

---

# ZENworks® 11 Support Pack 3

## Discovery, Deployment, and Retirement Reference

December 2014

## 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 © 2007-2014 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.

1800 South Novell Place

Provo, UT 84606

U.S.A.

[www.novell.com](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	11
1.4 LDAP Discovery Technology	16
1.5 Advertised Devices	17
1.6 Discovered Devices	17
1.7 Deployable Devices	18
<b>2 Discovering Devices By Using IP Addresses</b>	<b>19</b>
2.1 Configuring Discovery Settings	19
2.2 Designating a Discovery and Deployment Proxy Server	23
2.2.1 Designating a Windows Proxy Server	23
2.2.2 Designating a Linux Proxy Server	24
2.3 Creating an IP Discovery Task	25
<b>3 Discovering Devices in LDAP Directories</b>	<b>35</b>
<b>4 Importing Devices from CSV Files</b>	<b>41</b>
<b>5 Advertised Discovery</b>	<b>43</b>
5.1 Configuring the Advertised Discovery Settings	43
5.2 Discovering Advertised Devices	45
<b>6 Viewing or Updating Device Details</b>	<b>47</b>
<b>Part II ZENworks Adaptive Agent Deployment</b>	<b>49</b>
<b>7 Basic Concepts</b>	<b>51</b>
7.1 Deployment Methods	51
7.2 Deployment Packages	51
7.3 Adaptive Agent Versus Inventory-Only Module	52
<b>8 Managing Deployment Packages</b>	<b>55</b>
8.1 Package Types and Architectures	55
8.1.1 Package Types and Architectures for Windows	55
8.1.2 Package Types and Architectures for Linux	56
8.1.3 Package Types and Architectures for Macintosh	57

8.2	Default System Packages Versus Custom Packages	57
8.3	Customizing Packages	58
8.4	Rebuilding Packages	61
8.4.1	Rebuilding the Default Packages	62
8.4.2	Rebuilding the Custom Packages	62
<b>9</b>	<b>Registering Devices</b>	<b>63</b>
9.1	What Happens During Registration	63
9.2	Creating Registration Keys and Rules	64
9.2.1	Creating a Registration Key	64
9.2.2	Creating a Registration Rule	67
9.3	Modifying the Device Naming Template Used During Registration	72
9.4	Enabling Dynamic Renaming of Devices During Registration	73
9.4.1	Enabling the Setting at the Management Zone	74
9.4.2	Enabling the Setting for a Device Folder	75
9.5	Reconciling Devices with existing Device Objects During Registration	77
9.5.1	Creating Dummy Device Objects	77
9.5.2	Reconciling the Devices	79
9.5.3	Importing Managed Devices	86
9.6	Disabling the Use of Registration Rules	88
9.7	Manually Registering a Device	90
9.7.1	Performing an Initial Registration	91
9.7.2	Reregistering a Device with an Additional Registration Key	91
9.8	Unregistering a Device	91
<b>10</b>	<b>Deploying the ZENworks Adaptive Agent</b>	<b>93</b>
10.1	Coexisting with the ZENworks Desktop Management Agent	93
10.2	Customizing the Agent Features	94
10.2.1	Customizing Features before Deployment	95
10.2.2	Customizing Features after Deployment	97
10.3	Configuring the Agent Security	97
10.3.1	Customizing Security before Deployment	97
10.3.2	Customizing Security after Deployment	101
10.4	Changing the Target Installation Directory	101
10.5	Using a Task to Deploy the Agent	101
10.5.1	Prerequisites for Deploying to Windows Devices	102
10.5.2	Prerequisites for Deploying to Linux Devices	106
10.5.3	Deploying to a Discovered Device	107
10.5.4	Deploying to a Non-Discovered Device	117
10.6	Manually Deploying the Agent on Windows	127
10.7	Reboot-less Agent	129
10.8	Manually Deploying the Agent on Linux	129
10.9	Manually Deploying the Agent on a Macintosh Device	131
10.10	Agent Deployment in VDI environment	132
10.11	Agent Deployment on Citrix Server	133
10.12	Package Options for Windows, Linux, and Macintosh	133
10.13	Installing the Agent as an Add-on Product in SLES/SLED	134
10.13.1	Installing the ZENworks Agent on SLES/SLED 10	134
10.13.2	Installing the ZENworks Agent on SLES/SLED 11	135
10.14	Installing the Agent by Using YUM on RHEL	136

<b>11 Uninstalling the Agent</b>	<b>139</b>
<b>12 Deploying the Inventory-Only Module</b>	<b>141</b>
12.1 Downloading the Module from a ZENworks Server	141
12.2 Installing on Linux	142
12.3 Installing on NetWare	143
12.4 Installing on Windows	143
12.5 Installing on Macintosh OS X	144
12.5.1 Editing the Inventory Configuration File and Refreshing the zenumia Process	144
12.6 Uninstalling the Inventory-Only Module	145
12.7 Upgrading Inventory-Only Agent	145
12.8 Re-registering Inventory-Only Devices	145
12.8.1 Re-registering Inventory-Only Devices for All Platforms	146
12.8.2 Re-registering Inventory-Only Devices for Individual Platforms	146
12.9 Running Scannow on an Inventory-Only Device	147
<b>Part III Device Removal and Retirement</b>	<b>149</b>
<b>13 Deleting Devices from Your ZENworks System</b>	<b>151</b>
<b>14 Retiring or Unretiring Devices</b>	<b>153</b>
<b>Part IV Appendixes</b>	<b>157</b>
<b>A Viewing the Predefined Reports</b>	<b>159</b>
<b>B Schedules</b>	<b>161</b>
B.1 Now	161
B.2 No Schedule	161
B.3 Date Specific	161
B.3.1 Start Dates	161
B.3.2 Run Event Every Year	161
B.3.3 Select When Schedule Execution Should Start	161
B.3.4 Use Coordinated Universal Time (UTC)	162
B.4 Recurring	162
B.4.1 Days of the Week	162
B.4.2 Monthly	162
B.4.3 Fixed Interval	163
<b>C Configuring NMAP for ZENworks</b>	<b>165</b>
<b>D Troubleshooting Discovery, Deployment, and Retirement</b>	<b>167</b>
<b>E Documentation Updates</b>	<b>175</b>



---

# About This Guide

This *Novell ZENworks 11 SP3 Discovery, Deployment, and Retirement Reference* helps you add devices to your ZENworks Management Zone 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 49](#)
- ♦ [Part III, “Device Removal and Retirement,” on page 149](#)
- ♦ [Part IV, “Appendixes,” on page 157](#)

## Audience

This guide is intended for anyone who configures and manages 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.

## Additional Documentation

ZENworks 11 SP3 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 [ZENworks 11 SP3 documentation web site \(http://www.novell.com/documentation/zenworks113\)](http://www.novell.com/documentation/zenworks113).





---

# 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 19](#)
- ◆ [Chapter 3, “Discovering Devices in LDAP Directories,” on page 35](#)
- ◆ [Chapter 4, “Importing Devices from CSV Files,” on page 41](#)
- ◆ [Chapter 5, “Advertised Discovery,” on page 43](#)
- ◆ [Chapter 6, “Viewing or Updating Device Details,” on page 47](#)



---

# 1 Basic Concepts

Device discovery is the process of adding workstation and server information to the Novell ZENworks 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 11](#)
- ♦ [Section 1.4, “LDAP Discovery Technology,” on page 16](#)
- ♦ [Section 1.5, “Advertised Devices,” on page 17](#)
- ♦ [Section 1.6, “Discovered Devices,” on page 17](#)
- ♦ [Section 1.7, “Deployable Devices,” on page 18](#)

## 1.1 Discovery Methods

There are four 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 eDirectory or Microsoft Active Directory 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.
- ♦ **Advertised discovery:** Use the ZENworks discovery engine to collect information about devices that have the ZENworks preagent installed.

## 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. LDAP discovery requires Novell eDirectory or Microsoft Active Directory to search for devices.

## 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 19](#)) or override the settings in the discovery task.

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

---

**NOTE:** We do not support using SSH or ZENworks ping to discover Macintosh devices.

---

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 19](#).

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. If a high priority discovery technology is successful and returns the information, then the other lower priority discovery technologies are aborted for better performance. For example, if WinAPI or WMI is successful, then MAC address and NMAP technologies are aborted.

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.

- ◆ 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.

The following table provides detailed information about the IP discovery technologies:

**Table 1-1** IP Discovery Technologies

IP Discovery Technology	Functionality	Requirements	Prerequisites
WMI (Windows Management Instrumentation)	<p>WMI is the infrastructure for management data and operations on Windows-based operating systems. Discovery issues a remote request to the WMI service on the devices identified by the IP-based discovery task to obtain information. Retrieves the OS type and version, MAC address, Network Adapters, and CPU details of the device.</p> <p>For more information on WMI, see the <a href="http://msdn.microsoft.com/en-us/library/aa384642%28VS.85%29.aspx">MSDN Web site (http://msdn.microsoft.com/en-us/library/aa384642%28VS.85%29.aspx)</a>.</p>	<p>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 <a href="#">Section 2.2, “Designating a Discovery and Deployment Proxy Server,”</a> on page 23.</p>	<ul style="list-style-type: none"> <li>◆ Microsoft Windows Management Instrumentation Service to be installed and running on the target Windows device.</li> <li>◆ Credentials of an administrator account on the target device should be specified as Windows credentials in the discovery task. This is required for connecting to the WMI Service.</li> <li>◆ To authenticate by using the Windows credentials, set the value of the <i>Network access: Sharing and security model for local accounts</i> Local Security setting to <i>Classic - local users authenticate as themselves</i>. For more information on how to configure the Local Security settings, see <a href="#">“Enabling Classic File Sharing”</a> on page 104.</li> <li>◆ Since the Remote WMI connection establishes a RPC connection with the target Windows device, the TCP ports 139 and 445 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 <a href="#">“Enabling File and Printer Sharing through Windows Firewall”</a> on page 103.</li> </ul>

IP Discovery Technology	Functionality	Requirements	Prerequisites
WinAPI	Issues a request to the registry on the devices identified by the IP-based discovery task to retrieve the OS type and version, and CPU details.	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 <a href="#">Section 2.2, "Designating a Discovery and Deployment Proxy Server," on page 23.</a>	<ul style="list-style-type: none"> <li>◆ Microsoft Remote Registry Service to be installed and running on the target Windows device.</li> <li>◆ Credentials of an administrator account with read privileges on the Windows registry of the target device should be specified as Windows credentials in the discovery task. This is required for connecting to the Remote Registry Service.</li> <li>◆ The <i>File and Printer Sharing for Microsoft Networks</i> option must be enabled. For more information, see <a href="#">"Enabling File and Printer Sharing for Microsoft Networks" on page 102.</a></li> <li>◆ To authenticate by using the Windows credentials, set the value of the <i>Network access: Sharing and security model for local accounts</i> Local Security setting to <i>Classic - local users authenticate as themselves</i>. For more information on how to configure the Local Security settings, see <a href="#">"Enabling Classic File Sharing" on page 104.</a></li> <li>◆ Since the Remote Registry connection establishes a RPC connection with the target Windows device, the TCP ports 139 and 445 must be allowed by the Windows Firewall of the target device. For more information on how to open these ports, see <a href="#">"Enabling File and Printer Sharing through Windows Firewall" on page 103.</a> If the target device is in a different subnet than the Windows Proxy or the Primary server running the task, then the scope of the Firewall exception should include them.</li> </ul>

IP Discovery Technology	Functionality	Requirements	Prerequisites
MAC Address	<p>Retrieves the MAC Address of the discovered device. 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.</p> <p>The MAC Address discovery gets only the MAC address of the device and does not give any OS information.</p>		<ul style="list-style-type: none"> <li>◆ For the <code>arp</code> command to be successful, the target devices must reside in the same network as the ZENworks Server that performs the discovery request.</li> <li>◆ For the <code>ping</code> command to be successful, the incoming ICMP echo requests (<code>ping</code>) must be enabled on the device, and the ICMP echo requests and echo responses must be allowed on the network.</li> </ul>
NMAP	<p>Uses NMAP (Network Mapper) to retrieve the OS type and version details of the devices identified by the IP-based discovery task.</p> <p><b>IMPORTANT:</b> NMAP has certain known limitations. For more information on these limitations, see the <a href="http://www.nmap.org">NMAP Web site (http://www.nmap.org)</a>.</p>		<ul style="list-style-type: none"> <li>◆ NMAP must be installed on the ZENworks Server that is processing the discovery request.</li> </ul> <p>NMAP is freely available from <a href="http://www.insecure.org">InSecure.org (http://www.insecure.org)</a>. For more information on how to configure NMAP for ZENworks, see <a href="#">Appendix C, "Configuring NMAP for ZENworks,"</a> on page 165.</p>
ZENworks	<p>Issues a request to the ZENworks Adaptive Agent or ZENworks preagent on the devices identified by the IP-based discovery task. If the device has the ZENworks Adaptive Agent, the agent responds with the OS type and version, MAC Address, Network Adapters, CPU, managed device GUID, Management Zone GUID, Management Zone name, Adaptive Agent version, disk space, and memory details. If the device has the ZENworks preagent installed, the preagent responds with the OS type, CPU, disk space, memory, and the GUID details that should be used to register the device in the Management Zone.</p>		<ul style="list-style-type: none"> <li>◆ The preagent is only installed on OEM devices or on devices whose registration was removed from the zone.</li> </ul>

IP Discovery Technology	Functionality	Requirements	Prerequisites
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. Retrieves the OS type and version, MAC address, Network Adapters, and CPU details.	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 23.	<ul style="list-style-type: none"> <li>◆ To query a device using SNMP, the device must have SNMP enabled.</li> <li>◆ The SNMP community string must be specified as a SNMP credential in the Discovery Task.</li> <li>◆ SNMP uses the UDP Port 161. The firewall must be configured to allow access through this port.</li> </ul>
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 retrieves the OS type, OS or Kernel version, CPU, Network Adapters, and memory details.		<ul style="list-style-type: none"> <li>◆ 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.</li> </ul> <p>For more information on how to open port 22, see <a href="#">“Prerequisites for Deploying to Linux Devices”</a> on page 106.</p>

## 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.

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.



## 1.5 Advertised Devices

The ZENworks discovery engine allows you to discover devices that have the ZENworks preagent installed, such as OEM devices or devices whose registration was removed from the Management Zone. Only those devices that have the preagent installed respond to an advertised discovery; devices that have the ZENworks Adaptive Agent do not respond to an advertised discovery.

## 1.6 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
<b>Discovered</b>		
📁		
Type	Discovered	
📁 <a href="#">All Types</a>	0	
📁 <a href="#">Servers</a>	0	
📁 <a href="#">Workstations</a>	0	
📁 <a href="#">Printers</a>	0	
📁 <a href="#">DRAC Devices</a>	0	
📁 <a href="#">Intel® AMT Devices</a>	0	
📁 <a href="#">Network Equipment</a>	0	
📁 <a href="#">Thin Clients</a>	0	
📁 <a href="#">Embedded Workstations</a>	0	
📁 <a href="#">Other Devices</a>	0	
📁 <a href="#">Unknown Devices</a>	0	
📁 <a href="#">Deployable Types</a>	0	
📁 <a href="#">Devices created via ZENworks Migration</a>	0	
📁 <a href="#">Devices created via ZENworks Asset Management Migration</a>	0	

Each discovered device 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.
- ♦ **DRAC Devices:** All discovered devices that have been identified as Dell Remote Access Controllers (DRAC).

