

# Novell ZENworks® 10 Configuration Management

10.0.3

May 16, 2008

DISCOVERY AND DEPLOYMENT  
REFERENCE

[www.novell.com](http://www.novell.com)



Novell®

## 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 \(http://www.novell.com/info/exports/\)](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 © 2008 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., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the [Novell Legal Patents Web page \(http://www.novell.com/company/legal/patents/\)](http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.  
404 Wyman Street, Suite 500  
Waltham, MA 02451  
U.S.A.  
[www.novell.com](http://www.novell.com)

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

## **Novell Trademarks**

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

## **Third-Party Materials**

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



# Contents

<b>About This Guide</b>	<b>7</b>
<b>Part I Device Discovery</b>	<b>9</b>
<b>1 Basic Concepts</b>	<b>11</b>
1.1 Discovery Methods	11
1.2 IP and LDAP Discovery Tasks	11
1.3 IP Discovery Technologies	12
1.4 LDAP Discovery Technology	14
1.5 Discovered Devices	14
1.6 Deployable Devices	15
<b>2 Discovering Devices By Using IP Addresses</b>	<b>17</b>
2.1 Configuring Discovery Settings	17
2.2 Designating a Discovery and Deployment Proxy Server	19
2.3 Creating an IP Discovery Task	21
<b>3 Discovering Devices in LDAP Directories</b>	<b>27</b>
<b>4 Importing Devices from CSV Files</b>	<b>31</b>
<b>Part II ZENworks Adaptive Agent Deployment</b>	<b>33</b>
<b>5 Basic Concepts</b>	<b>35</b>
5.1 Deployment Methods	35
5.2 Deployment Packages	35
5.3 Adaptive Agent Versus Inventory-Only Module	36
<b>6 Managing Deployment Packages</b>	<b>39</b>
6.1 Package Types and Architectures	39
6.2 Default System Packages Versus Custom Packages	40
6.3 Packages without the Remote Management Module	40
6.4 Customizing a Package	41
6.5 Enabling the No Remote Management Packages	43
<b>7 Registering Devices</b>	<b>45</b>
7.1 What Happens During Registration	45
7.2 Creating Registration Keys and Rules	46
7.2.1 Creating a Registration Key	46
7.2.2 Creating a Registration Rule	49
7.3 Modifying the Device Naming Template Used During Registration	53

7.4	Enabling Dynamic Renaming of Devices During Registration . . . . .	54
7.4.1	Enabling the Setting at the Management Zone . . . . .	55
7.4.2	Enabling the Setting for a Device Folder . . . . .	56
7.5	Disabling the Use of Registration Rules . . . . .	57
7.6	Manually Registering a Device . . . . .	58
7.6.1	Performing an Initial Registration . . . . .	58
7.6.2	Reregistering a Device with an Additional Registration Key . . . . .	59
7.7	Unregistering a Device . . . . .	59
<b>8</b>	<b>Deploying the ZENworks Adaptive Agent</b>	<b>61</b>
8.1	Changing the Target Installation Directory . . . . .	61
8.2	Using a Task to Deploy the Agent . . . . .	61
8.2.1	Prerequisites for Deploying to a Device . . . . .	62
8.2.2	Deploying to a Discovered Device . . . . .	63
8.2.3	Deploying to a Non-Discovered Device . . . . .	66
8.3	Manually Deploying the Agent . . . . .	77
<b>9</b>	<b>Deploying the Inventory-Only Module</b>	<b>81</b>
9.1	Downloading the Module from a ZENworks Server . . . . .	81
9.2	Installing on Linux/UNIX . . . . .	82
9.3	Installing on NetWare . . . . .	83
9.4	Installing on Windows . . . . .	83
9.5	Installing on Macintosh OS X . . . . .	83
	<b>Part III Appendixes</b>	<b>85</b>
<b>A</b>	<b>Schedules</b>	<b>87</b>
A.1	Now . . . . .	87
A.2	No Schedule . . . . .	87
A.3	Date Specific . . . . .	87
A.3.1	Start Dates . . . . .	87
A.3.2	Run Event Every Year . . . . .	87
A.3.3	Select When Schedule Execution Should Start . . . . .	87
A.3.4	Use Coordinated Universal Time (UTC) . . . . .	87
A.4	Recurring . . . . .	88
A.4.1	Days of the Week . . . . .	88
A.4.2	Monthly . . . . .	88
A.4.3	Fixed Interval . . . . .	89
<b>B</b>	<b>Configuring NMAP for ZENworks</b>	<b>91</b>

# About This Guide

This *Novell ZENworks 10 Configuration Management Discovery and Deployment Reference* helps you add devices to your Novell® ZENworks® system and then install the ZENworks Adaptive Agent or Inventory Only Module to the devices.

The information in this guide is organized as follows:

- ♦ **Part I, “Device Discovery,” on page 9**
- ♦ **Part II, “ZENworks Adaptive Agent Deployment,” on page 33**
- ♦ **Part III, “Appendixes,” on page 85**

## Audience

This guide is intended for anyone who will configure and manage a ZENworks system.

## Feedback

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

## Additional Documentation

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

## Documentation Conventions

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

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

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



# Device Discovery

The following sections provide information and instructions to help you add devices to your ZENworks® database. After a device is added to the database, a ZENworks Server can automatically deploy the ZENworks Adaptive Agent to the device.

- ♦ Chapter 1, “Basic Concepts,” on page 11
- ♦ Chapter 2, “Discovering Devices By Using IP Addresses,” on page 17
- ♦ Chapter 3, “Discovering Devices in LDAP Directories,” on page 27
- ♦ Chapter 4, “Importing Devices from CSV Files,” on page 31



# Basic Concepts

# 1

Device discovery is the process of adding workstation and server information to the ZENworks<sup>®</sup> database so that you can use that information to automatically deploy the ZENworks Adaptive Agent from a ZENworks Server to the devices. The following sections provide information to help you understand the discovery terminology and concepts:

- ♦ [Section 1.1, “Discovery Methods,” on page 11](#)
- ♦ [Section 1.2, “IP and LDAP Discovery Tasks,” on page 11](#)
- ♦ [Section 1.3, “IP Discovery Technologies,” on page 12](#)
- ♦ [Section 1.4, “LDAP Discovery Technology,” on page 14](#)
- ♦ [Section 1.5, “Discovered Devices,” on page 14](#)
- ♦ [Section 1.6, “Deployable Devices,” on page 15](#)

## 1.1 Discovery Methods

There are three discovery methods you can use:

- ♦ **IP discovery:** Use the ZENworks discovery engine to collect information about devices on your network. The engine uses various protocols and standards (WMI, WinAPI, MAC Address, NMAP, ZENworks, SNMP, SSH) to discover and collect information from devices that you identify through IP address ranges.
- ♦ **LDAP directory discovery:** Use the ZENworks discovery engine to search Novell<sup>®</sup> eDirectory<sup>™</sup> or Microsoft<sup>®</sup> Active Directory<sup>®</sup> for device objects. You specify the contexts to search and the filter to use for the search.
- ♦ **CSV import:** Import device information from a comma-separated values (CSV) file. At the minimum, the file must contain the IP address or DNS name for each device.

## 1.2 IP and LDAP Discovery Tasks

IP and LDAP discoveries are performed through discovery tasks. You create a discovery task in ZENworks Control Center.

IP discovery tasks require the following information:

- ♦ The range of IP addresses for the devices you want discovered.
- ♦ The credentials required for the SSH, WMI, WinAPI, and SNMP discovery technologies to retrieve information from devices. The NMAP, MAC Address, and ZENworks technologies do not require credentials.

Not all technologies use the same credentials, and all devices might not have the same credentials, so you might need to specify multiple credentials to cover all targeted devices and to utilize all discovery technologies. For example, WMI and WinAPI require Windows credentials, and SNMP requires SNMP credentials.

By default, all technologies are used except for SNMP, WMI, and NMAP; you can use the Discovery configuration setting on the Configuration page to change which technologies are used.

- ♦ The schedule for running the task. You can schedule it to run immediately or at a specified date and time. Optionally, you can choose to not set a schedule, in which case the task is not run until you manually initiate it or schedule a time.
- ♦ The ZENworks Server that you want to run the task.

LDAP discovery tasks require the following information:

- ♦ The connection information (address and port) for the LDAP server.
- ♦ The credentials required for reading information from the LDAP directory.
- ♦ The directory contexts to search for devices.
- ♦ The schedule for running the task. You can schedule it to run immediately or at a specified date and time. Optionally, you can choose to not set a schedule, in which case the task is not run until you manually initiate it or schedule a time.
- ♦ The ZENworks Server that you want to run the task.

## 1.3 IP Discovery Technologies

The ZENworks discovery engine can utilize a variety of different technologies for IP-based discoveries. When more than one technology is used, the discovery engine initiates a discovery request for each technology. This is done for each target IP address. For example, if you use MAC Address, SNMP, and WMI, the discovery engine creates three requests for each target IP address. The requests are queued and the discovery engine processes five requests at a time until no requests remain. Five requests is the default. You can change the default if necessary; see [Section 2.1, “Configuring Discovery Settings,” on page 17](#).

If more than one technology request returns information for a discovered device, the information is merged together. In the case of conflicting information, the discovery process chooses the “best” information.

By default, the MAC Address, SSH, WinAPI, and ZENworks technologies are enabled; the SNMP, WMI, and NMAP technologies are disabled. You can change the default if necessary; see [Section 2.1, “Configuring Discovery Settings,” on page 17](#).

Using fewer discovery technologies reduces the time required to complete the discovery task but might also reduce the amount of information received.

Following are descriptions of each IP discovery technology:

- ♦ **WMI:** Issues a request to the WMI (Windows\* Management Instrumentation) service on the devices identified by the IP-based discovery task. It requires Microsoft Windows Management Instrumentation Service to be installed and running on the target Windows device. Since the Remote WMI establishes a DCOM connection with the target Windows device, the DCOM port TCP 445 and the RPC port TCP 135 must be allowed by the Windows Firewall of the target device for the WMI discovery technology. For more information on how to open these ports, see [“Enabling File and Printer Sharing through Windows Firewall” on page 62](#).

To authenticate and connect to the device using the Windows credentials, set the value of the *Network access: Sharing and security model for local accounts* Local Security setting to *Classic - local users authenticate as themselves*. For more information on how to configure the Local Security settings, see [“Enabling Classic File Sharing” on page 62](#).

Because WMI is a Windows-specific technology, the requests generated from a ZENworks Server running on Linux must be routed to a Windows proxy for processing. For more information, see [Section 2.2, “Designating a Discovery and Deployment Proxy Server,” on page 19](#).

- ♦ **WinAPI:** Issues a request to the registry on the devices identified by the IP-based discovery task in an attempt to determine a device’s OS type and version. This requires Microsoft Remote Registry Service to be installed and running on the target Windows device. To authenticate and connect to the device using the Windows credentials, set the value of the *Network access: Sharing and security model for local accounts* Local Security setting to *Classic - local users authenticate as themselves*. For more information on how to configure the Local Security settings, see [“Enabling Classic File Sharing” on page 62](#). Because WinAPI is a Windows-specific technology, the requests generated from a ZENworks Server running on Linux must be routed to a Windows proxy for processing. For more information, see [Section 2.2, “Designating a Discovery and Deployment Proxy Server,” on page 19](#).
- ♦ **MAC Address:** Uses the `ping` and `arp` (Address Resolution Protocol) commands to map the IP addresses of the devices identified by the IP-based discovery task to their associated MAC addresses. For the `arp` command to be successful, the target devices must reside in the same network as the ZENworks Server that performs the discovery request. For the `ping` command to be successful, the incoming ICMP echo requests (`ping`) must be enabled on the device, and the ICMP echo requests and echo responses must be allowed on the network.
- ♦ **NMAP:** Uses NMAP (Network Mapper) to discover the OS type and version of the devices identified by the IP-based discovery task. NMAP must be installed on the ZENworks Server or Windows Proxy that is processing the discovery request. NMAP is freely available from [InSecure.org](http://www.insecure.org) (<http://www.insecure.org>).
- ♦ **ZENworks:** Issues a request to the ZENworks preagent on the devices identified by the IP-based discovery task. The preagent responds with OS type, CPU information, disk information, memory information, and the GUID (global unique identifier) that should be used to register the device in the Management Zone.  
  
The preagent is only installed on OEM devices or on devices whose registration was removed from the zone.
- ♦ **SNMP:** Issues a request to the SNMP service on the devices identified by the IP-based discovery task. SNMP versions 2 and 1 are supported, with SNMP version 2 tried first. To query a device using SNMP, the device must have SNMP enabled and the SNMP community string must be specified as a SNMP credential in the Discovery Task. SNMP uses the UDP Port 161. The firewall must be configured to allow access through this port. Because the discovery process uses a Windows-based SNMP technology, requests generated from a ZENworks Server running on Linux must be routed to a Windows proxy for processing. For more information, see [Section 2.2, “Designating a Discovery and Deployment Proxy Server,” on page 19](#).
- ♦ **SSH:** Uses the SSH protocol to communicate with the SSH server on the devices identified by the IP-based discovery task. Depending on the device OS (Linux or NetWare®), the device responds with version, CPU information, and memory information. To query a device using SSH, the device should have SSH enabled, and the username and password must be specified as General or Linux credentials in the Discovery task.

## 1.4 LDAP Discovery Technology





For LDAP discoveries, the ZENworks discovery engine issues an LDAP request to the LDAP server. The LDAP request contains the LDAP server name, LDAP port, credentials, the context or group to search, and whether or not to recursively search subcontainers or subgroups.

Device objects that are found are queried for well-known attributes (dnsHostName, OperatingSystem, wmNameDNS, wmNameOS, and so forth) to attempt to determine the OS version and DNS name of the device. If the request specifies a recursive search, the context is searched for well-known container objects. For each container object found, a new LDAP request is created for the container object and appended to the search context of the current request.

## 1.5 Discovered Devices

As devices are discovered, they are added to the ZENworks database and listed in the appropriate device type folder in the Discovered panel on the Discovered Devices page.

**Figure 1-1** Discovered panel (Devices tab > Discovered page)

Discovered		Inventoried	Managed
Discovered			
Type		Discovered	
	<a href="#">All Types</a>	<a href="#">4</a>	
	<a href="#">Servers</a>	<a href="#">0</a>	
	<a href="#">Workstations</a>	<a href="#">0</a>	
	<a href="#">Printers</a>	<a href="#">0</a>	
	<a href="#">Network Equipment</a>	<a href="#">0</a>	
	<a href="#">Thin Clients</a>	<a href="#">0</a>	
	<a href="#">Other Devices</a>	<a href="#">0</a>	
	<a href="#">Unknown Devices</a>	<a href="#">4</a>	
	<a href="#">Deployable Types</a>	<a href="#">4</a>	
	<a href="#">Devices created via ZENworks Migration</a>	<a href="#">0</a>	
	<a href="#">Devices created via ZENworks Asset Management</a>	<a href="#">0</a>	

Each discovered devices is categorized by type.

- ♦ **All Types:** All discovered devices, regardless of type.
- ♦ **Servers:** All discovered devices that have been identified as servers.
- ♦ **Workstations:** All discovered devices that have been identified as workstations.
- ♦ **Printers:** All discovered devices that have been identified as printers. ZENworks does not manage printers; therefore, you cannot deploy the ZENworks Adaptive Agent to them.
- ♦ **Network Equipment:** All discovered devices that have been identified as network equipment. This includes such devices as routers. ZENworks does not manage network equipment; therefore, you cannot deploy the ZENworks Adaptive Agent to network equipment.
- ♦ **Thin Clients:** All discovered devices that have been identified as thin clients.
- ♦ **Other Devices:** All discovered devices that have been identified but don't fit into one of the other categories. This category includes devices that already have the ZENworks Adaptive Agent installed.
- ♦ **Unknown Devices:** All discovered devices whose operating system cannot be identified. The devices might be listed as unknown because the firewall configuration of the device may block

the usage of discovery technologies, or invalid credentials are provided to the discovery technology. You can deploy the ZENworks Adaptive Agent to these devices if you can manually ensure that ZENworks Configuration Management is supported on these devices. For more information on list of supported devices, see “[Managed Device Requirements](#)” in *ZENworks 10 Configuration Management Installation Guide*.

- ♦ **Deployable Types:** All discovered devices that have been identified as types to which you can deploy the ZENworks Adaptive Agent.
- ♦ **Devices Created Via ZENworks Migration:** All devices that were migrated from ZENworks 7 through the ZENworks Migration utility.
- ♦ **Devices Created Via ZENworks Asset Management:** All devices that were migrated from ZENworks Asset Management through the ZENworks Asset Management Migration utility.

## 1.6 Deployable Devices

Devices that meet the requirements for the ZENworks Adaptive Agent are displayed in ZENworks Control Center in the Deployable Devices panel on the Deployment page.

**Figure 1-2** Deployable Devices panel (Deployment tab)

Deployable Devices					Advanced
Delete Action View					
<input type="checkbox"/>	Name	IP Address	Operating System	Discovered Date	Deployment Status
<input type="checkbox"/>	<a href="#">roshambo-t60p.dnsdhcp.provo.novell.com</a>	137.65.164.51	Unknown OS	Jun 25, 2007	Inactive
<input type="checkbox"/>	<a href="#">dvandenbosdp360.dnsdhcp.provo.novell.com</a>	137.65.164.52	Unknown OS	Jun 25, 2007	Inactive
<input type="checkbox"/>	<a href="#">rbf-dell.dnsdhcp.provo.novell.com</a>	137.65.164.53	Unknown OS	Jun 25, 2007	Inactive
<input type="checkbox"/>	<a href="#">kevinsxp-pro.dnsdhcp.provo.novell.com</a>	137.65.164.54	Unknown OS	Jun 25, 2007	Inactive
1 - 4 of 4					show 25 items

Using this panel, you can deploy the Adaptive Agent to devices, remove them from the ZENworks database, or ignore them by filtering them out of the list.



