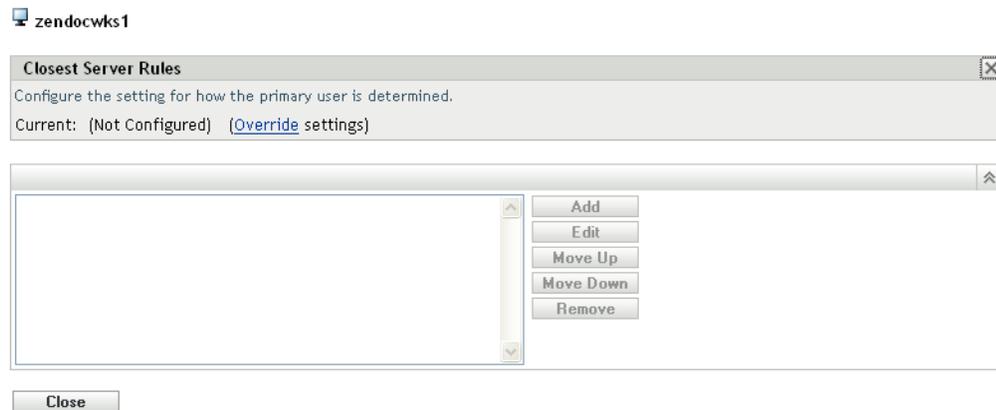
3 If you are creating Closest Server rules on a device or device folder, click *Override settings* to activate the Closest Server Rules panel.

The *Override* option (not depicted) displays only at the device and device folder levels.

4 Click *Add* to display the Rule Construction dialog box:

5 In the *Rule Name* field, specify a name for the rule.

The name displays in the Closest Server Rules listing in ZENworks Control Center. To access this listing, click *Configuration* in the left pane, click the *Configuration* tab, click the *Management Zone Settings* panel to open it, click *Infrastructure Management* section to open it, then click *Closest Server Rules*. All defined rules for the current level are displayed there.

6 Using the *Rule Logic* fields, create the rule expression.

An expression consists of a criteria option, operator, and value. For example:

```
DNS Name Filter equal to *.novell.com
```

`DNS Name Filter` is the criteria option, `equal to` is the operator, and `*.novell.com` is the value. In the above example, the Closest Server rule is applied only to devices whose DNS name ends with `.novell.com`.

If necessary, you can use NOT to perform a logical negation of the expression. For example:

```
NOT DNS Name Filter equal to *.novell.com
```

In the above example, the Closest Server rule is applied only to devices whose DNS name does not end with `.novell.com`.

You can use more than one expression for the rule. For example:

```
DNS Name Filter equal to provo.novell.com or
IP Address equal to 123.45.678.12/24
```

The criteria options you can use are listed below:

Option	Explanation
DNS Name Filter	Matches DNS names that meet the filter criteria. You can specify an exact filter or use a question mark (?) or an asterisk (*) as a wildcard to match one or more characters in the DNS name. A ? matches one character and an * matches one or more characters. Examples:
	provo.novell.com: Matches all devices in the provo subdomain of the novell.com top-level domain.
	*.novell.com: Matches all devices in the novell.com top-level domain, including any devices in subdomains.
	provo?.novell.com: Matches all devices in the provo1 and provo 2 subdomains of the novell.com top-level domain; does not match devices in the provo12 subdomain.
IP Address /n	Matches IP addresses that fall within the specified CIDR (Classless Inter-Domain Routing) block. With CIDR, the dotted decimal portion of the IP address is interpreted as a 32-bit binary number that has been broken into four 8-bit bytes. The number following the slash (/n) is the prefix length, which is the number of shared initial bits, counting from the left side of the address. The /n number can range from 0 to 32, with 8, 16, 24, and 32 being commonly used numbers. Examples:
	123.45.678.12/16: Matches all IP addresses that start with 123.45.
	123.45.678.12/24: Matches all IP addresses that start with 123.45.678.

7 In the *Content Servers* box, click *Add* to add ZENworks Servers and Distribution Points to the list.

To remove a server, select it and then click *Remove*.

8 Use the *Move Up* and *Move Down* buttons to determine the order devices should use to contact the servers for their content.

The order in which the ZENworks Servers are listed is the order in which a device contacts them. If the first ZENworks Server is not available, the second server is contacted, and so on.

9 When you are finished, click *OK* to add the rule to the *Closest Server Rules* list.

10 Repeat Step 2 through Step 9 to create additional rules.

11 If necessary, when you are finished creating rules, use the *Move Up* and *Move Down* buttons to reorder the rules in the *Closest Server Rules* list.

The rules are evaluated in the order they are listed. You should place the rules in the order you want them evaluated.

8.2 Scheduling Delivery Blackout Dates

If there are times when you don't want managed devices to download content, you can create a content blackout schedule. Schedules can be defined at the following levels:

- **Management Zone:** The schedule is inherited by all devices.
- **Device Folder:** The schedule is inherited by all devices within the folder and its subfolders. Overrides the Management Zone blackout schedule.
- **Device:** The schedule applies only to the device for which it is defined. Overrides any schedules set at the Management Zone and folder levels.

A blackout schedule can include one or more time periods. For example, you could create a schedule that prevents content from being delivered on Sundays from 7:00 p.m. to 9:00 p.m or on Fridays from 6:00 p.m. to 9:00 p.m.

To create a content blackout schedule:

1 Launch ZENworks Control Center.

2 Do one of the following:

  ◆ To create a content blackout schedule for your Management Zone, click the *Configuration* tab, then click *Content* (in the Management Zone Settings panel) > *Content Blackout Schedule*.

  ◆ To create a content blackout schedule for a device folder, open the folder's details page, click *Settings* > *Content* (in the Settings panel) > *Content Blackout Schedule*.

  ◆ To create a content blackout schedule for a device, open the device's details page, click *Settings* > *Content* (in the Settings panel) > *Content Blackout Schedule*.

Devices > Workstations > zendocwks1 > **Content Blackout Schedule**

🖥 **zendocwks1**

Content Blackout Schedule	☒
Configuration of the blackout schedule for preventing content delivery to managed devices.	
Current: /Devices/Workstations/zendocwks1	
Revert the settings to: (Not Configured)	

Content Blackout Schedule			⌃
Add Remove			
☐ **Start Date**	**Start Time**	**End Date**	**End Time**
No items available.			

[OK] [Apply] [Reset] [Cancel]
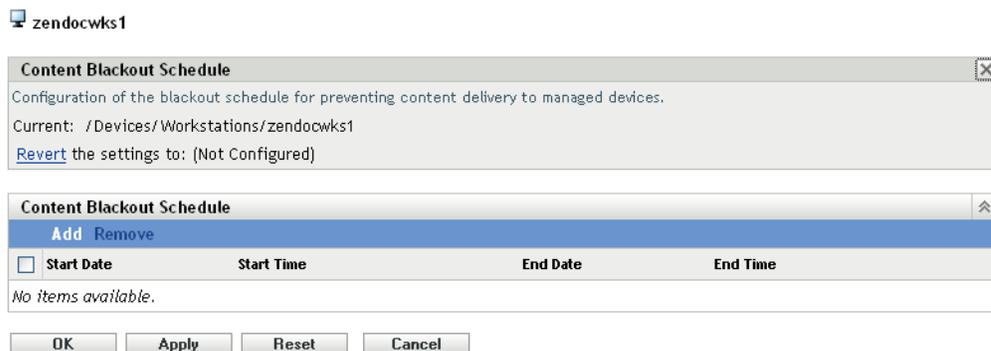
3 If you are creating content blackout schedules for a device or device folder, click *Override settings* to activate the Content Blackout Schedule panel.

4 Click *Add* to display the Specify Blackout Time Period dialog box, then fill in the following fields:

Start Date: Select the first date you want to include in the schedule.

End Date: Select the last date you want to include in the schedule. The blackout time period (specified by the start and end times) occurs on each day from the start date to the end date.

Start Time: Select the hour you want the blackout time period to start each day.

End Time: Select the hour you want the blackout time period to end each day. If you want the blackout time period to extend for 24 hours, select the same time as the start time.

5 Click *OK* to save the blackout period.

6 Repeat Step 4 to create additional blackout periods.

7 When you are finished, click *OK* or *Apply* to save the schedule.

8.3 Setting the Device Refresh Schedule

At device startup, the ZENworks Adaptive Agent on a device contacts a ZENworks Server to refresh its information. If information changes after startup, the Adaptive Agent must refresh its information again before the changes can show up on the device.

If the refreshed information indicates that there is new content to be downloaded, the Adaptive Agent contacts its content server and begins the download process.

You can use the device refresh schedule to determine how often a device contacts a ZENworks Server to update bundle, policy, configuration, and registration information. Schedules can be defined at the following levels:

* **Management Zone:** The schedule is inherited by all devices.
* **Device Folder:** The schedule is inherited by all devices within the folder and its subfolders. Overrides the Management Zone schedule.
* **Device:** The schedule applies only to the device for which it is defined. Overrides any schedules set at the Management Zone and folder levels.

To create a device refresh schedule:

1 Launch ZENworks Control Center.

2 Do one of the following:

* To create a device refresh schedule for your Management Zone, click the *Configuration* tab, then click *Device Management* (in the Management Zone Settings panel) > *Device Refresh Schedule*.
* To create a device refresh schedule for a device folder, open the folder's details page, then click *Settings* > *Device Management* (in the Settings panel) > *Device Refresh Schedule*.
* To create a device refresh schedule for a device, open the device's details page, then click *Settings* > *Content* (in the Settings panel) > *Device Refresh Schedule*.

Devices > Workstations > zendocwks1 > Device Refresh Schedule

zendocwks1

Device Refresh Schedule
Configure the refresh interval for this device.
Current: /Devices/Workstations/zendocwks1
Revert the settings to: (System)

Device Refresh Schedule
○ Manual Refresh
 Device won't get refreshed until the user manually does so
◉ Timed Refresh
 Full Refresh Schedule
 Refresh everything: Policies, Bundles, Settings, Registration, etc.

 [0] Days [12] Hours [0] Minutes

 ☑ Random Time to Wait

 Minimum: [300] Seconds Maximum: [360] Seconds
 Partial Refresh Schedule
 Only perform Policies, Settings, and Registration refresh

 [0] Days [2] Hours [0] Minutes

[OK] [Apply] [Reset] [Cancel]

3 If you are creating a device refresh schedule for a device or device folder, click *Override settings* to activate the Device Refresh Schedule panel, the choose from the following schedules:

Manual Refresh: If you want a device refreshed only when its user manually initiates the refresh, select *Manual Refresh,* then click *Apply*. Users can initiate a refresh by clicking the ZENworks icon located in the desktop's notification area (system tray).

Timed Refresh: Select *Timed Refresh* if you want to establish a refresh schedule. There are two schedules you can use: the Full Refresh Schedule and the Partial Refresh Schedule.

- **Full Refresh Schedule:** The full refresh schedule defines how often you want a device to update all of its information from the ZENworks Server, including bundle, policy, setting, and registration information. Use the following fields to create the full refresh schedule:

    - **Days, Hours, Minutes:** Specifies the amount of time between refreshes. For example, to set a refresh interval of 8.5 hours, you would specify 0 Days, 8 Hours, 30 Minutes. The default is 12 hours.

    - **Random Time to Wait:** Select this option to ensure that multiple devices that have the same refresh schedule do not all initiate their refresh at the same time. For example, if you have 1000 devices with the same refresh schedule, you might overburden your ZENworks Server. By selecting this option, the device waits a randomly generated amount of time before initiating its refresh. Use the *Minimum* and *Maximum* fields to specify the range (in seconds) for the randomly generated time.

- **Partial Refresh Schedule:** The partial refresh schedule defines how often you want a device to update its policy, configuration setting, and registration information from the ZENworks Server. Bundle information is not updated.

    In the *Days*, *Hours*, and *Minutes* fields, specify the amount of time between refreshes. For example, to set a refresh interval of 3 hours, you would specify 0 Days, 3 Hours, 0 Minutes. The default is 2 hours.

The refresh interval is not reset until the device refresh is complete. For example, assume you set a refresh interval of 8 hours. The device's first refresh occurs at 6:00 p.m. and takes 13 seconds to complete. The second refresh occurs at 2:00:13 a.m. (8 hours after the refresh was completed at 6:00:13). If the second refresh takes 15 seconds to complete, the third refresh occurs at 10:00:28 a.m.

4 When you are finished, click *OK* or *Apply* to save the schedule.

Content Distribution Point

<div align="right" style="font-size:3em">9</div>

If you want to improve content access for a group of devices without creating another ZENworks® Server, you can create a Distribution Point. For example, if you have devices that are accessing a ZENworks Server outside of their network segment, you can create a Distribution Point within the network segment to service those devices.

You can add any managed device as a Distribution Point. A Distribution Point provides the same content delivery service as a ZENworks Server but requires only the Distribution Point module that is installed with the ZENworks Adaptive Agent. The module is inactive until you promote the managed device to be a Distribution Point.

When you create a Distribution Point, you assign a ZENworks Server as its parent content server. The Distribution Point downloads content from its parent ZENworks Server only. Therefore, any content you want hosted on a Distribution Point must also be hosted on its parent ZENworks Server.

9.1 Adding a New Distribution Point

This can be done either from the Configuration or the Devices tab:

9.1.1 Using the Configuration Tab

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

2 In the Server Hierarchy panel, select the ZENworks Server that you want to serve as the new Distribution Point's parent content server.

3 Click *Action > New Content Distribution Point* to display the New Content Distribution Point dialog box.

4 If desired, change the default port number (80) to the port number you want the device to use for content replication HTTP requests.

5 In the *Device* field, click 🔍 to browse for and select the desired device.

6 Click *OK* to add the device as a Distribution Point.

In the Server Hierarchy panel, the new Distribution Point is added as a child of the ZENworks Server.

For information about controlling the content that is replicated to the Distribution Point, see Chapter 7, "Content Replication," on page 59.

9.1.2 Using the Devices Tab

1 In ZENworks Control Center, click the *Devices* tab, then on the *Managed* tab, click *Workstations*.

2 In the Workstations panel, select the check box of the desired managed device, then click *Action > New Content Distribution Point* to display the New Content Distribution Point dialog box.

3 In the Parent Primary Server field, click 🔍 to browse for and select the ZENworks Server that you want to serve as the new Distribution Point's parent server.

If server roles are in effect for this workstation, the Parent Primary Server field already displays the assigned parent server.

4 If desired, change the default port number (80) to the port number you want the device to use for content replication HTTP requests.

If roles are in effect for this workstation, the Port field already displays the assigned port.

5 Click *OK* to add the device as a Distribution Point.

In the Server Hierarchy panel, the new Distribution Point is added as a child of the ZENworks Server.

