AUTHORIZED DOCUMENTATION

# Administration Quick Start

# Novell® ZENworks® 11

## Support Pack 1

August 08, 2011

www.novell.com

## Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2007-2011 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

*Online Documentation:* To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

## Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

## Third-Party Materials

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

# Contents


**About This Guide** 7

**Part I Overview** 9

**1 ZENworks 11 SP1 Products** 11

**2 Product Overview** 13

2.1 ZENworks Capabilities . . . 13
2.2 System Architecture . . . 14
2.2.1 Primary Server . . . 15
2.2.2 Satellite . . . 16
2.2.3 Managed Device . . . 16
2.2.4 Inventoried-Only Device . . . 17
2.2.5 Management Zone . . . 17

**3 ZENworks Terminology** 19

**Part II System Configuration** 23

**4 Quick List** 25

4.1 Management Tools . . . 25
4.2 Zone Configuration . . . 25
4.3 Agent Deployment . . . 27
4.4 System Messages and Reports . . . 28

**5 Management Tools** 29

5.1 ZENworks Control Center . . . 29
5.1.1 Accessing ZENworks Control Center . . . 29
5.1.2 Navigating ZENworks Control Center . . . 30
5.2 zman Command Line Utility . . . 31
5.2.1 Location . . . 32
5.2.2 Syntax . . . 32
5.2.3 Help with Commands . . . 32
5.3 zac Command Line Utility . . . 33
5.3.1 Location . . . 33
5.3.2 Syntax . . . 33
5.3.3 Help with Commands . . . 33

**6 Management Zone Configuration** 35

6.1 Organizing Devices: Folders and Groups . . . 35
6.1.1 Folders . . . 35
6.1.2 Groups . . . 37
6.1.3 Assignment Inheritance for Folders and Groups . . . 41
6.2 Creating Registration Keys and Rules . . . 41

6.2.1 Registration Keys . . . 41
6.2.2 Registration Rules . . . 43
6.2.3 Device Naming Template . . . 44
6.2.4 Where to Find More Information . . . 46
6.3 Connecting to User Sources . . . 46
6.4 Creating ZENworks Administrator Accounts . . . 48
6.4.1 Creating Administrator Account . . . 48
6.4.2 Creating Administrator Group Account . . . 50
6.5 Modifying Configuration Settings . . . 53
6.5.1 Modifying Configuration Settings at the Zone . . . 54
6.5.2 Modifying Configuration Settings on a Folder . . . 54
6.5.3 Modifying Configuration Settings on a Device . . . 54
6.6 Updating ZENworks Software . . . 55
6.7 Creating Locations . . . 55
6.7.1 Defining a Network Environment . . . 56
6.7.2 Creating Locations . . . 58
6.7.3 Location and Network Environment Selection on a Managed Device . . . 59

**7 ZENworks Adaptive Agent Deployment 61**

7.1 Configuring Adaptive Agent Features . . . 61
7.1.1 Coexisting with the ZENworks Desktop Management Agent . . . 62
7.1.2 Customizing the Adaptive Agent Features . . . 62
7.2 Installing the ZENworks Adaptive Agent . . . 64
7.2.1 Manual Installation on Windows . . . 64
7.2.2 Manual Installation on Linux . . . 65
7.2.3 ZENworks Control Center Deployment Task . . . 66
7.3 Using the ZENworks Adaptive Agent . . . 67
7.3.1 Logging In to the Management Zone . . . 67
7.3.2 Navigating the Adaptive Agent Views . . . 68
7.3.3 Promoting a Managed Device to be a Satellite . . . 71

**8 System Messages and Reports 73**

8.1 Viewing System Messages . . . 73
8.1.1 Viewing a Summary of Messages . . . 73
8.1.2 Acknowledging Messages . . . 74
8.1.3 Where to Find More Information . . . 76
8.2 Creating a Watch List . . . 76
8.3 Generating Reports . . . 76

**Part III Product Administration 79**

**9 Quick List 81**

9.1 Asset Management . . . 81
9.2 Configuration Management . . . 82
9.3 Endpoint Security Management . . . 83
9.4 Patch Management . . . 84

**10 Asset Management 87**

10.1 Activating Asset Management . . . 87
10.2 Enabling Asset Management in the ZENworks Adaptive Agent . . . 87
10.3 Collecting Software and Hardware Inventory . . . 88

10.3.1 Initiating a Device Scan . . . 88
10.3.2 Viewing a Device Inventory . . . 89
10.3.3 Generating an Inventory Report . . . 90
10.3.4 Where to Find More Information . . . 90
10.4 Monitoring Software Usage . . . 91
10.5 Monitoring License Compliance . . . 92
10.5.1 License Compliance Components . . . 92
10.5.2 Discovering Installed Products . . . 93
10.5.3 Creating a Catalog Product and Purchase Record . . . 94
10.5.4 Creating a Licensed Product . . . 96
10.5.5 Viewing Compliance Data . . . 98
10.5.6 Where to Find More Information . . . 99
10.6 Allocating Licenses . . . 99

**11 Configuration Management 103**

11.1 Activating Configuration Management . . . 103
11.2 Enabling Configuration Management in the ZENworks Adaptive Agent . . . 103
11.3 Distributing Software . . . 104
11.3.1 Creating a Bundle . . . 104
11.3.2 Assigning a Bundle . . . 104
11.3.3 Where to Find More Information . . . 105
11.4 Applying Policies . . . 105
11.4.1 Creating a Policy . . . 106
11.4.2 Assigning a Policy . . . 108
11.4.3 Where to Find More Information . . . 108
11.5 Imaging Devices . . . 108
11.5.1 Setting Up Preboot Services . . . 109
11.5.2 Taking an Image . . . 110
11.5.3 Applying an Image . . . 112
11.5.4 Where to Find More Information . . . 114
11.6 Remotely Managing Devices . . . 114
11.6.1 Creating a Remote Management Policy . . . 116
11.6.2 Configuring Remote Management Settings . . . 118
11.6.3 Performing Remote Control, Remote View, and Remote Execute Operations on a Windows Device . . . 119
11.6.4 Performing a Remote Diagnostic Operation . . . 122
11.6.5 Performing a File Transfer Operation . . . 123
11.6.6 Performing Remote Control, Remote View, and Remote Login Operations on a Linux Device . . . 125
11.6.7 Performing Remote SSH Operation on a Linux Device . . . 126
11.6.8 Where to Find More Information . . . 127
11.7 Collecting Software and Hardware Inventory . . . 127
11.7.1 Initiating a Device Scan . . . 127
11.7.2 Viewing a Device Inventory . . . 128
11.7.3 Generating an Inventory Report . . . 128
11.7.4 Where to Find More Information . . . 129
11.8 Personality Migration . . . 129
11.9 Linux Management . . . 130

**12 Endpoint Security Management 131**

12.1 Activating Endpoint Security Management . . . 131
12.2 Enabling the Endpoint Security Agent . . . 131
12.3 Creating Locations . . . 132
12.4 Creating a Security Policy . . . 132

12.5 Assigning a Policy to Users and Devices . . . . . 136
12.6 Assigning a Policy to the Zone . . . . . 137

**13 Patch Management 139**

13.1 Activating Patch Management . . . . . 139
13.2 Enabling Patch Management in the ZENworks Adaptive Agent . . . . . 140
13.3 Starting the Subscription Service . . . . . 140
13.4 Deploying a Patch . . . . . 141
13.5 Where to Find More Information . . . . . 142

**Part IV Appendix 145**

**A Installation and Setup Documentation 147**

**B Administration Documentation 149**

# About This Guide

This *ZENworks 11 SP1 Administration Quick Start* helps you quickly master the basics of administering your ZENworks 11 SP1 Management system. You should already have installed your ZENworks system. If not, see the *ZENworks 11 SP1 Installation Guide*.

The information in this guide is organized as follows:

- Overview (page 9): Provides information about the editions of ZENworks 11 SP1, a high-level overview of the ZENworks system architecture and capabilities, and the new features and enhancements.
- System Configuration (page 23): Provides instructions for configuring your ZENworks Management Zone prior to using the ZENworks 11 SP1 products.
- Product Administration (page 79): Provides instructions for using ZENworks 11 SP1 products (Asset Management, Configuration Management, Endpoint Security Management, 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 User Comments feature at the bottom of each page of the online documentation.

## Additional Documentation

ZENworks 11 SP1 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 11 SP1 documentation Web site (http://www.novell.com/documentation/zenworks11).

# Overview

The following sections provides information about ZENworks 11 SP1 products, and overview of the ZENworks system architecture and new features and capabilities:


- Chapter 1, “ZENworks 11 SP1 Products,” on page 11
- Chapter 2, “Product Overview,” on page 13
- Chapter 3, “ZENworks Terminology,” on page 19

# ZENworks 11 SP1 Products

1

Novell ZENworks 11 SP1 includes the following products:

- Asset Management
- Configuration Management
- Endpoint Security Management
- Patch Management

The products are available for purchase separately and as suites. If you choose to purchase an individual ZENworks 11 SP1 product, such as Configuration Management, then the other three products (Asset Management, Endpoint Security Management, and Patch Management) are also installed along with Configuration Management but are available only for an evaluation period of 60 days. Subsequently, you can activate the desired product by supplying a valid product license through the ZENworks management console.

The following table lists the available ZENworks 11 SP1 suites:

***Table 1-1*** *ZENworks 11 SP1 Suites*

| ZENworks 11 SP1 Suites | Products with Full License |
|---|---|
| ZENworks 11 SP1 Enterprise Edition | ◆ ZENworks 11 SP1 Configuration Management<br>◆ ZENworks 11 SP1 Asset Management<br>◆ ZENworks 11 SP1 Patch Management<br>◆ ZENworks 11 SP1 Endpoint Security Management<br>◆ ZENworks Reporting Server powered by BusinessObjects Enterprise<br>◆ AdminStudio 10.0 Standard Edition<br>◆ ZENworks Handheld Management |
| ZENworks 11 SP1 Advanced Edition[1] | ◆ ZENworks 11 SP1 Configuration Management<br>◆ ZENworks 11 SP1 Patch Management<br>◆ ZENworks Reporting Server powered by BusinessObjects Enterprise<br>◆ AdminStudio 10.0 Standard Edition<br>◆ ZENworks Handheld Management |
| Endpoint Lifecycle Management Suite | ◆ ZENworks 11 SP1 Configuration Management<br>◆ ZENworks 11 SP1 Asset Management<br>◆ ZENworks 11 SP1 Patch Management<br>◆ ZENworks Reporting Server powered by BusinessObjects Enterprise<br>◆ AdminStudio 10.0 Standard Edition<br>◆ ZENworks Application Virtualization 8.0.3 |

[1] ZENworks 11 SP1 Advanced Edition also includes a 60-day evaluation license for ZENworks 11 SP1 Asset Management and ZENworks 11 SP1 Endpoint Security Management.

# Product Overview

2

Novell ZENworks 11 SP1 provides comprehensive management of Windows and Linux servers and workstations, collectively referred to as devices. Both Windows and Linux devices can act as servers in ZENworks 11 SP1.

Review the following sections:


- Section 2.1, “ZENworks Capabilities,” on page 13
- Section 2.2, “System Architecture,” on page 14


## 2.1 ZENworks Capabilities

The following table lists the capabilities provided by the products bundled in ZENworks 11 SP1:

***Table 2-1*** *ZENworks 11 SP1 Capabilities*

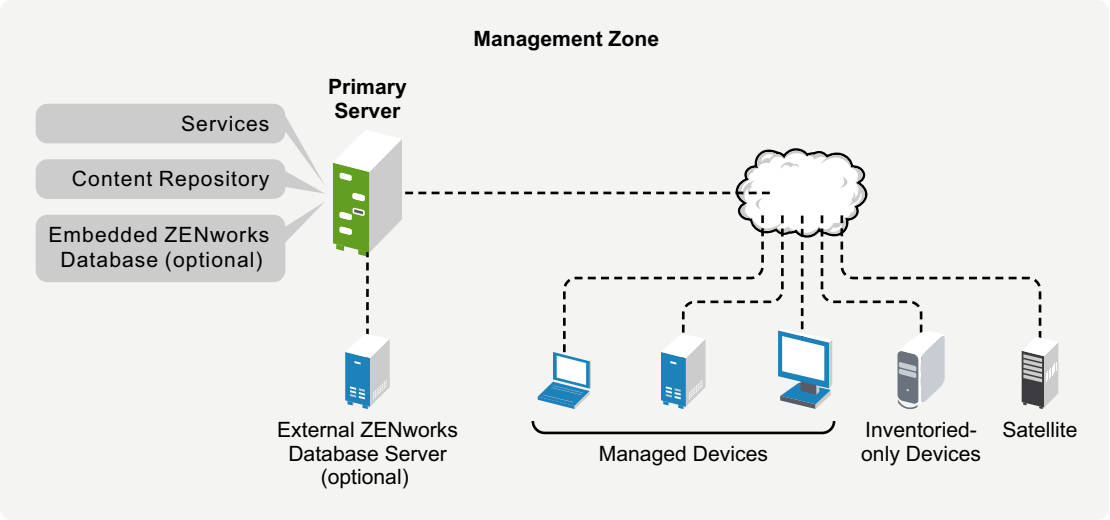
| ZENworks Capabilities | Asset Management | Configuration Management | Endpoint Security Management | Patch Management |
|---|---|---|---|---|
| Discover deployable devices in your network and create deployment tasks to deploy ZENworks software to them | ✓ | ✓ | ✓ | ✓ |
| Manage and deploy software on your devices | | ✓ | | |
| Manage your device configuration and application settings through the use of policies | | ✓ | | |
| Automate the application of images and scripts | | ✓ | | |
| Remotely manage devices by using a secure and fast interface | | ✓ | | |
| Creating configurations by applying policies for Windows and Linux devices | | ✓ | | |
| Collect hardware and software inventory | ✓ | ✓ | ✓ | ✓ |
| Generate reports for policies, inventory, bundles, and messages | ✓ | ✓ | ✓ | ✓ |
| Convert and customize legacy software installations to industry standard MSIs for easy deployment (http://www.novell.com/documentation/zenworks11/pdfdoc/adminstudio/AS10UserGuide.pdf) | | ✓ | | |
| Manage application of software patches automatically and consistently to minimize vulnerabilities and issues | | | | ✓ |

| ZENworks Capabilities | Asset Management | Configuration Management | Endpoint Security Management | Patch Management |
|---|---|---|---|---|
| Manage your software assets | ✓ | | | ✓ |
| Control the use of local optical media and all attached storage devices | | ✓ | ✓ | |
| Update your ZENworks 11 SP1 software on all devices in the Management Zone where the software is installed | ✓ | ✓ | ✓ | ✓ |
| Automate the process of migrating a set of customized system and application settings | | ✓ | | |
| Manage Linux devices | ✓ | ✓ | | ✓ |
| Implement endpoint security by combining security policy enforcement for data, devices, and connectivity under a single management console | | ✓ | ✓ | ✓ |
| Provision Intel AMT capable devices and manage their power states through out-of-band means. | | ✓ | | |

## 2.2 System Architecture

The ZENworks system architecture consists of components such as Primary Servers, Satellite Servers, and managed devices. These components are organized into management domains, referred to as Management Zones.

***Figure 2-1*** *Management Zone*



A Management Zone consists of at least one Primary Server, Satellites (if needed), and one or more managed devices or inventoried-only devices. The Primary Servers and Satellites work together to manage the devices. The zone's information is stored in a database that resides on one of the Primary Servers or externally on another server that does not have ZENworks installed on it.

### 2.2.1 Primary Server

The Primary Server is the focal point of the ZENworks system. Depending on the number and location of the devices that you want to manage with ZENworks, you might need additional Primary Servers. The ZENworks services are added to each Primary Server (physical or virtual) during installation and configuration of the ZENworks software.

You can also set up the Primary Server by deploying ZENworks Appliance to the supported virtual infrastructure. ZENworks Appliance is built on the customized SUSE Linux Enterprise Server 11 JeOS (SLES 11), and is preinstalled with the ZENworks Server.

The Primary Server contains the following ZENworks components:

- **ZENworks services:** The ZENworks software that provides software management, policy enforcement, imaging, inventory collection, asset management, and so forth. The main services are ZENworks Server Service, ZENworks Loader, ZENworks Imaging Service, and ZENworks Management Service.
- **Content repository:** The content repository is used extensively with ZENworks Configuration Management to store software files waiting to be distributed to devices; however, it has limited use with ZENworks Asset Management.

  In ZENworks Configuration Management, it contains the software, policies, and configuration metadata (stored in the database). The policies and software are available for delivery to managed devices within the system. The content is compressed and encrypted. By default, content is automatically replicated among all Primary Servers in the Management Zone, based on a schedule that you control. However, you can configure this to exclude certain servers. It also contains the update packages used to update the ZENworks system files.

  In ZENworks Asset Management, it contains the update packages used to update the ZENworks system files and the Product Recognition Updates used for product recognition during inventorying of software and hardware.
- **ZENworks database:** Contains information about the software bundles for delivery, the hardware and software inventory lists collected from devices, information about the ZENworks Control Center objects (devices, users, bundles, policies, and so on), centralized system messages, license tracking and usage data, and other transactional data, and the actions scheduled to take place within the system.

  You can install the embedded Sybase SQL Anywhere database that is included with ZENworks 11 SP1, or you can use an external Sybase SQL database, Oracle database, or a Microsoft SQL database. For detailed information about the supported database versions, see"Database Requirements" in the *ZENworks 11 SP1 Installation Guide*.

  If you use the embedded database, it must reside on one, and only one, Primary Server per Management Zone. If you use an external database, you can install the database on a server that is not a Primary Server. By default, all Primary Servers require access to the ZENworks database, wherever it resides, to write their data.

You can also specify that certain servers roll up their information to other servers.

If you want to use a Microsoft SQL database, you might want to consider locating a Microsoft SQL database in a Microsoft server cluster for accessibility and reliability purposes.

### 2.2.2 Satellite

A Satellite is a device that can perform certain roles that a ZENworks Primary Server normally performs. A Satellite can be any managed or Linux device (server or workstation). When you configure a Satellite device, you specify which roles it performs:

- **Imaging:** Installs the Imaging services and adds the Imaging role to the device. With this role, the device can be used as an Imaging server to perform all the Imaging operations, such as taking an image and applying an image within as well as across subnets by using unicast or multicast imaging.
- **Collection:** If you want to improve information roll-up access for a group of devices to minimize traffic to the ZENworks Primary Server that is hosting the ZENworks database, you can enable the Collection role on a device. For example, if you have devices that are rolling up information to a Primary Server outside of their network segment, you can minimize network traffic by enabling the Collection role on a device within the network segment to accept the information from the other devices in that segment. That Collection role device is then the only device from that segment that is rolling up information to the Primary Server.
- **Content:** If you want to improve content access for a group of devices without creating another Primary Server, you can create the Content role on a device. For example, if you have devices that are accessing a Primary Server outside of their network segment, you can create the Content role on a device within the network segment to service those devices.
- **Authentication:** If you want to speed up the authentication process of the devices with the ZENworks Management Zone, you can enable the Authentication role on a device. Satellite devices with the Authentication role can now speed the authentication process by spreading the workload among various devices and by performing authentication locally to managed devices.You can have multiple Satellite devices with the Authentication role. In addition, each Satellite with the Authentication role can have multiple user sources configured and each Satellite can have multiple connections to each user source to provide failover.

For more information, see "Satellites" in the *ZENworks 11 SP1 System Administration Reference*.

### 2.2.3 Managed Device

A managed device is a Windows or Linux device that you can use ZENworks to manage. The ZENworks Adaptive Agent must be installed on each device in order for it to be managed. The Adaptive Agent communicates with a Primary Server to enable delivery of software, enforcement of configuration policies, inventorying of hardware and software, and remote management of the device.

Each managed device attempts to contact its initial Primary Server. However, if content is unavailable on that Primary Server, the managed device requests it from another Primary Server or a Satellite Server with the Content role configured in the Management Zone, and continues until it finds a server that can provide the content.

A managed device can be registered in only one Management Zone and is therefore managed only in that zone.

### 2.2.4 Inventoried-Only Device

You might have devices where the Adaptive Agent cannot be installed, or devices where you do not want to install the Adaptive Agent. To inventory these devices, you can either install the Inventory-Only agent or run the Portable Collector.

For more information, see the *ZENworks 11 SP1 Discovery, Deployment, and Retirement Reference*.

### 2.2.5 Management Zone

A Management Zone consists of one or more Primary Servers and one or more managed devices. The Primary Servers in the zone work together to manage the devices. The zone's information is stored in a database that resides on one of the Primary Servers or externally on another server that does not have ZENworks installed on it. The zone might also contain Satellites.

# ZENworks Terminology

3

| Term | Description |
|---|---|
| bundle | ZENworks Configuration Management has four types of bundles:<br>◆ **Linux Bundle:** Allows you to configure and manage applications on Linux devices<br>◆ **Linux Dependency Bundle:** Allows the software packages to be available on Linux devices to resolve package dependencies.<br>◆ **Preboot Bundle:** Performs operations before the operating system boots. The various Imaging bundle types let you install images on one or more devices, or run ZENworks scripts containing any commands that you can issue from the imaging bash prompt.<br>◆ **Windows Bundle:** Distributes a Microsoft Windows Installer (MSI) package, Microsoft Windows Software Patch (MSP) package, thin-client application, or other Windows-based applications to a Windows device.<br>For more information, see the *ZENworks 11 SP1 Software Distribution Reference*. |
| content repository | Contains the files, policies, and other items that are available for delivery to managed devices within the system. The content is compressed and encrypted. For more information, see "Content" in the *ZENworks 11 SP1 System Administration Reference*. |
| inventoried-only device | Device where the ZENworks Adaptive Agent is not or cannot be installed. Instead, you install the Inventory Only Module on these devices so that you can use Asset Inventory to inventory them. Optionally, you can run the Portable Collector to inventory them. For more information, see "Adaptive Agent Versus Inventory-Only Module" and "Deploying the Inventory-Only Module" in the *ZENworks 11 SP1 Discovery, Deployment, and Retirement Reference*. |
| Inventory Only Module | Software installed on a device that enables it to be inventoried. This is normally installed on devices running the Mac OS X, NetWare 5.1/6/6.5, OES (NetWare), Unix (Sun Solaris, HP UX, or IBM AIX), or Linux operating systems, which are not supported as managed devices. |
| managed device | A Windows or Linux device that has the Adaptive Agent installed and is registered in the Management Zone. |
| management console or administration workstation | The device where you run ZENworks Control Center in your Web browser. |
| Management Zone | Consists of at least one Primary Server. It can contain other Primary Servers and one or more workstations as managed devices. It can also contain inventoried-only devices. |
| policy | A set of rules and information that can define both operating system and application configuration settings for a managed device. For more information, see the *ZENworks 11 SP1 Configuration Policies Reference*. |

| Term | Description |
|---|---|
| Primary Server | A machine that contains the ZENworks services and content repository. Optionally, it might also contain the ZENworks database, but on only one of the Primary Servers per zone. A Management Zone can have multiple Primary Servers. |
| Portable Collector | A software utility that can inventory any device and create a file that is accessible in ZENworks Control Center as if it were a device. This file is then used for obtaining inventory data about the device. For more information, see "Using the Portable Collector" in the *ZENworks 11 SP1 Asset Inventory Reference*. |
| Remote Management Service | A managed device component that enables remote operators to perform remote sessions on the device. For more information, see the*ZENworks 11 SP1 Remote Management Reference*. |
| Remote Management Proxy | A proxy server that forwards Remote Management operation requests from the Remote Management Viewer to a managed device. The proxy is useful when the viewer cannot directly access a managed device that is in a private network or on the other side of a firewall or router that is using NAT (Network Address Translation). As a prerequisite, the proxy must be installed on a Windows managed device or a Linux device. For more information, see the *ZENworks 11 SP1 Remote Management Reference*. |
| Satellite | A Satellite is a device that can perform certain roles that a ZENworks Primary Server normally performs. A Satellite can be any managed Windows or Linux device (server or workstation). When you configure a Satellite device, you specify which roles it performs (Imaging, Collection, or Content).<br><br>For more information, see "Satellites" in the *ZENworks 11 SP1 System Administration Reference*. |
| ZENworks Adaptive Agent | Software installed on a Windows or Linux device that enables it to be managed by a Primary Server. The Adaptive Agent consists of modules that support software delivery, policy enforcement, imaging, remote management, inventory, and so forth. For more information, see"ZENworks Adaptive Agent Deployment" in the *ZENworks 11 SP1 System Administration Reference*. |
| ZENworks Control Center | The Web-based administrative console used to manage the ZENworks Configuration Management system. For more information, see"ZENworks Control Center" in the *ZENworks 11 SP1 Administration Quick Start*. |
| ZENworks database | The database that contains information about the software available for delivery, the hardware and software inventory lists collected from devices, and the actions scheduled to take place within the system.<br><br>The database can reside on a Primary Server, or it can reside on a remote server as an external database. By default, all Primary Servers require access to the database.<br><br>For information on supported databases, see "Database Requirements" in the *ZENworks 11 SP1 Installation Guide*.<br><br>For more information on the ZENworks database, see "Database Management" in the *ZENworks 11 SP1 System Administration Reference*. |

| Term | Description |
| --- | --- |
| zman | A command line interface for managing your ZENworks system. The zman utility is useful for automating tasks (through scripts) and performing mass management tasks that might be tedious to perform in ZENworks Control Center. For example, configuring settings for a large number of devices, or adding an action to a large number of bundles.<br><br>zman is available on all Primary Servers.<br><br>For more information, see "ZENworks Command Line Utilities" in the *ZENworks 11 SP1 Command Line Utilities Reference*. |
| zac | A command line management interface for the Novell ZENworks Adaptive Agent. The zac utility performs command line management functions on the ZENworks managed device, including installing and removing software bundles, applying policies, and registering and unregistering the device. |

# System Configuration

The following sections provide information to help you configure your ZENworks system. The configuration tasks apply regardless of which ZENworks 11 SP1 products (Configuration Management, Patch Management, Asset Management, and Endpoint Security Management) you are using.


- Chapter 4, “Quick List,” on page 25
- Chapter 5, “Management Tools,” on page 29
- Chapter 6, “Management Zone Configuration,” on page 35
- Chapter 7, “ZENworks Adaptive Agent Deployment,” on page 61
- Chapter 8, “System Messages and Reports,” on page 73

# Quick List

# 4

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 Novell ZENworks 11 SP1.