# Discovering Devices By Using IP Addresses

# 2

You can perform an IP-based discovery of your network to add devices to your ZENworks® database. With an IP discovery, the ZENworks Server uses a set of technologies (WMI, WinAPI, MAC Address, NMAP, ZENworks, SNMP, SSH) to discover as much information about the target devices as possible. The target devices are determined by the IP address range you specify.

- [Section 2.1, “Configuring Discovery Settings,” on page 17](#)
- [Section 2.2, “Designating a Discovery and Deployment Proxy Server,” on page 19](#)
- [Section 2.3, “Creating an IP Discovery Task,” on page 21](#)

## 2.1 Configuring Discovery Settings

IP discoveries use several configuration settings that you can modify if necessary. This includes the number of discoveries that can be processed concurrently (the default is 5) and the discovery technologies that are used (the default is LDAP, MAC Address, WinAPI, ZENworks, and SSH).

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

Configuration	Registration	System Information	Asset Inventory	System Updates	Asset Management
Management Zone Settings					⤴
Content					⤵
Device Management					⤵
Discovery and Deployment					⤴
Category	Description				Is Configured
<a href="#">Advertised Discovery Settings</a>	Configure the interval and subnets of advertised devices on your network.				Yes
<a href="#">Discovery</a>	Configure settings related to discovering new devices.				Yes
<a href="#">Windows Proxy</a>	Configure a managed Windows device to be used as the Windows Proxy for discovery and deployment.				No
Event and Messaging					⤵
Infrastructure Management					⤵
Inventory					⤵
Reporting Services					⤵
Asset Management					⤵
Patch Management Services					⤵

- 2 In the Management Zone Settings panel, click *Discovery and Deployment*, then click the *Discovery* option.
- 3 In the Discovery Process Settings panel, modify the following settings as necessary:

**Maximum Concurrent Discoveries:** A discovery task consists of one or more discovery requests. For IP-based discovery tasks, a request is created for each discovery technology and each IP address in the specified range. Therefore, if you use six technologies to discover 10 IP addresses, 60 requests are created. For LDAP-based discovery tasks, a request is created for each context or group to be searched.

You use this field to specify the maximum number of discovery requests that the ZENworks Server can process at one time. A smaller number eases the traffic load on the network but requires more time to complete the discovery task; you should use a smaller number if you schedule discovery tasks during peak network load times. A larger number has the opposite effect; heavier traffic load with less time to complete the task.

**Discovery Technologies:** The discovery process can utilize a variety of different technologies. When more than one technology is used, the discovery process initiates a discovery request for each technology, with all technology requests running simultaneously. This is done for each target IP address. For example, if you use MAC Address, SNMP, and WMI, the discovery process creates three requests for each target IP address. The requests are queued and run according to the *Maximum Concurrent Discoveries* setting.

If more than one technology request returns information for a discovered device, the information is merged together. In the case of conflicting information, the discovery process chooses the “best” information.

Using fewer discovery technologies reduces the time required to complete the discovery task but might also reduce the amount of information received.

Following are brief descriptions of each technology:

- ♦ **MAC Address:** Uses the `ping` and `arp` (Address Resolution Protocol) commands to map the IP addresses of the devices identified by the IP-based discovery task to their associated MAC addresses. The target devices must reside in the same network as the ZENworks Server that performs the discovery request.
- ♦ **NMAP:** Uses NMAP (Network Mapper) to discover the OS type and version of the devices identified by the IP-based discovery task. NMAP must be installed on the ZENworks Server or Windows Proxy that is processing the discovery request. NMAP is freely available from [InSecure.org](http://www.insecure.org) (<http://www.insecure.org>). For detail information on how to configure NMAP for ZENworks, see the [Appendix B, “Configuring NMAP for ZENworks,” on page 91](#).
- ♦ **SNMP:** Issues a request to the SNMP service on the devices identified by the IP-based discovery task. SNMP versions 2 and 1 are supported, with SNMP version 2 tried first. Because the discovery process uses a Windows-based SNMP technology, requests generated from a ZENworks Server running on Linux must be routed to a Windows proxy for processing. For more information, see [“Designating a Discovery and Deployment Proxy Server” on page 19](#).
- ♦ **SSH:** Uses the SSH protocol to communicate with the SSH server on the devices identified by the IP-based discovery task. Depending on the device OS (Linux or NetWare<sup>®</sup>), the device responds with version, CPU information, and memory information.
- ♦ **WinAPI:** Issues a request to the registry on the devices identified by the IP-based discovery task in an attempt to determine a device’s OS type and version. Because WinAPI is a Windows-specific technology, requests generated from a ZENworks Server running on Linux must be routed to a Windows proxy for processing. For more information, see [“Designating a Discovery and Deployment Proxy Server” on page 19](#).
- ♦ **WMI:** Issues a request to the WMI (Windows Management Instrumentation) service on the devices identified by the IP-based discovery task. Because WMI is a Windows-specific technology, requests generated from a ZENworks Server running on Linux must be routed to a Windows proxy for processing. For more information, see [“Designating a Discovery and Deployment Proxy Server” on page 19](#).
- ♦ **ZENworks:** Issues a request to the ZENworks preagent on the devices identified by the IP-based discovery task. The preagent responds with OS type, CPU information, disk

information, memory information, and the GUID (global unique identifier) that should be used to register the device in the Management Zone.

The preagent is only installed on OEM devices or on devices whose registration was removed from the zone.

- 4 In the Network Discovery Settings panel, modify the following settings as necessary:

**IP Settings:** These settings apply when using the WMI and SNMP discovery technologies.

- ♦ **Initial ping timeout:** Specifies how long the discovery technology waits for a response to an ICMP query (ping).
- ♦ **Maximum ping retries:** Specifies the number of times a ping is repeated before giving up.
- ♦ **Increment ping timeout on retries by:** Adds the specified amount of time to each retry. For example, if the initial ping timeout is 200 milliseconds, the maximum ping retries is 3, and the increment is 200 milliseconds, the first retry timeout is 400, the second retry timeout is 600, and the third retry timeout is 800.
- ♦ **Perform name lookups:** Uses a reverse lookup to associate the target IP address with a DNS name. Deselect this option if you do not want the DNS name discovered.

**SNMP Settings:** These settings apply when using the SNMP discovery technology.

- ♦ **Initial SNMP timeout:** Specifies how long the discovery technology waits for a response to an SNMP query before assuming that the packet is lost.
- ♦ **Maximum SNMP retries:** Specifies the number of times an SNMP query is repeated before giving up.
- ♦ **Increment SNMP timeout on retries by:** Adds the specified amount of time to each retry. For example, if the initial SNMP timeout is 500 milliseconds, the maximum SNMP retries is 3, and the increment is 1000 milliseconds, the first retry timeout is 1500, the second retry timeout is 2500, and the third retry timeout is 3500.

- 5 Click *OK* to save the changes.

## 2.2 Designating a Discovery and Deployment Proxy Server

ZENworks Servers running on Linux cannot perform discovery tasks that use Windows-specific technologies such as WMI and WinAPI. Linux servers also cannot perform deployment of ZENworks Adaptive Agents to Windows devices, as deployment uses Windows-specific technologies. In order to enable the execution of discovery and deployment tasks by Linux ZENworks Servers, you can designate a managed Windows device in your zone to function as a discovery and deployment proxy server. The managed device can be either a Windows server or workstation.

When a Linux ZENworks Server receives a discovery task that includes Windows-specific technologies, it processes the non-Windows discovery technologies and offloads the Windows-specific technologies to the proxy. The proxy performs the discoveries and returns the results to the Linux ZENworks Server. The deployment task is totally offloaded to the Windows proxy.

If you have only Linux servers in your environment, you must first manually install ZENworks Adaptive Agent on a Windows device by downloading the agent from <https://>

*IP\_address\_of\_the\_ZENworks\_Server/zenworks-setup*, then designate the device as a proxy for discovery and deployment tasks.

To designate a proxy:

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

Configuration	Registration	System Information	Asset Inventory	System Updates	Asset Management	
Management Zone Settings						⤴
Content						⤴
Device Management						⤴
Discovery and Deployment						⤴
Category	Description				Is Configured	
<a href="#">Advertised Discovery Settings</a>	Configure the interval and subnets of advertised devices on your network.				Yes	
<a href="#">Discovery</a>	Configure settings related to discovering new devices.				Yes	
<a href="#">Windows Proxy</a>	Configure a managed Windows device to be used as the Windows Proxy for discovery and deployment.				No	
Event and Messaging						⤴
Infrastructure Management						⤴
Inventory						⤴
Reporting Services						⤴
Asset Management						⤴
Patch Management Services						⤴


- 2 In the Management Zone Settings panel, click *Discovery and Deployment*, then click the *Windows Proxy* option.

[Configuration](#) > **Discovery and Deployment**

**Discovery and Deployment**  
Configure settings related to deploying and discovering new devices.

**Windows Proxy Settings**  
In order to deploy management agents to Microsoft Windows devices, a managed device running Microsoft Windows may be needed. Specify what device should be used. This device should reside in the same network as the machines targeted for deployment. Also, specify how long the deployment processes should wait (in seconds) for responses from the Windows Proxy.  
  
Windows Proxy  
  
  
Windows Proxy Timeout  
 seconds

- 3 Fill in the following fields:

**Windows Proxy:** Click  to browse for and select the managed Windows device (server or workstation) that you want to perform discovery tasks in behalf of Linux-based ZENworks Servers.

**Windows Proxy Timeout:** Specify the number of seconds you want the ZENworks Server to wait for a response from the Windows Proxy. Any responses received after the specified timeout period are discarded.

- 4 Click *OK* to save the changes.

## 2.3 Creating an IP Discovery Task


You use the Create New Discovery Task Wizard to create and schedule the tasks used by ZENworks Servers to discover devices on your network and add them to the ZENworks database.

When a discovery task runs, the ZENworks Server creates a discovery request for each IP address and discovery technology (WMI, WinAPI, MAC Address, NMAP, ZENworks, SNMP, SSH) used. For example, if you specify one IP address and use all seven discovery technologies, the ZENworks Server initiates seven discovery requests. Therefore, the more IP addresses you specify and the more discovery processes you use, the longer the discovery task takes to complete. For fastest results, you should create tasks that target smaller ranges of IP addresses and, if possible, assign different ZENworks Servers to process the tasks.

- 1 In ZENworks Control Center, click the *Deployment* tab.
- 2 In the Discovery Tasks panel, click *New* to launch the New Discovery Task Wizard.

[Deployment](#) > **New Discovery Task Wizard**

New Discovery Task Wizard

 **Step 1: Select Discovery Type**

Select the type of discovery task you would like to create. Enter a name and an optional description for this task.

☒ IP Discovery Task  
☐ LDAP Discovery Task

Name: \*

Description:

\* Fields marked with an asterisk are required.

- 3 Complete the wizard by using information from the following table to fill in the fields.

Wizard Page	Details
Select Discovery Type page	Select <i>IP Discovery Task</i> .  Specify a name for the task. The name cannot include any of the following invalid characters: / \ * ? : " ' < >   ` % ~

Wizard Page	Details
Discovery Settings page > <i>Override Zone Discovery Settings</i> field	<p>Chose whether to override the discovery settings configured at the Management Zone.</p> <p>If you want to configure the settings on a device folder or a device, you must select <i>Override Zone Discovery Settings</i> before you can modify the settings.</p>
Discovery Settings page > <i>Discovery Technologies</i>	<p>The discovery process can utilize a variety of different technologies. When more than one technology is used, the discovery process initiates a discovery request for each technology, with all technology requests running simultaneously. This is done for each target IP address. For example, if you use MAC Address, SNMP, and WMI, the discovery process creates three requests for each target IP address. The requests are queued and run according to the <i>Maximum Concurrent Discoveries</i> setting.</p> <p>If more than one technology request returns information for a discovered device, the information is merged together. In the case of conflicting information, the discovery process chooses the “best” information.</p> <p>Using fewer discovery technologies reduces the time required to complete the discovery task but might also reduce the amount of information received.</p> <p>Following are brief descriptions of each technology:</p> <ul style="list-style-type: none"> <li>♦ <b>MAC Address:</b> Uses the <code>ping</code> and <code>arp</code> (Address Resolution Protocol) commands to map the IP addresses of the devices identified by the IP-based discovery task to their associated MAC addresses. The target devices must reside in the same network as the ZENworks Server that performs the discovery request.</li> <li>♦ <b>NMAP:</b> Uses NMAP (Network Mapper) to discover the OS type and version of the device’s identified by the IP-based discovery task. NMAP must be installed on the ZENworks Server or Windows Proxy that is processing the discovery request. NMAP is freely available from <a href="http://www.insecure.org">InSecure.org</a> (<a href="http://www.insecure.org">http://www.insecure.org</a>). For detail information on how to configure NMAP for ZENworks, see the <a href="#">Appendix B, “Configuring NMAP for ZENworks,”</a> on page 91</li> <li>♦ <b>SNMP:</b> Issues a request to the SNMP service on the devices identified by the IP-based discovery task. SNMP versions 2 and 1 are supported, with SNMP version 2 tried first. Because the discovery process uses a Windows-based SNMP technology, requests generated from a ZENworks Server running on Linux must be routed to a Windows proxy for processing. For more information, see <a href="#">Section 2.2, “Designating a Discovery and Deployment Proxy Server,”</a> on page 19.</li> <li>♦ <b>SSH:</b> Uses the SSH protocol to communicate with the SSH server on the devices identified by the IP-based discovery task. Depending on the device OS (Linux or NetWare®), the device responds with version, CPU information, and memory information.</li> </ul>

- ◆ **WinAPI:** Issues a request to the registry on the devices identified by the IP-based discovery task in an attempt to determine a device's OS type and version. Because WinAPI is a Windows-specific technology, requests generated from a ZENworks Server running on Linux must be routed to a Windows proxy for processing. For more information, see [Section 2.2, "Designating a Discovery and Deployment Proxy Server,"](#) on page 19.
- ◆ **WMI:** Issues a request to the WMI (Windows\* Management Instrumentation) service on the devices identified by the IP-based discovery task. Because WMI is a Windows-specific technology, requests generated from a ZENworks® Server running on Linux\* must be routed to a Windows proxy for processing. For more information, see [Section 2.2, "Designating a Discovery and Deployment Proxy Server,"](#) on page 19.
- ◆ **ZENworks:** Issues a request to the ZENworks pre-agent on the devices identified by the IP-based discovery task. The pre-agent responds with OS type, CPU information, disk information, memory information, and the GUID (global unique identifier) that should be used to register the device in the Management Zone.  
  
The pre-agent will only be installed on OEM devices or on devices whose registration was removed from the zone.

Enter IP Discovery Settings  
page > *Range* field

To specify a range of IP addresses for the discovery task:

1. In the *Range* field, specify an IP address range using one of the following formats:  
  
xxx.xxx.xxx.xxx: Standard dotted-decimal notation. For example, 123.45.167.100.  
  
xxx.xxx.xxx.xxx - xxx.xxx.xxx.xxx: Standard dotted-decimal notation. For example, 123.45.167.100 - 123.45.167.125.  
  
xxx.xxx.xxx.xxx/n: Standard CIDR (Classless Inter-Domain Routing) notation. With CIDR, the dotted decimal portion of the IP address is interpreted as a 32-bit binary number that has been broken into four 8-bit bytes. The number following the slash (/n) is the prefix length, which is the number of shared initial bits, counting from the left side of the address. The /n number can range from 0 to 32, with 8, 16, 24, and 32 being commonly used numbers. For example, 123.45.167.100/24 matches all IP addresses that start with 123.45.167. When you add the IP address range to the *Selected IP Ranges* list (see the next step), it is automatically expanded to show the range of addresses in dotted-decimal notation.
2. Click *Add* to add the IP address range to the *Selected IP Ranges* list.
3. Repeat Step 1 and Step 2 to add additional ranges.

