

ZENworks 2017 Update 1 Administration Quick Start

July 2017

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.novell.com/company/legal/>.

Copyright © 2017 Micro Focus Software Inc. All Rights Reserved.

Contents

About This Guide	7
Part I System Configuration	9
1 Quick List	11
Management Tools	11
Zone Configuration	11
Agent Deployment	13
System Messages	14
2 Management Tools	15
ZENworks Control Center	15
Accessing ZENworks Control Center	15
Navigating ZENworks Control Center	16
zman Command Line Utility	18
Location	18
Syntax	18
Help with Commands	18
zac Command Line Utility	19
Location	19
Syntax	19
Help with Commands	20
3 Management Zone Configuration	21
Organizing Devices: Folders and Groups	21
Folders	21
Groups	22
Assignment Inheritance for Folders and Groups	24
Creating Registration Keys and Rules	24
Registration Keys	25
Registration Rules	25
Device Naming Template	26
Where to Find More Information	26
Connecting to User Sources	26
Creating ZENworks Administrator Accounts	27
Creating an Administrator Account	27
Creating an Administrator Group Account	28
Modifying Configuration Settings	29
Modifying Configuration Settings at the Zone	29
Modifying Configuration Settings on a Folder	29
Modifying Configuration Settings on a Device	30
Zone Sharing and Subscription	30
Updating ZENworks Software	31
Creating Locations	31
Defining a Network Environment	31
Creating Locations	32
Location and Network Environment Selection on a Managed Device	33

4	ZENworks Agent Deployment	35
	Configuring ZENworks Agent Features	35
	Customizing the ZENworks Agent Features	36
	Coexisting with the ZENworks Desktop Management Agent	36
	Configuring ZENworks Agent Security	37
	Installing the ZENworks Agent	38
	Manual Installation on Windows	38
	Manual Installation on Linux	39
	Manual Installation on Macintosh	40
	Using the ZENworks Agent	41
	Logging In to the Management Zone	41
	Navigating the ZENworks Agent Views	41
	Promoting a Managed Device to be a Satellite	43
5	System Messages	45
	Viewing System Messages	45
	Viewing a Summary of Messages	45
	Acknowledging Messages	46
	Where to Find More Information	47
	Creating a Watch List	47
6	Audit Management	49
	Types of Audit Events	49
	Enabling an Event	49
	Viewing a Generated Event	50
	Part II Product Administration	53
7	Quick List	55
	Asset Management	55
	Configuration Management	56
	Endpoint Security Management	57
	Full Disk Encryption	58
	Patch Management	59
8	Asset Management	61
	Activating Asset Management	61
	Enabling Asset Management in the ZENworks Agent	61
	Collecting Software and Hardware Inventory	62
	Initiating a Device Scan	62
	Viewing a Device Inventory	63
	Generating an Inventory Report	63
	Where to Find More Information	63
	Monitoring Software Usage	63
	Monitoring License Compliance	64
	License Compliance Components	64
	Discovering Installed Products	66
	Creating a Catalog Product and Purchase Record	66
	Creating a Licensed Product	67
	Viewing Compliance Data	69
	Where to Find More Information	70

Allocating Licenses	70
9 Configuration Management	73
Activating Configuration Management	73
Enabling Configuration Management in the ZENworks Agent	73
Distributing Software	74
Creating a Bundle	74
Assigning a Bundle	75
Where to Find More Information	75
Applying Policies	75
Creating a Policy	76
Assigning a Policy	77
Where to Find More Information	77
Imaging Devices	77
Setting Up Preboot Services	78
Taking an Image	81
Applying an Image	82
Where to Find More Information	85
Remotely Managing Devices	85
Creating a Remote Management Policy	87
Configuring Remote Management Settings	88
Performing Remote Control, Remote View, and Remote Execute Operations on a Windows Device	88
Performing a Remote Diagnostic Operation	90
Performing a File Transfer Operation	91
Performing Remote Control, Remote View, and Remote Login Operations on a Linux Device	92
Performing Remote SSH Operation on a Linux Device	93
Where to Find More Information	93
Collecting Software and Hardware Inventory	93
Initiating a Device Scan	94
Viewing a Device Inventory	94
Generating an Inventory Report	94
Where to Find More Information	94
Linux Management	94
10 Endpoint Security Management	97
Activating Endpoint Security Management	97
Enabling the Endpoint Security Agent	97
Creating Locations	98
Creating a Security Policy	98
Assigning a Policy to Users and Devices	100
Assigning a Policy to the Zone	101
Where to Find More Information	101
11 Full Disk Encryption	103
Activating Full Disk Encryption	103
Enabling the Full Disk Encryption Agent	104
Creating a Disk Encryption Policy	104
Assigning the Policy to Devices	105
Understanding What Happens After a Policy Is Assigned to a Device	105
Disk Encryption	105
Pre-Boot Authentication	106
Where to Find More Information	106

12 Patch Management	107
Activating Patch Management	107
Enabling Patch Management in the ZENworks Agent	108
Starting the Subscription Service	108
Creating Patch Policies	108
Where to Find More Information	109
Part III Mobile Management	111
13 Getting Started with Mobile Management	113
Overview	113
Using the Mobile Management Getting Started Page.	113
14 Enrolling Mobile Devices	115
Types of Enrollment	115
Modes of Enrollment.	116
Enrolling an iOS DEP Device	117
Prerequisites	117
Procedure.	117
Enrolling an iOS Device through Apple Configurator	118
Prerequisites	118
Procedure.	118
Enrolling devices using the ZENworks User Portal.	121
Prerequisites	121
Procedure: Enrolling an Android Device	122
Procedure: Enrolling an iOS Device.	130
Procedure: Enrolling an Email-only Device	138
Allowing Manual Reconciliation by User	142

About This Guide

This *ZENworks Administration Quick Start* helps you quickly master the basics of administering your ZENworks Management system. You should already have installed your ZENworks system. If not, see the [ZENworks Server Installation Guide](#).

The information in this guide is organized as follows:

- ♦ [System Configuration \(page 9\)](#): Provides instructions for configuring your ZENworks Management Zone prior to using the ZENworks products.
- ♦ [Product Administration \(page 53\)](#): Provides instructions for using ZENworks products (Asset Management, Configuration Management, Endpoint Security Management, Full Disk Encryption, and Patch Management).

Audience

This guide is intended for anyone who will configure the ZENworks system, monitor the ZENworks system, or perform any ZENworks tasks related to managing devices or users.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the *comment on this topic* link at the bottom of each page of the online documentation.

Additional Documentation

ZENworks is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the [ZENworks documentation website \(http://www.novell.com/documentation/zenworks2017\)](http://www.novell.com/documentation/zenworks2017).

System Configuration

The following sections provide information to help you configure your ZENworks system. The configuration tasks apply regardless of which ZENworks products (Configuration Management, Patch Management, Asset Management, and Endpoint Security Management) you are using.

For more information on the Mobile Management component of ZENworks, see [“Mobile Management” on page 111](#).

- ◆ [Chapter 1, “Quick List,” on page 11](#)
- ◆ [Chapter 2, “Management Tools,” on page 15](#)
- ◆ [Chapter 3, “Management Zone Configuration,” on page 21](#)
- ◆ [Chapter 4, “ZENworks Agent Deployment,” on page 35](#)
- ◆ [Chapter 5, “System Messages,” on page 45](#)
- ◆ [Chapter 6, “Audit Management,” on page 49](#)

1 Quick List




You've installed your ZENworks Server (or maybe a couple of servers) and are eager to start using all of the time-saving functionality in ZENworks.

Before you begin using any of the ZENworks products (Configuration Management, Patch Management, Asset Management, Endpoint Security Management and Full Disk Encryption) that you've licensed or are evaluating, you should review the concepts and tasks in the following sections. These sections are designed to quickly introduce you to what you need to know and do to configure your Management Zone:

- ♦ [“Management Tools” on page 11](#)
- ♦ [“Zone Configuration” on page 11](#)
- ♦ [“Agent Deployment” on page 13](#)
- ♦ [“System Messages” on page 14](#)



Management Tools






ZENworks provides both a Web-based console (ZENworks Control Center) and a command line utility (zman) that you can use to manage your ZENworks system. You should become familiar with at least ZENworks Control Center.

Task	Details
 Launch ZENworks Control Center	For instructions, see “ZENworks Control Center” on page 15 .
 Discover how to run the zman utility	The zman utility is a command line interface that lets you perform many of the same tasks as ZENworks Control Center. For instructions, see “zman Command Line Utility” on page 18 .
 Discover how to run the zac utility	The zac utility is a command line interface for the ZENworks Agent. For instructions, see “zac Command Line Utility” on page 19 .

Zone Configuration





Before you start taking full advantage of the management capabilities provided by the ZENworks products you activated during installation of your Management Zone, there are a few configuration tasks you need to complete to ensure that your Management Zone is configured correctly.

Task	Details
	<p data-bbox="574 247 889 300">Create folders and groups for organizing devices</p> <p data-bbox="932 247 1435 478">Organize devices into folders and groups to ease the overhead involved in applying ZENworks configuration settings and performing tasks on similar devices. Rather than making assignments or performing tasks on individual devices, you can manage the folders and groups, with each device in a folder or group inheriting the assignment or task.</p> <p data-bbox="932 499 1377 554">For instructions, see “Organizing Devices: Folders and Groups” on page 21.</p>
	<p data-bbox="574 583 915 611">Create registration keys or rules</p> <p data-bbox="932 583 1435 695">ZENworks Agent must be deployed on each device that you want to manage. When you deploy the ZENworks Agent to a device, the device is registered in your Management Zone.</p> <p data-bbox="932 716 1435 863">You can use registration keys or rules to automatically assign devices to the appropriate folders and groups, enabling the devices to immediately inherit any assignments associated with the folders and groups.</p> <p data-bbox="932 884 1386 940">For instructions, see “Creating Registration Keys and Rules” on page 24.</p>
	<p data-bbox="574 968 764 995">Add user sources</p> <p data-bbox="932 968 1435 1052">You can connect to one or more LDAP directories to provide authoritative user sources in ZENworks.</p> <p data-bbox="932 1073 1435 1241">Adding a user source lets you associate ZENworks administrator accounts with LDAP user accounts and associate devices with the users who primarily use them. In addition, adding users enables additional functionality for the following ZENworks products:</p> <ul data-bbox="954 1262 1435 1598" style="list-style-type: none"> <li data-bbox="954 1262 1435 1388">◆ Configuration Management: Enables you to assign bundles and policies to users as well as devices. Enables user-based inventory reports. <li data-bbox="954 1398 1435 1482">◆ Asset Management: Enables you to account for software licenses on a user basis as well as a device basis. <li data-bbox="954 1493 1435 1598">◆ Endpoint Security Management: Enables you to assign policies to users as well as devices. <p data-bbox="932 1619 1370 1682">For instructions, see “Connecting to User Sources” on page 26.</p>

Task	Details
	<p data-bbox="574 222 902 275">Create additional administrator accounts</p> <p data-bbox="932 222 1430 359">During installation, a default ZENworks administrator account (named Administrator) is created. This is a Super Administrator account. It has full administrative rights within the Management Zone.</p> <p data-bbox="932 390 1430 558">You can create additional administrator accounts and give them Super Administrator rights. Or, you can create administrator accounts with restricted rights to limit the administrator's scope of accessible tasks, devices, and users.</p> <p data-bbox="932 583 1430 636">For instructions, see "Creating an Administrator Account" on page 27.</p>
	<p data-bbox="574 667 862 720">Create administrator group accounts</p> <p data-bbox="932 667 1430 772">You can choose to create administrator groups. If you assign rights and roles to an administrator group, the assigned rights and roles are applicable to all the members within the group.</p> <p data-bbox="932 804 1430 852">For instructions, see "Creating an Administrator Group Account" on page 28.</p>
	<p data-bbox="574 884 849 936">Modify zone configuration settings</p> <p data-bbox="932 884 1430 1020">The Management Zone settings are preset to provide the most common configuration. You don't need to change any settings at this time, but you might want to browse the settings to become more familiar with them.</p> <p data-bbox="932 1052 1430 1098">For instructions, see "Modifying Configuration Settings" on page 29.</p>
	<p data-bbox="574 1129 870 1150">Update ZENworks Software</p> <p data-bbox="932 1129 1430 1245">The System Updates feature allows you to obtain updates to the ZENworks software on a timely basis, and also allows you to schedule automatic downloads of the updates.</p> <p data-bbox="932 1266 1430 1314">For instructions, see "Updating ZENworks Software" on page 31.</p>
	<p data-bbox="574 1346 756 1367">Create Locations</p> <p data-bbox="932 1346 1430 1514">Security policies can be global or specific to locations. A global policy is applied in all locations. A location-based policy is applied only when the ZENworks Agent determines that the device's network environment matches the environment defined for the location.</p> <p data-bbox="932 1545 1430 1591">For instructions, see "Creating Locations" on page 31.</p>



Agent Deployment

The ZENworks Agent communicates with the ZENworks Server to perform management tasks on a device. You must deploy the ZENworks Agent to all devices you want to manage. Deploying the ZENworks Agent installs the agent files and registers the device in your Management Zone.

Task	Details
 Enable the ZENworks Agent features	<p>The ZENworks Agent includes features specific to each of the ZENworks products (Asset Management, Configuration Management, Endpoint Security Management, Full Disk Encryption, and Patch Management). By default, the features for your activated products (licensed and evaluation) are enabled during Management Zone installation. However, you should verify the configuration in ZENworks Control Center.</p> <p>For instructions, see “Configuring ZENworks Agent Features” on page 35.</p>
 Secure the ZENworks Agent	<p>You can configure the ZENworks Agent uninstall and self-defense settings.</p> <p>For instructions, see “Configuring ZENworks Agent Security” on page 37.</p>
 Install the ZENworks Agent	<p>You can use a variety of methods to install the ZENworks Agent to a device:</p> <ul style="list-style-type: none"> ◆ Use ZENworks Control Center to deploy the agent from a ZENworks Server to the device. ◆ At the device, use a Web browser to download the agent from a ZENworks Server and install it. ◆ Include the agent in an image and apply the image to the device. <p>For instructions, see “Installing the ZENworks Agent” on page 38.</p>
 Log in and use the ZENworks Agent	<p>To receive user-assigned bundles and policies on a device, you must log in to the Management Zone.</p> <p>For instructions, see “Using the ZENworks Agent” on page 41.</p>

System Messages

As you perform management tasks in your zone, information is recorded so that you can view the status of your zone and the activities taking place within it.

Task	Details
 View system messages	<p>The ZENworks system generates informational, warning, and error messages to help you monitor activities such as the distribution of software and application of policies.</p> <p>For instructions, see “Viewing System Messages” on page 45.</p>
 Create a Watch List	<p>If you have devices, bundles, and policies whose activity you want to closely monitor, you can add them to the Watch List.</p> <p>For instructions, see “Creating a Watch List” on page 47.</p>

2 Management Tools

ZENworks provides both a web-based console (ZENworks Control Center) and a command line utility (zman) that you can use to manage your ZENworks system. The following sections explain how to access and use the management tools:

- ♦ “ZENworks Control Center” on page 15
- ♦ “zman Command Line Utility” on page 18
- ♦ “zac Command Line Utility” on page 19

ZENworks Control Center

ZENworks Control Center is installed on all ZENworks Servers in the Management Zone. You can perform all management tasks on any ZENworks Server. Because it is a web-based management console, ZENworks Control Center can be accessed from any supported workstation.

If you use Novell iManager to administer other Micro Focus products in your network environment, you can enable ZENworks Control Center to be launched from iManager. For more information, see “[Accessing ZENworks Control Center through Novell iManager](#)” in the *ZENworks Control Center Reference*.

- ♦ “Accessing ZENworks Control Center” on page 15
- ♦ “Navigating ZENworks Control Center” on page 16

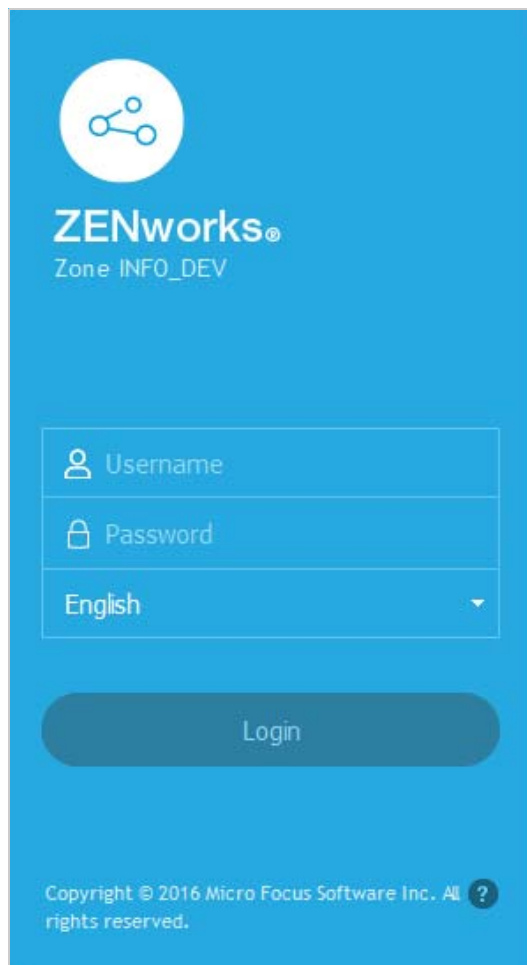
Accessing ZENworks Control Center

- 1 Enter the following URL in a Web browser:

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

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

The login dialog box is displayed.



2 In the **Username** field, type `Administrator`.

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

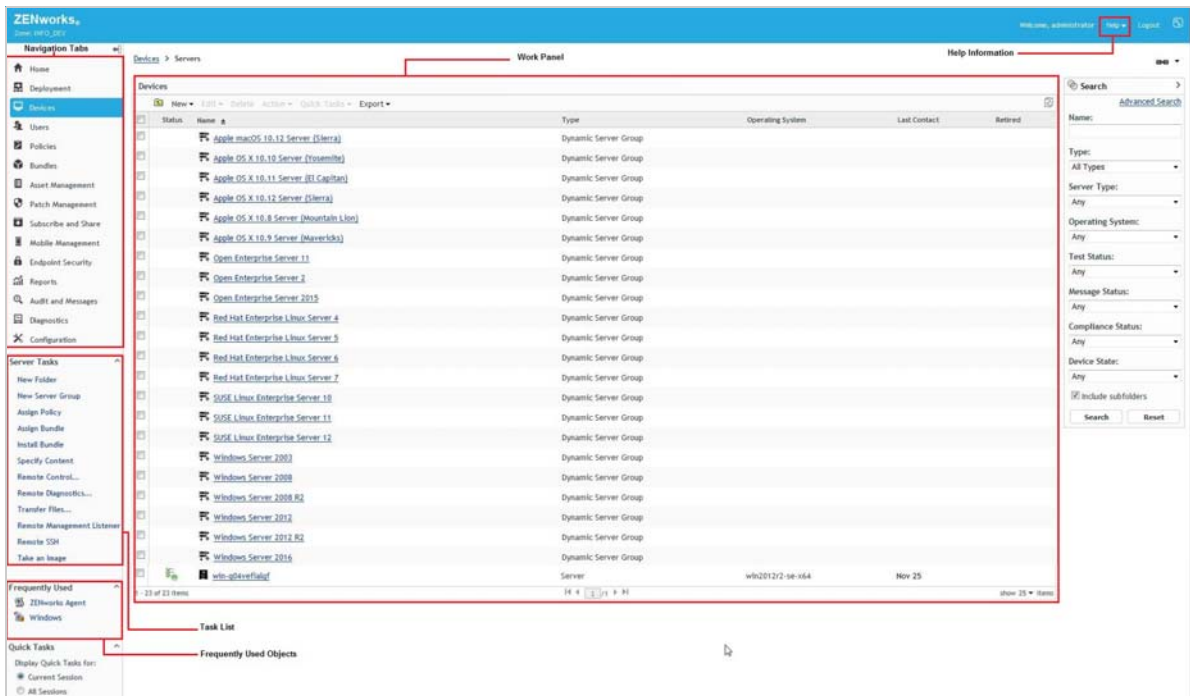
To prevent unauthorized users from gaining access to ZENworks Control Center, the administrator account is disabled after three unsuccessful login attempts, and a 60-second timeout is enforced before you can attempt another login. To change these default values, see “[Changing the Default Login Disable Values](#)” in the *ZENworks Control Center Reference*.

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

For more detailed information on logging in as a different administrator, see “[Accessing ZENworks Control Center](#)” in the *ZENworks Control Center Reference*.

Navigating ZENworks Control Center

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



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

Task List: The task list in the left pane provides quick access to the most commonly performed tasks for the current page. The task list changes for each page. For example, the task list on the Devices page displays device-related tasks and the task list on the Configuration page displays configuration-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: **Devices** and **Search**. The **Devices** panel lists the servers, folders, server groups, and dynamic server groups that have been created; you use this panel to manage servers. The **Search** panel lets you filter the Devices panel based on criteria such as a server's name, operating system, or status.

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

zman Command Line Utility

The zman utility provides a command line management interface that lets you perform many of the tasks available in ZENworks Control Center. For example, you can add content to bundles, assign policies to devices, and register devices. The main advantage to using the command line utility is the ability to create scripts for handling repetitive or mass operations. Like ZCC, the zman utility is installed on all Primary Servers, but it can only run from the command line on the server.

The primary purpose of the zman utility is to enable you to perform operations through a script. However, you can also perform operations manually at a command line.

- ♦ [“Location” on page 18](#)
- ♦ [“Syntax” on page 18](#)
- ♦ [“Help with Commands” on page 18](#)

Location

The utility is installed on all ZENworks Servers in the following location:

```
%ZENWORKS_HOME%\bin
```

where %ZENWORKS_HOME% represents the ZENworks installation path. On Windows, the default path is C:\Program Files (x86)\Novell\Zenworks\bin. On Linux, the default path is /opt/novell/zenworks/bin.

Syntax

The zman utility uses the following basic syntax:

```
zman category-action [options]
```

For example, to assign a software bundle to a device, you use the following command:

```
zman bundle-assign workstation bundle1 wks1
```

where `bundle-assign` is the `category-action` and `workstation bundle1 wks1` are the options. In this example, the options are device type (`workstation`), bundle name (`bundle1`), and target device (`wks1`).

For example, to initiate an inventory scan of a device, you use the following command:

```
zman inventory-scan-now device/servers/server1
```

where `inventory-scan-now` is the `category-action` and `device/servers/server1` is an option that specifies the folder path of the device to be scanned.

Help with Commands

The best way to understand the commands is to use the online help or see [“zman\(1\)”](#) in the [ZENworks Command Line Utilities Reference](#).

To use the online help:

- 1 On the ZENworks Server, enter `zman --help` at a command prompt.

This command displays the basic usage (syntax) and a list of the available command categories. You can also use the following to get help:

Command	Description
<code>zman --help more</code>	Displays a complete list of commands by category.
<code>zman category --help more</code>	Displays a complete list of commands within a category.
<code>zman command --help more</code>	Displays help for a command

zac Command Line Utility

The zac utility provides a command line management interface that lets you perform tasks available in the ZENworks Agent.

- ♦ [“Location” on page 19](#)
- ♦ [“Syntax” on page 19](#)
- ♦ [“Help with Commands” on page 20](#)

Location

The utility is installed on all Windows managed devices in the following location:

```
%ZENWORKS_HOME%\bin
```

where `%ZENWORKS_HOME%` represents the ZENworks installation path. The default path is `c:\program files\novell\zenworks\bin` on a 32-bit Windows device and `c:\program files (x86)\novell\zenworks\bin` on a 64-bit Windows device.

Syntax

The zac utility uses the following basic syntax:

```
zac command options
```

For example, to launch a bundle on a device, you use the following command:

```
zac bundle-launch "bundle 1"
```

where `bundle-launch` is the command and `bundle 1` is the command option. In this example, the option is the display name of the bundle to be launched. Enclosing quotation marks are required only if the bundle display name includes spaces.

For example, to initiate an inventory scan on a device, you use the following command:

```
zac inv scannow
```

where `inv` is the command and `scannow` is the command option.

Help with Commands

The best way to understand the commands is to use the online help or see “[zac for Windows\(1\)](#)” in the [ZENworks Command Line Utilities Reference](#).

To use the online help:

- 1 On the managed device, enter one of the following commands at a command prompt.

Command	Description
<code>zac --help</code>	Displays a complete list of commands.
<code>zac <i>command</i> --help</code>	Displays detailed help for a command.

3 Management Zone Configuration

ZENworks is designed to let you efficiently manage a large number of devices and users with as little effort as possible. The first step in easing this management burden is to ensure that you've configured your Management Zone so that you can take full advantage of the ZENworks capabilities.

The following sections introduce the basic concepts you need to set up a Management Zone that best supports the ongoing management tasks you perform. Each section explains a management concept and provides general steps to perform the tasks associated with the concept.

- ◆ [“Organizing Devices: Folders and Groups” on page 21](#)
- ◆ [“Creating Registration Keys and Rules” on page 24](#)
- ◆ [“Connecting to User Sources” on page 26](#)
- ◆ [“Creating ZENworks Administrator Accounts” on page 27](#)
- ◆ [“Modifying Configuration Settings” on page 29](#)
- ◆ [“Zone Sharing and Subscription” on page 30](#)
- ◆ [“Updating ZENworks Software” on page 31](#)
- ◆ [“Creating Locations” on page 31](#)

Organizing Devices: Folders and Groups

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

You can create folders and groups at any time. However, the best practice is to create folders and groups before you register devices in your zone. This allows you to use registration keys and rules to automatically add devices to the appropriate folders and groups when they register (see [“Creating Registration Keys and Rules” on page 24](#)).

- ◆ [“Folders” on page 21](#)
- ◆ [“Groups” on page 22](#)
- ◆ [“Assignment Inheritance for Folders and Groups” on page 24](#)

Folders

Folders are a great tool to help you organize devices in order to simplify management of those devices. You can apply configuration settings, assign content, and perform tasks on any folder. When you do so, the folder's devices inherit those settings, assignments, and tasks.

For best results, you should place devices with similar configuration setting requirements in the same folder. If all devices in the folder require the same content or tasks, you can also make content or task assignments on the folder. However, all devices in the folder might not have the same content and task requirements. Therefore, you can organize the devices into groups and assign the appropriate content and tasks to each groups (see [“Groups” on page 22](#) below).

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

Creating a Folder

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

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

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

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

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

Groups

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

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

For example, let’s revisit the example of the workstations at three different sites (see [“Folders” on page 21](#)). Assume that some of the workstations at each site need the same accounting software. Because groups can be assigned software, you could create an Accounting group, add the target workstations to the group, and then assign the appropriate accounting software to the group. Likewise, you could use the groups to assign Windows configuration and security policies.

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

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

ZENworks include several predefined dynamic server groups for example, Windows 2012 Servers, Windows 2003 Servers and SUSE Linux Enterprise Server.

ZENworks also includes dynamic workstation groups for example, Windows XP Workstation, Windows 8 Workstation, Windows Vista Workstations and SUSE Linux Enterprise Desktop. Devices that have these operating systems are automatically added to the appropriate dynamic group.

Creating a Group

- 1 In ZENworks Control Center, click the **Devices** tab.
- 2 If you want to create a group for servers, click the **Servers** folder.
or
If you want to create a group for workstations, click the **Workstations** folder.
or
If you want to create a group for mobile devices, click the **Mobile Devices** folder.
- 3 Click **New > Server Group** (**New > Workstation Group** for workstations or **New > Mobile Device Group** for mobile devices.) to launch the Create New Group Wizard.
- 4 On the Basic Information page, type a name for the new group in the **Group Name** field, then click **Next**.
The group name must follow the [naming conventions](#).
- 5 On the Summary page, click **Finish** to create the group without adding members.
or
Click **Next** if you want to add members to the group, then continue with [Step 6](#).
- 6 On the Add Group Members page, click **Add** to add devices to the group, then click **Next** when finished adding devices.
- 7 On the Summary page, click **Finish** to create the group.

You can also use the `workstation-group-create` and `server-group-create` commands in the `zman` utility to create device groups. For more information, see “[Workstation Commands](#)” and “[Server Commands](#)” in the [ZENworks Command Line Utilities Reference](#).

Creating a Dynamic Group

- 1 In ZENworks Control Center, click the **Devices** tab.
- 2 If you want to create a group for servers, click the **Servers** folder.
or
If you want to create a group for workstations, click the **Workstations** folder.
or
If you want to create a group for mobile devices, click the **Mobile Device** folder.

- 3 Click **New > Dynamic Server Group** (**New > Dynamic Workstation Group** for workstations or **New > Dynamic Mobile Device Group** for mobile devices) to launch the Create New Group Wizard.
- 4 On the Basic Information page, type a name for the new group in the **Group Name** field, then click **Next**.
The group name must follow the [naming conventions](#).
- 5 On the Define Filter for Group Members page, define the criteria that a device must meet to become a member of the group, then click **Next**.
Click the **Help** button for details about creating the criteria.
- 6 On the Summary page, click **Finish** to create the group.

Assignment Inheritance for Folders and Groups

When you assign content to a folder, all objects (users, devices, subfolders) except groups that are located in the folder inherit the assignment. For example, if you assign BundleA and PolicyB to DeviceFolder1, all devices within the folder (including all devices in subfolders) inherit the two assignments. However, none of the device groups located in DeviceFolder1 inherit the assignments. Essentially, folder assignments do not flow down to groups located within the folder.

Creating Registration Keys and Rules

When you deploy the ZENworks Agent to a device, the device is registered in your Management Zone and becomes a managed device. As part of the registration, you can specify the device's ZENworks name and the folder and groups to which you want the device added.

By default, a device's hostname is used as its ZENworks name, it is added to the `/Servers` or `/Workstations` folder, and it is not given membership in any groups. You can manually move devices to other folders and add them to groups, but this can be a burdensome task if you have a large number of devices or if you are consistently adding new devices. The best way to manage a large number of devices is to have them automatically added to the correct folders and groups during registration.

To add devices to folders and groups during registration, you can use registration keys, registration rules, or both. Both registration keys and registration rules let you assign folder and group memberships to a device. However, there are differences between keys and rules that you should be aware of before choosing whether you want to use one or both methods for registration.

This feature is not applicable for Mobile Devices.

- ◆ [“Registration Keys” on page 25](#)
- ◆ [“Registration Rules” on page 25](#)
- ◆ [“Device Naming Template” on page 26](#)
- ◆ [“Where to Find More Information” on page 26](#)

Registration Keys

A registration key is an alphanumeric string that you manually define or randomly generate. During deployment of the ZENworks Agent on a device, the registration key must be provided. When the device connects to a ZENworks Server for the first time, the device is added to the folder and groups defined within the key.

You can create one or more registration keys to ensure that devices are placed in the desired folders and groups. For example, you might want to ensure that all of the Sales department's workstations are added to the `/Workstations/Sales` folder but are divided into three different groups (SalesTeam1, SalesTeam2, SalesTeam3) depending on their team assignments. You could create three different registration keys and configure each one to add the Sales workstations to the `/Workstations/Sales` folder and the appropriate team group. As long as each workstation uses the correct registration key, it is added to the appropriate folder and group.

To create a registration key:

- 1 In ZENworks Control Center, click the **Configuration** tab, then click the **Registration** tab.
- 2 In the Registration Keys panel, click **New** > **Registration Key** to launch the Create New Registration Key Wizard.
- 3 Follow the prompts to create the key.

For information about what you need to supply at each step of the wizard, click the **Help** button.

You can also use the `registration-create-key` command in the `zman` utility to create a registration key. For more information, see “[Registration Commands](#)” in the *ZENworks Command Line Utilities Reference*.

Registration Rules

If you don't want to enter a registration key during deployment, or if you want devices to be automatically added to different folders and groups based on predefined criteria (for example, operating system type, CPU, or IP address), you can use registration rules.

ZENworks includes a default registration rule for servers and another one for workstations. If a device registers without a key and you haven't created registration rules, the default registration rules are applied to determine the folder assignments. The two default rules cause all servers to be added to the `/Servers` folder and all workstations to the `/Workstations` folder.

The two default rules are designed to ensure that no server or workstation registration fails. Therefore, you cannot delete or modify these two default rules. You can, however, define additional rules that enable you to filter devices as they register and add them to different folders and groups. If, as recommended in “[Organizing Devices: Folders and Groups](#)” on page 21, you've established folders for devices with similar configuration settings and groups for devices with similar assignments, then newly registered devices automatically receive the appropriate configuration settings and assignments.