Before you begin using any of the ZENworks 11 SP1 products (Configuration Management, Patch Management, Asset Management, and Endpoint Security Management) 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:


- Section 4.1, "Management Tools," on page 25
- Section 4.2, "Zone Configuration," on page 25
- Section 4.3, "Agent Deployment," on page 27
- Section 4.4, "System Messages and Reports," on page 28


## 4.1 Management Tools

ZENworks 11 SP1 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 Section 5.1, "ZENworks Control Center," on page 29. |
| 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.<br><br>For instructions, see Section 5.2, "zman Command Line Utility," on page 31. |
| Discover how to run the zac utility | The zac utility is a command line interface for the ZENworks Adaptive Agent.<br><br>For instructions, see Section 5.3, "zac Command Line Utility," on page 33. |

## 4.2 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 |
|---|---|
| Create folders and groups for organizing devices | 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.<br><br>For instructions, see Section 6.1, “Organizing Devices: Folders and Groups,” on page 35. |
| Create registration keys or rules | The ZENworks Adaptive Agent must be installed on each device that you want to manage. When you deploy the ZENworks Adaptive Agent to a device, the device is registered in your Management Zone.<br><br>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.<br><br>For instructions, see Section 6.2, “Creating Registration Keys and Rules,” on page 41. |
| Add user sources | You can connect to one or more LDAP directories to provide authoritative user sources in ZENworks.<br><br>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:<br><br>◆ **Configuration Management:** Enables you to assign bundles and policies to users as well as devices. Enables user-based inventory reports.<br>◆ **Asset Management:** Enables you to account for software licenses on a user basis as well as a device basis.<br>◆ **Endpoint Security Management:** Enables you to assign policies to users as well as devices.<br><br>For instructions, see Section 6.3, “Connecting to User Sources,” on page 46. |
| Create additional administrator accounts | 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.<br><br>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.<br><br>For instructions, see Section 6.4.1, “Creating Administrator Account,” on page 48. |

| Task | Details |
|---|---|
| Create administrator group accounts | 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.<br><br>For instructions, see Section 6.4.2, “Creating Administrator Group Account,” on page 50. |
| Modify zone configuration settings | 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.<br><br>For instructions, see Section 6.5, “Modifying Configuration Settings,” on page 53. |
| Updating ZENworks Software | The System Updates feature allows you to obtain updates to the Novell ZENworks 11 SP1 software on a timely basis, and also allows you to schedule automatic downloads of the updates.<br><br>For instructions, see Section 6.6, “Updating ZENworks Software,” on page 55. |
| Creating Locations | 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 Adaptive Agent determines that the device’s network environment matches the environment defined for the location.<br><br>For instructions, see Section 6.7, “Creating Locations,” on page 55. |

## 4.3 Agent Deployment

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

| Task | Details |
|---|---|
| Enable the ZENworks Adaptive Agent features | The ZENworks Adaptive Agent includes features specific to each of the ZENworks 11 SP1 products (Configuration Management, Patch Management, Asset Management, and Endpoint Security 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.<br><br>For instructions, see Section 7.1, “Configuring Adaptive Agent Features,” on page 61. |

| Task | Details |
|---|---|
| Discover devices | If you choose to use ZENworks Control Center to deploy the agent to devices, you must first add the devices to your Management Zone. You can do this by performing a network discovery. |
| Import devices | You can also import devices into your Management Zone from a comma-separated values (CSV) file. Each device entry must include its IP address or DNS name. |
| Install the ZENworks Adaptive Agent | You can use a variety of methods to install the ZENworks Adaptive Agent to a device:<br>◆ Use ZENworks Control Center to deploy the agent from a ZENworks Server to the device.<br>◆ At the device, use a Web browser to download the agent from a ZENworks Server and install it.<br>◆ Include the agent in an image and apply the image to the device.<br>For instructions, see Section 7.2, "Installing the ZENworks Adaptive Agent," on page 64. |
| Log in and use the ZENworks Adaptive Agent | To receive user-assigned bundles and policies on a device, you must log in to the Management Zone.<br>For instructions, see Section 7.3, "Using the ZENworks Adaptive Agent," on page 67. |

## 4.4 System Messages and Reports

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 | The ZENworks system generates informational, warning, and error messages to help you monitor activities such as the distribution of software and application of policies.<br>For instructions, see Section 8.1, "Viewing System Messages," on page 73. |
| Create a Watch List | If you have devices, bundles, and policies whose activity you want to closely monitor, you can add them to the Watch List.<br>For instructions, see Section 8.2, "Creating a Watch List," on page 76. |
| Generate reports | Generate reports for devices, bundles, policies, and much more.<br>For instructions, see Section 8.3, "Generating Reports," on page 76. |

# Management Tools

Novell ZENworks 11 SP1 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:


- Section 5.1, “ZENworks Control Center,” on page 29
- Section 5.2, “zman Command Line Utility,” on page 31
- Section 5.3, “zac Command Line Utility,” on page 33


## 5.1 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, ZCC can be accessed from any supported workstation.

If you use Novell iManager to administer other Novell products in your network environment, you can enable ZCC to be launched from iManager. For more information, see the *ZENworks 11 SP1 System Administration Reference*.


- Section 5.1.1, “Accessing ZENworks Control Center,” on page 29
- Section 5.1.2, “Navigating ZENworks Control Center,” on page 30


### 5.1.1 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 11 SP1 System Administration Reference*.

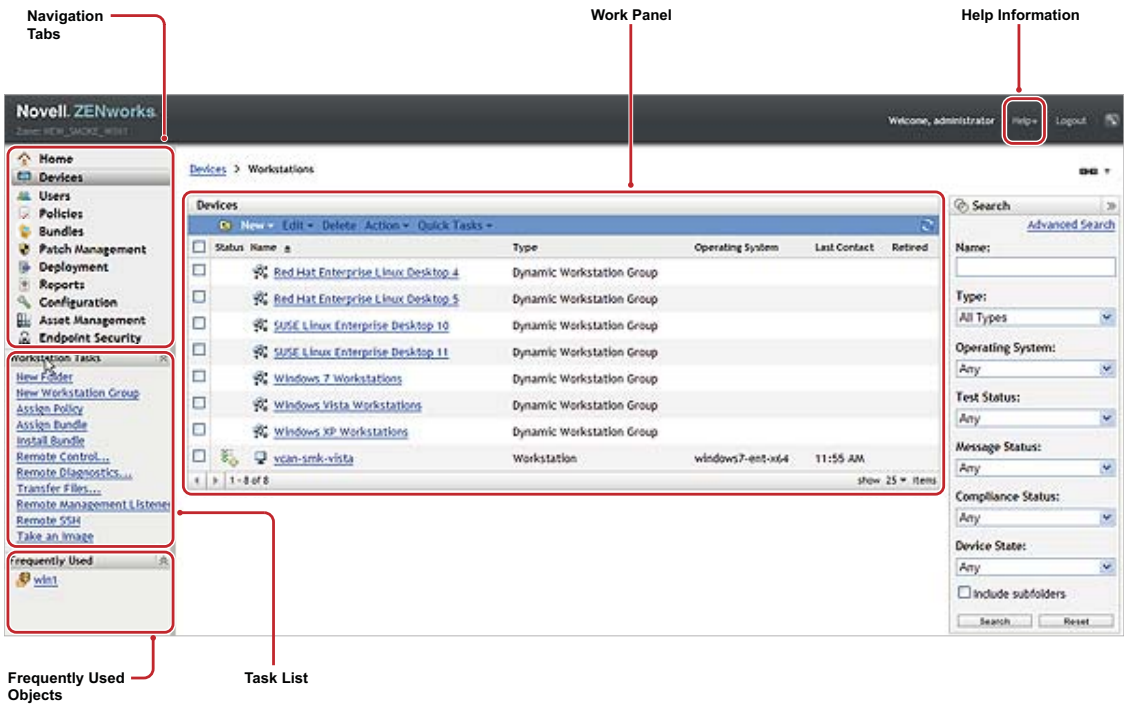
4 Click *Login* to display ZENworks Control Center.

   For more detailed information on logging in as a different administrator, see "Accessing ZENworks Control Center" in the *ZENworks 11 SP1 System Administration Reference*.

If you use Novell iManager as the management tool for other Novell products, you can set up ZENworks Control Center to be available through iManager. For instructions, see "Accessing ZENworks Control Center through Novell iManager" in the *ZENworks 11 SP1 System Administration Reference*.

### 5.1.2 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.

## 5.2 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.


- Section 5.2.1, "Location," on page 32
- Section 5.2.2, "Syntax," on page 32
- Section 5.2.3, "Help with Commands," on page 32


## 5.2.1 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:\novell\zenworks\bin`. On Linux, the default path is `/opt/novell/zenworks/bin`.

## 5.2.2 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.

## 5.2.3 Help with Commands

The best way to understand the commands is to use the online help or see "zman(1)" in the *ZENworks 11 SP1 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 |
|---|---|
| `zman --help \| more` | Displays a complete list of commands by category. |
| `zman` *`category`* `--help \| more` | Displays a complete list of commands within a category. |

| Command | Description |
| --- | --- |
| `zman` *`command`* `--help \| more` | Displays help for a command |

# 5.3 zac Command Line Utility

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


- Section 5.3.1, “Location,” on page 33
- Section 5.3.2, “Syntax,” on page 33
- Section 5.3.3, “Help with Commands,” on page 33


## 5.3.1 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.

## 5.3.2 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.

## 5.3.3 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 11 SP1 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 |
|---|---|
| `zac --help` | Displays a complete list of commands. |
| `zac` *`command`* `--help` | Displays detailed help for a command. |

# Management Zone Configuration

Novell ZENworks 11 SP1 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.


- Section 6.1, "Organizing Devices: Folders and Groups," on page 35
- Section 6.2, "Creating Registration Keys and Rules," on page 41
- Section 6.3, "Connecting to User Sources," on page 46
- Section 6.4, "Creating ZENworks Administrator Accounts," on page 48
- Section 6.5, "Modifying Configuration Settings," on page 53
- Section 6.6, "Updating ZENworks Software," on page 55
- Section 6.7, "Creating Locations," on page 55


## 6.1 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 41).


- Section 6.1.1, "Folders," on page 35
- Section 6.1.2, "Groups," on page 37
- Section 6.1.3, "Assignment Inheritance for Folders and Groups," on page 41


### 6.1.1 Folders

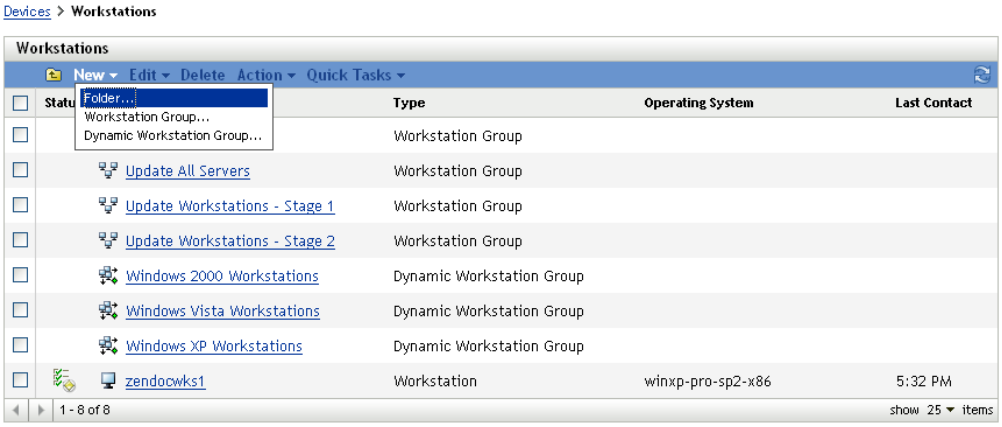
Folders are a great tool to help you organize devices in order to simplify management of those devices. You can apply configuration settings, assign content, and perform tasks on any folder. When you do so, the folder's devices inherit those settings, assignments, and tasks.

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 37 below).

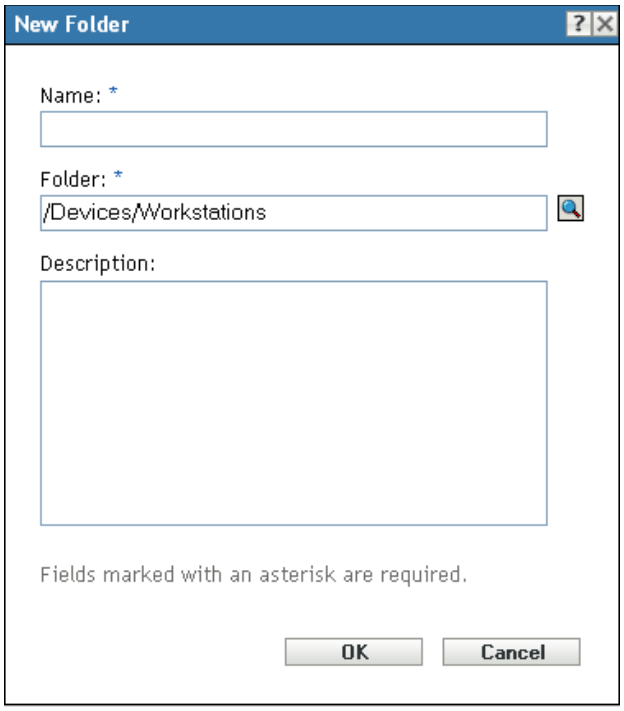
For example, assume that you have workstations at three different sites. You want to apply different configuration settings to the workstations at the three sites, so you create three folders (`/Workstations/Site1`, `/Workstations/Site2`, and `/Workstations/Site3`) and place the appropriate workstations 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* 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 11 SP1 Command Line Utilities Reference*.

## 6.1.2 Groups

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

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

For example, let's revisit the example of the workstations at three different sites (see Section 6.1.1, "Folders," on page 35). 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.

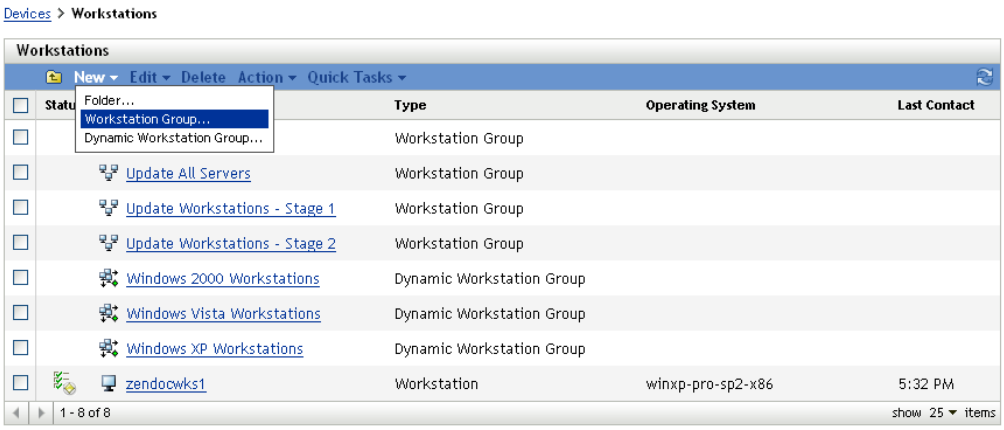
ZENworks include several predefined dynamic server groups (Windows 2000 Servers and Windows 2003 Servers) and dynamic workstation groups (Windows XP Workstation, Windows 2000 Workstation, and Windows Vista Workstations). Any devices that have these operating systems are automatically added to the appropriate dynamic group.

### Creating a Group

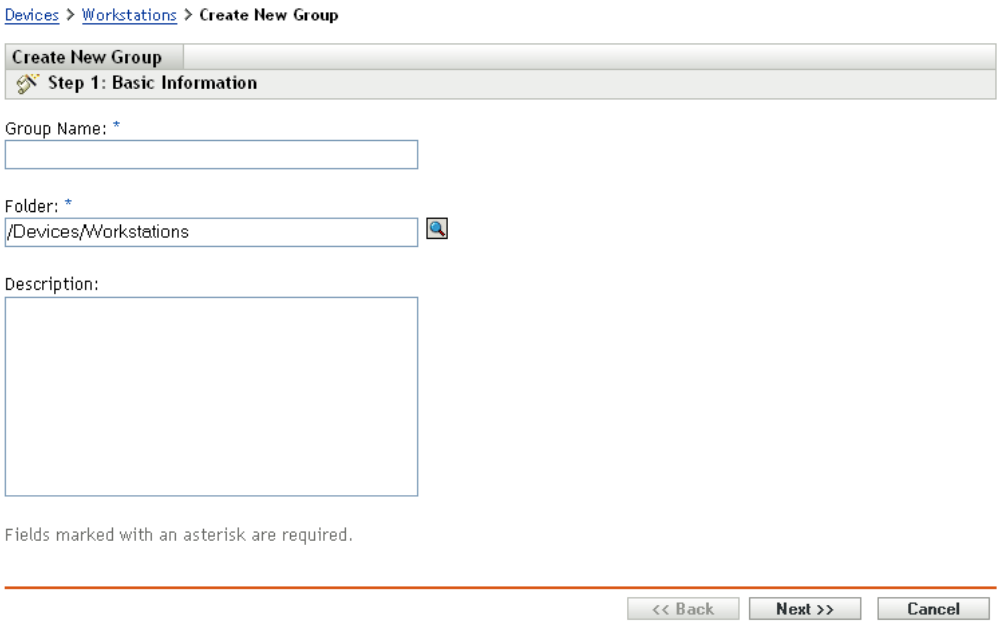
1. In ZENworks Control Center, click the *Devices* tab.
2. If you want to create a group for servers, click the *Servers* folder.

   or

   If you want to create a group for workstations, click the *Workstations* folder.




3. Click *New* > *Server Group* (or *New* > *Workstation Group* for workstations) 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 11 SP1 Command Line Utilities Reference*.

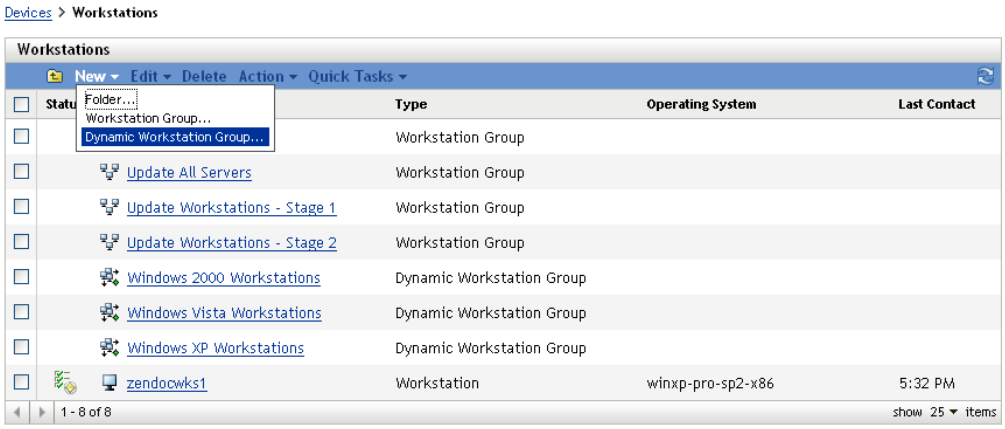
### Creating a Dynamic Group

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

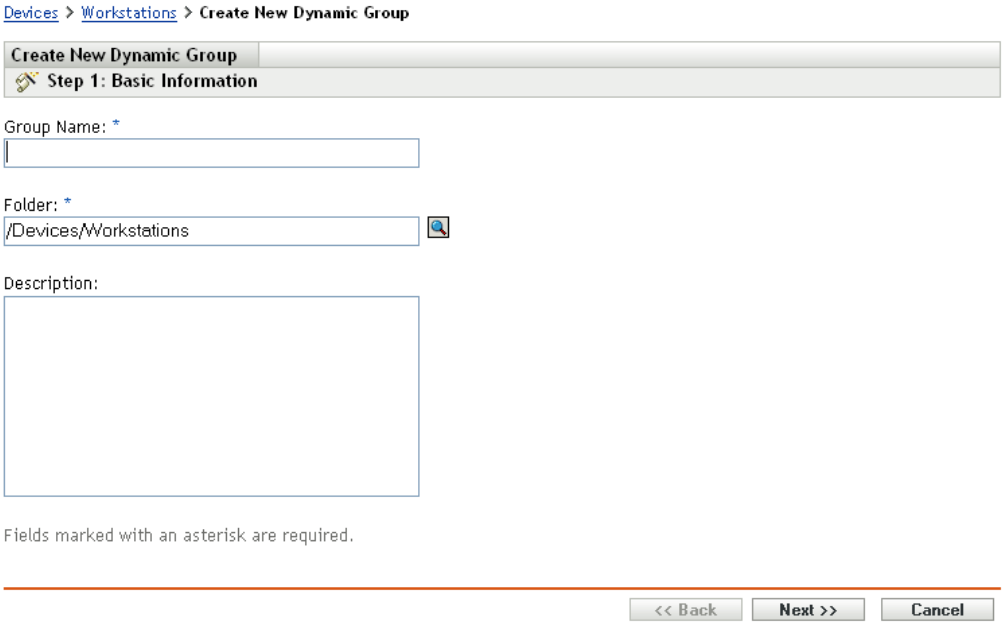
2 If you want to create a group for servers, click the *Servers* folder.

   or

   If you want to create a group for workstations, click the *Workstations* folder.




**3** Click *New* > *Dynamic Server Group* (or *New* > *Dynamic Workstation Group* for workstations) to launch the Create New Group Wizard.




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

The group name must follow the naming conventions.

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

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

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

### 6.1.3 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.

## 6.2 Creating Registration Keys and Rules

When you deploy the ZENworks Adaptive 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.


- Section 6.2.1, "Registration Keys," on page 41
- Section 6.2.2, "Registration Rules," on page 43
- Section 6.2.3, "Device Naming Template," on page 44
- Section 6.2.4, "Where to Find More Information," on page 46

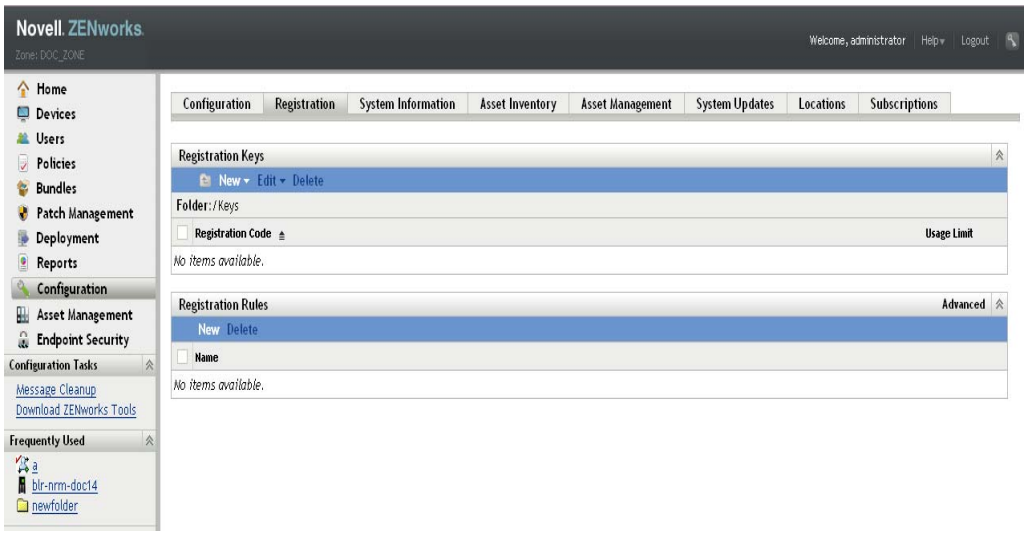

### 6.2.1 Registration Keys

A registration key is an alphanumeric string that you manually define or randomly generate. During deployment of the ZENworks Adaptive 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.

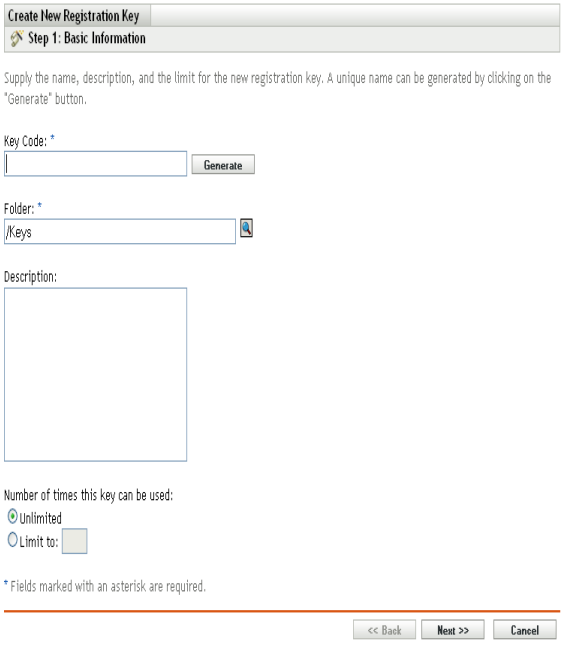
You can create one or more registration keys to ensure that devices are placed in the desired folders and groups. For example, you might want to ensure that all of the Sales department's workstations are added to the `/Workstations/Sales` folder but are divided into three different groups (SalesTeam1, 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 11 SP1 Command Line Utilities Reference*.

## 6.2.2 Registration Rules

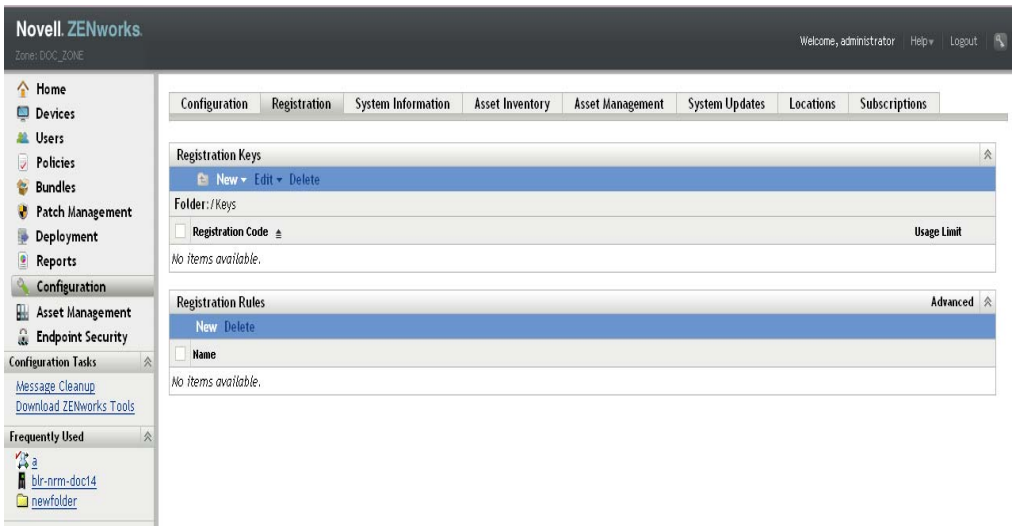
If you don't want to enter a registration key during deployment, or if you want devices to be automatically added to different folders and groups based on predefined criteria (for example, operating system type, CPU, or IP address), you can use registration rules.