Wizard Page	Details
Enter IP Discovery Settings page > <i>Save Credentials to DataStore</i> field	<p data-bbox="699 258 1411 401">In order for the SSH, WMI, WinAPI, and SSH discovery technologies to retrieve information from devices, you must provide credentials that the discovery technologies can use. The NMAP, MAC Address, and ZENworks technologies do not require credentials.</p> <p data-bbox="699 426 1411 512">Unless you save the credentials, they are stored only in memory. Saved credentials are encrypted in the database for increased security.</p> <p data-bbox="699 537 1411 651">Credentials that are not saved are cleared from memory when the ZENworks Server is restarted. If you are creating a scheduled deployment task, you might want to save the credentials to ensure that they are still available when the deployment is performed.</p>

Wizard Page	Details
Enter IP Discovery Settings page > <i>Credentials</i> field	<p>Not all technologies use the same credentials, and all devices might not have the same credentials, so you might need to specify multiple credentials to cover all targeted devices and to utilize all discovery technologies.</p> <p>To add a credential:</p> <ol style="list-style-type: none"> <li>1. In the Credentials panel, click <i>Add</i> to display the Enter Credential Information dialog box.</li> <li>2. In the <i>Type</i> field, select the type of credentials you are defining: <p><b>General:</b> Specifies credentials to be used by all discovery technologies except for SNMP.</p> <p><b>LDAP:</b> Specifies credentials to access an LDAP directory. This option does not apply to an IP-based discovery; ignore it.</p> <p><b>Linux:</b> Specifies credentials for the SSH technology to communicate with the SSH server on a Linux device.</p> <p><b>Windows:</b> Specifies credentials for the WMI and WinAPI technology to access the WMI service and Windows registry on a Windows device.</p> <p><b>SNMP:</b> Specifies community strings for the SNMP technology to access the SNMP service on a device. By default, the discovery process uses <code>public</code> as the community string.</p> </li> <li>3. If you selected <i>General</i>, <i>Linux</i>, or <i>Windows</i>, fill in the username and password. <p>You can enter the username for Windows devices in of the following formats:</p> <pre>username domain_name\username username@domain_name username@fully_qualified_domain_name</pre> </li> <li>4. If you selected <i>SNMP</i>, fill in a community string.</li> <li>5. Click <i>OK</i> to add the credentials to the Credentials panel.</li> <li>6. Repeat Step 1 through Step 5 to add additional credentials.</li> </ol> <p>If you add multiple credentials of the same type (for example, multiple Windows credentials), the technologies that require those credentials use them in the order they are displayed in the Credentials panel, moving from top to bottom. Therefore, you should make sure that you place the most common credentials first in order to speed up the discovery process.</p>

Wizard Page	Details
Set the Discovery Schedule page	<p>Choose whether you want the task to run as soon as it is created (the <i>Now</i> option) or if you want to schedule the task to run at a future date and time. If you select <i>On a Schedule</i>, choose one of the following schedules:</p> <p><b>No Schedule:</b> Indicates that no schedule has been set. The task does not run until a schedule is set or it is manually launched. This is useful if you want to create the task and come back to it later to establish the schedule or run it manually.</p> <p><b>Date Specific:</b> Specifies one or more dates on which to run the task.</p> <p><b>Recurring:</b> Identifies specific days each week, month, or a fixed interval on which to run the task.</p> <p>See <a href="#">Appendix A, "Schedules," on page 87</a> or click the <i>Help</i> button for more detailed information about the schedules.</p>
Select Primary Server page > <i>Primary Server</i> field	<p>Select the ZENworks Server that you want to perform the discovery task.</p> <p>If you are using any Windows-specific discovery technologies (WMI, WinAPI), you must select a ZENworks Server on Windows (not Linux) or you must have already designated a Windows ZENworks Server as a discovery proxy for your Linux servers. For information about discovery proxies, see <a href="#">Section 2.2, "Designating a Discovery and Deployment Proxy Server," on page 19</a>.</p>
<p>When you finish the wizard, the discovery task is added to the list in the Discovery Tasks panel. You can use the panel to monitor the status of the task. As devices are discovered, they are listed in the Deployable Devices panel.</p>	

# Discovering Devices in LDAP Directories

# 3

You can search an LDAP directory for devices to add to your ZENworks® database. The directory can be one that is already defined as a user source in your Management Zone, or it can be a new directory.

You can search all of the directory from the root context. Or, you can limit the search by specifying one or more contexts to search. Device objects that are found are queried for well-known attributes (dnsHostName, OperatingSystem, wmNameDNS, wmNameOS, and so forth) to attempt to determine the OS version and DNS name of the device.

Before performing an LDAP discovery, make sure the following prerequisites are satisfied:

- ♦ An LDAP search requires the ZENworks Server to provide credentials that give read access to the contexts being searched. When accessing Novell® eDirectory™, the account also requires read rights to the WM:NAME DNS attributes on the workstation and server objects.
- ♦ An LDAP search of Active Directory requires the ZENworks Server to use a DNS server to resolve the device's DNS name (as recorded on the object's DNS name attribute in Active Directory) to its IP address. Otherwise, the device is not added as a discovered device.

You use the Create New Discovery Task Wizard to create and schedule an LDAP discovery task:

- 1 In ZENworks Control Center, click the *Deployment* tab.
- 2 In the Discovery Task panel, click *New* to launch the New Discovery Task Wizard.
- 3 Complete the wizard by using information from the following table to fill in the fields.

Wizard Page	Details
Select Discovery Type page	Select <i>LDAP Discovery Task</i> .  Specify a name for the task. The name cannot include any of the following invalid characters: / \ * ? : " ' < >   ` % ~

Wizard Page	Details
Enter LDAP Settings page > <i>Search pre-configured LDAP source</i> field	<p>The Enter LDAP Settings page lets you identify the LDAP directory and contexts where you want to perform the discovery task.</p> <p>A preconfigured LDAP source is one that has already been defined as a user source in your Management Zone. If you want to select a new source, see <a href="#">Enter LDAP Settings page &gt; Specify an LDAP Source field</a> below.</p> <p>To use a preconfigured source:</p> <ol style="list-style-type: none"> <li>1. Select <i>Search pre-configured LDAP source</i>, then select the desired source.</li> <li>2. If you don't want to search the entire LDAP directory, you can identify specific search contexts/groups. To do so: <ol style="list-style-type: none"> <li>a. In the LDAP Search Contexts/Groups panel, click <i>Add</i> to display the <i>Enter Context or Group Information</i> dialog box.</li> <li>b. Fill in the following fields: <p><b>Context/Group DN:</b> Click <i>Browse</i> to locate and select the context/group you want to search.</p> <p><b>Recursive Search:</b> Select this option to search all subcontexts/subgroups.</p> </li> <li>c. Click <i>OK</i> to save the search context/group.</li> </ol> </li> <li>3. If necessary, modify the LDAP search filter.</li> </ol> <p>By default, the filter searches for the computer objectClass or server objectClass. When modifying the filter, you can use the standard filter syntax for your LDAP directory.</p>

Enter LDAP Settings page >  
Specify an LDAP Source field

You can create a new connection to a LDAP directory in order to discover devices in the directory. If you want to use an existing connection, see [Enter LDAP Settings page > Search pre-configured LDAP source field](#) above.

To create a new connection to an LDAP directory:

1. Select *Specify an LDAP source*, then fill in the following fields:

**LDAP Server:** Specify the IP address or DNS hostname of the server where the LDAP directory resides.

**LDAP Port/Use SSL:** Defaults to the standard SSL port (636) or non-SSL port (389) depending on whether the *Use SSL* option is enabled or disabled. If your LDAP server is listening on a different port, select that port number.

**Root Context:** Establishes the entry point in the directory; nothing located above the entry point is available for searching. Specifying a root context is optional. If you don't specify a root context, the directory's root container becomes the entry point.

**Save Credentials to Datastore:** Unless you save the credentials (defined in the *Credentials* list), they are stored only in memory. Saved credentials are encrypted in the database for increased security. Credentials are cleared from memory when the ZENworks Server is restarted. If you want to permanently retain the credentials, you should save them.

**Credentials:** Click *Add* to specify a username and password that provides read-only access to the directory. The user can have more than read-only access, but read-only access is all that is required and recommended. When accessing Novell eDirectory, the user account also requires read rights to the WM:NAME DNS attributes on the workstation and server objects.

For Novell eDirectory™ access, use standard LDAP notation. For example,

`cn=admin_read_only,ou=users,o=mycompany`

For Microsoft Active Directory, use standard domain notation. For example, `AdminReadOnly@mycompany.com`

2. If you don't want to search the entire LDAP directory, you can identify specific search contexts/groups. To do so:
  - a. In the LDAP Search Contexts/Groups panel, click *Add* to display the *Enter Context or Group Information* dialog box.
  - b. Fill in the following fields:
 

**Context/Group DN:** Click *Browse* to locate and select the context/group you want to search.

**Recursive Search:** Select this option to search all subcontexts/subgroups.
  - c. Click *OK* to save the search context/group.
3. If necessary, modify the LDAP search filter. By default, the filter searches for the computer objectClass or server objectClass.

Wizard Page	Details
Set the Discovery Schedule page	<p>Choose whether you want the task to run as soon as it is created (the <i>Now</i> option) or if you want to schedule the task to run at a future date and time. If you select <i>Scheduled</i>, choose one of the following schedules:</p> <p><b>No Schedule:</b> Indicates that no schedule has been set. The task does not run until a schedule is set or it is manually launched. This is useful if you want to create the task and come back to it later to establish the schedule or run it manually.</p> <p><b>Date Specific:</b> Specifies one or more dates on which to run the task.</p> <p><b>Recurring:</b> Identifies specific days each week, month, or a fixed interval on which to run the task.</p> <p>Click the <i>Help</i> button for more detailed information about the schedules.</p>
Select Primary Server page	Select the ZENworks Server that you want to perform the deployment task.

When you finish the wizard, the discovery task is added to the list in the Discovery Tasks panel. You can use the panel to monitor the status of the task. As devices are discovered, they are listed in the Deployable Devices panel.

# Importing Devices from CSV Files

# 4


You can add devices to the ZENworks database by importing their information from a CSV (comma-separated values) file. When you import information from a CSV file, you map the CSV fields to ZENworks® database fields. At a minimum, the CSV file must contain the DNS name or IP address for each device you want to import.

To import devices from a CSV file:

- 1 In ZENworks Control Center, click the *Deployment* tab.
- 2 In the *Deployment Activities* list in the left navigation panel, click *Import Deployable Devices* to launch the Import Devices from CSV File Wizard.

[Deployment](#) > **New Discovery Task Wizard**

**Import Devices from CSV file**

 **Step 1: Select file to import**

Select a comma separated value file that contains information about the devices you want to import

CSV file

Browse...

- 3 Complete the wizard by using information from the following table to fill in the fields.

Wizard Page	Details
Select File to Import page	Browse for and select the CSV file that contains the devices you want to import. At a minimum, the CSV file must contain the DNS name or IP address for each device you want to import.

Wizard Page	Details
Configure Import	<p data-bbox="699 258 1398 369">Map the columns in the CSV file to the device fields in the ZENworks database. At a minimum, you must map the CSV file's DNS name or IP address to the ZENworks database's DNS Name field or IP Address field.</p> <p data-bbox="699 396 1078 420">To create the information mappings:</p> <ol data-bbox="721 438 1386 852" style="list-style-type: none"> <li data-bbox="721 438 1386 462">1. Click <i>Add</i> to display the Specify Import Columns dialog box.</li> <li data-bbox="721 480 1386 573">2. Fill in the following fields:  <b>Field:</b> Select the device field you want to map to a column in the CSV file.  <b>Column:</b> Specify the number of the column to map to the selected field.</li> <li data-bbox="721 663 1386 714">3. Click <i>OK</i> to create the information mapping and add it to the list.</li> <li data-bbox="721 732 1386 783">4. To verify that the field is mapped to the correct column, click <i>Show Sample</i>.</li> <li data-bbox="721 802 1386 852">5. Repeat the above steps to create and verify additional information mappings.</li> </ol>

When you finish the wizard, the devices are added to the list in the Deployable Devices panel.

# ZENworks Adaptive Agent Deployment



The following sections provide information and instructions to help you deploy the ZENworks<sup>®</sup> Adaptive Agent to devices so that you can manage them through ZENworks Configuration Management.

- ♦ Chapter 5, “Basic Concepts,” on page 35
- ♦ Chapter 6, “Managing Deployment Packages,” on page 39
- ♦ Chapter 7, “Registering Devices,” on page 45
- ♦ Chapter 8, “Deploying the ZENworks Adaptive Agent,” on page 61
- ♦ Chapter 9, “Deploying the Inventory-Only Module,” on page 81



Deployment is the process of installing the ZENworks® Adaptive Agent on devices and registering them within your Management Zone. The following sections provide information to help you understand the deployment terminology and concepts:

- ♦ [Section 5.1, “Deployment Methods,” on page 35](#)
- ♦ [Section 5.2, “Deployment Packages,” on page 35](#)
- ♦ [Section 5.3, “Adaptive Agent Versus Inventory-Only Module,” on page 36](#)

## 5.1 Deployment Methods

There are several deployment methods you can use:

- ♦ **Deployment task:** The ZENworks Server can deliver the ZENworks Adaptive Agent to devices and initiate the installation of the agent. This requires that you create a task, called a deployment task, for the ZENworks Server. The task identifies the target devices, the credentials required to perform an installation on the devices, the registration key to use (optional), and other tasks you want performed on the devices either before or after the installation. You can have a ZENworks Server immediately perform the task, or you can schedule the task for a specific date and time.
- ♦ **Manual deployment:** You can manually download the ZENworks Adaptive Agent deployment package from a ZENworks Server to a device and initiate the installation.
- ♦ **Automated deployment:** You can automate deployment by using any method that can launch the Adaptive Agent deployment package. For example, you can use a login script, or, if you have a previous version of ZENworks, you can distribute the Adaptive Agent deployment package as an Application object through Novell® Application Launcher™.

Installation instructions are provided in [Chapter 8, “Deploying the ZENworks Adaptive Agent,” on page 61](#).

## 5.2 Deployment Packages

Deployment packages contain the files and information needed to install the ZENworks Adaptive Agent on devices and register the devices in the Management Zone. There are 12 default system packages that are included on each ZENworks Server. These packages provide for local or network installation of the Adaptive Agent (full agent or partial agent) on various operating system architectures (32-bit and 64-bit).

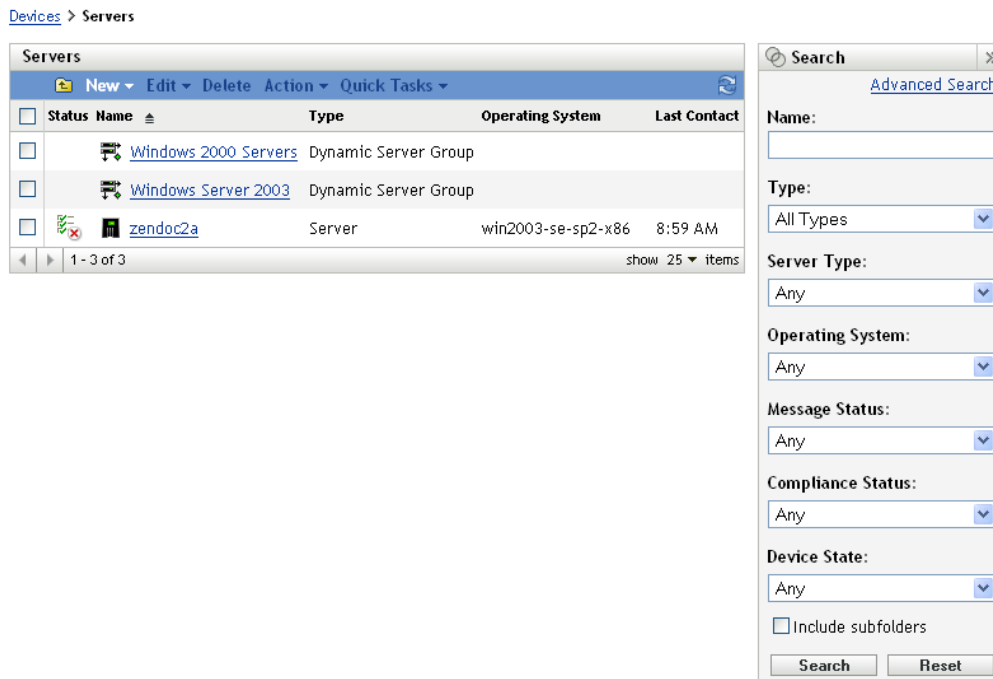
If necessary, you can modify a deployment package to change the ZENworks Server address or registration key included in the package. For example, assume that you want to use the same package to deploy the agent to devices on your private network and to devices on the other side of a firewall or router that is using NAT (Network Address Translation). You could modify a package in order to list the ZENworks Server’s private network address (IP address, DNS name, or both) and also list its NAT address.

For more information about deployment packages and how to use them, see [Chapter 6, “Managing Deployment Packages,” on page 39](#).

## 5.3 Adaptive Agent Versus Inventory-Only Module

The ZENworks Adaptive Agent supports Windows 2000, XP, 2003, and Vista devices. You can fully manage devices on which the Adaptive Agent is deployed. This includes distributing software, enforcing policies, remotely managing the device, and so forth. The ZENworks Control Center displays managed devices on the Device page's Managed tab.

**Figure 5-1** *Managed Devices page > Servers folder*



Deployment instructions for the Adaptive Agent are provided in [Chapter 8, “Deploying the ZENworks Adaptive Agent,”](#) on page 61.

If a Windows device does not meet the requirements for deploying the Adaptive Agent (see “[Minimum Requirements](#)” in the *ZENworks 10 Configuration Management Installation Guide* for details), or if you want to inventory a Linux, NetWare®, or Macintosh\* device, you can deploy the Inventory-Only module.



After you deploy the module, the device is added to the ZENworks database. The ZENworks Control Center displays inventoried-only devices on the Device page's *Inventoried* tab.

**Figure 5-2** *Inventoried Devices page > Workstations folder*

[Inventoried Devices](#) > Workstations

Workstations

New Edit Delete

<input type="checkbox"/>	Name	Operating System	Type
<input type="checkbox"/>	 <a href="#">ZENDOCWKS2</a>	winxp-pro-sp2-x86	Workstation
<input type="checkbox"/>	 <a href="#">ZENDOCWKS3</a>	winxp-pro-sp2-x86	Workstation

1 - 2 of 2

show 10 items

Search

Name:

Type:  
All Types

Operating System:  
Any

☐ Include subfolders

Search Reset

Deployment instructions for the Inventory-Only module are provided in [Chapter 9, “Deploying the Inventory-Only Module,”](#) on page 81.



# Managing Deployment Packages

# 6

Deployment packages contain the files and information needed to install the ZENworks® Adaptive Agent on devices and register the devices in the Management Zone.

Each ZENworks Server contains 12 default system packages. These packages are built during installation of the ZENworks Server. In addition to the Adaptive Agent files, each default system package includes the ZENworks Server's address and (optionally) a key to use when registering. You cannot change which files a default system package includes, but you can customize the ZENworks Server address and registration key (which is blank unless you specify one).

For example, assume that you are deploying the Adaptive Agent to devices on your private network and to devices on the other side of a firewall or router that is using NAT (Network Address Translation). You could modify a package in order to list the ZENworks Server's private network address (IP address, DNS name, or both) and also list its NAT address.