- ♦ **Intel AMT Devices:** All discovered devices that have the Intel Active Management Technology (AMT) capability.
- ♦ **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.
- ♦ **Embedded Workstations:** All discovered devices that have been identified as embedded workstations.
- ♦ **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 the agent is supported on these devices. For more information on list of supported devices, see "Managed Device Requirements" in *ZENworks 11 SP3 System Requirements*.
- ♦ **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.

## 1.7 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)*

Name	IP Address	Operating System	Initial Discovery	Deployment Status
<a href="#">blr-nrm-doc14.labs.blr.novell.com</a>	164.99.93.61	Unknown OS	Aug 31, 2010 3:49 PM	Inactive
<a href="#">RNIKASH</a>	164.99.93.87	Microsoft Windows XP	Aug 30, 2010 1:32 PM	Inactive
<a href="#">SANJANA-202B2B0</a>	164.99.93.127	Unknown OS	Aug 31, 2010 3:56 PM	Inactive

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.

# 2 Discovering Devices By Using IP Addresses

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 19](#)
- ◆ [Section 2.2, “Designating a Discovery and Deployment Proxy Server,” on page 23](#)
- ◆ [Section 2.3, “Creating an IP Discovery Task,” on page 25](#)

## 2.1 Configuring Discovery Settings

IP discoveries use the following configuration settings that can be modified, if necessary:

- ◆ Number of discoveries that can be processed concurrently (default is 5)
- ◆ IP subnets or address ranges that are to be excluded from the discovery
- ◆ 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	Asset Management	System Updates	Locations	Subscriptions
<b>Management Zone Settings</b>							
Content							
<b>Device Management</b>							
<b>Category</b>	<b>Description</b>						
<a href="#">Local Device Logging</a>	Enable and configure local logging of warnings and errors encountered by managed devices.						
<a href="#">Device Refresh and Removal Schedule</a>	Configure the device refresh interval.						
<a href="#">ZENworks Agent</a>	ZENworks Agent Configuration.						
<a href="#">System Update Agent</a>	Configure system update behavior on ZENworks Agents.						
<a href="#">Registration</a>	Configure registration settings.						
<a href="#">ZENworks Explorer Configuration</a>	Configure the behavior of the ZENworks Explorer on managed devices.						
<a href="#">System Variables</a>	Configure system variables.						
<a href="#">Preboot Services</a>	Configure Preboot Services.						
<a href="#">Primary User</a>	Configure the setting for how the primary user is determined.						
<a href="#">Primary Workstation</a>	Configure the setting for how the primary workstation is determined.						
<a href="#">Dynamic Group Refresh Schedule</a>	Configure dynamic group refresh schedule.						
<a href="#">Wake-on-LAN</a>	Configure the Wake-on-LAN settings.						
<a href="#">Power Management Settings</a>	Configure the schedule for the power management of Intel AMT devices.						
<a href="#">Remote Management</a>	Enable and configure remote management.						
<b>Discovery and Deployment</b>							
<b>Event and Messaging</b>							
<b>Infrastructure Management</b>							
<b>Inventory</b>							
<b>Reporting Services</b>							
<b>Endpoint Security Management</b>							
<b>Asset Management</b>							
<b>Patch Management</b>							

- 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:

**Discovery** [X]

Configure settings related to discovering new devices.

---

**Discovery Process Settings** [^]

Set the maximum number of threads to use for concurrent device discoveries.

Maximum Concurrent discoveries

Discovery technologies:

MAC Address    NMAP    SNMP  
 SSH    WinAPI    WMI  
 ZENworks

---

**IP Addresses to be Excluded** [v]

---

**Network Discovery Settings** [v]

[OK]   [Apply]   [Reset]   [Cancel]

**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.

For more information on the IP discovery process, see [Section 1.3, “IP Discovery Technologies,” on page 11](#).

**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.

For detailed information about each technology, see [Section 1.3, “IP Discovery Technologies,” on page 11](#).

- 4 In the IP Addresses to be Excluded panel, specify the IP subnets or address ranges to be excluded from the discovery.

**NOTE:** All the discovery tasks inherit the IP address ranges specified at the Management Zone level. If the IP address range is specified at a task level, the combined ranges of the Management Zone and discovery task are excluded from the discovery.

The screenshot shows a dialog box titled "Discovery" with a close button (X) in the top right corner. Below the title bar is a subtitle: "Configure settings related to discovering new devices." The main content area is divided into sections by expandable headers. The "Discovery Process Settings" header is collapsed. The "IP Addresses to be Excluded" header is expanded, showing a text area with the instruction: "Enter the IP subnets and/or address ranges to be excluded from the search." Below this is a "Range" label above a text input field. To the right of the input field is an "Add" button. Below the input field is a list box labeled "Selected IP Ranges:" which is currently empty. To the right of the list box are "Import" and "Remove" buttons. At the bottom of the dialog box is the "Network Discovery Settings" header, which is collapsed. At the very bottom are four buttons: "OK", "Apply", "Reset", and "Cancel".

You can manually add the IP addresses to be excluded or import the IP addresses to be excluded from a CSV file.

- ◆ To manually add the IP address to be excluded:
  1. In the *Range* field, enter the IP address range in one of the following formats:
    - xxx.xxx.xxx.xxx:** Standard dotted-decimal notation for a single address. For example, 123.45.167.100.
    - xxx.xxx.xxx.xxx - xxx.xxx.xxx.xxx:** Standard dotted-decimal notation for a range of addresses. 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. To add the IP address range to the *Selected IP Ranges* list, click *Add*.
- ◆ To use a CSV list to import an IP address to be excluded:
  1. In the *Selected IP Ranges* list, click *Import*.

The Import CSV File dialog box is displayed.

2. Click *Browse* to browse for and select a file that contains a comma-separated or columnar list of IP addresses.
3. Click *OK*.

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

The screenshot shows the 'Discovery' dialog box with the 'Network Discovery Settings' panel expanded. The 'Ping Settings' section includes: Initial ping timeout: 200 ms, Maximum ping retries: 1, Increment ping timeout on retries by: 200 ms, and an unchecked checkbox for 'Perform name lookups'. The 'SNMP Settings' section includes: Initial SNMP timeout: 500 ms, Maximum SNMP retries: 1, and Increment SNMP timeout on retries by: 1000 ms. The 'SSH Settings' section includes: SSH connection timeout: 5000 ms. At the bottom are buttons for 'OK', 'Apply', 'Reset', and 'Cancel'.

**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.

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

- ♦ **SSH connection timeout:** Specifies how long the discovery technology waits to establish a SSH connection with the Linux device.

6 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 Windows managed 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.

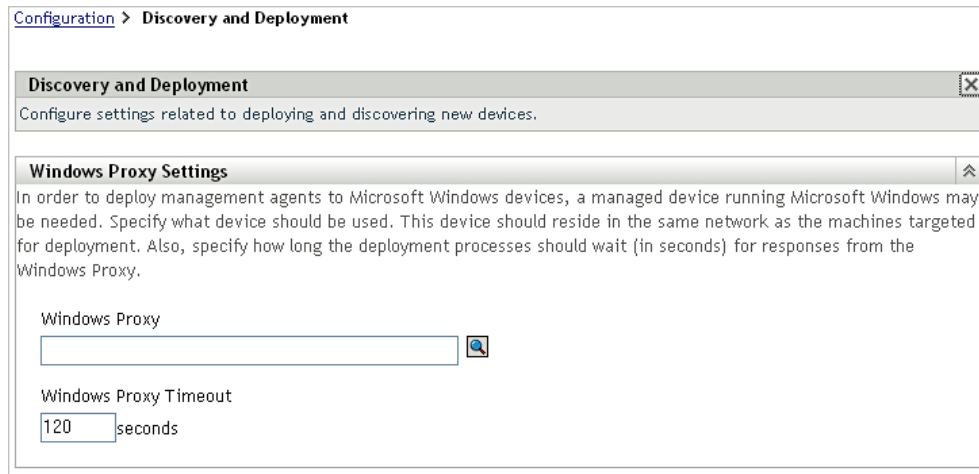
If you have only Linux servers in your environment, you must first manually install ZENworks Adaptive Agent on a Windows device by downloading the agent from [https://IP\\_address\\_of\\_the\\_ZENworks\\_Server/zenworks-setup](https://IP_address_of_the_ZENworks_Server/zenworks-setup), then designate the device as a proxy for discovery and deployment tasks.

### 2.2.1 Designating a Windows Proxy Server


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

Configuration	Registration	System Information	Asset Inventory	Asset Management	System Updates	Locations	Subscriptions
Management Zone Settings							
Content							
Device Management							
Category		Description					
<a href="#">Local Device Logging</a>		Enable and configure local logging of warnings and errors encountered by managed devices.					
<a href="#">Device Refresh and Removal Schedule</a>		Configure the device refresh interval.					
<a href="#">ZENworks Agent</a>		ZENworks Agent Configuration.					
<a href="#">System Update Agent</a>		Configure system update behavior on ZENworks Agents.					
<a href="#">Registration</a>		Configure registration settings.					
<a href="#">ZENworks Explorer Configuration</a>		Configure the behavior of the ZENworks Explorer on managed devices.					
<a href="#">System Variables</a>		Configure system variables.					
<a href="#">Preboot Services</a>		Configure Preboot Services.					
<a href="#">Primary User</a>		Configure the setting for how the primary user is determined.					
<a href="#">Primary Workstation</a>		Configure the setting for how the primary workstation is determined.					
<a href="#">Dynamic Group Refresh Schedule</a>		Configure dynamic group refresh schedule.					
<a href="#">Wake-on-LAN</a>		Configure the Wake-on-LAN settings					
<a href="#">Power Management Settings</a>		Configure the schedule for the power management of Intel AMT devices.					
<a href="#">Remote Management</a>		Enable and configure remote management.					
Discovery and Deployment							
Event and Messaging							
Infrastructure Management							
Inventory							
Reporting Services							
Endpoint Security Management							
Asset Management							
Patch Management							

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



- 3 Fill in the following fields:

**Windows Proxy:** Click  to browse for and select a Windows managed device (server or workstation) to be used as a Windows Proxy for performing the discovery and deployment tasks instead of a ZENworks Server. The Windows Proxy must reside in the same network as the target devices.

**Windows Proxy Timeout:** Specify the number of seconds you want the ZENworks Server to wait for a response from the Windows Proxy.

- 4 Click *OK* to save the changes.

## 2.2.2 Designating a Linux Proxy Server

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



Configuration	Registration	System Information	Asset Inventory	Asset Management	System Updates	Locations	Subscriptions
<b>Management Zone Settings</b>							
Content							
<b>Device Management</b>							
<b>Category</b>	<b>Description</b>						
<a href="#">Local Device Logging</a>	Enable and configure local logging of warnings and errors encountered by managed devices.						
<a href="#">Device Refresh and Removal Schedule</a>	Configure the device refresh interval.						
<a href="#">ZENworks Agent</a>	ZENworks Agent Configuration.						
<a href="#">System Update Agent</a>	Configure system update behavior on ZENworks Agents.						
<a href="#">Registration</a>	Configure registration settings.						
<a href="#">ZENworks Explorer Configuration</a>	Configure the behavior of the ZENworks Explorer on managed devices.						
<a href="#">System Variables</a>	Configure system variables.						
<a href="#">Preboot Services</a>	Configure Preboot Services.						
<a href="#">Primary User</a>	Configure the setting for how the primary user is determined.						
<a href="#">Primary Workstation</a>	Configure the setting for how the primary workstation is determined.						
<a href="#">Dynamic Group Refresh Schedule</a>	Configure dynamic group refresh schedule.						
<a href="#">Wake-on-LAN</a>	Configure the Wake-on-LAN settings						
<a href="#">Power Management Settings</a>	Configure the schedule for the power management of Intel AMT devices.						
<a href="#">Remote Management</a>	Enable and configure remote management.						
<b>Discovery and Deployment</b>							
Event and Messaging							
Infrastructure Management							
Inventory							
Reporting Services							
Endpoint Security Management							
Asset Management							
Patch Management							

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

- Fill in the following fields:
  - Linux Proxy:** Click to browse for and select a Linux managed device (server or workstation) to be used as a Linux Proxy for performing the discovery and deployment tasks instead of a ZENworks Server. The Linux Proxy must reside in the same network as the target devices.
  - Linux Proxy Timeout:** Specify the number of seconds you want the ZENworks Server to wait for a response from the Linux Proxy.
- 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	<p>Select <i>IP Discovery Task</i>.</p> <p>Specify a name for the task. The name cannot include any of the following invalid characters: / \ * ? : " ' &lt; &gt;   ` % ~</p>
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>For more information about each technology, see <a href="#">Section 1.3, “IP Discovery Technologies,”</a> on page 11.</p>

Wizard Page	Details
Enter IP Discovery Settings page > <i>Range</i> field	<p>To specify a range of IP addresses for the discovery task:</p> <ol style="list-style-type: none"> <li>In the <i>Range</i> field, specify an IP address range using one of the following formats: <ul style="list-style-type: none"> <li><b>xxx.xxx.xxx.xxx:</b> Standard dotted-decimal notation for a single address. For example, 123.45.167.100.</li> <li><b>xxx.xxx.xxx.xxx - xxx.xxx.xxx.xxx:</b> Standard dotted-decimal notation for a range of addresses. For example, 123.45.167.100 - 123.45.167.125.</li> <li><b>xxx.xxx.xxx.xxx/n:</b> 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 <i>Selected IP Ranges</i> list (see the next step), it is automatically expanded to show the range of addresses in dotted-decimal notation.</li> </ul> <p>You are recommended to specify an IP address range that does not contain more than 50,000 devices. A task that has a large IP address range does not get started. For more information, see the troubleshooting scenario <a href="#">“Discovery task remains in a pending state if it has a large IP address range” on page 170</a>.</p> </li> <li>To add an IP address range to the <i>Selected IP Ranges</i> list, click <i>Add</i>.</li> <li>(Optional) To exclude the IP subnets or address ranges from the discovery, click <i>Exclude</i>. <ul style="list-style-type: none"> <li>The Excluded Addresses dialog box is displayed.</li> <li>For more information on how to exclude the IP subnets or address ranges, see <a href="#">“Device Discovery” on page 9</a>.</li> </ul> </li> <li>To add additional ranges, repeat Step 1 and Step 2.</li> </ol>