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.

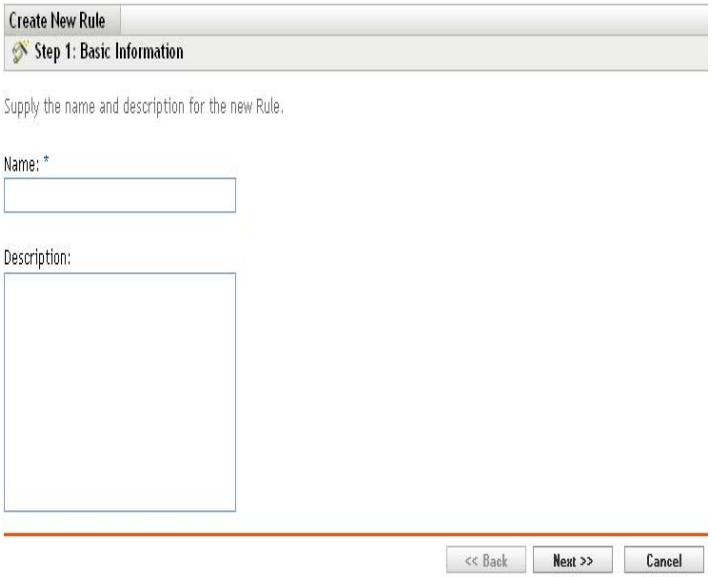
The two default rules are designed to ensure that no server or workstation registration fails. Therefore, you cannot delete or modify these two default rules. You can, however, define additional rules that enable you to filter devices as they register and add them to different folders and groups. If, as recommended in Section 6.1, "Organizing Devices: Folders and Groups," on page 35, 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.

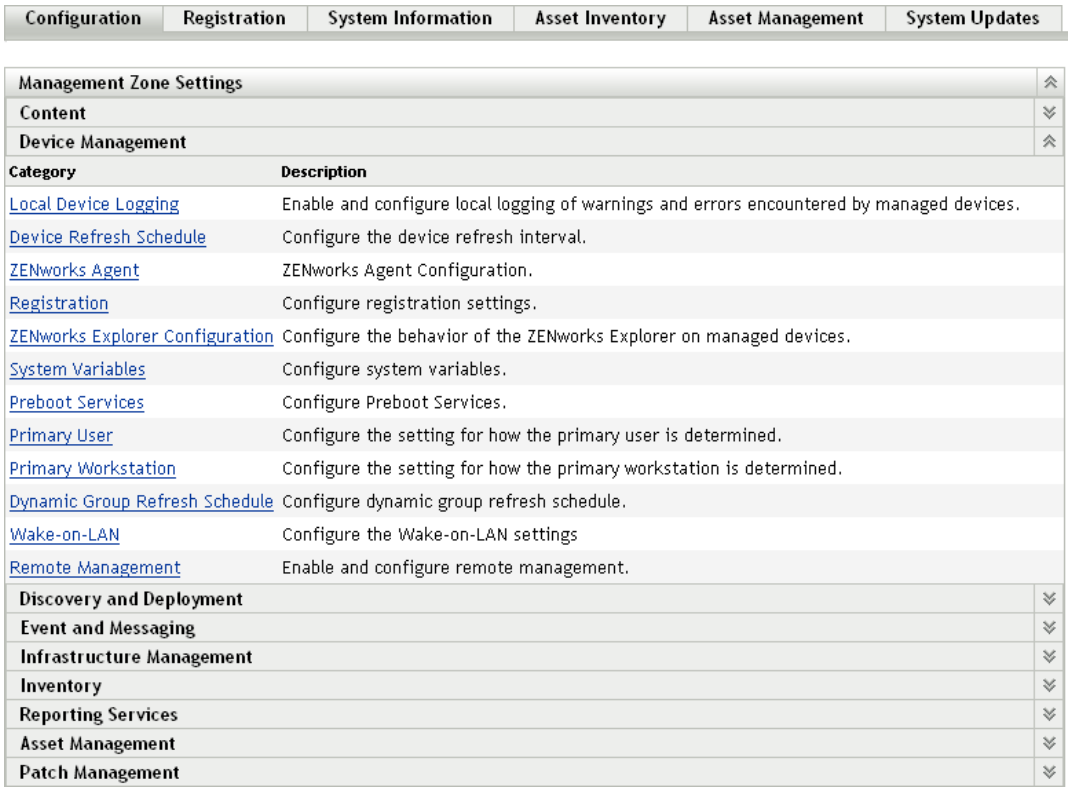
You can also use the `ruleset-create` command in the zman utility to create a registration rule. For more information, see "Ruleset Commands" in the *ZENworks 11 SP1 Command Line Utilities Reference*.

### 6.2.3 Device Naming Template

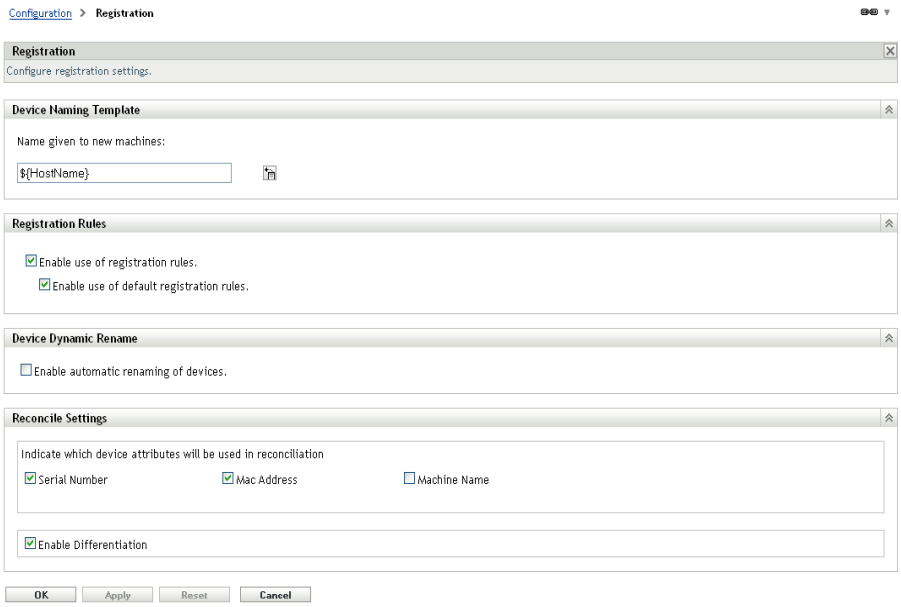
The device naming template determines how devices are named when they register. By default, a device's hostname is used. You can change it to use any combination of the following machine variables: ${HostName}, ${GUID}, ${OS}, ${CPU}, ${DNS}, ${IPAddress}.

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.

### 6.2.4 Where to Find More Information

For more information about registering devices, see the *ZENworks 11 SP1 Discovery, Deployment, and Retirement Reference*.

## 6.3 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 the *ZENworks 11 SP1 System Administration Reference*.

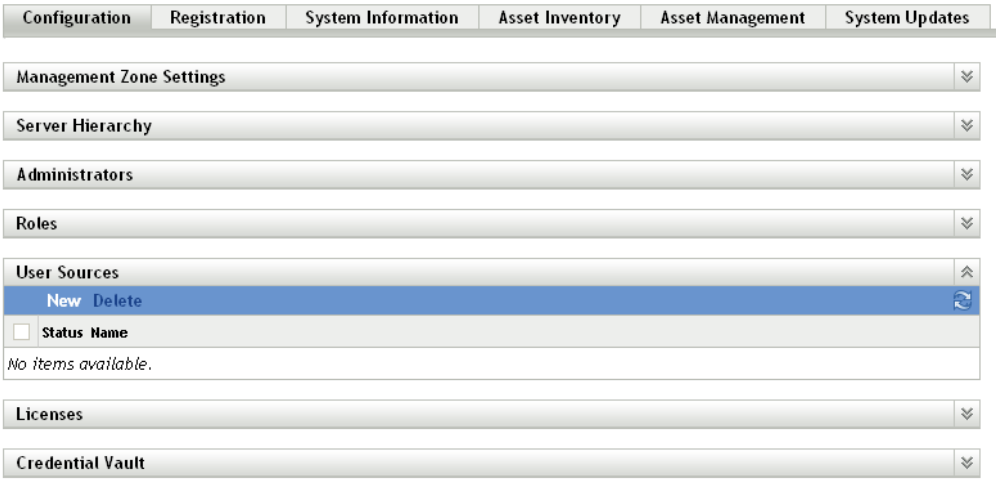
You can connect to Novell eDirectory and Microsoft Active Directory as user sources. The minimum requirements are Novell eDirectory 8.7.3 and Microsoft Active Directory on Windows 2000 SP4. The minimum LDAP requirement is version 3.

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.

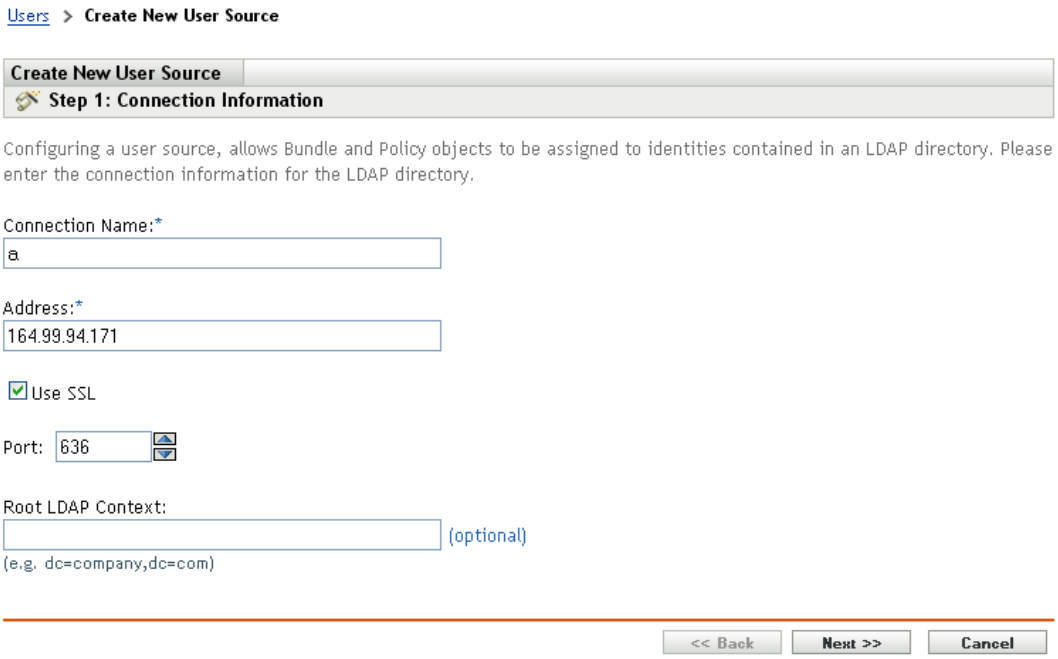
In addition to the users that reside within the containers you add, ZENworks Control Center also displays any user groups located in the containers. This enables management of both individual user and groups of users

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 11 SP1 Command Line Utilities Reference*.

# 6.4 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.

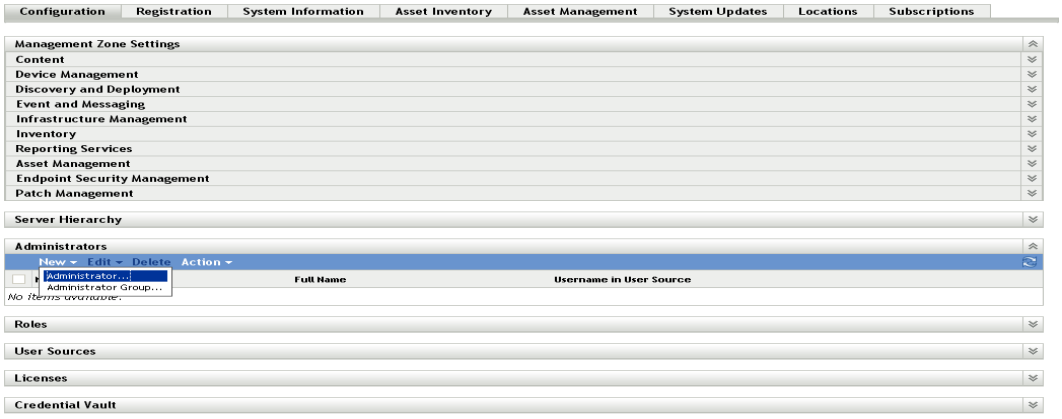
Typically, you should create administrator accounts for each person who will perform administrative tasks. You can define these accounts as Super Administrator accounts, or you can define them as administrator accounts with restricted rights. For example, you could give a user an administrator account that only enables him or her 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.

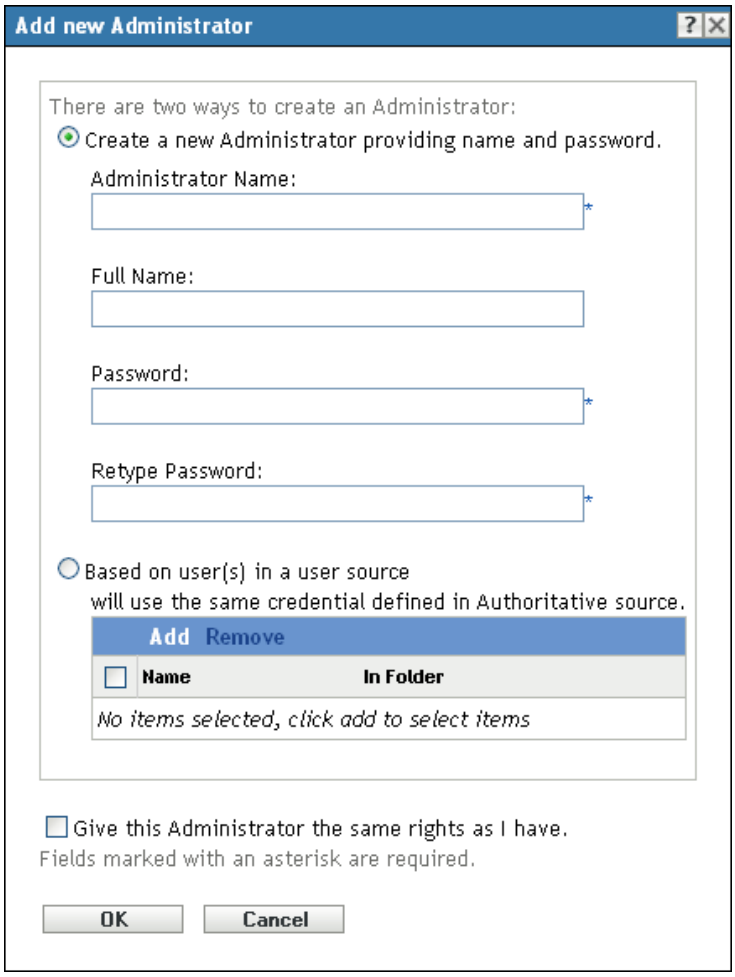
You can choose to create administrator groups. If you assign rights and roles to an administrator group, the assigned rights and roles are applicable to all the members within the group.

## 6.4.1 Creating Administrator Account

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

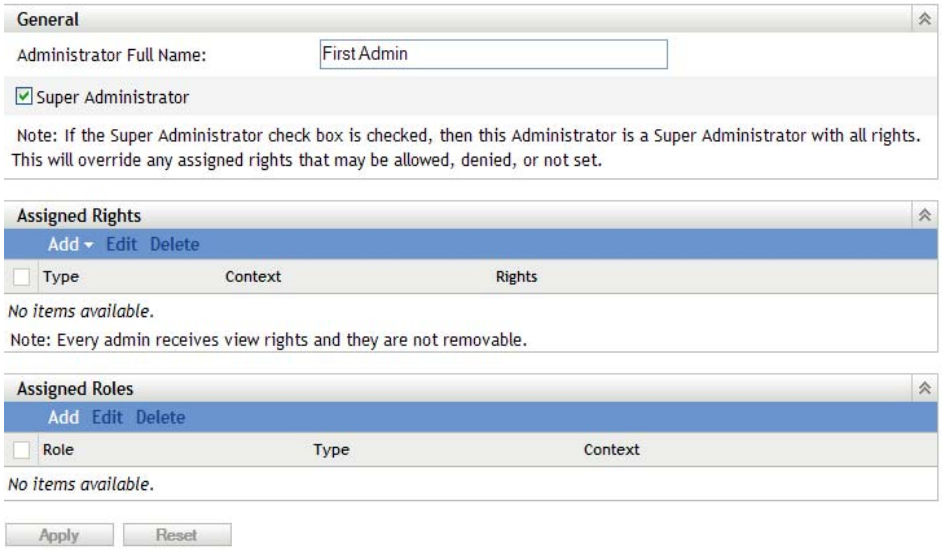
**Create a New Administrator by Providing Name, Password:** Select this option if you want to create a new administrator account by manually specifying the name and password.

**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** When you have finished filling in the fields, 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 *Super Administrator* is selected, deselect the option.

   You cannot modify Super Administrator rights.

7 Using the Assigned Rights panel, modify the assigned rights.

   For information about the options on the page, click the *Help* button, or see "Managing Administrator Rights" in the *ZENworks 11 SP1 System Administration Reference*.

8 Using the Assigned Roles panel, modify the assigned roles.

   For information about the options on the page, click the *Help* button, or see "Managing Administrator Roles" in the *ZENworks 11 SP1 System Administration Reference*.

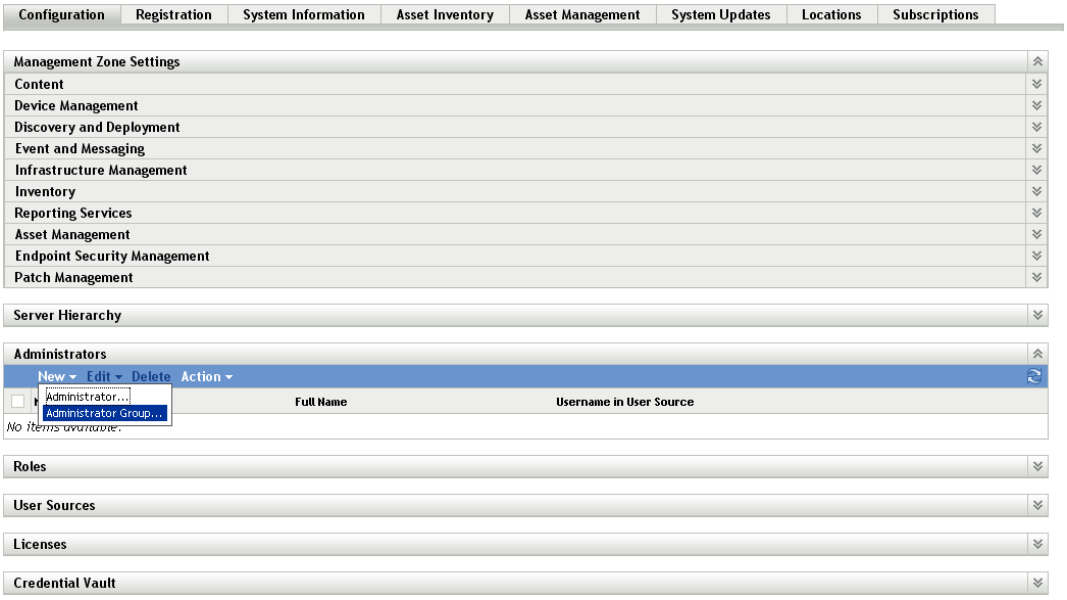
9 When you have finished modifying the rights, click *Apply* to save the changes.

For more information about creating ZENworks administrator accounts, administrator rights, or administrator roles, see "Administrators and Administrator Groups" in the *ZENworks 11 SP1 System Administration Reference*.

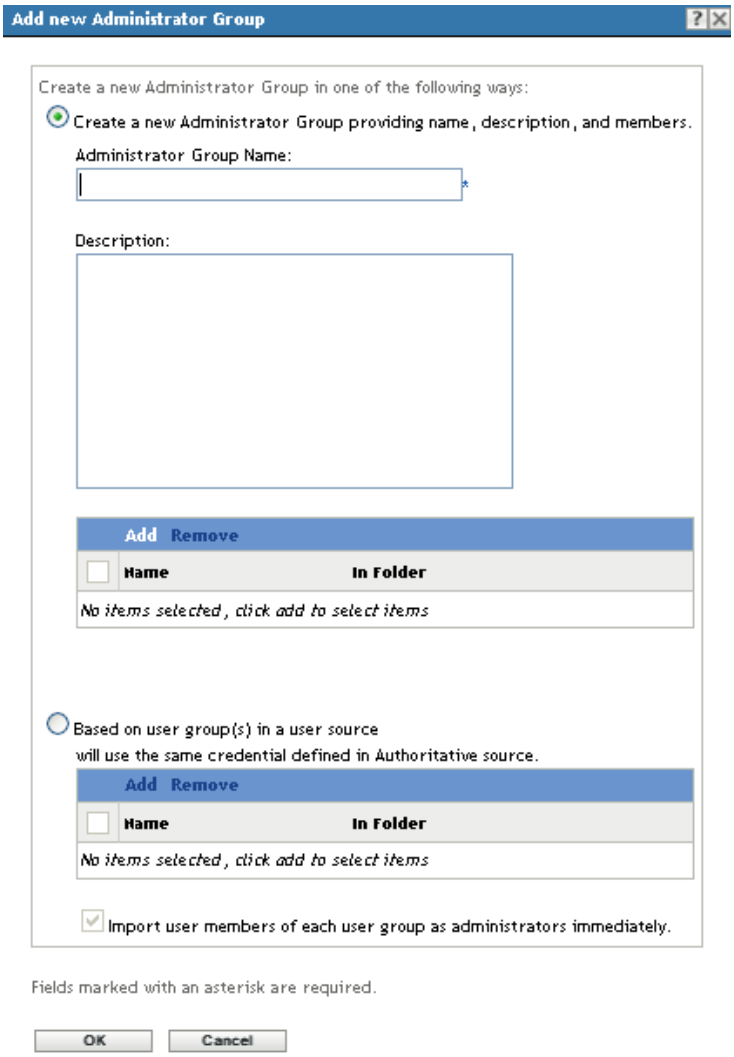
You can also use the `admin-create` command in the zman utility to create a ZENworks administrator account. For more information, see "Administrator Commands" in the *ZENworks 11 SP1 Command Line Utilities Reference*.

## 6.4.2 Creating Administrator Group Account

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




**2** In the Administrators panel, click *New* > *Administrator Group* to display the Add 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 administrators you want.

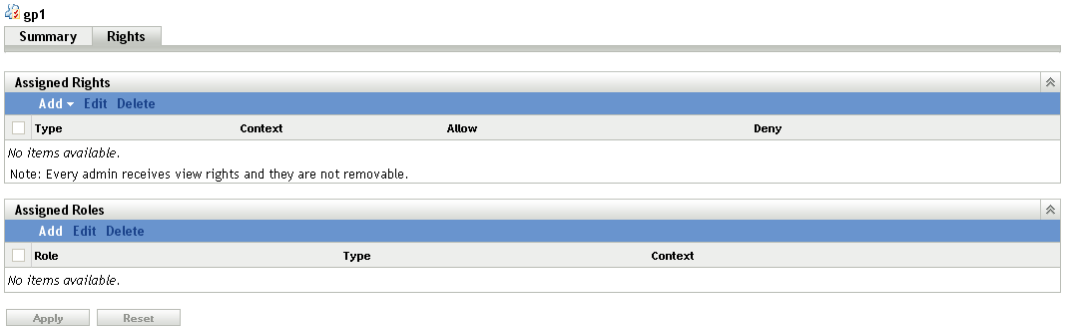
You can add any number of administrators to the group. You cannot add other administrator groups to the group.

**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 user group you want.

**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 When you have finished filling in the fields, 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.

For information about the options on the page, click the *Help* button, or see "Managing Administrator Group Rights" in the *ZENworks 11 SP1 System Administration Reference*.

7 Using the Assigned Roles panel, modify the assigned roles.

For information about the options on the page, click the *Help* button, or see "Managing Administrator Roles" in the *ZENworks 11 SP1 System Administration Reference*.

8 When you have finished modifying the rights, click *Apply* to save the changes.

For more information about creating ZENworks administrator Group accounts, administrator rights, or administrator roles, see "Administrators and Administrator Groups" in the *ZENworks 11 SP1 System Administration Reference*.

## 6.5 Modifying Configuration Settings

The Management Zone configuration settings enable you to control a wide range of functionality behavior for you 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 Adaptive 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 discussed in Section 6.1, "Organizing Devices: Folders and Groups," on page 35, 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, as necessary, override the settings on folders and devices.

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


- Section 6.5.1, "Modifying Configuration Settings at the Zone," on page 54
- Section 6.5.2, "Modifying Configuration Settings on a Folder," on page 54
- Section 6.5.3, "Modifying Configuration Settings on a Device," on page 54


## 6.5.1 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 (*Device Management*, *Discovery and Deployment*, *Event and Messaging*, and so forth) whose settings you want to modify.
3. Click the setting to display its details page.
4. Modify the setting as desired.

   For information about the setting, see "Management Zone Settings" in the *ZENworks 11 SP1 System Administration Reference* or click the *Help* button in ZENworks Control Center.
5. When you have finished modifying the setting, click *OK* (or *Apply*) to save your changes.

   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.

## 6.5.2 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. When you've found the folder, click *Details* next to the folder name to display the folder's 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, see "Management Zone Settings" in the *ZENworks 11 SP1 System Administration Reference* or click the *Help* button in ZENworks Control Center.
8. When you have finished modifying the setting, click *OK* (or *Apply*) to save your changes.

   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.

## 6.5.3 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 the 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, see "Management Zone Settings" in the *ZENworks 11 SP1 System Administration Reference* or click the *Help* button in ZENworks Control Center.

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

## 6.6 Updating ZENworks Software

You can update your ZENworks 11 SP1 software on all devices in the Management Zone where the software is installed. Update downloads can be scheduled. Software updates are provided at the Interim Release level and you can choose whether to apply each update after viewing its content (interim releases are cumulative). You can also download the latest Product Recognition Update (PRU) to update your knowledgebase so that ZENworks Inventory can recognize newer software.