The following sections provide information and instructions to help you manage your deployment packages:

- ♦ [Section 6.1, “Package Types and Architectures,” on page 39](#)
- ♦ [Section 6.2, “Default System Packages Versus Custom Packages,” on page 40](#)
- ♦ [Section 6.3, “Packages without the Remote Management Module,” on page 40](#)
- ♦ [Section 6.4, “Customizing a Package,” on page 41](#)
- ♦ [Section 6.5, “Enabling the No Remote Management Packages,” on page 43](#)

## 6.1 Package Types and Architectures

In order to support deployment of the ZENworks Adaptive Agent from files on either local or network media, there are two types of deployment packages:

- ♦ **Network:** A network package contains only the preagent. After the preagent is installed to the device, it downloads and installs the ZENworks Adaptive Agent from a ZENworks Server. There are two network packages:
  - ♦ `PreAgentPkg_Agent.exe`: Includes all Adaptive Agent modules (Bundles, Policies, Inventory, Remote Management, and Content Distribution Point).
  - ♦ `PreAgentPkg_AgentNoRM.exe`: Includes all Adaptive Agent modules except the Remote Management module.

A network package requires that Microsoft .NET is installed on a device prior to the deployment of the agent to the device.

- ♦ **Standalone:** A standalone package contains the preagent and the ZENworks Adaptive Agent files. Because this package does not require access to the ZENworks Server to install the Adaptive Agent, you can distribute it via removable media (CD, USB drive, etc.) to devices that don't have network access to a ZENworks Server. After the Adaptive Agent is installed, it registers with the Management Zone the next time it has access to the ZENworks Server. There are two standalone packages:
  - ♦ `PreAgentPkg_AgentComplete.exe`: Includes all Adaptive Agent modules (Bundles, Policies, Inventory, Remote Management, and Content Distribution Point).

- ◆ `PreAgentPkg_AgentCompleteNoRM.exe`: Includes all Adaptive Agent modules except the Remote Management module.

In order provide support for the various Windows operating system architectures, there are three versions of each of the four packages:

- ◆ **x86 version:** You can use the x86 version for manual deployments to 32-bit Windows devices. The only time this package is used is if you do a manual deployment; it is not used by the ZENworks Server when completing a deployment task.

The x86 packages (`PreAgentPkg_Agent.exe`, `PreAgentPkg_AgentNoRM.exe`, `PreAgentPkg_AgentComplete.exe`, and `PreAgentPkg_CompleteNoRM.exe`) are located in the following ZENworks Server directory:

```
..\novell\zenworks\install\downloads\setup\x86
```

- ◆ **x86\_64 version:** You can use the x86\_64 version for manual deployments to 64-bit Windows devices. The only time this package is used is if you do a manual deployment; it is not used by the ZENworks Server when completing a deployment task.

The x86\_64 packages (`PreAgentPkg_Agent.exe`, `PreAgentPkg_AgentNoRM.exe`, `PreAgentPkg_AgentComplete.exe`, and `PreAgentPkg_CompleteNoRM.exe`) are located in the following ZENworks Server directory:

```
..\novell\zenworks\install\downloads\setup\x86_64
```

- ◆ **All Architectures version:** This package is used by the ZENworks Server when completing a deployment task. It contains files for both 32-bit and 64-bit Windows devices.

The All Architectures packages (`PreAgentPkg_Agent.exe`, `PreAgentPkg_AgentNoRM.exe`, `PreAgentPkg_AgentComplete.exe`, and `PreAgentPkg_CompleteNoRM.exe`) are located in the following ZENworks Server directory:

```
..\novell\zenworks\install\downloads\setup\_all
```

## 6.2 Default System Packages Versus Custom Packages

You can customize any of the default system packages to change the package or to create a new custom package. When you do so, you can modify the ZENworks Server address and registration key; you cannot modify, add, or remove the Adaptive Agent files.

As mentioned in [Section 6.2, “Default System Packages Versus Custom Packages,”](#) on page 40, only the All Architectures packages are used by the ZENworks Server when completing a deployment task. Therefore, any custom packages you create, or any modifications you make to the x86 or x86\_64 system packages, are used only during manual deployments of the Adaptive Agent.

## 6.3 Packages without the Remote Management Module

By default, the packages that include the Remote Management module (`PreAgentPkg_Agent.exe` and `PreAgentPkg_AgentComplete.exe`) are used when installing the agent through a deployment task.

If you want deployment tasks to use the packages that don't include the Remote Management module (PreAgentPkg\_AgentNoRM.exe and PreAgentPkg\_AgentCompleteNoRM.exe), you must change the Remote Management Module option in the ZENworks Agent zone configuration setting from *Enabled* (the default) to *Uninstalled*.


For help changing the Remote Management Module option, see [Section 6.5, “Enabling the No Remote Management Packages,” on page 43](#).

## 6.4 Customizing a Package

- 1 In ZENworks Control Center, click the *Deployment* tab.
- 2 Click *Edit Deployment Package* (located in *Deployment Activities* list in the left navigation pane) to launch the Edit Deployment Package Wizard.

[Deployment](#) > **Deployment Package Editor**

**Edit Deployment Package**

 **Step 1: Select Deployment Package to edit**

First select the target operating system, architecture, and installation type of the package you wish to edit. Then select the package name.

Target Operating System	Microsoft Windows ▼
Target Architecture	All Supported Architectures ▼
Package Install Type	Network installation ▼
Package Name	System ▼

- 3 Complete the wizard by using information from the following table to fill in the fields.

Wizard Page	Details
Select Deployment Package to Edit page	<p>In the <i>Target Architecture</i> list, select the architecture of the package you want to edit.</p> <ul style="list-style-type: none"> <li>♦ <b>x86 Architecture (32 bit):</b> Used in manual deployments of the agent to 32-bit devices.</li> <li>♦ <b>x86_64 Architecture (64 bit):</b> Used in manual deployments of the agent to 64-bit devices.</li> <li>♦ <b>All Supported Architectures:</b> Used by the ZENworks Server to complete deployment tasks for either 32-bit or 64-bit devices.</li> </ul> <p>In the <i>Package Install Type</i> list, select the installation type of the package you want to edit.</p> <ul style="list-style-type: none"> <li>♦ <b>Network Installation:</b> Contains only the preagent. The preagent downloads the Adaptive Agent files from a ZENworks Server.</li> <li>♦ <b>Standalone Installation:</b> Contains the preagent and all of the Adaptive Agent files.</li> </ul> <p>In the <i>Package Name</i> list, select the name of the package you want to edit.</p> <p>The names in the list are determined by the architecture and installation type you previously selected. The list displays the names of any packages with the selected architecture and installation type.</p> <p>By default, the system package is always displayed. The system package is the predefined deployment package (<code>PreAgentPkg_Agent.exe</code>, <code>PreAgentPkg_AgentNoRM.exe</code>, <code>PreAgentPkg_AgentComplete.exe</code>, or <code>PreAgentPkg_AgentCompleteNoRm.exe</code>) that meets the architecture and installation type criteria you specified.</p> <p>Other package names are displayed only if you have previously edited the system package and saved the customized version as a new package.</p>
Provide Primary Server Information page	<p>Specify the addresses that can be used to access the ZENworks Server. A device needs to access the ZENworks Server when the deployment is a network installation (the preagent must download the ZENworks Adaptive Agent files from the ZENworks Server) and when it registers as a managed device. All addresses you specify must belong to the same ZENworks Server.</p> <p>For example, assume that you are deploying the Adaptive Agent to devices on your private network and to devices on the other side of a firewall or router that is using NAT (Network Address Translation). You would list the ZENworks Server's private network address (IP address, DNS name, or both) and also list its NAT address.</p>

Wizard Page	Details
Add Registration Key page	<p>Select a registration key to use during the registration portion of the deployment process. A registration key provides information about the folders and groups to which a device is assigned during registration.</p> <p>Selecting a registration key is optional; if you don't select one, registration rules are used to determine the folder and group assignments. To deploy to servers or workstations, choose a server registration key or a workstation registration key respectively.</p> <p>For more information about registration keys and rules, see <a href="#">Chapter 7, "Registering Devices," on page 45</a>.</p>
Select Destination for the New Deployment Package page	<p>Select whether you want to overwrite the existing package or save the edited package as a custom package. The two options are:</p> <p><b>Overwrite Original Deployment Package:</b> Replace the original package with this edited package.</p> <p><b>Select a Name for the New Deployment Package</b> Saves the edited package as a new custom package. The original package remains unchanged.</p> <p>You can specify any name you want for the new custom package. In actuality, the package name remains the same (PreAgentPkg_Agent.exe, PreAgentPkg_AgentNoRM.exe, PreAgentPkg_AgentComplete.exe, or PreAgentPkg_AgentCompleteNoRM.exe) and the directory used to store the package is given the name you specify.</p> <p>All new packages are saved in the ZENworks Server's \Novell\ZENworks\install\downloads\custom directory. For example, if you modify the x86 version of the PreAgentPkg_Agent.exe package and save it with a name of ExternalPack, the file is stored as follows:</p> <pre>\Novell\ZENworks\install\downloads\custom\ExternalPack\x86\PreAgentPkg_Agent.exe</pre>

## 6.5 Enabling the No Remote Management Packages

By default, the packages that include the Remote Management module (PreAgentPkg\_Agent.exe and PreAgentPkg\_AgentComplete.exe) are used when installing the agent through a deployment task.

If you want deployment tasks to use the packages that don't include the Remote Management module (PreAgentPkg\_AgentNoRM.exe and PreAgentPkg\_AgentCompleteNoRM.exe), you must change the Remote Management Module option in the ZENworks Agent zone configuration setting from *Enabled* (the default) to *Uninstalled*.

To change the setting:

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

Configuration	Registration	System Information	Asset Inventory	System Updates	Asset Management
Management Zone Settings					⌵
Content					⌵
Device Management					⌵
Category	Description	Is Configured			
<a href="#">Local Device Logging</a>	Enable and configure local logging of warnings and errors encountered by managed devices.	Yes			
<a href="#">Device Refresh Schedule</a>	Configure the device refresh interval.	Yes			
<a href="#">ZENworks Agent</a>	ZENworks Agent Configuration.	No			
<a href="#">Registration</a>	Configure registration settings.	Yes			
<a href="#">Remote Management</a>	Enable and configure remote management.	Yes			
<a href="#">Preboot Services</a>	Configure Preboot Services.	Yes			
<a href="#">Primary User</a>	Configure the setting for how the primary user is determined.	No			
<a href="#">Dynamic Group Refresh Schedule</a>	Configure dynamic group refresh schedule.	No			
Discovery and Deployment					⌵
Event and Messaging					⌵
Infrastructure Management					⌵
Inventory					⌵
Reporting Services					⌵
Asset Management					⌵
Patch Management Services					⌵

- 2 In the Management Zone Settings panel, click *Device Management*, then click *ZENworks Agent*.

[Configuration](#) > **ZENworks Agent**

**ZENworks Agent**

ZENworks Agent Configuration.

**General**

☒ Allow users to uninstall agent

Cache hours to live: 336

Cache orphaning days threshold: 30

**Enable/Disable Agents**

Remote Management Agent: ☒ Enabled ☐ Uninstalled

- 3 In the Enable/Disable Agents panel, click *Uninstalled*.
- 4 Click *OK* to save the change.

# Registering Devices

# 7

When you install the ZENworks® Adaptive Agent to a device, the device is registered in your Management Zone and becomes a managed device. The following sections provide information to help you understand and manage the registration process:

- ♦ [Section 7.1, “What Happens During Registration,” on page 45](#)
- ♦ [Section 7.2, “Creating Registration Keys and Rules,” on page 46](#)
- ♦ [Section 7.3, “Modifying the Device Naming Template Used During Registration,” on page 53](#)
- ♦ [Section 7.4, “Enabling Dynamic Renaming of Devices During Registration,” on page 54](#)
- ♦ [Section 7.5, “Disabling the Use of Registration Rules,” on page 57](#)
- ♦ [Section 7.6, “Manually Registering a Device,” on page 58](#)
- ♦ [Section 7.7, “Unregistering a Device,” on page 59](#)

## 7.1 What Happens During Registration

The ZENworks Adaptive Agent includes a service that performs all registration tasks. The tasks performed by the Registration service depend on whether the device is registering for the first time, performing a scheduled refresh, or reregistering with a new registration key. The following table lists the tasks performed in each scenario.

**Table 7-1** *Registration tasks*

Task	Initial Registration	Refresh	Reregistration <sup>1</sup>
Create device object in ZENworks database	Yes	No	No
Name device object according to device naming template	Yes	Yes <sup>2</sup>	Yes <sup>2</sup>
Add device to folder	Yes	No	No
Add device to groups <sup>3</sup>	Yes	No	Yes
Add site, department, and location information <sup>3</sup>	Yes	No	Yes
Update device attributes (GUID, IP address, DNS name, last contact time, etc.)	Yes	Yes	Yes

<sup>1</sup> Reregistration assumes that the device object has not been removed from the ZENworks database and that the device is simply being reregistered using a new registration key.

<sup>2</sup> Occurs only if the *Device Dynamic Rename* option is enabled. See [Section 7.4, “Enabling Dynamic Renaming of Devices During Registration,” on page 54](#) for more information.

<sup>3</sup> Occurs only if the key or rule being used for registration includes this information. See [Section 7.2, “Creating Registration Keys and Rules,” on page 46](#) for more information.

## 7.2 Creating Registration Keys and Rules

The first time a device registers, it is added to a folder. By default, it is added to either the `/Servers` folder or the `/Workstations` folder, depending on the device type.

You can use registration keys and registration rules to override the default folder assignment and specify another folder, and to assign the device to groups. Although you can manually move a device to another folder and add it to groups after the device registers, this can become burdensome 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 use registration keys and rules to automatically add them to the correct folders and groups during registration.

- ♦ **Registration key:** 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.
- ♦ **Registration rule:** A registration rule is a set of predefined criteria (for example, operating system type, CPU, or IP address) that you define. If the device meets the criteria, the rule is used for registration. You can create multiple rules; all rules are checked before the default folder is used. Registration rules are applied only if a registration key is not used.

The following sections provide instructions for creating registration keys and rules:

- ♦ [Section 7.2.1, “Creating a Registration Key,” on page 46](#)
- ♦ [Section 7.2.2, “Creating a Registration Rule,” on page 49](#)

### 7.2.1 Creating a Registration Key

The steps in this section explain how to create a registration key. After you’ve created a key, you can use the key in the following ways:

- ♦ Include the key in a deployment task so that it is used during installation of the ZENworks Adaptive Agent. See [Chapter 8.2, “Using a Task to Deploy the Agent,” on page 61](#).
- ♦ Add the key to a deployment package so that when the package is used in either a deployment task or a manual installation, the registration key is applied. See [Chapter 6, “Managing Deployment Packages,” on page 39](#).
- ♦ Use the key with the ZENworks Adaptive Agent command line utility (`zac`) to initially register a device within a zone (`zac register` command), or to manually reregister the device with an additional key (`zac add-reg-key` command). See [Section 7.6, “Manually Registering a Device,” on page 58](#).

To create a registration key:

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

Configuration	Registration	System Information	Asset Inventory	System Updates	Asset Management								
<div> <div>Registration Keys</div> <div> <div>New</div> <div>Edit</div> <div>Delete</div> </div> <div>Folder: /Keys</div> <table border="1"> <thead> <tr> <th><input type="checkbox"/> Registration Code</th> <th>Usage Limit</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> <a href="#">darrin</a></td> <td>(unlimited)</td> </tr> <tr> <td><input type="checkbox"/> <a href="#">darrin2</a></td> <td>(unlimited)</td> </tr> <tr> <td><input type="checkbox"/> <a href="#">test</a></td> <td>(unlimited)</td> </tr> </tbody> </table> <div> <div>1 - 3 of 3</div> <div>show 5 items</div> </div> </div>						<input type="checkbox"/> Registration Code	Usage Limit	<input type="checkbox"/> <a href="#">darrin</a>	(unlimited)	<input type="checkbox"/> <a href="#">darrin2</a>	(unlimited)	<input type="checkbox"/> <a href="#">test</a>	(unlimited)
<input type="checkbox"/> Registration Code	Usage Limit												
<input type="checkbox"/> <a href="#">darrin</a>	(unlimited)												
<input type="checkbox"/> <a href="#">darrin2</a>	(unlimited)												
<input type="checkbox"/> <a href="#">test</a>	(unlimited)												
<div> <div>Registration Rules</div> <div> <div>New</div> <div>Delete</div> </div> <div> <div><input type="checkbox"/> Name</div> <div><input type="checkbox"/> <a href="#">test</a></div> <div><input type="checkbox"/> <a href="#">testasdasd</a></div> </div> <div> <div>1 - 2 of 2</div> <div>show 5 items</div> </div> </div>													

- In the Registration Keys panel, click *New > Registration Key* to launch the Create New Registration Key Wizard.

[Registration Keys](#) > **Create New Registration Key**

Create New Registration Key

**Step 1: Basic Information**

Supply the name, description, and the limit for the new registration key. A unique name can be generated by clicking on the "Generate unique key name" icon.

Name (used as the registration key code):

Folder: \*


Description:

Number of times this key can be used:

☒ Unlimited
 ☐ Limit to:

- Complete the wizard by using information from the following table to fill in the fields.