Wizard Page	Details
Enter IP Discovery Settings page > Excluded Addresses dialog box	<p>To specify the IP subnets or address ranges to be excluded from the IP discovery. These ranges are added to the ranges specified in the Management Zone, and the combined ranges are excluded while running the discovery task.</p> <p>To specify the IP subnets or address ranges to be excluded from the discovery, do one of the following:</p> <ul style="list-style-type: none"> <li>◆ Manually add the IP address to be excluded: <ol style="list-style-type: none"> <li>1. In the <i>Range</i> field, enter the IP address range using one of the following formats: <p><b>xxx.xxx.xxx.xxx</b>: Standard dotted-decimal notation for a single address. For example, 123.45.167.100.</p> <p><b>xxx.xxx.xxx.xxx - xxx.xxx.xxx.xxx</b>: Standard dotted-decimal notation for a range of addresses. For example, 123.45.167.100 - 123.45.167.125.</p> <p><b>xxx.xxx.xxx.xxx/n</b>: 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 <i>Selected IP Ranges</i> list (see the next step), it is automatically expanded to show the range of addresses in dotted-decimal notation.</p> </li> <li>2. To add an IP address range to the <i>Selected IP Ranges</i> list, click <i>Add</i>.</li> </ol> </li> <li>◆ Use a CSV file to import an IP address to be excluded: <ol style="list-style-type: none"> <li>1. In the <i>Selected IP Ranges</i> list, click <i>Import</i>. The Import CSV File dialog box is displayed.</li> <li>2. Click <i>Browse</i> to browse for and select a file that contains a comma-separated or columnar list of IP addresses.</li> <li>3. Click <i>OK</i>.</li> </ol> </li> </ul>
Enter IP Discovery Settings page > <i>Save Credentials to DataStore</i> field	<p>In order for the SSH, WMI, WinAPI, and SNMP 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>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> <p><b>NOTE:</b> Credentials are not saved in the credential vault.</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>In the <i>Credentials</i> panel, click <i>Add</i> to display the Enter Credential Information dialog box.</li> <li>In the <i>Type</i> field, select the type of credentials you are defining: <ul style="list-style-type: none"> <li><b>General:</b> Specifies credentials to be used by all discovery technologies except for SNMP.</li> <li><b>Linux:</b> Specifies credentials for the SSH technology to communicate with the SSH server on a Linux device.</li> <li><b>Windows:</b> Specifies credentials for the WMI and WinAPI technology to access the WMI service and Windows registry on a Windows device.</li> <li><b>SNMP:</b> Specifies community strings for the SNMP technology to access the SNMP service on a device. For example, <i>public</i> as the community string.</li> </ul> </li> <li>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 one of the following formats:</p> <pre>username domain_name\username username@domain_name username@fully_qualified_domain_name</pre> <p><b>NOTE:</b> Windows Server 2008 does not support the <i>username@domain_name</i> format.</p> </li> <li>If you selected <i>SNMP</i>, fill in a community string.</li> <li>Click <i>OK</i> to add the credentials to the <i>Credentials</i> panel.</li> <li>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 <i>Credentials</i> 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 B, “Schedules,” on page 161</a> or click the <i>Help</i> button for more information on 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 on discovery proxies, see <a href="#">Section 2.2, “Designating a Discovery and Deployment Proxy Server,” on page 23</a>.</p>
Select or Edit a Proxy Device page	<p>The Select or Edit a Proxy Device page lets you choose whether you want to use a proxy device to perform the discovery task.</p>

Wizard Page	Details
Select or Edit a Proxy Device page > <i>Windows Proxy</i>	<p>If you want to use a Windows Proxy instead of the Primary Server to perform the discovery tasks on Windows devices, click the <i>Windows Proxy</i> option and configure the settings in the Select Windows Proxy dialog box.</p> <p>A Windows Proxy is used to perform the following actions:</p> <ul style="list-style-type: none"> <li>◆ Enable Linux Primary Servers to perform discovery tasks that use Windows-specific discovery technologies (such as WMI, WinAPI, and SNMP).</li> <li>◆ Discover Windows devices that are in a different subnet than the Primary Server.</li> <li>◆ Discover Windows devices in a network enabled for NAT.</li> </ul> <p>Discovery through WMI, WinAPI and SNMP requires certain ports to be reachable on the target devices, so the Primary Server can send Remote Registry, WMI, or SNMP requests to the target devices. Ports are opened by adding them as an exception in the Windows Firewall configuration settings. 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 discovery is run, you need to add the IP address of the Primary Server as an exception. However, if you use a Windows Proxy in the same subnet as a target device, you do not need to change the scope of the Windows Firewall exception.</p> <p>The connection between the ZENworks Server and the Windows Proxy is secured through SSL.</p> <p><b>Override Zone Window Proxy Settings:</b> Select this option if you want to override the Windows Proxy settings configured at the Management Zone and configure new settings for the task.</p> <p><b>Windows Proxy:</b> Select a Windows managed device (server or workstation) to be used as a Windows Proxy for performing the discovery tasks instead of a ZENworks Server. The Windows Proxy must reside in the same network as the target devices.</p> <p><b>Windows Proxy Timeout:</b> Specify the number of seconds you want the ZENworks Server to wait for a response from the Windows Proxy.</p>



Wizard Page	Details
Select or Edit a Proxy Device page > <i>Linux Proxy</i>	<p>If you want to use a Linux Proxy instead of the Primary Server to perform the discovery tasks on Linux devices, click the <i>Linux Proxy</i> option and configure the settings in the Select Linux Proxy dialog box.</p> <p>A Linux Proxy is used to perform the following actions:</p> <ul style="list-style-type: none"> <li>◆ Enable Primary Servers that cannot perform discovery tasks that use Linux-specific discovery technologies like SSH.</li> <li>◆ Discover Linux devices in a different subnet than the Primary Server.</li> <li>◆ Discover Linux devices in a network enabled for NAT.</li> </ul> <p>The SSH discovery requires port 22 to be reachable in order to enable the Primary Server to connect to the target device. If the SSH port is blocked in the Network Firewall, you use a Linux managed device in the same subnet as the target device.</p> <p>The connection between the ZENworks Server and Linux Proxy is secured through SSL.</p> <p>For more information on how to open port 22, see <a href="#">“Prerequisites for Deploying to Linux Devices” on page 106</a>.</p> <p><b>Override Zone Linux Proxy Settings:</b> Select this option if you want to override the Linux Proxy settings configured at the Management Zone and configure new settings for the task.</p> <p><b>Linux Proxy:</b> Select a Linux managed device (server or workstation) to be used as a Linux Proxy for performing the discovery tasks instead of a ZENworks Server. The Linux Proxy must reside in the same network as the target devices.</p> <p><b>Linux Proxy Timeout:</b> Specify the number of seconds you want the ZENworks Server to wait for a response from the Linux Proxy.</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. If you have specified IP addresses to be excluded from a discovery task, then the discovery is not run for those IP addresses and the excluded IP addresses are not included in the *Results* tab.



# 3 Discovering Devices in LDAP Directories

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 recursively search for device in all the directories 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	<p>Select <i>LDAP Discovery Task</i>.</p> <p>Specify a name for the task. The name cannot include any of the following invalid characters: / \ * ? : " ' &lt; &gt;   ` % ~</p>
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>” on page 37.</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. <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> </li> </ol>

Wizard Page	Details
Enter LDAP Settings page > <i>Specify an LDAP Source</i> field	<p>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 <a href="#">Enter LDAP Settings page &gt; Search pre-configured LDAP source field</a> above.</p> <p>To create a new connection to an LDAP directory:</p> <ol style="list-style-type: none"> <li>Select <i>Specify an LDAP source</i>, then fill in the following fields: <ul style="list-style-type: none"> <li><b>LDAP Server:</b> Specify the IP address or DNS hostname of the server where the LDAP directory resides.</li> <li><b>LDAP Port/Use SSL:</b> The default is 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 number.</li> <li><b>Root Context:</b> 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.</li> <li><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, you should save them.</li> <li><b>Credentials:</b> Click <i>Add</i> 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.</li> </ul> <p>For Novell eDirectory access, use standard LDAP notation. For example,  <code>cn=admin_read_only,ou=users,o=mycompany</code></p> <p>For Microsoft Active Directory, use standard domain notation. For example, <code>AdminReadOnly@mycompany.com</code></p> </li> <li>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>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>Fill in the following fields: <ul style="list-style-type: none"> <li><b>Context/Group DN:</b> Click <i>Browse</i> to locate and select the context/group you want to search.</li> <li><b>Recursive Search:</b> Select this option to search all subcontexts/subgroups.</li> </ul> </li> <li>Click <i>OK</i> to save the search context/group.</li> </ol> </li> <li>If necessary, modify the LDAP search filter. By default, the filter searches for the computer objectClass or server objectClass.</li> </ol>

Wizard Page	Details
Discovery Settings page	<p>LDAP discovery retrieves the hostname, operating system type and version, and IP address of a discovered device from the LDAP source. Based on the selected discovery technologies, you can obtain the following additional information on a device:</p> <ul style="list-style-type: none"> <li>◆ ZENworks Management Status</li> <li>◆ Operating System Suites</li> <li>◆ MAC Address</li> <li>◆ Network Adapters</li> <li>◆ CPU</li> <li>◆ Memory and Disk Space</li> </ul> <p>To obtain additional information on a device:</p> <ol style="list-style-type: none"> <li>1. Select the <i>Use the IP discovery technologies to gather more information</i> option.</li> <li>2. Select <i>Override Zone Discovery Settings</i>, then select the discovery technologies.</li> <li>3. In the Credentials panel, add the credential information.</li> </ol> <p>For more information on how to add the credential information, click the <i>Help</i> button.</p>
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>For more information about the schedules, click the <i>Help</i> button.</p>
Select Primary Server page	<p>Select the ZENworks Server that you want to perform the deployment task.</p>
Select or Edit a Proxy Device page	<p>The Select or Edit a Proxy Device page lets you choose whether you want to use a proxy device to perform the discovery task.</p>

Wizard Page	Details
Select or Edit a Proxy Device page > <i>Windows Proxy</i>	<p>If you want to use a Windows Proxy instead of the Primary Server to perform the discovery tasks on Windows devices, click the <i>Windows Proxy</i> option and configure the settings in the Select Windows Proxy dialog box.</p> <p>A Windows Proxy is used to perform the following actions:</p> <ul style="list-style-type: none"> <li>◆ Enable Linux Primary Servers to perform discovery tasks that use Windows-specific discovery technologies (such as WMI, WinAPI, and SNMP).</li> <li>◆ Discover Windows devices that are in a different subnet than the Primary Server.</li> <li>◆ Discover Windows devices in a network enabled for NAT.</li> </ul> <p>Discovery through WMI, WinAPI and SNMP requires certain ports to be reachable on the target devices, so the Primary Server can send Remote Registry, WMI, or SNMP requests to the target devices. Ports are opened by adding them as an exception in the Windows Firewall configuration settings. 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 discovery is run, you need to add the IP address of the Primary Server as an exception. However, if you use a Windows Proxy in the same subnet as a target device, you do not need to change the scope of the Windows Firewall exception.</p> <p>The connection between the ZENworks Server and Windows Proxy is secured through SSL.</p> <p><b>Override Zone Window Proxy Settings:</b> Select this option if you want to override the Windows Proxy settings configured at the Management Zone and configure new settings for the task.</p> <p><b>Windows Proxy:</b> Select a Windows managed device (server or workstation) to be used as a Windows Proxy for performing the discovery tasks instead of a ZENworks Server. The Windows Proxy must reside in the same network as the target devices.</p> <p><b>Windows Proxy Timeout:</b> Specify the number of seconds you want the ZENworks Server to wait for a response from the Windows Proxy.</p>

Wizard Page	Details
Select or Edit a Proxy Device page > <i>Linux Proxy</i>	<p>If you want to use a Linux Proxy instead of the Primary Server to perform the discovery tasks on Linux devices, click the <i>Linux Proxy</i> option and configure the settings in the Select Linux Proxy dialog box.</p> <p>A Linux Proxy is used to perform the following actions:</p> <ul style="list-style-type: none"> <li>◆ Enable Primary Servers that cannot perform discovery tasks that use Linux-specific discovery technologies like SSH.</li> <li>◆ Discover Linux devices in a different subnet than the Primary Server.</li> <li>◆ Discover Linux devices in a network enabled for NAT.</li> </ul> <p>The SSH discovery requires port 22 to be reachable in order to enable the Primary Server to connect to the target device. If the SSH port is blocked in the Network Firewall, you use a Linux managed device in the same subnet as the target device.</p> <p>The connection between the ZENworks Server and Linux Proxy is secured through SSL.</p> <p>For more information on how to open port 22, see <a href="#">“Prerequisites for Deploying to Linux Devices” on page 106</a>.</p> <p><b>Override Zone Linux Proxy Settings:</b> Select this option if you want to override the Linux Proxy settings configured at the Management Zone and configure new settings for the task.</p> <p><b>Linux Proxy:</b> Select a Linux managed device (server or workstation) to be used as a Linux Proxy for performing the discovery tasks instead of a ZENworks Server. The Linux Proxy must reside in the same network as the target devices.</p> <p><b>Linux Proxy Timeout:</b> Specify the number of seconds you want the ZENworks Server to wait for a response from the Linux Proxy.</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.



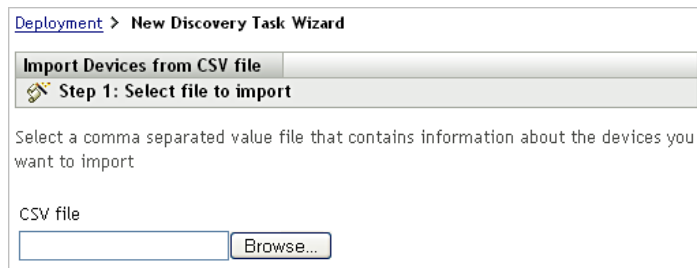
---

# 4 Importing Devices from CSV Files

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. The CSV file can contain the information in any order. An option to choose the column (which contains a valid number that is to be mapped with the selected device field) is provided while importing devices from a CSV file.

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.



The screenshot shows a web interface for the 'Import Devices from CSV file' wizard. At the top, there is a breadcrumb trail: 'Deployment > New Discovery Task Wizard'. Below this, the main title is 'Import Devices from CSV file' and the current step is 'Step 1: Select file to import'. The instructions read: 'Select a comma separated value file that contains information about the devices you want to import'. There is a text input field labeled 'CSV file' and a 'Browse...' button next to it.

- 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.
Configure Import	<p>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>To create the information mappings:</p> <ol style="list-style-type: none"> <li>1. Click <i>Add</i> to display the Specify Import Columns dialog box.</li> <li>2. Fill in the following fields: <ul style="list-style-type: none"> <li><b>Field:</b> Select the device field you want to map to a column in the CSV file.</li> <li><b>Column:</b> Specify a column and then number it to match the selected device field.</li> </ul> <p>For example</p> <p>If the first column in a CSV file contains IP address information, the second column contains DNS name information while the third column contains operating system information, then the values of the above fields would be:</p> <p>Field: IP Address, Column:1</p> <p>Field: DNS Name, Column: 2</p> <p>Field: Operating System, Column: 3</p> </li> <li>3. Click <i>OK</i> to create the information mapping and add it to the list.</li> <li>4. To verify that the field is mapped to the correct column, click <i>Verify</i>.</li> <li>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.

# 5 Advertised Discovery

The ZENworks discovery engine allows you to collect information about [advertised devices](#) on your network.

- ◆ [Section 5.1, “Configuring the Advertised Discovery Settings,”](#) on page 43
- ◆ [Section 5.2, “Discovering Advertised Devices,”](#) on page 45

## 5.1 Configuring the Advertised Discovery Settings

Advertised discovery uses the following configuration settings that can be modified, if necessary:

- ◆ Advertised discovery interval.
- ◆ IP addresses and subnets to scan for advertised devices. By default, only the local subnet is scanned.