To create a registration rule:


- 1 In ZENworks Control Center, click the **Configuration** tab, then click the **Registration** tab.
- 2 In the Registration Rules panel, click **New** to launch the Create New Registration Rule Wizard.
- 3 Follow the prompts to create the rule.

For information about what you need to supply at each step of the wizard, click the **Help** button.

You can also use the `ruleset-create` command in the `zman` utility to create a registration rule. For more information, see “[Ruleset Commands](#)” in the *ZENworks Command Line Utilities Reference*.

Device Naming Template

The device naming template determines how devices are named when they register. By default, a device's hostname is used. You can change it to use any combination of the following machine variables: `${HostName}`, `${GUID}`, `${OS}`, `${CPU}`, `${DNS}`, `${IPAddress}` and `${MACAddress}`.

- 1 In ZENworks Control Center, click the **Configuration** tab.
- 2 In the Management Zone Settings panel, click **Device Management**.
- 3 Click **Registration** to display the Registration page.
- 4 In the Device Naming Template panel, click , then select the desired machine variable from the list.

You can use any combination of one or more variables. For example:

```
${HostName}${GUID}
```

- 5 Click **OK** to save the changes.

Where to Find More Information

For more information about registering devices, see the [ZENworks Discovery, Deployment, and Retirement Reference](#).

Connecting to User Sources

You can connect to one or more LDAP directories to provide authoritative user sources in ZENworks.

Adding a user source lets you associate ZENworks administrator accounts with LDAP user accounts and associate devices with the users who primarily use them. In addition, adding users enables additional functionality for the following ZENworks products:

- ♦ **Configuration Management:** Enables you to assign bundles and policies to users as well as devices. Enables user-based inventory reports.
- ♦ **Asset Management:** Enables you to account for software licenses on a user basis as well as a device basis.
- ♦ **Endpoint Security Management:** Enables you to assign policies to users as well as devices.

When you define an LDAP directory as a user source, the directory is not affected; ZENworks requires only read access to the LDAP directory and stores all assignment information in the ZENworks database. For more detailed information about the specific read rights required when connecting to a user source, see “[Creating User Source Connections](#)” in the [ZENworks User Source and Authentication Reference](#).

You can connect to Novell eDirectory and Microsoft Active Directory as user sources. The minimum requirements are Novell eDirectory 8.7.3 and Microsoft Active Directory on Windows 2000 SP4. The minimum LDAP requirement is version 3.

After you connect to an LDAP directory, you define the containers within the directory that you want exposed. For example, assume you have a Microsoft Active Directory domain tree named MyCompany. All users reside in two containers in the MyCompany tree: MyCompany/Users and MyCompany/Temp/Users. You could reference the MyCompany tree as the source and the MyCompany/Users and MyCompany/Temp/Users as separate user containers. This limits access within the directory to only those containers that include users.

In addition to the users that reside within the containers you add, ZENworks Control Center also displays any user groups located in the containers. This enables management of both individual user and groups of users

To connect to 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 user source.

For information about what you need to supply at each step of the wizard, click the **Help** button.

You can also use the `user-source-create` command in the `zman` utility to create a connection to a user source. For more information, see “[User Commands](#)” in the [ZENworks Command Line Utilities Reference](#).

For more information on enabling user sources for mobile device enrollment, see [Configuring User Sources](#) in [ZENworks 2017 Mobile Management Reference](#).

Creating ZENworks Administrator Accounts

During installation, a default ZENworks administrator account (named Administrator) is created. This account, called a Super Administrator account, provides full administrative rights to the Management Zone.

Typically, you should create administrator accounts for each person who will perform administrative tasks. You can define these accounts as super administrator accounts, or you can define them as administrator accounts with restricted rights. For example, you could give a user an administrator account that only enables the user to discover and register devices in the Management Zone. Or the account could only enable the user to assign bundles to devices. Or, the account might be limited to performing asset management tasks such as contract, license, and document management.

In some cases, you might have multiple administrator accounts that require the same administrative rights. Rather than assign rights to each account individually, you can create an administrator role, assign the administrative rights to the role, and then add the accounts to the role. For example, you might have a Help Desk role that provides administrative rights required by several of your administrators.

You can choose to create administrator groups. If you assign rights and roles to an administrator group, the assigned rights and roles are applicable to all the members within the group.

Creating an Administrator Account

- 1 In ZENworks Control Center, click the **Administrators** tab.
- 2 In the Administrators panel, click **New** > Administrator to display the Add New Administrator dialog box.
- 3 Fill in the fields.

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.

Create a new Administrator by providing name, password: Select this option if you want to create a new administrator account by manually specifying a name and password.

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

Give this Administrator the same rights as I have: Select this option to assign the new administrator the same rights that you have as the currently logged-in administrator. If you have Super Administrator rights, the new administrator is created as a Super Administrator.

- 4 Click **OK** to add the new administrator to the Administrators panel.
- 5 If you need to change the new administrator's rights or roles, click the administrator account and then the **Rights** tab to display the account details.
- 6 If the **Super Administrator** option is selected, deselect the option.
You cannot modify Super Administrator rights.
- 7 Using the Assigned Rights panel, modify the assigned rights.
- 8 Using the Assigned Roles panel, modify the assigned roles.
- 9 Click **Apply** to save the changes.

For more information about creating ZENworks administrator accounts, administrator rights, or administrator roles, see [ZENworks Administrator Accounts and Rights Reference](#).

You can also use the `admin-create` command in the `zman` utility to create a ZENworks administrator account. For more information, see "Administrator Commands" in the [ZENworks Command Line Utilities Reference](#).

Creating an Administrator Group Account

- 1 In ZENworks Control Center, click the **Administrators** tab.
- 2 In the Administrators panel, click **New > Administrator Group** to display the Add a New Administrator Group dialog box.
- 3 Fill in the fields.

The Add New Administrator Group dialog box lets you create a new administrator group account by providing a group name and adding members to the group, or you can create a new administrator group based on an existing user group in the user source. Each administrator group name must be unique.

Create a new Administrator Group by providing a name and adding members: Select this option if you want to create a new administrator group account by manually specifying the name and adding the members. To add members, click **Add**, then browse for, and select the required administrators.

You can add any number of administrators to the group. You cannot add other administrator groups to the group.

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

Import user members of each user group as administrators immediately: Select this option to enable the user members of the selected user groups to be immediately added as administrators.

- 4 Click **OK** to add the new administrator group to the Administrators panel.
- 5 If you need to change the new administrator group's rights or roles, click the administrator group account and then the **Rights** tab to display the account details.
- 6 Using the Assigned Rights panel, modify the assigned rights.

- 7 Using the Assigned Roles panel, modify the assigned roles.
- 8 Click **Apply** to save the changes.

For more information about creating ZENworks administrator group accounts, administrator rights, or administrator roles, see the [ZENworks Administrator Accounts and Rights Reference](#).

You can also use the `admin-create` command in the `zman` utility to create a ZENworks administrator account. For more information, see “Administrator Commands” in the [ZENworks Command Line Utilities Reference](#).

Modifying Configuration Settings

The Management Zone configuration settings enable you to control a wide range of functionality behavior for your zone. There are Device Management settings that let you control how often devices access a ZENworks Server for refreshed information, how often dynamic groups are refreshed, and what levels of messages (informational, warning, or error) are logged by the ZENworks Agent. There are Event and Messaging settings, Discovery and Deployment settings, and much more.

Management Zone settings that apply to devices are inherited by all devices in the zone. As mentioned in “[Organizing Devices: Folders and Groups](#)” on page 21, you can override zone settings by configuring them on device folders or on individual devices. This allows you to establish zone settings that apply to the largest number of devices, and then override the settings on folders and devices, as required.

By default, your zone settings are pre-configured with values that provide a common functionality. You can however, change the settings to best adapt them to the behavior you need in your environment.

- ♦ “[Modifying Configuration Settings at the Zone](#)” on page 29
- ♦ “[Modifying Configuration Settings on a Folder](#)” on page 29
- ♦ “[Modifying Configuration Settings on a Device](#)” on page 30

Modifying Configuration Settings at the Zone

- 1 In ZENworks Control Center, click the **Configuration** tab.
- 2 In the Management Zone Settings panel, click the settings category (for example, **Device Management**, **Discovery and Deployment**, and **Event and Messaging**) whose settings you want to modify.
- 3 Click the setting to display its details page.
- 4 Modify the setting as required.
For information about the setting, see the [ZENworks Management Zone Settings Reference](#).
- 5 Click **OK** or **Apply**.

If the configuration setting applies to devices, the setting is inherited by all devices in the zone, unless the setting is overridden at a folder level or a device level.

Modifying Configuration Settings on a Folder

- 1 In ZENworks Control Center, click the **Devices** tab.
- 2 In the Devices panel (on the **Managed** tab), browse for the folder whose settings you want to modify.

- 3 Click **Details** next to the folder name to display the details.
- 4 Click the **Settings** tab.
- 5 In the Settings panel, click the settings category (**Device Management, Infrastructure Management**, and so forth) of the settings that you want to modify.
- 6 Click the setting to display the details page.
- 7 Modify the setting as required.

For information about the setting, see the [ZENworks Management Zone Settings Reference](#).

- 8 Click **OK** or **Apply**.

The configuration setting is inherited by all devices in the folder, including any devices contained in subfolders, unless the setting is overridden on a subfolder or individual device.

Modifying Configuration Settings on a Device

- 1 In ZENworks Control Center, click the **Devices** tab.
- 2 In the Devices panel (on the **Managed** tab), browse for the device whose settings you want to modify.
- 3 When you've found the device, click the device name to display its details.
- 4 Click the **Settings** tab.
- 5 In the Settings panel, click the settings category (**Device Management, Infrastructure Management**, and so forth) whose settings you want to modify.
- 6 Click the setting to display its details page.
- 7 Modify the setting as desired.

For information about the setting, click the **Help** button in ZENworks Control Center.

- 8 When you have finished modifying the setting, click **OK** (or **Apply**) to save your changes.

Zone Sharing and Subscription

The Subscribe and Share feature in ZENworks allows you to share content objects (for example, bundles and policies) that can be assigned across multiple ZENworks zones:

- ♦ **Sharing Zone:** Shares content.
- ♦ **Subscriber Zone:** Subscribes to the sharing zone, and replicates the shared content in its own zone.

In the ZENworks Control Center, you can use the Zone Sharing settings link in the Infrastructure Management panel to manage the sharing activities of the zone.

In the Sharing zone, a Primary Server is identified as a Sharing server. All content sharing activities are done through this server. The Subscriber zone registration is done by providing a subscriber key from the sharing zone. Subscriber key does not entitle a subscriber for any content. The Subscriber key is for Subscriber registration.

The required content is then shared from the Sharing zone and is replicated in the Subscriber zone. You will be notified if there are any replication issues; you can take the corrective actions.

For more details, see [ZENworks Subscribe and Share Reference](#).

Updating ZENworks Software

The ZENworks software can be updated on all devices in the Management Zone, in which the software is installed. Update downloads can be scheduled. Software updates are provided at the Support Pack release level. You can choose whether to apply each update after viewing its content (Support Pack releases are cumulative). You can also download the latest Product Recognition Update (PRU) to update your knowledge base, so that ZENworks Inventory can recognize newer software.

For more information, see the [ZENworks System Updates Reference](#).

Creating Locations

Security requirements for a device might differ from location to location. For example, you might have different personal firewall restrictions for a device located in an airport terminal than for a device located in an office inside your corporate firewall.

To ensure that a device's security requirements are appropriate for the location that it is in, ZENworks supports both global policies and location-based policies. A global policy is applied regardless of the device's location. A location-based policy is applied only when the device's current location meets the criteria for a location associated with the policy. For example, if you create a location-based policy for your corporate office and assign it to a laptop, the policy is applied only when the laptop's location is the corporate office.

If you want to use location-based policies, you must first define the locations that suit your organization. A location is a place, or type of place, for which you have specific security requirements. For example, you might have different security requirements when a device is used in the office, at home, or in an airport.

Locations are defined by network environments. Assume that you have an office in New York and an office in Tokyo. Both offices have the same security requirements. Therefore, you create an Office location and associate it with two network environments: New York Office Network and Tokyo Office Network. Each of these environments is explicitly defined by a set of gateway, DNS server, and wireless access point services. Whenever the ZENworks Agent determines that its current environment matches the New York Office Network or Tokyo Office Network, the agent sets its location to Office and applies the security policies associated with the Office location.

The following sections explain how to create locations:

- ♦ [“Defining a Network Environment” on page 31](#)
- ♦ [“Creating Locations” on page 32](#)
- ♦ [“Location and Network Environment Selection on a Managed Device” on page 33](#)

Defining a Network Environment

Network environment definitions are the building blocks for locations. Network environments can be defined while creating a location. However, it is recommended that you define network environments first, and then add them while creating locations.

To create a network environment:

- 1 In ZENworks Control Center, click **Configuration > Locations**.
- 2 In the Network Environments panel, click **New** to launch the Create New Network Environment wizard.

3 On the Define Details page, specify a name for the network environment, then click **Next**.

4 On the Network Environment Details page, specify the following:

Limit to Adapter Type: By default, the network services you define on this page are evaluated against a device's wired, wireless, and dial-up network adapters. If you want to limit the evaluation to a specific adapter type, select **Wired**, **Wireless**, or **Dial Up**.

Minimum Match: Specify the minimum number of defined network services that should match in order to select this network environment.

Specify the minimum number of defined network services that should match, in order to select this network environment.

For example, if you define one gateway address, three DNS servers, and one DHCP server, you have a total of five services. You can specify that at least three of those services must match in order to select this network environment.

When specifying a minimum match number, ensure the following:

- ◆ The number cannot be less than the number of services marked as Match Required.
- ◆ The number should not exceed the total number of defined services. If it exceeds, the minimum match will never be reached, and the network environment will never be selected.

Network Services: Enables you to define the network services that the ZENworks Agent evaluates to see if its current network environment matches this network environment. Select the tab for the network service that you want to define. Click **Add**, then specify the required information.

5 Click **Next** to display the Summary page, then click **Finish**.

Creating Locations

When you create a location, you provide a location name and then associate the required network environments with the location.

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

2 In the Locations panel, click **New** to launch the Create New Location wizard.

3 On the Define Details page, specify a name for the location, then click **Next**.

4 On the Assign Network Environments page:

4a Select **Assign existing Network Environments to the Location**.

4b Click **Add**, select the network environments for which you want to define the location, then click **OK** to add them to the list.

4c Click **Next** when you are finished adding network environments.

5 On the summary page, click **Finish** to create the location and add it to the Locations list.

When multiple locations include the network environment identified by the ZENworks Agent, the order of the list determines which location is used. The location listed first is selected, by default. To reorder the list, use the **Move Up** and **Move Down** options.

You can also use the `network-environment-create` and `location-create` commands in the `zman` utility to create a network environment and the related location using the created network environment. For more information, see "Registration Commands" in the [ZENworks Command Line Utilities Reference](#).

Location and Network Environment Selection on a Managed Device

If you have multiple locations and network environments defined in ZENworks Control Center, the ZENworks Agent on the managed device scans all the defined network environments to identify matched environments. From the identified environments, the ZENworks Agent selects the network environments that have the highest number of matched network services (such as Client IP Address and DNS Servers). The ZENworks Agent then scans the ordered list of locations, identifies the first location that contains any of the selected network environments, and selects the location and the first matched network environment contained within this location.

For example:

- ◆ The locations defined in ZENworks Control Center are listed in the following order: L1 and L2.
- ◆ The network environments within L1 are listed in the following order: NE1, NE2, and NE4.
- ◆ The network environments within L2 are listed in the following order: NE2, NE3, and NE4.
- ◆ The ZENworks Agent on the managed device detects that NE2, NE3 and NE4 all match on the managed device.

If NE2 and NE4 each have two network service matches each, and NE3 has just one network service match, the ZENworks Agent selects NE2 and NE4 because they have the most network service matches. Because NE2 is the first listed network environment in L1, L1 and NE2 are selected as the location and network environment.

NOTE: For a network environment to be considered matched on the managed device, it must meet all the restrictions set in the network environment. These include the **Minimum Match** attribute specified for the network environment, and also the **Match Required** attribute specified for the network services, within the network environment.

4 ZENworks Agent Deployment

The ZENworks Agent must be deployed to the devices that you want to manage. The following sections provide instructions to help you understand the process of deploying the agent:

- ♦ “Configuring ZENworks Agent Features” on page 35
- ♦ “Configuring ZENworks Agent Security” on page 37
- ♦ “Installing the ZENworks Agent” on page 38
- ♦ “Using the ZENworks Agent” on page 41

NOTE: If a device does not meet the requirements for installing the ZENworks Agent (see “[Managed Device Requirements](#)” in the *ZENworks 2017 Update 1 System Requirements*), you might be able to install the Inventory Only Module on it to support inventorying of the device. For more information, see the *ZENworks Discovery, Deployment, and Retirement Reference*.

Configuring ZENworks Agent Features

The ZENworks Agent utilizes various modules to perform functions on a device. These modules are referred to as the ZENworks Agent features. Each ZENworks product has specific features associated with it, as shown in the following table. The ZENworks products are listed in the left column; the other columns represent the ZENworks Agent features.

	Asset Management	Bundle Management	Endpoint Security	Full Disk Encryption	Image Management	Patch Management	Policy Management	Remote Management	User Management
ZENworks Asset Management	✓								✓
ZENworks Configuration Management		✓			✓		✓	✓	✓
ZENworks Endpoint Security Management			✓						✓
ZENworks Full Disk Encryption				✓					
ZENworks Patch Management						✓			

By default, when you activate a ZENworks product, all of its ZENworks Agent features are installed and enabled. The one exception is ZENworks Asset Management, which does not automatically enable the User Management feature.

The User Management feature is only supported on Windows managed devices across all the ZENworks products.

If you do not want a feature installed or enabled on a device, you can uninstall it or disable it at the Management Zone, device folder, or individual device.

For example, if you are using ZENworks Configuration Management and do not want to use Remote Management with any devices, you can disable it at the Management Zone. Or, if you have ZENworks Configuration Management and ZENworks Asset Management, but do not want to use Asset Management on all devices, you can enable the Asset Management feature at the Management Zone and then disable (or uninstall) it on device folders or individual devices.

To customize the ZENworks Agent features, either before or after the agent is deployed, see the following sections:

- ◆ [“Customizing the ZENworks Agent Features” on page 36](#)
- ◆ [“Coexisting with the ZENworks Desktop Management Agent” on page 36](#)

Customizing the ZENworks Agent Features

During initial deployment, the ZENworks Agent installs and enables the features selected at the Management Zone level. After the agent registers, it then uses the settings defined at the device folder or device level (if they are different than the zone settings).

NOTE: Customizing ZENworks Agent features is not applicable to Macintosh devices.

The following steps explain how to customize settings at the Management Zone level. For information about customizing settings on a device folder or individual device, see [“Customizing the Agent Features”](#) in the *ZENworks Discovery, Deployment, and Retirement Reference*.

- 1 In ZENworks Control Center, click the **Configuration** tab.
- 2 In the Management Zone Settings panel, click **Device Management > ZENworks Agent**.
- 3 In the Agent Features panel:
 - ◆ If you do not want to install a feature, deselect **Installed** next to a feature. The selected feature is not installed on the device. If you choose to deselect all the features, then only the core agent is installed.
 - ◆ If you want to install but disable a feature, select **Installed** and **Disabled** next to a feature. The feature is installed on the device, but it is nonfunctional.

The installation of Bundle Management, Remote Management, or User Management features requires a reboot of the device. The installation of Image Management feature requires a reboot only on Windows 2008 and Windows Vista. You are prompted to reboot the device based on the selected reboot option.

- 4 To save the changes, click **OK**.

Coexisting with the ZENworks Desktop Management Agent

You can deploy the ZENworks Agent to devices that have the ZENworks Desktop Agent installed.

The ZENworks Agent and the ZENworks Desktop Agent can coexist on the same device to support the use of ZENworks Asset Management with ZENworks Desktop Management. In this case, when you deploy the ZENworks Agent to a device that has the ZENworks Desktop Agent installed, you should only use the ZENworks Agent features that are not associated with ZENworks Configuration Management; do not use the Bundle Management, Image Management, Policy Management, Remote Management, or User Management features. If you select any of these features, the ZENworks Desktop Agent is uninstalled before the ZENworks Agent is installed.

For more information on the coexistence of the ZENworks Agent and ZENworks Desktop Agent, see “ZENworks Agent Deployment” in the *ZENworks Discovery, Deployment, and Retirement Reference*.

Configuring ZENworks Agent Security

To secure the ZENworks Agent on devices, you can configure both uninstall and self-defense settings for the agent.

- 1 In ZENworks Control Center, click the **Configuration** tab.
- 2 In the Management Zone Settings panel, click **Device Management**, then click **ZENworks Agent**.
- 3 In the Agent Security panel, configure the following settings:

- ◆ **Allow Users to Uninstall the ZENworks Agent:** Select this option to uninstall the ZENworks Agent.
- ◆ **Require an Uninstall Password for the ZENworks Agent:** Select this option to specify a password that is required to uninstall the ZENworks Agent. Click **Change** to set the password.

To avoid distributing the uninstall password to users, we recommend that you use the Password Key Generator utility to generate a password key. The key, which is based on the uninstall password, functions the same as the uninstall password but can be tied to a single device or user, so that its use is limited.

The Password Key Generator utility is accessible under the Configuration Tasks list in the left navigation pane.

- ◆ **Enable an Override Password for the ZENworks Agent:** Select this option to specify an override password that can be used in the ZENworks Agent to:
 - ◆ Access information about the device's current location and how the location was assigned.
 - ◆ Access the Administrative options in the Endpoint Security Agent. These options let you disable the currently applied security policies (with the exception of the Data Encryption policy), view detailed policy information, and view agent status information.
 - ◆ Access the Administrative options in the Full Disk Encryption Agent. These options let you view detailed policy information, view agent status information, and perform functions such as enabling user capturing and decrypting volumes.
 - ◆ Uninstall the ZENworks Agent.

- ◆ **Enable Self Defense for the ZENworks Agent:** Select this option to enable self defense. Currently, the self-defense functionality protects only the ZENworks Endpoint Security Agent. It does not protect the other ZENworks Agent modules.

Self defense protects the Endpoint Security Agent from being shut down, disabled, or tampered with, in any way. If a user performs any of the following activities, the device is automatically rebooted to restore the correct system configuration:

- ◆ Using Windows Task Manager to terminate any Endpoint Security Agent process.
- ◆ Stopping or pausing any Endpoint Security Agent service.
- ◆ Removing critical files and registry entries. If a change is made to any registry key or value associated with the Endpoint Security Agent, the registry key or value is immediately reset.
- ◆ Disabling the NDIS filter driver binding to adapters.

- 4 To save the changes, click **OK**.

Installing the ZENworks Agent

The following sections provide instructions for manually installing the ZENworks Agent on devices.

- ◆ [“Manual Installation on Windows” on page 38](#)
- ◆ [“Manual Installation on Linux” on page 39](#)
- ◆ [“Manual Installation on Macintosh” on page 40](#)

NOTE: In addition to manually installing the ZENworks Agent, you can automate installation by using network device discovery and deployment. The discovery and deployment process is beyond the scope of this Quick Start. To learn how to use this process, see the [ZENworks Discovery, Deployment, and Retirement Reference](#).

Manual Installation on Windows

- 1 Ensure that the device meets the necessary requirements (see [“Managed Device Requirements”](#) in the [ZENworks 2017 Update 1 System Requirements](#)).
- 2 On the target device, open a web browser and navigate to the following address:

`https://server:port/zenworks-setup`

Replace *server* with the DNS name or IP address of a ZENworks server and replace the *port* only if the ZENworks server is not using the default port (80 or 443).

The web browser displays a list of deployment packages for the ZENworks Agent. For each architecture (32-bit and 64-bit), these are the following types of packages:

- ◆ **Network (.NET required):** The network (.NET required) package installs only the pre-agent on the target device; the pre-agent then downloads and installs the ZENworks Agent from the ZENworks Server. The network (.NET required) package requires that Microsoft .NET 4.0 or later is installed on the device prior to the deployment of the agent to the device.
 - ◆ **Standalone (.NET required):** The standalone (.NET required) package requires that Microsoft .NET 4.0 or later is installed on the device prior to the deployment of the agent to the device. This package contains all the executable files required for ZENworks Agent installation except the Microsoft .NET installer.
 - ◆ **Standalone:** The standalone package installs the pre-agent and extracts all executable files required for ZENworks Agent installation, including Microsoft .NET installer on the target device. The pre-agent then installs the ZENworks Agent from the local device. The standalone package is useful when you need to install the ZENworks Agent to a device that is currently disconnected from the network. You can save the package to removable media (CD, USB flash drive, and so on) and have the standalone device run the package from the media. The ZENworks Agent is installed on the device, but no registration or management occurs until the device connects to the network.
 - ◆ **Custom:** The package name, Default Agent, refers to the predefined deployment packages. The custom deployment packages created through [Deployment > Edit Deployment Package](#) are shown with the name given during the creation of the package.
- 3 Click the name of the deployment package that you want to use and save the package to the device’s local drive, or run it from the ZENworks Server.
 - 4 If you downloaded the package, launch the package on the device.

For information about options that you can use with the package, when launching it from a command line, see [“Package Options for Windows, Linux, and Macintosh”](#) in [ZENworks Discovery, Deployment, and Retirement Reference](#).

IMPORTANT: If you choose to install a complete package, the installation of Windows Installer or .NET Framework might require a reboot after you launch the package. A message is displayed showing various options on rebooting. Select one of the following options:

- ◆ Do nothing, and auto-reboot occurs after 5 minutes.
- ◆ Click **Cancel**. You need to reboot later.
- ◆ Click **OK** to reboot immediately.

When the device reboots, the installation automatically resumes.

- 5 After the completion of the installation, the device reboots automatically if you have rebooted the device while installing Windows Installer or .NET Framework.

When the device reboots, it is registered in the Management Zone and the ZENworks icon is placed in the notification area (system tray).

In ZENworks Control Center, the device appears in the `\Servers` folder or `\Workstation` folder on the Devices page.

For information about logging in and using the ZENworks Agent on a device, see [“Using the ZENworks Agent” on page 41](#).

Manual Installation on Linux

Instead of having a ZENworks Server deliver the ZENworks Agent to a device, you can manually download the ZENworks Agent deployment package from the server and install the agent.

IMPORTANT: You can install the ZENworks Agent on Linux if you have root or administrator permissions.

- 1 Make sure the device meets the necessary requirements (see [“Managed Device Requirements”](#) in the *ZENworks 2017 Update 1 System Requirements*).
- 2 On the target device, open a Web browser and navigate to the following address:

```
http://server:port/zenworks-setup
```

Replace *server* with the DNS name or IP address of a ZENworks Server and replace the *port* only if the ZENworks Server is not using the default port (80 or 443).

The web browser displays a list of deployment packages. For each architecture (32-bit and 64-bit), these are the following types of packages:

- ◆ **Network:** This package installs only the pre-agent on the target device; the pre-agent then downloads and installs the ZENworks Agent from the ZENworks Server.
- ◆ **Standalone:** The standalone package installs the pre-agent and extracts all executable files required for ZENworks Agent installation, including the JRE installer on the target device. The pre-agent then installs the ZENworks Agent from the local device. The standalone package is useful when you need to install the ZENworks Agent on a device that is currently disconnected from the network. You can save the package to removable media (for example, CD, or USB flash drive) and have the standalone device run the package from the media. The ZENworks Agent is installed on the device, but no registration or management occurs until the device connects to the network.
- ◆ **Custom:** The package name, Default Agent, refers to the predefined deployment packages. The custom deployment packages that are created through **Deployment > Edit Deployment Package** are shown with the name given during the creation of the package.

- 3 Click the name of the deployment package that you want to use, save the package to the device's local drive, then give executable permissions to the file by running the command `chmod 755 filename`.

For information about options that you can use with the package, when launching it from a command line, see “[Package Options for Windows, Linux, and Macintosh](#)” in [ZENworks Discovery, Deployment, and Retirement Reference](#).

- 4 (Optional) On a RHEL device, run the following command:

```
chcon -u system_u -t rpm_exec_t filename
```

- 5 In the terminal window, go to the directory where you have downloaded the package, then launch the package on the device by running the `./filename` command, where **filename** is the name of the package that you downloaded in [Step 3](#).
- 6 (Conditional) If you want to view the ZENworks notify icon in the notification area, after the agent installation for the Linux device, log out and log in to the device.

In ZENworks Control Center, the device appears in the `\Servers` folder or `\Workstation` folder, on the Devices page.

Manual Installation on Macintosh

You can deploy the ZENworks Agent to a Macintosh device by downloading the deployment package from the ZENworks download page.

IMPORTANT

- ♦ You can install the ZENworks Agent on a Macintosh device if you have root or administrator permissions.

-
- 1 On the target Macintosh device, open a Web browser and enter the following address:

```
http://<server>/zenworks-setup
```

Replace `<server>` with DNS name or the IP address of a ZENworks Server.

- 2 Click the appropriate Macintosh package to download.

NOTE: There are two types of packages:

- ♦ **Network:** This package requires network access to the ZENworks Server to download the necessary PKG files.
- ♦ **Standalone:** Access to the ZENworks Server is not required to install the agent.

-
- 3 At the command prompt, specify executable permissions to the downloaded `.bin` file by running the `chmod +x <file_name>` command.

For more information on the options that you can use with the package, see “[Package Options for Windows, Linux, and Macintosh](#)” in [ZENworks Discovery, Deployment, and Retirement Reference](#)

- 4 At the command prompt, navigate to the directory where you have downloaded the package, then launch the package on the device by running the following command:

```
sudo ./filename
```

The `filename` is the name of the package you downloaded in [Step 2 on page 40](#).

- 5 Log out and log in to the device to view the ZENworks notify icon in the notification area, after agent installation for the Macintosh device.

In ZENworks Control Center, the device appears in the `\Servers` folder or `\Workstation` folder, on the Devices page.

NOTE: After deploying the ZENworks Agent on a Macintosh device, `/opt/novell/zenworks/bin` is not added to the PATH variable and hence, the commands in that directory cannot be used directly. Do any of the following on the Macintosh device to run the commands from `/opt/novell/zenworks/bin`:

- ◆ Re-login to the device.
- ◆ Specify the complete path to access the command.

For example: `/opt/novell/zenworks/bin/zac`.

Using the ZENworks Agent

The following sections provide information to help you log in and use the ZENworks Agent:

- ◆ [“Logging In to the Management Zone” on page 41](#)
- ◆ [“Navigating the ZENworks Agent Views” on page 41](#)
- ◆ [“Promoting a Managed Device to be a Satellite” on page 43](#)

Logging In to the Management Zone

When a Windows managed device boots its operating system, the ZENworks Agent is started and all bundles and policies assigned to the device are available. For bundles and policies assigned to a user to be available, the user must log in to the Management Zone.

The ZENworks 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 Agent 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, the user is automatically logged in to the Management Zone. However, if the user logs in to Tree2, the ZENworks Agent login screen appears and prompts the user for the Tree1 credentials.

Navigating the ZENworks Agent Views

The ZENworks Agent provides the following views:

- ◆ [“ZENworks Application” on page 42](#)
- ◆ [“ZENworks Explorer” on page 42](#)
- ◆ [“ZENworks Icon” on page 42](#)

ZENworks Application

The ZENworks Application is a standalone window that provides access to bundles. You can launch the window from the Start menu (**Start menu > Programs > Novell ZENworks > ZENworks Application**).

The ZENworks Application left pane displays the following:

- ♦ **[All] folder:** Contains all bundles that have been distributed to you, regardless of the folder in which they are located.
- ♦ **ZENworks folder:** Contains all bundles that have not been assigned to a different folder. The ZENworks folder is the default folder for bundles; however, administrators can create additional folders to organize bundles, and can even rename the ZENworks folder.

When you select a folder in the left pane, the bundles that are contained within the folder are displayed in the right pane. You can:

- ♦ Install a bundle or launch an application that is already installed.
- ♦ View the properties of a bundle. The properties include a description of the bundle, information about who to contact for help with the bundle, when the bundle is available for use, and the system requirements established for the bundle.
- ♦ Repair an installed application.
- ♦ Uninstall an application. This is an administrator-controlled feature that might not be enabled.


ZENworks Explorer

ZENworks Explorer is an extension to Windows Explorer that enables bundles to be displayed in Windows Explorer, on the desktop, on the Start menu, on the Quick Launch toolbar, and in the notification area (system tray). The following graphic shows bundles displayed in Windows Explorer.

The following graphic shows bundles displayed on the desktop.

The tasks performed on the bundles in the ZENworks Window can also be performed in the ZENworks Explorer.