For information about controlling the content that is replicated to the Distribution Point, see Chapter 7, "Content Replication," on page 59.

9.2 Deleting a Distribution Point

Deleting a Distribution Point does not remove the device as a managed device. It only disables the device as a Distribution Point and removes the content from the device.

IMPORTANT: If you established any Closest Server rules to direct managed devices to the Distribution Point, you should rework your rules. For more information, see Section 8.1, "Setting Up Closest Server Rules," on page 65.

This can be done either from the Configuration or the Devices tab:

- Section 9.2.1, "Using the Configuration Tab," on page 76
- Section 9.2.2, "Using the Devices Tab," on page 76

9.2.1 Using the Configuration Tab

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

2 In the Server Hierarchy panel, select the Distribution Point that you want to delete.

3 Click *Action > Delete Content Distribution Point*.

4 Click *OK* to confirm the deletion.

The Distribution Point is removed from the Server Hierarchy panel.

9.2.2 Using the Devices Tab

1 In ZENworks Control Center, click the *Devices* tab, then on the *Managed* tab, click *Workstations*.

2 In the Workstations panel, select the check box for Distribution Point that you want to delete.

3 Click *Action > Delete Content Distribution Point*.

4 Click *OK* to confirm the deletion.

The Distribution Point is removed from the Server Hierarchy panel.

9.3 Modifying the Content Replication Schedule

By default, a Distribution Point checks for new or removed content every 5 minutes. You can change the replication schedule. For example, you might want to increase the time between replication cycles if you are not adding content very often to your system or if the connection between the Distribution Point and its parent ZENworks Server is slow.

A Distribution Point uses up to five threads to update the content in its repository during a replication cycle. If the current replication cycle does not complete before the next scheduled cycle, the schedule is ignored and replication automatically continues into the next cycle.

To modify the schedule:

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

2 In the Server Hierarchy panel, select the Distribution Point whose schedule you want to modify.

3 Click *Action > Edit Content Replication Schedule*.

4 Use the *Days*, *Hours*, and *Minutes* fields to set the schedule.

You can use any combination of the fields. For example, to specify every 30 hours, you can enter 30 hours or 1 day, 6 hours.

5 Click *OK* to save the new schedule.

9.4 Specifying the Content to Host

By default, a Distribution Point includes the same content as its parent ZENworks Server. If you want to limit the content that it hosts, you can exclude content from being replicated to it.

If you want to include content that its parent ZENworks Server does not have, you must first add the content to the parent ZENworks Server.

For additional information and instructions about how to specify the content to be hosted on a Distribution Point, see Section 7.2, "Including or Excluding Content," on page 60.

User Sources

10

Novell® ZENworks® 10 Configuration Management enables you to assign content to users as well as devices. Device-assigned content is available whenever the device is running and connected to the network; user-assigned content is available only when the user is logged in to the Management Zone. For example, if you assign a bundle to a user, the bundle is available only after the user logs in.

Unlike devices, users are not defined in your Management Zone. Instead, you connect to the LDAP directory that you want to use as your authoritative user source. If necessary, you can connect to multiple directories.

The following sections provide instructions to define user sources:

- Section 10.1, "Prerequisites," on page 79
- Section 10.2, "Adding a User Source," on page 79
- Section 10.3, "Deleting a User Source," on page 83
- Section 10.4, "Adding a Container from a User Source," on page 83

10.1 Prerequisites

- ❑ **Minimum directory version:** Novell eDirectory™ 8.7.3 or Microsoft Active Directory* on Windows 2000 SP4.
- ❑ **Minimum LDAP version:** LDAPv3
- ❑ **Minimum user account rights:** Read rights.

  For Active Directory, you can use a basic user account. This provides sufficient read access to the directory.

  For eDirectory, you need inheritable read rights to the following attributes: CN, O, OU, C, DC, GUID, WM:NAME DNS, and Object Class. You can assign the rights at the directory's root context or at another context you designate as the ZENworks root context.
- ❑ **DNS name resolution:** With Active Directory, your ZENworks Servers (in particular, the DNS clients on the ZENworks Server) must be able to resolve the DNS name of each Active Directory domain defined as a user source. Otherwise, users from the Active Directory domain cannot log in to the ZENworks Management Zone.

10.2 Adding a User Source

1 In ZENworks Control Center, click the *Configuration* tab.
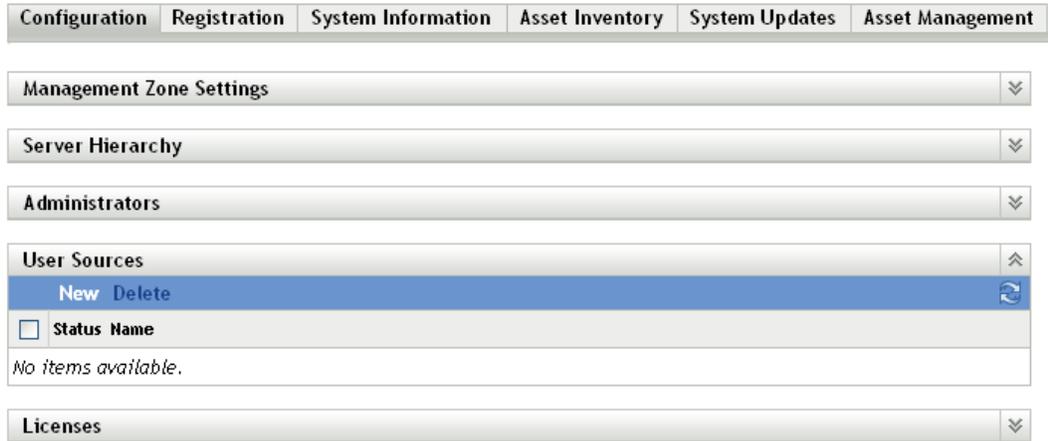
2 In the User Sources panel, click *New* to launch the Create New User Source Wizard.

3 Follow the prompts to create the connection to the user source.

For information about each of the wizard pages, click the *Help* button or refer to the following table.

Wizard Page	Details
Connection Information page	Specify the information required to create a connection to the LDAP directory: • **Address:** Specify the IP address or DNS hostname of the server where the LDAP directory resides. • **Use SSL:** By default, this option is enabled. Disable the option if the LDAP server is not using the SSL (Secure Socket Layer) protocol. • **Port:** This field defaults to the standard SSL port (636) or non-SSL port (389) depending on whether the *Use SSL* option is enabled or disabled. If your LDAP server is listening on a different port, select that port number. • **Root Context:** The root context establishes the point in the directory where you can begin to browse for user containers. Specifying a root context can enable you to browse less of the directory, but it is optional. If you don't specify a root context, the directory's root container becomes the entry point.

Credentials page	Specify a username and password for accessing the directory:
	
	• **Username:** Specify the username for a user that has read-only access to the directory. The user can have more than read-only access, but read-only access is all that is required and recommended.
	
	For Novell eDirectory access, use standard LDAP notation. For example:
	
	`cn=admin_read_only,ou=users,o=mycompany`
	
	For Microsoft Active Directory, use standard domain notation. For example:
	
	`AdminReadOnly@mycompany.com`
	
	• **Password:** Specify the password for the user you specified in the Username field.

Wizard Page	Details
User Containers page	After you connect to an LDAP directory as a user source, you can define the containers within the directory that you want exposed. The number of user containers you define is determined by how much of the directory you want to expose. Consider the following example:

MyCompany

```
— EMEA
      — Accounting
            — Users
            — Groups
      — Sales
            — Users
            — Groups
      — Servers
      — Services
      — Groups
— ASIAPAC
— AMERICAS
```
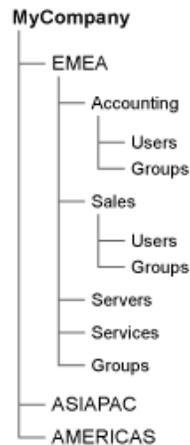
Assume you want to enable all users in the Accounting and Sales containers to receive ZENworks content. In addition, you want to be able to access the user groups located in the Accounting, Sales, and Groups containers in order to distribute content based on those groups. To gain access to the users and groups, you have two options:

◆ You can add MyCompany/EMEA as a user container, in which case all containers located below EMEA would be visible in ZENworks Control Center, including the Servers and Services containers. Only users and user groups located in the EMEA containers would be visible (servers and services would not), but the structure would still be exposed.

◆ You can add MyCompany/EMEA/Accounting as one user container, MyCompany/EMEA/Sales as a second container, and MyCompany/EMEA/Groups as a third container. Only these containers would become visible as folders beneath the MyCompany directory reference in ZENworks Control Center.

To add the containers where users reside:

1. Click *Add* to display the Add User Container dialog box.

2. In the *Context* field, click to browse for and select the desired container.

3. In the *Display Name* field, specify the name you want used for the user container when it is displayed in ZENworks Control Center.

4. Click *OK* to add the container to the list.

10.3 Deleting a User Source

When you delete a source, all assignments and messages for the source's users are removed. You cannot undo a source deletion.

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

2 In the User Sources panel, select the check box in front of the user source, then click *Delete*.

3 Click *OK* to confirm the deletion.

10.4 Adding a Container from a User Source

After you've defined a user source in your Management Zone, you can add containers from that source at any time.

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

2 In the User Sources panel, click the user source.

3 In the User Containers panel, click *Add* to display the Add User Container dialog box, then fill in the following fields:

Context: Click 🔍 to browse for and select the container you want to add.

Display Name: Specify the name you want used for the user container when it is displayed in ZENworks Control Center. The name cannot be the same as the name of any other user containers.

4 Click *OK* to add the user container.

The container, and its users and user groups, is now available on the *Users* page.

User Authentication 11

The following sections provide information about authentication of users to a ZENworks®
Management Zone.

11.1 User Source Authentication

By default, a user is automatically authenticated to the Management Zone when he or she logs in to
an LDAP directory (Novell® eDirectory™ or Microsoft* Active Directory) that has been defined as
a user source in the Management Zone. User authentication to ZENworks can occur only if the
user's LDAP directory (or the user's LDAP directory context) is defined as a user source in
ZENworks.

The ZENworks Adaptive Agent integrates with the Windows Login or Novell Login client to
provide a single login experience for users. When users enter their eDirectory or Active Directory
credentials in the Windows or Novell client, they are logged in to the Management Zone if the
credentials match the ones in a ZENworks user source. Otherwise, a separate ZENworks login
screen prompts the user for the correct credentials.

For example, assume that a user has accounts in two eDirectory trees: Tree1 and Tree2. Tree1 is
defined as a user source in the Management Zone, but Tree2 is not. If the user logs in to Tree1, he or
she is automatically logged in to the Management Zone. However, if the user logs in to Tree2, the
Adaptive Agent login screen appears and prompts the user for the Tree1 credentials.

11.2 Credential Storage

ZENworks uses Novell CASA (Common Authentication Services Adapter) to enable single sign-on.
When the ZENworks Adaptive Agent authenticates a user to the Management Zone via the
credentials entered in the Microsoft client, Novell client, or ZENworks login screen, the username
and password is stored in the secure CASA vault on the user's device.

CASA is installed with the ZENworks Adaptive Agent. It includes the CASA Manager, an interface
used to manage the credentials in the storage vault. The CASA Manager is available from the Start >
Program Files > Novell CASA menu. Generally, you or the device's user should not need to use the
CASA Manager. When a user's credentials change in their LDAP directory, they are updated in the
CASA storage vault the next time the user logs in. If you do run the CASA Manager, you are
prompted to install the GTK# Library. If you choose to install the library (which is necessary to run
the CASA Manager), you are directed to a Novell Website from which you can install it.

Do not remove CASA from the managed device. If you do not want the CASA Manager displayed
to users, you can remove the Novell CASA folder from the Start > Program Files menu.

11.3 Disabling ZENworks User Authentication

By default, if a user source is defined in the ZENworks Management Zone, the ZENworks Adaptive Agent attempts to authenticate a user to the zone whenever he or she logs in through the Microsoft or Novell client.

If necessary, you can disable user authentication to the zone. For example, you might have some users that only receive device-assigned content so you don't want the overhead of having them logged in to the zone.

To disable user authentication to the zone:

1 Locate the following key in the registry on the user's device:

   HKEY_LOCAL_MACHINE\SOFTWARE\Novell\ZENworks\ZenLgn

2 (Conditional) If you want to disable login, add the following DWORD value:

   Value name: DisablePassiveModeLogin

   Value data: Any non-zero value (for example, 1, 2, 3, 100)

   With login disabled, no attempt is made to authenticate to the Management Zone when the user logs in through the Microsoft or Novell client.

3 (Conditional) If you want to disable the ZENworks login prompt that appears if login through the Microsoft client or Novell client fails, add the following DWORD value:

   Value name: DisablePassiveModeLoginPrompt

   Value data: Any non-zero value (for example, 1, 2, 3, 100)

   Normally, the Adaptive Agent attempts to authenticate the user to the zone by using the credentials entered in the Microsoft or Novell client. If login fails, the ZENworks login prompt is displayed in order to give the user an opportunity to authenticate with different credentials. This value setting disables the ZENworks login prompt.

ZENworks System Updates

The System Updates feature allows you to obtain updates to the Novell® ZENworks® 10 Configuration Management software on a timely basis, and also allows you to schedule automatic downloads of the updates.

Software updates are provided periodically and you can choose whether to deploy each update after viewing its content.

ZENworks 10 Configuration Management Update 2 (v10.0.3) is cumulative. For example, if Update 2 is your first update, it includes all updates contained in Update 1 (v10.0.2).

In the future, updates are additive, meaning they contain files relevant to only the changes made since the previous update. For example, you need to apply Update 2 before you can apply Update 3.

You can also download the latest Product Recognition Update (PRU) to update your knowledgebase so that Inventory can recognize newer software.

When you select to update your ZENworks software, you can update globally in one step or in stages. You can also select to update specific devices, groups of devices, or all devices in the Management Zone that have the ZENworks software installed. You can use ZENworks Control Center to track the successes and failures per device for each software update.