For more information, see the *ZENworks 11 SP1 System Administration Reference*.

## 6.7 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, ZENworks supports both global policies and location-based polices. 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 ZENworks Adaptive 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.

The following sections explain how to create locations:

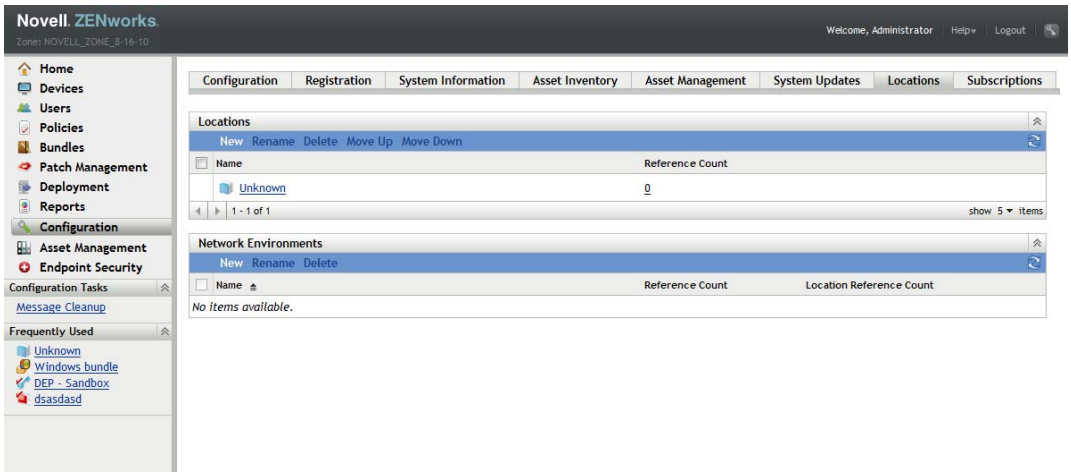
- Section 6.7.1, “Defining a Network Environment,” on page 56
- Section 6.7.2, “Creating Locations,” on page 58
- Section 6.7.3, “Location and Network Environment Selection on a Managed Device,” on page 59

## 6.7.1 Defining a Network Environment

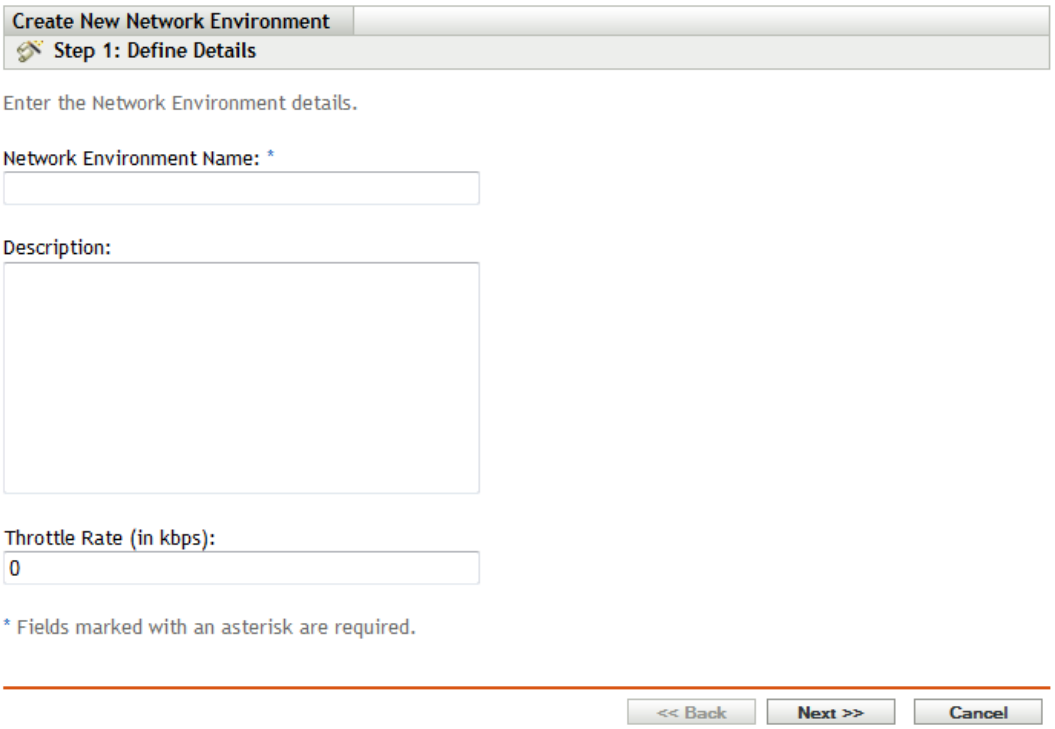
Network environment definitions are the building blocks for locations. You can define a network environment while you are creating a location, but we recommend that you define network environments first and then add them as you are creating locations.

To create a location:

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*.

As you complete the wizard, if you need more information about any fields or options, click the *Help* button located in the upper-right corner of ZENworks Control Center.

4 On the Network Environment Details page, fill in the following fields:

**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 must be matched in order to select this network environment.

Specify the minimum number of defined network services that must be matched 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, keep the following in mind:

- 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 so, the minimum match would never be reached, resulting in the network environment never being selected.

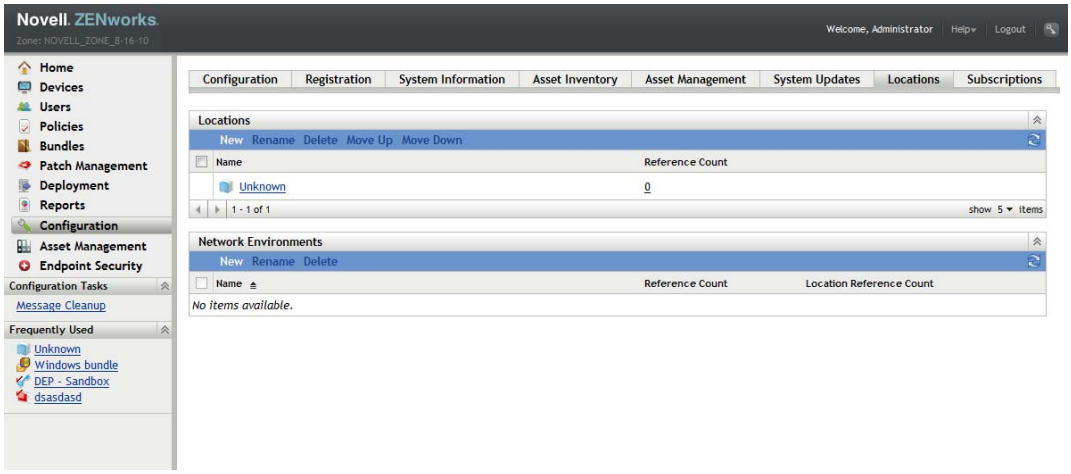
**Network Services:** The Network Services panel lets you define the network services that the Adaptive Agent evaluates to see if its current network environment matches this network environment. Select the tab for the network service you want to define, click *Add*, then fill in the required information

5 Click *Next* to display the Summary page, then click *Finish* to add the network environment definition to the list.

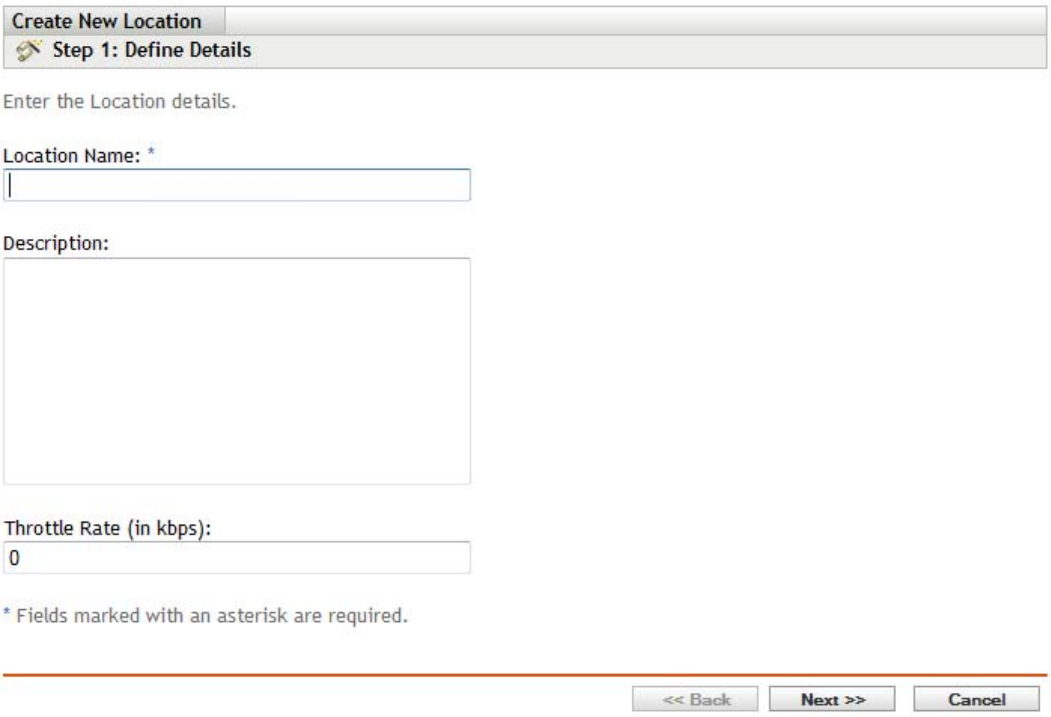
## 6.7.2 Creating Locations

When you create a location, you provide a location name and then associate the desired 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*.

As you complete the wizard, if you need more information about any fields or options, click the *Help* button located in the upper-right corner of ZENworks Control Center.

4 On the Assign Network Environments page:

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

   4b Click *Add*, select the network environments 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.

If you have multiple locations and network environments defined in ZENworks Control Center, you can use the *Move Up* and *Move Down* options to reorder the list.

### 6.7.3 Location and Network Environment Selection on a Managed Device

If you have multiple locations and network environments defined in ZENworks Control Center, the Adaptive Agent on the managed device scans all the defined network environments to identify matched environments. From the identified environments, the Adaptive Agent selects the network environments that have the highest number of matched network services (such as Client IP Address and DNS Servers). The Adaptive 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 Adaptive 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 Adaptive 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.

---

# ZENworks Adaptive Agent Deployment

The Discovery process is used to find devices in the network through querying a set of provided IP addresses and to collect inventory information by using technologies like SNMP, WMI, and SSH. Discovery process can also find devices from Novell eDirectory or Active Directory, and migrate your traditional ZENworks devices from Novell eDirectory.

The Deployment process is used to distribute and install ZENworks Adaptive Agent to a collection of devices that are identified by the discovery process or by providing a list of devices explicitly. These devices then become managed devices. The ZENworks Adaptive Agent must be installed to the devices you want to manage.

The following sections provide instructions to help you understand the process of deploying the agent:


- Section 7.1, "Configuring Adaptive Agent Features," on page 61
- Section 7.2, "Installing the ZENworks Adaptive Agent," on page 64
- Section 7.3, "Using the ZENworks Adaptive Agent," on page 67


**NOTE:** If a device does not meet the requirements for installing the ZENworks Adaptive Agent (see "Managed Device Requirements" in the *ZENworks 11 SP1 Installation Guide*), you might be able to install the Inventory Only Module on it to support inventorying of the device. For more information, see the *ZENworks 11 SP1 Discovery, Deployment, and Retirement Reference*.

## 7.1 Configuring Adaptive Agent Features

The ZENworks Adaptive Agent utilizes various modules to perform functions on a device. These modules are referred to as the Adaptive Agent features. Each ZENworks 11 SP1 product has specific features associated with it, as shown in the following table. The ZENworks 11 SP1 products are listed in the left column; the other columns represent the Adaptive Agent features.

| | Asset Management | Bundle Management | Endpoint Security | Image Management | Patch Management | Policy Management | Remote Management | User Management |
|---|---|---|---|---|---|---|---|---|
| ZENworks Asset Management | ✓ | | | | | | | ✓ |
| ZENworks Configuration Management | | ✓ | | ✓ | | ✓ | ✓ | ✓ |
| ZENworks Endpoint Security Management | | | ✓ | | | ✓ | | ✓ |
| ZENworks Patch Management | | | | | ✓ | | | |

By default, when you activate a ZENworks product, all of its Adaptive 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 you don't 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 you 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.

If you want to customize the Adaptive Agent features, either before you deploy the agent or after it is already deployed, the following sections provide instructions:


- Section 7.1.1, "Coexisting with the ZENworks Desktop Management Agent," on page 62
- Section 7.1.2, "Customizing the Adaptive Agent Features," on page 62


### 7.1.1 Coexisting with the ZENworks Desktop Management Agent

You can deploy the ZENworks Adaptive Agent to devices that have the traditional ZENworks Desktop Agent installed. The traditional ZENworks Desktop Agent is included with ZENworks 7 Desktop Management.

The ZENworks Adaptive Agent and the traditional ZENworks Desktop Agent can coexist on the same device, but only to support the use of ZENworks 11 SP1 Asset Management with traditional ZENworks Desktop Management. In this case, when you deploy the Adaptive Agent to a device that has the traditional ZENworks Desktop Agent installed, you should only use the Adaptive 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 traditional ZENworks Desktop Agent is uninstalled before the Adaptive Agent is installed.

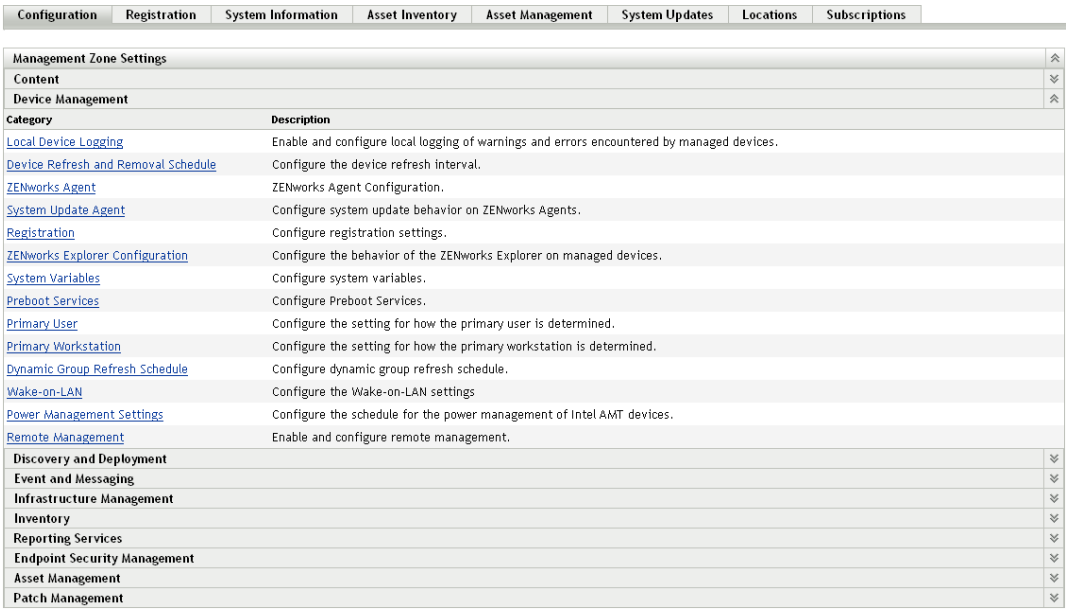
For more information on the coexistence of the ZENworks Adaptive Agent and traditional ZENworks Desktop Agent, see "ZENworks Adaptive Agent Deployment" in the *ZENworks 11 SP1 Discovery, Deployment, and Retirement Reference*.

### 7.1.2 Customizing the Adaptive Agent Features

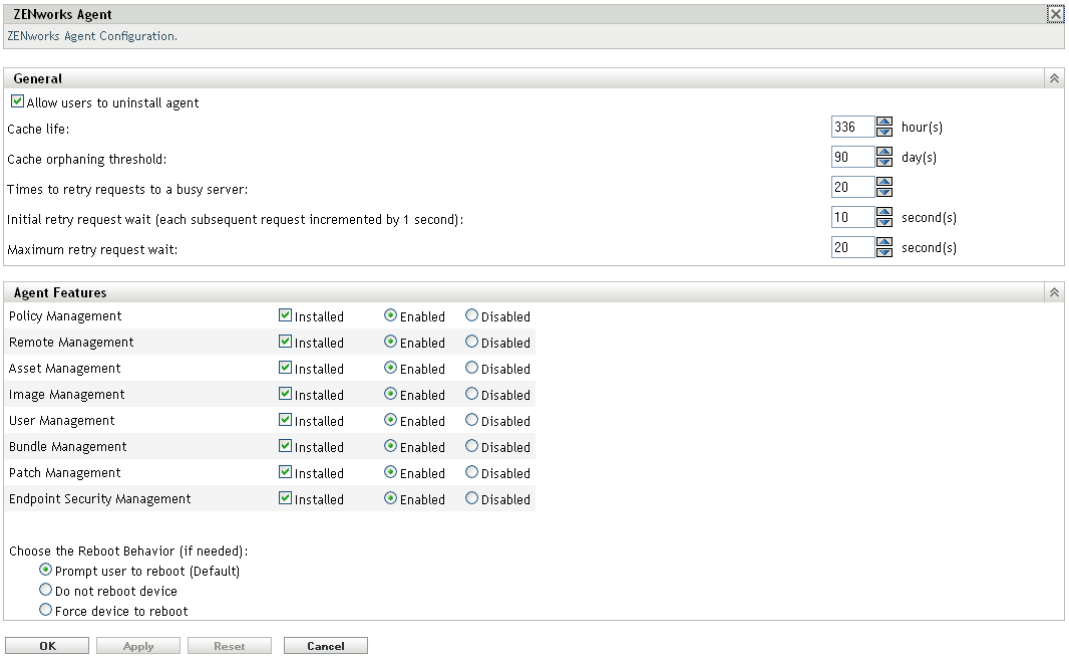
During initial deployment, the ZENworks Adaptive Agent installs and enables the features selected at the Management Zone level. After the agent registers, it then uses the settings defined at the device folder or device level (if they are different than the zone settings).

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 11 SP1 Discovery, Deployment, and Retirement Reference*.

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 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 your device. The installation of Image Management feature requires a reboot only on Windows 2008 and Windows Vista. You are prompted to reboot your device based on the selected reboot option.

4 To save the changes, click *OK*.

# 7.2 Installing the ZENworks Adaptive Agent

The following sections provide instructions for using the manual Web installation or a ZENworks Control Center deployment task to install the ZENworks Adaptive Agent on a device.


- Section 7.2.1, “Manual Installation on Windows,” on page 64
- Section 7.2.2, “Manual Installation on Linux,” on page 65
- Section 7.2.3, “ZENworks Control Center Deployment Task,” on page 66

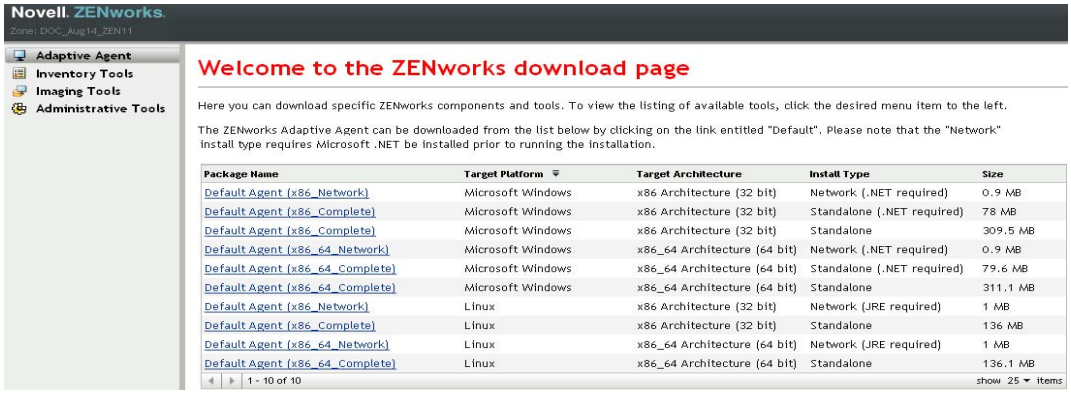

## 7.2.1 Manual Installation on Windows

1 Make sure the device meets the necessary requirements (see “Managed Device Requirements” in the *ZENworks 11 SP1 Installation Guide*).

2 On the target device, open a Web browser 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 Adaptive Agent. For each architecture (32-bit and 64-bit), there are three 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 Adaptive Agent from the ZENworks Server. The network (.NET required) package requires that Microsoft .NET 3.5.5 SP1 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 3.5.5 SP1 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 Adaptive Agent installation except the Microsoft .NET installer.

**Standalone:** The standalone package installs the pre-agent and extracts all executable files required for Adaptive Agent installation, including Microsoft .NET installer on the target device. The pre-agent then installs the Adaptive Agent from the local device. The standalone package is useful when you need to install the ZENworks Adaptive 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 Adaptive 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 you want to use; 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 you can use with the package when launching it from a command line, see "Package Options for Windows and Linux" in *ZENworks 11 SP1 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 Upon completion of the installation, the device reboots automatically if you have already reboot 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.

6 Skip to Section 7.3, "Using the ZENworks Adaptive Agent," on page 67 for information about logging in and using the Adaptive Agent on a device.

### 7.2.2 Manual Installation on Linux

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

1 Make sure the device meets the necessary requirements (see "Managed Device Requirements" in the *ZENworks 11 SP1 Installation Guide*).

2 On the target device, open a Web browser 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), there are two types of packages:

**Network (JRE required):** The network (JRE required) package installs only the pre-agent on the target device; the pre-agent then downloads and installs the ZENworks Adaptive Agent from the ZENworks Server. The network (JRE required) package requires that JRE 1.0.6 or later is installed on the device prior to the deployment of the agent to the device.

**Standalone:** The standalone package installs the pre-agent and extracts all executable files required for Adaptive Agent installation, including the JRE installer on the target device. The pre-agent then installs the Adaptive Agent from the local device. The standalone package is useful when you need to install the ZENworks Adaptive Agent on 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 Adaptive 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 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 you can use with the package when launching it from a command line, see "Package Options for Windows and Linux" in *ZENworks 11 SP1 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 command `./filename`, where *filename* is the name of the package you downloaded in Step 3.

6 (Conditional) If you want to view the ZENworks notify icon in the notification area after agent installation for the Linux device, log out of and log in to the device.

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

## 7.2.3 ZENworks Control Center Deployment Task

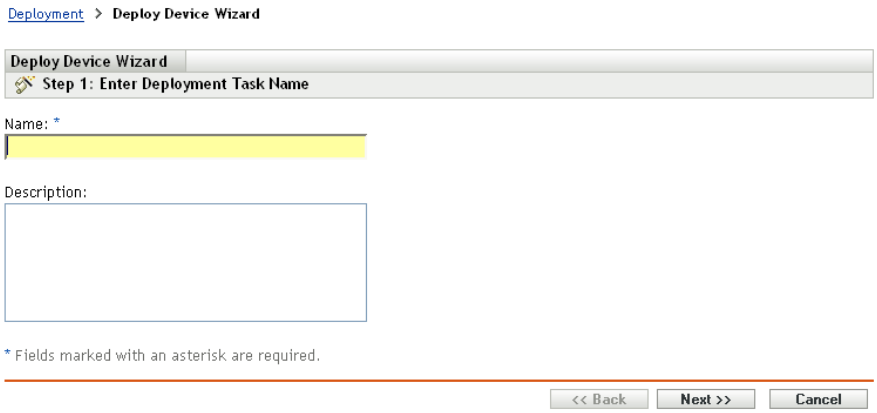
To install the Adaptive Agent by using a deployment task, the target device must be displayed in ZENworks Control Center.

To create a deployment task:

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

The Deployable Device panel lists all the devices (imported or discovered) to which you can deploy the Adaptive Agent.

**2** In the Deployment Tasks panel, click *New* to launch the Deploy Device Wizard.




**3** Follow the prompts to install the ZENworks Adaptive Agent.

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

When you complete the wizard, in ZENworks Control Center, the device appears in the `\Servers` folder or `\Workstation` folder on the Devices page.

**4** Continue with the next section, Using the ZENworks Adaptive Agent, for information about logging in and using the Adaptive Agent.

You can also use the `deployment-task-create` command in the zman utility to create a deployment task. For more information, see "Deployment Commands" in the *ZENworks 11 SP1 Command Line Utilities Reference*.

# 7.3 Using the ZENworks Adaptive Agent

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


- Section 7.3.1, "Logging In to the Management Zone," on page 67
- Section 7.3.2, "Navigating the Adaptive Agent Views," on page 68
- Section 7.3.3, "Promoting a Managed Device to be a Satellite," on page 71


## 7.3.1 Logging In to the Management Zone

When a Windows managed device boots its operating system, the Adaptive 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 Adaptive Agent integrates with the Windows Login or Novell Login client to provide a single login experience for users. When users enter their eDirectory or Active Directory credentials in the Windows or Novell client, they are logged in to the Management Zone if the credentials match the ones in a ZENworks user source. Otherwise, a separate Adaptive 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, he or she is automatically logged in to the Management Zone. However, if the user logs in to Tree2, the Adaptive Agent login screen appears and prompts the user for the Tree1 credentials.

## 7.3.2 Navigating the Adaptive Agent Views

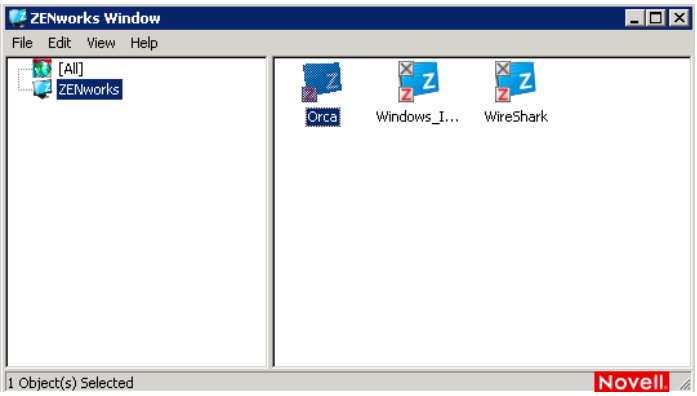
The Adaptive Agent provides the following three views:


- "ZENworks Window" on page 68
- "ZENworks Explorer" on page 69
- "ZENworks Icon" on page 70


### ZENworks Window

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

***Figure 7-1*** *ZENworks Window*




The ZENworks Window 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, your administrator can create additional folders in which to organize bundles, and can even rename the ZENworks folder.