ZENworks Icon

The ZENworks Icon  is located in the Windows notification area (system tray). You can click the icon to display the ZENworks Agent window.

To view the agent properties, right click the ZENworks icon and select Technician Application. The ZENworks Agent Properties window is displayed.

The left navigation pane of the properties window contains links for the ZENworks Agent status and its features:

- ♦ **Status:** Displays information such as the last time the agent contacted a ZENworks Server and whether the Agent features are running.
- ♦ **Policies:** Displays the policies assigned to the device and the logged-in user, and also displays whether the policy is effective. It is included only if ZENworks Configuration Management or ZENworks Endpoint Security Management is enabled.

- ◆ **Bundles:** Displays the bundles assigned to the device and the logged-in user. It also displays the current installation status of each bundle (available, downloading, installing, and so forth) and whether the bundle is effective (the device meets the requirements for distribution). It is included only if ZENworks Configuration Management or ZENworks Patch Management is enabled.
- ◆ **Inventory:** Displays inventory information for the device. You can view hardware details, such as the manufacturer and model of your hard drives, disk drives, and video card. You can also view software details, such as installed Windows hot fixes and patches, and the version numbers and locations of installed software products. It is included only if ZENworks Configuration Management or ZENworks Asset Management is enabled.
- ◆ **Endpoint Security:** Displays information about the Endpoint Security Agent and the location that is being used to determine which security policies are applied. It is included only if ZENworks Endpoint Security Management is enabled.
- ◆ **Remote Management:** Displays information about the currently connected remote operators and the Remote Management policy settings that are in effect for the device. It also lets you initiate a management session and control security settings for the session. It is included only if ZENworks Configuration Management is enabled.
- ◆ **Satellite:** Displays the satellite role information of a device that is used as a Satellite Server. The satellite roles include Collection, Content, Authentication, Imaging, and Join Proxy.
This feature is displayed only if your ZENworks administrator has used your device as a satellite.
- ◆ **Logging:** Displays information about the ZENworks Agent's log file, such as the location of the log file, the ZENworks Server to which the agent's log file will be uploaded, and the next time the log is scheduled to be uploaded. It also lets you determine the severity level for logged messages.
- ◆ **Windows Proxy** Displays the results of the discovery and deployment activities performed on the device when it acts as a Windows Proxy for the ZENworks Primary Server.

Promoting a Managed Device to be a Satellite

A Satellite is a managed device that can perform some of the roles that a ZENworks Primary Server normally performs, including authentication, information collection, content distribution, and imaging. A Satellite can be any managed Windows device, managed Linux device, or managed Macintosh device, but not a Primary Server. When you configure a Satellite, you specify which roles it performs (Authentication, Collection, Content, or Imaging). A Satellite can also perform roles that might be added by third-party products that are snap-ins to the ZENworks framework.

For detailed information about Satellites and how to promote a managed device to a Satellite, see “Satellites” in the [ZENworks Primary Server and Satellite Reference](#).

5 System Messages

ZENworks lets you monitor the activity within your Management Zone through system messages.

- ♦ “Viewing System Messages” on page 45
- ♦ “Creating a Watch List” on page 47

Viewing System Messages

The ZENworks system generates normal (informational), warning, and error messages to help you monitor activities such as the distribution of software and application of policies.




Each ZENworks Server and ZENworks Agent creates a log of the activities associated with it. These messages are displayed in ZENworks Control Center in various areas:

- ♦ **System Message Log:** The system message log, which can be accessed by selecting **Dashboard > System Messages**, displays messages from all ZENworks Servers and ZENworks Agents within the zone.
- ♦ **Device Message Log:** A device message log, located on the Summary page for a server or workstation, displays messages generated by the ZENworks Server or the ZENworks Agent. For example, the message log for Workstation1 includes all messages generated by the ZENworks Agent on Workstation1.
- ♦ **Content Message Log:** A content message log, located on the Summary page for a bundle or policy, displays only the ZENworks Server or ZENworks Agent messages associated with the bundle or policy. For example, the message log for Bundle1 might have messages generated by three different ZENworks Servers and 100 different ZENworks Agents.





Viewing a Summary of Messages

You can view a summary that shows the number of messages generated for the servers, workstations, bundles, and policies in the zone.

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

The Message Summary panel displays the status of all servers, workstations, policies, and bundles in the Management Zone. For example, if two servers have unacknowledged critical messages (those messages that you or another administrator have not yet acknowledged), the  column displays the number 2. Or, if you have three bundles with warning messages and five bundles with only normal messages, the  column displays the number 3 and the  column displays the number 5. You can do the following with the summary:

- ♦ Click an object type to display its root folder. For example, click **Servers** to display the Servers root folder (`/Servers`).

- ◆ For any object type, click the number in one of its status columns (  ) to display a listing of all the objects that currently have that status. For example, to see the list of servers that have a normal status, click the number in the  column.
- ◆ For any object type, click the number in the **Total** column to display all the objects that have critical, warning, or normal messages. For example, click the **Total** count for **Servers** to display a list of all servers that have any type of messages.

Acknowledging Messages

A message remains in a message log until you acknowledge it. You can acknowledge individual messages or acknowledge all messages in the message log at one time.

- 1 In ZENworks Control Center, click the **Devices** tab.
- 2 Navigate the **Servers** folder until you locate a ZENworks Server.
- 3 Click the server to display its details.
- 4 On the **Summary** tab, locate the Message Log panel.

The Message Log panel lists all messages (informational, warning, and error) generated by the ZENworks Server. The following table explains the various ways you can acknowledge and delete messages.

Task	Steps	Additional Details
Acknowledge a message	<ol style="list-style-type: none"> 1. Click the message to display the Message Detail Information dialog box. 2. Click Acknowledge. 	If you do not want to acknowledge the message, click Finished to close the dialog box. This causes the message to remain in the Message Log list.
Acknowledge all messages	<ol style="list-style-type: none"> 1. In the Tasks list located in the left navigation pane, click Acknowledge All Messages. 	
View all acknowledged or unacknowledged messages	<ol style="list-style-type: none"> 1. Click the Advanced button to display the Edit Message Log page. 	<p>In addition to viewing all acknowledged and unacknowledged messages, you can also view only those messages with a specific status or date, view more details about messages, and acknowledge messages.</p> <p>Click the Help button on the Edit Message Log page for specific information about performing tasks on that page.</p>
Delete a message	<ol style="list-style-type: none"> 1. Click the message to display the Message Detail Log dialog box. 2. Click Delete. 	Deleting a message completely removes the message from your ZENworks system.

You can also use the `messages-acknowledge` command in the `zman` utility to acknowledge messages associated with devices, bundles, and policies. For more information, see “[Message Commands](#)” in the *ZENworks Command Line Utilities Reference*.

Where to Find More Information

For more information about system messages, see “Using Message Logging” in the [ZENworks Control Center Reference](#).

Creating a Watch List

If you have devices, bundles, or policies whose status you want to closely monitor, you can add them to the Watch List. The Watch List provides the following information:

- ♦ **Agent:** For servers and workstations, displays whether the device’s ZENworks Agent is currently connected (🟢) or disconnected (🔴).
- ♦ **🚨:** Displays whether the object has any critical messages.
- ♦ **Type:** Displays an icon representing the object’s type. For example, a bundle might have a 🗄 icon to show that it is a Windows bundle. Or a device might have a 🖥 icon to show that it is a server. You can mouse over the icon to see a description.
- ♦ **Name:** Displays the object’s name. You can click the name to go to the object’s message log.

To add a device, bundle, or policy to the Watch List:

- 1 In ZENworks Control Center, click the **Home** tab.
- 2 In the Watch List panel, click **Add**, then select the type of object (device, bundle, or policy) that you want to add to the list.
- 3 In the selection dialog box, select the desired object, then click **OK** to add it to the Watch List.
For example, if you are adding servers, browse and select a server.

Objects remain in the Watch List until you remove them.

6 Audit Management

ZENworks enables you to successfully record and view activities that take place in your ZENworks system, by using the Audit Management feature. The Audit Management feature enables you to capture various events that occur in your zone. The details of a captured event can be used for security and compliance purposes, enabling you to identify who did what and on which system, when an important event occurs in your environment. Using this feature, you can centrally monitor activities related to Primary Servers, Satellite Servers, and managed devices.

- ♦ [“Types of Audit Events” on page 49](#)
- ♦ [“Enabling an Event” on page 49](#)
- ♦ [“Viewing a Generated Event” on page 50](#)

Types of Audit Events

ZENworks audit events are of two types:

- ♦ **Change Events:** These events capture configuration changes made to the zone through ZENworks Control Center or the zman command line utilities. You can capture a variety of changes ranging from bundle changes to ZENworks system changes. For example, you can configure an audit event that records the activity of an administrator assigning a bundle to a device.
- ♦ **Agent Events** These events capture actions that occur on the ZENworks managed devices. They are also called Device events.

Both change events and agent events can be enabled for all devices in the zone or for individual devices.

Enabling an Event

To audit an event, you must first enable the event in ZENworks Control Center. You can enable the event at the zone or device level. An event that is enabled at the zone level applies to all devices in the zone, and an event that is enabled at the device level applies to only the selected device.

- 1 Log in to ZENworks Control Center.
- 2 (Zone) To enable events at the zone, click **Configuration > Management Zone Settings > Audit Management**.
or
(Devices) To enable events at the device, click **Devices > Managed Devices**. Locate the device in the Servers or Workstations folders, click the device object to display its properties, then click **Settings > Audit Management**.
- 3 Click **Events Configuration** to display the Events Configuration dialog page.
- 4 In the **Change Events** or **Agent Events** tab, click **Add** to display the Add Change Events or Add Agent Events dialog box.

For information about the change and agent event categories, see [ZENworks Audit Management Reference](#).

- 5 Expand the **Change Events** or **Agent Events** tree and select the required event.
- 6 Specify the following information for the **Event Settings**:
 - ◆ **Event Classification:** Based on the importance of the event, select **Critical**, **Major**, or **Informational**.
 - ◆ **Days to Keep:** Indicate the number of days to keep the event before purging it.
 - ◆ **Notification Types:** Specify whether the notification should be sent via email, SNMP Trap, UDP, or to a local file when the event occurs. If you select **Log message to a local file**, you must configure the local log file settings.

You can also select all notification types. For more information, see [“Using Message Logging”](#).
 - ◆ (Agent Events) Specify the **Sample Frequency** rate at which data should be collected in order to generate audit events. This field is displayed only if a ZENworks Endpoint Security Management event or a ZENworks Agent event is selected.
- 7 Click **OK** to add the event.

You can edit or delete an event by selecting the event in the Event Configuration page and clicking **Edit** or **Delete** from the menu bar. To select multiple events at a time, press **Ctrl** and click to select.

Viewing a Generated Event

When an enabled event has occurred, an audit event is generated.

After an audit event is generated, you can access the details of the event from the following locations:

- ◆ **Dashboard:** You can view the audit data through the ZENworks Control Center Dashboard. The Dashboard has the following tabs:
 - ◆ **Dashboard:** From this tab you can see a summary of the audit events that have occurred in the zone. You can see key indicators about top events and impacted objects, and can drill into the event log view in a filtered manner. By default, this dashboard shows you an overview of events in the last 4 hours. If you want to see more data, you can change the time period.
 - ◆ **Events (Audit Log):** This tab enables you to view all of the events that have occurred in the zone. The information is displayed in a format similar to the Events Configuration page. A count is displayed against those categories for which an event has been generated. For example, if a **Bundle Assignment Management** event has been generated, **1** is displayed against the Bundle Assignment Management category in the tree structure. When you click the event, the details of the event are displayed in the right pane.
- ◆ **(Change Events) Object Folders:** The **Audit** tab in the object folders (**Devices**, **Bundles**, **Policies** and **Users**) enables you to view the audit events that are generated for all objects within the selected folder. For example, you can view the events generated for all bundles within a bundles folder. Hence, all bundle-related events can be viewed in the Bundles folder. The information is categorized similar to the **Events Configuration** page. You can browse through events that have occurred, and if you need more information, you can click the event to view the event details.
- ◆ **(Change Events) Objects:** You can also view the audit events for an object within the object folder. For example, if you select a particular bundle within a bundles folder, you can view the events generated for that specific bundle.
- ◆ **(Agent Events) Devices Folder:** The **Audit** tab in the **Devices** folder enables you to view the events that are generated for a particular device (server or workstation).

To view the generated event details:

1 Log in to ZENworks Control Center.

2 (Dashboard) To view the events in the Dashboard, click **Dashboard > Events**.

or

(Object Folder) To view the events for all objects in a folder (for example, a device folder, bundles folder, or policy folder), click the folder's **Details** link, then click the **Audit** tab.

or

(Object) To view the events for a specific object (for example, a device, bundle, or policy), click the object, then click the **Audit** tab.

(Devices Folder) To view the events in the Devices folder, in the left pane, click **Devices**. If the event has been performed on a server in the zone, click the server **Details**, or if the event has been performed on a managed device, click the workstation **Details**. Then click the **Audit** tab to view the Events screen.


3 Click the **Change Events** or **Agent Events** tab.

4 Expand the tree structure and navigate to the relevant category.

Depending on the number of audit events configured, the relevant count is displayed against the category.

5 Click the event.

The details of the generated event are displayed in the right pane.

NOTE: To view the details of the event in a new window, click 

Product Administration

The following sections provide information to help you use ZENworks products. Before attempting any of the sections, you should have already completed the configuration tasks in [Part I, “System Configuration,” on page 9](#).

- ◆ [Chapter 7, “Quick List,” on page 55](#)
- ◆ [Chapter 8, “Asset Management,” on page 61](#)
- ◆ [Chapter 9, “Configuration Management,” on page 73](#)
- ◆ [Chapter 10, “Endpoint Security Management,” on page 97](#)
- ◆ [Chapter 11, “Full Disk Encryption,” on page 103](#)
- ◆ [Chapter 12, “Patch Management,” on page 107](#)

7 Quick List

After you have configured your Management Zone (see [Part I, “System Configuration,” on page 9](#)), you should review the concepts and tasks in the following sections for any ZENworks products that you have licensed or are evaluating:

- ♦ [“Asset Management” on page 55](#)
- ♦ [“Configuration Management” on page 56](#)
- ♦ [“Endpoint Security Management” on page 57](#)
- ♦ [“Full Disk Encryption” on page 58](#)
- ♦ [“Patch Management” on page 59](#)

Asset Management

ZENworks Asset Management lets you monitor software license compliance, track software usage, and track software ownership through the allocation of licenses to devices, sites, departments, and cost centers.

Task	Details
Activate Asset Management	<p>If you did not activate Asset Management during installation of the Management Zone, either by providing a license key or by turning on the evaluation, you must do so before you can use the product.</p> <p>For instructions, see “Activating Asset Management” on page 61.</p>
Enable the ZENworks Agent to perform Asset Management operations	<p>The agent's Asset Management feature is enabled by default when ZENworks Asset Management is activated (full license or evaluation).</p> <p>You should verify that the agent's Asset Management feature is still enabled. In addition, if you want to track software licenses against users (rather than only against devices), you need to enable the User Management feature, which is disabled by default. For instructions, see “Enabling Asset Management in the ZENworks Agent” on page 61.</p>
Scan devices to collect software and hardware inventory	<p>Scan devices to collect software and hardware inventories for the devices. The inventory information can help you make decisions about software distribution and hardware upgrades.</p> <p>This task must be done before you can do any of the remaining tasks.</p> <p>For instructions, see “Collecting Software and Hardware Inventory” on page 62.</p>
Monitor software usage	<p>Generate to analyze how much and how often software products are being used.</p> <p>For instructions, see “Monitoring Software Usage” on page 63.</p>

Task	Details
Monitor software license compliance	See whether the installed software products are properly licensed, under licensed, or over licensed. For instructions, see “Monitoring License Compliance” on page 64.
Allocate licenses	Allocate licenses within your organization to track ownership and distribution of the licenses. You can allocate licenses to devices or demographics (sites, departments, and cost centers). For instructions, see “Allocating Licenses” on page 70.

Configuration Management

ZENworks Configuration Management lets you manage a device’s configuration, including distributing software to the device, applying Windows configuration policies, and imaging and applying images. In addition, you can collect device hardware and software inventory to inform your upgrade and buying decisions, and remotely access devices to troubleshoot and solve problems.

The following tasks can be done as needed and in any order.

Task	Details
Activate Configuration Management	If you did not activate Configuration Management during installation of the Management Zone, either by providing a license key or by turning on the evaluation, you must do so before you can use the product. For instructions, see “Activating Configuration Management” on page 73.
Enable the ZENworks Agent to perform Configuration Management operations	For the ZENworks Agent to perform Configuration Management operations on a device, the appropriate agent features must be enabled. These features (Bundle Management, Image Management, Policy Management, Remote Management, and User Management) are enabled by default when ZENworks Configuration Management is activated (full license or evaluation). You should verify that the features are enabled. Or, if you don’t want to use certain features, you can disable them. For instructions, see “Enabling Configuration Management in the ZENworks Agent” on page 73.
Enroll Mobile Devices	To enable Configuration Management operations on mobile devices such as deploy bundles, apply security policies, and various device management operations, you need to enroll mobile devices to the ZENworks Management Zone. For instructions, see Enrolling Mobile Devices.

Task	Details
Distribute software	<p>Distribute software through bundles. Bundles include the software files and instructions required to install, launch, and uninstall (when necessary) the software. You can create bundles to distribute Windows Installer applications (both MSI and MSP), non-Windows Installer applications, Web links, thin-client applications, Linux applications, and Macintosh applications..</p> <p>For instructions, see “Distributing Software” on page 74.</p>
Apply policies	<p>Control device behavior through the application of policies. ZENworks lets you create and apply Windows Group policies, roaming profile policies, browser bookmark policies, printer policies, and more.</p> <p>For instructions, see “Applying Policies” on page 75.</p>
Take images of and apply images to devices	<p>Create images of devices, apply images to devices, and run imaging scripts on devices. ZENworks Configuration Management uses its Preboot Services functionality to perform these imaging tasks on devices at startup.</p> <p>For instructions, see “Imaging Devices” on page 77.</p>
Scan devices to collect software and hardware inventory	<p>Scan devices to collect software and hardware inventories for the devices. The inventory information can help you make decisions about software distribution and hardware upgrades.</p> <p>For instructions, see “Collecting Software and Hardware Inventory” on page 93.</p>

Endpoint Security Management

ZENworks Endpoint Security Management lets you protect devices by enforcing security settings via policies. You can control a device's access to removable storage devices, wireless networks, and applications. In addition, you can secure data through encryption and secure network communication via firewall enforcement (ports, protocols, and access control lists). And you can change an endpoint device's security based on its location.

The following tasks must be done in the order listed.

Task	Details
Activate Endpoint Security Management	<p>If you did not activate Endpoint Security Management during installation of the Management Zone, either by providing a license key or by turning on the evaluation, you must do so before you can use the product.</p> <p>For instructions, see “Activating Endpoint Security Management” on page 97.</p>
Enable the Endpoint Security Agent	<p>The Endpoint Security Agent enforces security policies on devices. It must be installed and enabled on each device to which you want to distribute security policies.</p> <p>For instructions, see “Enabling the Endpoint Security Agent” on page 97.</p>

Task	Details
Create locations	<p>Security policies can be global or specific to locations. A global policy is applied in all locations. A location-based policy is applied only when the Endpoint Security Agent determines that the device's network environment matches the environment defined for the location.</p> <p>If you want to use location-based policies, you must create locations. For instructions, see "Creating Locations" on page 98.</p>
Create security policies	<p>A device's security settings are configured through security policies. There are 11 types of security policies you can create.</p> <p>For instructions, see "Creating a Security Policy" on page 98.</p>
Assign policies to users and devices	<p>Security policies can be assigned to users or to devices.</p> <p>For instructions, see "Assigning a Policy to Users and Devices" on page 100.</p>
Assign policies to zones	<p>To ensure that a device is always protected, you can define default security policies for each policy type by assigning policies to the zone. A zone-assigned policy is applied when a device is not covered by a user-assigned or device-assigned policy.</p> <p>For instructions, see "Assigning a Policy to the Zone" on page 101.</p>

Full Disk Encryption

ZENworks Full Disk Encryption protects a device's data from unauthorized access when the device is powered off or in hibernation mode. To provide data protection, the whole disk or partition is encrypted, including temporary files, swap files, and the operating system. The data cannot be accessed until an authorized user logs in, and can never be accessed by booting the device from media such as a CD/DVD, floppy disk, or USB drive. For an authorized user, accessing data on the encrypted disk is no different than accessing data on an unencrypted disk.

The following tasks must be done in the order listed.

Task	Details
Activate Full Disk Encryption	<p>If you did not activate Full Disk Encryption during installation of the Management Zone, either by providing a license key or by turning on the evaluation, you must do so before you can use the product.</p> <p>For instructions, see "Activating Full Disk Encryption" on page 103.</p>
Enable the Full Disk Encryption Agent	<p>The Full Disk Encryption Agent performs disk encryption. It must be installed and enabled on each device whose disks you want to encrypt.</p> <p>For instructions, see "Enabling the Full Disk Encryption Agent" on page 104.</p>

Task	Details
Create a Disk Encryption policy	<p>The information required to encrypt a devices disks is passed to the Full Disk Encryption Agent via a Disk Encryption policy. You must create at least one policy.</p> <p>For instructions, see “Creating a Disk Encryption Policy” on page 104.</p>
Assign the policy to devices	<p>Disk Encryption policies can only be assigned to devices, device groups, or device folders.</p> <p>For instructions, see “Assigning the Policy to Devices” on page 105.</p>

Patch Management

ZENworks Patch Management lets you automate the process of assessing software vulnerabilities and applying patches to eliminate the vulnerabilities.

The following tasks must be done in the order listed.

Task	Details
Activate Patch Management	<p>If Patch Management was not activated during installation of the ZENworks Management Zone, either by supplying a subscription license or turning on the evaluation, you need to activate the product.</p> <p>For instructions, see “Activating Patch Management” on page 107.</p>
Enable the ZENworks Agent to perform Patch Management operations	<p>For the ZENworks Agent to perform Patch Management operations on a device, the agent’s Patch Management feature must be enabled. The Patch Management feature is enabled by default when ZENworks Patch Management is activated (full license or evaluation).</p> <p>You should verify that the agent’s Patch Management feature is enabled. For instructions, see “Enabling Patch Management in the ZENworks Agent” on page 108.</p>
Start the subscription service	<p>You must start the subscription service on a ZENworks Server. This server downloads the patches and replicates them to other ZENworks Servers (if you have more than one).</p> <p>For instructions, see “Starting the Subscription Service” on page 108.</p>
Create patch policies	<p>After the subscription service has download patches, apply the desired patches.</p> <p>For instructions, see “Creating Patch Policies” on page 108.</p>

8 Asset Management

The following sections provide explanations and instructions for using ZENworks Asset Management to collect software and hardware inventory from devices, monitor software usage on devices, and monitor software license compliance.

- ♦ “Activating Asset Management” on page 61
- ♦ “Enabling Asset Management in the ZENworks Agent” on page 61
- ♦ “Collecting Software and Hardware Inventory” on page 62
- ♦ “Monitoring Software Usage” on page 63
- ♦ “Monitoring License Compliance” on page 64
- ♦ “Allocating Licenses” on page 70

Activating Asset Management

If you did not activate Asset Management during installation of the Management Zone, either by providing a license key or by turning on the evaluation, complete the following steps:

- 1 In ZENworks Control Center, click **Configuration**.
- 2 In the Licenses panel, click **ZENworks 2017 Asset Management**.
- 3 Select Evaluate/Activate product, then fill in the following fields:
 - Use Evaluation:** Select this option to enable a 60-day evaluation period. After the 60-day period, you must apply a product license key to continue using the product.
 - Product License Key:** Specify the license key you purchased for Asset Management. To purchase a product license, see the [ZENworks Asset Management product site \(http://www.novell.com/products/zenworks/assetmanagement\)](http://www.novell.com/products/zenworks/assetmanagement).
- 4 Click **OK**.

Enabling Asset Management in the ZENworks Agent

For the ZENworks Agent to perform Asset Management operations on a device, the agent’s Asset Management feature must be enabled. The Asset Management feature is enabled by default when ZENworks Asset Management is activated (full license or evaluation).

You should verify that the agent’s Asset Management feature is enabled. In addition, if you want to track software licenses against users (rather than only against devices), you need to enable the User Management feature, which is disabled by default. For instructions, see “[Configuring ZENworks Agent Features](#)” on page 35.

NOTE: After enabling the ZENworks Asset Management module, ensure that you enforce a full scan on all the devices by running the `zac inv -f scannow` command. Until you perform the scan, Asset Management report will not be accurate.

Collecting Software and Hardware Inventory

When you inventory a device, ZENworks Asset Management collects both software and hardware information from the device. Using ZENworks Control Center, you can view the inventory for an individual device, or you can generate for multiple devices based on specific criteria.

You can use the software inventory for a variety of purposes, including tracking usage of specific applications and ensuring that you have sufficient licenses for all copies of the application being used. For example, assume that your company owns 50 licenses of a word processing software. You do a software inventory and find that it is installed on 60 devices, which means that you are out of compliance with your license agreement. However, after viewing the usage for the software for the past 6 months, you see that it is actually being used on only 45 devices. To become compliant with the license agreement, you uninstall the software from the 15 devices that are not using it.

You can use the hardware inventory for a variety of purposes as well, including ensuring that your hardware meets the requirements for running specific software. For example, assume that your Accounting department wants to roll out a new version of their accounting software. The new software has increased processor, memory, and disk space requirements. Using the hardware inventory collected from your devices, you can create two reports, one that lists all devices that meet the requirements and one that lists the devices that don't meet the requirements. Based on the reports, you distribute the software to the compliant devices and create an upgrade plan for the noncompliant devices.

By default, devices are automatically scanned at 1:00 a.m. the first day of each month. You can modify the schedule, as well as many other **Inventory** configuration settings, on the **Configuration** tab in ZENworks Control Center.

The following sections provide instructions for initiating a device scan and using the collected inventory:

- ♦ [“Initiating a Device Scan” on page 62](#)
- ♦ [“Viewing a Device Inventory” on page 63](#)
- ♦ [“Generating an Inventory Report” on page 63](#)
- ♦ [“Where to Find More Information” on page 63](#)

Initiating a Device Scan

You can initiate a scan of a device at any time.

- 1 In ZENworks Control Center, click the **Devices** tab.
- 2 Navigate the **Servers** or **Workstations** folder until you locate the device you want to scan.
- 3 Click the device to display its details.
- 4 In the task list located in the left navigation pane, click **Server Inventory Scan** or **Workstation Inventory Scan** to initiate the scan.

The QuickTask Status dialog box displays the status of the task. When the task is complete, you can click the **Inventory** tab to view the results of the scan.

To scan multiple devices at one time, you can open the folder in which the devices are located, select the check boxes next to the devices, then click **Quick Tasks > Inventory Scan**.

You can also use the `inventory-scan-now` command in the `zman` utility to scan a device. For more information, see [“Inventory Commands”](#) in the *ZENworks Command Line Utilities Reference*.

Viewing a Device Inventory

- 1 In ZENworks Control Center, click the **Devices** tab.
- 2 Navigate the *Servers* or *Workstations* folder until you locate the device whose inventory you want to view.
- 3 Click the device to display its details.
- 4 Click the **Inventory** tab.

The Inventory page provides a summary of the hardware inventory. To see detailed inventory information, click **Detailed Hardware/Software Inventory**.

Generating an Inventory Report

ZENworks Asset Management includes several standard reports. In addition, you can create custom reports to provide different views of the inventory information.

- 1 In ZENworks Control Center, click the **Reports** tab.
- 2 In the Inventory Standard Reports panel, click **Software Applications**.
- 3 Click the **Operating System** report to generate the report.

Using the options at the bottom of the report, you can save the generated report as a Microsoft Excel spreadsheet, CSV (comma-separated values) file, PDF file, or PDF Graph file.

Where to Find More Information

For more information about inventory, see the [ZENworks Asset Inventory Reference](#).

Monitoring Software Usage

After you've inventoried devices, you can run reports to view how much the devices' applications are used. ZENworks Asset Management includes standard reports for application usage by product, user, and device. You can also customize reports to provide more detailed or focused information. For example, Asset Management includes a predefined custom report that shows application that have not been used in the last 90 days.

To run a report that shows how much a specific application is used:

- 1 In ZENworks Control Center, click the **Asset Management** tab, then click the **Software Usage** tab.
- 2 In the Software Usage Standard panel, click **Application Usage** to display the list of application usage reports.
- 3 In the panel, click **Local Application Usage by Product**.

The report shows all the products, grouped by software manufacturer, that are installed on the devices.

- 4 Find a manufacturer whose products you want to see, then click the number in the Installations column to display the installed products.

The resulting report shows the current number of installations for each product, how many of the installations have been used, when it was last used, and other usage information.

- 5 If you want to change the time period for the report, or change the list of products displayed (all products, used products, or unused products), click **Change Time Period/Filters** at the bottom of the report.

There are many other standard and predefined custom that you can use. For additional information about application usage, see “[Reports](#)” in the *ZENworks 2017 Asset Management Reference*.

Monitoring License Compliance

ZENworks Asset Management enables you to monitor your organization’s compliance with software license agreements by comparing purchased software licenses with actual software installations discovered during inventory scans.

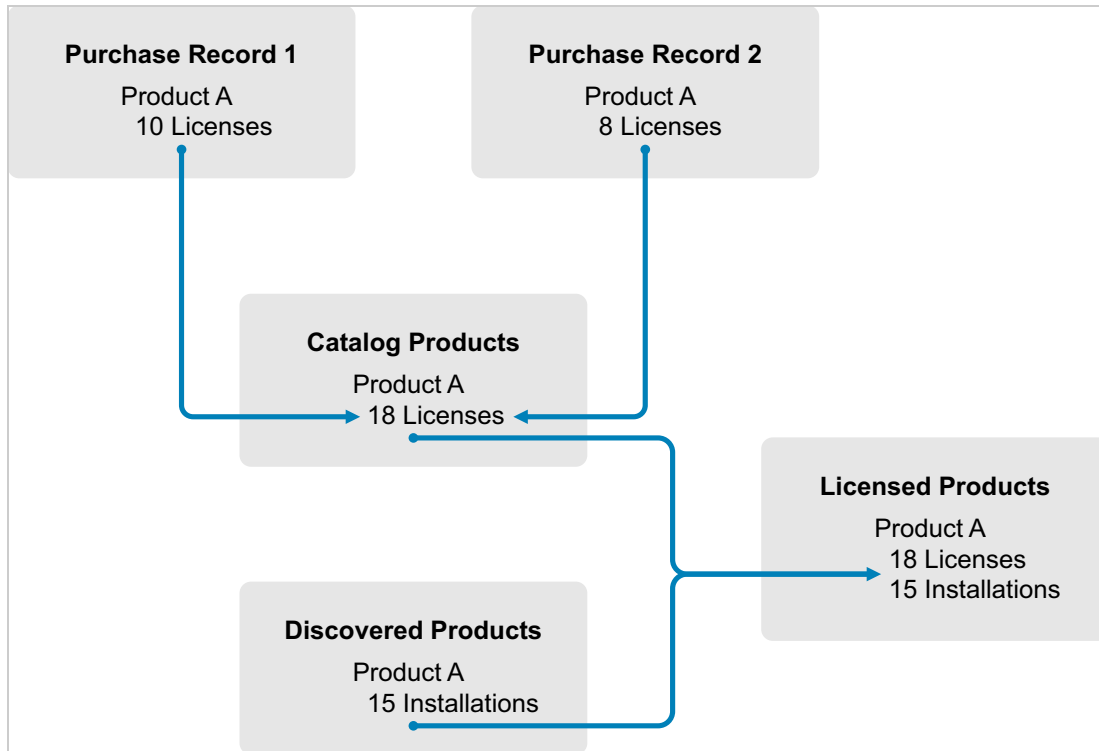
Asset Management license compliance is a powerful and flexible tool. As a result, there are multiple approaches and methods you can use when setting up license compliance. The following sections provide basic instructions with minimal explanation in order to help you quickly set up a single product for license compliance monitoring. After you finish this basic scenario, see “[License Compliance](#)” in the *ZENworks 2017 Asset Management Reference* for more detailed information and instructions.

- ♦ “[License Compliance Components](#)” on page 64
- ♦ “[Discovering Installed Products](#)” on page 66
- ♦ “[Creating a Catalog Product and Purchase Record](#)” on page 66
- ♦ “[Creating a Licensed Product](#)” on page 67
- ♦ “[Viewing Compliance Data](#)” on page 69
- ♦ “[Where to Find More Information](#)” on page 70

License Compliance Components

Before you begin implementing compliance monitoring, you need to understand the components involved and how they work together, as explained in the following illustration and subsequent text.