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

Configuration	Registration	System Information	Asset Inventory	Asset Management	System Updates	Locations	Subscriptions
Management Zone Settings							
Content							
Device Management							
Discovery and Deployment							
Category							
Description							
<a href="#">Advertised Discovery Settings</a>							
Configure the interval and subnets of advertised devices on your network.							
<a href="#">Discovery</a>							
Configure settings related to discovering new devices.							
<a href="#">Windows Proxy</a>							
Configure a managed Windows device to be used as the Windows Proxy for discovery and deployment.							
<a href="#">Linux Proxy</a>							
Configure a managed Linux device to be used as the Linux Proxy for discovery and deployment.							
Event and Messaging							
Infrastructure Management							
Inventory							
Reporting Services							
Endpoint Security Management							
Asset Management							
Patch Management							

2 In the Management Zone Settings panel, click *Discovery and Deployment*, then click *Advertised Discovery Settings*.

- 3 In the Advertised Discovery Interval panel, modify the following settings as necessary:
  - Allow the system to check for advertised devices:** Select this option to enable advertised discovery. All ZENworks Servers perform the discovery. When a preagent receives a discovery request, it responds to the ZENworks Server that initiated the request.
  - Days, Hours, Minutes:** Specify how often you want to perform the advertised discovery.
- 4 In the Advertised Discovery Subnets panel, specify subnets for the advertised discovery. By default, the ZENworks Server that performs the discovery scans on its local subnet only.
 

To specify a subnet:

  - 4a To specify a subnet, fill in the following fields:
    - IP Address:** Specify an IP address located within the subnet. Use the standard dotted-decimal notation. For example, 123.45.167.100.
    - Optional CIDR Subnet Mask:** Specify the subnet by using the standard CIDR (Classless Inter-Domain Routing) notation. With CIDR, the dotted decimal portion of the IP address (in the IP Address field) is interpreted as a 32-bit binary number that has been split into four 8-bit bytes. You can use this field to enter the prefix length, which is the number of shared initial bits, counting from the left side of the address. The prefix length can range from 0 to 32, with 8, 16, 24, and 32 being commonly used numbers. For example, 123.45.167.100 with an optional CIDR subnet mask (or prefix length) of 24 matches specifies the 123.45.167 subnet.
  - 4b To add the subnet to the list, click *Add*.
  - 4c (Optional) To add additional subnets, repeat [Step 4a](#) and [Step 4b](#).
  - 4d (Optional) To reorder the list, select a subnet, then click *Move Up* or *Move Down*.  
The subnets are scanned in the order listed, from top to bottom.
- 5 Click *OK*.

## 5.2 Discovering Advertised Devices

- 1 In ZENworks Control Center, click the *Deployment* tab.
- 2 In the *Deployment Activities* list located in the left pane, click *Discover Advertised Devices*.

The ZENworks Server sends an advertised discovery request to all the devices on the network. On receiving the request, the preagent responds to the ZENworks Server.

The discovered [advertised devices](#) are listed in the [Deployable Devices](#) panel.

The screenshot displays the Novell ZENworks Control Center interface. The top navigation bar includes the ZENworks logo, the user name 'Welcome, administrator', and links for 'Help' and 'Logout'. The left sidebar contains a navigation menu with categories: Home, Devices, Users, Policies, Bundles, Patch Management, Deployment (selected), Reports, Configuration, Asset Management, and Endpoint Security. Under the 'Deployment' category, the 'Deployment Activities' sub-menu is expanded, showing options: 'Deploy Managed Device', 'Edit Deployment Package', 'Schedule Discovery Task', 'Discover Advertised Devices' (highlighted), and 'Import Deployable Devices'. The main content area features a notification: 'Note: An Advertised Discovery Ping has been successfully initiated.' Below this, there are three panels: 'Discovery Tasks' (empty table with columns: Name, Schedule, Status, Devices Found Last Scan), 'Deployment Tasks' (empty table with columns: Name, Schedule, Status), and 'Deployable Devices' (empty table with columns: Name, IP Address, Operating System, Initial Discovery, Deployment Status). The 'Deployable Devices' panel includes a 'Delete' button and an 'Advanced' view toggle.



---

# 6 Viewing or Updating Device Details

After a device is discovered, its details are listed in ZENworks Control Center, based on the information available for a discovered device. For example, if the SNMP information is not available for a discovered device, then the SNMP Information panel is not displayed.

If the discovered information for a device is incorrect or insufficient, administrators with the Edit Discovered Device rights can manually change the details for the fields that have the *Edit* button next to them. However, except for the Asset information, manually updated information is overwritten with the discovered information when a discovery is run again for the same IP address.

You can view the following information about the discovered device:

- ♦ **Discovery Information:** Displays the identification information, device type, discovery process status, deployment process status, mode of the discovery, and network type of the device.
- ♦ **Network Information:** Displays the IP address, MAC address, and DNS name of the device.
- ♦ **Management Information:** Displays the Adaptive Agent version and Management Zone name. For a managed device that belongs to the same zone from which a discovery is run, you can also view the Summary page and hardware and software inventory information of the associated managed device.

These details are displayed for managed devices only.

- ♦ **Asset Information:** Displays the description, manufacturer, model, serial number, and asset tag number of the device.

For routers, hubs, and switches, the number of ports and firmware revision details are also displayed.
















For printers, the number of pages and firmware revision details are displayed.

- ♦ **OS Information:** Displays the operating system type and version, memory, disk space, and hardware information.
- ♦ **SNMP Information:** Displays the SNMP object identification, SNMP system name, and up-time of the SNMP service.

To view or update the device details:

- 1 In ZENworks Control Center, click *Devices > Discovered*.

Figure 6-1 Discovered panel (Devices tab > Discovered page)

Discovered	Inventoried	Managed
<b>Discovered</b>		
		
Type	Discovered	
 <a href="#">All Types</a>	<a href="#">0</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="#">DRAC Devices</a>	<a href="#">0</a>	
 <a href="#">Intel® AMT Devices</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="#">Embedded Workstations</a>	<a href="#">0</a>	
 <a href="#">Other Devices</a>	<a href="#">0</a>	
 <a href="#">Unknown Devices</a>	<a href="#">0</a>	
 <a href="#">Deployable Types</a>	<a href="#">0</a>	
 <a href="#">Devices created via ZENworks Migration</a>	<a href="#">0</a>	
 <a href="#">Devices created via ZENworks Asset Management Migration</a>	<a href="#">0</a>	

- 2 In the Discovered panel, click a device type, then click a discovered device for which you want to view or update the details.

The Details page lists information about the discovered devices.

- 3 (Conditional) If the discovered information for a device is incorrect or insufficient, click *Edit*, then manually change the details for the fields.

Your manual changes are overwritten the next time a discovery is run for this device.



---

# || ZENworks Adaptive Agent Deployment

The following sections provide information and instructions to help you deploy the ZENworks Adaptive Agent to devices so that you can manage them.

- ◆ [Chapter 7, “Basic Concepts,” on page 51](#)
- ◆ [Chapter 8, “Managing Deployment Packages,” on page 55](#)
- ◆ [Chapter 9, “Registering Devices,” on page 63](#)
- ◆ [Chapter 10, “Deploying the ZENworks Adaptive Agent,” on page 93](#)
- ◆ [Chapter 11, “Uninstalling the Agent,” on page 139](#)
- ◆ [Chapter 12, “Deploying the Inventory-Only Module,” on page 141](#)



---

# 7 Basic Concepts

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

- ♦ [Section 7.1, “Deployment Methods,” on page 51](#)
- ♦ [Section 7.2, “Deployment Packages,” on page 51](#)
- ♦ [Section 7.3, “Adaptive Agent Versus Inventory-Only Module,” on page 52](#)

## 7.1 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 10, “Deploying the ZENworks Adaptive Agent,” on page 93](#).

## 7.2 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 fourteen 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).

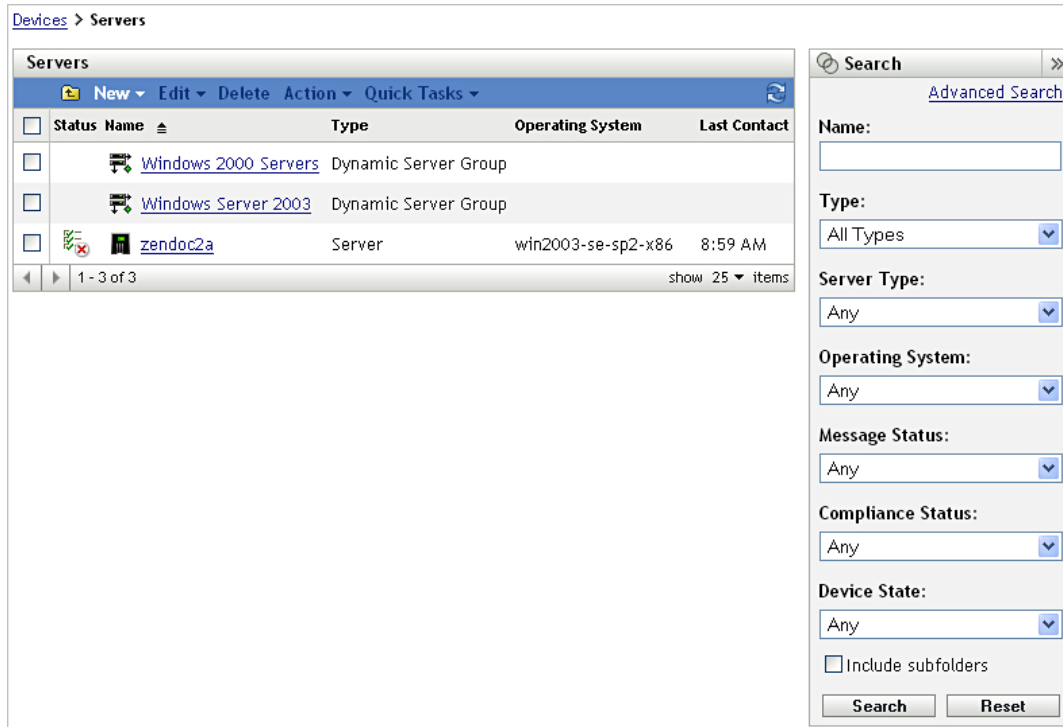
If necessary, you can modify a deployment package to change the ZENworks Server address or registration key included in the package. For example, assume that you want to use the same package to deploy the agent to devices on your private network and to devices on the other side of a firewall or router 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 the deployment packages and how to use them, see [Chapter 8, “Managing Deployment Packages,” on page 55](#).

## 7.3 Adaptive Agent Versus Inventory-Only Module

The ZENworks Adaptive Agent supports Windows XP, Windows 2003, Windows Vista, and Windows 7 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 7-1 Managed Devices page > Servers folder



Deployment instructions for the Adaptive Agent are provided in [Chapter 10, “Deploying the ZENworks Adaptive Agent,”](#) on page 93.

If a Windows device does not meet the requirements for deploying the Adaptive Agent or if you want to inventory a Linux, NetWare, or Macintosh device, you can deploy the Inventory-Only module.

For details see “System Requirements for ZENworks 11.2.1” in the [ZENworks 11 SP3 System Requirements](#) for details.

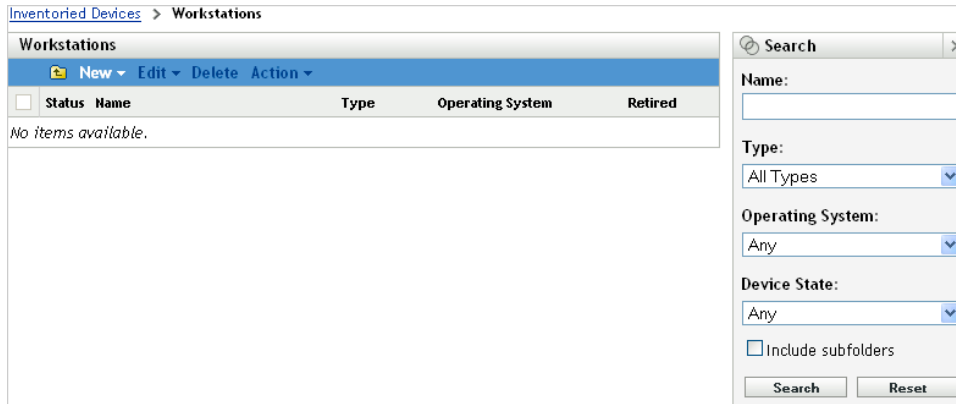
After you deploy the module, the device is added to the ZENworks database. The ZENworks Control Center displays inventoried-only devices on the Device page's *Inventoried* tab.

---

**NOTE:** The inventory-only module only collects and sends the inventory data. It does not perform any of the other tasks associated with the ZENworks Adaptive Agent.

---

**Figure 7-2** *Inventoried Devices page > Workstations folder*



Deployment instructions for the Inventory-Only module are provided in [Chapter 12, "Deploying the Inventory-Only Module,"](#) on page 141.



---

# 8 Managing 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.

Each ZENworks Server contains nine default system packages. These packages are built during installation and system update 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 8.1, "Package Types and Architectures," on page 55](#)
- ♦ [Section 8.2, "Default System Packages Versus Custom Packages," on page 57](#)
- ♦ [Section 8.3, "Customizing Packages," on page 58](#)
- ♦ [Section 8.4, "Rebuilding Packages," on page 61](#)

## 8.1 Package Types and Architectures

- ♦ [Section 8.1.1, "Package Types and Architectures for Windows," on page 55](#)
- ♦ [Section 8.1.2, "Package Types and Architectures for Linux," on page 56](#)
- ♦ [Section 8.1.3, "Package Types and Architectures for Macintosh," on page 57](#)

In order to support deployment of the ZENworks Adaptive Agent from files on either local or network media, there are various types of deployment packages for Windows, Linux and Macintosh operating systems. There are three versions of each of these packages: x86, x86\_64, and x86/x86\_64. The x86 and x86\_64 packages are used in deployments to 32-bit and 64-bit devices, while the x86/x86\_64 version is used in deployments to either 32-bit or 64-bit devices.

### 8.1.1 Package Types and Architectures for Windows

The following packages are available for installing the ZENworks Adaptive Agent on Windows:

- ♦ **Network (.NET required):** Contains only the pre-agent, which downloads the Adaptive Agent files from a ZENworks Server. The network (.NET required) package requires that Microsoft.NET Framework 4.0 is installed on the device prior to the deployment of the agent to the device.
- ♦ **Standalone (.NET required):** Contains the pre-agent, all the ZENworks Adaptive Agent module files. The Adaptive Agent is installed to the device, but no registration or management occurs until the device connects to the network. The standalone (.NET require) package requires that Microsoft.NET Framework 4.0 is installed on the device prior to the deployment of the agent to the device.

- ♦ **Standalone:** Contains the pre-agent, all the ZENworks Adaptive Agent module files, and the Microsoft.NET Framework 4.0 installables. The Adaptive Agent is installed to the device, but no registration or management occurs until the device connects to the network.

To support the various Windows architectures, there are three versions of each package:

- ♦ **x86 version:** You use the x86 version for manual deployment to 32-bit Windows devices.

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

`%ZENWORKS_HOME%\novell\zenworks\install\downloads\setup\x86` on Windows and `/opt/novell/zenworks/install/downloads/setup/x86` on Linux.

- ♦ **x86\_64 version:** You use the x86\_64 version for manual deployment to 64-bit Windows devices.

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

`%ZENWORKS_HOME%\novell\zenworks\install\downloads\setup\x86_64` on Windows and `/opt/novell/zenworks/install/downloads/setup/x86_64` on Linux.