Wizard Page	Details
Basic Information page	<p>Define the registration key's name and folder location, add information to describe the key, and specify the number of times the key can be used.</p> <p><b>Name:</b> Provide a name for the registration key. Any device that presents this name is given the assignments associated with this registration key.</p> <p>Choose something simple for reduced security, or click <i>Generate</i> to generate a complex registration string that is difficult to guess. Use the <i>Generate</i> option along with a registration key limit for increased security. If you manually enter a name, the name must be different than any other registration key names and must not use any of the following invalid characters: / \ * ? : " ' &lt; &gt;   ` % ~.</p> <p><b>Folder:</b> Specify the folder for this registration key. This is for organizational purposes only. Devices do not need to know where a registration key is located in order to use it to register, they simply need to know the key name.</p> <p><b>Description:</b> Use this field to provide information about the new registration key. This is for your benefit. This field appears only in ZENworks Control Center.</p> <p><b>Number of Times This Key Can Be Used:</b> For security purposes, this enables you to limit the number of devices that can register by using this key.</p>
Containment Rules page	<p>Specify the folder in which to place the devices.</p> <p>As a general rule, devices with similar configuration settings (refresh intervals, logging settings, remote management settings, and so forth) should be grouped in the same folder so that you can specify the configuration settings on the folder and have the devices in the folder inherit them. You should not use the same folder for devices that require different configuration settings; doing so prohibits you from using the folder to define the settings and forces you to define them on each individual device.</p>
Device Fields	<p>Specify the department, site, and location information you want entered on a device's details page when it registers. For example, if you enter <i>Accounting</i> in the <i>Department</i> field, then <i>Accounting</i> is entered in the <i>Department</i> field on the device's details page.</p>

Wizard Page	Details
Group Membership page	<p>Specify the groups that devices will become members of when they register.</p> <p>Adding groups causes registering devices to receive any assignments provided by membership in the groups. Assignments from group membership are additive, so if a device is assigned to both groups A and B, the device receives all assignments from both groups.</p> <p>You can only add groups that are valid for the type of device folder you specified on the previous page of the wizard. For example, if you specified the <code>/Devices/Workstations</code> folder, you can only choose workstation groups.</p> <p>To specify a group:</p> <ol style="list-style-type: none"> <li>1. Click <i>Add</i> to display the Groups dialog box.</li> <li>2. Browse for and select the group (or groups) to which you want to add the devices. To do so: <ol style="list-style-type: none"> <li>a. Click  next to a folder (for example, the <code>Workstations</code> folder or <code>Servers</code> folder) to navigate through the folders until you find the group you want to select.</li> <li>or</li> <li>Search for the group by entering its name in the <i>Item name</i> box. You can use an asterisk (*) as a wildcard. For example, entering <code>P*</code> finds all groups that start with P, or entering <code>*Accounting</code> finds all groups that end with Accounting.</li> <li>b. Click the underlined link in the <i>Name</i> column to select the group and display its name in the <i>Selected</i> list box.</li> <li>c. Repeat steps 2a and 2b until you've selected all groups to which you want to assign membership.</li> <li>d. Click <i>OK</i> to add the selected groups to the list.</li> </ol> </li> </ol>

When you complete the wizard, the key is added to the Registration Keys panel.

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 10 Configuration Management Command Line Utilities Reference*.

## 7.2.2 Creating a Registration Rule

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

Configuration	Registration	System Information	Asset Inventory	System Updates	Asset Management												
<div> <b>Registration Keys</b> <span>⌵</span> </div> <div> <span>New</span> <span>Edit</span> <span>Delete</span> </div> <div> <b>Folder:</b> / Keys         </div> <table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>Registration Code</th> <th>Usage Limit</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td> <a href="#">darrin</a></td> <td>(unlimited)</td> </tr> <tr> <td><input type="checkbox"/></td> <td> <a href="#">darrin2</a></td> <td>(unlimited)</td> </tr> <tr> <td><input type="checkbox"/></td> <td> <a href="#">test</a></td> <td>(unlimited)</td> </tr> </tbody> </table> <div> <span>⏪</span> <span>1 - 3 of 3</span> <span>show 5 items</span> </div>						<input type="checkbox"/>	Registration Code	Usage Limit	<input type="checkbox"/>	<a href="#">darrin</a>	(unlimited)	<input type="checkbox"/>	<a href="#">darrin2</a>	(unlimited)	<input type="checkbox"/>	<a href="#">test</a>	(unlimited)
<input type="checkbox"/>	Registration Code	Usage Limit															
<input type="checkbox"/>	<a href="#">darrin</a>	(unlimited)															
<input type="checkbox"/>	<a href="#">darrin2</a>	(unlimited)															
<input type="checkbox"/>	<a href="#">test</a>	(unlimited)															
<div> <b>Registration Rules</b> <span>Advanced</span> <span>⌵</span> </div> <div> <span>New</span> <span>Delete</span> </div> <table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>Name</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td> <a href="#">test</a></td> </tr> <tr> <td><input type="checkbox"/></td> <td> <a href="#">testasdasd</a></td> </tr> </tbody> </table> <div> <span>⏪</span> <span>1 - 2 of 2</span> <span>show 5 items</span> </div>						<input type="checkbox"/>	Name	<input type="checkbox"/>	<a href="#">test</a>	<input type="checkbox"/>	<a href="#">testasdasd</a>						
<input type="checkbox"/>	Name																
<input type="checkbox"/>	<a href="#">test</a>																
<input type="checkbox"/>	<a href="#">testasdasd</a>																

2 In the Registration Rules panel, click *New* to launch the Create New Registration Rule Wizard.

[Registration Rules](#) > **Create New Rule**

Create New Rule

**Step 1: Basic Information**


Supply the name and description for the new Rule.

Name:

Description:

3 Complete the wizard by using information from the following table to fill in the fields.

Wizard Page	Details
Basic Information page	<p>Define the rule's name and add information to describe the rule.</p> <p><b>Name:</b> Provide a name for the rule. Users never see the rule name; it displays only in ZENworks Control Center. The name must be different than any other registration key names and must not use any of the following invalid characters: / \ * ? : " ' &lt; &gt;   ` % ~.</p> <p><b>Description:</b> Provide information about the new registration rule. The information appears only in ZENworks Control Center.</p>
Device Criteria page	<p>Define the criteria that must be met for the registration rule to be applied to a device. The criteria are defined through the use of filters. At least one filter must be defined.</p> <ol style="list-style-type: none"> <li>Click <i>Add Filter</i> to add a filter line.</li> <li>Create the filter expression. <p>An expression consists of a criteria option, operator, and value. For example:</p> <pre>IPAddress starts with 123.456</pre> <p>IPAddress is the criteria option, starts with is the operator, and 123.456 is the value. In the above example, the registration rule is applied only to devices whose IP addresses start with 123.456.</p> <p>If necessary, you can use NOT to perform a logical negation of the expression. For example:</p> <pre>NOT IPAddress starts with 123.456</pre> <p>In the above example, the registration rule is applied only to devices whose IP addresses do not start with 123.456.</p> <p>The criteria options you can use are listed below, along with possible values. The format for all values, with the exception of Device Type and OS, is free form string.</p> <ul style="list-style-type: none"> <li>♦ CPU: Intel(R) Pentium(R) M processor 1600MHz</li> <li>♦ DNS: abc.xyz.com</li> <li>♦ Device Type: Workstation or Server</li> <li>♦ GUID: 5bf63fb9b1ed4cd880e1a428a1fcf737</li> <li>♦ Hostname: zenserver</li> <li>♦ IPAddress: 123.456.78.99</li> <li>♦ Language: Portuguese (Brazil)</li> <li>♦ OS: win2003-se-sp1-x86</li> </ul> </li> <li>If necessary, click <i>Add Filter</i> to create another filter. <p>Filters are combined with the AND operator, which means that the criteria defined in each filter must be met before the registration rule is applied to a device. For example:</p> <pre>OS equals Windows Server 2003 AND IPAddress starts with 123.456</pre> <p>In the above example, the registration rule is applied only to devices whose operating system is Windows 2003 and whose IP address starts with 123.456.</p> </li> </ol>

Wizard Page	Details
Containment Rules page	<p>Specify the folder in which to place the devices.</p> <p>As a general rule, devices with similar configuration settings (refresh intervals, logging settings, remote management settings, and so forth) should be grouped in the same folder so that you can specify the configuration settings on the folder and have the devices in the folder inherit them. You should not use the same folder for devices that require different configuration settings; doing so prohibits you from using the folder to define the settings and forces you to define them on each individual device.</p>
Device Fields	<p>Specify the department, site, and location information you want entered on a device's details page when it registers. For example, if you enter <i>Accounting</i> in the <i>Department</i> field, then <i>Accounting</i> is entered in the <i>Department</i> field on the device's details page.</p>
Group Membership page	<p>Specify the groups that devices will become members of when they register.</p> <p>Adding groups causes registering devices to receive any assignments provided by membership in the groups. Assignments from group membership are additive, so if a device is assigned to both groups A and B, the device receives all assignments from both groups.</p> <p>You can only add groups that are valid for the type of device folder you specified on the previous page of the wizard. For example, if you specified the <i>/Devices/Workstations</i> folder, you can only choose workstation groups.</p> <p>To specify a group:</p> <ol style="list-style-type: none"> <li>1. Click <i>Add</i> to display the Groups dialog box.</li> <li>2. Browse for and select the group (or groups) to which you want to add the devices. To do so: <ol style="list-style-type: none"> <li>a. Click  next to a folder (for example, the <i>Workstations</i> folder or <i>Servers</i> folder) to navigate through the folders until you find the group you want to select.</li> <li>or</li> <li>Search for the group by entering its name in the <i>Item name</i> box. You can use an asterisk (*) as a wildcard. For example, entering <i>P*</i> finds all groups that start with P, or entering <i>*Accounting</i> finds all groups that end with Accounting.</li> <li>b. Click the underlined link in the <i>Name</i> column to select the group and display its name in the <i>Selected</i> list box.</li> <li>c. Repeat steps 2a and 2b until you've selected all groups to which you want to assign membership.</li> <li>d. Click <i>OK</i> to add the selected groups to the list.</li> </ol> </li> </ol>

When you complete the wizard, the rule is added to the Registration Rules panel. Rules are applied from the top down. You want to list the more restrictive rules first, followed by the more general rules. If no rules apply, the default server and workstation rules are applied.

- 4 If you want to reorder the rules, click *Advanced* (located in the upper right corner of the Registration Rules panel).
- 5 Select the check box in front of the rule you want to move.
- 6 Click *Move Up* or *Move Down* to reposition the rule.

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 10 Configuration Management Command Line Utilities Reference*.

## 7.3 Modifying the Device Naming Template Used During Registration

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}`.

If the naming template causes conflicting device object names, another machine variable is automatically appended to make the second name unique. For example, if you are using the hostname for the name and you have two devices with the same hostname, the GUID is added to the hostname to create a unique name.

To modify the template:

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

Configuration	Registration	System Information	Asset Inventory	System Updates	Asset Management
Management Zone Settings					⌵
Content					⌵
Device Management					⌵
Category	Description	Is Configured			
<a href="#">Local Device Logging</a>	Enable and configure local logging of warnings and errors encountered by managed devices.	Yes			
<a href="#">Device Refresh Schedule</a>	Configure the device refresh interval.	Yes			
<a href="#">ZENworks Agent</a>	ZENworks Agent Configuration.	No			
<a href="#">Registration</a>	Configure registration settings.	Yes			
<a href="#">Remote Management</a>	Enable and configure remote management.	Yes			
<a href="#">Preboot Services</a>	Configure Preboot Services.	Yes			
<a href="#">Primary User</a>	Configure the setting for how the primary user is determined.	No			
<a href="#">Dynamic Group Refresh Schedule</a>	Configure dynamic group refresh schedule.	No			
Discovery and Deployment					⌵
Event and Messaging					⌵
Infrastructure Management					⌵
Inventory					⌵
Reporting Services					⌵
Asset Management					⌵
Patch Management Services					⌵


- 2 In the Management Zone Settings panel, click *Device Management*, then click *Registration* to display the Registration page.

**Registration**

Configure registration settings.

**Device Naming Template**

Name given to new machines:




**Registration Rules**

☒ Enable use of registration rules.

☒ Enable use of default registration rules.

**Device Dynamic Rename**

☐ Enable automatic renaming of devices.

- 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}`

- Click *OK* to save the changes.

## 7.4 Enabling Dynamic Renaming of Devices During Registration

The Device Dynamic Rename setting lets you enable devices to be renamed, if necessary, whenever they refresh their registration information. A device might need to be renamed for the following reasons:

- The naming template's settings have changed. For example, the name template is now using both the Hostname and GUID variables rather than only the Hostname.
- A different naming template is now being applied to the device. For example, a folder naming template is now being applied rather than the Management Zone naming template.
- The device variable being used for the name changed. For example, the device's hostname is being used for the name, and the device's actual hostname changed.

Because a device's GUID and not its name is used to establish relationships with other ZENworks objects (folders, groups, bundles, policies, and so forth), renaming the device does not affect anything other than the name that is displayed in ZENworks Control Center.

By default, the Device Dynamic Rename setting is disabled. You can enable the setting at the Management Zone, in which case all devices inherit the setting, or you can enable it on a device folder, in which case only the devices in the folder inherit the setting.

- [Section 7.4.1, "Enabling the Setting at the Management Zone," on page 55](#)
- [Section 7.4.2, "Enabling the Setting for a Device Folder," on page 56](#)

## 7.4.1 Enabling the Setting at the Management Zone

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

Configuration	Registration	System Information	Asset Inventory	System Updates	Asset Management
Management Zone Settings					⌵
Content					⌵
Device Management					⌵
Category	Description	Is Configured			
<a href="#">Local Device Logging</a>	Enable and configure local logging of warnings and errors encountered by managed devices.	Yes			
<a href="#">Device Refresh Schedule</a>	Configure the device refresh interval.	Yes			
<a href="#">ZENworks Agent</a>	ZENworks Agent Configuration.	No			
<a href="#">Registration</a>	Configure registration settings.	Yes			
<a href="#">Remote Management</a>	Enable and configure remote management.	Yes			
<a href="#">Preboot Services</a>	Configure Preboot Services.	Yes			
<a href="#">Primary User</a>	Configure the setting for how the primary user is determined.	No			
<a href="#">Dynamic Group Refresh Schedule</a>	Configure dynamic group refresh schedule.	No			
Discovery and Deployment					⌵
Event and Messaging					⌵
Infrastructure Management					⌵
Inventory					⌵
Reporting Services					⌵
Asset Management					⌵
Patch Management Services					⌵

- 2 In the Management Zone Settings panel, click *Device Management*, then click *Registration* to display the Registration page.

[Configuration](#) > [Registration](#)

**Registration**  
Configure registration settings.

**Device Naming Template**  
Name given to new machines:

**Registration Rules**  
☒ Enable use of registration rules.  
☒ Enable use of default registration rules.

**Device Dynamic Rename**  
☐ Enable automatic renaming of devices.


- 3 In the Device Dynamic Rename panel, click *Enable automatic renaming of devices*.

- 4 Click *OK* to save the changes.

## 7.4.2 Enabling the Setting for a Device Folder

- 1 In ZENworks Control Center, click the *Devices* tab.
- 2 Browse to find the device folder for which you want to change the setting. then click *Details* to display the folder's details.
- 3 Click the *Settings* tab.

[Devices](#) > [Servers](#)

 Servers

Summary	Relationships	Settings
<b>Settings</b>		
<b>Content</b>		⌵
<b>Device Management</b>		⌴
Category	Description	Inherited From
<a href="#">Device Refresh Schedule</a>	Configure the device refresh interval.	(System)
<a href="#">Local Device Logging</a>	Enable and configure local logging of warnings and errors encountered by managed devices.	(System)
<a href="#">Device Dynamic Rename</a>	Enables automatic renaming of devices.	(System)
<a href="#">Preboot Services</a>	Configure Preboot Services.	(System)
<a href="#">Remote Management</a>	Enable and configure remote management.	(System)
<a href="#">Primary User</a>	Configure the setting for how the primary user is determined.	---
<a href="#">Registration</a>	Configure registration settings.	(System)
<a href="#">Enable/Disable Managed Device Agents</a>	Configure whether each agent on a managed device is enabled.	(System)
<b>Infrastructure Management</b>		⌵
<b>Inventory</b>		⌵
<b>Asset Management</b>		⌵

- 4 In the Settings panel, click *Device Management*, then click *Device Dynamic Rename* to display the Device Dynamic Rename page.

[Devices](#) > [Servers](#) > [Device Dynamic Rename](#)

 Servers

**Device Dynamic Rename** 

Enables automatic renaming of devices.

Current: (System) ([Override settings](#))

**Device Dynamic Rename** 

☐ Enable automatic renaming of devices.

- 5 Click *Override settings* to activate the Device Dynamic Rename panel.
- 6 In the Device Dynamic Rename panel, click *Enable automatic renaming of devices*.
- 7 Click *OK* to save the changes.

## 7.5 Disabling the Use of Registration Rules

By default, the registration rules feature is enabled. This ensures that devices that register without a registration key are at least added to the correct folder, which is the `/servers` or `/workstations` folder, depending on the device type.

If you want to rely completely on registration keys, you can disable registration rules. You have two options when you disable registration rules:

- ♦ **Disable the default registration rules only:** Any device that attempts to register without a registration key or that does not meet the criteria in a custom registration rule is rejected. The default registration rules are ignored.
- ♦ **Disable all registration rules:** Any device that attempts to register without a registration key is rejected.