Figure 8-1 License Compliance Components



- ◆ You scan the devices in your Management Zone to collect the list of installed software products. These are called *discovered products*. In the above illustration, the inventory scan discovered that ProductA is installed on 15 devices.
- ◆ You create *catalog products* to represent the software products your organization has purchased. Typically, each catalog product corresponds to a specific manufacturer part number. In the above illustration, ProductA is the only catalog product. However, you might have catalog products for ProductA, ProductA Upgrade, and ProductB.
- ◆ You create *purchase records* to represent the purchase orders or invoices for software products. Each line item in the purchase record lists a catalog product along with the license purchase quantity. If a catalog product is listed in multiple purchase records, the catalog product's total licenses equal the purchase quantity for both purchase records. In the above illustration, one purchase record includes 10 licenses of ProductA and another purchase record includes 8 licenses. The total license count for ProductA is 18.
- ◆ You create *licensed products* and associate the corresponding discovered products and catalog products to them. This gives you a single licensed product that includes the number of licenses and installations for the product. The result is a quick view of whether or not the product usage complies with the license agreement. In the above illustration, ProductA has 18 licenses and is installed on 15 devices, so ProductA complies with your license agreement.

Discovering Installed Products

If you have not already scanned the devices in your Management Zone to collect information about installed products (referred to as **discovered products**), complete the steps in [“Collecting Software and Hardware Inventory” on page 62](#).

After you have discovered products, choose one whose compliance you want to monitor.

- 1 In ZENworks Control Center, click the **Asset Management** tab, then click the **License Management** tab.
- 2 In the License Management panel, click **Discovered Products** to display the Discovered Products list.
- 3 Browse the list to choose the discovered product you want to use.

The product must have a least one installation listed in the **Installed Quantity** column. If possible, you should choose a product for which you have a purchase order or invoice readily available. This allows you to complete the scenario using real information. Otherwise, you can invent the purchase information as you go. Remember your product choice so that you can use it later.

- 4 Continue with the next section, [“Creating a Catalog Product and Purchase Record” on page 66](#).

Creating a Catalog Product and Purchase Record

Discovered products provide the installation information for products. To provide information about product purchases, you create catalog products and purchase records.

A catalog product represents a software product. A purchase record populates the catalog product with the number of product licenses you've purchased.

The following steps explain how to create a catalog product and purchase record for the discovered product you chose in [“Discovering Installed Products” on page 66](#).

- 1 In ZENworks Control Center, click the **Asset Management** tab, then click the **License Management** tab.
- 2 Create the catalog product:
 - 2a In the License Management panel, click **Catalog Products**.
 - 2b Click **New > Catalog Product** to launch the Create New Catalog Product Wizard.
 - 2c Fill in the following fields:


Manufacturer: Select the software manufacturer from the list. If the correct manufacturer is not listed, type the manufacturer name (for example, Novell, Symantec, or Microsoft).

Product: Type the name of the product. The product should represent the purchased software product package (SKU). For example, the purchased package might be Product A Single License or Product A 10-Pack. If you have an invoice record that includes the product for which you are creating the catalog product, use the product name from the invoice.

Licenses Per Package: Specify the number of licenses included in the product package.

Product Type - Notes: These fields are optional. You can use them to further identify the product.

Excluded: Do not select this check box.

- 2d Click **Next** to display the Summary page, then click **Finish** to add the product to the Catalog Products list.
- 2e Click **License Management** (in the breadcrumb path at the top of the page) to return to the License Management page.
- 3 Create the purchase record:
 - 3a In the License Management panel, click **Purchase Records**.
 - 3b Click **New > Purchase Record** to launch the Create New Purchase Record Wizard.
 - 3c Fill in the following fields:
 - PO Number:** Specify the purchase order number or invoice number associated with the software product purchase. If you don't have PO or invoice for this product, use any number.
 - Order Date:** Select the date the software was purchased.
 - Recipient - Reseller:** These fields are optional. You can use them to further identify the purchase record.
 - 3d Click **Next** to display the Summary page.
 - 3e Select the **Define Additional Properties** box, then click **Finish** to create the purchase record and display its Purchase Details page.
 - 3f Click **Add** to display the Add Purchase Detail dialog box, then fill in the following fields:
 - Product:** Click  to browse for and select the catalog product you created in [Step 2](#).
 - Quantity:** Specify the quantity of product purchased. For example, if the catalog product you selected is ProductA 10-Pack and the purchase order was for 5 ProductA 10-Packs, specify 5.
 - Unit MSRP - Extended Price:** These fields are required. Specify the manufacturer's suggested retail price (MSRP), the price you paid per unit, and the extended price. If you leave the **Extended Price** field blank, the wizard populates it by multiplying the **Purchase Quantity** and the **Unit Price**.
 - Invoice # - Comments:** These fields are optional. You can use them to further identify the purchase.
 - 3g Click **OK**.
- 4 Continue with the next section, [Creating a Licensed Product](#).

Asset Management can also import purchase information from electronic files. During the process, the purchase record is created as well as any catalog products for software products included in the purchase record. For more information, see "[License Compliance](#)" in the [ZENworks 2017 Asset Management Reference](#).


Creating a Licensed Product

The final step in setting up compliance for the software product is to create a licensed product and associate the discovered product and catalog product with it. Doing so populates the license product with the installation and license information needed to determine its license compliance status.

The following steps explain how to use the Auto-Reconcile Wizard to create the licensed product and associate the discovered product and catalog product with it.

- 1 In ZENworks Control Center, click the **Asset Management** tab, then click the **License Management** tab.
- 2 In the License Management panel, click **Licensed Products**.

- 3 In the Licensed Products panel, click **Action > Auto-Reconcile: Create Licensed Products** to launch the Auto-reconcile Wizard. Complete the wizard using information from the following table to fill in the fields.

Wizard Page	Details
Discovered Product Filter	<p>The Auto-Reconcile Wizard creates licensed products from existing discovered products. To find your discovered product:</p> <ol style="list-style-type: none"> 1. Click the Products Specified Below option. 2. In the Select list, select the manufacturer of your discovered product. 3. In the Product field, enter the name of your discovered product.
Select Licensed Products to Create	<p>Based on the information you specified on the Discovered Product Filter page, this page should display your discovered product and the licensed that will be created for it.</p> <p>The wizard attempts to match catalog products to the discovered product by comparing the Manufacturer and Product fields. If the wizard was able to match the catalog product you created to your discovered product, the catalog product is listed as well. Select the catalog product to associate it with the licensed product.</p> <p>If the wizard is unable to match the catalog product to the discovered product, you will need to manually assign the catalog product after completing the wizard.</p>
Destination Folder	<p>Select the folder where you want to place the new licensed product.</p> <p>The field defaults to the current folder (the folder from which you launched the Auto-Reconcile Wizard). To specify another folder, click  to browse for and select the folder. The folder must already exist; you cannot use the selection dialog to create a new folder.</p>
License Entitlements	<p>Every licensed product must have at least one entitlement and license model.</p> <p>An entitlement typically represents a license agreement. In many cases, a licensed product might have only one entitlement. However, by allowing multiple entitlements, you can determine compliance for a licensed product that has several license agreements. For example, you might have a full license agreement and an upgrade license agreement for the same product. Rather than creating two separate licensed products for the same product, you create one licensed product with two different entitlements.</p> <p>The license model determines how the licenses are counted. Licenses can be counted per installation, user, or device.</p> <p>For this scenario, specify Per-Installation as the description and select Per-Installation as the license model. This causes each installation of the product to consume a license.</p>
Auto-reconcile Create Summary	Review your data.

- 4 If you haven't done so already, click **Finish** to create the licensed product and add it to the Licensed Products list.

5 If the Auto-Reconcile Wizard was unable to associate your catalog product with the licensed product:

5a Click the licensed product.

5b Click the **License Entitlements** tab.

5c In the Entitlements panel, click the entitlement.

5d Click the **Proof of Ownership** tab.

5e In the Catalog Products panel, click **Add**.

5f Select the catalog product, then click **OK** to add it to the Catalog Products panel.

The Catalog Products panel displays the catalog product's Purchase Quantity, which is the number of units of the catalog product that you've purchased (according to the purchase record). It also displays the License Quantity, which is the total number of licenses included in the purchased units.

6 Continue with the next section, [Viewing Compliance Data](#), for information about monitoring compliance.

Viewing Compliance Data

There are two views you can use to see the compliance status of your licensed products. You can view the Licensed Products page to get a compliance status summary for all products, or you can generate the Software Compliance report to see more detailed information.




- ♦ ["Viewing the Compliance Status Summary" on page 69](#)
- ♦ ["Generating the Software Compliance Report" on page 69](#)

Viewing the Compliance Status Summary

1 In ZENworks Control Center, click the **Asset Management** tab, then click the **License Management** tab.

2 In the License Management panel, click **Licensed Products** to display the Licensed Products page.

The Licensed Products list displays all licensed products and their current compliance status:

- ♦  The software product is properly licensed. The number of purchased licenses equals the number of installations.
- ♦  The software product is over licensed. There are more purchased licenses than installations.
- ♦  The software product is under licensed. There are fewer purchased licenses than installations.

Generating the Software Compliance Report

1 In ZENworks Control Center, click the **Asset Management** tab, then click the **License Management** tab.

2 In the License Management panel, click **License Management**.

3 In the License Management Standard panel, click **Software Compliance**.

- 4 In the panel, click **Compliance Report**.

A report appears showing compliance data by license. You can filter the data by compliance status, manufacturer and value, or demographic criteria. Drill in to **License Quantity** to see compliance details for a particular licensed product. For information on other, see the [ZENworks 2017 Asset Management Reference](#).

Where to Find More Information

The scenario described in the previous sections shows only a small portion of the license compliance functionality available in ZENworks Asset Management. For more information, see “[License Compliance](#)” in the [ZENworks 2017 Asset Management Reference](#).

Allocating Licenses

ZENworks Asset Management lets you allocate licenses within your organization to track ownership and distribution of the licenses. You can allocate licenses to devices or demographics (sites, departments, and cost centers).

A *device allocation* is the assignment of a license to a specific device. The device can have the product installed or not installed. For example, you purchase 10 licenses of ProductA. You can allocate the licenses to the target devices before ProductA is even installed on the devices.

A *demographic allocation* is the assignment of one or more licenses to a site, department, or cost center. Any device that is assigned the demographic and has the product installed shows up as an installation associated with the allocation. For example, you purchase 15 licenses of ProductA and allocate them to DepartmentQ. There are 20 devices assigned to DepartmentQ. Of those 20 devices, 12 have ProductA installed. The result is that the DepartmentQ allocation shows 15 allocated licenses with 12 installations.

The following steps explain how to allocate licenses to devices. For information about allocating licenses to demographics, see “[License Allocation](#)” in the [ZENworks 2017 Asset Management Reference](#).

- 1 In ZENworks Control Center, click the **Asset Management** tab.
- 2 On the License Management page, click **Licensed Products**.
- 3 In the Licensed Products list, click the licensed product for which you want to allocate licenses.
- 4 By default, only device allocation is enabled to track ownership for product licenses. To allocate licenses to demographics, a user has to perform the following steps to enable demographic allocation for the product:
 - 4a Click the **General** tab.
 - 4b In the License Allocation Settings panel, fill in the following fields:
 - Enable demographic allocations:** Select this option.
 - Demographic allocation type:** All demographic allocations for a single licensed product must be of the same type. Select the type (**Site**, **Department**, **Cost Center**) you want to use for this product.
 - Update license allocations with demographic data from future purchase record imports:** Select this option if, when importing future purchase records for the product, you want to automatically update the allocated license quantity based on the purchase record’s demographic data.

For example, assume that the product is using Department allocations. You import a purchase record that includes licenses assigned to DepartmentQ. The licenses are added as a DepartmentQ demographic allocation.

Also creates new allocations if necessary. For example, if a purchase record includes ProductA licenses that are assigned to a DepartmentZ (a new department not listed in ProductA's allocations), a new allocation for DepartmentZ is created.

Allocated Quantity: Displays the total number of allocated licenses, either to devices or to demographics.

- 4c Click **Apply** to save any changes.
 - 5 Click the **License Allocations** tab.
 - 6 (Optional) To see which devices have the product installed but do not have an allocated license, click the **Installations with no allocations** number in the Device Allocations panel.
 - 7 Click **Add > Devices with Product Installed** if the device you want to allocate a license to has the product installed.
or
Click **Add > Any Devices** if the device you want to allocate a license to does not have the product installed.
- The Search for Device dialog box is displayed.
- 8 In the **Device Type** field, select whether you want to search **Managed Devices**, **Inventoried Devices**, **Managed or Inventoried Devices**, **ZAM Migrated Devices**, or **All**.
If you are not sure of the device type, select **All**.
 - 9 To limit the search, use the filters to create the search criteria.
If you don't create filters, all devices (or all devices with the product installed) are displayed, up to the maximum display number.
 - 10 Specify the maximum number of devices you want the search to display.
 - 11 Select the columns you want displayed in the resulting search dialog box. Control-click to select multiple fields.
 - 12 Click **Search** to display a Select Device dialog box that lists the search results.
 - 13 Select the devices you want to allocate licenses to, then click **OK**.

The following information is provided for the allocation:

- ◆ **Machine Name, Login Name, and IP Address:** Standard information about the device, including the login name of the user who was logged in at the time the device was inventoried.
- ◆ **Site, Department, Cost Center:** Demographic data about the device. If one or more of the fields is empty, the device's inventory data does not contain that information.
- ◆ **Installed Quantity:** The number of installations of the licensed product on the device. This should typically be 1.
- ◆ **Duplicate Allocation:** Includes a check mark if the device's installation is also included in a demographic allocation.
- ◆ **Installations with No Allocations:** Displays the number of installations that are not allocated a license either through a demographic allocation or a device allocation. Click the number to display the list of installations.

9 Configuration Management

The following sections provide explanations and instructions for the tasks you can perform with ZENworks Configuration Management. Depending on your environment and the functionality you plan to use, you might not need to know how to perform all tasks. For the ones you decide to learn about, you can review them in any order.

For more information on the Mobile Management component of ZENworks, see [“Mobile Management” on page 111](#).

- ◆ [“Activating Configuration Management” on page 73](#)
- ◆ [“Enabling Configuration Management in the ZENworks Agent” on page 73](#)
- ◆ [“Distributing Software” on page 74](#)
- ◆ [“Applying Policies” on page 75](#)
- ◆ [“Imaging Devices” on page 77](#)
- ◆ [“Remotely Managing Devices” on page 85](#)
- ◆ [“Collecting Software and Hardware Inventory” on page 93](#)
- ◆ [“Linux Management” on page 94](#)

Activating Configuration Management

If you did not activate Configuration Management during installation of the Management Zone, either by providing a license key or by turning on the evaluation, complete the following steps:

- 1 In ZENworks Control Center, click **Configuration**.
- 2 In the Licenses panel, click **ZENworks 2017 Configuration Management**.
- 3 Select Evaluate/Activate product, then fill in the following fields:
 - Use Evaluation:** Select this option to enable a 60-day evaluation period. After the 60-day period, you must apply a product license key to continue using the product.
 - Product License Key:** Specify the license key you purchased for Configuration Management. To purchase a product license, see the [Novell ZENworks Configuration Management product site \(http://www.novell.com/products/zenworks/configurationmanagement\)](http://www.novell.com/products/zenworks/configurationmanagement).
- 4 Click **OK**.

Enabling Configuration Management in the ZENworks Agent

For the ZENworks Agent to perform Configuration Management operations on a device, the appropriate agent features must be enabled. These features (Bundle Management, Image Management, Policy Management, Remote Management, and User Management) are enabled by default when ZENworks Configuration Management is activated (full license or evaluation).

You should verify that the features are enabled. Or, if you don't want to use certain features, you can disable them. For instructions, see [“Configuring ZENworks Agent Features” on page 35](#).

Distributing Software

ZENworks Configuration Management provides great flexibility in distributing software. You can distribute applications and individual files; simply make modifications to existing files on a device; install, remove, and roll back applications on your devices.

Software is distributed through the use of bundles. A bundle consists of all the files, configuration settings, installation instructions, and so forth required to deploy and manage the application or files on a device. When you assign a bundle to a device, you can install and launch it on the device according to the schedules (distribution, launch, and availability) that you define.

There are four types of bundles you can create:

- ♦ **iOS Bundle:** Allows you to configure and manage applications on iOS devices.
- ♦ **Linux Bundle:** Allows you to configure and manage applications on Linux devices.
- ♦ **Linux Dependency Bundle:** Allows the software packages to be available on Linux devices to resolve package dependencies.
- ♦ **Macintosh Bundle:** Allows you to configure and manage applications on Macintosh devices.
- ♦ **Preboot Bundle:** Allows you to perform a set of tasks on a managed or unmanaged device before the operating system boots up on the device.
- ♦ **Windows Bundle:** Allows you to configure and manage applications on Windows devices.

The software included with a bundle is uploaded to the ZENworks Server repository. This enables the ZENworks Server to distribute the software without requiring access to any other network locations.



Watch the following videos to learn about distributing software to Windows, Linux, and Macintosh devices:

- ♦ [Deploying Windows Software with ZENworks](#)
 - ♦ [Deploying Linux Software with ZENworks](#)
 - ♦ [Mac Management with ZENworks: Agent Deployment](#)
 - ♦ [Mac Management with ZENworks: Standardized Application Deployment](#)
-

Creating a Bundle

To create a software bundle, you use the Create New Bundle Wizard. In addition to helping you create the bundle, the wizard also lets you assign it to devices and users and create distribution, launch, and availability schedules.

- 1 In ZENworks Control Center, click the **Bundles** tab.
- 2 In the Bundles panel, click **New > Bundle** to launch the Create New Bundle Wizard.
- 3 Follow the prompts to create the bundle.

Click the **Help** button on each wizard page for detailed information about the page.

When you complete the wizard, the bundle is added to the Bundles panel. You can click the bundle to view and modify the bundle's details.

- 4 Continue with the next section, [Assigning a Bundle](#).

You can also use the `bundle-create` command in the `zman` utility to create a software bundle. For more information, see "[Bundle Commands](#)" in the *ZENworks Command Line Utilities Reference*.

Assigning a Bundle

After you create a bundle, you need to assign it to the devices where you want it installed. You can make assignments to devices or to users.

- 1 In the Bundles panel, select the bundle you want to assign by selecting the check box next to it.
- 2 Click **Action > Assign to Device**.

or

Click **Action > Assign to User**.

- 3 Follow the prompts to assign the bundle.

Click the **Help** button on each wizard page for detailed information about the page.

When you complete the wizard, the assigned devices or users are added to the bundle's Relationships page. You can click the bundle to view the assignments.

You can also use the `bundle-assign` command in the `zman` utility to assign a bundle. For more information, see “[Bundle Commands](#)” in the *ZENworks Command Line Utilities Reference*.

Where to Find More Information

For more information about distributing software, see the *ZENworks Software Distribution Reference*.

Applying Policies

ZENworks Configuration Management lets you use policies to create a set of configurations that can be assigned to any number of managed devices. It helps you to provide the devices with a uniform configuration, and it eliminates the need to configure each device separately.

ZENworks Configuration Management policies help you manage the external services, puppet policy related settings, Internet Explorer favorites, Windows Group policies, local file rights, A/C Power Management settings, printers, SNMP service settings, roaming profiles, and configure dynamic local user accounts and manage them on the managed devices. You can also configure the behavior or execution of a Remote Management session on the managed device, and administer as well as centrally manage the behavior and features of ZENworks Explorer.

The following section contains the list of Windows Configuration policies that can be created and assigned to a user or a managed device.

- ♦ **Browser Bookmarks Policy:** Configures Internet Explorer favorites for Windows devices and users.
- ♦ **Dynamic Local User Policy:** Configures users created on Windows XP, Windows Vista, Windows 7 workstations; and Windows 2003, Windows 2008, Windows 2008 R2 Terminal Servers after the users have successfully authenticated to Novell eDirectory.
- ♦ **Local File Rights Policy:** Configures rights for files or folders that exist on the NTFS file systems.

The policy can be used to configure basic and advanced permissions for both local and domain users and groups. It provides the ability for an administrator to create custom groups on managed devices.

- ♦ **Power Management Policy:** Configures Power Management settings on the managed devices.



Watch a [video](#) that demonstrates how to use configure a Power Management policy.

- ♦ **Printer Policy:** Configures Local, SMB, HTTP, TCP/IP, CUPS, and iPrint printers for Windows devices and users.
- ♦ **Remote Management Policy:** Configures the behavior or execution of a Remote Management session on a managed device. The policy includes properties such as Remote Management operations, security, and so forth. A Remote Management policy can be assigned to users as well as managed devices.
- ♦ **Roaming Profile Policy:** Allows the user to configure the path where his or her user profile should be stored.

A user profile contains information about a user's desktop settings and personal preferences, which are retained from session to session.

Any user profile that is stored in a network path is known as a roaming profile. Every time the user logs on to a machine, his or her profile is loaded from the network path. This helps the user to move from machine to machine and still retain consistent personal settings.

- ♦ **SNMP Policy:** Configures SNMP parameters on the managed devices.
- ♦ **Windows Group Policy:** Configures Group Policy for Windows devices and users.
- ♦ **ZENworks Explorer Configuration Policy:** Allows you to administer and centrally manage the behavior and features of ZENworks Explorer.

The following section contains the list of Linux Configuration policies that can be created and assigned to a user or a managed device.

- ♦ **External Services Policy:** Configures the external services on a Linux-managed device for the YUM, ZYPP or MOUNT repositories. It provides the ability for an administrator to download and install software packages or updates from these repositories, on the managed devices.
- ♦ **Puppet Policy:** Specifies how to run puppet manifests and modules on a managed device, upload the script files, and specifies if a dry run of the script should be performed on the device.

The following section lists the policies that are applicable for mobile devices enrolled in the zone.

- ♦ **Mobile Device Control Policy:** Enables you to allow or restrict users from accessing the various features of a mobile device.
- ♦ **Mobile Email Policy:** Enables you to manage the corporate email account on mobile devices.
- ♦ **Mobile Enrollment Policy:** Enforces which users can enroll their mobile devices, what mobile devices the users can enroll, the mode to be used for mobile device enrollment, and the location and naming of the device.
- ♦ **Mobile Security Policy:** Configures the password restrictions, encryption settings, and device inactivity settings on devices.

Creating a Policy

To create a policy, you use the Create New Policy Wizard. In addition to helping you create the policy, the wizard also lets you assign it to devices and users and decide whether to enforce the policy immediately or wait until the device refreshes its information.

- 1 In ZENworks Control Center, click the **Policies** tab.
- 2 In the Policies panel, click **New > Policy** to display the Select Platform page.
- 3 Select the policy category, then click **Next** to display the Select Policy Category page.
- 4 Select the category of policy you want to create, then click **Next**.
- 5 Select a Policy Type from the list of policies provided. Follow the on-screen prompts to create the policy.

Click the **Help** button on each wizard page for detailed information about the page.

When you complete the wizard, the policy is added to the Policies panel. You can click the policy to view the policy's details and modify assignments.

You can also use the `policy-create` command in the `zman` utility to create a policy. For more information, see “[Policy Commands](#)” in the *ZENworks Command Line Utilities Reference*.

Assigning a Policy

After you create a policy, you need to assign it to the devices where you want it applied. You can make assignments to devices or to users.

- 1 In the Policies panel, select the policy you want to assign by selecting the check box next to it.
- 2 Click **Action > Assign to Device**.

or

Click **Action > Assign to User**.

- 3 Follow the prompts to assign the policy.

Click the **Help** button on each wizard page for detailed information about the page.

When you complete the wizard, the assigned devices or users are added to the policy's Relationships page. You can click the policy to view the assignments.

You can also use the `policy-assign` command in the `zman` utility to assign a policy. For more information, see “[Policy Commands](#)” in the *ZENworks Command Line Utilities Reference*.

Where to Find More Information

For more information about applying policies, see the *ZENworks Configuration Policies Reference*.

Imaging Devices

ZENworks Configuration Management includes a preboot service that enables you to perform tasks on devices before their operating systems boot up. Using Preboot Services, you can automatically or manually do the following to a device when it boots up:

- ♦ Run ZENworks imaging scripts containing any commands that you can issue at the bash prompt
- ♦ Take an image of the device's hard drives and other storage devices
- ♦ Restore an image to the device
- ♦ Take part in a session where an existing image is applied to multiple devices via multicast
- ♦ Take or restore a WIM image by using ImageX
- ♦ Take or restore a Ghost image by using Symantec Ghost

To accomplish some of these tasks automatically, you simply need to have PXE (Preboot Execution Environment) enabled on your devices, then configure prebootable tasks in ZENworks Control Center and assign them to the devices. Then, the devices can automatically implement these tasks when they boot.

To manually implement the tasks, you can configure devices to require user intervention during bootup.

Using ZENworks Control Center, you can also replicate the `tftp` directory changes from a Primary Server to other Imaging servers (Primary Server or Satellite device with the Imaging role).

- ◆ [“Setting Up Preboot Services” on page 78](#)
- ◆ [“Taking an Image” on page 81](#)
- ◆ [“Applying an Image” on page 82](#)
- ◆ [“Where to Find More Information” on page 85](#)

Setting Up Preboot Services

To use Preboot Services, you need to complete the tasks in the following sections:

- ◆ [“Enabling PXE on a Device” on page 78](#)
- ◆ [“Setting Up an Imaging Server” on page 78](#)
- ◆ [“Configuring the Third-Party Imaging Settings” on page 78](#)
- ◆ [“Configuring Third Party NTFS Driver Settings” on page 80](#)

Enabling PXE on a Device

Preboot Services requires PXE (Preboot Execution Environment) to be enabled on any managed device where you want to take or apply an image.

To check if PXE is enabled on a device, restart the device and select the boot option (F12 on most devices). PXE is enabled if there is a network boot option.

If PXE is not enabled on a device, edit the device BIOS to enable it. In order to ensure that the PXE environment is available each time the device starts, you can also change the boot order so that the NIC (Network Interface Card) option is listed before the other boot options.

Setting Up an Imaging Server

The Imaging Server is the PXE server that a device’s PXE engine connects to. To enable a ZENworks Server to function as an Imaging Server, you simply need to start the Novell Proxy DHCP Service on the ZENworks Server. When you start the service, you should also change the startup type from Manual to Automatic so that it starts whenever the server reboots.

Configuring the Third-Party Imaging Settings

If you want to use the third-party imaging solutions, you must configure the Third-Party Imaging Settings in ZENworks Control Center. ZENworks supports the following third-party imaging tools:

- ◆ Microsoft ImageX that uses the WIM image file format and WINPE as the distro
- ◆ Symantec Ghost that uses the Ghost image file format and WINPE as the distro

The ZENworks third-party Imaging supports only PXE as the boot mechanism.

To configure the Third-Party Imaging settings:

- 1 Install ZENworks Configuration Management on your Imaging Server.

For more information on how to install ZENworks 2017, see [“Installing a ZENworks Primary Server on Windows”](#) in the *ZENworks Server Installation Guide*.


2 Configure the third-party Imaging settings in ZENworks Control Center.

2a Ensure that Microsoft Windows Automated Installation Kit (WAIK) or Windows Assessment and Deployment Kit (WADK) is installed on the device running ZENworks Control Center.

2b In ZENworks Control Center, click **Configuration** tab.

2c In the **Management Zone Settings** panel, click **Device Management > Preboot Services > the Third Party Imaging Settings** panel.

2d For **32 Bit Upload Settings**:

Upload WinPE Base Distribution (Requires Windows AIK / Windows ADK): Click the  icon to upload the WIM Imaging file. In the Upload WIM Imaging Files dialog box, do the following:

1. To upload a 32-bit `winpe.wim` file:

From WAIK: Browse to the `Windows AIK\Tools\PETools\x86` folder under the installed directory, then select the `winpe.wim` file.

From WADK: Browse to the `Windows Kits\<version>\Assessment and Deployment Kit\Windows Preinstallation Environment\x86\en-us` folder under the installed directory, then select the `winpe.wim` file.


Where `<version>` is a Windows Operating System version.

NOTE: Re-uploading the `winpe.wim` file overwrites the previous instance of this file from the server.

2. Click **OK**.

This downloads the imaging files from the server to the device where you access ZENworks Control Center and rebuilds `winpe.wim` with imaging files and then uploads files from the device to the server. The progress of the download and upload files is displayed in the **Status** field.

Upload ImageX Files to Support WIM Imaging (ImageX.exe):


1. Click the  icon to browse for and select the Microsoft Imaging engine (`imagex.exe`) on the device where you can access ZENworks Control Center.

2. After configuring the third-party imaging settings, click **Apply**.

3. Click **Status** to view the status of content replication across all Primary Servers and Satellites with the Imaging role in the management zone. Ensure that you start the Imaging operation only when the status is Available.

NOTE: If you are uploading both 32-bit and 64-bit ImageX files, ensure that you do so in different instances.


Upload Ghost 11.5 or Higher Files to Support Ghost Imaging (Ghost32.exe):

1. Click the  icon to browse for and select the Symantec GHOST engine (`ghost32.exe`) on the device from where you can access the ZENworks Control Center.

2. After configuring the third-party imaging settings, click **Apply**.

3. Click **Status** to view the status of content replication across all Primary Servers and Satellites with the Imaging role in the management zone. Ensure that you start the Imaging operation only when the status is Available.

2e For **64 bit Upload Settings**:

Upload WinPE Base Distribution (Requires Windows AIK / Windows ADK): Click the  icon to upload the WIM Imaging file. In the Upload WIM Imaging Files dialog box, do the following:


1. To upload a 64-bit `winpe.wim` file from WADK, browse to `Windows Kits\<version>\Assessment and Deployment Kit\Windows Preinstallation environment\amd64\en-us` folder under the installed directory, then select the `winpe.wim` file.

Where `<version>` is a Windows Operating System version.

2. Click **OK**.


This downloads the imaging files from the server to the device where you access ZENworks Control Center and rebuilds `winpe.wim` with imaging files and then uploads files from the device to the server. The progress of the download and upload files is displayed in the **Status** field.

Upload ImageX Files to Support WIM Imaging (ImageX.exe):

1. Click the  icon to browse for and select the Microsoft Imaging engine (`imagex.exe`) on the device where you can access ZENworks Control Center.
2. After configuring the third-party imaging settings, click **Apply**.
3. Click **Status** to view the status of content replication across all Primary Servers and Satellites with the Imaging role in the management zone. Ensure that you start the Imaging operation only when the status is Available.

NOTE: If you are uploading both 32-bit and 64-bit ImageX files, ensure that you do so in different instances.

Upload Ghost 11.5 or Higher Files to Support Ghost Imaging (Ghost64.exe):

1. Click the  icon to browse for and select the Symantec GHOST engine (`ghost64.exe`) on the device from where you can access the ZENworks Control Center.
 2. After configuring the third-party imaging settings, click **Apply**.
 3. Click **Status** to view the status of content replication across all Primary Servers and Satellites with the Imaging role in the management zone. Ensure that you start the Imaging operation only when the status is Available.
- 3 Enable PXE on the device.
 - 4 Ensure that you have a standard DHCP server, either on your Imaging Server or on another network server.

Configuring Third Party NTFS Driver Settings

You can download the latest high performance NTFS driver and save it on your system. You can view content replication status across all Primary and Satellite Servers with the Imaging role in the management zone. You can start the Imaging operation by using the Third Party NTFS driver when the status is Available.

To configure these settings, click **Configuration** in the left pane to display the **Configuration** tab. If it's not expanded, click **Management Zone Settings**, then click **Device Management > Preboot Services** to display the Preboot Services page.


Taking an Image



You can take and restore ZENworks images on a device by using ZENworks Imaging and third-party images by using the ZENworks Third-Party Imaging utility. This utility allows you to take an image and restore it on a local device or server by using Windows Imaging format (WIM) or Ghost Imaging format.

- 1 In ZENworks Control Center, click the **Devices** tab.
- 2 Navigate the **Servers** or **Workstations** folder until you locate the device whose image you want to take.
- 3 Click the device to display its details.
- 4 In the task list located in the left navigation pane, click **Take an Image** to launch the Take an Image Wizard.
- 5 On the File Information page, fill in the following fields, then click **Next**.

For ZENworks imaging, specify the following:

Image Format: Select the format of the image to be taken for the device

Server and File Path: Click the  icon to display the Server and Path Information dialog box. Configure the following options.