- ♦ **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_AgentComplete.exe`, and `PreAgentPkg_AgentCompleteDotNet.exe`) are located in the following directory on the ZENworks Server:

`%ZENWORKS_HOME%\novell\zenworks\install\downloads\setup\_all` on Windows and `/opt/novell/zenworks/install/downloads/setup/_all` on Linux.

## 8.1.2 Package Types and Architectures for Linux

The following packages are available for installing the ZENworks Adaptive Agent on Linux:

- ♦ **Network (JRE required):** Contains only the pre-agent, which downloads the ZENworks Adaptive Agent files from the ZENworks Server. The network (JRE required) package requires that JRE 1.6 is installed on the device prior to the deployment of the agent to the device.
- ♦ **Standalone:** Contains the pre-agent, all the ZENworks Adaptive Agent module files, and the JRE 1.6 installables.

To support the various Linux architectures, there are three versions of each package:

- ♦ **x86 version:** You use the x86 version for manual deployment to 32-bit Linux devices.

The x86 packages (`PreAgentPkg_AgentLinux.bin` and `PreAgentPkg_AgentLinuxComplete.bin`) are located in the following directory on the ZENworks Server:

`%ZENWORKS_HOME%\novell\zenworks\install\downloads\setup\x86` on Windows and `/opt/novell/zenworks/install/downloads/setup/x86` on Linux.

- ♦ **x86\_64 version:** You use the x86\_64 version for manual deployment to 64-bit Linux devices.

The x86\_64 packages (`PreAgentPkg_AgentLinux.bin` and `PreAgentPkg_AgentLinuxComplete.bin`) are located in the following directory on the ZENworks Server:



`%ZENWORKS_HOME%\novell\zenworks\install\downloads\setup\x86_64` on Windows and /  
`opt/novell/zenworks/install/downloads/setup/x86_64` on Linux.

- ♦ **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 Linux devices.

The All Architectures packages (`PreAgentPkg_AgentLinux.bin` and `PreAgentPkg_AgentLinuxComplete.bin`) are located in the following directory on the ZENworks Server:

`%ZENWORKS_HOME%\novell\zenworks\install\downloads\setup\_all` on Windows and /  
`opt/novell/zenworks/install/downloads/setup/_all` on Linux.

## 8.1.3 Package Types and Architectures for Macintosh

The following packages are available for installing the ZENworks Adaptive Agent on Macintosh devices:

- ♦ **Network (JRE required):** Contains only the pre-agent, which downloads the ZENworks Adaptive Agent files from the ZENworks Server. The network (JRE required) package requires that JRE 1.6 is installed on the device prior to the deployment of the agent to the device.
- ♦ **Standalone (JRE required):** Contains the pre-agent and all the ZENworks Adaptive Agent module files. The standalone (JRE required) package requires that JRE 1.6 is installed on the device prior to the deployment of the agent to the device.

The architecture of the agent to be installed depends upon the architecture of Java installed on the device. To support the various Macintosh architectures, there are three versions of each package:

- ♦ **x86 version:** You use the x86 version for manual deployment to Macintosh devices having 32-bit Java installed on the device.

The x86 packages (`PreAgentPkg_AgentMac.bin` and `PreAgentPkg_AgentMacComplete.bin`) are located in the following directory on the ZENworks Server:

`%ZENWORKS_HOME%\novell\zenworks\install\downloads\setup\x86` on Windows and /  
`opt/novell/zenworks/install/downloads/setup/x86` on Linux and Macintosh devices.

- ♦ **x86\_64 version:** You use the x86\_64 version for manual deployment to 64-bit Macintosh devices.

The x86\_64 packages (`PreAgentPkg_AgentMac.bin` and `PreAgentPkg_AgentMacComplete.bin`) are located in the following directory on the ZENworks Server:

`%ZENWORKS_HOME%\novell\zenworks\install\downloads\setup\x86_64` on Windows and /  
`opt/novell/zenworks/install/downloads/setup/x86_64` on Linux and Macintosh devices.

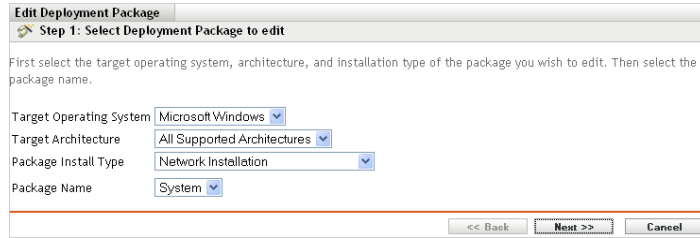
## 8.2 Default System Packages Versus Custom Packages

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.

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.

## 8.3 Customizing Packages

- 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.



The screenshot shows a wizard window titled "Edit Deployment Package" with a sub-header "Step 1: Select Deployment Package to edit". Below the sub-header is a brief instruction: "First select the target operating system, architecture, and installation type of the package you wish to edit. Then select the package name." The form contains four dropdown menus: "Target Operating System" set to "Microsoft Windows", "Target Architecture" set to "All Supported Architectures", "Package Install Type" set to "Network Installation", and "Package Name" set to "System". At the bottom of the form are three buttons: "<< Back", "Next >>", and "Cancel".

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 Operating System</i> field, select the operating system of the package that you want to edit.</p> <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 manually deploying the agent to 32-bit devices.</li><li>◆ <b>x86_64 Architecture (64-bit):</b> Used in manually deploying 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 that you want to edit.</p> <p>The packages in the list are determined by the <i>Target Operating System</i> that you selected for the device.</p> <p>The following packages are available for Windows:</p> <ul style="list-style-type: none"><li>◆ <b>Network Installation (.NET required):</b> Contains only the pre-agent, which downloads the Adaptive Agent files from the ZENworks Server and the Microsoft .NET Framework 3.5 SP1 installables.</li><li>◆ <b>Standalone Installation (.NET required):</b> Contains the pre-agent and all the ZENworks Adaptive Agent module files.</li><li>◆ <b>Standalone Installation:</b> Contains the pre-agent, all the ZENworks Adaptive Agent module files, and the Microsoft .NET Framework 3.5 SP1 installables.</li></ul> <p>The following packages are available for Linux:</p> <ul style="list-style-type: none"><li>◆ <b>Network Installation (JRE required):</b> Contains only the pre-agent, which downloads the Adaptive Agent files from the ZENworks Server and the JRE 1.6 Update 16 installables.</li><li>◆ <b>Standalone Installation:</b> Contains the pre-agent, all the ZENworks Adaptive Agent module files, and the JRE 1.6 Update 16 installables.</li></ul> <p>In the <i>Package Name</i> list, select the name of the package that you want to edit.</p> <p>The names in the list are determined by the architecture and installation type you 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 that meets the architecture and installation type criteria you specified.</p>

Wizard Page	Details
Provide Primary Server Information page	<p data-bbox="667 218 1373 390">Other package names are displayed only if you have edited the system package and saved the customized version as a new package. You can specify any name for the customized package. The name must not contain any of the following invalid characters: / \ * ? : " ' &lt; &gt;   ` % ~. The directory, used to store the package, is given the specified name and the package name remains the same.</p> <p data-bbox="667 443 1373 611">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 pre-agent 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 data-bbox="667 642 1373 779">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>
Add Registration Key page	<p data-bbox="667 810 1373 915">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 data-bbox="667 947 1373 1052">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 data-bbox="667 1083 1373 1136">For more information about registration keys and rules, see <a href="#">Chapter 9, "Registering Devices," on page 63</a>.</p>
Additional Language Selection page	<p data-bbox="667 1167 1373 1220">On Windows, select additional language packages to be included with the deployment package.</p> <p data-bbox="667 1251 1373 1346">The progress and message logs for the deployment process are displayed in English by default. If you want to receive the messages in the language of the machine locale, then you must add the necessary additional language packs to the deployment package.</p>

Wizard Page	Details
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. The name must not contain any of the following invalid characters: / \ * ? : " ' &lt; &gt;   ` % ~. The name that you specify is used to identify the updated packages on the zenworks-setup page. The package name remains the same 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 <code>%ZENworks_HOME%\novell\zenworks\install\downloads\custom</code> directory on Windows and <code>/opt/novell/zenworks/install/downloads/custom</code> on Linux. For example, if you modify the x86 version of the <code>PreAgentPkg_Agent.exe</code> package and save it with a name of <code>ExternalPack</code>, the file is stored as follows:</p> <p><code>%ZENworks_HOME%\Novell\ZENworks\install\downloads\custom\ExternalPack\x86\PreAgentPkg_Agent.exe</code> on Windows and <code>/opt/novell/zenworks/install/downloads/custom/ExternalPack/x86/PreAgentPkg_Agent.exe</code> on Linux.</p> <p><b>NOTE:</b> If you want to delete custom deployment packages, you must manually delete the directory containing the packages.</p>

## 8.4 Rebuilding Packages

You must rebuild the default and custom deployment packages in the following scenarios:

- If the Primary Server port has been changed or is incorrect in the package.
- To include all the new and updated MSI or RPM files that are provided as patches.

The new and updated MSI files are located in the

`%ZENWORKS_HOME%\novell\zenworks\install\downloads\msi` directory on Windows and in the `/opt/novell/zenworks/install/downloads/msi` directory on Linux.

The new and updated RPM files are located in the

`%ZENWORKS_HOME%\novell\zenworks\install\downloads\rpm` directory on Windows and in the `/opt/novell/zenworks/install/downloads/rpm` directory on Linux.

- If the server certificate has been changed.

The following sections provide instructions for rebuilding the default and custom packages:

- [Section 8.4.1, “Rebuilding the Default Packages,” on page 62](#)
- [Section 8.4.2, “Rebuilding the Custom Packages,” on page 62](#)

## 8.4.1 Rebuilding the Default Packages

The default packages are the system packages that are included on each ZENworks Server to deploy the agent to your device. For more information on the default packages, see [“Deployment Packages” on page 51](#).

To rebuild the default packages:

1 Do one of the following:

- ◆ **On Windows:** At the command prompt, enter:

```
novell-zenworks-configure -c CreateExtractorPacks -Z
```

- ◆ **On Linux:** At the console prompt, change to the `/opt/novell/zenworks/bin` directory, then enter:

```
./novell-zenworks-configure -c CreateExtractorPacks -Z
```

2 When prompted to select the packages to be rebuilt, (by default, only the Agent Network Package - Windows is selected), do one of the following:

- ◆ To rebuild only the default package, press Enter.
- ◆ To rebuild additional packages, type the number corresponding to a package, then press Enter twice.

For example, if you type 2, then press Enter twice, the Agent Network Package - Windows (default) and Agent Complete Package - Windows are rebuilt.

- ◆ To rebuild all the packages, type 2,3,4,5,6,7 then press Enter twice.

## 8.4.2 Rebuilding the Custom Packages

The custom packages are created by customizing any of the default system packages. For more information on the custom packages, see [“Default System Packages Versus Custom Packages” on page 57](#).

To rebuild the custom packages:

1 Do one of the following:

- ◆ **On Windows:** At the command prompt, enter:

```
novell-zenworks-configure -c RebuildCustomPacks -Z
```

- ◆ **On Linux:** At the console prompt, change to the `/opt/novell/zenworks/bin` directory, then enter:

```
./novell-zenworks-configure -c RebuildCustomPacks -Z
```

2 When prompted to select whether to rebuild the custom packages, press Enter.

---

# 9 Registering Devices

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 9.1, “What Happens During Registration,” on page 63](#)
- ♦ [Section 9.2, “Creating Registration Keys and Rules,” on page 64](#)
- ♦ [Section 9.3, “Modifying the Device Naming Template Used During Registration,” on page 72](#)
- ♦ [Section 9.4, “Enabling Dynamic Renaming of Devices During Registration,” on page 73](#)
- ♦ [Section 9.5, “Reconciling Devices with existing Device Objects During Registration,” on page 77](#)
- ♦ [Section 9.6, “Disabling the Use of Registration Rules,” on page 88](#)
- ♦ [Section 9.7, “Manually Registering a Device,” on page 90](#)
- ♦ [Section 9.8, “Unregistering a Device,” on page 91](#)

## 9.1 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 9-1 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 9.4, “Enabling Dynamic Renaming of Devices During Registration,” on page 73](#) for more information.

<sup>3</sup> Occurs only if the key or rule being used for registration includes this information. See [Section 9.2, “Creating Registration Keys and Rules,”](#) on page 64 for more information.

## 9.2 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 9.2.1, “Creating a Registration Key,”](#) on page 64
- ♦ [Section 9.2.2, “Creating a Registration Rule,”](#) on page 67

### 9.2.1 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 10.5, “Using a Task to Deploy the Agent,”](#) on page 101.
- ♦ 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 [“Deployment Packages”](#) on page 51.
- ♦ 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 9.7, “Manually Registering a Device,”](#) on page 90.

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	Asset Management	System Updates
<b>Registration Keys</b>					
New Edit Delete					
Folder: /Keys					
<input type="checkbox"/>	<b>Registration Code</b>				<b>Usage Limit</b>
<input type="checkbox"/>	85263e				(unlimited)
<input type="checkbox"/>	e66366				(unlimited)
1 - 2 of 2					show 5 items
<b>Registration Rules</b>					
New Delete					
<input type="checkbox"/>	<b>Name</b>				
<input type="checkbox"/>	Doc				
1 - 1 of 1					show 5 items

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

**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" button.

Key Code: \*

Folder: \*

Description:

Number of times this key can be used:


Unlimited

Limit to:

\* 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
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>Key Code:</b> Provide a key code for the registration key. When devices register during installation, this is the key code the device provides to be assigned to the folder and groups associated with this registration. Any device that presents this key code is given the assignments associated with this registration.</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: <code>/\ * ? : " ' &lt; &gt;   ` % ~</code>.</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 times the devices can use this key to register.</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 <code>Accounting</code> in the <i>Department</i> field, then <code>Accounting</code> is entered in the <i>Department</i> field on the device's details page.</p>

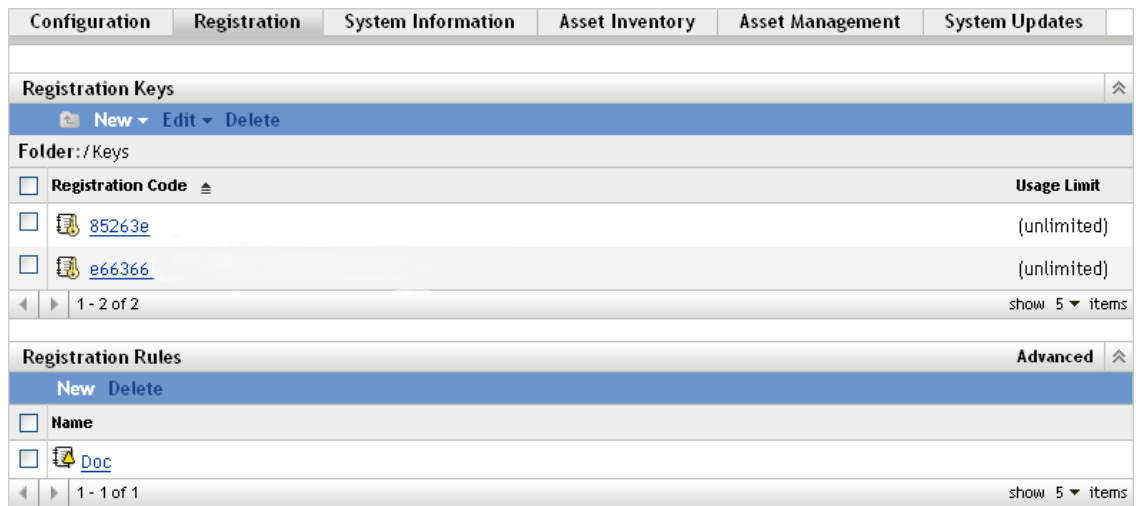
Wizard Page	Details
Group Membership page	<p>Specify the groups that devices will become members of when they register.</p> <p>Adding groups causes registering devices to receive any assignments provided by membership in the groups. Assignments from group membership are additive, so if a device is assigned 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.