To disable registration rules:

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

Configuration	Registration	System Information	Asset Inventory	System Updates	Asset Management
Management Zone Settings					⌵
Content					⌵
Device Management					⌵
Category	Description			Is Configured	
<a href="#">Local Device Logging</a>	Enable and configure local logging of warnings and errors encountered by managed devices.			Yes	
<a href="#">Device Refresh Schedule</a>	Configure the device refresh interval.			Yes	
<a href="#">ZENworks Agent</a>	ZENworks Agent Configuration.			No	
<a href="#">Registration</a>	Configure registration settings.			Yes	
<a href="#">Remote Management</a>	Enable and configure remote management.			Yes	
<a href="#">Preboot Services</a>	Configure Preboot Services.			Yes	
<a href="#">Primary User</a>	Configure the setting for how the primary user is determined.			No	
<a href="#">Dynamic Group Refresh Schedule</a>	Configure dynamic group refresh schedule.			No	
Discovery and Deployment					⌵
Event and Messaging					⌵
Infrastructure Management					⌵
Inventory					⌵
Reporting Services					⌵
Asset Management					⌵
Patch Management Services					⌵

- 2 In the Management Zone Settings panel, click *Device Management*, then click *Registration* to display the Registration page.

The screenshot shows a configuration window titled "Registration" with a close button in the top right corner. Below the title bar is a subtitle "Configure registration settings." The window is divided into three main sections:

- Device Naming Template:** Contains the text "Name given to new machines:" followed by a text input field containing "\${HostName}" and a small icon to its right.
- Registration Rules:** Contains two checked checkboxes: "Enable use of registration rules." and "Enable use of default registration rules."
- Device Dynamic Rename:** Contains an unchecked checkbox labeled "Enable automatic renaming of devices."

- 3 In the Registration Rules panel, deselect one of the following options:

**Enable Use of Registration Rules:** Disable this option to force devices to use a registration key when registering. Any devices that attempt to register without a key are rejected.

**Enable Use of Default Registration Rules:** Disable this option to force devices to use a registration key or meet the criteria defined in a custom registration rule. Any devices that do not are rejected.

- 4 Click *OK* to save the changes.

## 7.6 Manually Registering a Device

A device is automatically registered when the ZENworks Adaptive Agent is installed. You should only need to manually register a device in the following situations:

- ♦ The device was unregistered.
- ♦ The device's object was deleted from the ZENworks database. The Adaptive Agent is still installed on the device and you now want to register the device again.
- ♦ You want to reregister an already registered device with an additional registration key.

Manual registration of a device must be done at the device using the ZENworks Adaptive Agent command line utility (zac).

The following sections provide instructions:

- ♦ [Section 7.6.1, "Performing an Initial Registration," on page 58](#)
- ♦ [Section 7.6.2, "Reregistering a Device with an Additional Registration Key," on page 59](#)

### 7.6.1 Performing an Initial Registration

- 1 At the device, open a command prompt.
- 2 Enter the following command:

```
zac reg [-k key] [-u username -p password] [server_url:port]
```

For example:

```
zac reg -k acct -u zadmin -p novell https://zserver.novell.com
```

The `-k`, `-u`, and `-p` parameters are optional. If you don't use the `-u` and `-p` parameters, you are prompted to enter a username and password. For the `server_url:port` parameter, you can also use an IP address; the port is required only if the ZENworks Server is not using the default port (80 or 443).

## 7.6.2 Reregistering a Device with an Additional Registration Key

- 1 At the device, open a command prompt.
- 2 Enter the following command:

```
zac add-reg-key registration_key
```

For example:

```
zac add-reg-key acct
```

Registration keys are additive. If you register with more than one key, the device receives all group memberships associated with each registration key.

## 7.7 Unregistering a Device

A device is automatically unregistered when the following situations:

- ♦ The ZENworks Adaptive Agent is uninstalled.
- ♦ The device's object is deleted from the ZENworks database.

You can manually unregister a device if necessary. Unregistration of a device must be done at the device using the ZENworks Adaptive Agent command line utility (`zac`).

- 1 At the device, open a command prompt.
- 2 Enter the following command:

```
zac unr [-f] [-u username -p password]
```

For example:

```
zac unr -u zadmin -p novell
```

The `-f`, `-u`, and `-p` parameters are optional. If you don't use the `-u` and `-p` parameters, you are prompted to enter a username and password. The `-f` parameter ignores the ZENworks database and forces the device to be unregistered locally; this option is only necessary if the device object has already been deleted from the ZENworks database or if the device cannot connect to the database.



# Deploying the ZENworks Adaptive Agent

# 8

Any devices you want to manage through ZENworks® must have the ZENworks Adaptive Agent deployed to them. The Adaptive Agent distributes software, enforces bundles, collects software and hardware inventory, and performs all other ZENworks management tasks on the managed device.

For detailed information about the supported platforms and system requirements for a managed device, see “[Managed Device Requirements](#)” in the *ZENworks 10 Configuration Management Installation Guide*.

There are several ways to deploy the agent. The following sections provide instructions:

- ♦ [Section 8.1, “Changing the Target Installation Directory,” on page 61](#)
- ♦ [Section 8.2, “Using a Task to Deploy the Agent,” on page 61](#)
- ♦ [Section 8.3, “Manually Deploying the Agent,” on page 77](#)

## 8.1 Changing the Target Installation Directory

By default, the ZENworks Adaptive Agent is installed to the following location on a Windows device:

```
Windows_drive:\Program Files\Novell\ZENworks
```

To install the agent to a different location, you can create a ZENWORKS\_HOME environment variable on the device prior to deployment and set the variable to the new target installation directory. The path must always end with \Novell\ZENworks. Some examples of acceptable paths are:

```
c:\Novell\ZENworks
```

```
c:\Program Files\Corporate\Novell\ZENworks
```

```
d:\Applications\Novell\ZENworks
```

## 8.2 Using a Task to Deploy the Agent

The ZENworks Server can deploy the ZENworks Adaptive Agent to devices. This requires that you create a task, called a deployment task, for the ZENworks Server. The task identifies the target devices, the credentials required to perform an installation on the devices, the registration key to use (optional), the date and time to perform the installation, and other tasks you want performed on the devices either before or after the installation.

The steps for creating a deployment task vary slightly depending on whether or not the target devices are already listed as discovered devices in your Management Zone (see [Part I, “Device Discovery,” on page 9](#)):

- ♦ [Section 8.2.1, “Prerequisites for Deploying to a Device,” on page 62](#)
- ♦ [Section 8.2.2, “Deploying to a Discovered Device,” on page 63](#)

- ♦ [Section 8.2.3, “Deploying to a Non-Discovered Device,” on page 66](#)

## 8.2.1 Prerequisites for Deploying to a Device

Before the ZENworks Server can deploy the ZENworks Adaptive Agent to a device, make sure the following prerequisites are satisfied:

- ♦ [“Enabling File and Printer Sharing through Windows Firewall” on page 62](#)
- ♦ [“Enabling Classic File Sharing” on page 62](#)

### Enabling File and Printer Sharing through Windows Firewall

Any target device that is using Windows Firewall needs to be configured to allow file and printer sharing through the firewall. This is done by enabling the *File and Printer Sharing* exception in the Windows Firewall configuration settings. You can access Windows Firewall through the Control Panel or through the Windows Security Center.

By default, the scope of the exception applies only to the local subnet. If the target device is in a different subnet than the Primary Server from which the deployment is run, you must add the IP Address of the Primary Server along with the local subnet to the Windows Firewall.

- 1 From the desktop *Start* menu, click *Settings > Control Panel*.
- 2 Double-click *Windows Firewall*.  
The Windows Firewall window is displayed.
- 3 Click the *Exceptions* tab.
- 4 In the *Programs and Services* list, select *File and Printer Sharing*, then click *Edit*.  
The Edit a Service window is displayed.
- 5 Click *Change Scope* to include the IP Address of the Primary Server and the local subnet.
- 6 Click *OK*.

### Enabling Classic File Sharing

The ZENworks Server needs classic file sharing access to the administrative share (displayed as Admin\$) on target devices. The following sections provide the steps for configuring classic file sharing for the various Windows versions.

#### Windows 2000

Windows 2000 devices use classic file sharing by default. If deployment of the Adaptive Agent to a Windows 2000 device fails, check the HKLM\System\currentcontrolset\services\lanmanserver\parameters\AutoShareWrks entry to see if it is set to 0 (disabled). If it is set to 0, Admin\$ share is not accessible and the error is displayed. Delete the entire setting.

#### Windows 2003

Windows 2003 devices use classic file sharing by default. If deployment of the Adaptive Agent to a Windows 2003 device fails with an invalid credentials error, you must enable classic file sharing.

- 1 On the Windows 2003 device, click the desktop *Start* menu > *Settings > Control Panel*.

- 2 Double-click *Administrative Tools > Local Security Policy*.  
The Local Security Settings window is displayed.
- 3 In *Security Settings*, navigate to *Local Policies > Security Options*.
- 4 Change the value of *Network access: Sharing and security model for local accounts* to *Classic - local users authenticate as themselves*.

You can also use a Windows Group Policy to change the setting.

## Windows XP

Windows XP uses simple file sharing by default. You need to disable simple file sharing to enable classic file sharing.

- 1 At the Windows XP device, right-click the My Computer icon, then click *Open*.
- 2 Click the *Tools* menu > *Folder Options* to display the Folder Options dialog box.
- 3 Click the *View* tab.
- 4 In the *Advanced Settings* list, deselect the *Use simple file sharing* option, then click *OK* to save the change.

Disabling this option changes the setting for the *Network access: Sharing and security model for local accounts* option in the Local Security Policy (Local Policies > Security Options) to *Classic - local users authenticate as themselves*. You can also use a Windows Group Policy to change the setting.

## Windows Vista

- 1 Open the Windows Registry and access the following:

```
HKLM/Software/Microsoft/Windows/CurrentVersion/Policies/System/
LocalAccountTokenFilterPolicy
```

If the registry key does not exist, you need to create it.

- 2 Change its DWORD (32-bit) value to 1.  
This allows remote users to log in and not be forced to be “guest.”
- 3 Close the registry to save the change.
- 4 Open the Services window and set Remote Registry service to start automatically, then start it.
- 5 Click *Start > Settings > Control Panel*.
- 6 Double-click *Network and Sharing Center*.
- 7 Enable the *File Sharing* option.

## 8.2.2 Deploying to a Discovered Device

This section assumes that you’ve already performed a discovery task to add the target devices to your ZENworks database. If you have not, you can perform the discovery task before continuing (see [Part I, “Device Discovery,” on page 9](#)) or you can perform the discovery as part of the deployment task (see [Section 8.2.3, “Deploying to a Non-Discovered Device,” on page 66](#)).

To deploy the ZENworks Adaptive Agent to a discovered device:

- 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.

[Deployment](#) > **Device Deployment Wizard**

**Deploy Device Wizard**

**Step 1: Enter Deployment Task Name**

Name: \*

Description:

\* Fields marked with an asterisk are required.

- 3 Complete the wizard by using information from the following table to fill in the fields.

Wizard Page	Details
Enter Deployment Task page	Specify a name for the task. The name cannot include any of the following invalid characters: / \ * ? : " ' < >   ` % ~
Select Devices page	<ol style="list-style-type: none"> <li>1. Click <i>Add</i> to display the Discovered Device Browser dialog box. The default view displays all discovered devices in your Management Zone.</li> <li>2. Click  to select a device.</li> <li>3. When you have finished selecting devices, click <i>OK</i> to return the Select Devices page. The devices you selected are displayed in the list.</li> </ol>
Enter Credentials page > <i>Save Credentials to DataStore</i> field	<p>The Enter Credentials page lets you provide the usernames and passwords required to deploy the Adaptive Agent to the devices included in the task.</p> <p>Unless you save the credentials, they are stored only in memory. Saved credentials are encrypted in the database for increased security.</p> <p>Credentials that are not saved are cleared from memory when the ZENworks Server is restarted. If you are creating a scheduled deployment task, you might want to save the credentials to ensure that they are still available when the deployment is performed.</p>

Wizard Page	Details
Enter Credentials page > <i>Credentials</i> field	<p>To add a credential:</p> <ol style="list-style-type: none"> <li>Click <i>Add</i> to display the Enter Credential Information dialog box. In the <i>Username</i> field, specify the appropriate username.</li> </ol> <p>To deploy the Adaptive Agent, the ZENworks Server must be able to map a drive to the device's administrative share (ADMIN\$). This requires the following credentials:</p> <ul style="list-style-type: none"> <li>♦ <b>If the device is a member of a domain:</b> You can use a domain or local Administrator group credential. If you use the local credential, you must specify the username as <code>workstation_name\username</code> to distinguish it from domain credentials.</li> <li>♦ <b>If the device is not a member of a domain:</b> You must use a local Administrator group credential.</li> </ul> <ol style="list-style-type: none"> <li>Enter the user password in the <i>Password</i> and <i>Reenter Password</i> fields.</li> <li>Click <i>OK</i> to save the credential.</li> </ol> <p>Depending on your environment, one credential might not provide access to all of the devices where you want to deploy the Adaptive Agent. In this case, you need to add as many credentials as necessary to cover the devices included in the task. The ZENworks Server uses the first credential that works.</p>
Select Schedule page	<p>The Select Schedule page lets you choose whether you want the task to run as soon as it is created (the <i>Now</i> option) or if you want to schedule the task to run at a future date and time. If you select <i>Scheduled</i>, choose one of the following schedules:</p> <p><b>No Schedule:</b> Indicates that no schedule has been set. The task does not run until a schedule is set or it is manually launched. This is useful if you want to create the task and come back to it later to establish the schedule or run it manually.</p> <p><b>Date Specific:</b> Specifies one or more dates on which to run the task.</p> <p><b>Recurring:</b> Identifies specific days each week, month, or a fixed interval on which to run the task.</p> <p>See <a href="#">Appendix A, "Schedules," on page 87</a> or click the <i>Help</i> button for more detailed information about the schedules.</p>
Select Primary Server page > <i>Primary Server</i> field	<p>Select the ZENworks Server that you want to perform the deployment task.</p>
Add Registration Key page	<p>Select a registration key to use during the registration portion of the deployment process. A registration key provides information about the folders and groups to which a device is assigned during registration. Selecting a registration key is optional; if you don't select one, registration rules are used to determine the folder and group assignments. To deploy to servers or workstations, choose a server registration key or a workstation registration key respectively.</p> <p>For more information about registration keys and rules, see <a href="#">Chapter 7, "Registering Devices," on page 45</a>.</p>

Wizard Page	Details
Pre/Post Deployment page	<p>Specify commands that you want run before and after the Adaptive Agent is installed on a device. For example, you can execute operating system commands, run scripts, and launch executables.</p> <p>The commands are passed to the preagent as part of the deployment task package. The preagent executes the commands in the system space, so you must specify commands that do not require user interaction.</p> <p>Click the <i>Help</i> button for more detailed information about predeployment and post-deployment commands.</p>

### 8.2.3 Deploying to a Non-Discovered Device

If a target device has not been added to your ZENworks database through a discovery task, you can select the device while you are creating the deployment task. The following sections explain how to create the discovery task depending on whether you want to identify the target device by its IP address/hostname, from a CSV file, or from an LDAP directory.


- ♦ “IP Address/Hostname” on page 66
- ♦ “New CSV File” on page 69
- ♦ “Existing LDAP Source” on page 72
- ♦ “New LDAP Source” on page 74

#### IP Address/Hostname

- 1 In ZENworks Control Center, click the *Deployment* tab.
- 2 In the Deployment Tasks panel, click *New* to launch the Deploy Device Wizard.

[Deployment](#) > **Device Deployment Wizard**

Deploy Device Wizard

 Step 1: Enter Deployment Task Name

Name: \*

Description:

\* Fields marked with an asterisk are required.

- 3 Complete the wizard by using information from the following table to fill in the fields.

Wizard Page	Details
Enter Deployment Task page	Specify a name for the task. The name cannot include any of the following invalid characters: / \ * ? : " ' < >   ` % ~
Select Devices page	<ol style="list-style-type: none"> <li>1. Click <i>Add</i> to display the Discovered Device Browser dialog box.</li> <li>2. In the <i>Source</i> list, select <i>IP Address</i>.</li> <li>3. Fill in the <i>IP Address Range/Host Name</i> field.  The address can use any of the following formats:  xxx.xxx.xxx.xxx: Standard dotted-decimal notation. For example, 123.45.167.100.  xxx.xxx.xxx.xxx - xxx.xxx.xxx.xxx: Standard dotted-decimal notation. For example, 123.45.167.100 - 123.45.167.125.  xxx.xxx.xxx.xxx/n: Standard CIDR (Classless Inter-Domain Routing) notation. For example, 123.45.167.100/24 matches all IP addresses that start with 123.45.167.  hostname: Standard device hostname. For example, workstation1.</li> <li>4. Click <i>Add</i> to add the device to the <i>Selected Devices</i> list.</li> <li>5. When you are finished selecting devices, click <i>OK</i>.</li> </ol>
Enter Credentials page > <i>Save Credentials to DataStore</i> field	<p>The Enter Credentials page lets you provide the usernames and passwords required to deploy the Adaptive Agent to the devices included in the task.</p> <p>Unless you save the credentials, they are stored only in memory. Saved credentials are encrypted in the database for increased security.</p> <p>Credentials that are not saved are cleared from memory when the ZENworks Server is restarted. If you are creating a scheduled deployment task, you might want to save the credentials to ensure that they are still available when the deployment is performed.</p>

Wizard Page	Details
Enter Credentials page > <i>Credentials</i> field	<p>To add a credential:</p> <ol style="list-style-type: none"> <li>Click <i>Add</i> to display the Enter Credential Information dialog box. In the <i>Username</i> field, specify the appropriate username.</li> </ol> <p>To deploy the Adaptive Agent, the ZENworks Server must be able to map a drive to the device's administrative share (ADMIN\$). This requires the following credentials:</p> <ul style="list-style-type: none"> <li>♦ <b>If the device is a member of a domain:</b> You can use a domain or local Administrator group credential. If you use the local credential, you must specify the username as <code>workstation_name\username</code> to distinguish it from domain credentials.</li> <li>♦ <b>If the device is not a member of a domain:</b> You must use a local Administrator group credential.</li> </ul> <ol style="list-style-type: none"> <li>Enter the user password in the <i>Password</i> and <i>Reenter Password</i> fields.</li> <li>Click OK to save the credential.</li> </ol> <p>Depending on your environment, one credential might not provide access to all of the devices where you want to deploy the Adaptive Agent. In this case, you need to add as many credentials as necessary to cover the devices included in the task. The ZENworks Server uses the first credential that works.</p>
Select Schedule page	<p>The Select Schedule page lets you choose whether you want the task to run as soon as it is created (the <i>Now</i> option) or if you want to schedule the task to run at a future date and time. If you select <i>Scheduled</i>, choose one of the following schedules:</p> <p><b>No Schedule:</b> Indicates that no schedule has been set. The task does not run until a schedule is set or it is manually launched. This is useful if you want to create the task and come back to it later to establish the schedule or run it manually.</p> <p><b>Date Specific:</b> Specifies one or more dates on which to run the task.</p> <p><b>Recurring:</b> Identifies specific days each week, month, or a fixed interval on which to run the task.</p> <p>See <a href="#">Appendix A, "Schedules," on page 87</a> or click the <i>Help</i> button for more detailed information about the schedules.</p>
Select Primary Server page > <i>Primary Server</i> field	Select the ZENworks Server that you want to perform the deployment task.
Add Registration Key page	<p>Select a registration key to use during the registration portion of the deployment process. A registration key provides information about the folders and groups to which a device is assigned during registration. Selecting a registration key is optional; if you don't select one, registration rules are used to determine the folder and group assignments. To deploy to servers or workstations, choose a server registration key or a workstation registration key respectively.</p> <p>For more information about registration keys and rules, see <a href="#">Chapter 7, "Registering Devices," on page 45</a>.</p>


Wizard Page	Details
Pre/Post Deployment page	<p>Specify commands that you want run before and after the Adaptive Agent is installed on a device. For example, you can execute operating system commands, run scripts, and launch executables.</p> <p>The commands are passed to the preagent as part of the deployment task package. The preagent executes the commands in the system space, so you must specify commands that do not require user interaction.</p> <p>Click the <i>Help</i> button for more detailed information about predeployment and post-deployment commands.</p>

## New CSV File

- 1 In ZENworks Control Center, click the *Deployment* tab.
- 2 In the Deployment Tasks panel, click *New* to launch the Deploy Device Wizard.