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

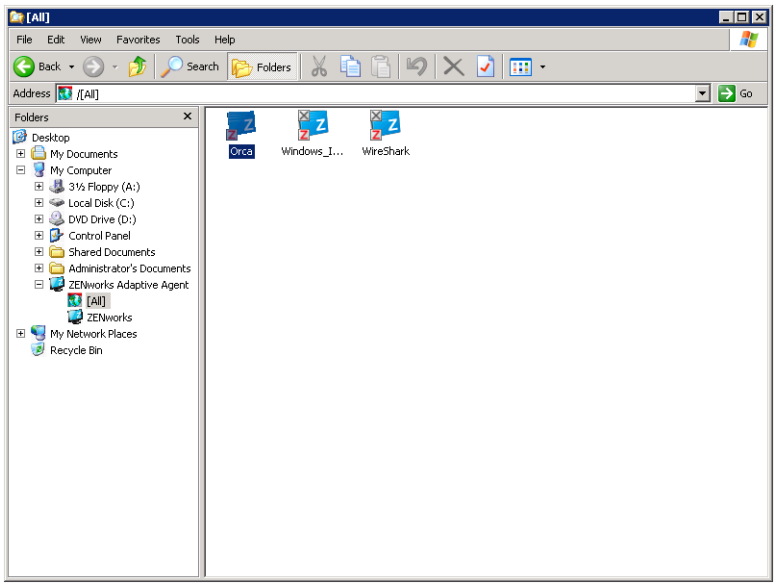
- Install a bundle or launch an application that is already installed.

- View the properties of a bundle. The properties include a description of the bundle, information about people to contact for help with the bundle, the times 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

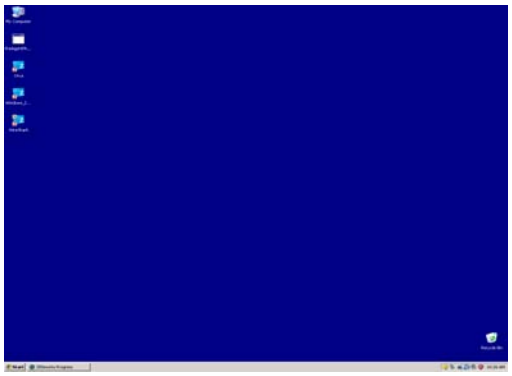
ZENworks Explorer is an extension to Windows Explorer that enables bundles to be displayed in Windows Explorer, on the desktop, on the Start menu, on the Quick Launch toolbar, and in the notification area (system tray). The following graphic shows bundles displayed in Windows Explorer.

***Figure 7-2*** *ZENworks Explorer - Windows Explorer view*




The following graphic shows bundles displayed on the desktop.

***Figure 7-3*** *ZENworks Explorer - Windows desktop view*

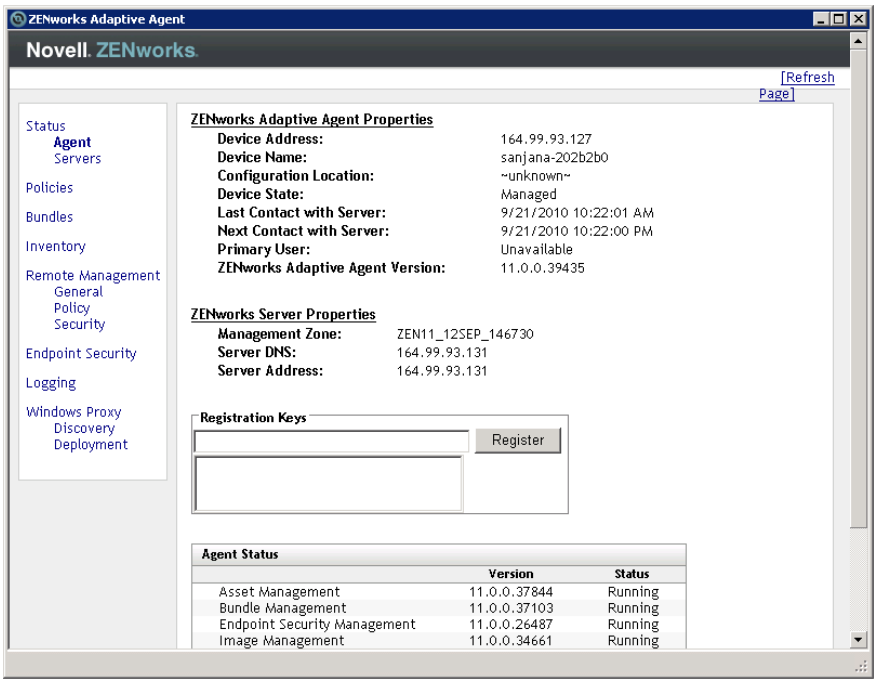


You can perform the same tasks on the bundles in the ZENworks Explorer as you can in the ZENworks Window.

## ZENworks Icon

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

***Figure 7-4*** *ZENworks Adaptive Agent Properties*




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

- **Status:** Displays information such as the last time the agent contacted a ZENworks Server and whether or not the Agent features are running.
- **Policies:** Displays the policies assigned to the device and the logged-in user. Also displays whether the policy is effective. 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. 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). 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. 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. 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. Also lets you initiate a management session and control security settings for the session. Included only if ZENworks Configuration Management is enabled.
- **Satellite:** Displays the satellite role information of a device that is used as a satellite. The satellite roles include Collection, Content, and Imaging.

  This feature is displayed only if your ZENworks administrator has used your device as a satellite.
- **Logging:** Displays information about the Adaptive 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. Also lets you determine the severity level for logged messages.
- **Windows Proxy** Displays the results of the discovery and deployment activities performed on your device when it acts as a Windows Proxy for the ZENworks Primary Server.

### 7.3.3 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 (server or workstation) or any Linux 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 11 SP1 framework.

For detailed information about Satellites and how to promote managed device to be a Satellite, see "Satellites" in the *ZENworks 11 SP1 System Administration Reference*.

# System Messages and Reports

Novell ZENworks 11 SP1 lets you monitor the activity within your Management Zone through system messages and reports.


- Section 8.1, “Viewing System Messages,” on page 73
- Section 8.2, “Creating a Watch List,” on page 76
- Section 8.3, “Generating Reports,” on page 76


## 8.1 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.

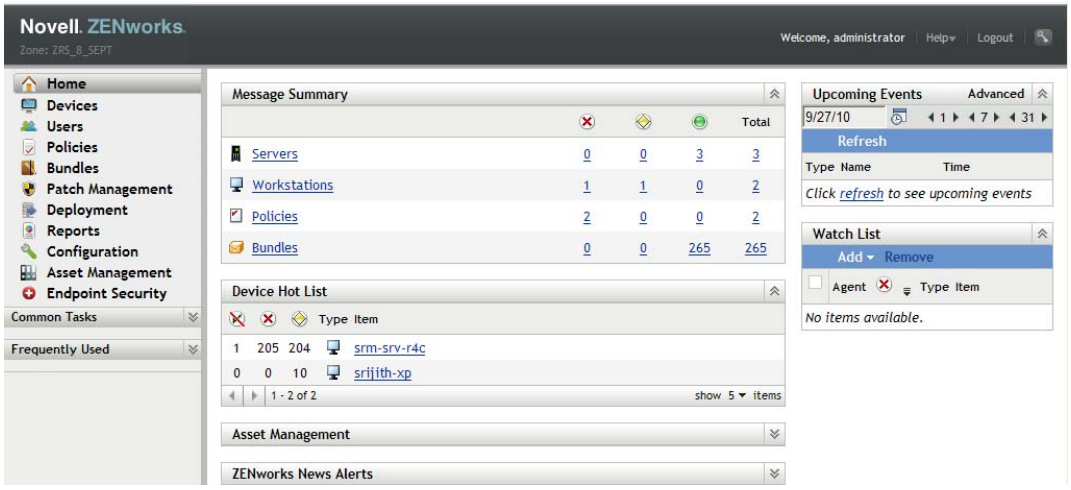
Each ZENworks Server and ZENworks Adaptive Agent creates a log of the activities associated with it. These messages are displayed in ZENworks Control Center in a variety of areas:

- **System Message Log:** The system message log, located on the System Information page (*Configuration* tab), displays messages from all ZENworks Servers and Adaptive 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 Adaptive Agent. For example, the message log for Workstation1 includes all messages generated by the Adaptive 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 Adaptive 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 Adaptive Agents.

### 8.1.1 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 your zone.

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



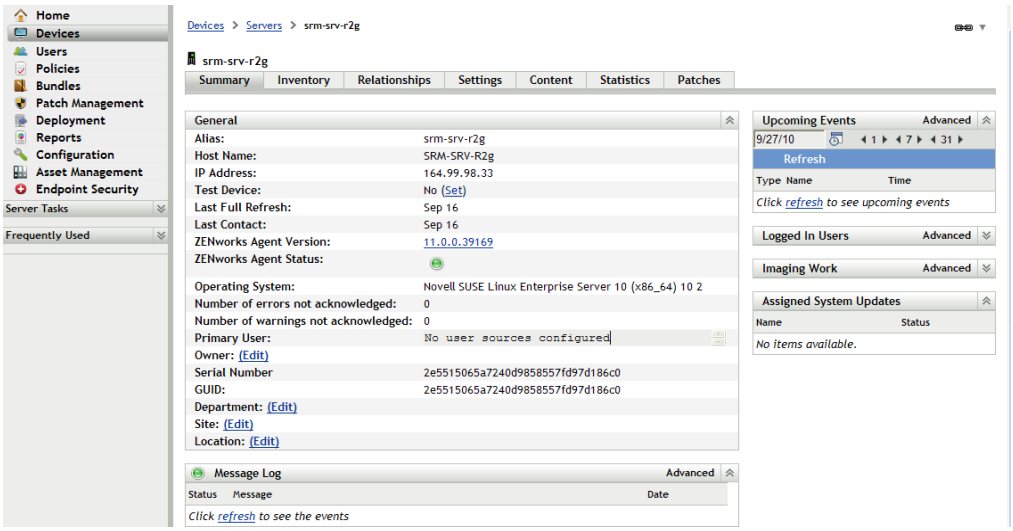

The Message Summary panel displays the status of all servers, workstations, policies, and bundles in your Management Zone. For example, if two servers have unacknowledged critical messages (messages that you or another administrator have not yet acknowledged as having seen), the column displays the number 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 of 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.

## 8.1.2 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 | 1. Click the message to display the Message Detail Information dialog box.<br>2. Click *Acknowledge*. | If you decide that you don't want to acknowledge the message, click *Finished* to dismiss the dialog box. This causes the message to remain in the *Message Log* list. |
| Acknowledge all messages | 1. In the *Tasks* list located in the left navigation pane, click *Acknowledge All Messages*. | |
| View all acknowledged or unacknowledged messages | 1. Click the *Advanced* button to display the Edit Message Log page. | 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.<br><br>Click the *Help* button on the Edit Message Log page for specific information about performing tasks on that page. |
| Delete a message | 1. Click the message to display the Message Detail Log dialog box.<br>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 11 SP1 Command Line Utilities Reference*.

### 8.1.3 Where to Find More Information

For more information about system messages, see "Message Logging" in the *ZENworks 11 SP1 System Administration Reference*.

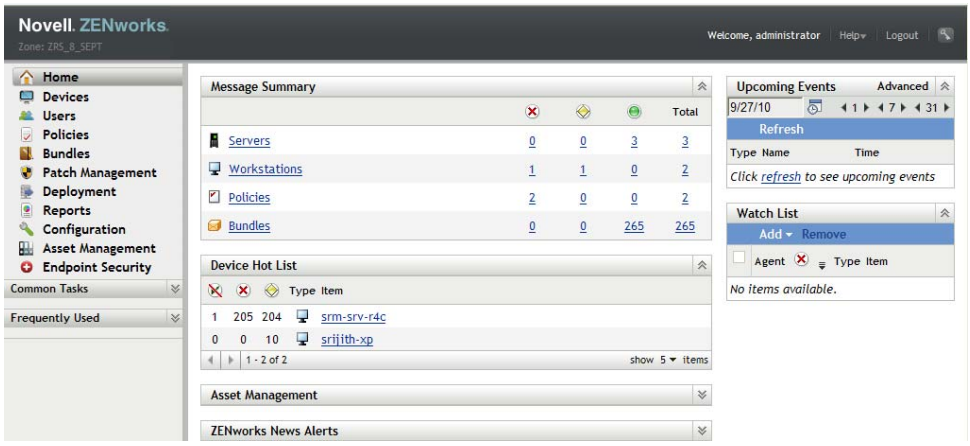
## 8.2 Creating a Watch List

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 Adaptive Agent is currently connected ( ) or disconnected ( ).
- : Displays whether or not 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) 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 for and select a server.

Objects remain in the Watch List until you remove them.

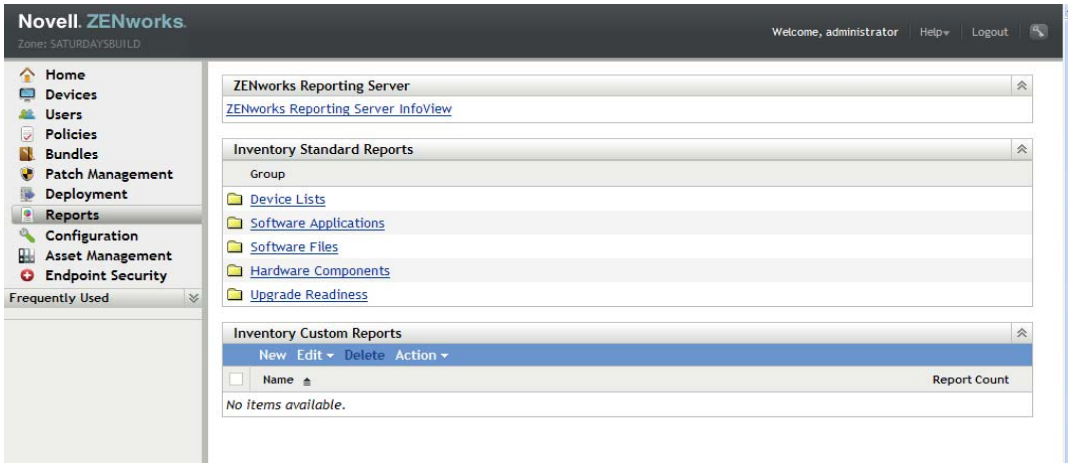
## 8.3 Generating Reports

ZENworks provides advanced reporting capabilities with ZENworks Reporting Server. ZENworks Reporting Server uses an embedded BusinessObjects Enterprise XI R3.1 SP3 engine to create customized reports. You can use the predefined reports in ZENworks Reporting Server to report on

Asset Management, Patch Management, Discovery and Deployment, Bundles and Policies, ZENworks Systems, and Endpoint Security Management. You can also create custom reports, edit reports, assign rights on reports, and schedule reports to a set of users.

To access the reports:

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




2 In the ZENworks Reporting Server panel, click *ZENworks Reporting Server InfoView* to launch the ZENworks Reporting Server InfoView. The ZENworks Reporting Server InfoView page is displayed with initial view as *Document List*.

The following table explains the various tasks you can perform in the ZENworks Reporting Server InfoView.

| Task | Steps |
|---|---|
| Generate a predefined report | 1. Navigate the `Predefined Reports` folder until you locate the report definition on which you want to generate a report.<br>2. Click *Actions* > *Schedule*, or right-click the report, then select *Schedule*. |
| Generate a custom report | 1. In the InfoView toolbar, click *New* > *Web Intelligence Document*. The *Universe* pane is displayed.<br>2. Click *ZENworks* to view the ZENworks Universe.<br>3. In the *Data* tab, navigate to the universe object for which you want to create a report, and drag the object to the right pane.<br>4. Click *Run Query*.<br>5. Save the report in the `Custom Reports` folder. |
| View the earlier instances of a report | 1. Navigate the `Predefined Reports` or the `Custom Reports` folder until you locate the report whose earlier instances you want to view.<br>2. Click *Actions* > *History,* or right-click the report, and select *History*. |

| Task | Steps |
|---|---|
| View the latest instance of a report | 1. Navigate the `Predefined Reports` or the `Custom Reports` folder until you locate the report whose latest instances you want to view.<br>2. Click *Actions* > *View Latest Instance*, or right-click the report, and select *View Latest Instance*. |
| View the properties of a report | 1. Navigate the `Predefined Reports` or the `Custom Reports` folder until you locate the report whose properties you want to view.<br>2. Click *Actions* > *Properties*, or right-click the report and select *Properties*. |

You can also use the `report-generate-now` command, as well as other report commands, in the zman utility to manage reports. For more information, see "Report Commands" in the *ZENworks 11 SP1 Command Line Utilities Reference*.

For more information about reporting, see the *ZENworks 11 SP1 System Reporting Reference*.

# Product Administration

III

The following sections provide information to help you use ZENworks 11 SP1 products. Before attempting any of the sections, you should have already completed the configuration tasks in Part II, “System Configuration,” on page 23.


- Chapter 9, “Quick List,” on page 81
- Chapter 10, “Asset Management,” on page 87
- Chapter 11, “Configuration Management,” on page 103
- Chapter 12, “Endpoint Security Management,” on page 131
- Chapter 13, “Patch Management,” on page 139

# Quick List

# 9

After you've configured your Management Zone (see Part II, "System Configuration," on page 23), you should review the concepts and tasks in the following sections for any ZENworks products that you have licensed or are evaluating:


- Section 9.1, "Asset Management," on page 81
- Section 9.2, "Configuration Management," on page 82
- Section 9.3, "Endpoint Security Management," on page 83
- Section 9.4, "Patch Management," on page 84


## 9.1 Asset Management

ZENworks 11 SP1 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 | 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.<br><br>For instructions, see Section 10.1, "Activating Asset Management," on page 87. |
| Enable the ZENworks Adaptive Agent to perform Asset Management operations | The agent's Asset Management feature is enabled by default when ZENworks Asset Management is activated (full license or evaluation).<br><br>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 Section 10.2, "Enabling Asset Management in the ZENworks Adaptive Agent," on page 87. |
| Scan devices to collect software and hardware inventory | 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.<br><br>This task must be done before you can do any of the remaining tasks.<br><br>For instructions, see Section 10.3, "Collecting Software and Hardware Inventory," on page 88. |
| Monitor software usage | Generate reports to analyze how much and how often software products are being used.<br><br>For instructions, see Section 10.4, "Monitoring Software Usage," on page 91. |

| Task | Details |
|---|---|
| Monitor software license compliance | See whether your installed software products are properly licensed, under licensed, or over licensed.<br><br>For instructions, see Section 10.5, “Monitoring License Compliance,” on page 92. |
| 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).<br><br>For instructions, see Section 10.6, “Allocating Licenses,” on page 99. |

## 9.2 Configuration Management

ZENworks 11 SP1 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.<br><br>For instructions, see Section 11.1, “Activating Configuration Management,” on page 103. |
| Enable the ZENworks Adaptive Agent to perform Configuration Management operations | For the ZENworks Adaptive 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).<br><br>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 Section 11.2, “Enabling Configuration Management in the ZENworks Adaptive Agent,” on page 103. |
| Distribute software | Distribute software through the use of 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, and thin-client applications.<br><br>For instructions, see Section 11.3, “Distributing Software,” on page 104. |

| Task | Details |
|---|---|
| Apply policies | 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.<br><br>For instructions, see Section 11.4, “Applying Policies,” on page 105. |
| Take images of and apply images to devices | 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.<br><br>For instructions, see Section 11.5, “Imaging Devices,” on page 108. |
| Remotely manage devices | Remotely access devices to provide user assistance or perform operations. You can control or view a device. You can also execute and transfer files, as well as perform diagnostics to troubleshoot problems with the device.<br><br>For instructions, see Section 11.6, “Remotely Managing Devices,” on page 114. |
| Scan devices to collect software and hardware inventory | 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.<br><br>For instructions, see Section 11.7, “Collecting Software and Hardware Inventory,” on page 127. |
| Automate the process of migrating a set of customized system and application settings | |

# 9.3 Endpoint Security Management

ZENworks 11 SP1 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 | 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.<br><br>For instructions, see Section 12.1, “Activating Endpoint Security Management,” on page 131. |

| Task | Details |
|---|---|
| Enable the Endpoint Security Agent | 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.<br><br>For instructions, see Section 12.2, “Enabling the Endpoint Security Agent,” on page 131. |
| Create locations | 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.<br><br>If you want to use location-based policies, you must create locations. For instructions, see Section 12.3, “Creating Locations,” on page 132. |
| Create security policies | A devices security settings are configured through security policies. There are 11 types of security policies you can create.<br><br>For instructions, see Section 12.4, “Creating a Security Policy,” on page 132. |
| Assign policies to users and devices | Security policies can be assigned to users or to devices.<br><br>For instructions, see Section 12.5, “Assigning a Policy to Users and Devices,” on page 136. |
| Assign policies to zones | 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.<br><br>For instructions, see Section 12.6, “Assigning a Policy to the Zone,” on page 137. |

## 9.4 Patch Management

ZENworks 11 SP1 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 | 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.<br><br>For instructions, see Section 13.1, “Activating Patch Management,” on page 139. |

| Task | Details |
|---|---|
| Enable the ZENworks Adaptive Agent to perform Patch Management operations | For the ZENworks Adaptive 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).<br><br>You should verify that the agent's Patch Management feature is enabled. For instructions, see Section 13.2, "Enabling Patch Management in the ZENworks Adaptive Agent," on page 140. |
| Start the subscription service | 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).<br><br>For instructions, see Section 13.3, "Starting the Subscription Service," on page 140. |
| Deploy patches | After the subscription service has download patches, apply the desired patches.<br><br>For instructions, see Section 13.4, "Deploying a Patch," on page 141. |

# Asset Management

The following sections provide explanations and instructions for using ZENworks 11 SP1 Asset Management to collect software and hardware inventory from devices, monitor software usage on devices, and monitor software license compliance.


- Section 10.1, “Activating Asset Management,” on page 87
- Section 10.2, “Enabling Asset Management in the ZENworks Adaptive Agent,” on page 87
- Section 10.3, “Collecting Software and Hardware Inventory,” on page 88
- Section 10.4, “Monitoring Software Usage,” on page 91
- Section 10.5, “Monitoring License Compliance,” on page 92
- Section 10.6, “Allocating Licenses,” on page 99


## 10.1 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 11 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 Novell ZENworks Asset Management product site (http://www.novell.com/products/zenworks/assetmanagement).
4. Click *OK*.

## 10.2 Enabling Asset Management in the ZENworks Adaptive Agent

For the ZENworks Adaptive 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 Section 7.1, “Configuring Adaptive Agent Features,” on page 61.

# 10.3 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 reports 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 reports 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.

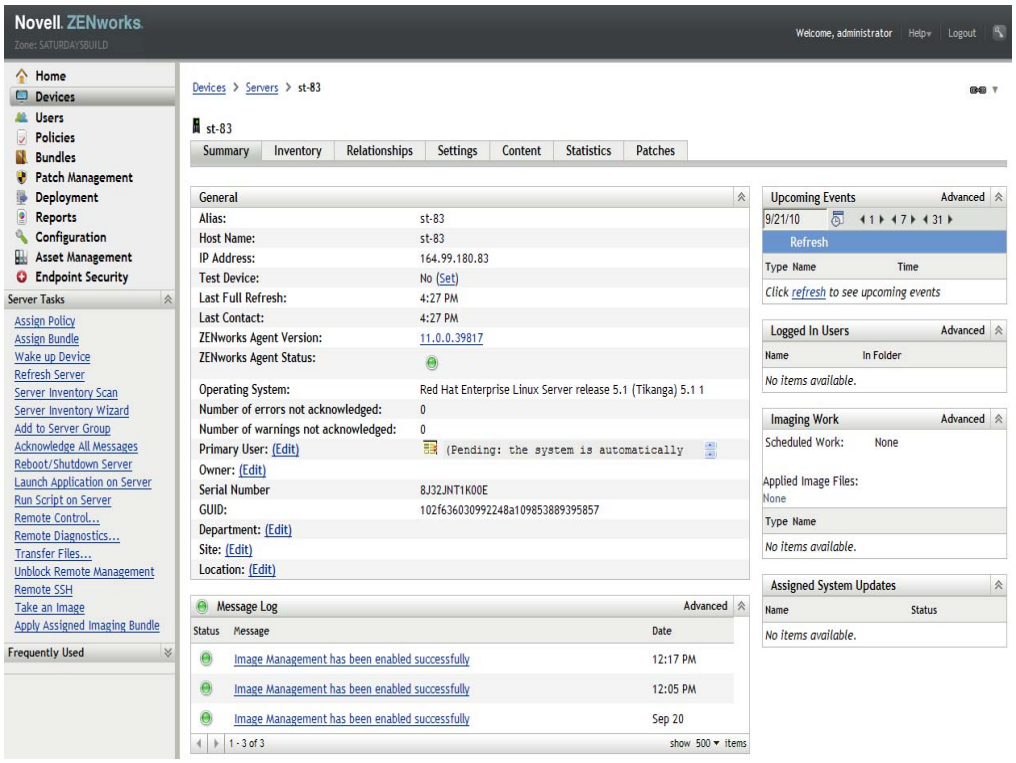
The following sections provide instructions for initiating a device scan and using the collected inventory:


- Section 10.3.1, "Initiating a Device Scan," on page 88
- Section 10.3.2, "Viewing a Device Inventory," on page 89
- Section 10.3.3, "Generating an Inventory Report," on page 90
- Section 10.3.4, "Where to Find More Information," on page 90


## 10.3.1 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 11 SP1 Command Line Utilities Reference*.

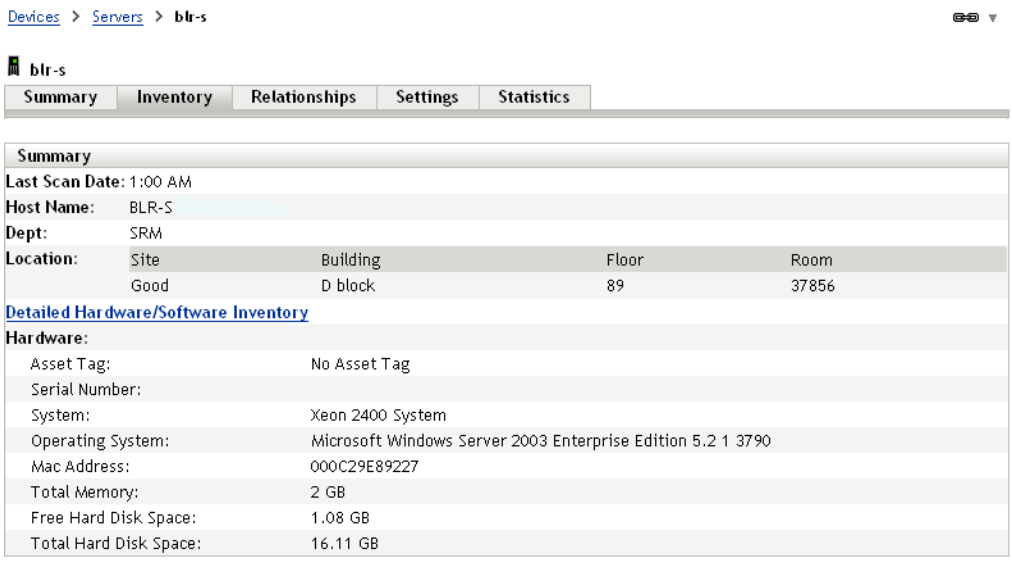
## 10.3.2 Viewing a Device Inventory

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.