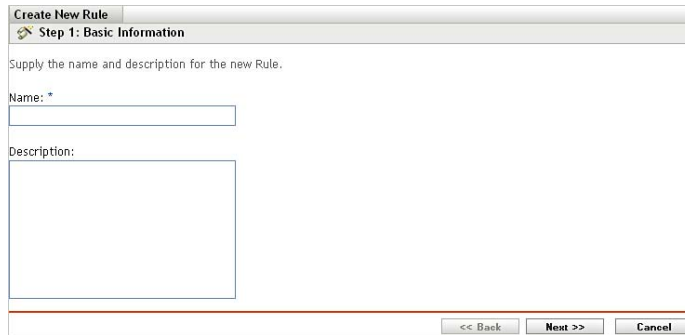
You can also use the `registration-create-key` command in the `zman` utility to create a registration key. For more information, see “[Registration Commands](#)” in the [ZENworks 11 SP3 Command Line Utilities Reference](#).

## 9.2.2 Creating a Registration Rule

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



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



3 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>

---

Wizard Page	Details
-------------	---------

---

Device Criteria page	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.
----------------------	---

1. Click *Add Filter* to add a filter line.
2. Create the filter expression.

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

Example 1:

```
IPAddress Equal to 123.45.67.89
```

IPAddress is the criteria option, Equal to is the operator, and 123.45.67.89 is the value. In the above example, the registration rule is applied only to devices whose IP addresses is equal to 123.45.67.89.

Example 2:

```
NOT IPAddress Equal to 123.45.67.89
```

You can use NOT to perform a logical negation of the expression.

In the above example, the registration rule is applied only to devices whose IP addresses is not equal to 123.45.67.89.

Example 3:

```
IPAddress Within 123.45.67.89-123.45.67.99
```

You can use the Within operator to specify the IP address range. Two types of IP address ranges are supported:

- ◆ Standard dotted-decimal notation

Example: 123.45.67.89-123.45.67.99

- ◆ CIDR notation

Example: 123.45.67.89/24, where /24 represents the prefix length, which is the number of shared initial bits, counting from the left side of the address.

The criteria options you can use are listed below, along with possible values. The format for all values, with the exception of CPU, Language, Device Type and OS, are free form string.

- ◆ CPU: Intel(R) Pentium(R) M processor 1600MHz
- ◆ DNS: abc.xyz.com
- ◆ Device Type: Workstation or Server
- ◆ GUID: 5bf63fb9b1ed4cd880e1a428a1fcf737
- ◆ Hostname: zenserver
- ◆ IPAddress: 123.45.67.89
- ◆ Language: Portuguese (Brazil)
- ◆ MAC Address: 00-0c-29-e8-cd-3a
- ◆ OS: win2003-se-sp1-x86

3. If necessary, click *Add Filter* to create another filter.

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: OS equals Windows Server 2003 AND IPAddress Equal to 123.45.67.89

In the above example, the registration rule is applied only to devices whose operating system is Windows 2003 and whose IP address is equal to 123.45.67.89.

---

---

Wizard Page	Details
-------------	---------

---

Device Criteria page (continued)	You can add filters individually or in sets. Logical operators, either <i>AND</i> or <i>OR</i> , are used to combine each filter and filter set. By default, filters are combined using <i>OR</i> (as determined by the <i>Combine Filters Using</i> field) and filter sets are combined using <i>AND</i> .
----------------------------------	---

You can change the default and use *AND* to combined filters, in which case filter sets are automatically combined using *OR*. In other words, the logical operator that is to combine individual filters (within in a set) must be the opposite of the operator that is used between filter sets.

You can easily view how these logical operators work. Click both the *Add Filter* and *Add Filter Set* options a few times each to create a few filter sets, then switch between *AND* and *OR* in the *Combine Filters Using* field and observe how the operators change.

As you construct filters and filter sets, you can think in terms of algebraic notation parentheticals, where filters are contained within parentheses, and sets are separated into a series of parenthetical groups. Logical operators (*AND* and *OR*) separate the filters within the parentheses, and the operators are used to separate the parentheticals.

For example, “(u AND v AND w) OR (x AND y AND z)” means “match either uvw or xyz.” In the filter list, this looks like:


```
u AND
v AND
w
OR
x AND
y AND
z
```

Containment Rules page	Specify the folder in which to place the devices.
------------------------	---

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.

Device Fields	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.
---------------	--

---

Wizard Page	Details
Group Membership page	<p data-bbox="532 218 1328 245">Specify the groups that devices will become members of when they register.</p> <p data-bbox="532 270 1422 384">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 data-bbox="532 409 1409 493">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 data-bbox="532 518 732 546">To specify a group:</p> <ol data-bbox="553 560 1422 1108" style="list-style-type: none"> <li data-bbox="553 560 1040 588">1. Click <i>Add</i> to display the Groups dialog box.</li> <li data-bbox="553 602 1357 653">2. Browse for and select the group (or groups) to which you want to add the devices. To do so: <ol data-bbox="607 678 1422 1108" style="list-style-type: none"> <li data-bbox="607 678 1422 762">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 data-bbox="643 779 659 806">or</li> <li data-bbox="643 821 1422 934">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 data-bbox="607 951 1422 1001">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 data-bbox="607 1018 1422 1068">c. Repeat steps 2a and 2b until you've selected all groups to which you want to assign membership.</li> <li data-bbox="607 1085 1130 1113">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 11 SP3 Command Line Utilities Reference](#).

## 9.3 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	Asset Management	System Updates	Locations	Subscriptions
<b>Management Zone Settings</b>							
Content							
Device Management							
<b>Category</b>		<b>Description</b>					
<a href="#">Local Device Logging</a>		Enable and configure local logging of warnings and errors encountered by managed devices.					
<a href="#">Device Refresh and Removal Schedule</a>		Configure the device refresh interval.					
<a href="#">ZENworks Agent</a>		ZENworks Agent Configuration.					
<a href="#">System Update Agent</a>		Configure system update behavior on ZENworks Agents.					
<a href="#">Registration</a>		Configure registration settings.					
<a href="#">ZENworks Explorer Configuration</a>		Configure the behavior of the ZENworks Explorer on managed devices.					
<a href="#">System Variables</a>		Configure system variables.					
<a href="#">Preboot Services</a>		Configure Preboot Services.					
<a href="#">Primary User</a>		Configure the setting for how the primary user is determined.					
<a href="#">Primary Workstation</a>		Configure the setting for how the primary workstation is determined.					
<a href="#">Dynamic Group Refresh Schedule</a>		Configure dynamic group refresh schedule.					
<a href="#">Wake-on-LAN</a>		Configure the Wake-on-LAN settings					
<a href="#">Power Management Settings</a>		Configure the schedule for the power management of Intel AMT devices.					
<a href="#">Remote Management</a>		Enable and configure remote management.					
Discovery and Deployment							
Event and Messaging							
Infrastructure Management							
Inventory							
Reporting Services							
Endpoint Security Management							
Asset Management							
Patch Management							

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



- 3 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}
```

- 4 Click *OK* to save the changes.

## 9.4 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, 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 9.4.1, “Enabling the Setting at the Management Zone,” on page 74](#)
- ♦ [Section 9.4.2, “Enabling the Setting for a Device Folder,” on page 75](#)

## 9.4.1 Enabling the Setting at the Management Zone

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

Configuration	Registration	System Information	Asset Inventory	Asset Management	System Updates	Locations	Subscriptions
<b>Management Zone Settings</b>							
Content							
<b>Device Management</b>							
<b>Category</b>	<b>Description</b>						
<a href="#">Local Device Logging</a>	Enable and configure local logging of warnings and errors encountered by managed devices.						
<a href="#">Device Refresh and Removal Schedule</a>	Configure the device refresh interval.						
<a href="#">ZENworks Agent</a>	ZENworks Agent Configuration.						
<a href="#">System Update Agent</a>	Configure system update behavior on ZENworks Agents.						
<a href="#">Registration</a>	Configure registration settings.						
<a href="#">ZENworks Explorer Configuration</a>	Configure the behavior of the ZENworks Explorer on managed devices.						
<a href="#">System Variables</a>	Configure system variables.						
<a href="#">Preboot Services</a>	Configure Preboot Services.						
<a href="#">Primary User</a>	Configure the setting for how the primary user is determined.						
<a href="#">Primary Workstation</a>	Configure the setting for how the primary workstation is determined.						
<a href="#">Dynamic Group Refresh Schedule</a>	Configure dynamic group refresh schedule.						
<a href="#">Wake-on-LAN</a>	Configure the Wake-on-LAN settings						
<a href="#">Power Management Settings</a>	Configure the schedule for the power management of Intel AMT devices.						
<a href="#">Remote Management</a>	Enable and configure remote management.						
<b>Discovery and Deployment</b>							
<b>Event and Messaging</b>							
<b>Infrastructure Management</b>							
<b>Inventory</b>							
<b>Reporting Services</b>							
<b>Endpoint Security Management</b>							
<b>Asset Management</b>							
<b>Patch Management</b>							

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

Configuration > Registration

**Registration** [X]

Configure registration settings.

---

**Device Naming Template** [^]

Name given to new machines:

[icon]

---

**Registration Rules** [^]

Enable use of registration rules.

Enable use of default registration rules.

---

**Device Dynamic Rename** [^]

Enable automatic renaming of devices.

---

**Reconcile Settings** [^]

Indicate which device attributes will be used in reconciliation

Serial Number       Mac Address       Machine Name

Enable Differentiation

OK    Apply    Reset    Cancel

- 3 In the Device Dynamic Rename panel, click *Enable automatic renaming of devices*.
- 4 Click *OK* to save the changes.

## 9.4.2 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 > Workstations

Workstations

Summary Relationships Settings

Settings

Content

Device Management

Category	Description	Inherited From
<a href="#">Local Device Logging</a>	Enable and configure local logging of warnings and errors encountered by managed devices.	(System)
<a href="#">Device Refresh and Removal Schedule</a>	Configure the device refresh interval.	(System)
<a href="#">ZENworks Agent</a>	ZENworks Agent Configuration.	(System)
<a href="#">System Update Agent</a>	Configure system update behavior on ZENworks Agents.	---
<a href="#">Registration</a>	Configure registration settings.	(System)
<a href="#">ZENworks Explorer Configuration</a>	Configure the behavior of the ZENworks Explorer on managed devices.	(System)
<a href="#">System Variables</a>	Configure system variables.	---
<a href="#">Preboot Services</a>	Configure Preboot Services.	---
<a href="#">Primary User</a>	Configure the setting for how the primary user is determined.	---
<a href="#">Remote Management</a>	Enable and configure remote management.	(System)
<a href="#">Device Dynamic Rename</a>	Enables automatic renaming of devices.	(System)
<a href="#">Power Management Settings</a>	Configure the schedule for the power management of Intel AMT devices.	---
<b>Infrastructure Management</b>		
<b>Inventory</b>		
<b>Endpoint Security Management</b>		
<b>Asset Management</b>		

- 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** [X]

Enables automatic renaming of devices.  
Current: (System) [\(Override settings\)](#)

---

**Device Dynamic Rename** [^]

Enable automatic renaming of devices.

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

## 9.5 Reconciling Devices with existing Device Objects During Registration

ZENworks 11 SP3 enables you to create a device object in the zone prior to actually registering the device with the zone. This feature allows you to pre configure all the variables and other configurations for a given device prior to booting the device.

You can create dummy device objects and register them in the Management Zone by importing their information from a comma-separated value (CSV) file. This creates managed workstation device objects in the database. Later, when the Primary Agent is deployed to these devices, the ZENworks Reconcile settings (hostname, serial number, and MAC address) are used to reconcile the new Primary Agent to the device object that has already been registered in the database. This helps you to avoid the possibility of duplicates in the database during the registration of the devices in the Management Zone.

Review the following sections:

- ♦ [Section 9.5.1, “Creating Dummy Device Objects,” on page 77](#)
- ♦ [Section 9.5.2, “Reconciling the Devices,” on page 79](#)
- ♦ [Section 9.5.3, “Importing Managed Devices,” on page 86](#)

### 9.5.1 Creating Dummy Device Objects

You can create dummy device objects that are added to the ZENworks database in one of the following ways:

- ♦ [“Manually Creating a Dummy Device Object” on page 77](#)
- ♦ [“Creating Dummy Device Objects by Using a CSV File” on page 78](#)

#### Manually Creating a Dummy Device Object

- 1 Ensure that you have created registration keys as explained in [Section 9.2.1, “Creating a Registration Key,” on page 64](#).
- 2 In ZENworks Control Center, click the *Devices* tab.
- 3 In the Devices Tasks panel, click *Add Device*.

The Add Device wizard is displayed.

- 4 On the Device Attributes and Registration Key page, provide the following information used to identify and register the device in the ZENworks database:

**Registration Key:** Select a registration key to use when registering the device. The key must already exist.

**Host Name:** Specify a hostname for the device. For example: workstation1.

The hostname appears as the first part of the DNS name (for example, workstation1.company.com). Because of DNS limitations, the maximum number of characters that can be used in the hostname is 63.

**Serial Number:** Specify the device’s serial number if you want to later reconcile a managed device with this dummy device object based on the serial number.

**MAC Address:** Specify the device's MAC address if you want to later reconcile a managed device with this dummy device object based on the serial number. MAC address is a 12-digit alphanumeric string in which you can use a hyphen (-) or a colon (:) as separator. You can specify the MAC address in one of the following formats.

- ◆ xxxxxxxxxxxx
- ◆ xx-xx-xx-xx-xx
- ◆ xx:xx:xx:xx:xx

- 5 Review the information and, if necessary, use the *Back* button to make changes to the information. Click *Finish* to add the device.

A workstation device object with the hostname that you specified in [Step 4 on page 77](#) is created in the ZENworks database and is registered in the Management Zone. To view the device object in ZENworks Control Center, click *Devices > Managed > the Workstations* folder.

## Creating Dummy Device Objects by Using a CSV File

- 1 Using a text editor, create a CSV file with the following fields as an entry for each device objects:
  - ◆ WS\_1.0. This is the first field that must be specified for each entry. You must not change it.
  - ◆ hostname
  - ◆ serial number
  - ◆ MAC address

Use the following format to list the devices in the file:

`WS_1.0, hostname of the device being registered or imported, serial number, MAC address`


The value for hostname is mandatory, and the values for serial number and MAC address are optional.

A sample CSV file is as follows:

```
WS_1.0,img-linux1,121456125622,000C298062A8
WS_1.0,img-linux2,121456125623,000C29935FF8
```

- 2 Log into ZENworks Control Center.
- 3 Click the *Devices* tab.
- 4 In the Device Tasks panel, click *Import Managed Devices*.

The Import Devices dialog box is displayed.

- 5 Specify or click  to browse for and select a key to use when registering the device. The key must already exist.

To create a registration key in ZENworks Control Center, see [Section 9.2, "Creating Registration Keys and Rules," on page 64](#).

- 6 In the *File Path* option, browse for and select the CSV file that you created in [Step 1](#).
- 7 Click *OK*.

The device entries listed in the CSV file are created as workstation device objects in the database and are registered in the Management Zone. To view the device objects in ZENworks Control Center, click *Devices > Managed > the Workstations* folder.

## 9.5.2 Reconciling the Devices

You can reconcile a new device that is being registered to an existing device object with its own bundles and policies. Reconciliation occurs only if the GUID of the new device that is getting registered does not match the GUID of the existing device object. Reconciliation does not occur with every refresh or registration call.

### Device Reconciliation Settings

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

Configuration	Registration	System Information	Asset Inventory	Asset Management	System Updates	Locations	Subscriptions
<b>Management Zone Settings</b>							
<b>Content</b>							
<b>Device Management</b>							
<b>Category</b>		<b>Description</b>					
<a href="#">Local Device Logging</a>		Enable and configure local logging of warnings and errors encountered by managed devices.					
<a href="#">Device Refresh and Removal Schedule</a>		Configure the device refresh interval.					
<a href="#">ZENworks Agent</a>		ZENworks Agent Configuration.					
<a href="#">System Update Agent</a>		Configure system update behavior on ZENworks Agents.					
<a href="#">Registration</a>		Configure registration settings.					
<a href="#">ZENworks Explorer Configuration</a>		Configure the behavior of the ZENworks Explorer on managed devices.					
<a href="#">System Variables</a>		Configure system variables.					
<a href="#">Preboot Services</a>		Configure Preboot Services.					
<a href="#">Primary User</a>		Configure the setting for how the primary user is determined.					
<a href="#">Primary Workstation</a>		Configure the setting for how the primary workstation is determined.					
<a href="#">Dynamic Group Refresh Schedule</a>		Configure dynamic group refresh schedule.					
<a href="#">Wake-on-LAN</a>		Configure the Wake-on-LAN settings					
<a href="#">Power Management Settings</a>		Configure the schedule for the power management of Intel AMT devices.					
<a href="#">Remote Management</a>		Enable and configure remote management.					
<b>Discovery and Deployment</b>							
<b>Event and Messaging</b>							
<b>Infrastructure Management</b>							
<b>Inventory</b>							
<b>Reporting Services</b>							
<b>Endpoint Security Management</b>							
<b>Asset Management</b>							
<b>Patch Management</b>							

- 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.

**Reconcile Settings**

Indicate which device attributes will be used in reconciliation

Serial Number       Mac Address       Machine Name

Enable Differentiation

OK    Apply    Reset    Cancel

**3** Indicate the device attributes that are used in reconciliation.

You can choose to reconcile the new devices with the existing device objects by using one or more of the following attributes:

- ◆ *Serial Number*
- ◆ *MAC Address*
- ◆ *Machine Name* (hostname)

**3a Enable Differentiation:**

- ◆ If differentiation is enabled, it uses **AND** logic, meaning that all the selected attributes must match for a device to reconcile.
- ◆ If differentiation is disabled, it uses **OR** logic, meaning that any one of the selected attributes must match for a device to reconcile.

**Differentiation disabled:** If multiple device objects with matching attributes (such as Mac address or hostname) are found, the device object with the matching serial number gets the first preference, even if none of the attributes are selected.

**4** Click *Apply*.

By default, Serial Number and MAC Address are selected with differentiation enabled.

---

**NOTE:** For accurate reconciliation, we recommend that you select at least two attributes with differentiation enabled.

---



# Sample Illustrations - Enable Differentiation and Reconciliation

## Scenario 1

**Serial Number and MAC Address are selected with differentiation enabled:** For a device to reconcile to the existing device object, the Serial Number and MAC address of the existing device must match the Serial Number and MAC address of the new device.

## Scenario 2

**MAC Address and Machine Name selected with differentiation disabled:** For a device to reconcile to the existing device object, the MAC Address or the Machine name of the existing device must match the MAC address or Machine name of the new device

## Scenario 3

**Serial Number and MAC Address selected with differentiation enabled and with device having multiple MAC addresses:** The existing device object has multiple MAC addresses and the new device has multiple MAC addresses, which includes two new and one old. In this case, the new device object will still reconcile to the existing device object if any one of the MAC addresses and the Serial Number match the existing object.

## Scenario 4

**The new device and the existing device object have the same GUID but different passwords:**

Typically, reconciliation of a new device to an existing object occurs only if the device and object have different GUIDs. In this case, however, because the passwords are different, the reconciliation occurs and the new password is retained. During reconciliation, the reconciliation settings configured in ZENworks Control Center are ignored; instead, the default reconciliation settings (Serial Number and MAC Address with differentiation enabled) are used. If necessary, you can customize the default reconciliation settings in the `<Zenworks home>\conf\authreconcile.xml` file.

The default settings are as follows:



















- ◆ `authreconcile disableAuthfailure = true` [false: in case if above behavior is not desired]
- ◆ `enableReconcileignore = true` [false: in case if configured reconcile settings are to be considered]
- ◆ `disableClientID = true` [false: in case if device GUID needs to be considered for reconciliation]
- ◆ `createNewDevice = true` [false: not to create new device object in case of reconciliation failure]
















---













**NOTE:** The `authreconcile.xml` file and its settings that could be customized are considered only when there is a device which has the same GUID as the existing device object but with a different password.













---

The following table shows how different settings can help or fail device reconciliation:

	Serial number (SN)	Mac Address	Hostname	Expected
<b>Differentiation Enabled</b>				<p><b>Success:</b> The attributes of the new device must match all attributes of the existing object for successful reconciliation.</p> <p><b>Failure:</b> If there is no match with even a single attribute, reconciliation fails and a new device object is created.</p>
				The reconciliation settings are not set and thus, a new device object is created for every new device.
				<p><b>Success:</b> The Serial Number, as well as MAC address of the new device, must match the Serial Number and MAC address of the existing device object.</p> <p><b>Failure:</b> If only one of the two attributes match, then reconciliation of the new device with the existing object fails.</p>
				<p><b>Success:</b> The Serial Number, as well as the Hostname of the new device, must match the Serial Number and Hostname of the existing device object.</p> <p><b>Failure:</b> If only one of these two attributes match, then reconciliation of the new device with the existing object fails.</p>
				<p><b>Success:</b> The MAC address, as well as Hostname of the new device, must match the MAC address and Hostname of the existing device object.</p> <p><b>Failure:</b> If only one of these two attributes match, then reconciliation of the new device with the existing object fails.</p>
				<p><b>Success:</b> The Serial Number of the new device must match the Serial Number of the existing device object.</p> <p><b>Failure:</b> If the Serial Number doesn't match, then reconciliation of the new device with the existing object fails.</p>

	Serial number (SN)	Mac Address	Hostname	Expected
<b>Differentiation Enabled</b>				<p><b>Success:</b> The MAC address of the new device must match the MAC address of the existing device object.</p> <p><b>Failure:</b> If the MAC address doesn't match, then reconciliation with the existing object fails.</p>
				<p><b>Success:</b> The Hostname of the new device must match the Hostname of the existing device object.</p> <p><b>Failure:</b> If the Hostname doesn't match, then reconciliation of the new device with the existing object fails.</p>
		 <i>(multiple≥2)</i>		<p><b>Success:</b> If a device consists of multiple MAC addresses, all of them are queried and stored with the reconciliation request. Any one of the multiple MAC addresses and the Hostname of the existing device must match with any one of the MAC addresses and the Hostname of the new device for successful reconciliation.</p> <p><b>Failure:</b> If none of the MAC addresses match, reconciliation fails.</p>
		 <i>(same≥2)</i>		<p><b>Success:</b> If two or more devices have the same MAC addresses, then devices are distinguished by the Serial Number, and the device with the matching Serial Number is reconciled with the existing object.</p>
			 <i>(same≥2)</i>	<p>If two or more devices have the same Hostname, then the devices are distinguished by the Serial Number. The new device with the matching Serial Number is reconciled with the existing object.</p>

	Serial number (SN)	Mac Address	Hostname	Expected
<b>Differentiation Disabled</b>				<p><b>Success:</b> New device attributes must match with either the attributes of the existing object for successful reconciliation.</p> <p><b>Failure:</b> If none of the attributes match, reconciliation fails and a new device object is created.</p>
				<p>If the settings for device reconciliation are not set, then a new device object is created for every new device.</p> <p><b>NOTE:</b> If multiple device objects with matching attributes (such as MAC address or hostname) are found, the device object with the matching serial number gets the first preference, even if none of the attributes are selected.</p>
				<p><b>Success:</b> Either the Serial Number or the MAC address of the new device must match the Serial Number or the MAC address of the existing device object.</p> <p><b>Failure:</b> If neither of these two attributes match, then reconciliation of the new device with the existing object fails.</p>
				<p><b>Success:</b> Either the Serial Number or the Hostname of the new device must match the Serial Number or the Hostname of the existing device object.</p> <p><b>Failure:</b> If neither of these two match, then reconciliation of the new device with the existing object fails.</p>

	Serial number (SN)	Mac Address	Hostname	Expected
<b>Differentiation Disabled</b>				<p><b>Success:</b> Either the MAC address or the Hostname of the new device must match the MAC address or the Hostname of the existing device object.</p> <p><b>Failure:</b> If neither of these two match, then reconciliation of the new device with the existing object fails.</p>
				<p><b>Success:</b> The Serial Number of the new device must match the Serial Number of the existing device object.</p> <p><b>Failure:</b> If the Serial Number of the new device doesn't match, then reconciliation of the new device with the existing object fails.</p>
				<p><b>Success:</b> The MAC address of the new device must match the MAC address of the existing device object.</p> <p><b>Failure:</b> If the MAC address of the new device doesn't match, then reconciliation of the new device with the existing object fails.</p>
				<p><b>Success:</b> The Hostname of the new device must match the Hostname of the existing device object.</p> <p><b>Failure:</b> If the Hostname of the new device doesn't match, then reconciliation of the new device with the existing object fails.</p>

**IMPORTANT:** In VDI environment during the recompose of Desktop pools, if you are using VMware view 5.1 version and above, you must set the reconcile settings to Serial Number + Mac address with Enable Differentiation.

For VMware view prior to 5.1 versions, set the reconcile settings to Serial Number + Mac address + Machine Name with Enable Differentiation.

## Undoing /Resetting Device Reconciliation Settings

The changes in reconciliation settings will not reset or un-reconcile the device, because reconciliation is triggered only when a new device GUID is found.

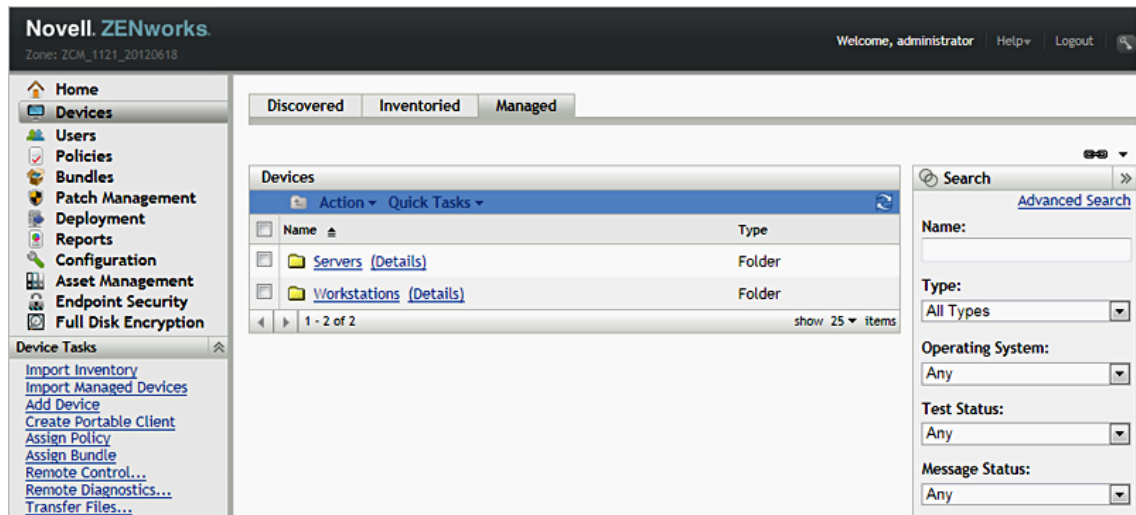
To undo device reconciliation, do the following on the device after selecting the appropriate settings in ZENworks Control Center:

- 1 Unregister the device by using the `zac unr` command.
- 2 Clear the Workstation GUID by using the `zac fsg -d` command.
- 3 Open the command prompt as an administrator, go to `%ZENworks_Home%\bin\preboot` folder, then run the `ZISWIN.exe -w` command to clear Image-safe Data.
- 4 Clear the cache by using the `zac cc` command.
- 5 Register the agent `zac reg <server url>`.

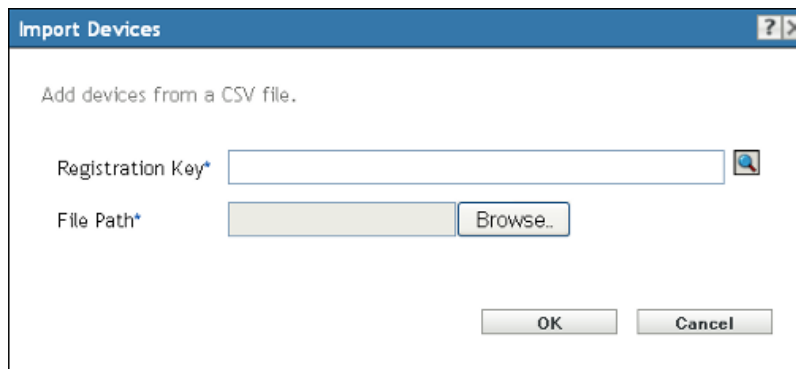
### 9.5.3 Importing Managed Devices


You can use the Import Devices dialog box to register one or more devices in the Management Zone by importing the information from a comma-separated value (CSV) file. Before importing the managed device, ensure that the registry keys have been created. Also ensure that there are limited and unlimited usage registration keys. You are allowed to execute the Import Managed Devices action regardless of whether you have registration rights or not, if you select an unlimited usage registration key.

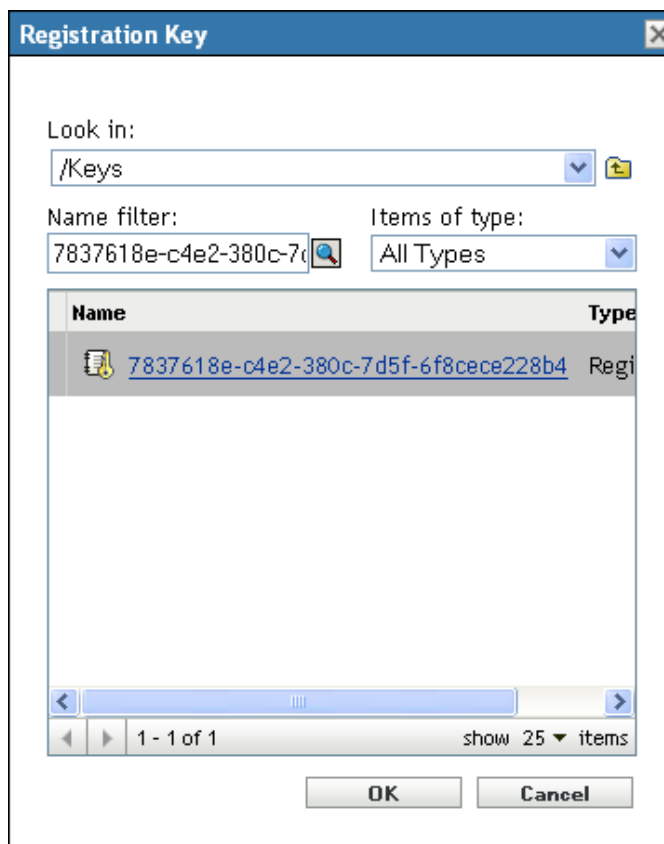
- 1 In ZENworks Control Center, click the *Devices* tab.



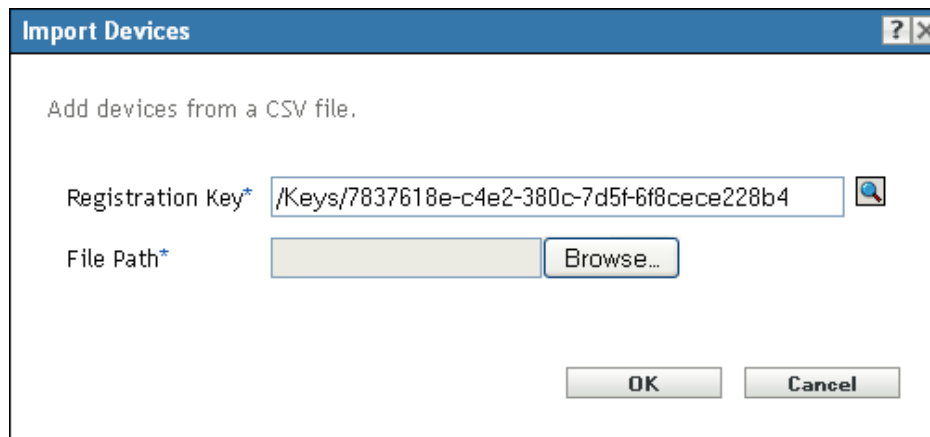
- 2 In the Device Tasks panel, click *Import Managed Devices* to display the Import Devices dialog box.



- 3 Click  to browse for and select a key in the Registration Key dialog box. The key must already exist. For more information on creating registration keys, see Section 9.2.1, "Creating a Registration Key," on page 66.



- 4 Click *OK*.



5 In the *File Path* option, browse for and select the CSV file that you created earlier. For more information see “[Creating Dummy Device Objects by Using a CSV File](#)” on page 78.

6 Click *OK*.

Choose an unlimited usage registration key to execute *Import Managed Devices* action, even when you do not have registration rights.

If you choose a limited registration key and if you do not have registration rights, the following error message is displayed:

Unable to proceed as you do not have sufficient rights on /~keys~. Contact your ZENworks Administrator.



## 9.6 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	Asset Management	System Updates	Locations	Subscriptions
<b>Management Zone Settings</b>							
Content							
<b>Device Management</b>							
<b>Category</b>	<b>Description</b>						
<a href="#">Local Device Logging</a>	Enable and configure local logging of warnings and errors encountered by managed devices.						
<a href="#">Device Refresh and Removal Schedule</a>	Configure the device refresh interval.						
<a href="#">ZENworks Agent</a>	ZENworks Agent Configuration.						
<a href="#">System Update Agent</a>	Configure system update behavior on ZENworks Agents.						
<a href="#">Registration</a>	Configure registration settings.						
<a href="#">ZENworks Explorer Configuration</a>	Configure the behavior of the ZENworks Explorer on managed devices.						
<a href="#">System Variables</a>	Configure system variables.						
<a href="#">Preboot Services</a>	Configure Preboot Services.						
<a href="#">Primary User</a>	Configure the setting for how the primary user is determined.						
<a href="#">Primary Workstation</a>	Configure the setting for how the primary workstation is determined.						
<a href="#">Dynamic Group Refresh Schedule</a>	Configure dynamic group refresh schedule.						
<a href="#">Wake-on-LAN</a>	Configure the Wake-on-LAN settings						
<a href="#">Power Management Settings</a>	Configure the schedule for the power management of Intel AMT devices.						
<a href="#">Remote Management</a>	Enable and configure remote management.						
<b>Discovery and Deployment</b>							
<b>Event and Messaging</b>							
<b>Infrastructure Management</b>							
<b>Inventory</b>							
<b>Reporting Services</b>							
<b>Endpoint Security Management</b>							
<b>Asset Management</b>							
<b>Patch Management</b>							

- 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.

**Reconcile Settings**

Indicate which device attributes will be used in reconciliation

Serial Number       Mac Address       Machine Name

Enable Differentiation

OK    Apply    Reset    Cancel

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.

## 9.7 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 9.7.1, “Performing an Initial Registration,” on page 91](#)
- ♦ [Section 9.7.2, “Reregistering a Device with an Additional Registration Key,” on page 91](#)

## 9.7.1 Performing an Initial Registration

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