[Deployment](#) > **Device Deployment Wizard**

**Deploy Device Wizard**

 **Step 1: Enter Deployment Task Name**


Name: \*

Description:

\* Fields marked with an asterisk are required.

- 3 Complete the wizard by using information from the following table to fill in the fields.

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

Wizard Page	Details
Select Devices page	<ol style="list-style-type: none"> <li>1. Click <i>Add</i> to display the Discovered Device Browser dialog box.</li> <li>2. In the <i>Source</i> list, select <i>Add New CSV File</i> to display the Add New Source dialog box.</li> <li>3. Fill in the following fields: <p><b>CSV File:</b> Browse for and select the CSV file containing the devices to which you want to deploy the agent.</p> <p><b>DNS Name Column:</b> Select the number of the column that contains the DNS name information.</p> <p><b>IP Address Column:</b> Select the number of the column that contains the IP address information. If you want the IP address to be resolved from the DNS name rather than imported from the file, select the <i>Resolve IP from DNS name</i> option.</p> <p><b>OS Type Column:</b> Select the number of the column that contains the operating system information. If you want to specify a default OS type rather than importing it from the file, select the <i>Use default OS for all selections</i> option, then select the default operating system in the <i>Default OS Type</i> field.</p> </li> <li>4. Click OK to display the devices in the source list.</li> <li>5. Click  to move a device to the <i>Selected Devices</i> list.</li> <li>6. When you are finished selecting devices, click <i>OK</i>.</li> </ol>
Enter Credentials page > <i>Save Credentials to DataStore</i> field	<p>The Enter Credentials page lets you provide the user names and passwords required to deploy the Adaptive Agent to the devices included in the task.</p> <p>Unless you save the credentials, they are stored only in memory. Saved credentials are encrypted in the database for increased security.</p> <p>Credentials that are not saved are cleared from memory when the ZENworks Server is restarted. If you are creating a scheduled deployment task, you might want to save the credentials to ensure that they are still available when the deployment is performed.</p>

Wizard Page	Details
Enter Credentials page > <i>Credentials</i> field	<p>To add a credential:</p> <ol style="list-style-type: none"> <li>Click <i>Add</i> to display the Enter Credential Information dialog box. In the <i>Username</i> field, specify the appropriate user name.</li> </ol> <p>To deploy the Adaptive Agent, the ZENworks Server must be able to map a drive to the device's administrative share (ADMIN\$). This requires the following credentials:</p> <ul style="list-style-type: none"> <li>♦ <b>If the device is a member of a domain:</b> You can use a domain or local Administrator group credential. If you use the local credential, you must specify the user name as <code>workstation_name\username</code> to distinguish it from domain credentials.</li> <li>♦ <b>If the device is not a member of a domain:</b> You must use a local Administrator group credential.</li> </ul> <ol style="list-style-type: none"> <li>Enter the user password in the <i>Password</i> and <i>Reenter Password</i> fields.</li> <li>Click OK to save the credential.</li> </ol> <p>Depending on your environment, one credential might not provide access to all of the devices where you want to deploy the Adaptive Agent. In this case, you need to add as many credentials as necessary to cover the devices included in the task. The ZENworks Server uses the first credential that works.</p>
Select Schedule page	<p>The Select Schedule page lets you choose whether you want the task to run as soon as it is created (the <i>Now</i> option) or if you want to schedule the task to run at a future date and time. If you select <i>Scheduled</i>, choose one of the following schedules:</p> <p><b>No Schedule:</b> Indicates that no schedule has been set. The task does not run until a schedule is set or it is manually launched. This is useful if you want to create the task and come back to it later to establish the schedule or run it manually.</p> <p><b>Date Specific:</b> Specifies one or more dates on which to run the task.</p> <p><b>Recurring:</b> Identifies specific days each week, month, or a fixed interval on which to run the task.</p> <p>See <a href="#">Appendix A, "Schedules," on page 87</a> or click the <i>Help</i> button for more detailed information about the schedules.</p>
Select Primary Server page > <i>Primary Server</i> field	<p>Select the ZENworks Server that you want to perform the deployment task.</p>
Add Registration Key page	<p>Select a registration key to use during the registration portion of the deployment process. A registration key provides information about the folders and groups to which a device is assigned during registration. Selecting a registration key is optional; if you don't select one, registration rules are used to determine the folder and group assignments. To deploy to servers or workstations, choose a server registration key or a workstation registration key respectively.</p> <p>For more information about registration keys and rules, see <a href="#">Chapter 7, "Registering Devices," on page 45</a>.</p>


Wizard Page	Details
Pre/Post Deployment page	<p>Specify commands that you want run before and after the Adaptive Agent is installed on a device. For example, you can execute operating system commands, run scripts, and launch executables.</p> <p>The commands are passed to the preagent as part of the deployment task package. The preagent executes the commands in the system space, so you must specify commands that do not require user interaction.</p> <p>Click the <i>Help</i> button for more detailed information about predeployment and post-deployment commands.</p>

## Existing LDAP Source

- 1 In ZENworks Control Center, click the *Deployment* tab.
- 2 In the Deployment Tasks panel, click *New* to launch the Deploy Device Wizard.

[Deployment](#) > **Device Deployment Wizard**

Deploy Device Wizard


 Step 1: Enter Deployment Task Name

Name: \*

Description:

\* Fields marked with an asterisk are required.

- 3 Complete the wizard by using information from the following table to fill in the fields.

Wizard Page	Details
Enter Deployment Task page	Specify a name for the task. The name cannot include any of the following invalid characters: / \ * ? : " ' < >   ` % ~
Select Devices page	<ol style="list-style-type: none"> <li>1. Click <i>Add</i> to display the Discovered Device Browser dialog box.</li> <li>2. In the <i>Source</i> list, select the existing user source. The root of the user source is displayed in the source list.</li> <li>3. Browse the directory to find the desired device.</li> <li>4. Click  to move the device to the <i>Selected Devices</i> list.</li> <li>5. When you are finished selecting devices, click <i>OK</i>.</li> </ol>

Wizard Page	Details
Enter Credentials page > <i>Save Credentials to DataStore</i> field	<p>The Enter Credentials page lets you provide the user names and passwords required to deploy the Adaptive Agent to the devices included in the task.</p> <p>Unless you save the credentials, they are stored only in memory. Saved credentials are encrypted in the database for increased security.</p> <p>Credentials that are not saved are cleared from memory when the ZENworks Server is restarted. If you are creating a scheduled deployment task, you might want to save the credentials to ensure that they are still available when the deployment is performed.</p>
Enter Credentials page > <i>Credentials</i> field	<p>To add a credential:</p> <ol style="list-style-type: none"> <li>Click <i>Add</i> to display the Enter Credential Information dialog box. In the <i>Username</i> field, specify the appropriate user name. To deploy the Adaptive Agent, the ZENworks Server must be able to map a drive to the device's administrative share (ADMIN\$). This requires the following credentials: <ul style="list-style-type: none"> <li>♦ <b>If the device is a member of a domain:</b> You can use a domain or local Administrator group credential. If you use the local credential, you must specify the user name as <code>workstation_name\username</code> to distinguish it from domain credentials.</li> <li>♦ <b>If the device is not a member of a domain:</b> You must use a local Administrator group credential.</li> </ul> </li> <li>Enter the user password in the <i>Password</i> and <i>Reenter Password</i> fields.</li> <li>Click <i>OK</i> to save the credential.</li> </ol> <p>Depending on your environment, one credential might not provide access to all of the devices where you want to deploy the Adaptive Agent. In this case, you need to add as many credentials as necessary to cover the devices included in the task. The ZENworks Server uses the first credential that works.</p>
Select Schedule page	<p>The Select Schedule page lets you choose whether you want the task to run as soon as it is created (the <i>Now</i> option) or if you want to schedule the task to run at a future date and time. If you select <i>Scheduled</i>, choose one of the following schedules:</p> <p><b>No Schedule:</b> Indicates that no schedule has been set. The task does not run until a schedule is set or it is manually launched. This is useful if you want to create the task and come back to it later to establish the schedule or run it manually.</p> <p><b>Date Specific:</b> Specifies one or more dates on which to run the task.</p> <p><b>Recurring:</b> Identifies specific days each week, month, or a fixed interval on which to run the task.</p> <p>See <a href="#">Appendix A, "Schedules," on page 87</a> or click the <i>Help</i> button for more detailed information about the schedules.</p>


Wizard Page	Details
Select Primary Server page > <i>Primary Server</i> field	Select the ZENworks Server that you want to perform the deployment task.
Add Registration Key page	<p>Select a registration key to use during the registration portion of the deployment process. A registration key provides information about the folders and groups to which a device is assigned during registration. Selecting a registration key is optional; if you don't select one, registration rules are used to determine the folder and group assignments. To deploy to servers or workstations, choose a server registration key or a workstation registration key respectively.</p> <p>For more information about registration keys and rules, see <a href="#">Chapter 7, "Registering Devices," on page 45</a>.</p>
Pre/Post Deployment page	<p>Specify commands that you want run before and after the Adaptive Agent is installed on a device. For example, you can execute operating system commands, run scripts, and launch executables.</p> <p>The commands are passed to the preagent as part of the deployment task package. The preagent executes the commands in the system space, so you must specify commands that do not require user interaction.</p> <p>Click the <i>Help</i> button for more detailed information about predeployment and post-deployment commands.</p>

## New LDAP Source

- 1 In ZENworks Control Center, click the *Deployment* tab.
- 2 In the Deployment Tasks panel, click *New* to launch the Deploy Device Wizard.

[Deployment](#) > **Device Deployment Wizard**

Deploy Device Wizard


 Step 1: Enter Deployment Task Name

Name: \*

Description:

\* Fields marked with an asterisk are required.

- 3 Complete the wizard by using information from the following table to fill in the fields.

Wizard Page	Details
Enter Deployment Task page	Specify a name for the task. The name cannot include any of the following invalid characters: / \ * ? : " ' < >   ` % ~
Select Devices page	<ol style="list-style-type: none"> <li>1. Click <i>Add</i> to display the Discovered Device Browser dialog box.</li> <li>2. In the <i>Source</i> list, select <i>Add New LDAP Source</i> to display the Add New Source dialog box.</li> <li>3. Fill in the following fields: <p><b>LDAP Source Name:</b> Provide a name for the LDAP source.</p> <p><b>LDAP Server:</b> Specify the IP address or DNS hostname of the LDAP server.</p> <p><b>LDAP Port/Use SSL:</b> Defaults to the standard SSL port (636) or non-SSL port (389) depending on whether the <i>Use SSL</i> option is enabled or disabled. If your LDAP server is listening on a different port, select that port.</p> <p><b>LDAP Root Context:</b> Establishes the point in the directory where you can begin to browse. If you don't specify a base DN, the directory's root container becomes the entry point.</p> <p><b>Save Credentials to Datastore:</b> Unless you save the credentials (defined in the <i>Credentials</i> list), they are stored only in memory. Saved credentials are encrypted in the database for increased security. Credentials are cleared from memory when the ZENworks Server is restarted. If you want to permanently retain the credentials as part of the deployment task, you should save the credentials.</p> <p><b>Credentials:</b> Click <i>Add</i> to enter a username and password that provides read-only access to the directory. The user can have more than read-only access, but read-only access is all that is required and recommended.</p> <p>For Novell eDirectory access, use standard LDAP notation. For example:</p> <p>cn=admin_read_only,ou=users,o=mycompany</p> <p>For Microsoft Active Directory, use standard domain notation. For example:</p> <p>AdminReadOnly@mycompany.com</p> </li> <li>4. Click <i>OK</i> to display the LDAP directory in the source list.</li> <li>5. Browse the directory to find the desired device.</li> <li>6. Click  to move the device to the <i>Selected Devices</i> list.</li> <li>7. When you are finished selecting devices, click <i>OK</i>.</li> </ol>

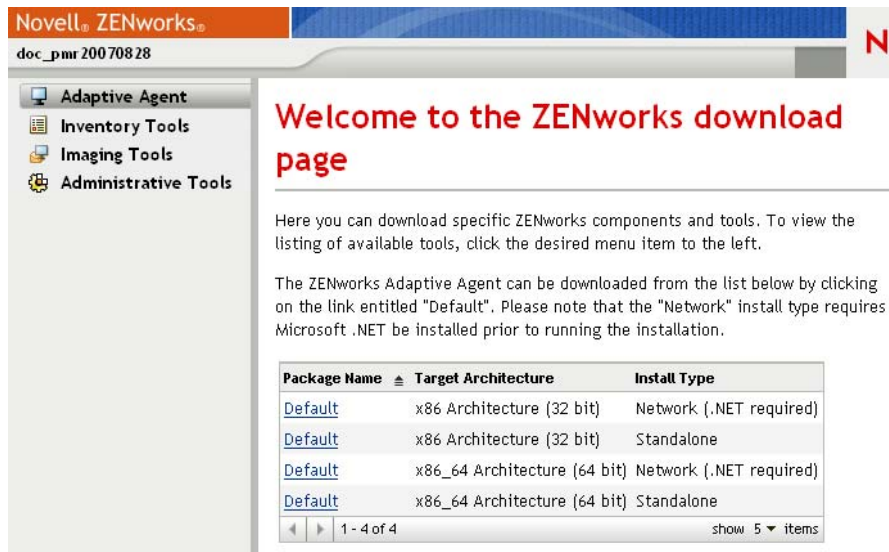
Wizard Page	Details
Enter Credentials page > <i>Save Credentials to DataStore</i> field	<p>The Enter Credentials page lets you provide the user names and passwords required to deploy the Adaptive Agent to the devices included in the task.</p> <p>Unless you save the credentials, they are stored only in memory. Saved credentials are encrypted in the database for increased security.</p> <p>Credentials that are not saved are cleared from memory when the ZENworks Server is restarted. If you are creating a scheduled deployment task, you might want to save the credentials to ensure that they are still available when the deployment is performed.</p>
Enter Credentials page > <i>Credentials</i> field	<p>To add a credential:</p> <ol style="list-style-type: none"> <li>Click <i>Add</i> to display the Enter Credential Information dialog box. In the <i>Username</i> field, specify the appropriate user name. To deploy the Adaptive Agent, the ZENworks Server must be able to map a drive to the device's administrative share (ADMIN\$). This requires the following credentials: <ul style="list-style-type: none"> <li>♦ <b>If the device is a member of a domain:</b> You can use a domain or local Administrator group credential. If you use the local credential, you must specify the user name as <code>workstation_name\username</code> to distinguish it from domain credentials.</li> <li>♦ <b>If the device is not a member of a domain:</b> You must use a local Administrator group credential.</li> </ul> </li> <li>Enter the user password in the <i>Password</i> and <i>Reenter Password</i> fields.</li> <li>Click OK to save the credential.</li> </ol> <p>Depending on your environment, one credential might not provide access to all of the devices where you want to deploy the Adaptive Agent. In this case, you need to add as many credentials as necessary to cover the devices included in the task. The ZENworks Server uses the first credential that works.</p>
Select Schedule page	<p>The Select Schedule page lets you choose whether you want the task to run as soon as it is created (the <i>Now</i> option) or if you want to schedule the task to run at a future date and time. If you select <i>Scheduled</i>, choose one of the following schedules:</p> <p><b>No Schedule:</b> Indicates that no schedule has been set. The task does not run until a schedule is set or it is manually launched. This is useful if you want to create the task and come back to it later to establish the schedule or run it manually.</p> <p><b>Date Specific:</b> Specifies one or more dates on which to run the task.</p> <p><b>Recurring:</b> Identifies specific days each week, month, or a fixed interval on which to run the task.</p> <p>See <a href="#">Appendix A, "Schedules," on page 87</a> or click the <i>Help</i> button for more detailed information about the schedules.</p>

Wizard Page	Details
Select Primary Server page > <i>Primary Server</i> field	Select the ZENworks Server that you want to perform the deployment task.
Add Registration Key page	<p>Select a registration key to use during the registration portion of the deployment process. A registration key provides information about the folders and groups to which a device is assigned during registration. Selecting a registration key is optional; if you don't select one, registration rules are used to determine the folder and group assignments. To deploy to servers or workstations, choose a server registration key or a workstation registration key respectively.</p> <p>For more information about registration keys and rules, see <a href="#">Chapter 7, "Registering Devices," on page 45</a>.</p>
Pre/Post Deployment page	<p>Specify commands that you want run before and after the Adaptive Agent is installed on a device. For example, you can execute operating system commands, run scripts, and launch executables.</p> <p>The commands are passed to the preagent as part of the deployment task package. The preagent executes the commands in the system space, so you must specify commands that do not require user interaction.</p> <p>Click the <i>Help</i> button for more detailed information about predeployment and post-deployment commands.</p>

## 8.3 Manually Deploying the Agent

Rather than 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 10 Configuration Management Installation Guide*).
- 2 On the target device, open a Web browser to the following:  
<http://server/zenworks-setup>  
where *server* is the DNS name or IP address of a ZENworks Server.