- ♦ **Server Object/IP/DNS:** Click the  icon to browse for and select the object, IP address, or DNS name of the Primary Server or the device that is promoted to the Imaging Server role.
- ♦ **File Path on Server:** Click the  icon to browse for and select an image file. The image file must have the `.zmg` filename extension, meaning it is a valid ZENworks image file.


NOTE: You cannot browse to the specified file system if multiple search domains with DHCP are configured for Linux and if the server is on Windows.

For Third-Party Imaging, specify the following:

Shared Network Path for Image File: Specify the shared-network path where you want to save the `.wim` or `.gho` files. The directory must be a Windows share or a Linux SMB or CIFS share.

If you have not installed the Novell File Upload extension on this device, you must do so before you can browse to and upload directories to be installed.

Image Filename: Specify the filename to save the `.wim` or the `.gho` file. This option is displayed only for the Windows Imaging Format (`.wim`) and Ghost Imaging Format (`.gho`).

Network Credential: Click  to browse for and select the network credentials to be used for accessing the device having `.wim` files. This option is displayed only for the Windows Image Format (`.wim`) and Ghost Image Format (`.gho`).

Use Compression: Compression is required. Choose one of the following:

- ♦ **Balanced:** Automatically balances compression between an average of the reimaging speed and the available disk space for the image file. This option is displayed only for the ZENworks Image format
- ♦ **None:** This option is displayed only for the Windows Image format and Ghost Image format.
- ♦ **Optimize for Speed:** Optimizes the compression to allow for the fastest reimaging time. Use this option if CPU speed is an issue.
- ♦ **Optimize for Space:** Optimizes the compression to minimize the image file's size to conserve disk space. This can cause reimaging to take longer.

Balanced is the default option for the ZENworks Image format and **Optimize for Speed** is the default option for the Windows Image format and Ghost Image format.

Create an Image Bundle: Leave this field deselected.

- 6 Review the information on the Image File Summary page, click **Finished**, then click **OK**.

Because imaging tasks are completed by Preboot Services, the image of the device is taken the next time the device reboots. The Imaging Work panel, located on the device's Summary page, shows that the work is scheduled. When the work is completed, the task is removed from this panel.

- 7 To reboot the device immediately and initiate the imaging work, click **Reboot/Shutdown Workstation** (or **Reboot/Shutdown Server**) in the left navigation panel.

The time required to take the image depends on the size of the device's drives.

Applying an Image

To apply an image to a device, you use the Create New Bundle Wizard to create an Imaging bundle. The bundle contains the image you want to apply. In addition to helping you create the bundle, the wizard also lets you assign it to devices. After creating the Imaging bundle, you then initiate the imaging work.

- ♦ [“Creating the ZENworks Image Bundle” on page 82](#)
- ♦ [“Creating the Third-Party Image Bundle” on page 83](#)
- ♦ [“Initiating the Imaging Work” on page 84](#)



Watch the following videos to learn about deploying Windows 7 images and Linux images to devices:


- ♦ [Deploying Windows 7 Image with ZENworks](#)
 - ♦ [Deploying Linux with ZENworks](#)
-

Creating the ZENworks Image Bundle

To restore ZENworks images on a device, you must create the ZENworks Image bundle.

- 1 In ZENworks Control Center, click the **Bundles** tab.
- 2 In the Bundles panel, click **New > Bundle** to launch the Create New Bundle Wizard.
- 3 On the Select Bundle Type page, select **Preboot Bundle**, then click **Next**.
- 4 On the Select Bundle Category page, select **ZENworks Image**, then click **Next**.
- 5 Complete the wizard using information from the following table to fill in the fields.

Wizard Page	Details
Define Details page	Specify a name for the task. The name cannot include any of the following invalid characters: <code>\/ * ? : " ' < > ` % ~</code>


Wizard Page	Details
Select ZENworks Image File page	<p>To select the image file:</p> <ol style="list-style-type: none"> 1. Click  to display the Server and Path Information dialog box. 2. Fill in the following fields: <ul style="list-style-type: none"> Device Object, IP, or DNS: Select the ZENworks Server where you stored the image. File Path on Server: Browse for and select the image file. The standard storage directory for image files is <code>\Novell\ZENworks\work\content-repo\images</code>. 3. Click OK.
Summary page	Click Next to continue with the wizard and assign the bundle to the target device.
Bundle Groups page	You should not assign the image bundle to any groups. Click Next to bypass this page.
Add Assignments page	Select the device where you want to apply the image.
Schedules page	You should not assign a schedule to the image bundle. Click Next to bypass this page.
Finish page	Click Finish to create the bundle and assign it to the selected device.

Creating the Third-Party Image Bundle

To restore the third-party images, you must create the Third-Party Image bundle.

- 1 In ZENworks Control Center, click the **Bundles** tab.
- 2 In the Bundles panel, click **New > Bundle** to launch the Create New Bundle Wizard.
- 3 On the Select Bundle Type page, select **Preboot Bundle**, then click **Next**.
- 4 On the Select Bundle Category page, select **Third-Party Image**, then click **Next**.
- 5 Complete the wizard using information from the following table to fill in the fields.

Wizard Page	Details
Define Details page	Specify a name for the task. The name cannot include any of the following invalid characters: <code>/ \ * ? : " ' < > ` % ~</code>

Wizard Page	Details
Select a Third-Party Image File page	<p>To select a third-party image file:</p> <ol style="list-style-type: none"> 1. Select the type of the image to be used in the bundle. In ZENworks Configuration Management, only the Windows Image Format (.wim) and GHOST Image Format (.gho) are available. 2. Specify the shared-network directory containing the .wim or .gho files. The directory must be a Windows share or a Linux SMB or CIFS share. 3. Click  to browse for and select the network credentials to be used for accessing the device having .wim or .gho files. 4. If you want to use the WIM bundle as an Add-on image, select Restore WIM as Add-on, and configure the following options: Image Number (WIM Only): Select the index number of the image to be restored. Path to Restore the Add-on Image: Specify the location on the device where you want to restore the Add-on image. 5. Click OK.
Summary page	Click Next to continue with the wizard and assign the bundle to the target device.
Bundle Groups page	You should not assign the image bundle to any groups. Click Next to bypass this page.
Add Assignments page	Select the device where you want to apply the image.
Schedules page	You should not assign a schedule to the image bundle. Click Next to bypass this page.
Finish page	Click Finish to create the bundle and assign it to the selected device.

Initiating the Imaging Work

- 1 In ZENworks Control Center, click the **Devices** tab.
- 2 Navigate the **Servers** or **Workstations** folder until you locate the device where you want to apply the image.
- 3 Click the device to display its details.
- 4 In the task list located in the left navigation pane, click **Apply Assigned Imaging Bundle** to schedule the work.

Because imaging tasks are completed by Preboot Services, the image is applied to the device the next time the device reboots. The Imaging Work panel, located on the device's Summary page, shows that the work is scheduled. When the work is completed, the task is removed from this panel.

- 5 To reboot the device immediately and initiate the imaging work, click **Reboot/Shutdown Workstation** (or **Reboot/Shutdown Server**) in the left navigation panel.

Where to Find More Information

For more information about imaging and Preboot Services, see the [ZENworks Preboot Services and Imaging Reference](#).

Remotely Managing Devices

ZENworks Configuration Management provides Remote Management functionality that lets you remotely manage devices. Remote Management supports the following operations:

Remote Operation	Description	Additional Details
Remote Control	Lets you control a managed device from the management console so you can provide user assistance and help resolve problems. You can perform all the operations that a user can perform on the device.	
		<p>For more information on Remote Controlling a Windows device, see “Performing Remote Control, Remote View, and Remote Execute Operations on a Windows Device” on page 88.</p> <p>For more information on Remote Controlling a Linux device, see “Performing Remote Control, Remote View, and Remote Login Operations on a Linux Device” on page 92.</p>
Remote View	Lets you connect with a managed device so that you can view the managed device instead of controlling it. This helps you troubleshoot problems that the user encountered.	
		<p>For example, you can observe how the user at a managed device performs certain tasks to make sure that the user performs a task correctly</p> <p>For more information on Remotely Viewing a Windows device, see “Performing Remote Control, Remote View, and Remote Execute Operations on a Windows Device” on page 88.</p> <p>For more information on Remotely Viewing a Linux device, see “Performing Remote Control, Remote View, and Remote Login Operations on a Linux Device” on page 92.</p>

Remote Operation	Description	Additional Details
Remote Execute	<p>Lets you run any executable on a managed device from the management console. To remotely execute an application, specify the executable name in the Remote Execute dialog box. If the application is not in the system path on the managed device, then provide the complete path of the application.</p> <p>For example, you can execute the <code>regedit</code> command to open the Registry Editor on the managed device. The Remote Execute dialog box displays the status of the command execution.</p> <p>For more information on Remotely Executing a Windows device, see “Performing Remote Control, Remote View, and Remote Execute Operations on a Windows Device” on page 88.</p>	This operation is supported only on a Windows managed device.
Remote Diagnostics	<p>Lets you diagnose and analyze the problems on a managed device. This helps you to shorten problem resolution times and assist users without requiring a technician to physically visit the problem device. This increases user productivity by keeping desktops up and running.</p> <p>For more information on Remote Diagnosis of a device, see “Performing a Remote Diagnostic Operation” on page 90.</p>	This operation is supported only on a Windows managed device.
File Transfer	<p>Lets you to transfer files between the management console and a managed device.</p> <p>For more information on File Transfer operation, see “Performing a File Transfer Operation” on page 91.</p>	This operation is supported only on a Windows managed device.
Remote Login	<p>Lets you log in to a managed device from the management console and start a new graphical session without disturbing the user on the managed device; however, the user on the managed device cannot view the Remote Login session.</p> <p>For more information on Remotely Logging a Linux device, see “Performing Remote Control, Remote View, and Remote Login Operations on a Linux Device” on page 92.</p>	<p>This operation is supported only on a Linux managed device.</p> <p>You must log into the device with a non-<code>root</code> user credentials.</p>
Remote SSH	<p>Lets you securely connect to a remote Linux device and safely execute commands on the device.</p> <p>For more information on Remotely Logging a Linux device, see “Performing Remote SSH Operation on a Linux Device” on page 93</p>	This operation is supported only on a Linux managed device.

The following sections explain how to set up Remote Management and perform each of the operations:

- ◆ [“Creating a Remote Management Policy”](#) on page 87
- ◆ [“Configuring Remote Management Settings”](#) on page 88
- ◆ [“Performing Remote Control, Remote View, and Remote Execute Operations on a Windows Device”](#) on page 88

- ◆ “Performing a Remote Diagnostic Operation” on page 90
- ◆ “Performing a File Transfer Operation” on page 91
- ◆ “Performing Remote Control, Remote View, and Remote Login Operations on a Linux Device” on page 92
- ◆ “Performing Remote SSH Operation on a Linux Device” on page 93
- ◆ “Where to Find More Information” on page 93



Watch a [video](#) to learn about remote management of devices.

Creating a Remote Management Policy

By default, a secure Remote Management policy is created on the managed device when the ZENworks Agent is deployed with the Remote Management component on the device. You can use the default policy to remotely manage a device. The default policy allows you to perform all the Remote Management operations on a device. To override the default policy, you can explicitly create a Remote Management policy for the device.

You can assign a Remote Management policy to devices or users.

To create a Remote Management policy:

- 1 In ZENworks Control Center, click the **Policies** tab.
- 2 In the Policies panel, click **New > Policy** to launch the Create New Policy Wizard.
- 3 Select **Windows Configuration Policies**, then click **Next**.
- 4 Follow the prompts to create the Remote Management policy.
Click the **Help** button on each wizard page for detailed information about the page. When you complete the wizard, the policy is added to the Policies panel. You can click the policy to view the policy’s details and modify assignments, schedules, and so forth.
- 5 Assign the Remote Management policy to users and devices:
 - 5a In the Policies panel, select the check box next to the policy.
 - 5b Click **Action > Assign to Device**.
or
Click **Action > Assign to User**.
 - 5c Follow the prompts to assign the policy.
Click the **Help** button on each wizard page for detailed information about the page.
When you complete the wizard, the assigned devices or users are added to the policy’s Relationships page. You can click the policy to view the assignments.

Configuring Remote Management Settings

The Remote Management configuration settings, located on the Configuration page, let you specify settings such as the Remote Management port, session performance, and available diagnostic applications.

The settings are predefined to provide the most common configuration. If you want to change the settings:

- 1 In ZENworks Control Center, click the **Configuration** tab.
- 2 In the Management Zone Settings panel, click **Device Management > Remote Management**.
- 3 Modify the settings as desired.
Click the **Help** button on the page for detailed information about the page.
- 4 When you are finished modifying the settings, click **Apply** or **OK** to save your changes.

Performing Remote Control, Remote View, and Remote Execute Operations on a Windows Device

- 1 In ZENworks Control Center, click the **Devices** tab.
- 2 Navigate the *Servers* or *Workstations* folder until you locate the device you want to manage.
- 3 Select the device by clicking the check box in front of the device.
- 4 In the task list located in the left navigation pane, click **Remote Control Workstation** or **Remote Control Server** to display the Remote Management dialog box.
- 5 In the Remote Management dialog box, fill in the following fields:

Device: Specify the name or the IP address of the device you want to remotely manage.

Always default to IP address for all devices: Select this if you want the system to display the device IP address instead of the DNS name.

The values that you provide to access a device while performing Remote Control operation are saved in the system, when you click **OK**. Some of these values are automatically selected during subsequent Remote Control operations, depending on the device or the remote operator.

Operation: Select the type of the remote operation (Remote Control, Remote View, or Remote Execute) you want to perform on the managed device:

Authentication: Select the mode you want to use to authenticate to the managed device. The two options are:

- ♦ **Password:** Provides password-based authentication to perform a Remote Control operation. You must enter the correct password as set by the user on the managed device or as configured by the administrator in the security settings of the Remote Management policy. The password set by the user takes precedence over the password configured by the administrator.
- ♦ **Rights:** This option is available only when you select the managed device on which you want to perform the remote operation. If an administrator has already assigned Remote Management rights to you to perform the desired remote operation on the selected managed device, you automatically gain access when the session initiates.

Port: Specify the port number on which the Remote Management Agent is listening. By default, the port number is 5950.

Session Mode: Select one of the following modes for the session:

- ♦ **Collaborate:** Allows you to launch a Remote Control session and a Remote View session in collaboration mode. However, you cannot first launch a Remote View session on the managed device. If you launch the Remote Control session on the managed device, then you get all the privileges of a master Remote Operator, which include:
 - ♦ Inviting other Remote Operators to join the remote session.
 - ♦ Delegating Remote Control rights to a Remote Operator.
 - ♦ Regaining control from the Remote Operator.
 - ♦ Terminating a Remote Session.

After the Remote Control session has been established for the managed device in the Collaborate mode, the other remote sessions on the managed device are Remote View sessions.

- ♦ **Shared:** Allows more than one Remote Operator to simultaneously control the managed device.
- ♦ **Exclusive:** Allows you to have an exclusive remote session on the managed device. No other remote session can be initiated on the managed device after a session has been launched in Exclusive mode.

Session Encryption: Ensures that the remote session is secured by using SSL encryption (TLSv1 protocol).

Enable Caching: Enables caching of the remote management session data to enhance performance. This option is available only for Remote Control operation. This option is currently supported only on Windows.

Enable Dynamic Bandwidth Optimization: Enables detection of the available network bandwidth and accordingly adjusts the session settings to enhance performance. This option is available only for Remote Control operation.

Enable Logging: Logs session and debug information in the `novell-zenworks-vncviewer.txt` file. The file is saved by default on the desktop if you launch ZENworks Control Center through Internet Explorer and in the Mozilla installed directory if you launch ZENworks Control Center through Mozilla FireFox.

Route Through Proxy: Enables the remote management operation of the managed device to be routed through a proxy server. If the managed device is on a private network or is on the other side of a firewall or router that is using NAT (Network Address Translation), the remote management operation of the device can be routed through a proxy server. Fill in the following fields:

- ♦ **Proxy:** Specify the DNS name or the IP address of the proxy server. By default, the proxy server configured in the Proxy Settings panel to perform the remote operation on the device is populated in this field. You can specify a different proxy server.
- ♦ **Proxy Port:** Specify the port number on which the proxy server is listening. By default, the port is 5750.

Use the Following Key Pair for Identification: If an internal certificate authority (CA) is deployed, the following options are not displayed. If an external CA is deployed, fill in the following fields:

- ♦ **Private Key:** Click **Browse** to browse to and select the private key of the remote operator.
- ♦ **Certificate:** Click **Browse** to browse to and select the certificate corresponding to the private key. This certificate must be chained to the certificate authority configured for the zone.

The supported formats for the key and the certificate are DER and PEM.

Install Remote Management Viewer: Click on the [Install Remote Management Viewer](#) link to install the Remote Management Viewer. This link is displayed only if you are performing the Remote Management session on the managed device for the first time or if the Remote Management Viewer is not installed on the managed device.

- 6 Click **OK** to launch the session.

Performing a Remote Diagnostic Operation

- 1 In ZENworks Control Center, click the **Devices** tab.
- 2 Navigate the **Servers** or **Workstations** folder until you locate the device you want to manage.
- 3 Select the device by clicking the check box in front of the device.
- 4 In the task list located in the left navigation pane, click **Remote Diagnostics** to display the Remote Diagnostics dialog box.
- 5 In the Remote Diagnostics dialog box, fill in the following fields:

Device: Specify the name or the IP address of the device you want to remotely diagnose.

Always default to IP address for all devices: Select this if you want the system to display the device IP address instead of the DNS name.

The values that you provide to access a device while performing Remote Control operation are saved in the system when you click **OK**. Some of these values are automatically selected during subsequent Remote Control operations, depending on the device or the remote operator

Application: Select the application you want to launch on the device to remotely diagnose.

Authentication: Select the mode you want to use to authenticate to the managed device. The two options are:

- ♦ **Password:** Provides password-based authentication to perform a Remote Diagnostic operation. You must enter the correct password as set by the user on the managed device or as configured by the administrator in the security settings of the Remote Management policy. The password set by the user takes precedence over the password configured by the administrator.
- ♦ **Rights:** This option is available only when you select the managed device on which you want to perform the remote operation. If an administrator has already assigned Remote Management rights to you to perform the desired remote operation on the selected managed device, you automatically gain access when the session initiates.

Port: Specify the port number on which the Remote Management Agent is listening. By default, the port number is 5950.

Session Mode: Does not apply to the Remote Diagnostics operation.

Session Encryption: Ensures that the remote session is secured by using SSL encryption (TLSv1 protocol).

Enable Caching: Enables caching of the remote management session data to enhance performance. This option is currently supported only on Windows.

Enable Dynamic Bandwidth Optimization: Enables detection of the available network bandwidth and accordingly adjusts the session settings to enhance performance.

Enable Logging: Logs session and debug information in the `novell-zenworks-vncviewer.txt` file. The file is saved by default on the desktop if you launch ZENworks Control Center through Internet Explorer and in the Mozilla installed directory if you launch ZENworks Control Center through Mozilla FireFox.

Route Through Proxy: Enables the remote management operation of the managed device to be routed through a proxy server. If the managed device is on a private network or is on the other side of a firewall or router that is using NAT (Network Address Translation), the remote management operation of the device can be routed through a proxy server. Fill in the following fields:

- ◆ **Proxy:** Specify the DNS name or the IP address of the proxy server. By default, the proxy server configured in the Proxy Settings panel to perform the remote operation on the device is populated in this field. You can specify a different proxy server.
- ◆ **Proxy Port:** Specify the port number on which the proxy server is listening. By default, the port is 5750.

6 Click **OK** to launch the session.

Performing a File Transfer Operation

- 1 In ZENworks Control Center, click the **Devices** tab.
- 2 Navigate the **Servers** or **Workstations** folder until you locate the device you want to manage.
- 3 Select the device by clicking the check box in front of the device.
- 4 In the task list located in the left navigation pane, click **Transfer Files** to display the File Transfer dialog box.
- 5 In the File Transfer dialog box, fill in the following fields:

Device: Specify the name or the IP address of the device you want to access.

Always default to IP address for all devices: Select this if you want the system to display the device IP address instead of the DNS name. The values that you provide to access a device while performing Remote Control operation are saved in the system when you click **OK**. Some of these values are automatically selected during subsequent Remote Control operations, depending on the device or the remote operator.

Authentication: Select the mode you want to use to authenticate to the managed device. The two options are:

- ◆ **Password:** Provides password-based authentication to perform an operation. You must enter the correct password as set by the user on the managed device or as configured by the administrator in the security settings of the Remote Management policy. The password set by the user takes precedence over the password configured by the administrator.
- ◆ **Rights:** This option is available only when you select the managed device on which you want to perform the remote operation. If an administrator has already assigned Remote Management rights to you to perform the desired remote operation on the selected managed device, you automatically gain access when the session initiates.

Port: Specify the port number on which the Remote Management Agent is listening. By default, the port number is 5950.

Session Mode: Does not apply to the File Transfer operation.

Session Encryption: Ensures that the remote session is secured by using SSL encryption (TLSv1 protocol).

Enable Logging: Logs session and debug information in the `novell-zenworks-vncviewer.txt` file. The file is saved by default on the desktop if you launch ZENworks Control Center through Internet Explorer and in the Mozilla installed directory if you launch ZENworks Control Center through Mozilla FireFox. On a Linux Management Console, the file is saved in the Home directory of the logged-in user.

Route Through Proxy: Enables the remote management operation of the managed device to be routed through a proxy server. If the managed device is on a private network or is on the other side of a firewall or router that is using NAT (Network Address Translation), the remote management operation of the device can be routed through a proxy server. Fill in the following fields:

- ◆ **Proxy:** Specify the DNS name or the IP address of the proxy server. By default, the proxy server configured in the Proxy Settings panel to perform the remote operation on the device is populated in this field. You can specify a different proxy server.
- ◆ **Proxy Port:** Specify the port number on which the proxy server is listening. By default, the port is 5750.

6 Click **OK** to launch the session

Performing Remote Control, Remote View, and Remote Login Operations on a Linux Device

- 1 In ZENworks Control Center, click the **Devices** tab.
- 2 Navigate the **Servers** or **Workstations** folder until you locate the device you want to manage.
- 3 Select a Linux device by clicking the check box in front of the device.
- 4 Click **Action** > **Remote Control** to display the Remote Management dialog box.
- 5 In the Remote Management dialog box, fill in the following fields:

Device: Specify the name or the IP address of the device you want to remotely manage.

Always default to IP address for all devices: Select this if you want the system to display the device IP address instead of the DNS name.

The values that you provide to access a device while performing Remote Control operation are saved in the system when you click **OK**. Some of these values are automatically selected during subsequent Remote Control operations, depending on the device or the remote operator.

Operation: Select the type of the remote operation (Remote Control, Remote View, or Remote Login) you want to perform on the managed device:

Port: Specify the port number on which the Remote Management Agent is listening. By default, the port number is 5950 for Remote Control and Remote View operations; and 5951 for Remote Login operation.

Enable Logging: Logs session and debug information in the `novell-zenworks-vncviewer.txt` file. The file is saved by default on the desktop if you launch ZENworks Control Center through Internet Explorer and in the Mozilla installed directory if you launch ZENworks Control Center through Mozilla FireFox. On a Linux Management Console, the file is saved in the Home directory of the logged-in user.

Route Through Proxy: Enables the remote management operation of the managed device to be routed through a proxy server. If the managed device is on a private network or is on the other side of a firewall or router that is using NAT (Network Address Translation), the remote management operation of the device can be routed through a proxy server. Fill in the following fields:

- ◆ **Proxy:** Specify the DNS name or the IP address of the proxy server. By default, the proxy server configured in the Proxy Settings panel to perform the remote operation on the device is populated in this field. You can specify a different proxy server.
- ◆ **Proxy Port:** Specify the port number on which the proxy server is listening. By default, the port is 5750.

Install Remote Management Viewer: Click on the [Install Remote Management Viewer](#) link to install the Remote Management Viewer. This link is displayed only if you are performing the Remote Management session on the managed device for the first time or if the Remote Management Viewer is not installed on the managed device.

- 6 Click **OK** to launch the session.

Performing Remote SSH Operation on a Linux Device

- 1 In ZENworks Control Center, click the **Devices** tab.
- 2 Navigate the `Servers` or `Workstations` folder until you locate the device you want to manage.
- 3 Select a Linux device by clicking the check box in front of the device.
- 4 Click **Action** > **Remote SSH** to display the Remote SSH dialog box.
- 5 In the Remote SSH dialog box, fill in the following fields:

Device: Specify the name or IP address of the device you want to remotely connect to. If the device is not in the same network, you must specify the IP address of the device.

User Name: Specify the username used to log in to in the remote device. By default, it is `root`.

Port: Specify the port number of the Remote SSH service. By default, the port number is 22.

Clicking **OK** prompts you to launch Remote SSH Java Web Start Launcher. Click **Yes** to accept the certificate, then click **Run**. To continue connecting to the device, Click **Yes**. You are prompted to enter the password to connect to the managed device.

- 6 Click **OK** to launch the session.

Where to Find More Information

For more information about remotely managing devices, see the [ZENworks 2017 Remote Management Reference](#).

Collecting Software and Hardware Inventory

ZENworks Configuration Management lets you collect software and hardware information from devices. You can view the inventory for an individual device and generate inventory based on specific criteria.

For example, you want to distribute a software application that has specific processor, memory, and disk space requirements. You create two , one that lists all devices that meet the requirements and one that lists the devices that don't meet the requirements. Based on the , you distribute the software to the compliant devices and create an upgrade plan for the noncompliant devices.

By default, devices are automatically scanned at 1:00 a.m. the first day of each month. You can modify the schedule, as well as many other **Inventory** configuration settings, on the **Configuration** tab in ZENworks Control Center.

- ♦ [“Initiating a Device Scan” on page 94](#)
- ♦ [“Viewing a Device Inventory” on page 94](#)
- ♦ [“Generating an Inventory Report” on page 94](#)
- ♦ [“Where to Find More Information” on page 94](#)

Initiating a Device Scan

You can initiate a scan of a device at any time.

- 1 In ZENworks Control Center, click the **Devices** tab.
- 2 Navigate the **Servers** or **Workstations** folder until you locate the device you want to scan.
- 3 Click the device to display its details.
- 4 In the task list located in the left navigation pane, click **Server Inventory Scan** or **Workstation Inventory Scan** to initiate the scan.

The QuickTask Status dialog box displays the status of the task. When the task is complete, you can click the **Inventory** tab to view the results of the scan.

You can also use the `inventory-scan-now` command in the `zman` utility to scan a device. For more information, see “[Inventory Commands](#)” in the [ZENworks Command Line Utilities Reference](#).

Viewing a Device Inventory

- 1 In ZENworks Control Center, click the **Devices** tab.
- 2 Navigate the **Servers** or **Workstations** folder until you locate the device you want to scan.
- 3 Click the device to display its details.
- 4 Click the **Inventory** tab.

Generating an Inventory Report

ZENworks Configuration Management includes several standard . In addition, you can create custom to provide different views of the inventory information.

- 1 In ZENworks Control Center, click the **Inventory** tab.
- 2 In the **Inventory Standard** panel, click **Software Applications**.
- 3 Click the **Operating System** report to generate the report.

Using the options at the bottom of the report, you can save the generated report as a Microsoft Excel spreadsheet, CSV (comma-separated values) file, PDF file, or PDF Graph file.

Where to Find More Information

For more information about inventory, see the [ZENworks Asset Inventory Reference](#).

Linux Management

Linux Management makes it easy to embrace and extend Linux within your existing environment. It uses policy-driven automation to deploy, manage, and maintain Linux resources. The automated and intelligent policies allow you to provide centralized control across the life cycle of Linux systems for

desktop lockdown, imaging, remote management, inventory management and software management. The result is a comprehensive Linux management solution that eliminates IT effort by dramatically reducing the required overhead needed to manage Linux systems.

You can patch your Linux devices by using any of the following:

- ◆ Patch Management
- ◆ Linux Package Management

Patch Management

Patch Management is a fully integrated feature of ZENworks that provides agent-based patch, vulnerability patch, and compliance management solution.

Patch Management provides the following capabilities:

- ◆ Uses signatures to determine the required patches and them back for easy reporting.
- ◆ Implements mandatory baselines for certain patches to always be present on a device.
- ◆ Patches only the SLES and RHEL distributions.

For more information, see the [Chapter 12, “Patch Management,” on page 107](#).

Linux Package Management

Linux Package Management is intended to handle the package management functionality of ZENworks Configuration Management for Linux devices (servers and desktops).

Linux Package Management provides the following capabilities:

- ◆ Provides a single point management for patching, installing, and updating packages for large number of Linux devices in an enterprise level.
- ◆ Mirrors updates and packages from the NU, RHN, RCE, and YUM repositories for patches and packages as ZENworks bundles. You can assign these bundles to Linux managed devices for package management.
- ◆ Supports the download of delta RPMs on the managed devices whenever the delta RPMs are available and applicable, thereby reducing the bandwidth required when patching.
- ◆ Allows you to choose the catalogs, packages, and bundles that you want to mirror.
- ◆ Allows you to patch OES servers.

10 Endpoint Security Management

ZENworks Endpoint Security Management simplifies endpoint security by providing centralized management of security policies for your managed devices. You can control a device's access to removable storage devices, wireless networks, and applications. In addition, you can secure data through encryption and secure network communication via firewall enforcement (ports, protocols, and access control lists). And you can change an endpoint device's security based on its location.

The following sections explain how to use Endpoint Security Management to secure your devices whether they are in your corporate office, at home, or in a public airport terminal:

- ♦ “Activating Endpoint Security Management” on page 97
- ♦ “Enabling the Endpoint Security Agent” on page 97
- ♦ “Creating Locations” on page 98
- ♦ “Creating a Security Policy” on page 98
- ♦ “Assigning a Policy to Users and Devices” on page 100
- ♦ “Assigning a Policy to the Zone” on page 101
- ♦ “Where to Find More Information” on page 101

Activating Endpoint Security Management

If you did not activate Endpoint Security Management during installation of the Management Zone, either by providing a license key or by turning on the evaluation, complete the following steps:

- 1 In ZENworks Control Center, click **Configuration**.
- 2 In the Licenses panel, click **ZENworks 2017 Endpoint Security Management**.
- 3 Select **Evaluate/Activate product**, then fill in the following fields:
 - Use Evaluation:** Select this option to enable a 60-day evaluation period. After the 60-day period, you must apply a product license key to continue using the product.
 - Product License Key:** Specify the license key you purchased for Endpoint Security Management. To purchase a product license, see the [ZENworks Endpoint Security Management product site \(http://www.novell.com/products/zenworks/endpointsecuritymanagement\)](http://www.novell.com/products/zenworks/endpointsecuritymanagement).
- 4 Click **OK**.

Enabling the Endpoint Security Agent

The ZENworks Agent is responsible for device registration, content distribution, and software updates for a device.

In addition to the ZENworks Agent, the Endpoint Security Agent is installed on devices when ZENworks Endpoint Security Management is activated (full license or evaluation). The Endpoint Security Agent is responsible for enforcing security policy settings on the device.

You should verify that the Endpoint Security Agent is enabled. For instructions, see “[Configuring ZENworks Agent Features](#)” on page 35.

Creating Locations

Security requirements for a device can differ from location to location. For example, you might have different personal firewall restrictions for a device located in an airport terminal than for a device located in an office inside your corporate firewall.

To make sure that a device's security requirements are appropriate for whatever location it is in, Endpoint Security Management supports both global policies and location-based policies. A global policy is applied regardless of the device's location. A location-based policy is applied only when the device's current location meets the criteria for a location associated with the policy. For example, if you create a location-based policy for your corporate office and assign it to a laptop, that policy is applied only when the laptop's location is the corporate office.

If you want to use location-based policies, you must first define the locations that make sense for your organization. A location is a place, or type of place, for which you have specific security requirements. For example, you might have different security requirements for when a device is used in the office, at home, or in an airport.






Locations are defined by network environments. Assume that you have an office in New York and an office in Tokyo. Both offices have the same security requirements. Therefore, you create an Office location and associate it with two network environments: New York Office Network and Tokyo Office Network. Each of these environments is explicitly defined by a set of gateway, DNS server, and wireless access point services. Whenever the Endpoint Security Agent determines that its current environment matches the New York Office Network or Tokyo Office Network, it sets its location to Office and applies the security policies associated with the Office location.





For detailed information on how to create locations, see [“Creating Locations” on page 31](#).

Creating a Security Policy



There are 11 different security policies:

A device's security settings are controlled through security policies applied by the Endpoint Security Agent. There are eight security policies that control a range of security-related functionality. You can use all or some of the policies depending on your organization's needs.