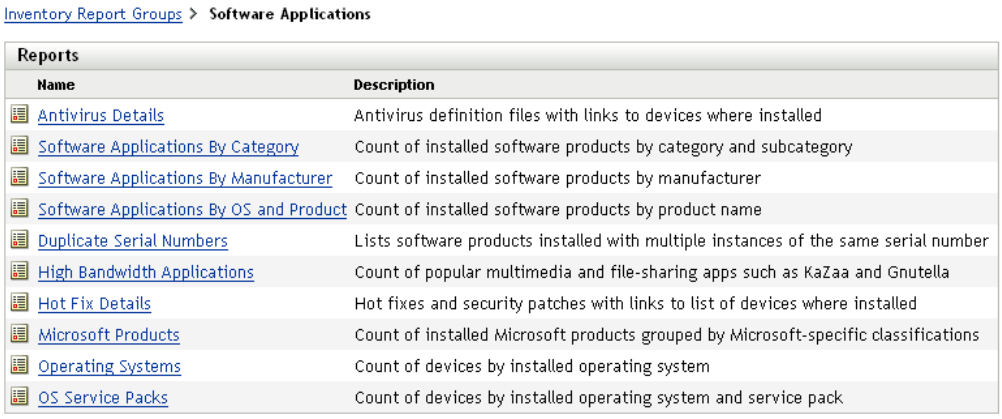



The Inventory page provides a summary of the hardware inventory. To see detailed inventory information, click *Detailed Hardware/Software Inventory*.

## 10.3.3 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.

## 10.3.4 Where to Find More Information

For more information about inventory, see the *ZENworks 11 SP1 Asset Inventory Reference*.

# 10.4 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 Reports panel, click *Application Usage* to display the list of application usage reports.

Software Usage Reports > **Application Usage**

**Reports**

| Name | Description |
|---|---|
| Total Application Usage by Product | Sum of local and served application usage organized by product |
| Total Application Usage by User | Sum of local and served application usage organized by user |
| Total Application Usage by Device | Sum of local and served application usage organized by device |
| Local Application Usage by Product | Local application usage organized by product |
| Local Application Usage by User | Local application usage organized by user |
| Local Application Usage by Device | Local application usage organized by device |
| Served Application Usage by Product | Served application usage organized by product |
| Served Application Usage by Server | Served application usage organized by server |
| Served Application Usage by User | Served application usage organized by user |
| Served Application Usage by Device | Served application usage organized by device |
| Usage Collection history | History of usage data collection |

**Grouping Criteria**

- (•) Zone
- ( ) Folder
- ( ) Group
- ( ) Demographic

3. In the Reports panel, click *Local Application Usage by Product*.

**Local Application Usage by Product** Run Date: 3/16/09

Products from 10 Software Manufacturer(s) Installed on 2 Device(s)

| Manufacturer | Installations |
|---|---|
| Cinematronics | 1 |
| Macromedia | 1 |
| Microsoft | 45 |
| Novell | 13 |
| Sun | 6 |
| Sun Microsystems | 32 |
| Sybase | 1 |
| Symantec | 1 |
| VMware | 2 |
| Yahoo! | 1 |

Excel CSV PDF Graph

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 reports that you can use. For additional information about application usage reports, see "Reports" in the *ZENworks 11 SP1 Asset Management Reference*.

# 10.5 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.

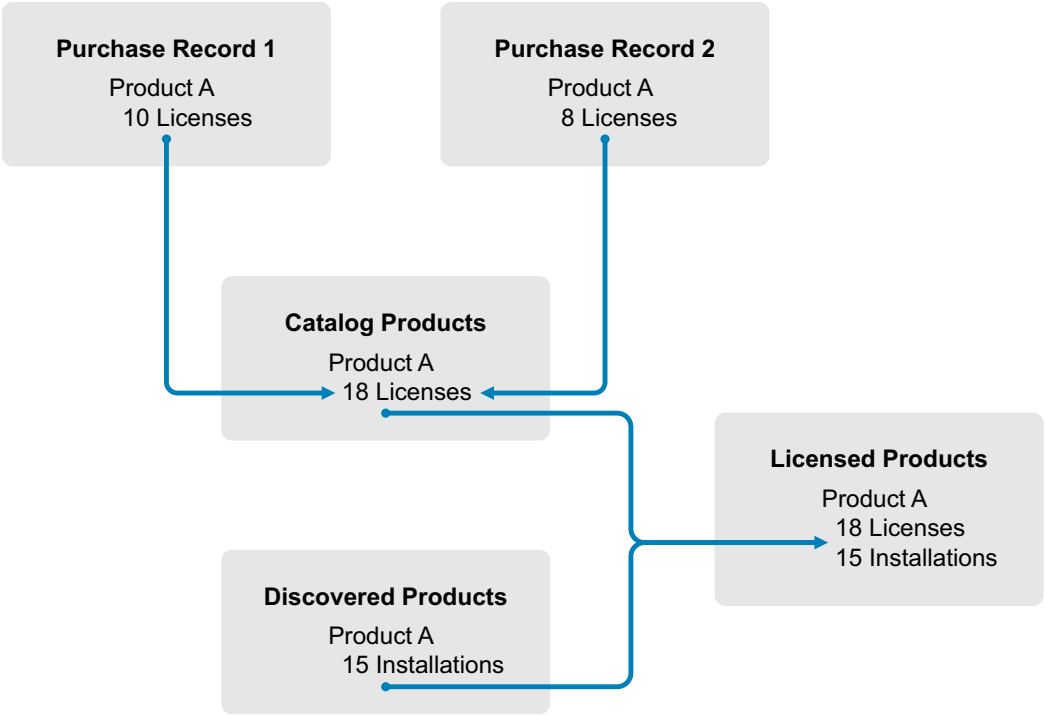
Asset Management license compliance is a powerful and flexible tool. As a result, there are multiple approaches and methods you can use when setting up license compliance. The following sections provide basic instructions with minimal explanation in order to help you quickly set up a single product for license compliance monitoring. After you finish this basic scenario, see "License Compliance" in the *ZENworks 11 SP1 Asset Management Reference* for more detailed information and instructions.


- Section 10.5.1, "License Compliance Components," on page 92
- Section 10.5.2, "Discovering Installed Products," on page 93
- Section 10.5.3, "Creating a Catalog Product and Purchase Record," on page 94
- Section 10.5.4, "Creating a Licensed Product," on page 96
- Section 10.5.5, "Viewing Compliance Data," on page 98
- Section 10.5.6, "Where to Find More Information," on page 99


## 10.5.1 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 10-1* *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.

## 10.5.2 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 Section 10.3, "Collecting Software and Hardware Inventory," on page 88.

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 94.

## 10.5.3 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 Section 10.5.2, "Discovering Installed Products," on page 93.

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*.

Catalog Products

New Move... Delete Action

| Name | Licenses Per Pkg | Mfr. Part # | Reseller SKU | Excluded | Purchase Quantity | Licensed Product |
|---|---|---|---|---|---|---|
| 4D TECHNOLOGIES INC CD DUPE MS OFFICE 2000 STANDARD 32 BIT WIN (CD)(NR) 2000 (FF_Media Duplication) (1) | 1 | C49567 | C49567 | | 1 | |
| ACME Jumble 2 (Full License) (1) | 1 | | | | 2 | Jumble |
| ACME Turbo (Version Upgrade) (1) | 1 | | | | | |
| ADOBE SYSTEMS INC ADOBE ACROBAT CAPTURE V3.0 PERSONAL ED WNT (CD) 3 (Shrinkwrap Product) (1) | 1 | 22101156 | A59587 | | 1 | |
| ADOBE SYSTEMS INC ADOBE ACROBAT V5.0 MP (CD) 5 (Shrinkwrap Product) (1) | 1 | 22001438 | A68210 | | 2 | |
| ADOBE SYSTEMS INC ADOBE ACROBAT V5.0 MP UPG (CD) 5 (Shrinkwrap Product) (1) | 1 | 22001440 | A68250 | | 3 | |
| ADOBE SYSTEMS INC ADOBE DESIGN COLLECTION V4.0 MP (CD) 4 (Shrinkwrap Product) (1) | 1 | 27590080 | A69412 | | 1 | |
| ADOBE SYSTEMS INC ADOBE GOLIVE V6.0 MP (CD) 6 (Shrinkwrap Product) (1) | 1 | 23200324 | A84261 | | 2 | |
| ADOBE SYSTEMS INC ADOBE PAGEMAKER V7.0 MP (CD)(EU) 7 (Shrinkwrap Product) (1) | 1 | 27530341 | A69856 | | 1 | |
| ADOBE SYSTEMS INC ADOBE PAGEMAKER V7.0.2 MP UPG (CD)(EU) 7 (Shrinkwrap Product) (1) | 1 | 27530402 | A104342 | | 1 | |

**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.

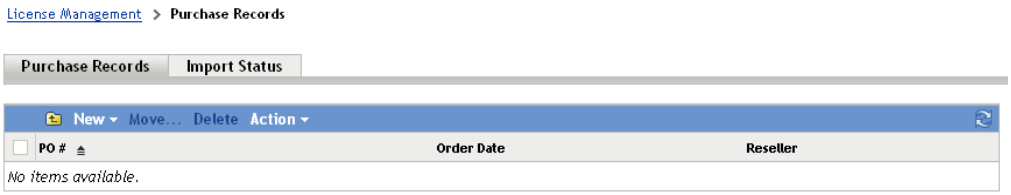
**Excluded:** Do not select this check box.

**2d** Click *Next* to display the Summary page, the 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*.



License Management > Purchase Records

Purchase Records | Import Status

New Move... Delete Action

| PO # | Order Date | Reseller |
|---|---|---|
| No items available. | | |

**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 11 SP1 Asset Management Reference*.

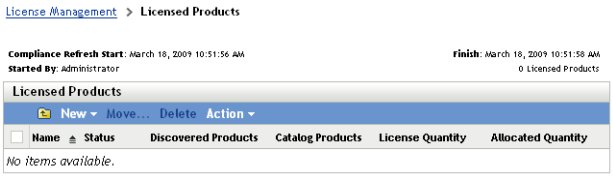
## 10.5.4 Creating a Licensed Product

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 | The Auto-Reconcile Wizard creates licensed products from existing discovered products.To find your discovered product:<br>1. Click the *Products Specified Below* option.<br>2. In the *Select* list, select the manufacturer of your discovered product.<br>3. In the *Product* field, enter the name of your discovered product. |
| Select Licensed Products to Create | 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.<br><br>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.<br><br>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. |
| Destination Folder | Select the folder where you want to place the new licensed product.<br><br>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. |
| License Entitlements | Every licensed product must have at least one entitlement and license model.<br><br>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.<br><br>The license model determines how the licenses are counted. Licenses can be counted per installation, user, or device.<br><br>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. |
| 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.

## 10.5.5 Viewing Compliance Data

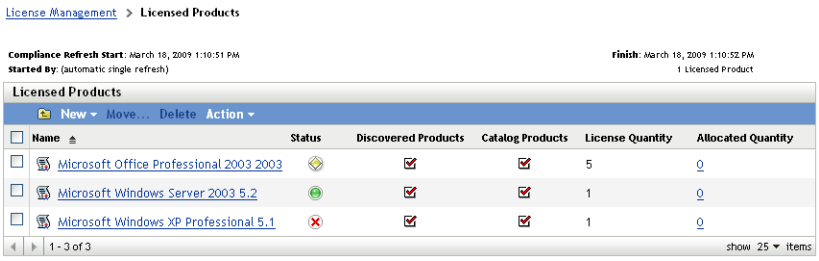
There are two views you can use to see the compliance status of your licensed products. You can view the Licensed Products page to get a compliance status summary for all products, or you can generate the Software Compliance report to see more detailed information.


- "Viewing the Compliance Status Summary" on page 98
- "Generating the Software Compliance Report" on page 99


### 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.



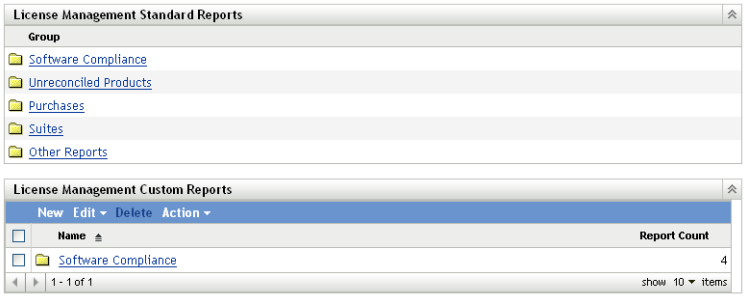

The Licensed Products list displays all licensed products and their current compliance status:

- 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

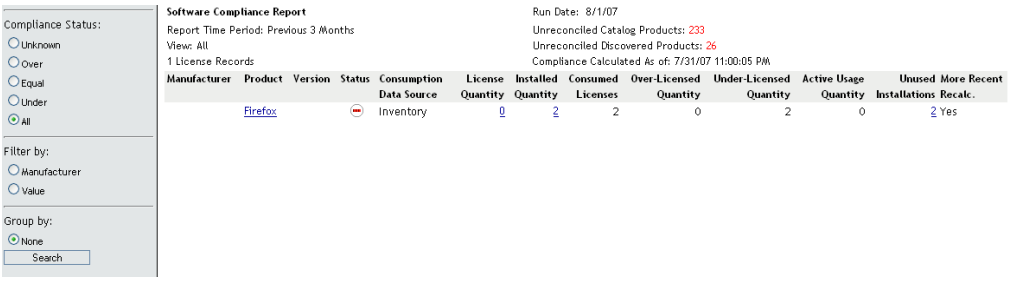
1 In ZENworks Control Center, click the *Asset Management* tab, then click the *License Management* tab.

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




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

4 In the Reports 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 reports, see the *ZENworks 11 SP1 Asset Management Reference*.

## 10.5.6 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 11 SP1 Asset Management Reference*.

# 10.6 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).

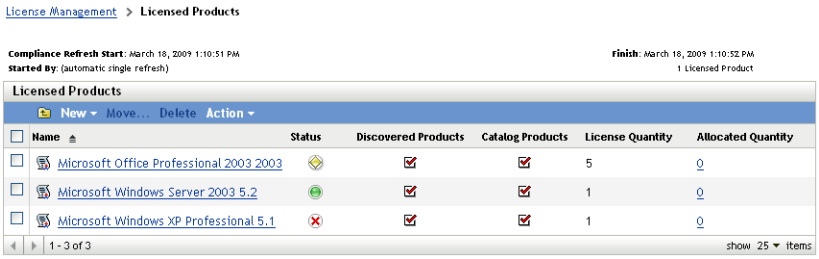
A *device allocation* is the assignment of a license to a specific device. The device can have the product installed or not installed. For example, you purchase 10 licenses of ProductA. You can allocate the licenses to the target devices before ProductA is even installed on the devices.

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 11 SP1 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.

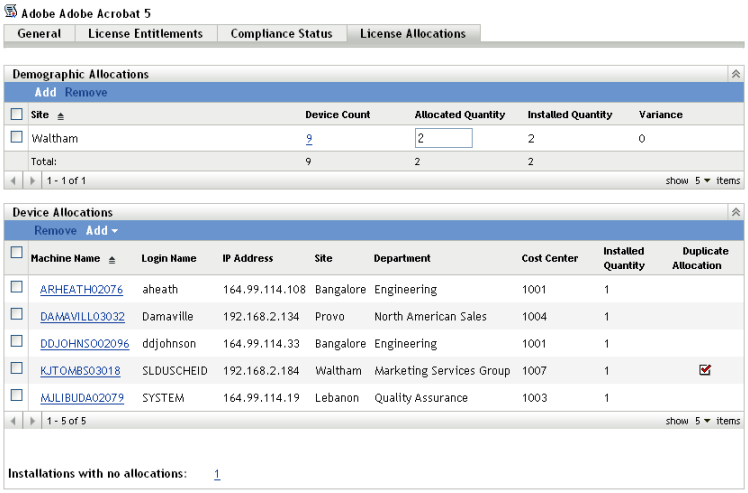
For example, assume that the product is using Department allocations. You import a purchase record that includes licenses assigned to DepartmentQ. The licenses are added as a DepartmentQ demographic allocation.

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.

# Configuration Management

The following sections provide explanations and instructions for the tasks you can perform with ZENworks 11 SP1 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.


- Section 11.1, “Activating Configuration Management,” on page 103
- Section 11.2, “Enabling Configuration Management in the ZENworks Adaptive Agent,” on page 103
- Section 11.3, “Distributing Software,” on page 104
- Section 11.4, “Applying Policies,” on page 105
- Section 11.5, “Imaging Devices,” on page 108
- Section 11.6, “Remotely Managing Devices,” on page 114
- Section 11.7, “Collecting Software and Hardware Inventory,” on page 127
- Section 11.8, “Personality Migration,” on page 129
- Section 11.9, “Linux Management,” on page 130


## 11.1 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 11 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).
4. Click *OK*.

## 11.2 Enabling Configuration Management in the ZENworks Adaptive Agent

For the ZENworks Adaptive 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 Section 7.1, “Configuring Adaptive Agent Features,” on page 61.

# 11.3 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 though 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:

- **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.
- **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 and ZENworks Adaptive Agent to distribute the software without requiring access to any other network locations.

## 11.3.1 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 11 SP1 Command Line Utilities Reference*.

## 11.3.2 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 11 SP1 Command Line Utilities Reference*.

### 11.3.3 Where to Find More Information

For more information about distributing software, see the *ZENworks 11 SP1 Software Distribution Reference*.

## 11.4 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.
- **Printer Policy:** Configures Local, SMB, HTTP, and iPrint printers for a 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.

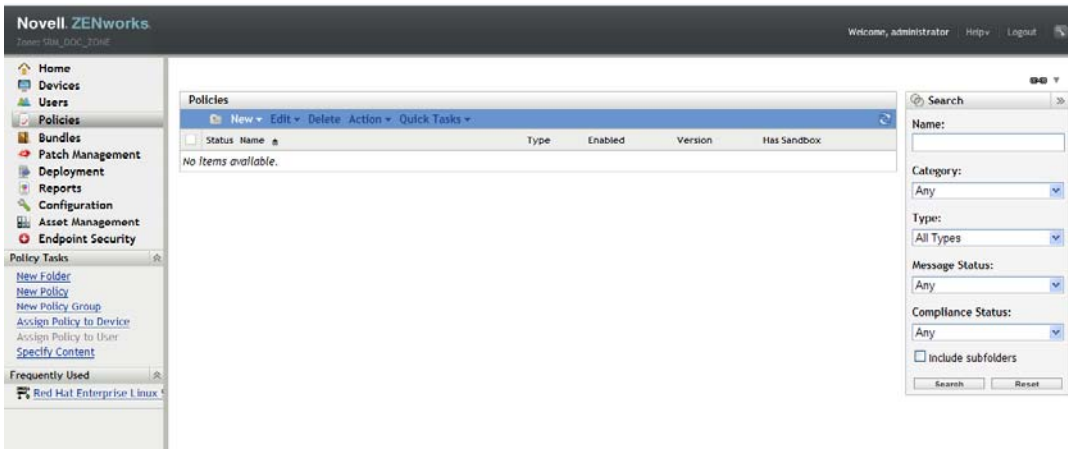
The following section contains the list of Linux Configuration policies that can be created and assigned to a user or a managed device.

- **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.

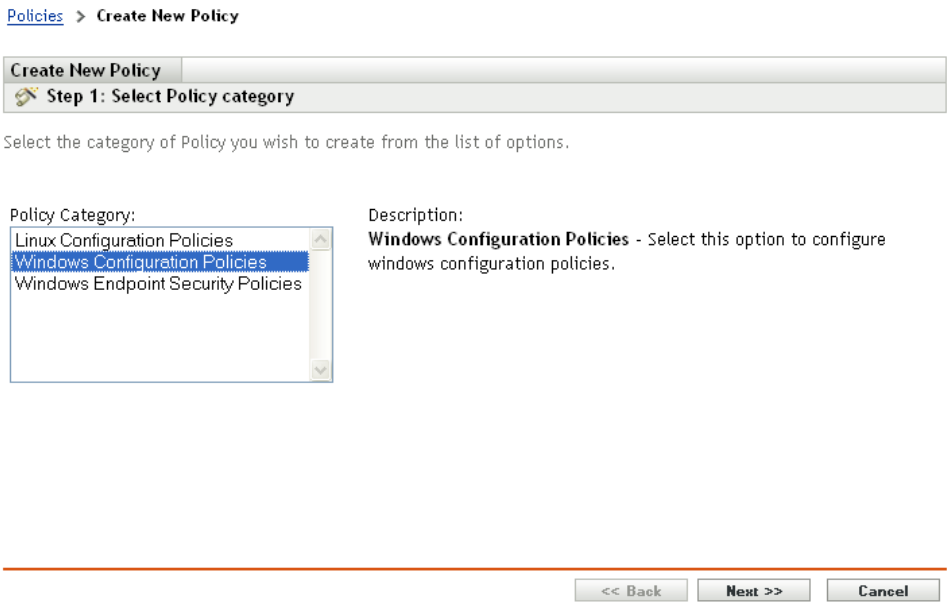
## 11.4.1 Creating a Policy

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.

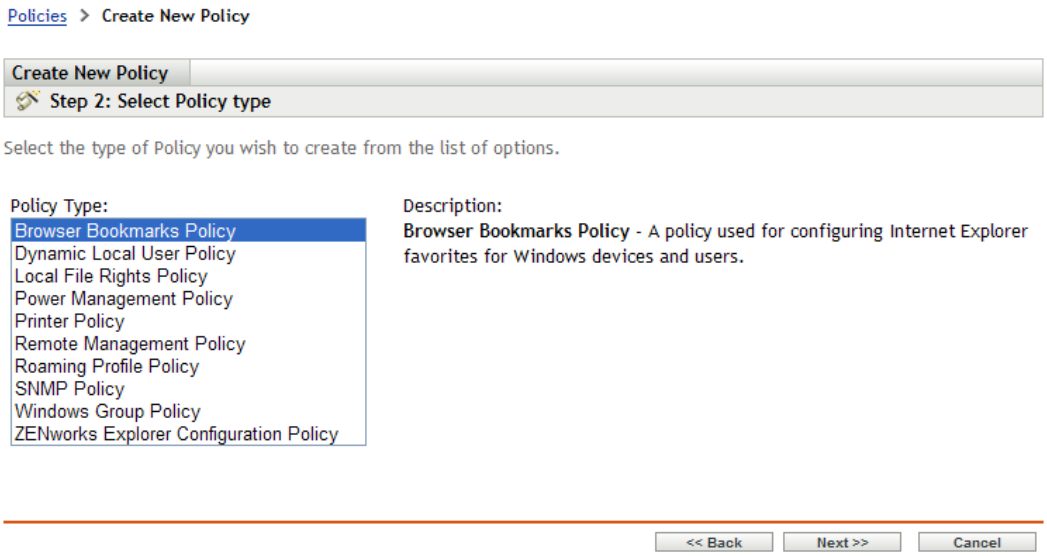



2. In the Policies panel, click *New* > *Policy* to launch the Create New Policy Wizard.




**3** Select *Windows Configuration Policies*, then click *Next*.

**NOTE:** To create a Linux configuration policy, select *Linux Configuration Policies* in the Create New Policy Wizard and continue with the on-screen prompts to create the policy.




**4** 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 11 SP1 Command Line Utilities Reference*.

### 11.4.2 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 11 SP1 Command Line Utilities Reference*.

### 11.4.3 Where to Find More Information

For more information about applying policies, see the *ZENworks 11 SP1 Configuration Policies Reference*.

## 11.5 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
- 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).


- Section 11.5.1, "Setting Up Preboot Services," on page 109
- Section 11.5.2, "Taking an Image," on page 110

- Section 11.5.3, “Applying an Image,” on page 112
- Section 11.5.4, “Where to Find More Information,” on page 114

## 11.5.1 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 109
- “Setting Up an Imaging Server” on page 109
- “Configuring the Third-Party Imaging Settings” on page 109

### 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 distro

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

To configure the Third-Party Imaging settings:

1. Ensure that Microsoft Windows Automated Installation Kit 1.0/1.1 (WAIK) is installed on the device running the ZENworks Control Center.

   You can freely downloaded WAIK from the Microsoft Download Center Web site (http://www.microsoft.com/downloads/details.aspx?FamilyID=c7d4bc6d-15f3-4284-9123-679830d629f2&displaylang=en).

2. (Conditional) If you want to run ZENworks Control Center on a 64-bit device, append the `WAIK_installation_path\Windows AIK\Tools\x86` to the `Path` Windows system environment variable.

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

3a In ZENworks Control Center, click *Configuration* tab.

3b In the *Management Zone Settings* panel, click *Device Management* > *Preboot Services* > the *Third-Party Imaging Settings* panel.

3c In the *Upload WinPE Base Distribution (Requires Windows Automation Installation Kit)* option, click to upload the WIM Imaging file. In the Upload WIM Imaging Files dialog box, do the following

3c1 Click *Browse* to browse for and select `winpe.wim`.

By default, `winpe.wim` is installed in `\waik\tools\petools\x86`.

---

**NOTE:** 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.

---

3c2 Click *OK*.

This downloads the Imaging files from server to the device running ZENworks Control Center and also uploads files from the device to the server. The progress of download and upload of files is displayed in the *Status* field.

3d In the *Upload ImageX Files to Support WIM Imaging (ImageX.EXE)* option, click to browse for and select the Microsoft Imaging engine (`imagex.exe`) installed on the device running ZENworks Control Center. By default, `imagex.exe` is installed in `\waik\tools\x86`.

3e In the *Upload Ghost 11.5 or higher files to support Ghost imaging(Ghost32.exe)* option, click to browse for and select the Symantec Ghost engine (`ghost32.exe`) installed along with the Ghost solution on any device in your network.