The following figure illustrates the System Updates page:

Figure 12-1 *System Updates Panels (Available System Updates, Deploying System Updates, and Deployment Stages)*
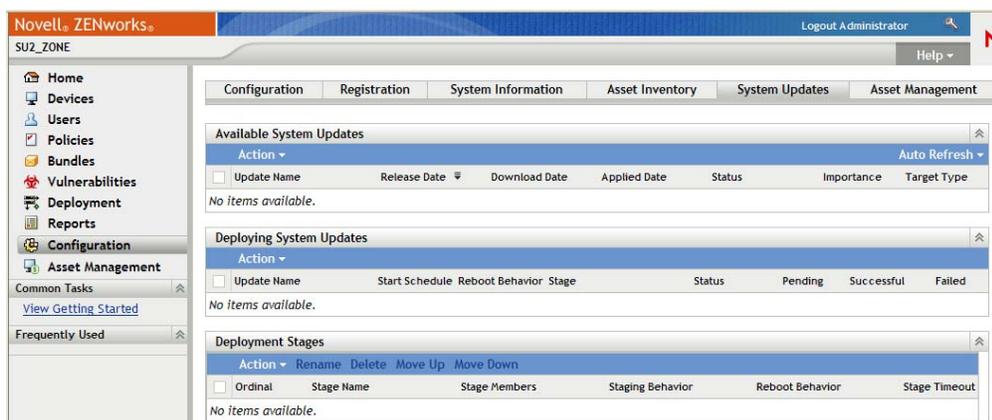
Review the following sections to set up and manage updates for your ZENworks software:

- Section 12.1, "Configuring Updates," on page 88
- Section 12.2, "Managing Update Downloads," on page 105
- Section 12.3, "Deploying Updates," on page 109
- Section 12.4, "Deleting Updates," on page 123
- Section 12.5, "Reviewing the Content of an Update," on page 123
- Section 12.6, "Update Statuses," on page 126

12.1 Configuring Updates

You should perform the following tasks to configure your update process:

12.1.1 Configuring System Update Settings

You should configure System Update before attempting to use it. Configure as many of the following settings as necessary for your system:

Check for Updates Schedule

The default is to not schedule update checking (*No Schedule* is displayed in the *Schedule Type* field). With this scheduling option selected, the only way you can check for software updates is to do so manually in the Available System Updates panel on the *System Updates* tab.

You can specify how often you want to check for updates. When you do this, information on available updates is automatically downloaded from Novell to the Available System Updates panel on the *System Updates* tab when the schedule fires. This does not download the update content itself. Downloading can be scheduled in the Download Schedule panel (see "Download Schedule" on page 90).

To schedule checking for the ZENworks software updates:

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 *System Update Settings*.

In the Check for Updates panel, there are two scheduling options for updates:

- **No Schedule:** The default is to not schedule update checking. With this scheduling option selected, the only way you can check for software updates is to do so manually in the Available System Updates panel on the *System Updates* tab. To specify the *No Schedule* option, continue with Step 3.

- **Recurring:** Lets you specify how often you want to check for updates. When you set this option, information on available updates is automatically downloaded from Novell to the Available System Updates panel on the *System Updates* tab when the schedule fires. This does not download the update content itself. To set a recurring schedule, skip to Step 4.

3 (Conditional) To exclude scheduled checking for software updates (the default), 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 check for updates manually. For more information, see "Manually Downloading Updates" on page 107.

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

Configuration > System Update Settings

System Update Settings ✕
Configure the server for downloading System Updates, proxy server settings, and scheduling updates

Check For Updates Schedule ⌃
This setting allows the administrator to configure a schedule to check for available updates from Novell.

Schedule Type:
Recurring ▾

⦿ Days of the week

   Sun Mon Tue Wed Thu Fri Sat
   ☐   ☐   ☐   ☐   ☐   ☐   ☐

Start Time: 1 ▾ : 00 ▾ am ▾

Hide Options
   ☐ Process immediately if device unable to execute on schedule
   ☐ Use Coordinated Universal Time (Current UTC 7:50 PM)
   ☐ Start at a random time between Start and End Times
       End Time: 1 ▾ : 00 ▾ am ▾
   ☐ Restrict schedule execution to the following date range:
       Start Date: 2/5/08 🗓
       End Date: 2/5/08 🗓

5 Fill in the fields:

5a Select one or more check boxes for the days of the week.

5b To set the time of day for checking to occur, use the *Start Time* box to specify the time.

5c (Optional) For additional scheduling options, click *More Options*, then select the following options as necessary:

- **Process Immediately if Device Unable to Execute on Schedule:** Causes the checking for 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, after the server comes back online, checking for updates immediately occurs.

- **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 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 for when the checking can occur.

5d 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 some of your changes effective, clicking *OK* does so. Clicking *Cancel* also closes the page, but loses your unapplied changes.

Download Schedule

The default is to not schedule downloading of updates (*No Schedule* is displayed in the *Schedule Type* field). With this scheduling option selected, the only way you can download updates is to do so manually in the Available System Updates panel on the *System Updates* tab.

If you do specify how often you want to download updates, you should set this schedule in conjunction with the schedule to check for updates (see "Check for Updates Schedule" on page 88).

After an update has been checked for and its information displayed in the Available System Updates panel on the *System Updates* tab, you can schedule the download from Novell to automatically occur when the schedule fires.

To schedule ZENworks software updates:

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 *System Update Settings*.

In the Download Schedule panel, there are two scheduling options for downloading updates:

 ◆ **No Schedule:** The default is to not schedule downloading of updates (*No Schedule* is displayed in the *Schedule Type* field). With this scheduling option selected, the only way you can download updates is to do so manually in the Available System Updates panel on the *System Updates* tab. To specify the *No Schedule* option, continue with Step 3.

 ◆ **Recurring:** You can specify how often you want to download updates. After an update has been checked for and its information displayed in the Available System Updates panel on the *System Updates* tab, you can schedule the download from Novell to automatically occur when the schedule fires. To set a recurring schedule, skip to Step 4.

3 (Conditional) To exclude scheduled downloading of software updates (the default), 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 updates manually. For more information, see Section 12.2.2, "Downloading Updates," on page 106.

4 (Conditional) To set a recurring schedule for downloading updates to your ZENworks software, click the down-arrow in the *Schedule Type* field, then select *Recurring*.

System Update Settings   ☒

Configure the server for downloading System Updates, proxy server settings, and scheduling updates

Check For Updates Schedule   ⌄

Download Schedule   ⌃

This setting allows the administrator to configure a download schedule for updates.

Schedule Type:

| Recurring | ▼ |

⦿ **Days of the week**

Sun	Mon	Tue	Wed	Thu	Fri	Sat
☐	☐	☐	☐	☐	☐	☐

Start Time: [1 ▼] : [00 ▼] [am ▼]

Hide Options

☐ Process immediately if device unable to execute on schedule
☐ Use Coordinated Universal Time (Current UTC 7:52 PM)
☐ Start at a random time between Start and End Times

End Time: [1 ▼] : [00 ▼] [am ▼]

☐ Restrict schedule execution to the following date range:

Start Date: [2/5/08] 🗓
End Date: [2/5/08] 🗓

5 Fill in the fields:

5a Select one or more check boxes for the days of the week.

5b To set the time of day for downloading to occur, use the *Start Time* field to specify the time.

5c (Optional) For additional scheduling options, click *More Options*, then select the following options as necessary:

- ◆ **Process Immediately if Device Unable to Execute on Schedule:** Causes the checking for 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, after the server comes back online, checking for updates immediately occurs.

- ◆ **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 downloading of 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 the days when the downloading can occur.

5d 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 some of your changes effective, clicking *OK* does so. Clicking *Cancel* also closes the page, but loses your unapplied changes.

EMail Notification

In conjunction with using stages, you can set up email notifications to indicate when each stage has completed. When you deploy an update, you can specify to use the e-mail notifications.

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 *Events and Messaging*, then select *SMTP Settings* to display the E-mail Notification panel:

Configuration > SMTP Settings

SMTP Settings

Configuration of settings related to SMTP Server

E-mail Notification

SMTP Server Address

SMTP Port

☐ SMTP Server requires authentication

User

Password

OK   Apply   Reset   Cancel

Staging must be used to receive notifications, and the stage behavior must be set to one of the following:

- *Advance Through Stage Automatically With Notification*
- *Advance To Next Stage and Notify When Complete*

SMTP must be configured in order for the staging email configuration to work.

3 (Conditional) If you do not have SMTP configured:

3a To access the SMTP Settings page, click *Configuration* in the left pane, click the arrows in the *Management Zone Settings* heading to expand its options, click *Event and Messaging*, then select *SMTP Settings*.

3b In the Email Notification section, fill in the fields:

SMTP Server Address: Specify the DNS name or IP address of the SMTP server.

SMTP Port: Specify the SMTP server's communication port.

SMTP Server Requires Authentication: If authentication is required, select this check box, then specify the *User* and *Password* information.

3c Click *OK* to save the changes.

3d Click *Management Zone Settings* to expand its options, click *Infrastructure Management*, then select *System Update Settings* to display the Email Notification panel:

4 Fill in the fields:

From: Either specify your administrator e-mail address, or type something descriptive, such as: `System Update Stage Notice.`

To: Specify your administrator's email address.

This is the person you want to be notified when the stage ends.

5 Click *Apply* to make the changes effective.

6 Either click *OK* to close the page, or continue with another configuration task.

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

Proxy Server Settings

This option is useful for restrictive environments where you do not want all of your production servers to have Internet access. This is used in conjunction with the Dedicated Server Settings panel.

To specify a proxy 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 *System Update Settings* to display the Proxy Server Settings panel.

3 In the Proxy Server Settings section, fill in the fields:

Proxy Server Address: Specify the DNS name or IP address of the proxy server.

Proxy Server Port: Specify the proxy server's communication port.

Proxy Server Requires Authentication: When you select this check box, the *User* and *Password* fields become editable. If authentication is required, select this check box and specify the username and password for access to the proxy server.

4 Click *Apply* to make the changes effective.

5 Either click *OK* to close the page, or continue with another configuration task.

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

Dedicated Server Settings

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

The following sections contain more information:

Specifying a Dedicated Update 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 *System Update Settings* to display the *Dedicated Server Settings* panel:
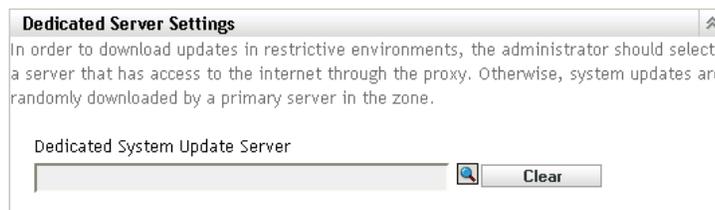
3 Browse for and select a ZENworks Primary Server.

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

This ZENworks Server must be a member of the Management Zone.

4 Click *Apply* to make the changes effective.

5 Either click *OK* to close the page, or continue with another configuration task.

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

Clearing a Dedicated Update Server

Clearing a dedicated update server causes your updates to be retrieved randomly from any Primary 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 *System Update Settings* to display the *Dedicated Server Settings* panel:

3 Click *Clear* to remove the dedicated server from the *Dedicated System Update 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.

IMPORTANT: Previous settings cannot be restored after you click *Apply*.

Stage Timeout Settings

Deployment stages are optional; however, stages allow you to deploy an update in stages, such as to a test group first, then to your managed devices. If a failure occurs during the update process, the process is halted. E-mail notifications can let you know when each stage has completed.

The global default timeout setting is 3 days. This provides the same timeout length for each stage. For information about setting the timeout for individual stages, see "Modifying Stage Timeout" on page 101.

Set this value to be long enough to accommodate updating all of the devices you plan to update. If you set it too short, some devices might not be updated.

If the timeout value is reached before a stage completes, the deployment process is paused and an error message is sent to the administrator. The deployment process is paused until the errors are resolved and the administrator restarts the process by clicking *Clear Error and Retry*.

You can use E-mail notification to know when a stage has completed.

To configure global stage timeout settings:

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

2 On the *Configuration* tab, expand the *Management Zone Settings* panel (if necessary), click *Infrastructure Management*, then click *System Update Settings* to display the *Stage Timeout Settings* panel:
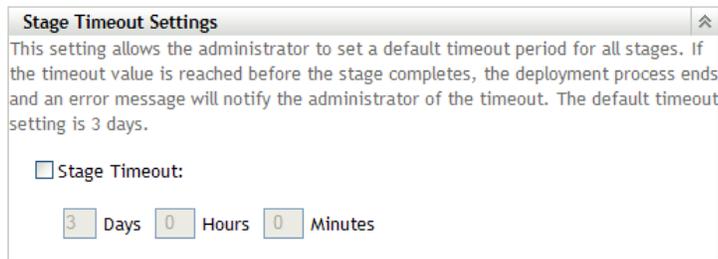
3 Select the Stage Timeout check box, then specify the days, hours, and minutes desired.

4 Click *Apply* to make the changes effective.

5 Either click *OK* to close the page, or continue with another configuration task.

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

Reboot Behavior

Some updates do not require a device to be rebooted after they have been deployed to a device. However, if a reboot is required to complete the update process, the deployment is not completed until the device is rebooted.

To configure the reboot behavior:

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

2 On the *Configuration* tab, expand the *Management Zone Settings* panel (if necessary), click *Infrastructure Management*, then click *System Update Settings* to display the *Reboot Behavior* panel:

3 Select one of the following options:

- ◆ **Prompt User to Reboot When Update Finishes Applying (Default):** After the update has been applied, a request to reboot is immediately displayed. If the user initially rejects rebooting, the user is periodically requested to reboot the device, which continues until the device is rebooted.

- ◆ **Do Not Reboot Device:** The device does not reboot; however, the user is periodically requested to reboot the device, until the device is rebooted.

- ◆ **Force Device to Reboot:** After the update has been applied, the device is automatically rebooted without user intervention if a reboot is required by the update.

4 Click *Apply* to make the changes effective.

5 Either click *OK* to close the page, or continue with another configuration task.

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

System Update Configuration Pages Setting

If you updated from a previous version of ZENworks 10 Configuration Management to version 10.0.3, you must use the previous version's ZEnworks Control Center (ZCC) Configuration page to complete the update.

If you have updated from a previous version, when you click the System Update tab (in ZCC, *Configuration > System Update*) the following dialog box displays:

Figure 12-2 *System Update Pop-up Message*
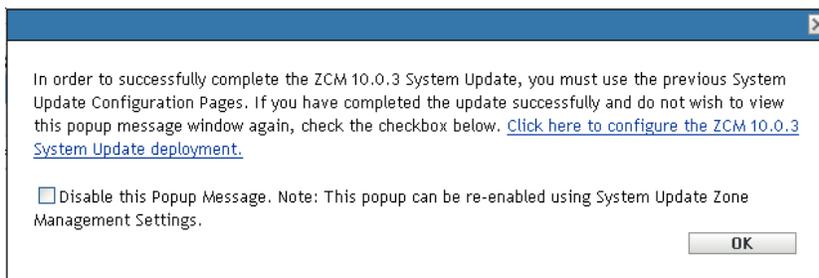
You can choose to disable the pop-up message that provides the link to the previous version's ZCC page if you successfully complete the update and do not want to view the pop-up message again. You can disable the pop-up by selecting the *Disable this Pop-up Message* check box in the pop-up message. You can also disable or enable the message in the System Update Configuration Pages Setting section (In ZCC, *Configuration > Configuration > Infrastructure Management > System Update Settings > System Update Configuration Pages Setting*).