Policy	Purpose
 Application Control	Blocks execution of applications or denies Internet access to applications. You specify the applications that are blocked or denied Internet access.
 Communication Hardware	Disables the following communication hardware: 1394-Firewire, IrDA-Infrared, Bluetooth, serial/parallel, dialup, wired, and wireless. Each communication hardware is configured individually, which means that you can disable some hardware types (for example, Bluetooth and dialup) while leaving others enabled
 Data Encryption	Enables data encryption of files on removable storage devices.
 Firewall	Controls network connectivity by disabling ports, protocols, and network addresses (IP and MAC).
 Scripting	Runs a script (JScript or VBScript) on a device. You can specify the triggers that cause the script to run. Triggers can be based on Endpoint Security Agent actions, location changes, or time intervals.

Policy	Purpose
 Storage Device Control	Controls access to CD/DVD drives, floppy drives, and removable storage drives. Each storage device type is configured individually, which means that you can disable some and enable others.
 USB Connectivity	Controls access to USB devices such as removable storage devices, printers, input devices (keyboards, mice, etc). You can specify individual devices or groups of devices. For example, you can disable access to a specific printer and enable access to all Sandisk USB devices.
 VPN Enforcement	Enforces a VPN connection based on the device's location. For example, if the device's location is unknown, you can force a VPN connection through which all Internet traffic is routed.
 Wi-Fi	Disables wireless adapters, blocks wireless connections, controls connections to wireless access points, and so forth.

In addition to the above security policies, the following security policies help protect and configure the Endpoint Security Agent. Because of the nature of these two policies, we recommend that you create and assign them first.

Policy	Purpose
 Security Settings	Protects the Endpoint Security Agent from being tampered with and uninstalled. For information about configuring the ZENworks Agent Security settings, see “Configuring ZENworks Agent Security” on page 37 .
 Location Assignment	Provides the list of allowed locations for a device or user. The Endpoint Security Agent evaluates its current network environment to see if it matches any of the allowed locations. If so, the location becomes the security location and the agent applies any security policies associated with the location. If none of the locations in the list are matched, the security policies associated with the Unknown location are applied. If you plan to use location-based policies, you should make sure a Location Assignment policy is assigned to each device or user. If a device, or the device's user, does not have an assigned Location Assignment policy, the Endpoint Security Agent cannot apply any location-based policies to the device.

To create a security policy:

- 1 In ZENworks Control Center, click **Policies** to display the Policies page.
- 2 In the Policies panel, click **New > Policy** to launch the Create New Policy Wizard.
- 3 On the Select Platform page, select **Windows**, then click **Next**.
- 4 On the Select Policy Category page, select **Windows Endpoint Security Policies**, then click **Next**.
- 5 On the Select Policy Type page, select the type of policy you want to create, then click **Next**.

If you created locations and plan to use location-based policies, you need to create at least one Location Assignment policy and assign it to devices or the devices' users. Otherwise, none of the locations you created will be available to the devices, which means that none of the location-based policies can be applied.

- 6 On the Define Details page, enter a name for the policy and select the folder in which to place the policy.
The name must be unique among all other policies located in the selected folder.
- 7 (Conditional) If the Configure Inheritance and Location Assignments page is displayed, configure the following settings, then click **Next**.
 - ♦ **Inheritance:** Leave the **Inherit from policy hierarchy** setting selected if you want to enable this policy to inherit settings from same-type policies that are assigned higher in the policy hierarchy. For example, if you assign this policy to a device and another policy (of the same type) to the device's folder, enabling this option allows this policy to inherit settings from the policy assigned to the device's folder. Deselect the **Inherit from policy hierarchy** setting if you don't want to allow this policy to inherit policy settings.
 - ♦ **Location Assignments:** Policies can be global or location-based. A global policy is applied regardless of location. A location-based policy is applied only when the device detects that it is within the locations assigned to the policy.
Select whether this is a global or location-based policy. If you select location-based, click **Add**, select the locations to which you want to assign the policy, then click **OK** to add them to the list.
- 8 Configure the policy specific settings, then click **Next** until you reach the Summary page.
For information about a policy's settings, click **Help > Current Page** in ZENworks Control Center.
- 9 On the Summary page, review the information to make sure it is correct. If it is incorrect, click the **Back** button to revisit the appropriate wizard page and make changes. If it is correct, select either of the following options (if desired), then click **Finish**.
 - ♦ **Create as Sandbox:** Select this option to create the policy as a sandbox version. The sandbox version is isolated from users and devices until you publish it. For example, you can assign it to users and devices, but it is applied only after you publish it.
 - ♦ **Define Additional Properties:** Select this option to display the policy's property pages. These pages let you modify policy settings and assign the policy to users and devices.

Assigning a Policy to Users and Devices

After you create a policy, you need to apply it to devices by assigning the policy to devices or to device users.

- 1 In the Policies panel, select the check box next to the policy you want to assign.
- 2 Click **Action > Assign to Device**.
or
Click **Action > Assign to User**.
- 3 Follow the prompts to assign the policy.
Click the **Help** button on each wizard page for detailed information about the page.
When you complete the wizard, the assigned devices or users are added to the policy's Relationships page. You can click the policy to view the assignments.

Assigning a Policy to the Zone

You can assign security policies to the Management Zone. When determining the effective policies to be enforced on a device, the Zone policies are evaluated after all user-assigned and device-assigned policies. Consider the following situations:

- ◆ No Firewall policies are assigned to a device or the device's user (either directly or through a group or folder). The Zone Firewall policy becomes the effective policy for the device and is enforced on the device.
- ◆ Firewall policies are assigned to a device and the device's user. Both policies are evaluated and merged to determine the effective Firewall policy to apply to the device. After the effective policy is determined from the user-assigned and device-assigned policies, the Zone Firewall policy is used to supply any values that 1) are unset in the effective Firewall policy and 2) are additive (such as the multi-valued Port/Protocol Rules tables).

You can define Zone policies at three levels. This enables you to assign different Zone policies to different devices within your Management Zone.

- ◆ **Management Zone:** The policies you assign at the Management Zone become the Zone policies for all devices, unless you specify different Zone policies at the device folder or device level.
- ◆ **Device Folder:** The policies you define at a device folder override the Management Zone (and any parent device folders) and become the Zone policies for all devices contained within the folder structure, unless you specify different Zone policies for a subfolder or an individual device.
- ◆ **Device:** The policies you define for an individual device override the Management Zone and device folder and become the Zone policies for the device.

The following steps provide instructions for assigning policies at the Management Zone.

- 1 In ZENworks Control Center, click **Configuration** to display the Configuration page.
- 2 In the Management Zone Settings panel, click **Endpoint Security Management**.
- 3 Click **Zone Policy Settings** to display the Zone Policy Settings page.
- 4 Click **Add**, browse for and select the policies you want to assign to the zone, then click **OK** to add them to the list.
- 5 When you are finished adding policies, click **OK**.

Where to Find More Information

For more information about ZENworks Endpoint Security Management, see the following:

- ◆ [ZENworks Endpoint Security Policies Reference](#)
- ◆ [ZENworks Endpoint Security Agent Reference](#)
- ◆ [ZENworks Endpoint Security Utilities Reference](#)
- ◆ [ZENworks Endpoint Security Scripting Reference](#)

11 Full Disk Encryption

ZENworks Full Disk Encryption protects a device's data from unauthorized access when the device is powered off or in hibernation mode. To do this, it uses a combination of disk encryption and pre-boot authentication.

Full Disk Encryption provides software-based encryption on standard, solid state, and self-encrypted hard disks. All disk volumes (or selected disk volumes) are encrypted, including any temporary files, swap files, and operating system files on the volumes. The data cannot be accessed until a valid user successfully logs in, and the data can never be accessed by booting the device from media such as a CD/DVD, floppy disk, or USB drive. For an authenticated user, accessing data on the encrypted disk is no different than accessing data on an unencrypted disk.

Full Disk Encryption provides optional pre-boot authentication for hard disks. The ZENworks Pre-Boot Authentication (PBA) component is installed as a small Linux partition on the hard disk. Login occurs through the ZENworks PBA, which is protected from alteration through the use of MDT checksums and password extraction by the use of strong encryption for the keys.

The ZENworks PBA supports single-sign on with the Windows login, enabling users to enter only one set of credentials (either user/password or smart card) to log in to both the ZENworks PBA and Windows operating system.

- ♦ [“Activating Full Disk Encryption” on page 103](#)
- ♦ [“Enabling the Full Disk Encryption Agent” on page 104](#)
- ♦ [“Creating a Disk Encryption Policy” on page 104](#)
- ♦ [“Assigning the Policy to Devices” on page 105](#)
- ♦ [“Understanding What Happens After a Policy Is Assigned to a Device” on page 105](#)
- ♦ [“Where to Find More Information” on page 106](#)

Activating Full Disk Encryption

If you did not activate Full Disk Encryption during installation of the Management Zone, either by providing a license key or by turning on the evaluation, you need to do so now.

To activate Full Disk Encryption:

- 1 In ZENworks Control Center, click **Configuration**.
- 2 In the Licenses panel, click **ZENworks 2017 Full Disk Encryption**.
- 3 Select **Evaluate/Activate product**, then fill in the following fields:
 - Use Evaluation:** Select this option to enable a 60-day evaluation period. After the 60-day period, you must apply a product license key to continue using the product.
 - Product License Key:** Specify the license key you purchased for ZENworks Full Disk Encryption. To purchase a product license, see the [ZENworks Full Disk Encryption product site \(http://www.novell.com/products/zenworks/full-disk-encryption\)](http://www.novell.com/products/zenworks/full-disk-encryption).
- 4 Click **OK**.

Enabling the Full Disk Encryption Agent

The ZENworks Agent is responsible for device registration, content distribution, and software updates for a device.

In addition to the ZENworks Agent, the Full Disk Encryption Agent is installed on devices when ZENworks Full Disk Encryption is activated (full license or evaluation). The Full Disk Encryption Agent is responsible for encrypting and decrypting disks according to the Disk Encryption policy applied to a device.

You should verify that the Full Disk Encryption Agent is enabled. For instructions, see [Configuring ZENworks Agent Features](#).

IMPORTANT: ZENworks Full Disk Encryption does not support Windows Secure Boot, and this feature must be disabled prior to the installation of the Full Disk Encryption Agent on devices. For more information about system requirements, see “[System Requirements](#)” in the [ZENworks Full Disk Encryption Agent Reference](#).

Creating a Disk Encryption Policy

Both the encryption of a device’s disks and the use of ZENworks Pre-boot Authentication (optional) are controlled through the Disk Encryption policy.

To create a Disk Encryption policy:

- 1 In ZENworks Control Center, click **Policies** to display the Policies page.
- 2 In the Policies panel, click **New > Policy** to launch the Create New Policy Wizard.
- 3 On the Select Platform page, select **Windows**, then click **Next**.
- 4 On the Select Policy Category page, select **Windows Full Disk Encryption Policies**, then click **Next**.
- 5 On the Select Policy Type page, select **Disk Encryption Policy**, then click **Next**.
- 6 On the Define Details page, enter a name for the policy and select the folder in which to place the policy.
The name must be unique among all other policies located in the selected folder.
- 7 Configure the policy specific settings, then click **Next** until you reach the Summary page.
For information about a policy’s settings, click **Help > Current Page** in ZENworks Control Center.
- 8 On the Summary page, review the information to make sure it is correct. If it is incorrect, click the **Back** button to revisit the appropriate wizard page and make changes. If it is correct, select either of the following options (if desired), then click **Finish**.
 - ♦ **Create as Sandbox:** Select this option to create the policy as a sandbox version. The sandbox version is isolated from users and devices until you publish it. For example, you can assign it to users and devices, but it is applied only after you publish it.
 - ♦ **Define Additional Properties:** Select this option to display the policy’s property pages. These pages let you modify policy settings and assign the policy to users and devices.

Assigning the Policy to Devices

After you create a Disk Encryption policy, you need to assign it to devices.

The Disk Encryption policy is a device-only policy. It can be assigned to devices and device folders. It cannot be assigned to device groups, users, user groups, or user folders.

In addition, only the policy closest to the device is applied. For example, if different policies are assigned to a device and to the device's folder, the policy that is assigned directly to the device is applied.

IMPORTANT: The Disk Encryption policy is not supported on Windows devices that use UEFI BIOS. If you assign a Disk Encryption policy to a Windows UEFI device, the policy is not applied to the device.

- 1 In the Policies panel, select the check box next to the Disk Encryption policy you want to assign.
- 2 Click **Action** > **Assign to Device**.
- 3 Follow the prompts to assign the policy.

Click the **Help** button on each wizard page for detailed information about the page.

When you complete the wizard, the assigned devices are added to the policy's Relationships page. You can click the policy to view the assignments.

Understanding What Happens After a Policy Is Assigned to a Device

After you assign a policy to a device, the policy enforcement and disk encryption workflow varies slightly if you are using pre-boot authentication. Below are the concepts for disk encryption and pre-boot authentication that you need to understand when you apply a Disk Encryption policy to a device.

Disk Encryption

ZENworks Full Disk Encryption provides software-based encryption on standard, solid state, and self-encrypted hard disks.

ZENworks Full Disk Encryption provides sector-based encryption of the entire disk or selected volumes (partitions). All files on a volume are encrypted, including any temporary files, swap files, or operating system files. Because all files are encrypted, the data cannot be accessed when booting the computer from external media such as a CD-ROM, floppy disk, or USB drive.

Compatible hard disks are any 3.5 or 2.5 inch disks that have the IDE, SATA, or PATA interface standard.

You can choose the industry-standard encryption algorithm (AES, Blowfish, DES, or DESX) and key length that best meets your organizations requirements. If the device firmware is configured for UEFI, the AES algorithm and 256 key length are automatically used.

NOTE: The cryptographic module used in ZENworks Full Disk Encryption to encrypt standard hard drives is *not* Federal Information Processing Standard (FIPS) 140-2 certified. However, the cryptographic module implements standards consistent with FIPS 140-2 Level 1 certification.

Pre-Boot Authentication

ZENworks Full Disk Encryption protects a device's data when the device is powered off or in hibernation mode. As soon as someone successfully logs in to the Windows operating system, the encrypted volumes are no longer protected and the data can be freely accessed. To provide increased login security, you can use ZENworks Pre-Boot Authentication (PBA).

The ZENworks PBA is a Linux-based component. When the Disk Encryption policy is applied to a device, a 500 MB partition containing a Linux kernel and the ZENworks PBA is created on the hard disk.

During normal operation, the device boots to the Linux partition and loads the ZENworks PBA. As soon as the user provides the appropriate credentials (user ID/password or smart card), the PBA terminates and the Windows operating system boots, providing access to the encrypted data on the previously hidden and inaccessible Windows drives.

The Linux partition is hardened to increase security, and the ZENworks PBA is protected from alteration through the use of MD5 checksums and uses strong encryption for authentication keys.

ZENworks Pre-Boot Authentication is strongly recommended. If you don't use the ZENworks PBA, encrypted data is protected only by Windows authentication.

For more information about ZENworks Pre-Boot Authentication, see the [ZENworks Full Disk Encryption PBA Reference](#)

Where to Find More Information

For more information about ZENworks Full Disk Encryption, see the following:

- ♦ [ZENworks Full Disk Encryption Policy Reference](#)
- ♦ [ZENworks Full Disk Encryption Agent Reference](#)
- ♦ [ZENworks Full Disk Encryption PBA Reference](#)
- ♦ [ZENworks Full Disk Encryption Emergency Recovery Reference](#)

12 Patch Management

Patch Management lets you apply software patches automatically and consistently to minimize vulnerabilities and issues.

Patch Management stays current with the latest patches and fixes by regular Internet communication with the ZENworks Patch Subscription Service. After the initial 60-day evaluation period, Patch Management requires a paid subscription for you to continue the daily download of the latest vulnerability and patch information.

When a new patch is available from the subscription service, a ZENworks Server downloads information about it. You can deploy the patch to devices or disregard the patch.

The following sections explain how to use ZENworks Patch Management to apply software patches automatically and consistently to devices in your Management Zone. Doing so minimizes vulnerabilities and issues that can occur with outdated or unpatched software.

- ◆ “Activating Patch Management” on page 107
- ◆ “Enabling Patch Management in the ZENworks Agent” on page 108
- ◆ “Starting the Subscription Service” on page 108
- ◆ “Creating Patch Policies” on page 108
- ◆ “Where to Find More Information” on page 109

Activating Patch Management

- 1 In ZENworks Control Center, click **Configuration**.
- 2 In the Licenses panel, click **ZENworks 2017 Patch Management**.
- 3 Select **Activate Product**, then fill in the fields:

Product Subscription Serial Number: The serial number provided to you when you purchased the subscription license. If you have not purchased a subscription license, you can enter the trial evaluation code. After the 60-day evaluation period, Patch Management requires a subscription license to continue receiving patches from the subscription service. To purchase a subscription license, see the [ZENworks Patch Management product site \(http://www.novell.com/products/zenworks/patchmanagement\)](http://www.novell.com/products/zenworks/patchmanagement).

Company Name: Your company’s name, as used to purchase the subscription license. Not required for evaluation.

Email Address: An e-mail address where you can be contacted, if necessary. Not required for evaluation.

- 4 Click **Apply**.

Enabling Patch Management in the ZENworks Agent

For the ZENworks Agent to perform Patch Management operations on a device, the agent's Patch Management feature must be enabled. The Patch Management feature is enabled by default when ZENworks Patch Management is activated (full license or evaluation).

You should verify that the agent's Patch Management feature is enabled. For instructions, see [“Configuring ZENworks Agent Features” on page 35](#).

Starting the Subscription Service

Before you can begin receiving patches, you need to start the subscription service on one of your ZENworks Servers and set the daily schedule for downloading patches.

When a new patch is available from the subscription service, a ZENworks Server downloads it automatically. The Patches page (on the **Patch Management** tab) displays the new patch, along with a description and business impact. You can deploy the patch to devices or disregard the patch.

Patch Management stays current with the latest patches and fixes by regular Internet communication with the ZENworks Patch Subscription Service. After the initial 60-day evaluation period, Patch Management requires a paid subscription to continue its daily download of the latest vulnerability and patch information.

If there are multiple ZENworks Servers in your Management Zone, you can select any one of them to be the Patch Management Server. The server that is selected as the Patch Management Server should have the best connectivity to the Internet, because it is downloading new patches and updates on a daily basis.

To start the subscription service:

- 1 In ZENworks Control Center, click the **Configuration** tab.
- 2 In the Management Zone Settings panel, click **Patch Management**, and then click **Subscription Service Information**.
- 3 In the **Start the Subscription Service** list, select the ZENworks Server that you want to run the subscription service, then click **Start Service**.

After the subscription service starts running, the **Start Service** button reads **Service Running**.

- 4 In the **Subscription Communication Interval (Every Day at)** list, select the time each day that you want patches downloaded.
- 5 Click **OK**.

Creating Patch Policies

Before you can begin deploying patches to devices, the ZENworks Agent must perform the Discover Applicable Updates (DAU) task. The DAU task allows the ZENworks Agent to detect the status (Patched, Not Patched, or Not Applicable) of each patch, depending on the devices in your network.

The patch detection cycle occurs each day at the ZENworks Server where a DAU task is scheduled for all managed devices (servers and workstations.) You can also initiate a DAU task from an individual agent. You can see the results of the patch detection scan in the Patches section under the **Patch Management** tab or the **Devices** tab of the ZENworks Server. The results are available even if a workstation is disconnected from the network.

To deploy patches, you can create patch policies or use Deploy Remediation. Patch policies automate the patch deployment process and are recommended over Deploy Remediation. You can define rules in patch policies to limit patch caching and distribution to only those patches that your devices require.

The following steps assume that one or more patches are available from the subscription service.

- 1 In ZENworks Control Center, navigate to **Patch Management > Patch Policies**.
- 2 Click **New** in the Patch Policies page.
- 3 Follow the prompts to create a patch policy.
Click the **Help** button on each page for detailed information about the page.
- 4 Click the patch policy after it is created, and select the **Relationships** page.
- 5 Click **Add** in the Relationships panel, and assign one or more devices to the policy.
- 6 Click **Publish** to distribute and apply applicable patches to the devices according to the patch policy configuration.

IMPORTANT: It is recommended that you initially apply patches to a test device before applying them to devices throughout the zone. Any devices that are configured as “Test” devices will automatically apply the patches to the assigned test devices via the Sandbox without executing Step 6 (publishing the policy).

When first creating the patch policy, you can also configure the policy to **auto approve patches after successful test enforcements**. Selecting this option in the policy configuration will automatically publish the policy to all devices assigned to the policy after 100 percent of Test devices pass (omitting the need to publish (Step 6 above)).

Where to Find More Information

For more information about configuring Patch Management, automating patch distribution across the management zone using patch policies, and using Deploy Remediation, see the [ZENworks 2017 Update 1 Patch Management Reference](#).



Mobile Management

The following sections provide information to help you enroll mobile devices in your ZENworks Management Zone.

- ◆ [Chapter 13, “Getting Started with Mobile Management,”](#) on page 113
- ◆ [Chapter 14, “Enrolling Mobile Devices,”](#) on page 115

13 Getting Started with Mobile Management

Overview

Mobile device management helps you to secure and manage any corporate or employee-owned mobile devices that are being used in the workplace. Mobile management in ZENworks uses the capabilities of ZENworks Configuration Management, which is the same management console and system infrastructure that has been managing laptops, desktops and servers over the years. By leveraging the features of ZENworks Control Center, you can perform multiple management operations on mobile devices:



- ♦ **Enroll (register) mobile devices** to your ZENworks Management Zone. Users can enroll their devices as:
 - ♦ **Fully Managed:** Android and iOS devices are supported. Full management of an Android device is enabled using the ZENworks Agent App that is installed on the device. Full management of an iOS device is enabled using the MDM profile that is installed on the device.
 - ♦ **Email Only:** Devices with native Exchange ActiveSync capabilities are supported, that is, iOS, Android, Windows, and Blackberry devices.
- ♦ **Enforce security and mobile control policies** on Android, iOS and devices with Exchange ActiveSync (EAS) capabilities (that include Windows and Blackberry devices). With a security policy, you can set password restrictions, inactivity timeout, and enforce encryption on the device. With a device control policy, you can control the use of applications such as the device camera, voice assistant, web browser, and other applications installed on the device.
- ♦ **Synchronize email** from ActiveSync servers on Android, iOS and devices with Exchange ActiveSync (EAS) capabilities (that include Windows and Blackberry devices). You can also remotely configure the default email client on iOS devices.
- ♦ **Install Apps** on iOS devices. You can distribute free App Store Apps to iOS devices using the bundles workflow in ZENworks.
- ♦ **Distribute and manage Apple VPP apps** purchased with your organization's Volume Purchase Program (VPP) account, by using the existing Bundles and Subscription workflow in ZENworks.
- ♦ **Distribute Configuration Profiles** to iOS devices to manage certain features on the device such as access to VPN and Wi-Fi.
- ♦ **Utilize Apple Device Enrollment Program (DEP) and Apple Configurator** to streamline deployment of multiple corporate owned iOS devices.


Using the Mobile Management Getting Started Page

ZENworks Control Center includes a [Getting Started with Mobile Management](#) page that guides you through the tasks that you need to complete in order to enroll and manage mobile devices in your zone.

To access the [Getting Started with Mobile Management](#) page:

- 1 In ZENworks Control Center, click **Mobile Management** (in the left navigation pane).

Each configuration task on this page includes an icon with a  or  mark indicating its completion status and one or more links to the page where you complete the task.

Additionally, you can click the  icon appearing against each task or the **Help** link provided at the top right corner of each page for information on the task.

- 2 Complete the **Configuration** tasks that are required to enroll the devices to the zone. Subsequently, you can complete the tasks listed in the **What's Next** section to manage these devices.

For more information on each of these tasks, see [ZENworks 2017 Mobile Management Reference](#).

14 Enrolling Mobile Devices

ZENworks supports enrollment through:

- ♦ **Apple Device Enrollment Program:** Applicable for DEP enabled iOS devices.
- ♦ **Apple Configurator:** Applicable for iOS devices
- ♦ **ZENworks User Portal:** Applicable for iOS and Android devices, and other devices with ActiveSync capabilities (including Windows and Blackberry devices).

Before enrolling (registering) a device to the ZENworks Management Zone, you need to understand the different ways in which ZENworks can manage a device. This will help you in evaluating the manner in which the device needs to be managed, thereby enabling you to select the right enrollment options. These enrollment options can be configured in the Mobile Device Enrollment policy that needs to be assigned to the users before their devices are enrolled.

For more information on the Mobile Management feature in ZENworks, see [ZENworks 2017 Mobile Management Reference](#).

IMPORTANT: Before enrolling the devices, you need to ensure that the ZENworks 2017 release version is deployed on all the Primary Servers within your management zone.

- ♦ [“Types of Enrollment” on page 115](#)
- ♦ [“Modes of Enrollment” on page 116](#)
- ♦ [“Enrolling an iOS DEP Device” on page 117](#)
- ♦ [“Enrolling an iOS Device through Apple Configurator” on page 118](#)
- ♦ [“Enrolling devices using the ZENworks User Portal” on page 121](#)
- ♦ [“Allowing Manual Reconciliation by User” on page 142](#)

Types of Enrollment

ZENworks lets you enroll your devices in either of the following ways:

- ♦ **Managed Device:** Enables ZENworks to fully manage a device by performing various device management operations such as apply policies to the device, deploy applications on the device, synchronize email for Exchange ActiveSync accounts, and capture device information (inventory). Only iOS or Android devices can be enrolled as fully managed devices. Full management of an Android device is performed through the ZENworks Agent App that is hosted on the Google Play Store. Full management of an iOS device is performed through the device’s in-built MDM client.

To enable ZENworks to manage the Exchange ActiveSync capabilities on these devices, you need to ensure that a Mobile Email Policy is assigned to these devices or users. This policy should use the ZENworks Server as the proxy server between the configured ActiveSync Server and the enrolled device.

In the assigned Mobile Email Policy, you also have the option to directly relay mails from the configured ActiveSync Server, however in this case, ZENworks will not manage the corporate email account configured on the device.

- ♦ **Email Only (ActiveSync Only):** Enables ZENworks to manage only the corporate email account on the device. Also, certain policies that are enforceable through the ActiveSync protocol can be applied. Mobile devices are enrolled to the ZENworks MDM Server using the ActiveSync email clients present on the devices. Android, iOS, Blackberry, and Windows devices can be enrolled as Email Only devices. Devices enrolled as Email Only devices can be managed in the following ways:
 - ♦ **Server Only Mode:** In this case, the device will be unable to send or receive emails. ZENworks can only apply certain policies that are enforceable through the ActiveSync protocol, such as the Mobile Device Control Policy and Mobile Security Policy, and can remotely wipe the devices. This might occur due to any one of the following reasons:
 - ♦ A Mobile Email Policy is not assigned to the device.
 - ♦ The assigned Mobile Email Policy does not use ZENworks as the proxy server between the configured ActiveSync Server and the device. The policy directly connects to the configured ActiveSync Server.
 - ♦ The ActiveSync server is not linked to the associated user source.
 - ♦ The ActiveSync server is not valid for the user.
 - ♦ **Proxy Mode:** In this case, corporate emails on the device will be managed by ZENworks. Also, ZENworks can apply certain policies that are enforceable through the ActiveSync protocol, such as the Mobile Device Control Policy and Mobile Security Policy, and can remotely wipe the devices. In a proxy mode, a Mobile Email Policy, with the ZENworks Server acting as the proxy server, is assigned to the device or the user.

Modes of Enrollment

As soon as you enroll your device, the mode in which the device is enrolled is displayed on the Device Information page. To access this page:

- 1 Navigate to the **Devices** section in ZCC.
- 2 Click **Mobile Devices**.
- 3 Click the relevant device.

The Device Information page displays the enrolled mode of the device.

The various enrollment modes are as follows:

- ♦ **Android App:** Indicates that as a part of full management of an Android device, the ZENworks Agent app enrollment is complete, but the corporate email account on the device is not managed by ZENworks.
- ♦ **Android App + ActiveSync:** Indicates that as a part of full management of an Android device, the ZENworks Agent app enrollment is complete and the corporate email account configured on the device is managed by ZENworks that acts as a proxy server for the configured ActiveSync Server.
- ♦ **iOS MDM:** Indicates that as a part of full management of an iOS device, the device is enrolled via the MDM client but the corporate email account on the device is not managed by ZENworks.
- ♦ **iOS MDM + ActiveSync:** Indicates that as a part of full management of an iOS device, the device is enrolled via the MDM client and the corporate email account configured on the device is managed by ZENworks that acts as a proxy server for the configured ActiveSync Server.
- ♦ **ActiveSync:** Indicates that as a part of Email Only enrollment, ZENworks manages only the corporate email account on the device and certain policies that are enforceable through the ActiveSync protocol, such as the Mobile Device Control Policy and Mobile Security Policy, can be applied on this device.

- ♦ **Unknown:** Indicates that the device is in a retired state.

Enrolling an iOS DEP Device

Enrolling a DEP device is simple for an end user, as you can enable the user to skip most of the device activation prompts by modifying the DEP Profile. Before enrolling a DEP device, ensure that you meet the following prerequisites:

Prerequisites

- ♦ Add a DEP Server in ZCC that links the ZENworks MDM Server and the virtual MDM Server in the Apple portal.
- ♦ Assign devices to the virtual MDM Server in the Apple portal. These devices are then discovered by ZENworks and populated in ZCC.
- ♦ (Optional) Assign users to the device, if you want only this user to be associated with the device during DEP enrollment.
- ♦ (Optional) Modify the DEP profile settings to enhance the enrollment process.
- ♦ (Conditional) If you modify the DEP profile, ensure that modified DEP profile is successfully assigned to the Apple Portal.

Additionally:

- ♦ Assign a Mobile Enrollment Policy that enables DEP enrollment for the users.
- ♦ (Conditional) If you are re-enrolling a device that was retired by another user, then ensure that the earlier device object is deleted in ZCC.
- ♦ (Optional) Assign a Mobile Email Policy to configure the email account on the device.

For more information, see [ZENworks 2017 Mobile Management Reference](#).

Procedure

Follow the setup prompts to enroll the device. After the user configures the Wi-Fi settings, log-in to the device with the user credentials. If the device is assigned to a specific user, then the credentials of only this user should be specified or else enrollment will fail.

After the device enrolls, you can view the **Deployment Status** of the device in ZCC, which should have changed from **Discovered** to **Managed**. You can view this status on the device's summary page. The enrolled device object is also created within the **Mobile Devices** folder (**Devices > Mobile Devices**) or in the appropriate folder as defined in the Mobile Enrollment Policy.

NOTE: Before re-enrolling a device, if the ownership (corporate or personal) is modified in the Mobile Enrollment Policy, the modified ownership is not applied on the re-enrolled device. The ownership defined during the initial phase of enrollment is considered.

A device that was enrolled using the ZENworks User Portal is being re-enrolled through Apple DEP using another user's credentials, then ensure that the earlier device object is deleted in ZCC.

Enrolling an iOS Device through Apple Configurator

Apple Configurator is a tool that assists administrators in the deployment of iOS devices in business or education settings. Apple Configurator makes reassigning devices quick and simple, allowing the next user to start with a clean slate of content.

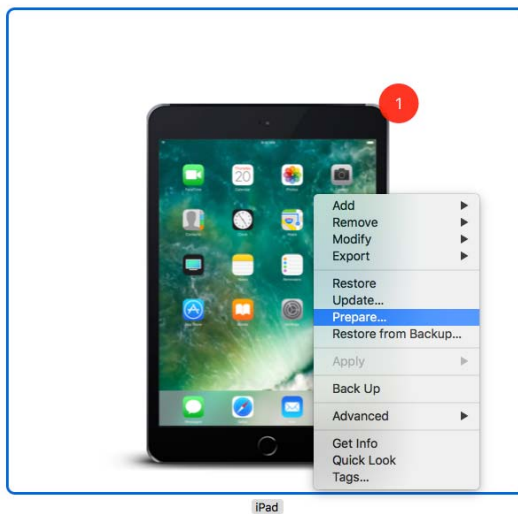
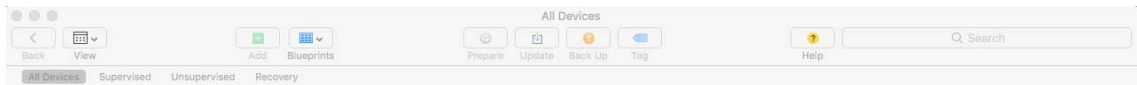
Prerequisites

- ◆ Assign a Mobile Enrollment Policy that enables enrollment through Apple Configurator for the users.
- ◆ Copy the Apple Enrollment URL, which specifies the MDM Server to which the device will enroll. To obtain this, in ZCC navigate to **Configuration > Infrastructure Management > MDM Servers**. Select a MDM Server and click **Apple Enrollment URL**.
- ◆ (Optional) Assign a Mobile Email Policy to configure the email account on the device.