3f After configuring the third-party Imaging settings, click *Apply*.

3g Click *Status* to view the status of content replication across all Primary Servers in the Management Zone. You must start the Imaging operation only when the status is *Available*.

---

**IMPORTANT:** You must start the Imaging operation only when the status is *Available*.

---

4 Enable PXE on the device.

5 Ensure that you have a standard DHCP server, either on your Imaging Server or on another network server.

## 11.5.2 Taking an Image

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*.

**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.

---

**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.

## 11.5.3 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 112
- "Creating the Third-Party Image Bundle" on page 113
- "Initiating the Imaging Work" on page 113


### 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 *Imaging 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: / \ * ? : " ' < > \| ` % ~ |
| Select ZENworks Image File page | To select the image file:<br>1. Click to display the Server and Path Information dialog box.<br>2. Fill in the following fields:<br>**Device Object, IP, or DNS:** Select the ZENworks Server where you stored the image.<br>**File Path on Server:** Browse for and select the image file. The standard storage directory for image files is `\Novell\ZENworks\work\content-repo\images`.<br>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 *Imaging 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: / \ * ? : " ' < > \| ` % ~ |
| Select a Third-Party Image File page | To select a third-party image file:<br>1. Select the type of the image to be used in the bundle.<br>In ZENworks 11 SP1 Configuration Management, only the Windows Image Format (`.wim`) and GHOST Image Format (`.gho`) are available.<br>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.<br>3. Click to browse for and select the network credentials to be used for accessing the device having `.wim` or `.gho` files.<br>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:<br>**Image Number (WIM Only):** Select the index number of the image to be restored.<br>**Path to Restore the Add-on Image:** Specify the location on the device where you want to restore the Add-on image.<br>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.

### 11.5.4 Where to Find More Information

For more information about imaging and Preboot Services, see the *ZENworks 11 SP1 Preboot Services and Imaging Reference*.

## 11.6 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.<br><br>For more information on Remote Controlling a Windows device, see Section 11.6.3, "Performing Remote Control, Remote View, and Remote Execute Operations on a Windows Device," on page 119.<br><br>For more information on Remote Controlling a Linux device, see Section 11.6.6, "Performing Remote Control, Remote View, and Remote Login Operations on a Linux Device," on page 125. | |

| Remote Operation | Description | Additional Details |
|---|---|---|
| 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.<br><br>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<br><br>For more information on Remotely Viewing a Windows device, see Section 11.6.3, "Performing Remote Control, Remote View, and Remote Execute Operations on a Windows Device," on page 119.<br><br>For more information on Remotely Viewing a Linux device, see Section 11.6.6, "Performing Remote Control, Remote View, and Remote Login Operations on a Linux Device," on page 125. | |
| Remote Execute | 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.<br><br>For example, you can execute the `regedit` command to open the Registry Editor on the managed device. The Remote Execute dialog box displays the status of the command execution.<br><br>For more information on Remotely Executing a Windows device, see Section 11.6.3, "Performing Remote Control, Remote View, and Remote Execute Operations on a Windows Device," on page 119. | This operation is supported only on a Windows managed device. |
| Remote Diagnostics | 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.<br><br>For more information on Remote Diagnosis of a device, see Section 11.6.4, "Performing a Remote Diagnostic Operation," on page 122. | This operation is supported only on a Windows managed device. |
| File Transfer | Lets you to transfer files between the management console and a managed device.<br><br>For more information on File Transfer operation, see Section 11.6.5, "Performing a File Transfer Operation," on page 123. | This operation is supported only on a Windows managed device. |

| Remote Operation | Description | Additional Details |
|---|---|---|
| Remote Login | 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.<br><br>For more information on Remotely Logging a Linux device, see Section 11.6.6, "Performing Remote Control, Remote View, and Remote Login Operations on a Linux Device," on page 125. | This operation is supported only on a Linux managed device.<br><br>You must log into the device with a non-`root` user credentials. |
| Remote SSH | Lets you securely connect to a remote Linux device and safely execute commands on the device.<br><br>For more information on Remotely Logging a Linux device, see Section 11.6.7, "Performing Remote SSH Operation on a Linux Device," on page 126 | This operation is supported only on a Linux managed device.<br><br>To launch a Remote SSH session from a Management Console device, JRE version 1.5 or higher must be installed on the device |

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

- Section 11.6.1, "Creating a Remote Management Policy," on page 116
- Section 11.6.2, "Configuring Remote Management Settings," on page 118
- Section 11.6.3, "Performing Remote Control, Remote View, and Remote Execute Operations on a Windows Device," on page 119
- Section 11.6.4, "Performing a Remote Diagnostic Operation," on page 122
- Section 11.6.5, "Performing a File Transfer Operation," on page 123
- Section 11.6.6, "Performing Remote Control, Remote View, and Remote Login Operations on a Linux Device," on page 125
- Section 11.6.7, "Performing Remote SSH Operation on a Linux Device," on page 126
- Section 11.6.8, "Where to Find More Information," on page 127

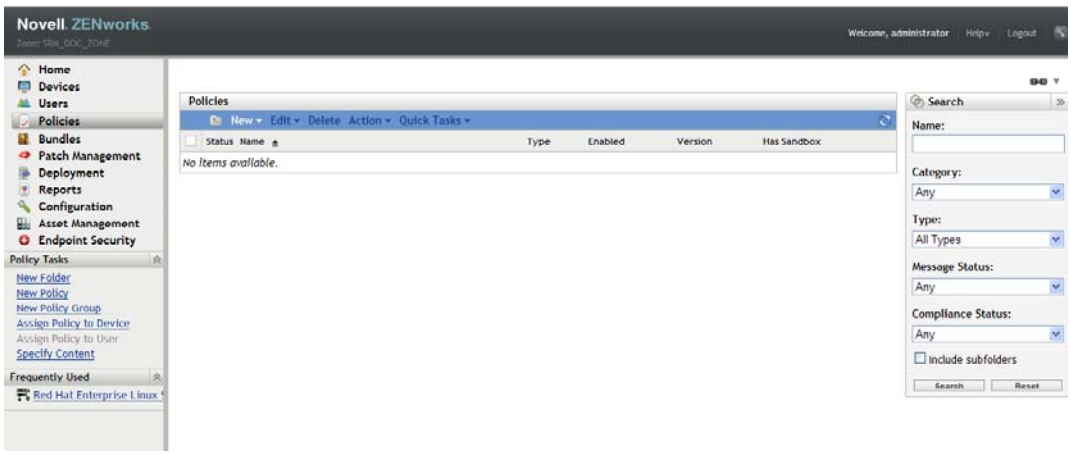
## 11.6.1 Creating a Remote Management Policy

By default, a secure Remote Management policy is created on the managed device when the ZENworks Adaptive 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.

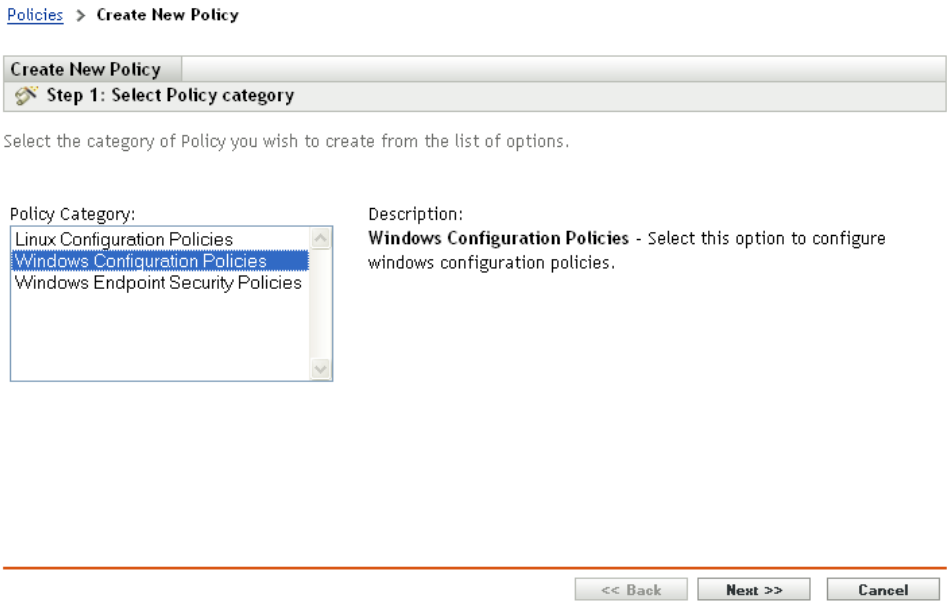
You can assign a Remote Management policy to devices or users.

To create a Remote Management policy:

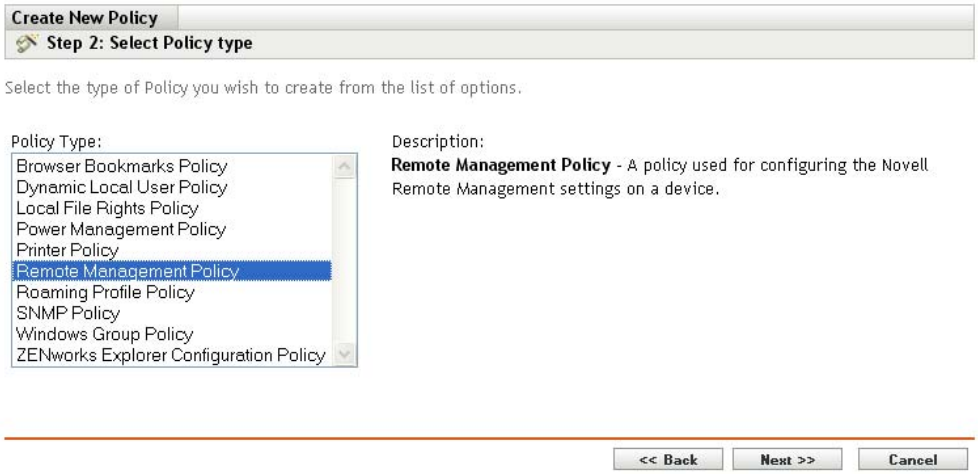
1. In ZENworks Control Center, click the *Policies* tab.




**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.

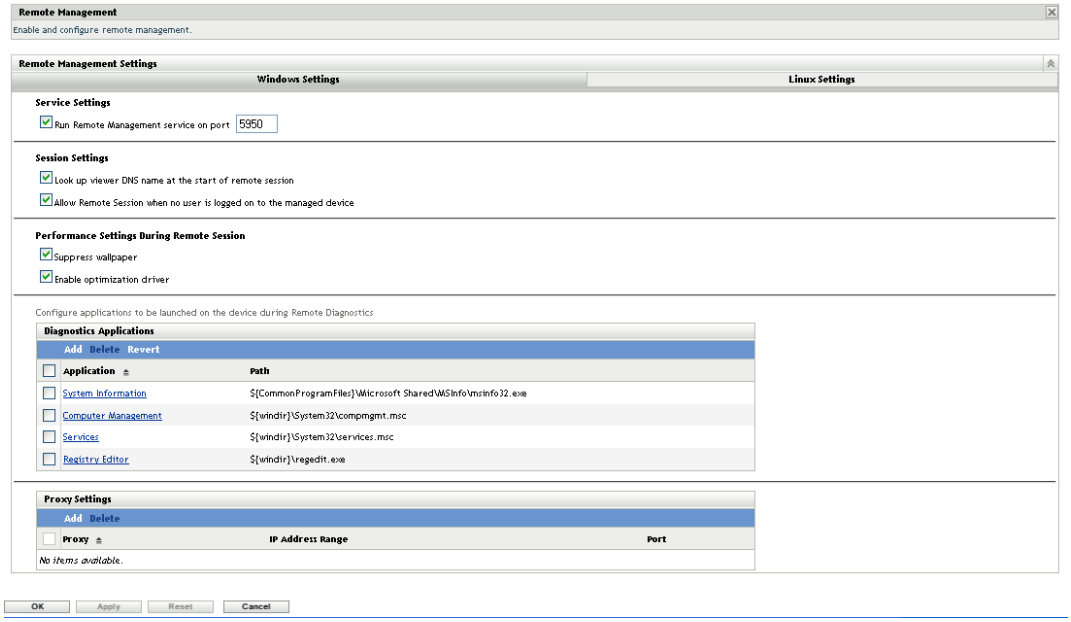
## 11.6.2 Configuring Remote Management Settings

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.

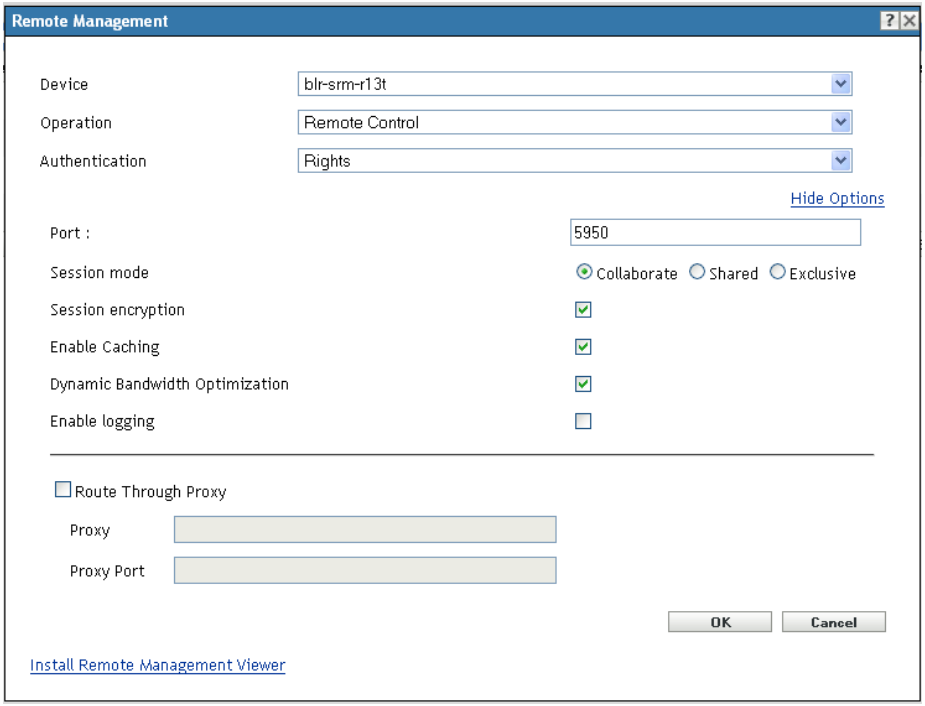
## 11.6.3 Performing Remote Control, Remote View, and Remote Execute Operations on a Windows Device

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.

**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.
- **Enable Cache Path:** Enables the primary key and the certificate paths to be cached on the management console.

**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.

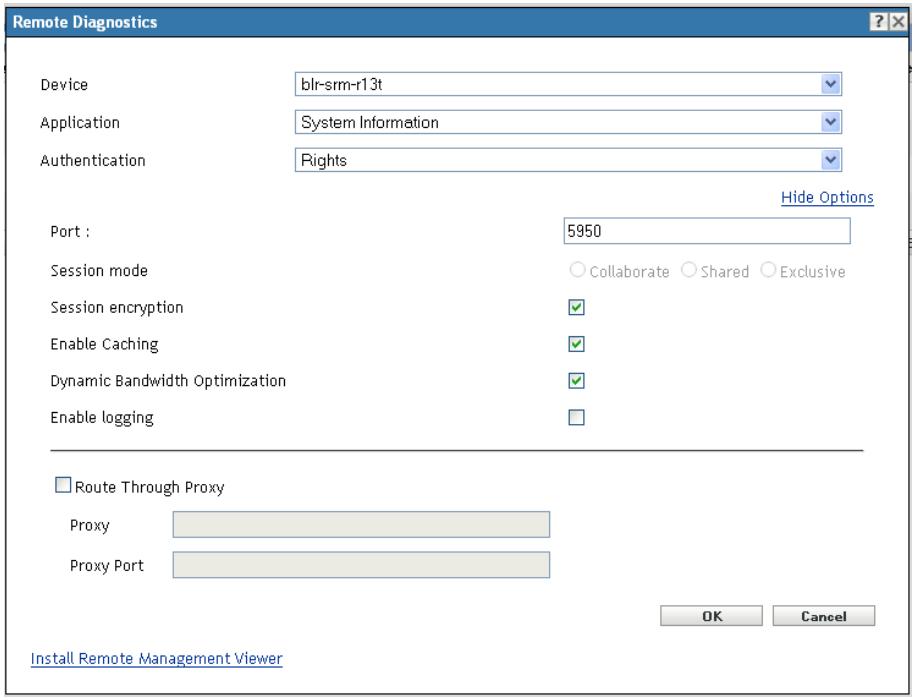
## 11.6.4 Performing a Remote Diagnostic Operation

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.

**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.

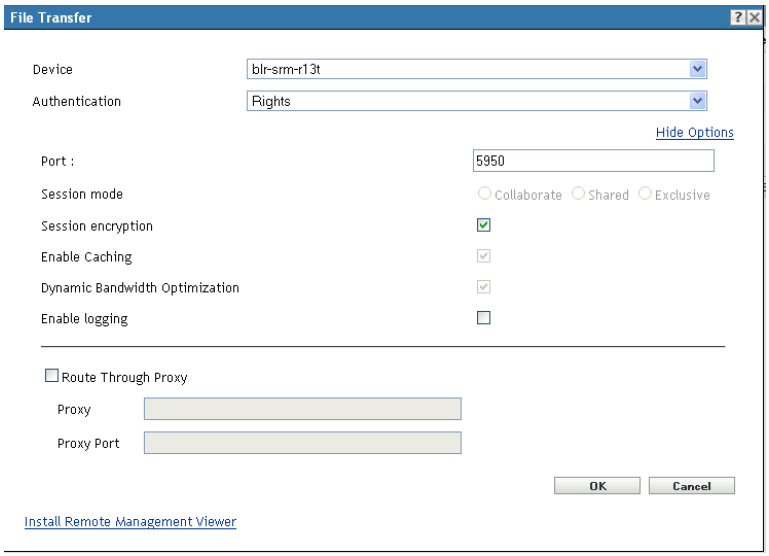
## 11.6.5 Performing a File Transfer Operation

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.

**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

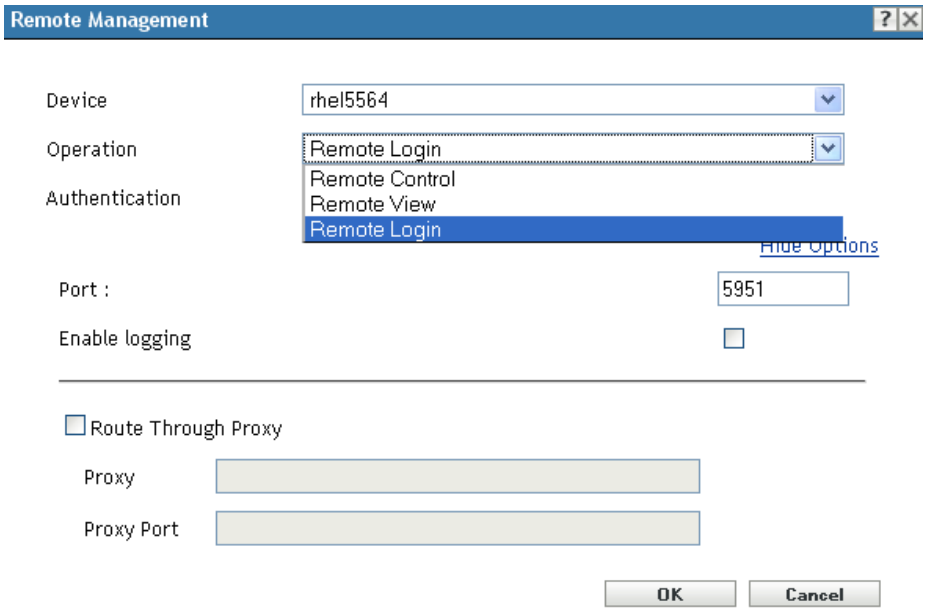
## 11.6.6 Performing Remote Control, Remote View, and Remote Login Operations on a Linux Device

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.

**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.

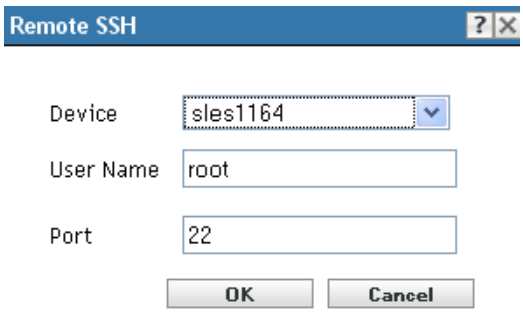
## 11.6.7 Performing Remote SSH Operation on a Linux Device

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.

### 11.6.8 Where to Find More Information

For more information about remotely managing devices, see the *ZENworks 11 SP1 Remote Management Reference*.

## 11.7 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 reports 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 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.

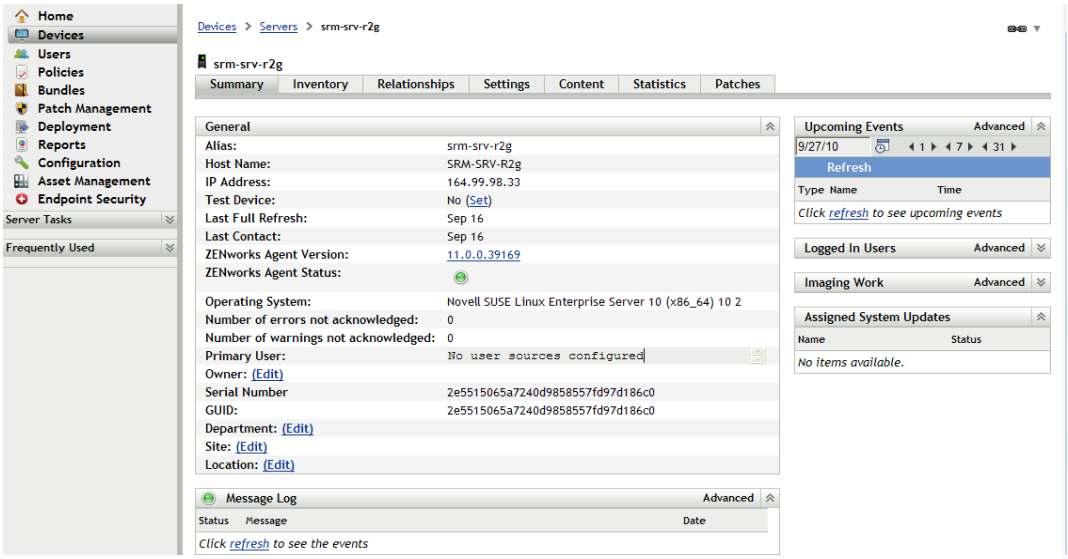
By default, devices are automatically scanned at 1:00 a.m. the first day of each month. You can modify the schedule, as well as many other *Inventory* configuration settings, on the *Configuration* tab in ZENworks Control Center.


- Section 11.7.1, "Initiating a Device Scan," on page 127
- Section 11.7.2, "Viewing a Device Inventory," on page 128
- Section 11.7.3, "Generating an Inventory Report," on page 128
- Section 11.7.4, "Where to Find More Information," on page 129


### 11.7.1 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 11 SP1 Command Line Utilities Reference*.

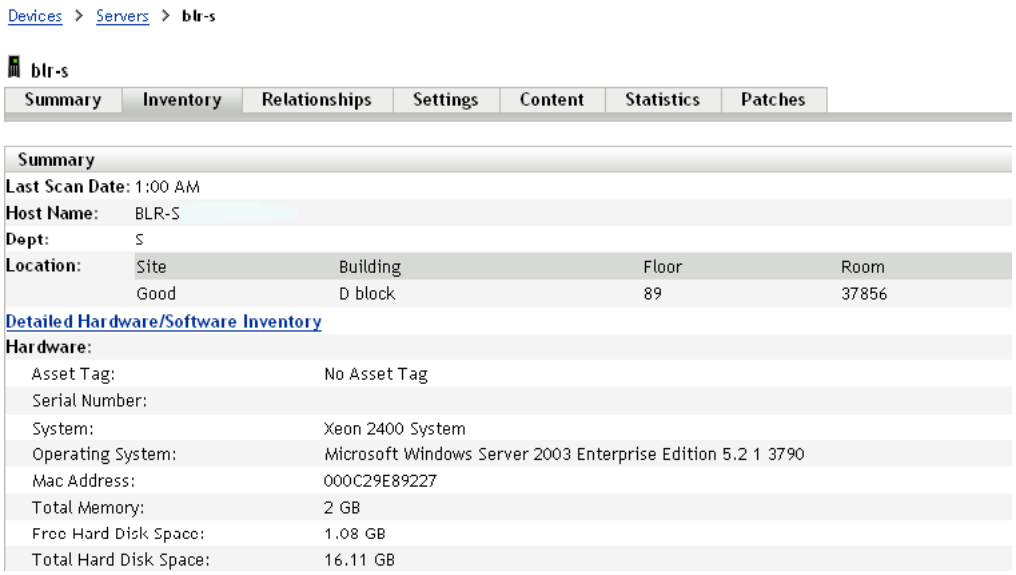
## 11.7.2 Viewing a Device Inventory

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.

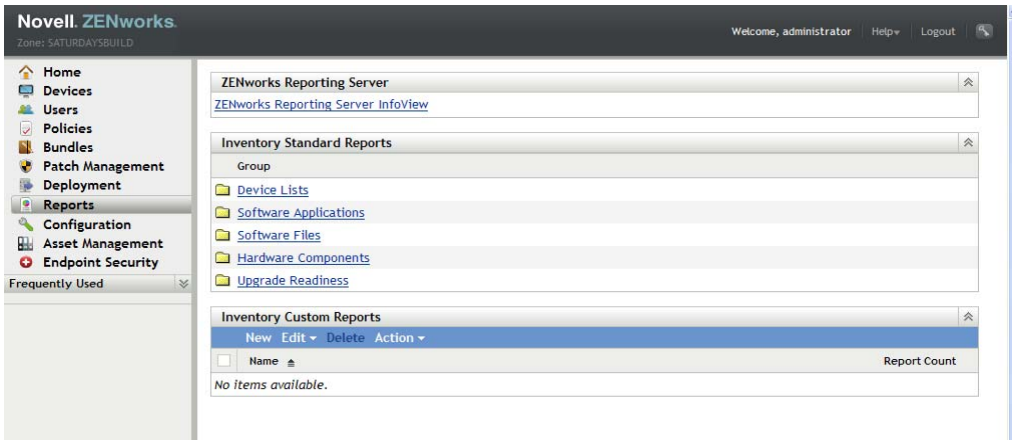
4 Click the *Inventory* tab.