To enable or disable the pop-up dialog box from ZENworks Control Center:

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

2 On the *Configuration* tab, expand the *Management Zone Settings* panel (if necessary), click *Infrastructure Management*, then click *System Update Settings* to display the *System Update Configuration Pages Setting*:

3 Select or deselect the *Disable the ability to use the configuration pages for ZCM 10.0.3 System Update* option to enable or disable the pop-up message.

4 Click *Apply* to make the changes effective.

5 Either click *OK* to close the page, or continue with another configuration task.

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

12.1.2 Creating Deployment Stages

Deployment stages are optional; however, stages allow you to deploy an update in stages, such as to a test group first, then to your managed devices. If a failure occurs during the update process, the process is halted. E-mail notifications can let you know when each stage has completed.

The following sections contain more information:

Understanding Stages

You can do the following with stages:

- Set them up for different devices or groups, such as for a test group, specific devices or device groups, or all managed devices in the zone.
- Modify an existing stage's membership.
- Change the order in which the stages run.
- Rename and delete stages.
- Specify the default timeout for a stage. If that time is reached, the update process is paused until the errors are resolved and the administrator restarts the process.
- Specify the reboot behavior when devices complete the update: prompt a reboot, force a reboot, or suppress rebooting.
- Specify how the update process is to advance through the stages:
  - Automatically, with or without notification
  - One stage at a time with notification when each stage is completed
  - Bypass the configured stages and immediately apply the update to all devices

There are many reasons for creating deployment stages:

- Testing the update on certain devices before deploying it to your production environment
- You can include all Primary servers in one stage so they can be updated at the same time.

  or
- You can group your servers in several stages so that the update process isn't too intensive for the Primary Server being used to perform the updates.
- You can group the workstations in several stages so that the update process isn't too intensive for the Primary Server being used to perform the updates.

Any managed devices that are not part of a stage are automatically updated after the last deployment stage has been processed.

You cannot configure stages when an update is in progress.

The following graphic illustrates the Deployment Stages panel on the System Updates page:

Figure 12-3 *The Deployment Stages Panel*

Deployment Stages							⊗
Action ▾ Rename Delete Move Up Move Down							
☐	Ordinal	Stage Name	Stage Members	Staging Behavior		Reboot Behavior	Stage Timeout
☐	1	Deployment Stage: Test	View/Modify Members	Advance Through Stage Automatically		Prompt User	3 days 0 hours 0 minutes
☐	2	Deployment Stage: Production	View/Modify Members	Advance Through Stage Automatically		Prompt User	3 days 0 hours 0 minutes

The following table explains the column information. For some columns, you can sort the listed information by clicking a column heading. Click it again to reverse the sorting order.

Column Heading	Explanation
Ordinal	Displays the order in which the stages are run. You can rearrange the staging order by using the *Move Up* and *Move Down* options. For more information, see "Rearranging the Order in Which Stages Start" on page 104.

The first stage listed always displays ordinal 1, the second, ordinal 2, and so on. Therefore, you do not need to include a sequence number in your stage names. |
| *Stage Name* | Name of the stage, which you specify when creating the stage by using the *Action > Add Stage* option.

Make this name descriptive enough to indicate its purpose. |
| *Stage Members* | This column contains the *View/Modify Members* option, which opens the Modify Stage Members dialog box that lists all of the members of the stage. You can add or remove members from the stage.

Stage membership can include individual devices and groups that contain devices.

For more information, see "Modifying the Membership of a Deployment Stage" on page 103. |
| *Staging Behavior* | Displays the current behavior for each stage, which you can change by using the *Action > Modify Staging Behavior* option. For more information, see "Modifying Staging Behavior" on page 102. |
| *Reboot Behavior* | Displays the reboot behavior of devices after the update is deployed.

Some updates do not require a device to be rebooted after they have been deployed to a device. However, if a reboot is required to complete the update process, the deployment is not completed until the device is rebooted.

The following explains how each option works:

- **Prompt User to Reboot When Update Finishes Applying (Default):** After the update has been applied, a request to reboot is immediately displayed. If the user initially rejects rebooting, the user is periodically requested to reboot the device, until the device is rebooted.

- **Do Not Reboot Device:** The device does not reboot; however, the user is periodically requested to reboot the device, until the device is rebooted.

- **Force Device to Reboot:** After the update has been applied, the device is automatically rebooted without user intervention, if a reboot is required by the update,.

For more information, see "Modifying Reboot Behavior" on page 102. |

Column Heading	Explanation
Stage Timeout	Displays the stage timeout, listed in minutes, which you can change by using the *Action > Modify Stage Timeout* option. The default is 3 days, 0 hours, and 0 minutes, which is the global timeout value that can be changed in "Stage Timeout Settings" on page 95. Changing the value here only changes it for the selected deployment stage. When this time value is reached, the stage's deployment terminates and the next stage starts. If the time is not long enough, the deployment might not be completed to all of the devices that are members of the stage. For more information, see "Modifying Stage Timeout" on page 101.

Creating and Populating a Deployment Stage

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

2 In the Deployment Stages panel, click *Action*, then select *Add Stage*.

You cannot add a stage while a deployment is in process.

3 Specify a deployment stage name, then click *OK*.

Deployment stages appear as device folders on the *Devices* tab, so you should specify names that help you to know a folder's purpose.

You might want to include something like "Deployment Stage" at the beginning of the name to sort the groups in the devices listing in ZENworks Control Center.

For information about naming in ZENworks Control Center, see Appendix A, "Naming Conventions in ZENworks Control Center," on page 143.

A newly created stage does not have any members. You must modify the stage's membership to add them.

4 Add devices to a deployment stage:

  4a In the Stage Members column, click *View/Modify Members* for the stage for which you want to add members.
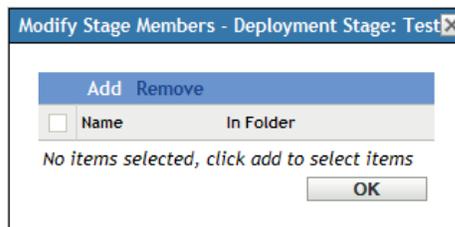
  4b Click *Add*, browse for and select the devices, then click *OK*.

    You can add individual devices or device groups, or any combination of them.

Keep in mind that you can have both servers and workstations in the same deployment stage, or in different stages, or that you can split your servers and workstations into multiple deployment stages for each type.

> **IMPORTANT:** You should update your Primary Servers before updating your managed workstations.

    4c Repeat Step 4b until you are finished adding members to the stage.

    4d To add members to another stage, repeat Step 4a through Step 4c.

5 Repeat Step 2 through Step 4 until you have created all of your deployment stages.

6 If you need to reorder the sequence of the deployment stages, select a stage, then click *Move Up* or *Move Down*.

If you are using one of the stages for test purposes, make sure that it is first in the listing.

Modifying Stage Timeout

A stage timeout sets the length of time before a stage terminates. The default timeout is 3 days. You set the value for individual stage timeouts here. The global stage timeout value can be established by following the steps in "Stage Timeout Settings" on page 95.

You cannot modify a stage if an update is in progress.

To set the timeout value for a selected stage:

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

2 In the Deployment Stages panel, select the check box for a stage, click *Action*, then select *Modify Stage Timeout* to display the following dialog box:
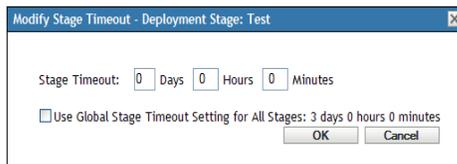
3 Specify the timeout value.

This change in timeout value only applies to the selected stage. If you specify a timeout value for this stage, set its value to be long enough to accommodate updating all of the devices in the stage. If you don't allow enough time, some devices might not be updated.

If the timeout value is reached before the stage completes, the deployment process is terminated and an error message is sent to the administrator.

4 (Optional) Select the *Use Global Stage Timeout Setting for All Stages* check box to specify using the global timeout value (default of 3 days, 0 hours, and 0 minutes).

For more information, see "Stage Timeout Settings" on page 95.

5 Click *OK*.

Modifying Staging Behavior

The default stage behavior is to automatically advance through the configured stages. You can change this default behavior for all stages.

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

2 In the Deployment Stages panel, select the check box for one or more stages, click *Action*, then select *Modify Stage Behavior* to display the following dialog box:
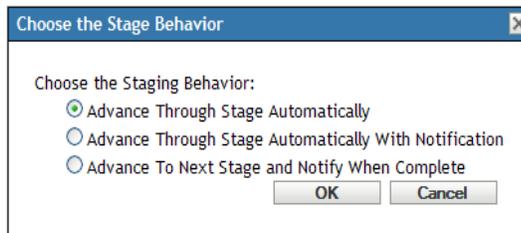
3 Select one of the following stage behaviors:

Advance Through Stages Automatically: As soon as one stage has completed its updates, the next stage begins. This is the default behavior (its check box is enabled).

After the last stage has completed, all applicable devices that are not members of a stage are then processed.

**Advance Through Stages Automatically with Notification:** Starts the first stage, sends an email notification when it has completed, then automatically starts the next stage, and so on.

To use this option, a notification method must be set up on the System Update Download Settings page in the *Email Notification* section.

Advance to Next Stage and Notify When Complete: Use this method for user action between the stages, such as to review the results of an update to a test group.

This option automatically starts the first stage. After any stage has completed, email notification is sent, then the system waits for you to manually start the next stage.

To use this option, a notification method must be set up on the System Update Download Settings page in the *Email Notification* section.

4 Click *OK*.

Modifying Reboot Behavior

Some updates do not require a device to be rebooted after they have been deployed to a device. However, if a reboot is required to complete the update process, the deployment is not completed until the device is rebooted.

To modify the reboot behavior:

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

2 In the Deployment Stages panel, select the check box for one or more the deployment stages, click *Action*, then click *Modify Reboot Behavior*.

3 Select one of the following options:

- **Prompt User to Reboot When Update Finishes Applying (Default):** After the update has been applied, a request to reboot is immediately displayed. If the user initially rejects rebooting, the user is periodically requested to reboot the device, until the device is rebooted.

- **Do Not Reboot Device:** The device does not reboot; however, the user is periodically requested to reboot the device, until the device is rebooted.

- **Force Device to Reboot:** After the update has been applied, the device is automatically rebooted without user intervention, if a reboot is required by the update,.

4 Click *OK*.

Modifying the Membership of a Deployment Stage

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

2 (Optional) Add devices to a deployment stage:

2a In the Stage Members column, click *View/Modify Members* for the stage for which you want to add members.
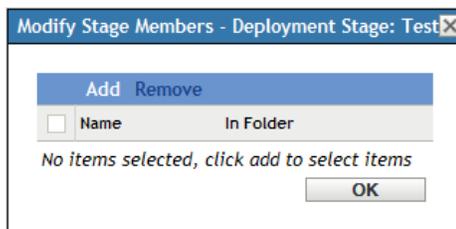
2b Click *Add*, browse for and select the devices, then click *OK*.

You can add individual devices or device groups, or any combination of them.

Keep in mind that you can have both servers and workstations in the same deployment stage, or in different stages, or that you can split your servers and workstations into multiple deployment stages for each type.

IMPORTANT: You should update your Primary Servers before updating your managed workstations.

2c Repeat Step 2b until you are finished adding members to the stage.

2d To add members to another stage, repeat Step 2a through Step 2c.

3 (Optional) Remove devices from a deployment stage:

   3a In the Stage Members column, click *View/Modify Members* for the stage for which you want to remove members.
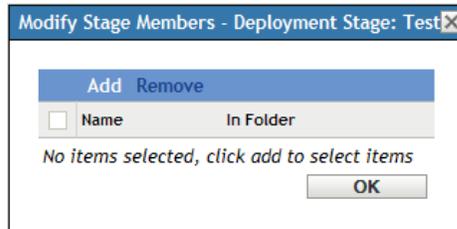
   3b Select the check box next one or more devices that you want to remove, click *Remove*.

4 Click *OK* when you have finished configuring the stage's membership.

Renaming a Deployment Stage

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

2 In the Deployment Stages panel, click the check box for the deployment stage to be renamed.

3 Click *Rename*.

4 In the Rename dialog box, specify the new name, then click *OK*.

For information about naming in ZENworks Control Center, see Appendix A, "Naming Conventions in ZENworks Control Center," on page 143.

Deleting a Deployment Stage

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

2 In the Deployment Stages panel, click the check box for one or more of the deployment stages to be deleted.

3 Click *Delete*.

Deleted stages cannot be recovered.

Rearranging the Order in Which Stages Start

All updates that use stages deploy to the devices that are members of the stages according to the currently listed staging order.

To rearrange the staging order:

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

2 In the Deployment Stages panel, click the check box for the deployment stage to be moved.

3 Click *Move Up* or *Move Down* as necessary to rearrange the staging order.

4 Repeat Step 2 and Step 3 as necessary for each stage.

12.2 Managing Update Downloads

The Available System Updates panel on the System Updates page displays the updates that are available after you have checked for them. This includes the Product Recognition Update (PRU), which Novell provides to update your knowledgebase so that ZENworks Inventory can recognize newer software. The display refreshed according to the schedule you set in "Check for Updates Schedule" on page 88.

Update 2 update is cumulative. For example, if Update 2 (v10.0.3) is your first update, it includes all updates contained in Update 1 (v10.0.2).

In the future, updates are additive, meaning they contain files relevant to only the changes made since the previous update. For example, you need to apply Update 2 before you can apply Update 3.

The following sections contain more information:

12.2.1 Understanding Available Updates

The following graphic illustrates the Available System Updates panel:

Figure 12-4   *Available System Updates Panel*

	Update Name ≡	Release Date	Download Date	Applied Date	Status	Importance	Target Type
☐	ZCM Update 10.0.5	Mar 7, 2008			Error	Optional	ZENworks Servers
☐	ZCM Update 10.0.4	Jan 1, 2008			Available	Optional	All Devices
☐	ZCM Update 10.0.3	Dec 25, 2007			Available	Optional	All Devices
☐	ZCM Update 10.0.2	Oct 31, 2007			Available	Optional	ZENworks Servers
☐	ZCM 10.0.2 (SU 1)	Oct 12, 2007			Baselined	Mandatory	ZENworks Servers

Available System Updates — Action ▾ — Auto Refresh ▾ — 1 - 5 of 10 — show 5 ▾ items

The following table explains the column information and the *Auto Refresh* drop-down list (on the right side of the panel, above *Target Type*). For some columns, you can sort the listed information by clicking a column heading. Click it again to reverse the sorting order.