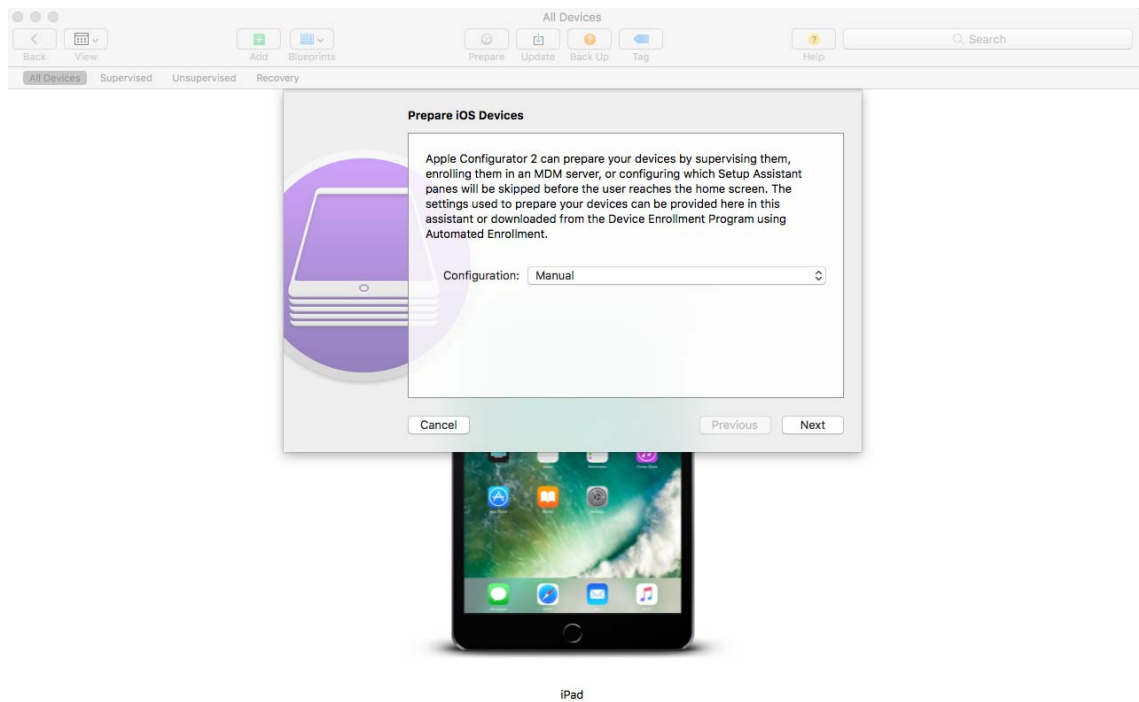
For more information, see [ZENworks 2017 Mobile Management Reference](#).

Procedure

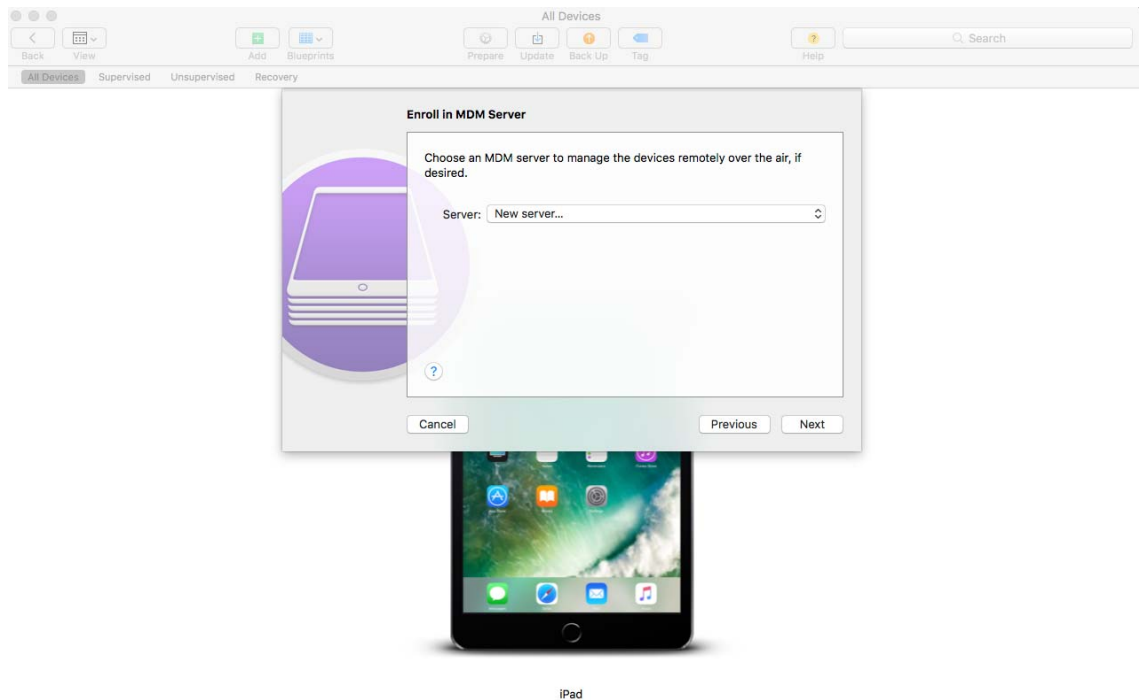
- 1 Connect the device through the USB port.
- 2 Right-click and select **Prepare** or select **Prepare** from the top menu bar in the Apple Configurator.



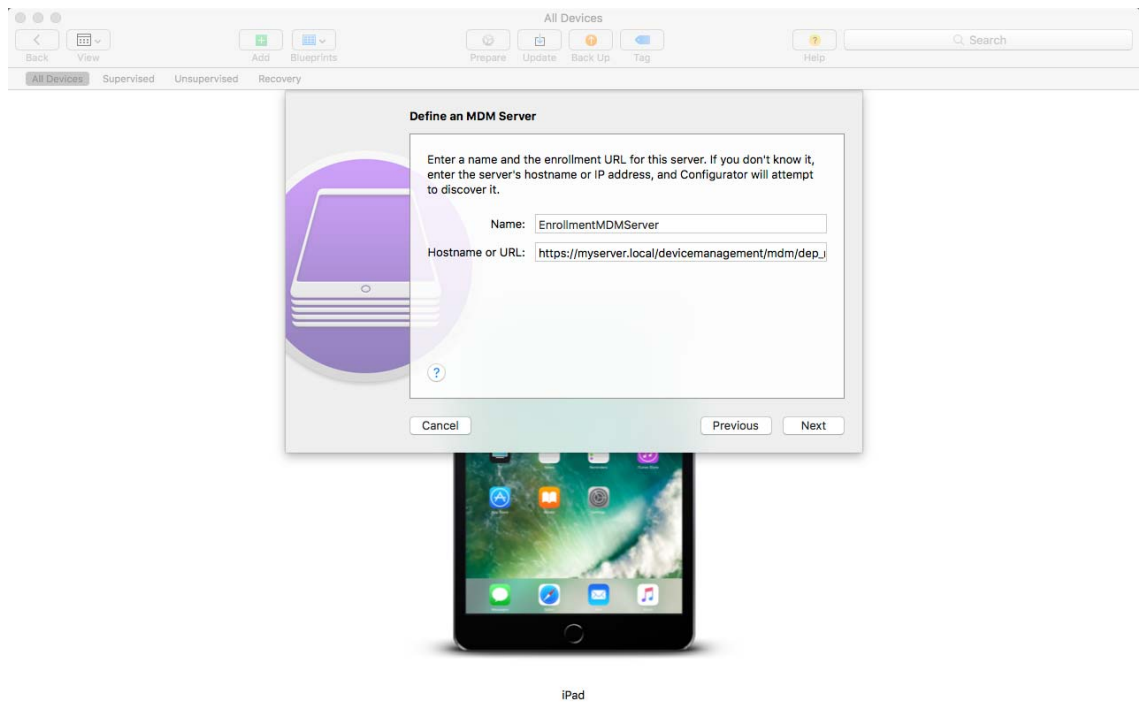
- 3 Select **Manual** in the **Configuration** drop down menu. Click **Next**.



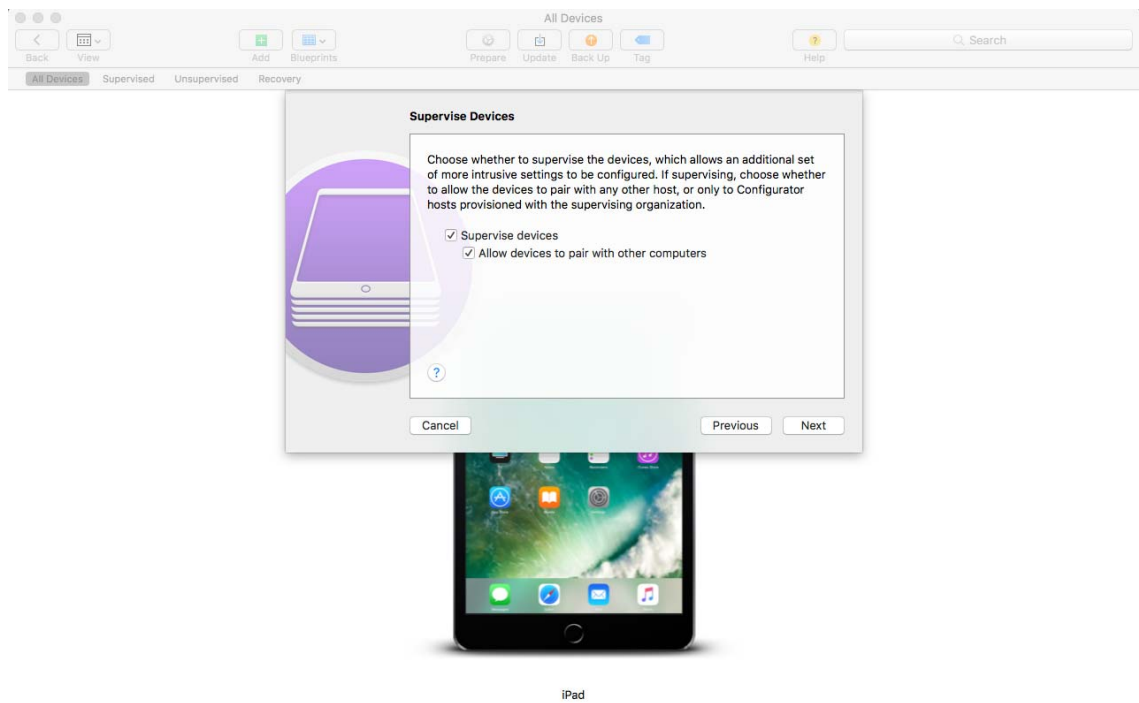
- 4 Select the MDM Server to which you want the device to enroll. If you do not have the MDM Server saved in the drop-down menu, then select **New Server**.



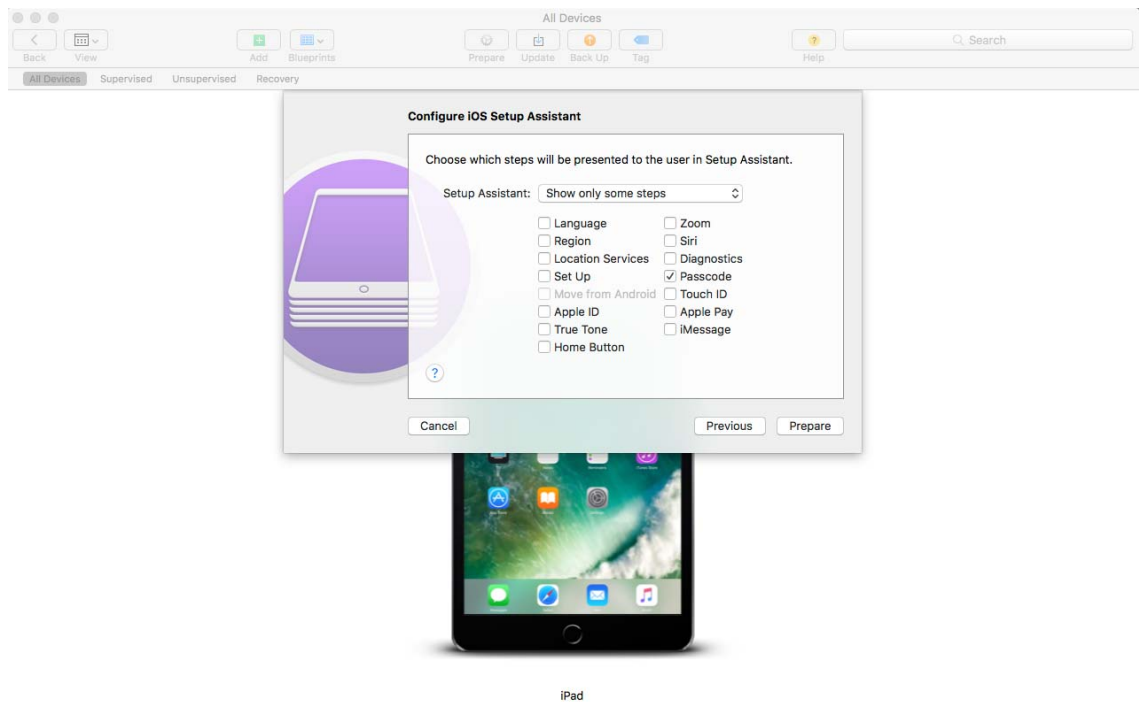
- 5 Specify a name for the server and paste the Apple Enrollment URL copied from ZCC. To obtain this, in ZCC navigate to **Configuration > Infrastructure Management > MDM Servers**. Select a MDM Server and click **Apple Enrollment URL**. Copy the URL and paste it in the Define an MDM Server page in the Apple Configurator. This MDM Server will be saved for future use.



- 6 Select **Supervise devices**, if you want to set the device as supervised. The check box to **Allow devices to pair with other computers** is automatically enabled.



- 7 Select the organization that will supervise these devices.
- 8 Select the appropriate option from the **Setup Assistant** drop-down menu, if you want to skip certain setup steps during enrollment of the device. Check the setup items that should be presented during device enrollment.



9 Click **Prepare** to prepare the connected device.

After the preparation stage, the device will reset to its factory settings. After the device is reset, follow the prompts that will be displayed as configured in the **Configure iOS Setup Assistant** page. After entering the Wi-Fi password, the user will be prompted for the user credentials.

After the device enrolls, the device object is created within the Mobile Devices folder (**Devices > Mobile Devices**) or in the appropriate folder as defined in the Mobile Enrollment Policy.

Enrolling devices using the ZENworks User Portal

This enrollment is preferable for BYOD devices. The following devices can be enrolled using the ZENworks User Portal:

- ◆ Android Devices
- ◆ iOS Devices
- ◆ Windows and Blackberry Devices (devices with Exchange ActiveSync capabilities).

Prerequisites

Before enrolling a mobile device as a fully managed device or an email only device, you need to ensure that the following prerequisites are met:

- ◆ ZENworks supports devices running on Android 4.1 and newer, and devices running iOS version 8 and newer. Also, ZENworks supports devices running ActiveSync 12.1 and newer.
- ◆ A user source is configured and enabled for mobile device enrollment.
- ◆ An enrollment policy is created and assigned to the user.
- ◆ An MDM role is assigned to a Primary Server.

- ◆ Push notifications for either Android or iOS devices are enabled.
- ◆ To enable ZENworks to synchronize emails for Exchange ActiveSync accounts, an ActiveSync server should be configured. Also, create and assign a Mobile Email Policy with the ZENworks Server configured as the proxy server for the ActiveSync Server. This will enable ZENworks to manage the corporate emails sent and received on the device.

For more information, see [ZENworks 2017 Mobile Management Reference](#).

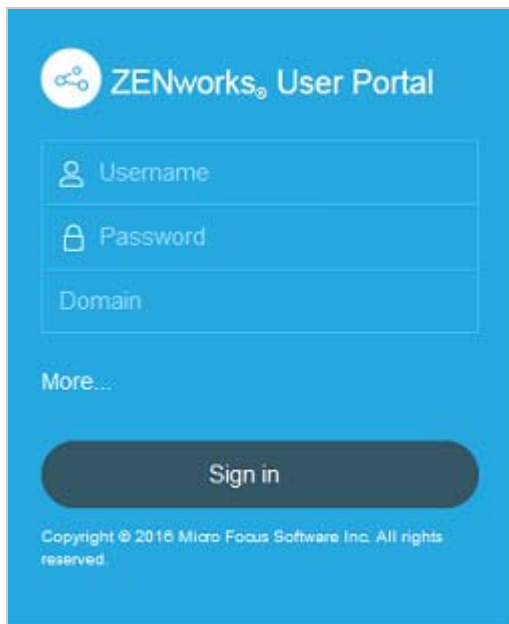
Procedure: Enrolling an Android Device

This scenario shows you how to enroll an Android device as a fully managed device in your ZENworks Management Zone.

- 1 In the Google Chrome browser on the Android device, enter `ZENworks_server_address/zenworks-eup`, where `ZENworks_server_address` is the DNS name or IP address of the ZENworks MDM Server.

NOTE: You must use Google Chrome. The built-in Internet browser is not supported.

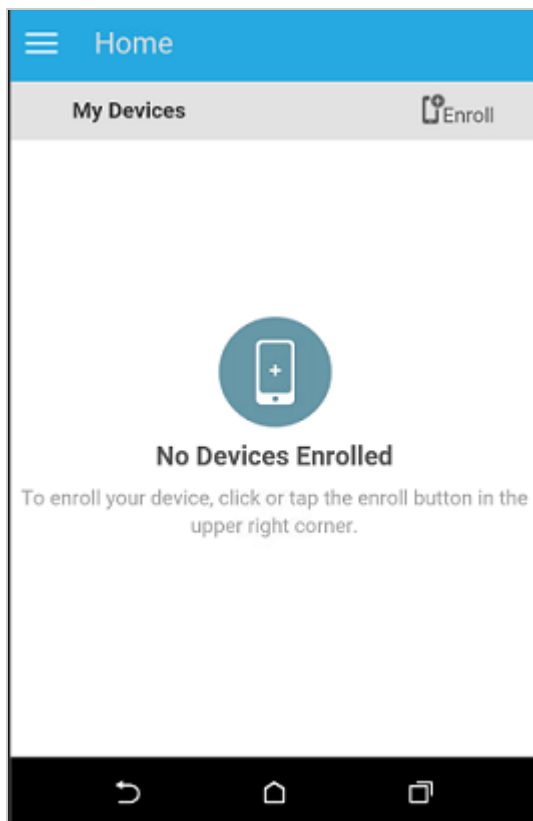
The login screen for the ZENworks User Portal is displayed. You use the user portal to enroll devices to the zone.



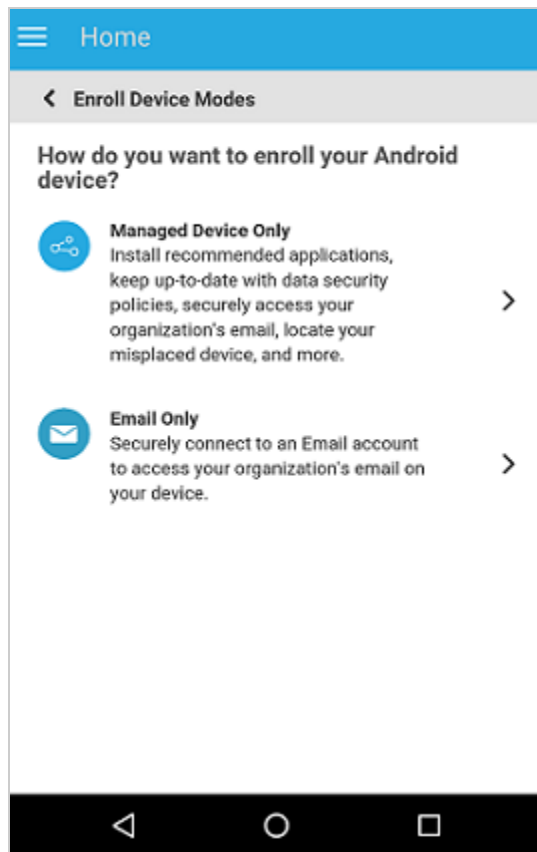
All devices associated with the user, are displayed in the ZENworks User Portal.

- 2 Enter the user's user name and password. If **Allow Simple Enrollment** option is selected for the user source to which the user belongs, then the registration domain need not be specified or else specify the registration domain. Tap **Sign In**.

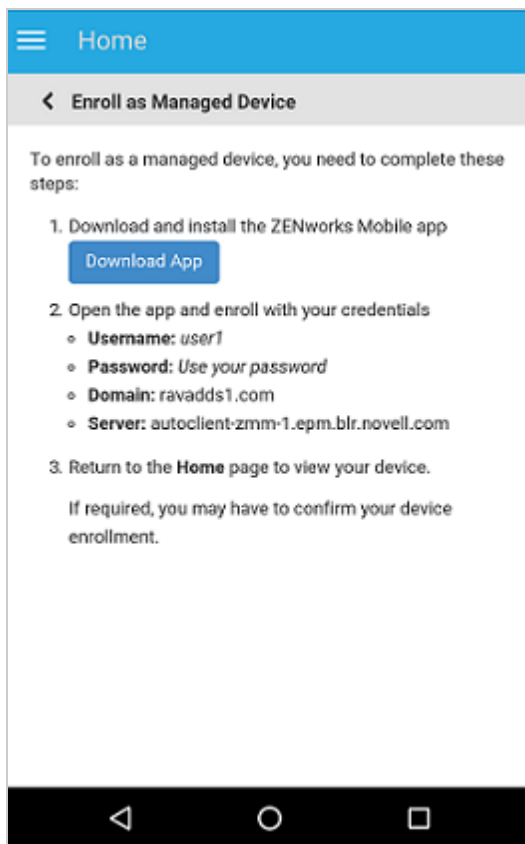
NOTE: If the **Allow Simple Enrollment** option is not enabled or the registration domain name is not configured, then you can specify the configured user source name in the **Domain** field while enrolling a device.



- 3 Tap **Enroll** in the upper-right corner to display the enrollment options for the device.
The enrollment options are determined by the Mobile Enrollment policy assigned to the user.

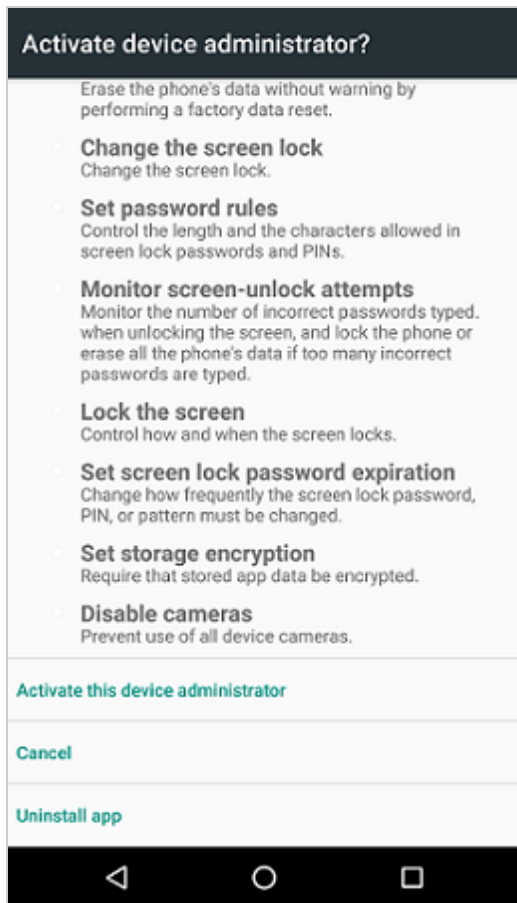


- 4 Tap **Managed Device Only**.



- 5 Tap **Download App**. The user will be directed to the Google Play Store, where the user needs to click **Install** to install the ZENworks Agent app. After installation, click **Open**.

- 6 Click **Activate this Device Administrator** to enable you to manage the device by performing the operations listed in this screen.



NOTE: For Android Marshmallow and subsequent versions, ensure that the user accepts the `READ_WRITE_PHONE` permission and `WRITE_EXTERNAL_STORAGE` permission after downloading and launching the app. Contrary to the statement mentioned in the dialog box, the `READ_WRITE_PHONE` permission does not make any calls and does not collect phone logs. This permission is required to identify the device's information such as the serial number and IMEI number. The `WRITE_EXTERNAL_STORAGE` permission is required to access the device storage to create logs that can be used for troubleshooting.

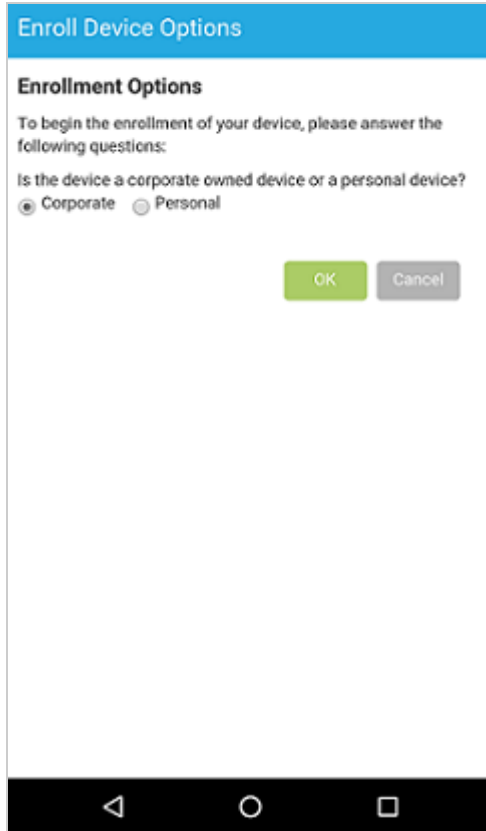
7 The ZENworks Agent app login screen is displayed.



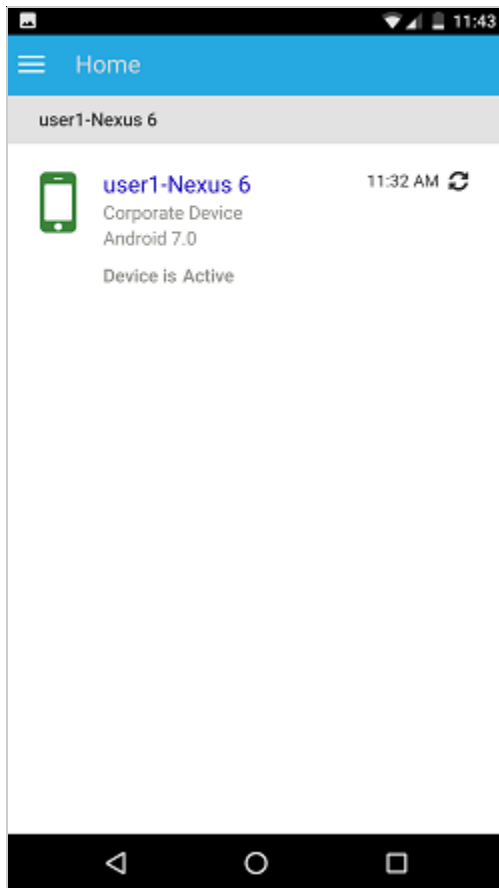
8 Fill in the fields, then tap **Sign In**.

- ◆ **User name, Password, Domain, Server URL:** Use the same user name, password, and registration domain (if required) that you had initially used to log in to the ZENworks User Portal along with the server URL of the ZENworks MDM Server. You can obtain this information from the ZENworks User Portal as displayed in [Step 4](#).

If you configured your Mobile Enrollment policy to allow the user to specify the device ownership (corporate or personal), you are prompted for that information. Tap **OK**. The device will be automatically enrolled to the zone.



- 9 The ZENworks Agent App Home screen is displayed, showing that the device is enrolled and active.



After the device is enrolled to the ZENworks Management Zone, you can view the device information in ZCC. To view the device information, from the left hand side navigation pane in ZCC, click **Devices > Mobile Devices** (or navigate to the folder as configured in the Mobile Enrollment Policy) and select the appropriate device. The enrollment mode will be displayed as **Android App**.

- 10 After ZENworks Agent app enrollment, based on the assigned Mobile Email Policy, an email is sent to the user with the corporate email account settings. This email can be accessed from the email client's web application or from any other device. With this information, the user needs to manually configure the email account on the device to send or receive corporate emails. You need to configure an SMTP server, to enable ZENworks to send these email notifications. For more information on configuring an SMTP server, see [Event and Messaging Settings](#) in the [ZENworks Management Zone Settings Reference](#) guide.
- 11 After configuring the corporate email account, the device will enroll and automatically reconcile to the device object that was initially created when the ZENworks Agent app enrollment was completed. The enrollment mode changes to **Android App + ActiveSync** on the Device Information page in ZCC.

NOTE: After configuring an ActiveSync account, if the device is unable to auto reconcile to the device object that was created after ZENworks Agent app enrollment and if **Allow Manual Reconciliation by User** is checked in the assigned Device Enrollment Policy, the user will be prompted to manually reconcile the device. For details, see [Allowing Manual Reconciliation by User](#).

If a Mobile Email Policy is unassigned from the device that is enrolled to the ZENworks Management Zone, then the user receives an email stating that corporate emails cannot be sent or received on the device. You can edit the contents of this email in ZCC by navigating to **Configuration > Mobile Management > Email Notifications**. Click the relevant email and edit its contents.

Procedure: Enrolling an iOS Device

This scenario shows you how to enroll an iOS device as a fully managed device in your ZENworks Management Zone.

- 1 In the Safari browser on the iOS device, enter `ZENworks_server_address/zenworks-eup`, where `ZENworks_server_address` is the DNS name or IP address of the ZENworks MDM Server.

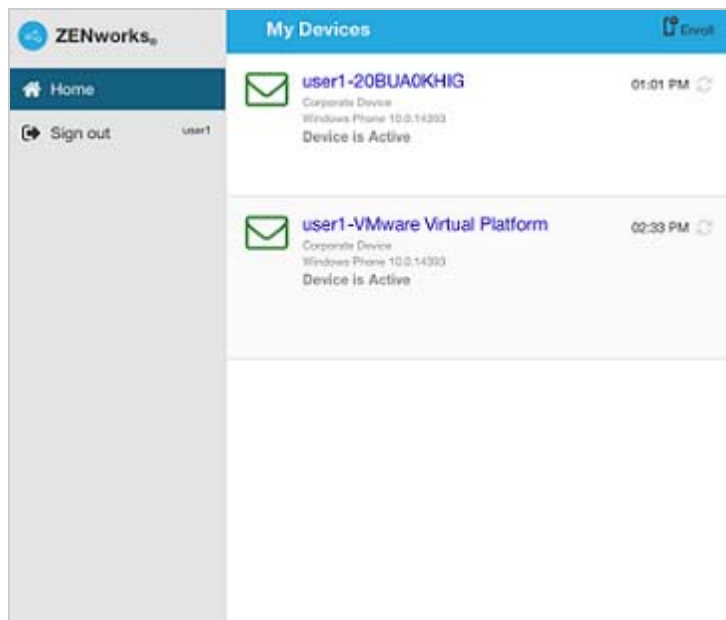
The login screen for the ZENworks User Portal is displayed. You use the ZENworks User Portal to enroll devices to the zone.



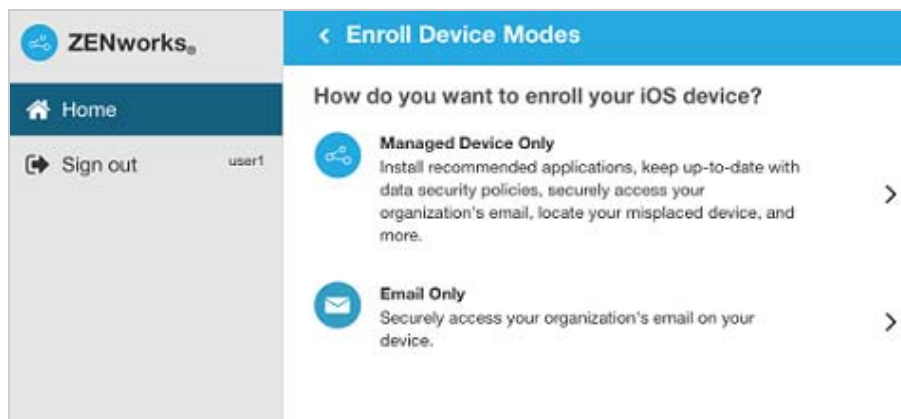
- 2 Enter the user's user name and password. If **Allow Simple Enrollment** option is selected for the user source to which the user belongs, then the registration domain need not be specified or else specify the registration domain. Tap **Sign In**.