The Web browser displays a list of deployment packages. For each architecture (32-bit and 64-bit), there are two types of packages:

**Network:** The network package downloads and installs only the preagent to the target device; the preagent then downloads and installs the ZENworks Adaptive Agent from the ZENworks Server. The network package requires that Microsoft .NET is installed on the device prior to the deployment of the agent to the device.

**Standalone:** The standalone package downloads the preagent and Adaptive Agent to the target device; the preagent 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 forth) and have the standalone device run the package from the media. The Adaptive Agent is installed to the device, but no registration or management occurs until the device connects to the network.

- 3 Click the name of the deployment package you want to use, then 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, see [Package Options](#) below.

- 5 Upon completion of the installation, a message is displayed asking whether to reboot. 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, 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 under the `\Servers` folder structure or `\Workstation` folder structure on the Devices page.

## Package Options

You can use the options listed below when launching a deployment package from the command line. The syntax is:

```
package name option1 option2 ...
```

For example:

```
PreAgentPkg_Agent.exe -x -v
```

**-d *target\_path*:** Extract the files to the specified target path. The default target path is `c:\windows\novell\zenworks\stage`.

**-h:** Display help information.

**-l:** List the contents of the package only. Do not extract the package and run the installation.

**-n:** Extract the package but do not run the installation.

**-x:** Suppress the reboot prompt; do not reboot after installation.

**-v:** Turn on verbose screen logging.

In addition to the options listed above, there are two additional BUILDTIME options (*-f file* and *-o output\_file*) that are used when building packages. These options should only be used under the direction of Novell Technical Services.



# Deploying the Inventory-Only Module

# 9

If a Windows device does not meet the requirements for deploying the Adaptive Agent, or if you want to inventory a Linux/UNIX, NetWare®, or Macintosh OS X device, you can deploy the Inventory-Only module. See “**Minimum Requirements**” in the *ZENworks 10 Configuration Management Installation Guide* for information about the platform versions on which the Inventory-Only module is supported.

The following sections provide instructions:

- ♦ Section 9.1, “Downloading the Module from a ZENworks Server,” on page 81
- ♦ Section 9.2, “Installing on Linux/UNIX,” on page 82
- ♦ Section 9.3, “Installing on NetWare,” on page 83
- ♦ Section 9.4, “Installing on Windows,” on page 83
- ♦ Section 9.5, “Installing on Macintosh OS X,” on page 83

## 9.1 Downloading the Module from a ZENworks Server

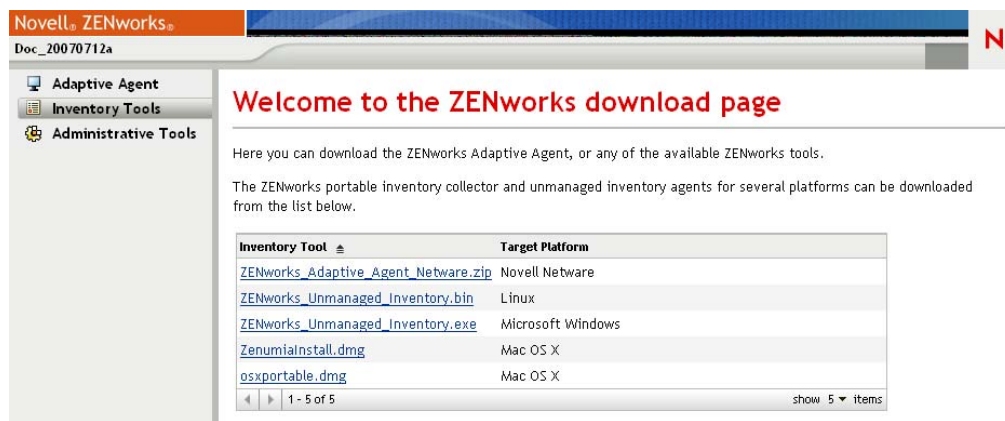
- 1 On the target device, open a Web browser to the following address:

`http://server/zenworks-setup`

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

If you are downloading the NetWare module, open the Web browser on a device from which you have file copy access to the NetWare server.

- 2 In the left navigation pane, click *Inventory Tools*.



The Inventory-Only module for each platform is listed on the page:

Platform	Filename
Novell® NetWare	ZENworks_Adaptive_Agent_Netware.zip
Microsoft Windows	ZENworks_Unmanaged_Inventory.exe
Mac OS X	ZenumiaInstall.dmg
Linux	zenumia-10.1.0-linux-x86.tar.gz
AIX	zenumia-10.1.0-aix-powerpc.tar.gz
HP-UX	zenumia-10.1.0-hpux.-parisc.tar.gz
Solaris	zenumia-10.1.0-sunos-sparc.tar.gz

- 3 Click the filename for the desired platform and download the file.
- 4 Skip to one of the following sections to continue with installation of the module:
  - ♦ [Section 9.2, “Installing on Linux/UNIX,” on page 82](#)
  - ♦ [Section 9.3, “Installing on NetWare,” on page 83](#)
  - ♦ [Section 9.4, “Installing on Windows,” on page 83](#)
  - ♦ [Section 9.5, “Installing on Macintosh OS X,” on page 83](#)

## 9.2 Installing on Linux/UNIX

- 1 Log in as a user with installation rights on the device.
- 2 Make sure you’ve downloaded the correct Inventory-Only module package to the target device. If you haven’t, see [Section 9.1, “Downloading the Module from a ZENworks Server,” on page 81](#).
- 3 Create a temporary directory to unpack the installation files in. Do not use /tmp as the temporary installation directory; it interferes with the package installation. You can, however, create a separate directory under /tmp, such as /tmp/zaaio.
- 4 Move the downloaded package to the directory created in [Step 3](#).
- 5 At a command prompt, change to the location of the Inventory-Only module package file.
- 6 Unpack the Inventory-Only module package by running the following command, using the Linux package as an example, from the directory in which the package is located:
 

```
tar -zxvf zenumia-10.1.0-linux-x86.tar.gz
```
- 7 Install the Inventory-Only module by running the following command, using the Linux package as an example, from the directory in which the file is located:
 

```
./zenumia-install.sh -s <server>
```

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

The installation program requires no user interaction. When it is finished, the Inventory-Only module is started and the device is added to the Inventoried devices page in ZENworks Control Center (*Devices* tab > *Inventoried* tab > *Workstations* or *Servers* folder).
- 8 Delete the directory created in [Step 3](#) and its contents.

## 9.3 Installing on NetWare

- 1 Make sure you've downloaded `ZENworks_Adaptive_Agent_Netware.zip` to a device that has access to the target NetWare server. If you haven't, see [Section 9.1, "Downloading the Module from a ZENworks Server,"](#) on page 81.
- 2 Extract `ZENworks_Adaptive_Agent_Netware.zip` to `sys:\temp\zen_aa` on the target NetWare server.
- 3 Enter the following command at the NetWare console to start the install:

```
sys:\temp\zen_aa\install ZENworks_Server_IP_Address
```

For example:

```
sys:\temp\zen_aa\install 123.456.78.90
```

The Inventory-Only module files are copied to `sys:\zenworks\zaa` and `zenaa.nlm` is loaded.

If `zenaa.nlm` is not loaded, enter the following command:

```
load zenaa
```

The device is added to the Inventoried devices page in ZENworks Control Center (*Devices* tab > *Inventoried* tab > *Workstations* or *Servers* folder).

## 9.4 Installing on Windows

- 1 Make sure you've downloaded `ZENworks_Unmanaged_Inventory.exe` to the target Windows device. If you haven't, see [Section 9.1, "Downloading the Module from a ZENworks Server,"](#) on page 81.
- 2 At a command prompt, run `ZENworks_Unmanaged_Inventory.exe` to launch the installation program.

The installation program requires no user interaction. When it is finished, the Inventory-Only module is started and the device is added to the Inventoried devices page in ZENworks Control Center (*Devices* tab > *Inventoried* tab > *Workstations* or *Servers* folder).

## 9.5 Installing on Macintosh OS X

- 1 Make sure you've downloaded the `ZenumiaInstall.dmg` disk image to the target Macintosh device. If you haven't, see [Section 9.1, "Downloading the Module from a ZENworks Server,"](#) on page 81.
- 2 Extract `zenumia.pkg` from the disk image to a writable location (for example, the desktop). Do not run the installation package from the disk image.
- 3 Double-click `zenumia.pkg` to launch the installation package.
- 4 If a message appears telling you a program needs to run to determine whether the package can be installed, click *Continue*.
- 5 Click *Continue* until you reach the Select Destination page.
- 6 Select a destination volume, then click *Continue* to display the Installation Type page.
- 7 Click *Install*.
- 8 When prompted to authenticate, enter a username and password for the target device, then click *OK*.

The installation begins. The `servername.txt` file opens in a TextEdit window, containing text that asks you to enter the name of a ZENworks Server.

- 9 On the bottom line of the text file, enter the IP address or DNS name of the ZENworks Server you want the device to communicate with.

- 10 Save the file and close the window.

The client files are installed.

If you are distributing the module to multiple devices, you can create an options file to include with the package. With the options file installed, the TextEdit window doesn't appear, and you can skip this step. For information on creating an options file, see [Customizing the Installer Options File](#) below.

- 11 When the installation is finished, click *Close*.

The Inventory-Only module is started and the device is added to the Inventoried devices page in ZENworks Control Center (*Devices* tab > *Inventoried* tab > *Workstations* or *Servers* folder).

## Customizing the Installer Options File

When you need to install the Inventory-Only module on a number of devices, and you want them to connect to the same ZENworks Server, you can create an options file that contains the name of the ZENworks Server. This causes the installation package to not prompt for the ZENworks Server name by launching the `servername.txt` file.

The options file is created automatically when you install the module on a device. If you want remaining devices to use the same options file, you can simply distribute the copy of the package you used to install the Collection Client.

To create a different options file:

- 1 Open a text editor other than TextEdit and enter the following line:

```
-s ZENworks_Server_name
```

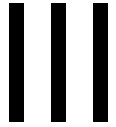
If your Macintosh devices are unable to resolve the DNS name of your ZENworks Server, you can use the following IP address:

```
-s 192.168.3.39
```

- 2 Save the text file as `options` (with no extension).
- 3 Make sure that the text file was saved as simple text.
- 4 Control-click the `zenumia.pkg` file and select *Get Info*. Make sure that the permissions are set to Read & Write.
- 5 Copy the text file into the `zenumia.pkg` file.

You can now use the package file without the TextEdit window appearing as part of the installation.

# Appendixes



- ♦ [Appendix A, “Schedules,” on page 87](#)
- ♦ [Appendix B, “Configuring NMAP for ZENworks,” on page 91](#)



# Schedules

# A

The following schedules are available for discovery and deployment tasks:

- ♦ [Section A.1, “Now,” on page 87](#)
- ♦ [Section A.2, “No Schedule,” on page 87](#)
- ♦ [Section A.3, “Date Specific,” on page 87](#)
- ♦ [Section A.4, “Recurring,” on page 88](#)

## A.1 Now

Runs the task immediately after completing the task wizard.


## A.2 No Schedule

Indicates that no schedule has been set. The task does not run until a schedule is set or it is manually launched. This is useful if you want to create the task and come back to it later to establish the schedule or run it manually.

## A.3 Date Specific

The *Date Specific* scheduling option lets you specify one or more dates on which to run the task.

### A.3.1 Start Dates

Click  to display a calendar you can use to select a date for the task. You can add multiple dates one at a time.

### A.3.2 Run Event Every Year

Select this option to run the task every year on the dates shown in the *Start Date(s)* list.

### A.3.3 Select When Schedule Execution Should Start

Select one of the following options:

- ♦ **Start Immediately at Start Time:** Starts the task at the time you specify in the *Start Time* field.
- ♦ **Start at a Random Time between Start Time and End Time:** Starts the task at a randomly selected time between the time you specify in the *Start Time* and *End Time* fields. You can use this option to avoid possible network overload from concurrently scheduled tasks.

### A.3.4 Use Coordinated Universal Time (UTC)

The Start Time is converted to Universal Coordinated Time (UTC). Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted.

For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you don't select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours.

## A.4 Recurring

The *Recurring* scheduling option lets you repeat the task at a specified interval.

### A.4.1 Days of the Week

This schedule lets you specify the days during the week that you want the event to run. The event is run on these same days each week.


Select *Days of the Week*, then fill in the following fields:

- ♦ **Sun ... Sat:** Specifies the days of the week you want to run the event.
- ♦ **Start Time:** Specifies the time you want to run the event.
- ♦ **Use Coordinated Universal Time:** The Start Time is converted to Universal Coordinated Time (UTC). Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted. For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you don't select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours.
- ♦ **Start at a Random Time between Start Time and End Time:** Starts the event at a randomly selected time between the time you specify in the *Start Time* and *End Time* fields. You can use this option to avoid possible network overload from concurrently scheduled events.
- ♦ **Restrict Schedule Execution to the Following Date Range:** Limits running the event to the time period specified by the starting and ending dates.

### A.4.2 Monthly

This schedule lets you specify one or more days during the month to run the event.

Select *Monthly*, then fill in the following fields:

- ♦ **Day of the Month:** Specifies the day of the month to run the event. Valid entries are 1 through 31. If you specify 29, 30, or 31 and a month does not have those days, the event does not run that month.
- ♦ **Last Day of the Month:** Runs the event on the last day of the month, regardless of its date (28, 30, or 31).
- ♦ **First Sunday:** Specifies a specific day of a week. For example, the first Monday or the third Tuesday. Click  to add multiple days.
- ♦ **Start Time:** Specifies the time you want to run the event.
- ♦ **Use Coordinated Universal Time:** The Start Time is converted to Universal Coordinated Time (UTC). Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted. For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you don't select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours.

- ♦ **Start at a Random Time between Start Time and End Time:** Starts the event at a randomly selected time between the time you specify in the Start Time and End Time boxes. You can use this option to avoid possible network overload from concurrently scheduled events.
- ♦ **Restrict Schedule Execution to the Following Date Range:** Limits running of the event to the time period specified by the starting and ending dates.

### A.4.3 Fixed Interval

This schedule lets you specify an interval between days to run the event. For example, you can run the event every 14 days.

Select *Fixed Interval*, then fill in the following fields:

- ♦ **Months, Weeks, Days, Hours, Minutes:** Specifies the interval between times when the event is run. You can use any combination of months, weeks, days, hours, and minutes. For example, both *7 days, 8 hours* and *1 week, 8 hours* provide the same schedule.
- ♦ **Start Date:** Specifies the initial start date for the interval.
- ♦ **Start Time:** Specifies the initial start time for the interval.
- ♦ **Use Coordinated Universal Time:** The Start Time is converted to Universal Coordinated Time (UTC). Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted. For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you don't select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours.
- ♦ **Restrict Schedule Execution to the Following Date Range:** Limits running of the event to the time period specified by the start date, end date, and end time.



# Configuring NMAP for ZENworks

# B

Network discovery is done by the ZENloader module, which runs with zenworks as the username, and the nmap command with the `-O` option. However, the nmap command needs root privileges to successfully execute. Hence, the nmap discovery fails when it runs with zenworks as the username. It is not recommended to run ZENloader with root as the username. The solution is to enable the zenworks user to run nmap for discovery with root privilege by configuring the NMAP for ZENworks®.

To configure NMAP for ZENworks, do the following on the Linux Primary Server:

- 1 Log in as a root.
- 2 Enter the `visudo` command to open the sudo user configuration file in a vi editor.

---

**TIP:** When you open the sudo configuration file in a vi editor, the editor also validates the file to ensure that correct syntax are used.

---

- 3 Comment following lines by typing “#” at the beginning of lines:  

```
Defaults targetpw      # ask for the password of the target user i.e.  
root  
ALL ALL=(ALL) ALL # WARNING! Only use this together with 'Defaults  
targetpw'!
```
- 4 Add `zenworks ALL=(ALL) NOPASSWD:/usr/bin/nmap` after the following lines:  

```
# User privilege specification  
root    ALL=(ALL) ALL
```
- 5 Exit the editor saving changes.
- 6 Change the user to zenworks by entering the `su - zenworks` command.
- 7 Enter `/usr/bin/nmap -O <any_existing_system_ip/host_name>`.