Column Heading or List	Explanation
Update Name	Displays the name of the update, which is created by Novell. Click the name to access the Release Details page. For more information, see Section 12.5, "Reviewing the Content of an Update," on page 123.
Release Date	Displays the date that Novell created the update.
Download Date	Displays the date that you downloaded the update.
Applied Date	Displays the date that you applied the update.

Column Heading or List	Explanation
Status	Displays the current status of the update, which is automatically updated every 15 seconds. For more information on the individual statuses, see Section 12.6, "Update Statuses," on page 126.
Importance	Displays the relative importance of the update's content to your ZENworks installation. Some possible entries include: **OPTIONAL:** Not required for normal operation of ZENworks 10 Configuration Management. **MANDATORY:** A required update that must be applied.
Target Type	Displays the type of update, such as: **ZENworks Servers:** The update applies only to ZENworks Servers. **All Devices:** The update applies to all managed devices, including ZENworks Servers.
Auto Refresh	Click *Auto Refresh* (the menu item on the right side of the panel, above *Target Type*), then select one of the following: ◆ No Auto Refresh ◆ 15-second Refresh ◆ 30-second Refresh ◆ 60-second Refresh By default the panel view is not automatically refreshed. However, you can manually refresh the view by clicking the *System Updates* tab.

12.2.2 Downloading Updates

You can schedule the update downloads, or download them manually:

- "Scheduling Update Downloads" on page 106
- "Manually Checking for Updates" on page 107
- "Manually Downloading Updates" on page 107
- "Manually Importing Updates to Servers without Internet Connectivity" on page 108

Scheduling Update Downloads

You can schedule both checking for updates and downloading them. For instructions, see:

- "Check for Updates Schedule" on page 88
- "Download Schedule" on page 90

Manually Checking for Updates

If the most recent updates are not being displayed in the Available System Updates panel on the System Updates page, you can manually refresh the display.

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

2 On the Available System Updates panel, click *Action > Check for Updates*.

Any available updates are displayed with a status of *Available*.

3 To re-sort the listed updates, click the heading for any of the columns in the Available System Updates panel.

Click the heading a second time to reverse the sorting order.

Manually Downloading Updates

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

2 In the Available System Updates panel, select the check box next to one or more updates, click *Action*, then click *Download Update*.

The update is downloaded and its status is eventually set to Downloaded.

Depending on the size of the update, the downloading process can take awhile.

3 To refresh the view of the download progress (*Status* column), click the *System Updates* tab or use the Auto Refresh option.

4 If you want to use deployment stages to apply the selected updates, to configure the stages and deploy the updates, go to Section 12.3, "Deploying Updates," on page 109.

or

To immediately apply the downloaded updates to all applicable devices in the Management Zone, select the check box for the downloaded update that you want to deploy, then click *Action > Deploy Update to Devices*. The Create System Update Deployment Wizard steps you through the deployment process. For more information, see Section 12.3, "Deploying Updates," on page 109.

Manually Importing Updates to Servers without Internet Connectivity

If you have servers in your environment that do not have Internet access, you can obtain the update or Product Recognition Update (PRU) files from the Novell Downloads page (http://download.novell.com), copy the files onto a CD, for example, and then use the CD to import the files to a Primary ZENworks server using the zman system-update-import command. For more information, see "System Update/Product Recognition Update Commands" in the "ZENworks Command Line Utilities" guide.

After the files are on a ZENworks Primary Server, the update or PRU displays in the Available System Updates panel on the System Updates tab in ZCC (Configuration > System Updates). You can then follow the instructions in Section 12.3, "Deploying Updates," on page 109 to deploy the update to managed devices.

12.2.3 Downloading and Installing the PRU

Novell provides a Product Recognition Update (PRU) to update your knowledgebase so that ZENworks Inventory can recognize newer software.

This action deploys the PRU to your database and sets its deployment to your managed devices to be scheduled. Deployment is then done by the ZENworks Adaptive Agent on the devices.

If the PRU is not up-to-date, Inventory might return some software as unrecognized. However, you can use the Local Software Products utility to take a fingerprint of the unrecognized software to update your knowledgebase.

To download and install the PRU:

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab.
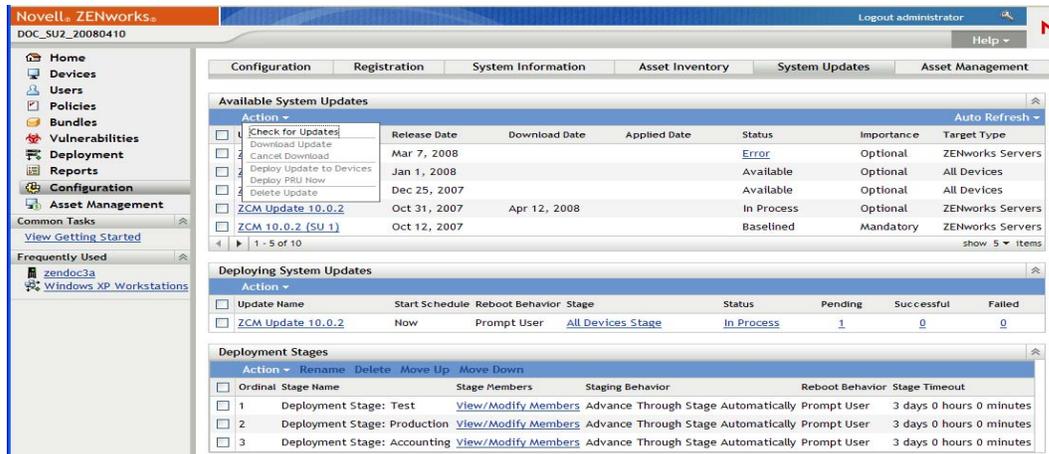
2 If a PRU is not displayed in the Available System Updates panel, click *Action > Check for Updates*.

Information for the latest PRU is displayed, if it is available.

3 To download a listed PRU, go to the Available System Updates panel, select the check box for a listed PRU, then click *Action > Download Update*.

4 To install a downloaded PRU, go to the Available System Updates panel, then click *Action > Deploy PRU Now*.

The PRU is now listed in the Deploying System Updates panel, where its progress is displayed.

12.3 Deploying Updates

The following sections contain more information:

- Section 12.3.1, "Understanding Deploying Updates," on page 109
- Section 12.3.2, "Deploying Updates," on page 112
- Section 12.3.3, "Starting the Pending Stage," on page 118
- Section 12.3.4, "Rescheduling a Deployment," on page 118
- Section 12.3.5, "Bypassing Staging," on page 118
- Section 12.3.6, "Canceling a Deployment," on page 119
- Section 12.3.7, "Clearing an Error to Retry a Deployment," on page 119
- Section 12.3.8, "Viewing Status by Device," on page 119

12.3.1 Understanding Deploying Updates

You have the following options for deploying an update:

- Deploy the update to all devices without using deployment stages. You can schedule the deployment.
- Deploy the update using deployment stages where one stage automatically starts after the previous one has completed, unless you have configured stages to pause the deployment and send email notifications to the administrator. You can schedule the deployment.

- ◆ Deploy the update using deployment stages with email notification to allow manual control over to start the next stage. You can use this option to test the update before deploying it to all devices in your production environment. You can schedule the deployment.
- ◆ Deploy the update to specific devices (selected individually and by device groups) without using deployment stages. You can use this option to test the update before deploying it to all devices in your production environment. You can schedule the deployment.

WARNING: After an update has been deployed, it cannot be removed by using ZENworks 10 Configuration Management. If you need to remove an update, contact Novell Support (http://www.novell.com/support) for assistance.

The Deploying System Updates panel displays the progress and results of deploying an update.

Updates are removed from this panel when the entire update process completes. You can view the Deployment History panel on the Release Details page for information on deployed updates.

The following figure illustrates the Deploying System Updates panel:

Figure 12-5 *Deploying System Updates Panel*

Deploying System Updates							
Action ▾							
Update Name	Start Schedule	Reboot Behavior	Stage	Status	Pending	Successful	Failed
☐ ZCM Update 10.0.2	Now	Prompt User	All Devices Stage	In Process	1	0	0

The following table explains the column information. For some columns, you can sort the listed information by clicking a column heading. Click it again to reverse the sorting order.

Column Heading	Explanation
Update Name	Displays the name of the update, which is created by Novell.
	Click the name to access the Status by Device page. You can also click the underlined number in the *Pending*, *Successful*, or *Failed* columns to view the appropriate Status by Device page, filtered to display devices with that status.
Start Schedule	Displays the current schedule, if any has been set. Use the Reschedule Deployment action to reschedule the update. For more information, see Section 12.3.4, "Rescheduling a Deployment," on page 118.
	Each device can have its own schedule.

Column Heading	Explanation
Reboot Behavior	Displays the reboot behavior of devices after the update is deployed.
	Some updates do not require a device to be rebooted after they have been deployed to a device. However, if a reboot is required to complete the update process, the deployment is not completed until the device is rebooted.
	The following explains how each option works:
	◆ **Prompt User to Reboot When Update Finishes Applying (Default):**
	After the update has been applied, a request to reboot is immediately displayed. If the user initially rejects rebooting, the user is periodically requested to reboot the device, until the device is rebooted.
	◆ **Do Not Reboot Device:** The device does not reboot; however, the user is periodically requested to reboot the device, until the device is rebooted.
	◆ **Force Device to Reboot:** After the update has been applied, the device is automatically rebooted without user intervention, if a reboot is required by the update.
Stage	Indicates the deployment state. The possible entries are:
	stage_name: The update is being deployed to the managed devices that are members of the current stage that is listed. *All Devices Stage* is displayed after the last stage has completed, which means any devices left in the Management Zone that were not part of a completed stage are then receiving the update. In other words, managed devices are not allowed to skip an update.
	Selected Devices Stage: The update is being deployed to selected managed devices without the use of stages.
	All Devices Stage: The update is being deployed to all managed devices in the Management Zone without the use of stages.
	If stages are being used, click a stage name to view the device status for each stage member. For more information, see Section 12.3.8, "Viewing Status by Device," on page 119.
Status	Indicates the status of the update being deployed (for the current stage, if stages are being used). For information on the possible statuses, see Section 12.6, "Update Statuses," on page 126.
	Click an item in the *Status* column to view a message explaining the current status.
	When the status for an update reaches either the APPLIED or BASELINE status, the update deployment item is no longer displayed in this panel, but is displayed in the Deployment History panel. For more information, see Section 12.3.8, "Viewing Status by Device," on page 119.
Pending	Displays the number of devices for which the update deployment process is pending. A device can be pending if it is a member of a stage when stages are not automatically started after another stage completes.
	Click the number to view the Status by Device page, which displays the devices that have a pending deployment of the update. For more information, see Section 12.3.8, "Viewing Status by Device," on page 119.

Column Heading	Explanation
Successful	Displays the number of devices for which the update deployment process is complete. Click the number to view the Status by Device page, which displays the devices that successfully received the update. For more information, see Section 12.3.8, "Viewing Status by Device," on page 119.
Failed	Number of devices for which the update deployment process has failed. Click the number to view the Status by Device page, which displays the devices that failed to receive the update. For more information, see Section 12.3.8, "Viewing Status by Device," on page 119. For failed deployments, you have the option of ignoring the error and continuing, or you can redeploy the update if the error has been resolved.

12.3.2 Deploying Updates

1 (Optional) If you want to use deployment stages, set them up if you have not previously done so.

For more information, see Section 12.1.2, "Creating Deployment Stages," on page 97.

2 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab to display the Available System Updates panel:

3 (Conditional) If new updates are not being displayed, click *Action > Check for Updates*.

The following illustrates available updates:

Available System Updates						
Action ▾						Auto Refresh ▾
☐ Update Name ⩯	Release Date	Download Date	Applied Date	Status	Importance	Target Type
☐ ZCM Update 10.0.5	Mar 7, 2008			Available	Optional	ZENworks Servers
☐ ZCM Update 10.0.4	Jan 1, 2008			Available	Optional	All Devices
☐ ZCM Update 10.0.3	Dec 25, 2007			Available	Optional	All Devices
☐ ZCM Update 10.0.2	Oct 31, 2007			Available	Optional	ZENworks Servers
☐ ZCM 10.0.2 (SU 1)	Oct 12, 2007			Baselined	Mandatory	ZENworks Servers
☐ ZCM 10.0.1 (PMR)	Jul 12, 2007			Baselined	Mandatory	ZENworks Servers
☐ Update for ZCM 10.0.8	Apr 8, 2008	Apr 11, 2008		Aborted	Optional	All Devices
☐ Update for ZCM 10.0.7	Apr 7, 2008			Available	Optional	All Devices
☐ Update for ZCM 10.0.6	Apr 7, 2008	Apr 10, 2008	Apr 10, 2008	Baselined	Optional	All Devices
☐ 20 content files	Aug 19, 2006	Apr 10, 2008		Downloaded	Optional	All Devices
◁ ▷ 1 - 10 of 10						show 10 ▾ items

4 (Optional) To view the content of an available update, click the name of the update (in the Update Name column) to display the Release Details page:

For more information, see .

5 To download an update, select the check box for it, click *Action* > then click *Download Updates*.

After an update has completed downloading, its status is automatically changed to downloaded. The length of time to download an update depends on its size and your hardware configuration.

You can download multiple updates at a time, but you can only deploy one at a time. Because these steps are repeated for each update, you only need to download the update you plan to deploy at this time.

The following illustrates downloaded updates:

Available System Updates						
Action ▾						Auto Refresh ▾
☐ Update Name ⩯	Release Date	Download Date	Applied Date	Status	Importance	Target Type
☐ ZCM Update 10.0.5	Mar 7, 2008			Error	Optional	ZENworks Servers
☐ ZCM Update 10.0.4	Jan 1, 2008			Available	Optional	All Devices
☐ ZCM Update 10.0.3	Dec 25, 2007			Available	Optional	All Devices
☐ ZCM Update 10.0.2	Oct 31, 2007	Apr 12, 2008		In Process	Optional	ZENworks Servers
☐ ZCM 10.0.2 (SU 1)	Oct 12, 2007			Baselined	Mandatory	ZENworks Servers
◁ ▷ 1 - 5 of 10						show 5 ▾ items

6 Determine whether to deploy the downloaded update, then select its check box.

You can deploy only one update at a time.

If in Step 4 you did not review the content of the update that you downloaded, but need to at this time to determine whether to deploy it, see Section 12.5, "Reviewing the Content of an Update," on page 123 for instructions about reviewing the content of a downloaded update.

If you want to download a different update for deployment, return to Step 4.

7 Click *Action > Deploy Update to Devices*.

This starts the Create System Update Deployment Wizard for deploying the update to all applicable devices. If deployment stages are enabled, they can be used.