NOTE: If the **Allow Simple Enrollment** option is not enabled or the registration domain name is not configured, then you can specify the configured user source name in the **Domain** field while enrolling a device.

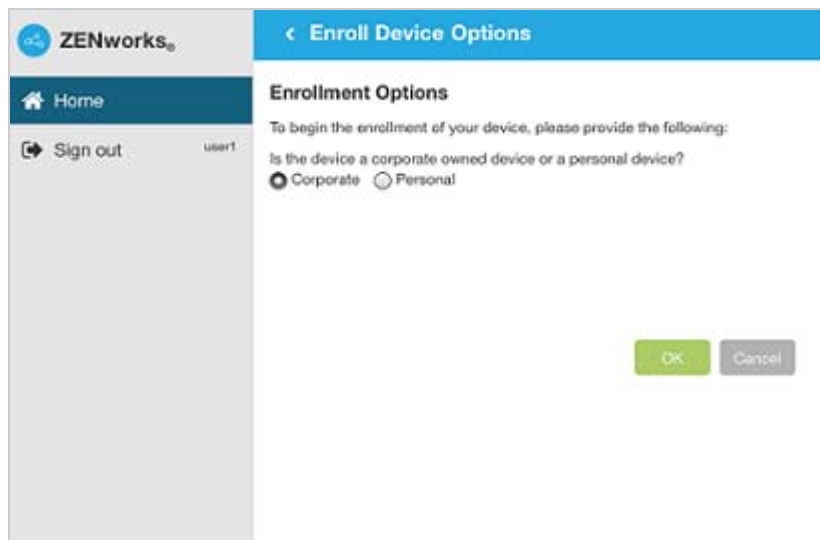
All devices associated with the user, are displayed in the ZENworks User Portal.



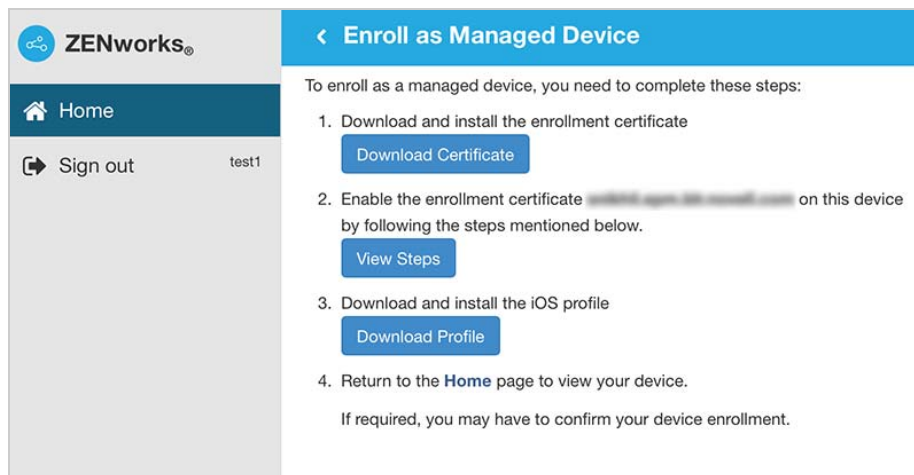
- 3 Tap **Enroll** in the upper-right corner to display the enrollment options for the device. The enrollment options are determined by the user's Mobile Enrollment policy.



- 4 Tap **Managed Device Only** to display the **Enroll Device Options** screen. If you have configured your Mobile Device Enrollment policy to allow the user to specify the device ownership (corporate or personal), you are prompted for that information. Select the appropriate device ownership option and click **OK**.

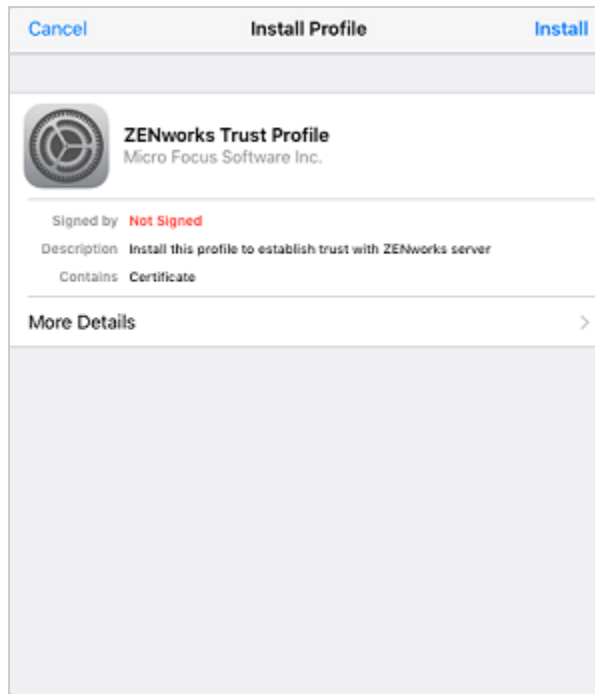


5 Tap **Download Certificate** to display the **Install Profile** screen.



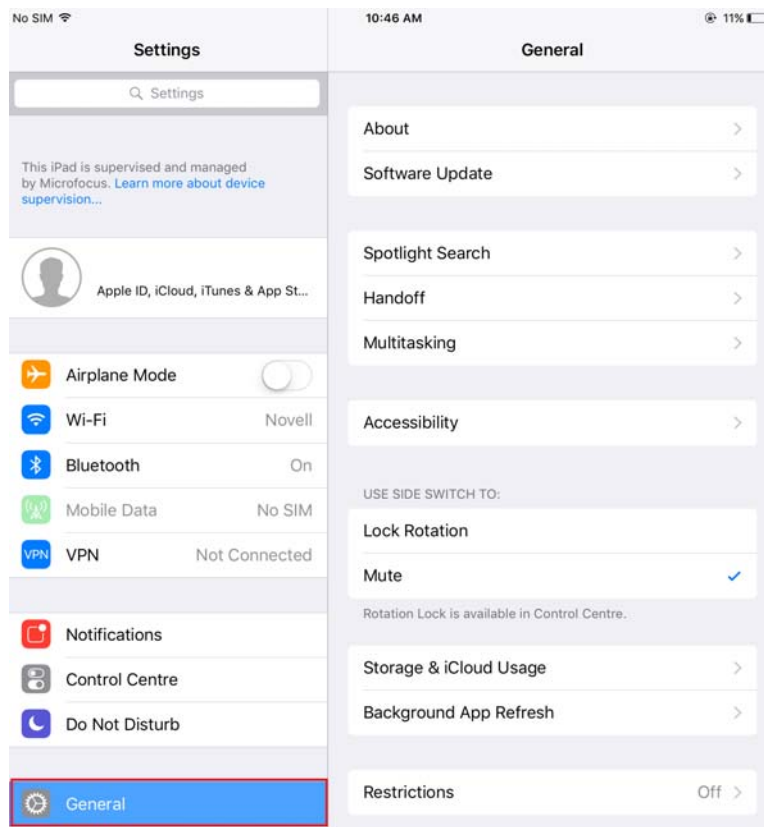
- 6 Tap **Install** and follow the prompts to install the certificate and return to the Enroll as Managed Device screen.

The ZENworks Trust Profile contains the certificate required for secure communication between the device and the ZENworks Primary Server.

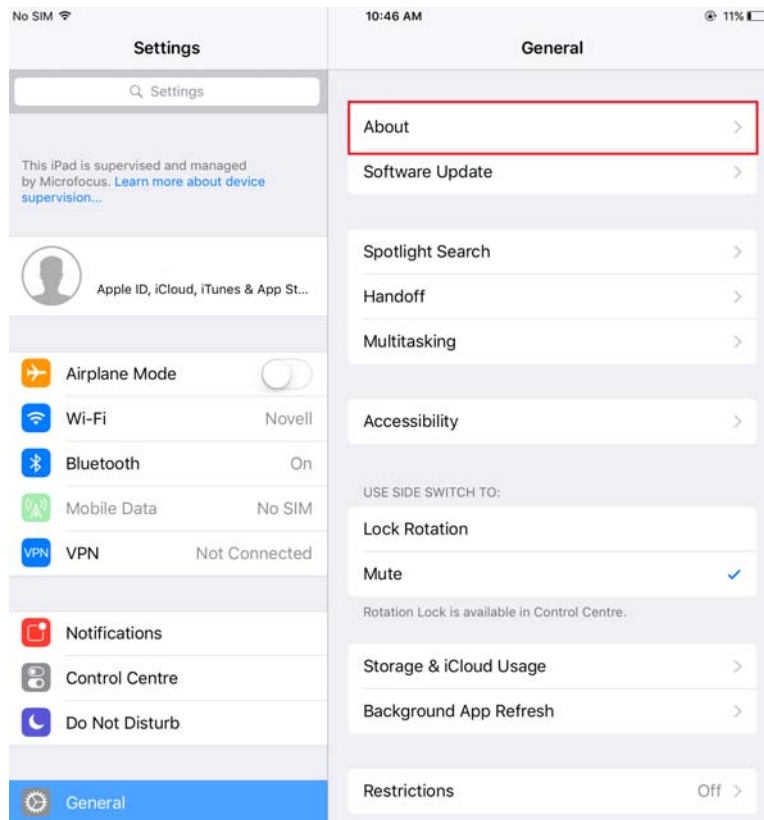


- 7 (Conditional) Enable the enrollment certificate on the device. This step will appear on devices running on iOS versions 10.3 or newer. To enable the certificate:

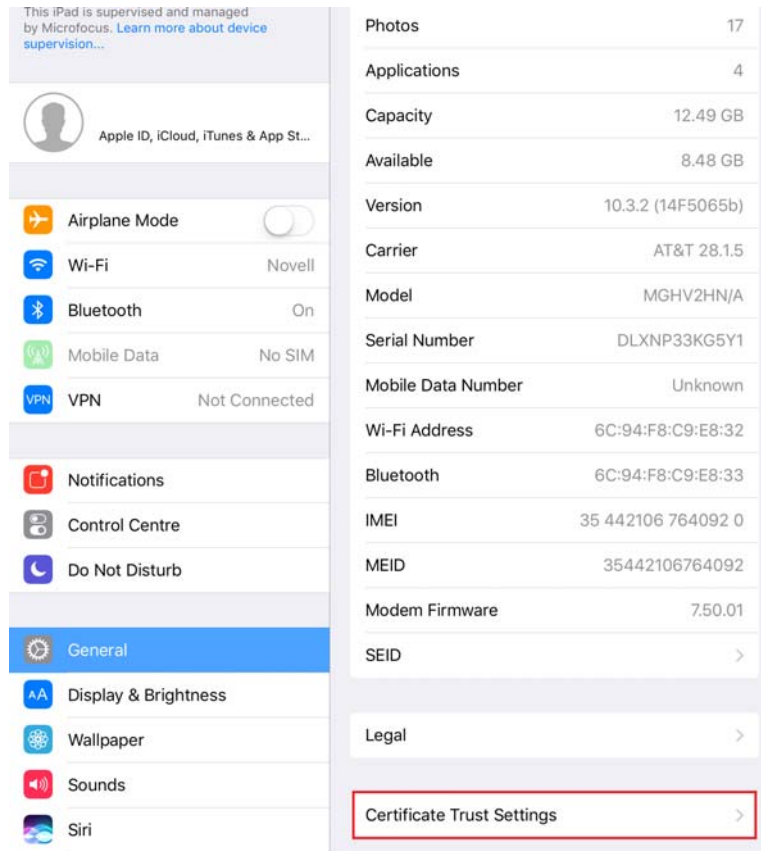
- 7a Navigate to the **Settings** menu on the device and click **General**.



7b Click About.



7c Click Certificate Trust Settings.

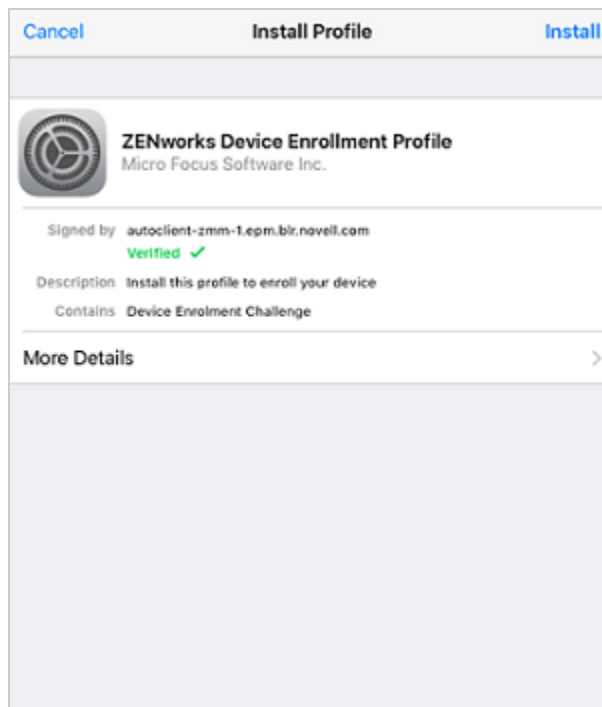


7d Enable the root certificate displayed on the screen.



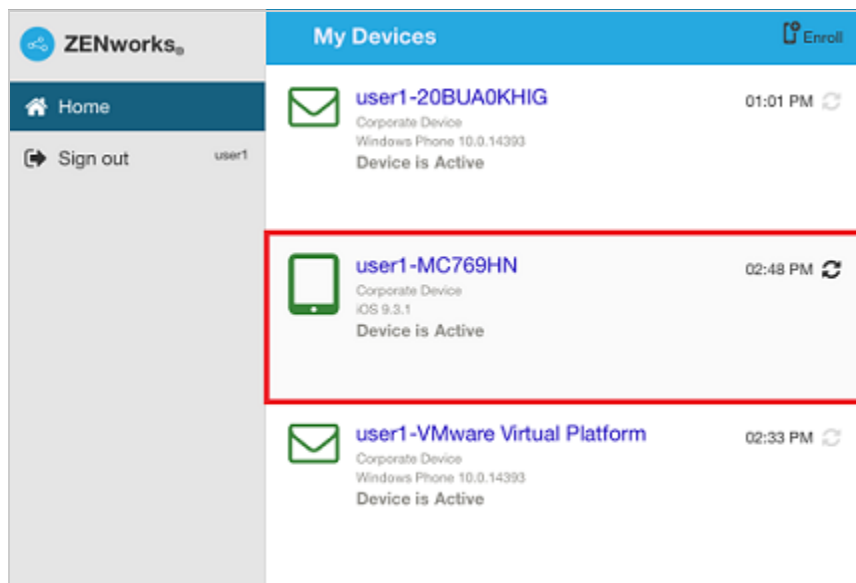
8 Tap **Download Profile** in the Enroll as Managed Device screen, to display the profile install screen. Tap **Install** and follow the prompts to install the profile and return to the Enroll as Managed Device screen.

The ZENworks Device Enrollment Profile contains the MDM profile required for ZENworks to manage the device.



- 9 Tap **Home** to return to the Home page. The device is displayed in the My Devices list with the status as **Enrollment in Progress**. You need to refresh the browser to update the status to **Device is Active**.

NOTE: If the device remains in **Enrollment in Progress** state for a considerable amount of time, then in the ZENworks User Portal, tap the refresh icon appearing against the device.



At this point in time, you can view the enrollment mode on the Device Information page in ZCC. To view the device information, from the left hand side navigation pane in ZCC, click **Devices > Mobile Devices** (or navigate to the folder as configured in the Mobile Enrollment Policy) and select the appropriate device. The enrollment will be displayed as **iOS MDM**.

- 10 An email account is automatically set up on the device based on the Mobile Email Policy assigned to the user or the device.

NOTE: If an Exchange ActiveSync account was manually configured on the iOS device before it was enrolled, then it should be deleted as an email account will be automatically configured on the iOS device if a Mobile Email policy is assigned.

After the device is enrolled to the ZENworks Management Zone, the enrollment mode of the device is displayed as **iOS MDM + ActiveSync** on the Device Information page in ZCC.

Procedure: Enrolling an Email-only Device

This scenario shows you how to enroll a device as an Email Only device in your ZENworks Management Zone. This scenario details the procedure to enroll an iOS device as an Email Only Device.

- 1 In a browser on the device, enter `ZENworks_server_address/zenworks-eup`, where `ZENworks_server_address` is the DNS name or IP address of the ZENworks MDM Server.

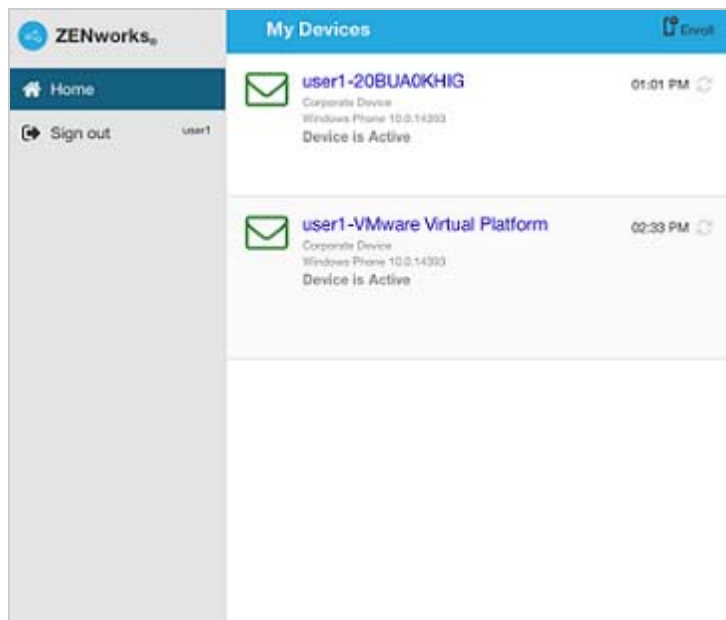
The login screen for the ZENworks User Portal is displayed. You use the ZENworks User Portal to enroll the device.



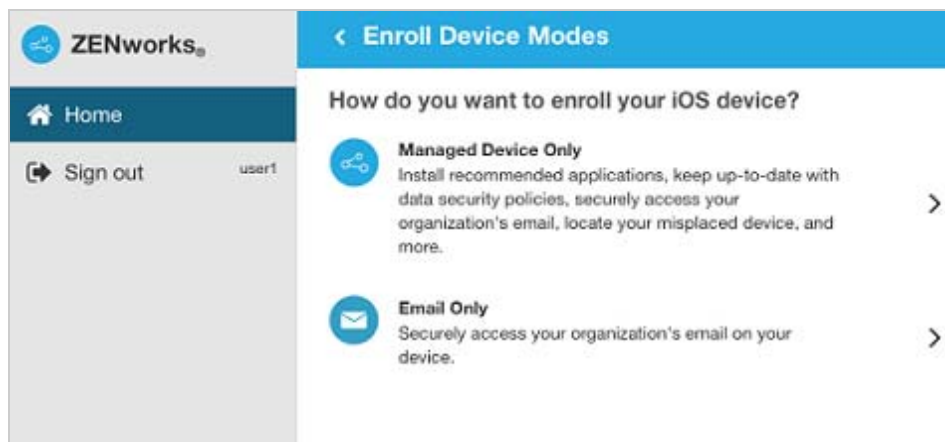
- 2 Enter the user's user name and password. If **Allow Simple Enrollment** option is selected for the user source to which the user belongs, then the registration domain need not be specified or else specify the registration domain. . Tap **Sign In**.

NOTE: If the **Allow Simple Enrollment** option is not enabled or the registration domain name is not configured, then you can specify the configured user source name in the **Domain** field while enrolling a device.

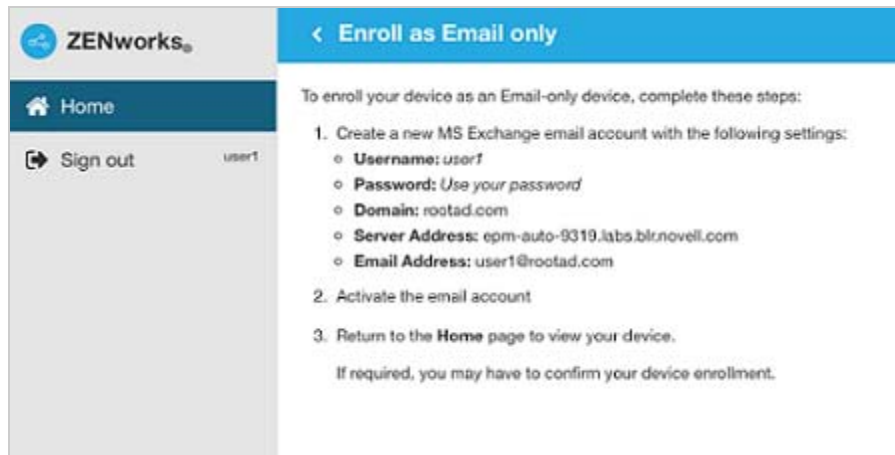
All devices associated with the user, are displayed in the ZENworks User Portal.



- 3 Tap **Enroll** on the upper-right corner, to display the enrollment options for the device. The enrollment options are determined by the user's Mobile Enrollment policy.



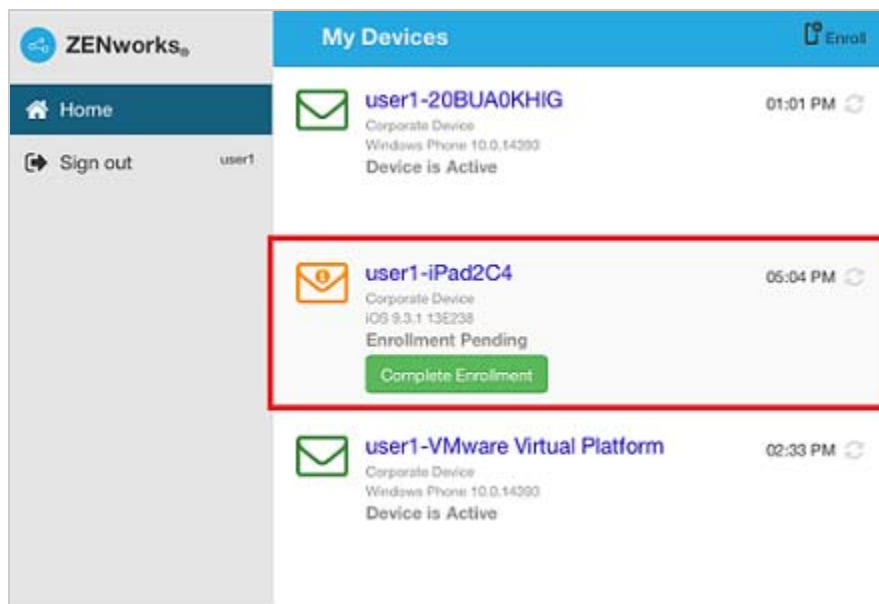
- 4 Tap **Email Only** to display the **Enroll as Email Only** screen. Use the displayed information to create an email account for the user.



- 5 After the user configures the email account, an email is sent to the user stating that the enrollment process needs to be completed. You can edit the contents of this email in ZCC, by navigating to **Configuration > ActiveSync > Email Notifications**. Click the relevant email and edit its contents.

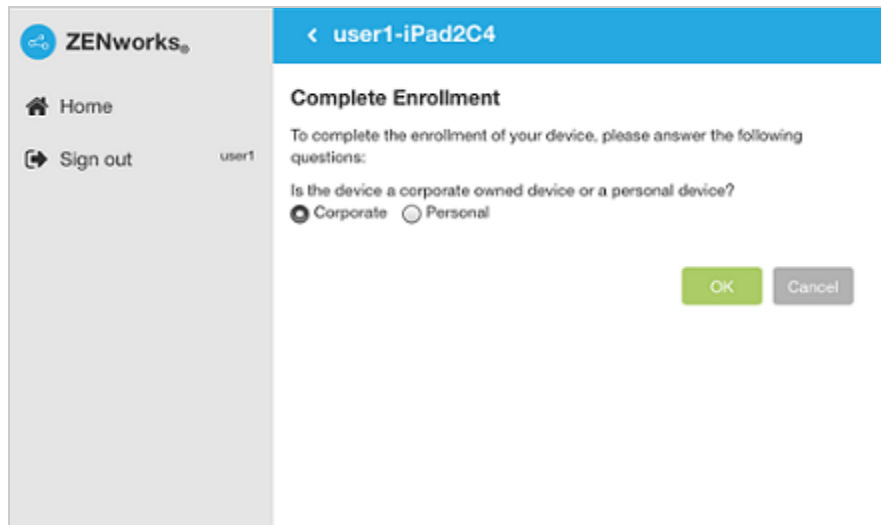
To complete the enrollment process, click the link to the ZENworks End User Portal provided in the email or visit the ZENworks End User Portal.

- 6 On the ZENworks User Portal, the device is displayed in the My Devices list. At this point, the device has been added to the ZENworks Management Zone but is pending enrollment.

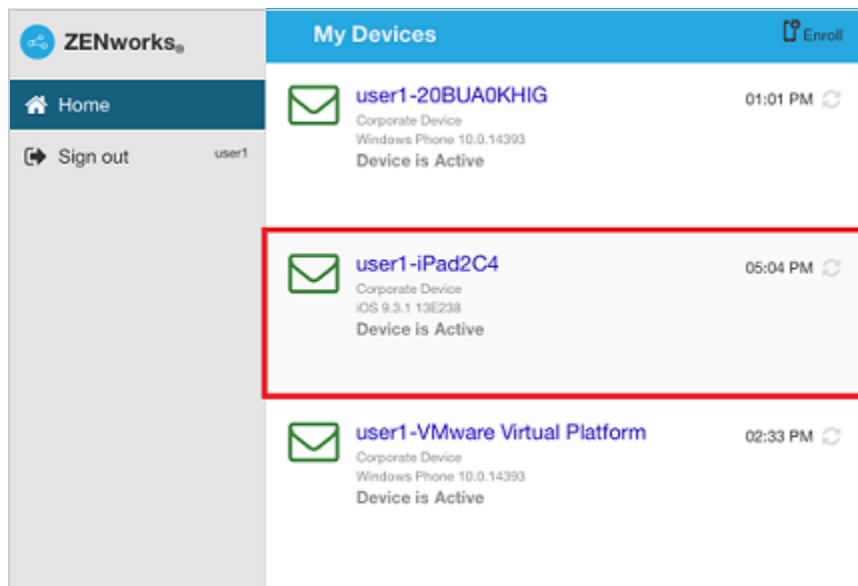


7 On the device, tap **Complete Enrollment**.

If you configured your Mobile Enrollment policy to allow the user to specify the device ownership (corporate or personal), you are prompted for that information. On the device, provide the required enrollment information, then tap **OK**.



8 The My Devices list is updated to show that the device is enrolled and active.



9 Verify that the device is receiving emails, by sending an email to the user from another account.

NOTE: If a Mobile Email policy is not assigned to the enrolled Email Only device or is unassigned from the already enrolled Email Only device, then an email is sent to the device stating that the user will be unable to send or receive corporate emails. You can edit the contents of this email in ZENworks Control Center by navigating to **Configuration > ActiveSync > Email Notifications**. Click the relevant email and edit the contents.

Also, if a Mobile Email policy is not assigned to the device enrolled as an Email Only device, the device can still be managed by the ZENworks Control Center wherein you can apply policies applicable for Email Only devices.

- 10 After the device is enrolled to the ZENworks Management Zone, the enrollment mode of the device is displayed as **ActiveSync** on the Device Information page in ZCC. To view the device information, from the left hand side navigation pane in ZCC, click **Devices > Mobile Devices** (or navigate to the folder as configured in the Mobile Enrollment Policy) and select the appropriate device.

Allowing Manual Reconciliation by User

When users attempt to enroll their devices, which they have previously enrolled, using the same enrollment mode or a different enrollment mode, ZENworks will update the existing device object in the management zone through reconciliation. However, for certain devices auto reconciliation might fail due to the following reasons:

- ◆ ZENworks is unable to access the IMEI number of certain non-cellular Android devices.
- ◆ ZENworks is unable to access the IMEI number of certain Android devices, as the IMEI number is masked.
- ◆ The ActiveSync ID of iOS devices change if they are reset to factory settings before re-enrolling.

Taking these scenarios into account, you can select the **Allow manual reconciliation by user** option while editing the Mobile Enrollment Policy.

If this feature is turned on and ZENworks is unable to reconcile with the existing device object, then a page is displayed that lets the user manually reconcile to the existing device object.

If the feature is turned off and ZENworks is unable to reconcile with the existing device object, then the device is automatically enrolled as a new device.

To enable this option:

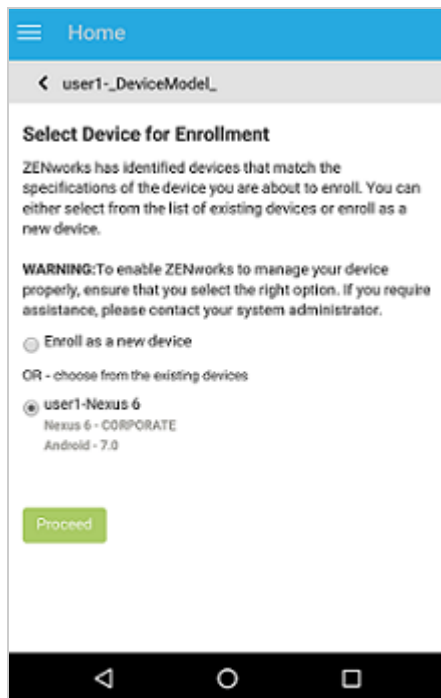
- 1 Navigate to the **Policies** section in ZCC.
- 2 Click the relevant Mobile Enrollment Policy.
- 3 Click the **Details** tab.
- 4 Click **Advanced Settings**.
- 5 Click **Allow Manual Reconciliation by User**.
- 6 Click **Apply**.
- 7 Publish as a new policy or as a new version of the policy.

IMPORTANT: During manual reconciliation, it is important that the user selects the right option. If an incorrect option is selected, then ZENworks will be unable to manage the device properly.

Consider the following scenarios:

For Android Devices: A user has downloaded the ZENworks Agent app and completed the enrollment procedure for a non-cellular Android device. Subsequently, a device object is created in the ZENworks Management Zone. Later, to enable ZENworks to manage corporate emails on the device, the user configures an ActiveSync account on the same device. After configuring the ActiveSync account, since the IMEI number of this device is not available, ZENworks will be unable to reconcile the device with the existing device object that was created during the ZENworks Agent app enrollment.

In such a scenario, if **Allow Manual Reconciliation by User** is allowed in the Mobile Enrollment policy and if reconciliation fails, ZENworks sends a mail to the user to complete the enrollment process. When the user re-visits the ZENworks User Portal to complete ActiveSync enrollment, the user needs to select the appropriate device ownership type. Subsequently, the ZENworks User Portal will list all active Android devices associated with the user that are enrolled to the ZENworks Management Zone. The user can select the appropriate device to manually reconcile it to the existing device object. The user also has the option to select **Enroll as New Device**. Click **Proceed**.



NOTE: If for any reason, platform related information of the device could not be obtained by ZENworks, then the ZENworks User Portal will initially list all the platforms before listing all devices for manual reconciliation. The user needs to select the relevant platform of the device before proceeding further. This page will be displayed regardless of whether the **Allow manual reconciliation by user** option is selected or not.

In a scenario, wherein an Android device is already enrolled via the ActiveSync mode and the user is about to re-enroll the same device by downloading the ZENworks App, then as a part of manual reconciliation, the ZENworks App will display all active Android devices that are enrolled as Email Only (ActiveSync Only) devices and are associated with the same user.

For iOS devices: An iOS device that was initially enrolled via Email Only mode is fully wiped and retired. You have now unretired the device for the user to re-enroll the device back to the zone using the same enrollment mode. Since the ActiveSync IDs of the re-enrolled device changes, auto reconciliation fails.

In such a scenario, enable **Allow Manual Reconciliation by User** in the Mobile Enrollment Policy. When the user re-visits the ZENworks User Portal page to complete ActiveSync Only enrollment of the unretired device and after selecting the device ownership type, the ZENworks User Portal will list all active iOS devices associated with the user that are enrolled to the ZENworks Management Zone. The user can select the appropriate device to manually reconcile the device to the existing device object. The user also has the option to select **Enroll as New Device**. Click **Proceed**.