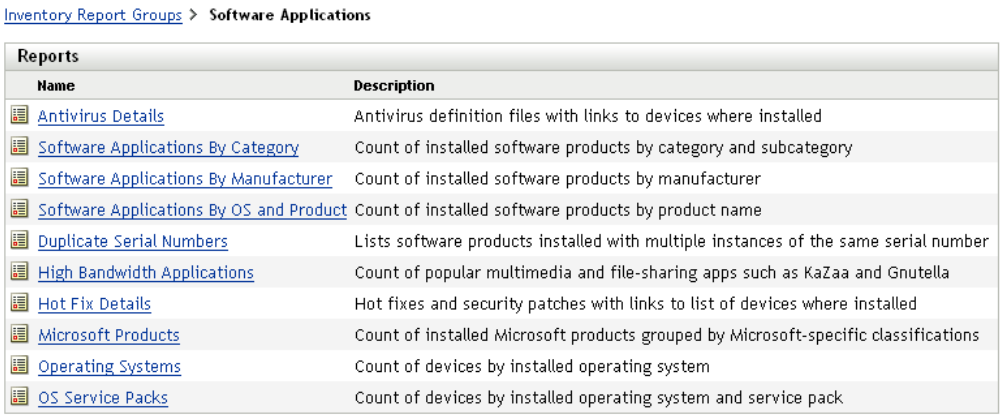

## 11.7.3 Generating an Inventory Report

ZENworks Configuration 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*.



Inventory Report Groups > **Software Applications**

**Reports**

| Name | Description |
|---|---|
| Antivirus Details | Antivirus definition files with links to devices where installed |
| Software Applications By Category | Count of installed software products by category and subcategory |
| Software Applications By Manufacturer | Count of installed software products by manufacturer |
| Software Applications By OS and Product | Count of installed software products by product name |
| Duplicate Serial Numbers | Lists software products installed with multiple instances of the same serial number |
| High Bandwidth Applications | Count of popular multimedia and file-sharing apps such as KaZaa and Gnutella |
| Hot Fix Details | Hot fixes and security patches with links to list of devices where installed |
| Microsoft Products | Count of installed Microsoft products grouped by Microsoft-specific classifications |
| Operating Systems | Count of devices by installed operating system |
| OS Service Packs | Count of devices by installed operating system and service pack |

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.

### 11.7.4 Where to Find More Information

For more information about inventory, see the *ZENworks 11 SP1 Asset Inventory Reference*.

## 11.8 Personality Migration

Personality Migration allows you to automate the process of migrating a set of customized system and application settings. A typical set of settings can be desktop wallpaper, e-mail account settings, browser proxy settings, files and folders, archived e-mails, Microsoft office templates, MS Excel Macros etc.This process significantly reduces the time and effort required in setting up or re-configuring a desktop for users.

For more information, see the *ZENworks 11 SP1 Personality Migration Reference*.

# 11.9 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 Novell ZENworks 11 SP1 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 reports 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 13, “Patch Management,” on page 139.

### 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.

# Endpoint Security Management

ZENworks 11 SP1 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:


- Section 12.1, “Activating Endpoint Security Management,” on page 131
- Section 12.2, “Enabling the Endpoint Security Agent,” on page 131
- Section 12.3, “Creating Locations,” on page 132
- Section 12.4, “Creating a Security Policy,” on page 132
- Section 12.5, “Assigning a Policy to Users and Devices,” on page 136
- Section 12.6, “Assigning a Policy to the Zone,” on page 137


## 12.1 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 11 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 Novell ZENworks Endpoint Security Management product site (http://www.novell.com/products/zenworks/endpointsecuritymanagement).
4. Click *OK*.

## 12.2 Enabling the Endpoint Security Agent

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

In addition to the ZENworks Adaptive 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 Section 7.1, “Configuring Adaptive Agent Features,” on page 61.

## 12.3 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 polices. 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 Section 6.7, "Creating Locations," on page 55.

## 12.4 Creating a Security Policy

There are 10 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 fixed disks and removable storage devices. With fixed disks, you specify the folders (referred to as **safe harbor folders**) that provide encryption; all other fixed disk folders are unaffected. |

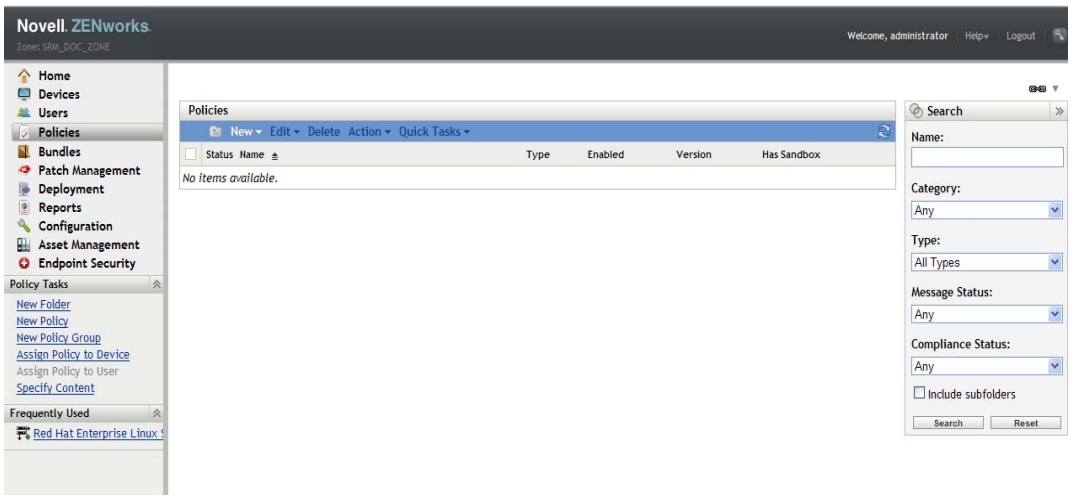
| Policy | Purpose |
|---|---|
| Firewall | Controls network connectivity by disabling ports, protocols, and network addresses (IP and MAC). |
| Storage Device Control | Controls access to CD/DVD drives, floppy drives, and removable storage drives. Each storage device type is configured individually, 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.

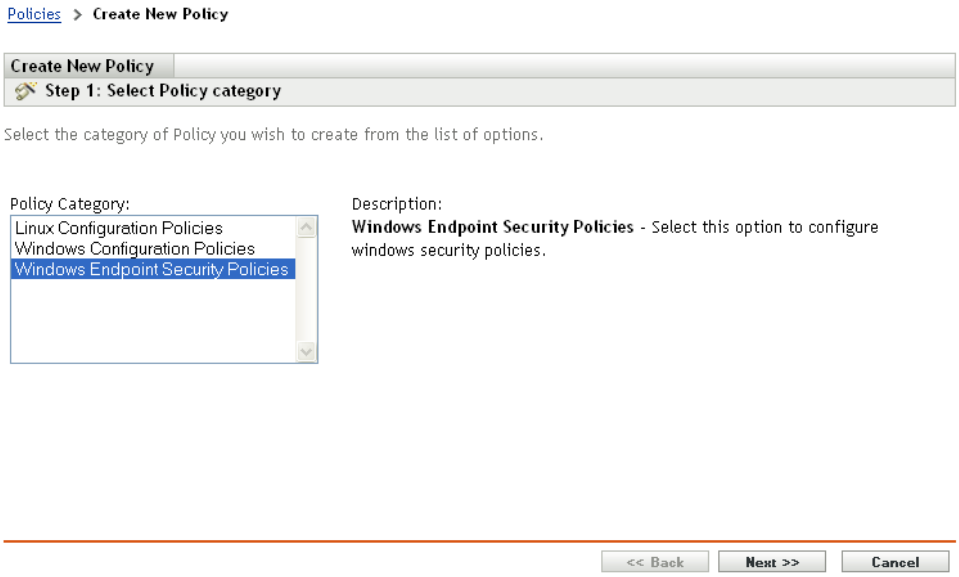
| Policy | Purpose |
|---|---|
| Security Settings | Protects the Endpoint Security Agent from being tampered with and uninstalled.<br><br>You should make sure a Security Settings policy is assigned to each device or user. |
| Location Assignment | Provides the list of allowed locations for a device 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.<br><br>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:

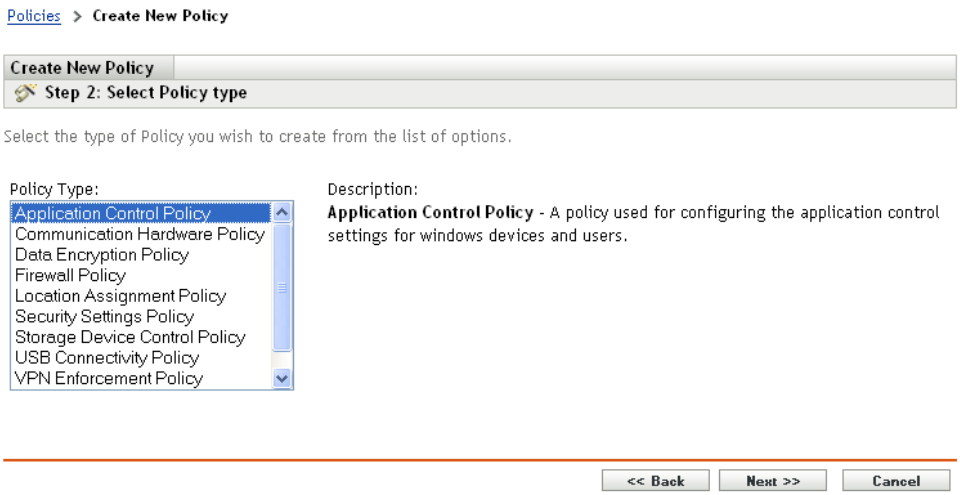
1. In ZENworks Control Center, click *Policies* to display the Policies page.




**2** In the Policies panel, click *New* > *Policy* to launch the Create New Policy Wizard.



3 On the Select Policy Category page, select *Windows Endpoint Security Policies*, then click *Next*.




4 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 polices can be applied.

5 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.

6 (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.

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.

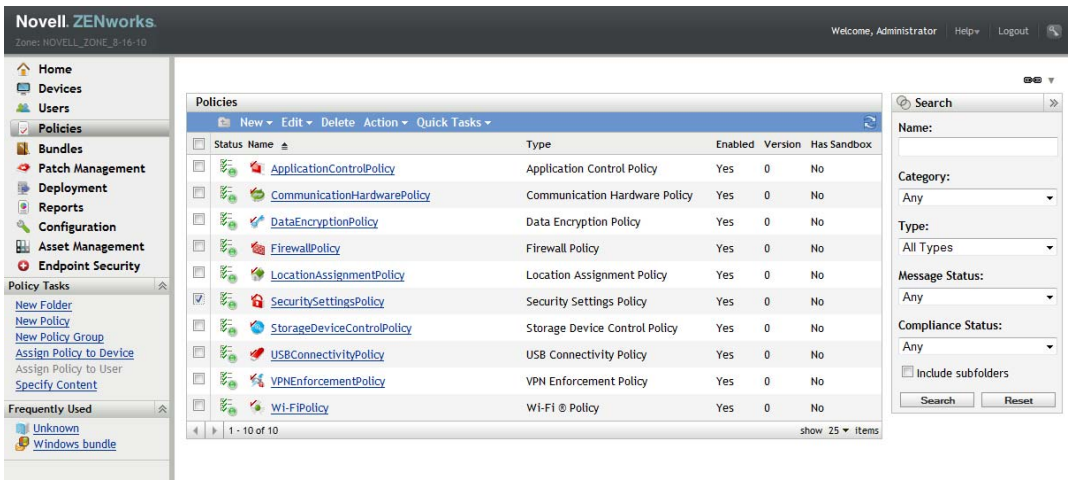
8 On the Summary page, review the information to make sure it is correct. If it is incorrect, click the *Back* button to revisit the appropriate wizard page and make changes. If it is correct, select either of the following options (if desired), then click *Finish*.

- **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.

## 12.5 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.

# 12.6 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:

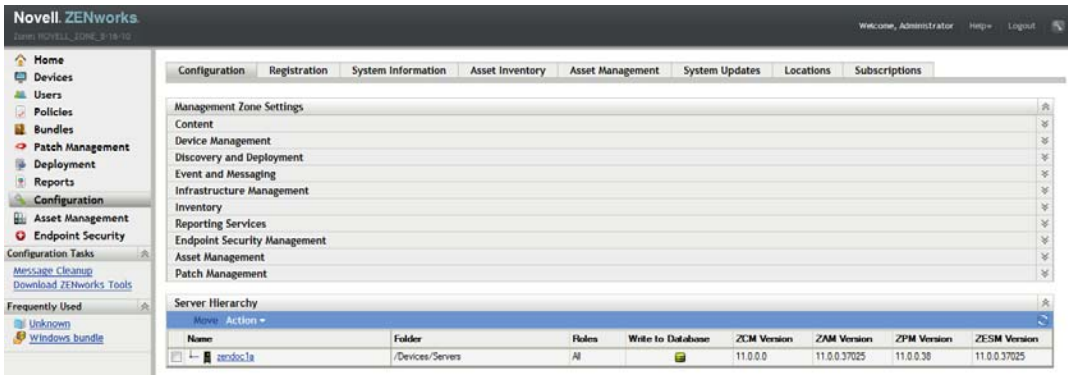
- No Firewall policies are assigned to a device or the device's user (either directly or through a group or folder). The Zone Firewall policy becomes the effective policy for the device and is enforced on the device.
- Firewall policies are assigned to a device and the device's user. Both policies are 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.

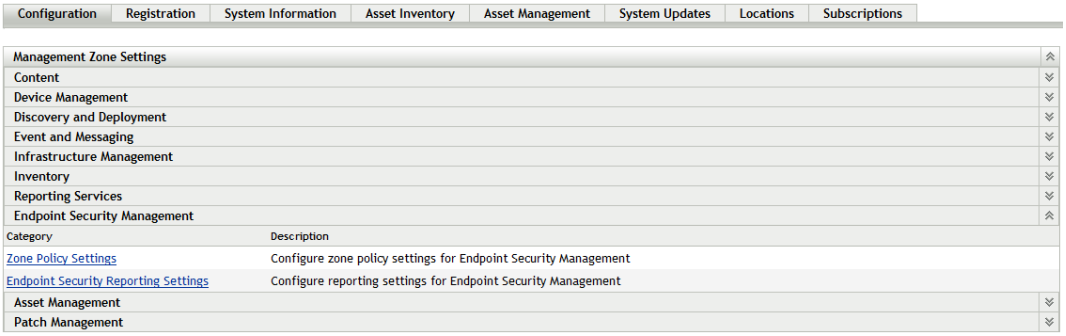
- **Management Zone:** The policies you assign at the Management Zone become the Zone policies for all devices, unless you specify different Zone policies at the device folder or device level.
- **Device Folder:** The policies you define at a device folder override the Management Zone (and any parent 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.

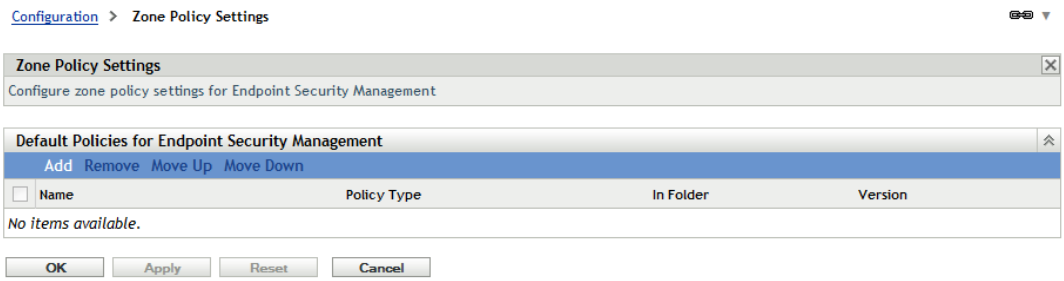
1. In ZENworks Control Center, click *Configuration* to display the Configuration page.




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*.

# 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 11 SP1 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.


- Section 13.1, “Activating Patch Management,” on page 139
- Section 13.2, “Enabling Patch Management in the ZENworks Adaptive Agent,” on page 140
- Section 13.3, “Starting the Subscription Service,” on page 140
- Section 13.4, “Deploying a Patch,” on page 141
- Section 13.5, “Where to Find More Information,” on page 142


## 13.1 Activating Patch Management

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

1. In ZENworks Control Center, click *Configuration*.
2. In the Licenses panel, click *ZENworks 11 Patch Management*.
3. 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 leave this field empty to activate the evaluation. 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 Novell ZENworks Patch Management product site (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*.

## 13.2 Enabling Patch Management in the ZENworks Adaptive Agent

For the ZENworks Adaptive 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 Section 7.1, "Configuring Adaptive Agent Features," on page 61.

## 13.3 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.

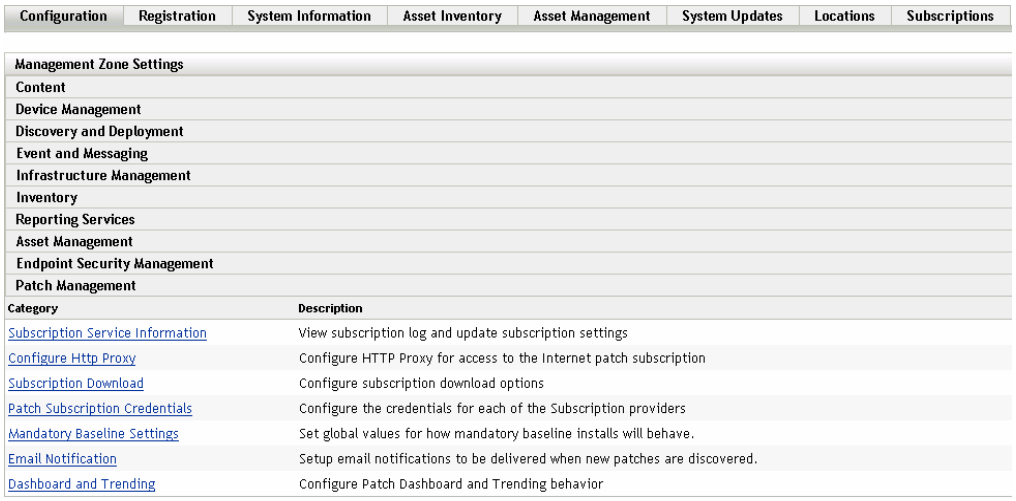
When a new patch is available from the subscription service, a ZENworks Server downloads it automatically. The Patches page (on the *Patch Management* tab) displays the new patch, along with a description and business impact. You can deploy the patch to devices or disregard the patch.

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.

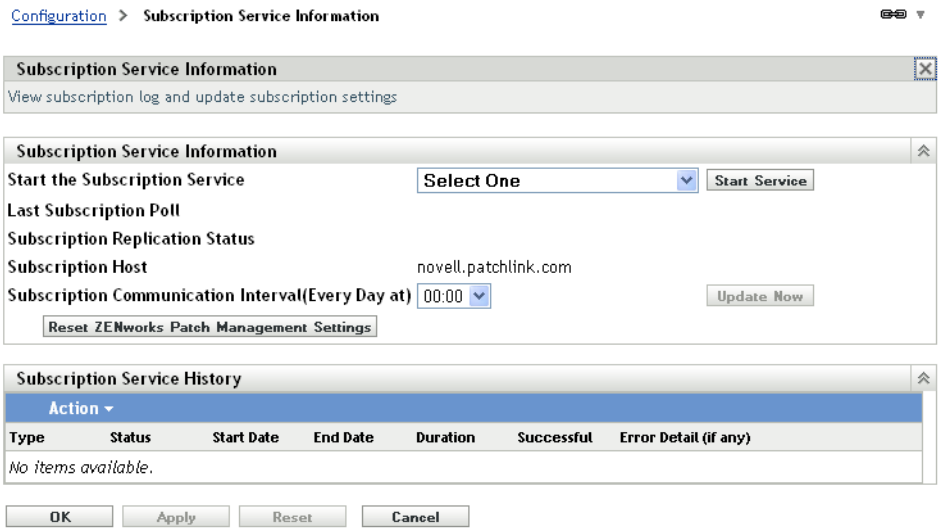
If there are multiple ZENworks Servers in your Management Zone, you can select any one of them to be the Patch Management Server. The server that is selected as the Patch Management Server should have the best connectivity to the Internet, because it is downloading new patches and updates on a daily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

## 13.4 Deploying a Patch

Before you can begin deploying patches to devices, the ZENworks Adaptive Agent must perform the Discover Applicable Updates (DAU) task. The DAU task allows the ZENworks Adaptive 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 a patch, you use the Deploy Remediation Wizard. The wizard lists only those devices to which the patch applies and lets you deselect any devices that you don't want patched. In addition, you can schedule when you want to deploy the patch.

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

1 In ZENworks Control Center, click the *Patch Management* tab.

2 In the *Patches* tab, select the patch you want to deploy by clicking the check box in front of the patch, then click *Actions* > *Deploy Remediation* to launch the Deploy Remediation Wizard.

3 Follow the prompts to deploy the patch.

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

## 13.5 Where to Find More Information

For more information about patching software, see the *ZENworks 11 SP1 Patch Management Reference*.

# 13

# Appendix IV

This part of the *Administration Quick Start Reference* includes sections with additional information that might help you as you work on ZENworks 11 SP1:


- Appendix A, “Installation and Setup Documentation,” on page 147
- Appendix B, “Administration Documentation,” on page 149

# Installation and Setup Documentation

# A

The following references provide information to install, upgrade, migrate to, and set up Novell ZENworks 11 SP1:

- *ZENworks 11 SP1 Installation Guide*

  Provides instructions on establishing the ZENworks Management Zone with one or more ZENworks Primary Servers. Includes instructions for GUI, command line, or silent installations.

- *ZENworks Virtual Appliance 11 SP1 Deployment and Administration Reference*

  Provides instructions on how to deploy and manage ZENworks Appliance.

- *ZENworks 11 SP1 Reporting Server Installation Guide*

  Provides instructions for installing ZENworks Reporting Server for ZENworks infrastructure reporting.

- *ZENworks 11 SP1 Upgrade Guide*

  Provides information to help you successfully upgrade to Novell ZENworks 11 SP1.

- *ZENworks 11 SP1 Configuration Management Migration Guide*

  Provides instructions on how to migrate your traditional ZENworks Novell eDirectory data into the ZENworks Configuration Management database. This includes migrating information from Application, Imaging, Policy, and Workstation objects, including associations and zone settings. It does not include migrating User objects. Instead, Configuration Management reads from existing user sources. It also does not migrate inventory data; that is done with the ZENworks Asset Management Migration Utility.

- *Novell ZENworks 11 SP1 Asset Management Migration Guide*

  Provides instructions on how to migrate ZENworks Asset Management 7.5 data to ZENworks 11 SP1.

- *ZENworks 11 SP1 Linux Management Migration Guide*

  Provides instructions on how to migrate the data from ZENworks 7.2 Linux Management with IR2 or later to ZENworks 11.

- *ZENworks 11 SP1 Personality Migration Reference*

  Provides instructions on the setup and installation of Personality Migration, and the use of Desktop DNA for migrating, upgrading, and backing up devices.

- *ZENworks 7 Handheld Management Installation Guide (http://www.novell.com/documentation/zenworks7/hm7install/data/a20gkue.html)*

  Provides instructions on how to install Handheld Management.

- *ZENworks 11 SP1 Administration Quick Start*

  ZENworks 11 SP1 is ready to use out of the box, but you probably want to configure it to suit your environment. The *Administration Quick Start* includes basic instructions to set up ZENworks for your network, including short tasks to familiarize you with the features of the product.

- *AdminStudio 9.5 Standard Edition Installation Guide (http://www.novell.com/documentation/zenworks11/pdfdoc/adminstudio/AS95ZENInstallGuide.pdf)*

  Provides information to install and activate AdminStudio.

# Administration Documentation

# B

The following references for ZENworks 11 SP1 provide overviews, setup instructions, usage instructions, ongoing management instructions, and other information:

- *ZENworks 11 SP1 System Administration Reference*

  Provides instructions on folder and group organization in ZCC, user sources, ZENworks administrator accounts, Management Zone configuration settings, alternate content repository configuration, database maintenance, and so on.

- *ZENworks 11 SP1 System Reporting Reference*

  Provides instructions on how to perform BusinessObjects Enterprise XI reporting on your ZENworks infrastructure.

- *ZENworks 11 SP1 Discovery, Deployment, and Retirement Reference*

  Provides instructions on device registration, the ZENworks Adaptive Agent, network device discovery, device importing, inventoried-only device setup, and deployment tasks.

- *ZENworks 11 SP1 Command Line Utilities Reference*

  Provides instructions on the zman, zac, and zeninfocollect command line utilities.

- *ZENworks 11 SP1 Software Distribution Reference*

  Provides instructions on software distribution through bundle creation and management, bundle assignments, bundle scheduling, and actions that can be added to bundles.

- *ZENworks 11 SP1 Configuration Policies Reference*

  Provides instructions on policy creation and application for configuring operating system and application settings.

- *ZENworks 11 SP1 Preboot Services and Imaging Reference*

  Provides instructions on Preboot Services setup, device imaging, Imaging bundles, and manual imaging operations.

- *ZENworks 11 SP1 Remote Management Reference*

  Provides instructions on how to remotely manage and control devices.

- *ZENworks 11 SP1 Asset Inventory Reference*

  Provides instructions on software and hardware inventory collection, including how to scan, view individual device inventory information, and generate inventory reports.

- *ZENworks 11 SP1 Out-of-Band Management Reference*

  Provides instructions on how to provision Intel AMT capable devices and manage their power states through out-of-band means.

- *ZENworks 11 SP1 Asset Management Reference*

  Provides instructions on how to manage your software assets.

- *ZENworks 11 SP1 Patch Management Reference*

  Provides instructions on automated patch application to minimize vulnerabilities and compliance issues.

- *ZENworks 11 SP1 Endpoint Security Policies Reference*

- *ZENworks 11 SP1 Endpoint Security Agent Reference*
- *ZENworks 7 Handheld Management Administration Guide (http://www.novell.com/documentation/zenworks7/hm7admin/data/a20gkue.html)*

  Provides instructions on how to set up and manage handheld devices.
- *AdminStudio 9.5 Standard Edition User Guide (http://www.novell.com/documentation/zenworks11/pdfdoc/adminstudio/AS95UserGuide.pdf)*

  Provides administration and end-user information about the functionality and features of all of the components of AdminStudio.