The Deployment Wizard provides you with many options, including scheduling the deployment.
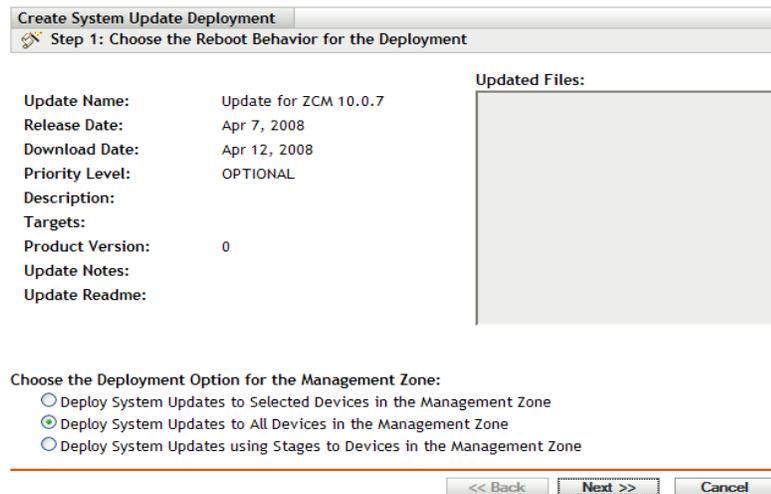
8 In the Deployment Wizard, complete the following steps:

8a On the Choose the System Update and Deployment Option page, select one of the following deployment options (all of them can be scheduled in a subsequent wizard page):

- **Deploy System Updates to Selected Devices in the Management Zone:** Deploys the selected update to only the devices that you select in Step 8e. Stages are not used.

- **Deploy System Updates to All Devices in the Management Zone:** Deploys the selected update to all devices in the Management Zone. Stages are not used.

- **Deploy System Updates Using Stages to Devices in the Management Zone:** The selected update is deployed to only the devices that have membership in one of the stages. The stages are executed one after the other; that is, a stage does not start until the previous stage completes.

   For more information on stages, see the Section 12.1.2, "Creating Deployment Stages," on page 97.

8b Click *Next* to display the Choose the Reboot Behavior for the Deployment page.

Create System Update Deployment

Step 2: Choose the Reboot Behavior for the Deployment

Choose the Reboot Behavior for the Deployment:

- ◉ Prompt user to reboot when update finishes applying
- ○ Do not reboot device
- ○ Force device to reboot

[<< Back] [Next >>] [Cancel]

8c Select one of the following options:

- ◆ **Prompt User to Reboot When Update Finishes Applying (Default):** After the update has been applied, a request to reboot is immediately displayed. If the user initially rejects rebooting, the user is periodically requested to reboot the device, until the device is rebooted.
- ◆ **Do Not Reboot Device:** The device does not reboot; however, the user is periodically requested to reboot the device, until the device is rebooted.
- ◆ **Force Device to Reboot:** After the update has been applied, the device is automatically rebooted without user intervention, if a reboot is required by the update,.

Some updates do not require a device to be rebooted after they have been deployed to a device. However, if a reboot is required to complete the update process, the deployment is not completed until the device is rebooted.

8d Click *Next*.

8e (Conditional) If you selected *Deploy System Updates to Selected Devices* in the Management Zone in Step 8a, the following wizard page displays:

Create System Update Deployment

Step 3: Choose the Deployment Devices and Groups

Add Remove	
☐ **Name**	**In Folder**
No items selected, click add to select items	

[<< Back] [Next >>] [Cancel]

8f To add devices or groups to the deployment configuration, click *Add*, browse for and select the devices or device groups to include in the update deployment, then click *OK*.

8g Click *Next* to display the Choose the Deployment Schedule page.

8h Fill in the fields:

Schedule Type: Select one of the schedule options:

- ◆ **Now:** Immediately deploys the update when you finish the wizard.
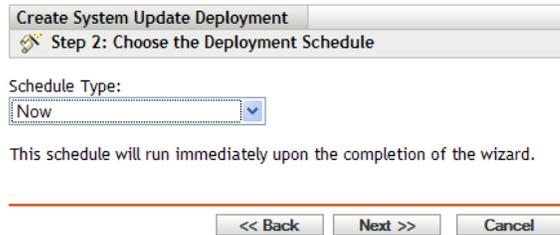
◆ **Date Specific:** Deploys the update according to the schedule that you set. The following options are displayed for the *Date Specific* option:
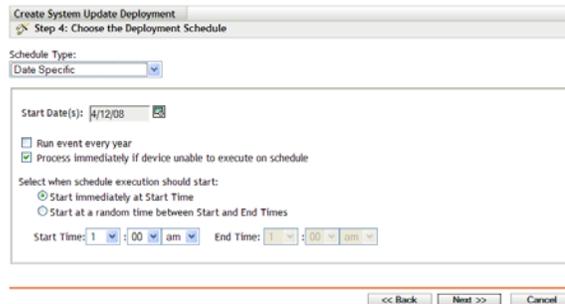
Fill in the fields:

   ◆ **Start Date:** Select the deployment date from the calendar.

   ◆ **Run Event Every Year:** Select to deploy the update every year on the start date.

   ◆ **Process Immediately if Device Unable to Execute on Schedule:** Do not use this option for updates. It applies only to bundles that you create in ZENworks Control Center.

   ◆ **Start Immediately at Start Time:** Lets you deploy updates at the start time you specify.

   ◆ **Start at a Random Time Between Start and End Times:** Lets you deploy updates at a random time between the times you specify. Fill in the *End Time* fields.

8i Click *Next* to display the Review Deployment Options page, then review the information.
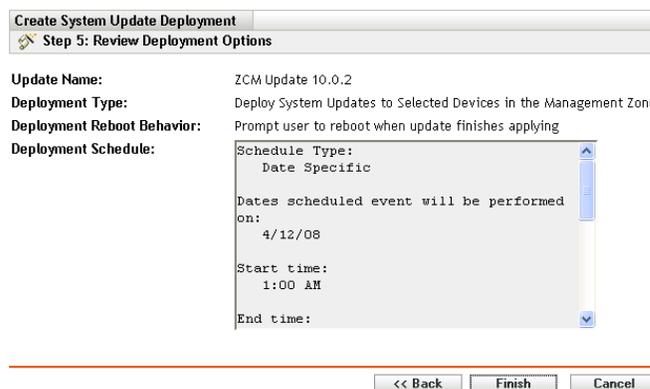
If satisfied, click *Finish* to start the update's deployment; otherwise, click *Back* to make changes.

9 To observe the progress of the update deployment, do any of the following:

- In ZENworks Control Center, observe the panels on the System Updates page:
  - The Available System Updates panel automatically displays `Baselined` in the *Status* column when the deployment has completed.
  - The Deployed System Updates panel displays the update in its listing when the deployment has completed.
- On a Windows device where the update is being deployed, right-click the ZENworks icon, then select *Show Progress* to open the ZENworks Progress dialog box.

  You cannot view the download progress on a Linux device because these devices are not managed in ZENworks 10 Configuration Management and do not have the ZENworks icon.

  The progress of downloading the update MSI files is displayed. When it has finished, the dialog box automatically closes and the *Show Progress* option is dimmed.

  After a 5-minute wait, all ZENworks services are closed on the device. Then the MSIs (for Windows) or RPMs (for Linux) are installed and the services are restarted.

10 To verify that the update was successfully deployed:

10a To verify that the MSIs or RPMs have been installed and the update process is complete, review the following log files:

Windows:

installation_path`\novell\zenworks\logs\systemupdate.log`

Linux: `/var/opt/novell/log/zenworks/SystemUpdate.log`

You can also look for the existence of the following file (the same path for both Windows and Linux):

installation_path`\novell\zenworks\work\system-`
`update\systemupdate.ini.`*timestamp*

10b Test the ZENworks software on the device to ensure that it is working properly.

10c To ensure that the update has been deployed on a Windows device, do one of the following to determine whether the version number has been incremented (for example, the first update for ZENworks should change the value from 10.0.*x* to 10.0.2):

- Open the Windows Registry and browse to the following:

  HKEY_LOCAL_MACHINE/Software/Novell

  For the *ZENworks* key, the update process should have incremented the *version* value.

- On a Windows device, review the following file:

  Installation_path`\Novell\ZENworks\version.txt`

- On a Linux device, review the following file:

  `/etc/opt/novell/zenworks/version.txt`

10d Repeat Step 10a through Step 10c for each test device.

11 (Conditional) If you are receiving e-mail notifications at the completion of the deployment stages and are ready to begin the next stage, go to the Deployed System Updates panel, then click *Action > Advance to Next Stage*.

12 To deploy another update, repeat from Step 4.

12.3.3 Starting the Pending Stage

The default stage behavior is to automatically advance through the configured stages. However, you can configure stage behavior for individual stages or for all stages.

The *Start Pending Stage* option is only available if you used the *Advance to Next Stage Manually and Notify When Complete* option to stop each stage for manual input before continuing, instead of having the stages complete automatically.

To start the pending stage:

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

2 In the Deploying System Updates panel, select the check boxes for an update.

3 Click *Action > Start Pending Stage*.

12.3.4 Rescheduling a Deployment

You can do reschedule a deployment only before a it starts.

To reschedule a deployment for a staged status or for All Stages status:

1 Select the check box for an update.

Because all devices do not need to have the update deployed at the same time, you can set individual deployment schedules for the devices.

2 Click *Action > Reschedule Deployment* to open the Redeployment Schedule dialog box.

3 Either click *OK* to accept the default schedule of *Now*, or select *Date Specific* in the *Schedule Type* field, specify the new date, then click *OK*.

To reschedule a deployment for other statuses:

1 Select the check box for an update.

2 Click *Action > Reschedule Deployment*.

3 In the Status by Device page, select the check box for an update, then click *Reschedule Deployment*.

4 On the Status by Device page, select one or more devices that are listed in the *Device* column.

5 Click *Reschedule Devices* to open the Redeployment Schedule dialog box.

6 Either click *OK* to accept the default schedule of *Now*, or select *Date Specific* in the *Schedule Type* field and specify the new date, then click *OK*.

12.3.5 Bypassing Staging

You can bypass the stages at any time and immediately deploy the update to all managed devices in the Management Zone.

1 Select the check box for an update.

2 Click *Action > Bypass Stages and Apply to All Devices*.

12.3.6 Canceling a Deployment

This option is mainly for canceling a deployment that has not yet started.

If you select to apply the update only through stages, and if you cancel the update deployment, the status in the Available System Updates panel is changed to *Aborted*.

However, for an update, you can select to deploy to individual devices, as well as through stages for the other devices. Therefore, the status in the Available System Updates panel is changed to:

- *Ready* if you cancel only the staged deployment.
- *Aborted* if you cancel both the staged deployment and the deployment for individually selected devices.

1 Select the check box for an update.

2 Click *Action > Cancel Deployment*.

> **WARNING:** If you cancel a deployment that is currently running (not just scheduled), all deployment actions performed up to that point cannot be reversed. There currently is no rollback option.

3 Click *OK* to confirm canceling the deployment.

12.3.7 Clearing an Error to Retry a Deployment

Allows you to continue with the deployment after determining whether the error is a reason to stop, or not serious enough and you can continue the deployment.

1 Click *Action > Clear Error and Continue*.

12.3.8 Viewing Status by Device

The following sections contain more information:

- "Understanding Device Statuses" on page 119
- "Viewing a Device's Properties" on page 120
- "Viewing Information on a Device's Status" on page 121
- "Toggling Ignored Devices" on page 121
- "Redeploying Updates to Devices" on page 122
- "Rescheduling Updates to Devices" on page 122

Understanding Device Statuses

The following graphic illustrates the Deploying System Updates panel on the System Updates page:

Figure 12-6   *Deploying System Updates Panel*

Deploying System Updates							
Action ▾							
☐ Update Name	Start Schedule	Reboot Behavior	Stage	Status	Pending	Successful	Failed
☐ ZCM Update 10.0.2	Now	Prompt User	All Devices Stage	In Process	1	0	0

You can click any of the underlined links to display the corresponding status of devices. For example, if you click the link in the *Pending* column, you see the status of devices on which the deployment is pending, as in the following figure:

Figure 12-7 *Device by Status Page for Devices with Pending Status*

The possible statuses that can be viewed on this page are:

All Devices: Lists all devices that were configured to receive the selected update, regardless of status.

Pending Devices: Lists only the devices where the selected update is pending.

Successful Devices: Lists all of the devices where the selected update has been successfully deployed.

Failed Devices: Lists only the devices where the selected update failed.

Update Assigned: Lists only the devices where the selected update has been assigned.

The following table explains the column information. For some columns, you can sort the listed information by clicking a column heading. Click it again to reverse the sorting order. This page refreshes automatically to allow you to work with devices as the update is applied on them.

Column Heading	Explanation
Device	The device's name. Click it to display the device's properties page in ZENworks Control Center.
Status	The current update deployment status for the device. Click the status item to view information about the status.
	For more information on the individual statuses, see Section 12.6, "Update Statuses," on page 126.
Device Type	Whether the device is a server or workstation.
In Folder	Displays the ZENworks Control Center folder where the device's ZENworks object resides.

Viewing a Device's Properties

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

2 In the Deploying System Updates panel, click an underlined link in the Update Name, Stage, Pending, Successful, or Failed column to display the appropriate Status by Device page.

For example, if you click the link in the Pending column, you see the status of devices on which the deployment is pending, as in the following figure:

3 Click the underlined link in the Device column to display the device's properties.

Viewing Information on a Device's Status

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

2 In the Deploying System Updates panel, click an underlined link in the Update Name, Stage, Pending, Successful, or Failed column to display the appropriate Status by Device page.

For example, if you click the link in the Pending column, you see the status of devices on which the deployment is pending, as in the following figure:

3 Click the underlined link in the Status column to display status information about the device.

Toggling Ignored Devices

Ignoring a device is helpful if an update fails on a device and you want to continue with the deployment without resolving the error. For example, if a device is offline, you might want to ignore that device so that the deployment can continue.

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

2 In the Deploying System Updates panel, click an underlined link in the *Update Name*, *Stage*, *Pending*, *Successful*, or *Failed* column to display the appropriate Status by Device page.

For example, if you click the link in the *Pending* column, you see the status of devices on which the deployment is pending, as in the following figure:

3 Click the check box next to one or more devices.

4 Click *Action > Toggle Ignored Devices*.

The options available from the Action menu vary, depending on whether you are viewing the All Assigned Devices Status panel, the Devices with Pending Status panel, or the Devices with

Failed Status panel. If you are viewing the Devices with Success Status panel, no options are available.

Redeploying Updates to Devices

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

2 In the Deploying System Updates panel, click an underlined link in the *Update Name*, *Stage*, *Pending*, *Successful*, or *Failed* column to display the appropriate Status by Device page.

For example, if you click the link in the *Pending* column, you see the status of devices on which the deployment is pending, as in the following figure:

3 Select the check box next to one or more devices.

4 Click *Action > Redeploy Update to Devices*.

The options available from the Action menu vary, depending on whether you are viewing the All Assigned Devices Status panel, the Devices with Pending Status panel, or the Devices with Failed Status panel. If you are viewing the Devices with Success Status panel, no options are available.

Rescheduling Updates to Devices

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

2 In the Deploying System Updates panel, click an underlined link in the *Update Name*, *Stage*, *Pending*, *Successful*, or *Failed* column to display the appropriate Status by Device page.

For example, if you click the link in the *Pending* column, you see the status of devices on which the deployment is pending, as in the following figure:

3 Select the check box next to one or more devices.

4 Click *Action > Reschedule Devices*.

The options available from the Action menu vary, depending on whether you are viewing the All Assigned Devices Status panel, the Devices with Pending Status panel, or the Devices with Failed Status panel. If you are viewing the Devices with Success Status panel, no options are available.

The *Reschedule Devices* option displays only when the update deployment is scheduled. If the update has a schedule of *Now,* this option is not available.

12.4 Deleting Updates

To clear out an update that fails to download, or an update that you do not want to deploy:

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

2 In the Available System Updates panel, select the check boxes for one or more updates.

3 Click *Action > Delete Update*.
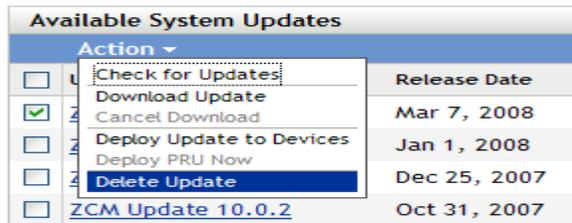
The update is deleted from the list and all downloaded files are removed. However, if the deleted update is still available on the update server, it is displayed in the list again for possible downloading the next time that you check for updates.

12.5 Reviewing the Content of an Update

You might want to review the content of an update for the following reasons:

- To determine whether to download the update
- To determine whether to deploy a downloaded update
- To review what was deployed by the update
- To review the history of the update

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

2 In the Available System Updates panel, click an update name in the *Update Name* column to display the Release Details page:
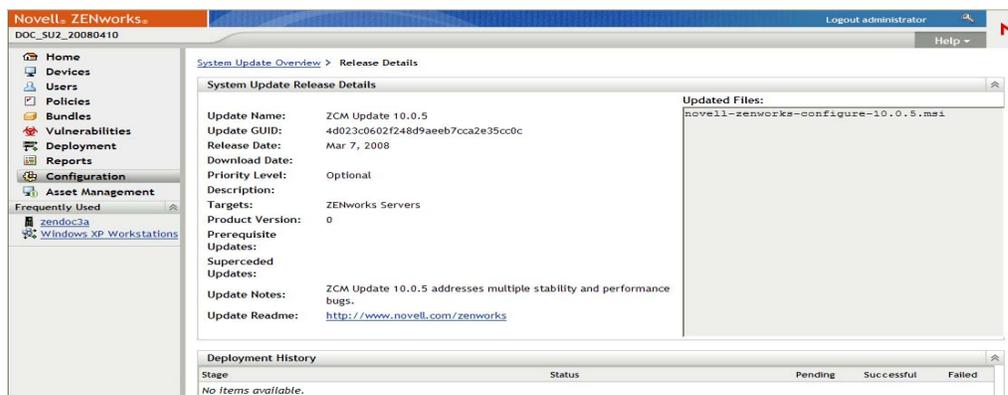
The Release Details page contains the following information:

12.5.1 Update Release Details

The System Update Release Details panel lists the following information:

Column Heading	Explanation
Update Name	Displays the name of the update, which is created by Novell.
Update GUID	Displays the update's GUID.
Release Date	Displays the date the update was released by Novell.
Download Date	Displays the date you downloaded the content of the update, including all files necessary to install the update.
Priority Level	Displays the relative importance of the update's content to your ZENworks installation. Some possible entries:
	OPTIONAL: Not required for normal operation of ZENworks 10 Configuration Management.
	MANDATORY: A required update that must be applied.
Description	Displays brief information about the purpose of the update and its content.
Targets	Indicates whether the target devices are Primary Servers only, all managed devices, or servers with ZENworks roles.
Product Version	The version of ZENworks in this update.
*Prerequisite Update*s	Displays any updates that are required for this update.
Superseded Updates	Displays any updates that the current update supersedes.
Update Notes	Displays brief information about important issues related to the update.
Update Readme	Information pertinent to deploying the update, such as last-minute instructions. Click this entry to open the Readme.
Updated Files	Lists all of the files contained in the update that will be applied to update your ZENworks software.

12.5.2 Deployment History

This Deployment History panel displays a current snapshot of the history for the selected update. It does not automatically refresh its content.

The following sections contain more information:

Understanding Deployment History Details

The following table explains the column information.

Column Heading	Explanation
Stage	Indicates the deployment method used. The possible entries are:
	stage_name: The update was deployed to the managed devices that are members of the stage that is listed.
	Selected Devices Stage: The update was deployed to selected managed devices in the Management Zone that are not members of a stage.
	All Devices Stage: The update was deployed to all managed devices in the Management Zone that are not members of a stage.
Status	Indicates the status of the update that was successfully deployed, such as *Applied* or *Baselined*.
	In Process: The update is currently being deployed to the members of the stage.
	For more information on the individual statuses, see Section 12.6, "Update Statuses," on page 126.
Pending	Displays the number of devices for which the update deployment process is pending. A device can be pending if it is a member of a stage when stages are not automatically started after another stage completes.
	Click the number to view the Status by Device page, with the devices displayed that have the deployment of the update pending.
Successful	Displays the number of devices for which the update deployment process has completed.
	Click the number to view the Status by Device page, with the devices displayed that successfully received the update.
Failed	Displays the number of devices for which the update deployment process has failed.
	Click the number to view the Status by Device page, with the devices displayed that failed to receive the update.
	For failed deployments, you have the option of ignoring the error and continuing, or you can redeploy the update if the error has been resolved.

Performing Deployment History Tasks

To evaluate an update's deployment history, perform the tasks in the following table:

Task	Steps	Additional Details
View which devices have their deployment pending	1. In the Deployment Stages panel, click the number in the *Pending* column. 2. On the Status by Device page, review the information.	Displays devices where the deployment of the update is pending.

Task	Steps	Additional Details
View the devices where deployment was successful	1. In the Deployment Stages panel, click the number in the *Successful* column. 2. On the Status by Device page, review the information.	Displays devices that have had the selected update successfully applied.
View which devices had their deployment fail	1. In the Deployment Stages panel, click the number in the *Failed* column. 2. On the Status by Device page, review the information.	Displays devices where the update deployment failed. In order to consider a deployment successfully finished when there are failed devices, the failed devices should either be ignored, or the error should be fixed before you redeploy the update to those failed devices.

12.6 Update Statuses

The following update statuses can be displayed in the *Status* column of several System Update panels in ZENworks Control Center:

Aborted: The deployment of the update was stopped, such as by selecting *Action > Cancel Deployment*.

Applied: The update was successfully applied to the managed devices.

Available: When updates availability is checked, this is their default status. Updates with this status have downloaded information about the update, which you can view by clicking the update name in the *Update ID* column.

Awaiting Reboot: The device is waiting for you to manually reboot after the update has been applied.

Baselined: Indicates that the update files have been placed in the download directory, so that when managed devices register with the server they can obtain the latest updates.

Canceled: Displays after you select *Action > Cancel Download* and the download or deployment was successfully canceled.

Canceling: Temporarily displays after you select *Action > Cancel Download*.

Deploying: Indicates that the update is currently being deployed. See Deploying System Updates for further deployment information and for actions that you can take on an update that is being deployed.

Downloaded: Indicates that you have downloaded the update's content. It is then ready for deployment. See Deploying System Updates for further deployment information and for actions that you can take on an update that has been deployed.

Downloading: Displays a percentage of completion during the downloading process. This status changes to *Downloaded* when the download is complete.

Error: Indicates that the stage failed to complete because of an error with one or more of the devices being updated. You can select to ignore the error and continue, or to fix the error before continuing. Can also indicate an error downloading the update.

In Process: Indicates that the current stage is active.

Installing Update: Indicates that the update is currently being installed on the device.

Ready: Indicates that the current stage is ready to start.

Reboot in Process: Indicates that rebooting of the device is in process.

Reboot Process Canceled: Indicates that rebooting of the device after the update was applied was canceled.

Scheduled: The update has a schedule defined for it. See Deploying System Updates when creating the deployment in the Create System Update Deployment Wizard. You can alter the update's schedule by using the *Action > Reschedule Deployment* option.

Stage Complete: Indicates that the stage has completed.

Status Unknown: The status of updates for the device is unknown.

Update Aborted: The update was canceled for the device.

Update Completed: The installation of the update has been completed on the device.

Update Completed with Errors: The installation of the update has been completed on the device, but there were errors. Check the update log for details.

Update Assigned: The update has been assigned to the device.

Zone Pre-Update Actions: Indicates that actions for the Management Zone are taking place before the server update begins.

Zone Post-Update Actions: Indicates that actions for the Management Zone are taking place after the server upgrade finishes.

Database Maintenance

13

Novell® ZENworks® 10 Configuration Management allows you to back up and restore the embedded Sybase* SQL Anywhere* database by using the zman command line utility. To back up and restore Remote Sybase SQL Anywhere or Microsoft SQL Server databases, refer to their documentation.

13.1 Backing Up the Embedded Sybase SQL Anywhere Database

The embedded Sybase SQL Anywhere database can be backed up to a directory on the local machine or to a network location.

13.1.1 Backing Up the Embedded Sybase SQL Anywhere Database on a Windows or Linux Server

1 Store the ZENworks administrator name and password by entering the following command at the command prompt:

```
zman admin-store-credential administrator
```

If you do not store the credentials, then you must enter the ZENworks administrator name and password for each zman command.

You can back up the embedded Sybase SQL Anywhere database immediately or schedule the backup to run at a specific time. To back up the embedded Sybase SQL Anywhere database immediately, continue with Step 2. To schedule the backup to run at a specific time, skip to Step 3.

2 To back up the embedded Sybase SQL Anywhere database immediately to a directory on the database server, enter the following command at the command prompt:

```
zman database-backup
complete_path_of_the_backup_directory_on_database_server
```

For example, to back up the database to the c:\dbbackup directory on a Windows database server, execute zman database-backup c:\dbbackup. To back up the database to the /root/dbBackup directory on a Linux database server, execute zman database-backup /root/dbBackup.

3 To schedule the backup to run at a specific time every day or on specific days of a month, you need to create a schedule file and run it.

3a Create a schedule file, `backupschedule`, with the following contents:

```
CREATE EVENT backup_schedule_name
SCHEDULE
specify_the_schedule
```

A sample schedule file to back up the database at a 11 P.M. every day is as follows:

```
CREATE EVENT ZENDBBackup
SCHEDULE
START TIME '11:00 PM' EVERY 24 HOURS
```

A sample schedule file to back up the database at 1:00 A.M on the first, second, third and fourth days of the month is as follows:

```
CREATE EVENT ZENDBBackup1
SCHEDULE
START TIME '1:00 AM'
ON (1,2,3,4)
```

Sample schedule files are available in the `ZENworks_Installation_directory:\Novell\Zenworks\share\zman\ samples\database` directory on a Windows server, and in the `/opt/novell/ zenworks/share/zman/samples/database` directory on a Linux server.

3b Enter the following command at the command prompt:

```
zman database-backup complete_path_of_the_backup_directory
backUpSchedule -d SQL_function_call
```

For example, to back up the database to the `c:\dbbackup\day_of_the_week` directory on a Windows server, enter the following command:

```
zman database-backup c:\dbbackup backUpSchedule -d
"DAYNAME(today())"
```

For more information about this command, view the zman man page (man zman) on the device, or see zman(1) in the *ZENworks 10 Configuration Management Command Line Utilities Reference*.

4 Clear the credentials stored in Step 1 by entering the following command at the command prompt:

```
zman admin-clear-credential
```

According to the backup schedule, `zenworks_zone_name.db` and `zenworks_zone_name.log` are created in the database backup directory. The backed-up database is stored in `zenworks_zone_name.db`. The result of the database backup is logged into `zenworks_zone_name.log`.

13.1.2 Backing up the Embedded Sybase SQL Anywhere Database Running on a Windows Server to a Network Location on a Remote Windows Machine

To back up an embedded Sybase SQL Anywhere database that is installed and running on a Windows server to a network location on another Windows machine, you need two machines, a local machine and a remote machine. The local machine is a Windows server having the ZENworks

server components and the embedded Sybase SQL Anywhere database installed. The remote machine is a Windows machine with the network location to which you want to back up the database.

1 Perform the following steps on the local machine:

    1a Create an administrative user and specify a password.

        For example, you could specify the administrative username as `Administrator` and the password as `novell`.

    1b From the desktop *Start* menu, click *Settings*, click *Control Panel*, double-click *Administrative Tools*, then double-click *Services*.

    1c Right-click the *Novell ZENworks Datastore* service, then click *Properties*.

    1d Click the *Log On* tab.

    1e Select *This account*, then specify the name and the password of the administrative user created in Step 1a.

        For example, specify the user as `Administrator` and the password as `novell`.

    1f Click *OK*.

2 Perform the following steps on the remote machine with the network location where you want to save the backup:

    2a Create an account with the same credentials as the user you created in Step 1a.

        For example, specify user as `Administrator` and password as `novell`.

    2b Provide Read/Write permission on the network location to the user.

        To immediately back up the database, continue with Step 3. To schedule the backup to run at a specific time every day or on specific days of a month, skip to Step 4.

3 To immediately back up the database to the network location on the remote machine, enter the following command at the command prompt:

```
zman database-backup
\\IP_address_of_the_remote_machine\backup_directory
```

Where *IP_address_of_the_remote_machine\backup_directory* is the network location on the remote machine.

4 To schedule the backup:

    4a Create a schedule file, `backupschedule`, with the following contents:

```
CREATE EVENT backup_schedule_name
SCHEDULE
specify_the_schedule
```

        A sample schedule file to back up the database at a 11 P.M. every day is as follows:

```
CREATE EVENT ZENDBBackup
SCHEDULE
START TIME '11:00 PM' EVERY 24 HOURS
```

        A sample schedule file to back up the database at 1:00 A.M on the first, second, third, and fourth days of the month is as follows:

```
CREATE EVENT ZENDBBackup1
SCHEDULE
START TIME '1:00 AM'
```

```
ON (1,2,3,4)
```

Sample schedule files are available in the
`ZENworks_Installation_directory\Novell\Zenworks\`
`share\zman\samples\database` directory.

4b Execute the following command at the command prompt:

```
zman database-backup
\\IP_address_of_the_remote_machine\backup_directory
backUpSchedule -d SQL_function_call
```

Where *IP_address_of_the_remote_machine\backup_directory* is the network location on the remote machine.

For more information about this command, view the zman man page (man zman) on the device, or see zman(1) in the *ZENworks 10 Configuration Management Command Line Utilities Reference*.

According to the backup schedule, zenworks_*zone_name*.db and zenworks_*zone_name*.log are created in the network location on the remote machine. The backed-up database is stored in zenworks_*zone_name*.db. The result of the database backup is logged into zenworks_*zone_name*.log.

13.1.3 Backing up the Embedded Sybase SQL Anywhere Database Running on a Linux Server to a Network Location on a Remote Linux Machine

To back up the embedded Sybase SQL Anywhere database that is installed and running on a Linux server to a network location on a Linux machine, you require two machines, a local machine and a remote machine. The local machine is a Linux server having the ZENworks server components and the embedded Sybase SQL Anywhere database installed. The remote machine is a Linux machine having the network location to which you want to back up the database.

1 Create a Samba share on the remote machine.

   1a Create a user by entering the `useradd user_name` command at the command prompt.

   1b Log in to the remote machine with the username created in Step 1a, and set the password by using the `passwd specify_the_password` command.

   1c Create a directory to save the database backup.

   For example, create a directory with the name `backup`.

   1d Open the Samba server settings by running the `yast2 samba-server` command.

   1e Click the *Shares* tab, then click *Add* to specify the share name and the path to the backup directory created in Step 1c.

   For example, specify the sharename as `dbbackup`.

   1f Select the `dbbackup` share, then click *Edit* to add the following attributes:

   - create mask = 0640
   - force user = *user_name_created_in_*Step 1a
   - guest ok = yes
   - public = yes
   - wide links = no

◆ writeable = yes

2 Create a directory on the local machine.

For example, create a directory with the name `zenworks_dbbackup` in `/root.`

3 Mount the Samba share on the `zenworks_dbbackup` directory on the local machine by entering the following command at the command prompt:

```
mount -t smbfs //IP_address of the remote_machine/share_name -o
username=user_name_specified_in_Step1a,password=password_
specified_in_Step_1b
local_directory_name_with_complete_path_created_in_Step2
```

For example:

```
mount -t smbfs //IP_address of the remote_machine/dbbackup -o
username=user_name_specified_in_Step1a,password=password_
specified_in_Step_1b /root/zenworks_dbbackup
```

To immediately back up the database, continue with Step 4. To schedule the backup to run at a specific time every day or on specific days of a month, skip to Step 5.

4 To immediately back up the database to the network location on the remote machine, enter the following command at the command prompt:

```
zman database-backup database_backup_directory
```

For example:

```
zman database-backup /root/zenworks_dbbackup
```

5 To schedule the backup:

5a Create a schedule file, `backupschedule`, with the following contents:
```
CREATE EVENT backup_schedule_name
SCHEDULE
specify_the_schedule
```
A sample schedule file to back up the database at a 11 P.M. every day is as follows:
```
CREATE EVENT ZENDBBackup
SCHEDULE
START TIME '11:00 PM' EVERY 24 HOURS
```
A sample schedule file to back up the database at 1:00 A.M on the first, second, third, and fourth days of the month is as follows:
```
CREATE EVENT ZENDBBackup1
SCHEDULE
START TIME '1:00 AM'
ON (1,2,3,4)
```
Sample schedule files are available in the `ZENworks_Installation_directory:\Novell\Zenworks\ share\zman\samples\database` directory.

5b Enter the following command at the command prompt:
```
zman database-backup database_backup_directory
backUpSchedule -d SQL_function_call
```
For example:

```
zman database-backup /root/zenworks_dbbackup backUpSchedule
-d SQL_function_call
```

For more information about this command, view the zman man page (man zman) on the device, or see zman(1) in the *ZENworks 10 Configuration Management Command Line Utilities Reference*.

According to the backup schedule, `zenworks_zone_name.db` and `zenworks_zone_name.log` are created in the network location on the remote machine (`/root/zenworks_dbbackup`). The backed-up database is stored in `zenworks_zone_name.db`. The result of the database backup is logged into `zenworks_zone_name.log`.

13.2 Restoring the Embedded Sybase SQL Anywhere Database

The following sections provide information on restoring the backed-up embedded Sybase SQL Anywhere database:

13.2.1 Restoring the Embedded Sybase SQL Anywhere Database on a Windows Server

1 At the Windows server prompt, go to `ZENworks_Installation_directory:\Novell\Zenworks\share\ASA\win32`, and enter the following command:

```
ZenworksWindowsDBRestore.bat
ZENworks_Installation_directory:\Novell\Zenworks\Database
c:\dbBackup\zenworks_zone_name.db
c:\dbBackup\zenworks_zone_name.log
```

2 Press any key when the following message is displayed:

```
Before proceeding, make sure you have backed up any files
in:<Installation directory>:\Novell\ZENworks\database Press any
key to continue.
```

3 Enter `Y` when the following message is displayed:

```
The following services are dependent on the Novell ZENworks
Datastore service. Stopping the Novell ZENworks Datastore service
will also stop these services: Novell ZENworks Loader, Novell
ZENworks Agent Service, Novell ZENworks Server. Do you want to
continue this operation? (Y/N) [N]:
```

4 Press any key when the following message is displayed:

```
The Novell ZENworks Datastore service was stopped successfully.
Press any key to continue...
```

5 Enter `Yes` when the following message is displayed:

```
Overwrite <installation
directory>:\Novell\ZENworks\database\zenworks_<zone_name>.db?
(Yes/No/All)
```

6 Enter `Yes` when the following message is displayed:

```
Overwrite <installation
directory>:\Novell\ZENworks\database\zenworks_<zone_name>.log?
(Yes/No/All):
```

The `backupFile` and the `backupLogFile` are copied to
ZENworks_Installation_directory:\Novell\ZENworks\database, and the
database is restored.

13.2.2 Restoring the Embedded Sybase SQL Anywhere Database on a Linux Server

1 Log in to the ZENworks server as `root`.

2 Change to `/opt/novell/zenworks/share/sybase/bin32`, and enter the following
command:

```
./ZenworksLinuxDBRestore.sh -F "/root/dbBackup/
zenworks_zone_name.db"
```

3 Enter `Y` when the following message is displayed:

```
The backup database file will OVERWRITE the existing database. Is
that OK? [y/n]
```

4 Enter `Y` when the following message is displayed:

```
The novell-zenloader needs to be stopped for the database restore
to be performed. Would you like to proceed [y/n]?
```

The `backup` file is copied to `/var/opt/novell/zenworks/database`, and the restore
log file to `/var/opt/novell/log/zenworks/dbrestore.log`. The database is
restored.

ZENworks Server Backup and Restore

14

Novell® ZENworks® 10 Configuration Management allows you to back up and restore the configuration files for a ZENworks Server. This enables you to maintain a ZENworks Server's identity and configuration if a server fails or if you need to upgrade to new server hardware.

Only the configuration files are backed up. The content repository (bundle, policy, and image files) is not backed up. In addition, if you are backing up the ZENworks Server that hosts the ZENworks database, the ZENworks database is not backed up. Therefore, in addition to backing up the ZENworks Server (which only needs to be done one time), you should also back up the ZENworks database on a regular basis. For information about backing up the database, see Chapter 13, "Database Maintenance," on page 129.

- Section 14.1, "Backing Up a ZENworks Server," on page 137
- Section 14.2, "Restoring a ZENworks Server," on page 137

14.1 Backing Up a ZENworks Server

When you back up a ZENworks Server, all files in the `Novell\ZENworks\conf` directory on a Windows server or the `etc/opt/novell/zenworks/conf` directory on a Linux server are stored in an encrypted backup file in a location you specify.

1 At a command prompt on the ZENworks Server, enter the following command:

   `zman zenserver-backup` *path_to_backup_file_to_create*

   For example:

   `zman zenserver-backup c:\zcm_backups\zone_backup.bak`

   or

   `zman zenserver-backup /root/zcm_backups\zone_backup.bak`

2 When prompted, enter a ZENworks administrator name and password.

3 When prompted, enter a passphrase (at least 10 characters) to be used for encrypting the backup file.

   Make sure you remember this passphrase. You must enter it if you ever need to restore the server.

14.2 Restoring a ZENworks Server

The following instructions assume the following:

- You have a backup of the ZENworks Server's configuration information. See Section 14.1, "Backing Up a ZENworks Server," on page 137.
- If the ZENworks database resides on the ZENworks Server, you have a backup of the database. See Section 13.1, "Backing Up the Embedded Sybase SQL Anywhere Database," on page 129.

◆ The bundles and policies that are stored on the ZENworks Server have been replicated to other ZENworks Servers. If not, distribution of a policy or bundle from the restored ZENworks Server will fail.

◆ The image files that are stored on the ZENworks Server are available on another ZENworks Server. If not, distribution of the image files from the restored ZENworks Server will fail.

1 Reinstall the ZENworks Server using the same IP address and DNS name.

If you do not use the same IP address and DNS name, any devices that connect to the server need to reregister.

2 Ensure that you have read/write rights to the `Novell\ZENworks\conf` directory on a Windows server or the `etc/opt/novell/zenworks` directory on a Linux server.

3 At a command prompt on the ZENworks Server, enter the following command:

`zman zenserver-restore` *path_to_backup_file_to_restore*

For example:

`zman zenserver-restore c:\zcm_backups\zone_backup.bak`

or

`zman zenserver-restore /root/zcm_backups\zone_backup.bak`

4 When prompted, enter a ZENworks administrator name and password.

5 When prompted, enter the passphrase (at least 10 characters) to be used for decrypting the backup file.

This is the same passphrase that was entered to encrypt the file when backing up the server.

6 (Conditional) If the database is located on the server, restore the database after the ZENworks Server information has been restored. For instructions, see Section 13.2, "Restoring the Embedded Sybase SQL Anywhere Database," on page 134.

7 (Conditional) If you have backups of the image files, restore the files to the `Novell\Zenworks\work\content-repo\images` directory on a Windows server or the `/var/opt/novell/zenworks/content-repo/images` directory on a Linux server.

8 Restart the ZENworks Server.

System Variables

15

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:

15.1 Understanding System Variables

The following examples illustrate a few 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 could create a system variable. For example, the name of the variable could be "OpenOffice INI" and the value could be the full path to the file. Now, instead of specifying the full path and filename when you create the action, you could 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 could 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 would still point to the correct path.

You could 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 one bundle, and depending on the location of the targeted device object in the folder hierarchy, the value could 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 could define the ProgramFiles variable at the Management Zone level to point to `C:\program files`. For the accounting applications, you could create a device folder called Accounting Department to contain the devices in the accounting department. You could 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 would be 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 would point to the `D:\` drive.

15.2 Adding System Variables

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

2 In the Management Zone Settings list, click *Content*.
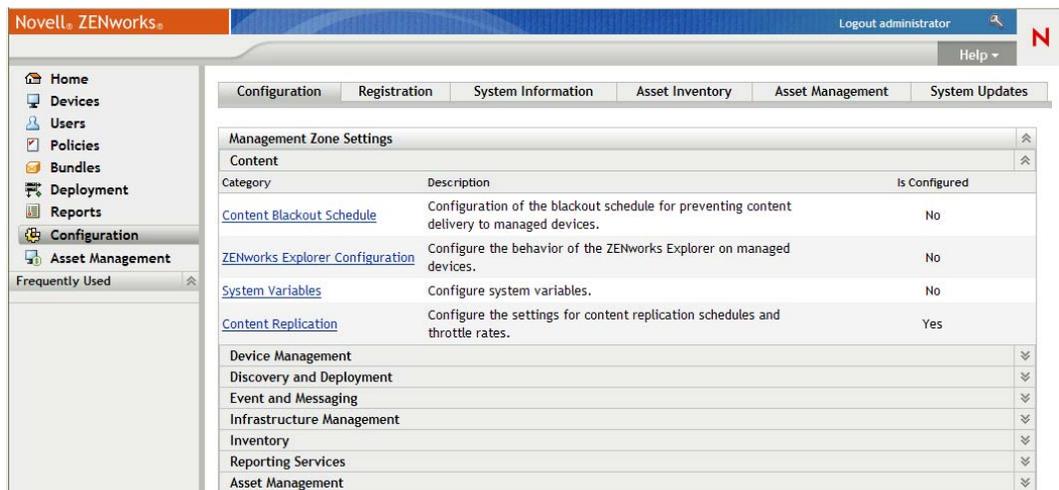
3 Click *System Variables*.
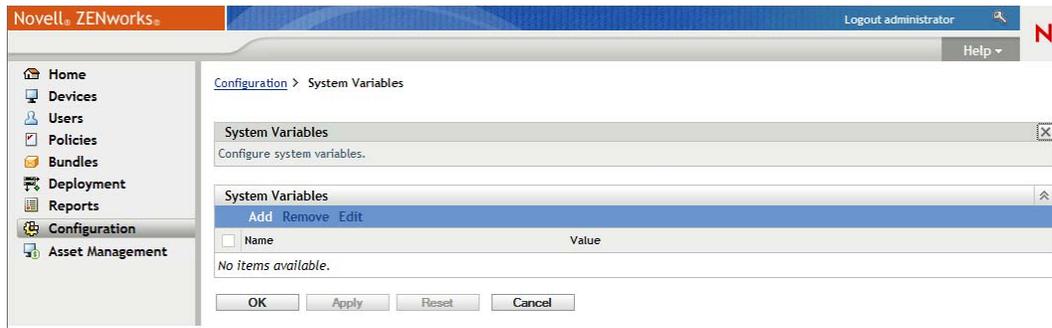
4 Click *Add*, provide the name and value for the variable, then click *OK*.

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).

5 Click *Apply*.

15.3 Removing System Variables

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

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

3 Click *System Variables*.

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

5 Click *Remove*.

6 Click *Apply*.

15.4 Editing System Variables

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

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

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*.

15.5 Using System Variables

1 Use the following syntax:

`${VAR_NAME}`

Replace `VAR_NAME` with the name of the variable.

Naming Conventions in ZENworks Control Center

<div style="text-align: right; font-size: 3em;">A</div>

When you name an object in the ZENworks® Control Center (folders, bundles, bundle groups, 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 10 Configuration Management 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 bundle 1 in quotes ("bundle 1") when entering it in the zman utility.
- The following characters are invalid and cannot be used: / \ * ? : " ' < > | ` % ~