```
zac reg [-k key] [-u ZENworks Administrator username -p ZENworks Administrator 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).

---

**NOTE:** The `-g` and `-k` options are meant only for the initial registration of a device. On subsequent registration requests, `-g` and `-k` options will not be honored because of the reconciliation of the device with an existing device object.

---

## 9.7.2 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.

## 9.8 Unregistering a Device

A device is automatically unregistered when the ZENworks Adaptive Agent is uninstalled. You can manually unregister a device if necessary.

### Unregistering a device by using `zac`

Unregistration of a device can be done at the device using ZENworks Adaptive Agent command line utility (`zac`):

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

```
zac unr [-f] [-u ZENworks Administrator username -p ZENworks Administrator 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.

## Unregistering a device by using the Unregister Device action

To manually unregister a device, do the following:

- 1 Log in to ZENworks Control Center.
- 2 Click *Devices > Managed*.
- 3 Select either *Servers* or *Workstations* as the type of the device, then select the devices you want to unregister from the Management zone.
- 4 Click *Action > Unregister Device*.

---

# 10 Deploying the ZENworks Adaptive Agent

Any devices you want to manage through ZENworks must have the ZENworks Adaptive Agent deployed to them. The Adaptive Agent performs all 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 11 SP3 System Requirements*.

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

- ◆ [Section 10.1, “Coexisting with the ZENworks Desktop Management Agent,” on page 93](#)
- ◆ [Section 10.2, “Customizing the Agent Features,” on page 94](#)
- ◆ [Section 10.3, “Configuring the Agent Security,” on page 97](#)
- ◆ [Section 10.4, “Changing the Target Installation Directory,” on page 101](#)
- ◆ [Section 10.5, “Using a Task to Deploy the Agent,” on page 101](#)
- ◆ [Section 10.6, “Manually Deploying the Agent on Windows,” on page 127](#)
- ◆ [Section 10.7, “Reboot-less Agent,” on page 129](#)
- ◆ [Section 10.8, “Manually Deploying the Agent on Linux,” on page 129](#)
- ◆ [Section 10.9, “Manually Deploying the Agent on a Macintosh Device,” on page 131](#)
- ◆ [Section 10.10, “Agent Deployment in VDI environment,” on page 132](#)
- ◆ [Section 10.11, “Agent Deployment on Citrix Server,” on page 133](#)
- ◆ [Section 10.12, “Package Options for Windows, Linux, and Macintosh,” on page 133](#)
- ◆ [Section 10.13, “Installing the Agent as an Add-on Product in SLES/SLED,” on page 134](#)
- ◆ [Section 10.14, “Installing the Agent by Using YUM on RHEL,” on page 136](#)

## 10.1 Coexisting with the ZENworks Desktop Management Agent

This section applies only if you want to deploy the ZENworks Adaptive Agent to devices that have the traditional ZENworks Desktop Agent installed. The traditional ZENworks Desktop Agent is included with ZENworks 7 Desktop Management.

The ZENworks Adaptive Agent and the traditional ZENworks Desktop Agent can coexist on the same device, but only to support the use of ZENworks 11 SP3 Asset Management or ZENworks 11 SP3 Patch Management with traditional ZENworks Desktop Management. ZENworks 11 SP3 Configuration Management cannot be used on the same device as traditional ZENworks Desktop Management.

When Configuration Management is activated in your Management Zone, either through a full license or an evaluation license, the following Adaptive Agent features are available for installation:

- ◆ Bundle Management
- ◆ Image Management
- ◆ Policy Management

- ◆ Remote Management
- ◆ User Management

The *Bundle Management*, *Image Management*, and *User Management* features overlap with the ZENworks Desktop Management features. Therefore, when you deploy the Adaptive Agent to a device that has the traditional ZENworks Desktop Agent installed, if you install any of these three feature modules (Bundle, Image, or User Management), the Adaptive Agent removes the ZENworks Desktop Agent before installing the features.

During deployment, the pre-agent is installed first. It then contacts the ZENworks Management Zone to identify which Adaptive Agent features should be installed. If the Bundle Management, Image, Management, or User Management features are selected to be installed, the pre-agent uninstalls the ZENworks Desktop Agent before installing the features. If the pre-agent is unable to contact the server, it stops installation of the Adaptive Agent and does not uninstall the traditional ZENworks Desktop Agent.

## 10.2 Customizing the Agent Features

The ZENworks Adaptive Agent is used with the following ZENworks 11 products: Asset Management, Configuration Management, Endpoint Security, Full Disk Encryption, and Patch Management.

To provide support for each of these products, the agent utilizes feature modules. Each feature module provides functionality for one or more products, as shown in the following table:

Product	Feature Modules
Asset Management	<ul style="list-style-type: none"> <li>◆ Asset Management</li> <li>◆ User Management</li> </ul>
Configuration Management	<ul style="list-style-type: none"> <li>◆ Bundle Management</li> <li>◆ Image Management</li> <li>◆ Policy Management</li> <li>◆ Remote Management</li> <li>◆ User Management</li> </ul>
Endpoint Security Management	<ul style="list-style-type: none"> <li>◆ Endpoint Security Management</li> <li>◆ User Management</li> </ul>
Full Disk Encryption	<ul style="list-style-type: none"> <li>◆ Full Disk Encryption</li> </ul>
Patch Management	<ul style="list-style-type: none"> <li>◆ Patch Management</li> </ul>

By default, the Adaptive Agent is configured to be installed with the feature modules associated with the products that are active (either full or evaluation license) in the Management Zone. For example, if Configuration Management and Endpoint Security Management are both active, the Bundle Management, Image Management, Policy Management, Remote Management, User Management, and Endpoint Security Management feature modules are installed and enabled by default.

Each feature module can be installed or uninstalled. If it is installed, it can either be enabled or disabled. The following sections explain how to customize the feature modules both before the Adaptive Agent is deployed and after:

- ◆ [Section 10.2.1, “Customizing Features before Deployment,” on page 95](#)
- ◆ [Section 10.2.2, “Customizing Features after Deployment,” on page 97](#)

## 10.2.1 Customizing Features before Deployment

The ZENworks Adaptive Agent is deployed with the feature modules that are enabled in the ZENworks Agent settings in the Management Zone Settings. If you don't want to deploy the agent with the default feature modules installed and enabled, you should customize the features before performing any of the following tasks:

- ◆ Creating and starting a new deployment task
- ◆ Starting an existing deployment task
- ◆ Downloading or deploying the agent manually

To customize which feature modules are installed and enabled:

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

Configuration	Registration	System Information	Asset Inventory	Asset Management	System Updates	Locations	Subscriptions
<b>Management Zone Settings</b>							
<b>Content</b>							
<b>Device Management</b>							
<b>Category</b>	<b>Description</b>						
<a href="#">Local Device Logging</a>	Enable and configure local logging of warnings and errors encountered by managed devices.						
<a href="#">Device Refresh and Removal Schedule</a>	Configure the device refresh interval.						
<a href="#">ZENworks Agent</a>	ZENworks Agent Configuration.						
<a href="#">System Update Agent</a>	Configure system update behavior on ZENworks Agents.						
<a href="#">Registration</a>	Configure registration settings.						
<a href="#">ZENworks Explorer Configuration</a>	Configure the behavior of the ZENworks Explorer on managed devices.						
<a href="#">System Variables</a>	Configure system variables.						
<a href="#">Preboot Services</a>	Configure Preboot Services.						
<a href="#">Primary User</a>	Configure the setting for how the primary user is determined.						
<a href="#">Primary Workstation</a>	Configure the setting for how the primary workstation is determined.						
<a href="#">Dynamic Group Refresh Schedule</a>	Configure dynamic group refresh schedule.						
<a href="#">Wake-on-LAN</a>	Configure the Wake-on-LAN settings.						
<a href="#">Power Management Settings</a>	Configure the schedule for the power management of Intel AMT devices.						
<a href="#">Remote Management</a>	Enable and configure remote management.						
<b>Discovery and Deployment</b>							
<b>Event and Messaging</b>							
<b>Infrastructure Management</b>							
<b>Inventory</b>							
<b>Reporting Services</b>							
<b>Endpoint Security Management</b>							
<b>Asset Management</b>							
<b>Patch Management</b>							

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

**ZENworks Agent**  
ZENworks Agent Configuration.

---

**Agent Security**

Allow users to uninstall the ZENworks Adaptive Agent

The following settings are not currently saved. Configure the settings as desired (either enabled or disabled), then click OK to save the settings. After they are saved, the settings override the agent's default security settings and any assigned Security Settings policies.

Require an uninstall password for the ZENworks Adaptive Agent

    Password:  [Change...](#)

Enable an override password for the ZENworks Adaptive Agent

    Password:  [Change...](#)

Enable self defense for the ZENworks Adaptive Agent

---

**Agent Features**

Asset Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Patch Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
User Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Image Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Remote Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Bundle Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Full Disk Encryption	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Endpoint Security Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Policy Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled

Choose the Reboot Behavior (if needed):

Prompt user to reboot (Default)

Do not reboot device

Force device to reboot

---

**General**

Cache life:  hour(s)

Cache orphaning threshold:  day(s)

Times to retry requests to a busy server:

Initial retry request wait (each subsequent request incremented by 1 second):  second(s)

Maximum retry request wait:  second(s)

### 3 In the Agent Features panel:

- ◆ If you do not want to install a feature, deselect *Installed* next to a feature. The selected feature is not installed on the device. If you choose to deselect all the features, then only the core agent is installed.
- ◆ If you want to install but disable a feature, select *Installed* and *Disabled* next to a feature. The disabled feature is not uninstalled from the currently managed devices. The feature is installed on the device, but it is nonfunctional.



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

The installation of Bundle Management, Remote Management, or User Management features requires a reboot of your device. The installation of Image Management feature requires a reboot only on Windows 2008, Windows Vista, and Windows 7. The user is prompted to reboot the device based on the selected reboot option.

## 10.2.2 Customizing Features after Deployment

The ZENworks Adaptive Agent is deployed with the security settings selected at the Management Zone level. After deploying the agent to a device, you can do any of the, following:

- ♦ Change the security settings configured at the Management Zone level
- ♦ Override the Management Zone settings at the device folder or device level

The new settings are applied to the agent on a device refresh.

For more information on how to override and configure the settings for an existing agent, see [“Configuring Adaptive Agent Settings after Deployment”](#) in the *ZENworks 11 SP3 Adaptive Agent Reference*.

## 10.3 Configuring the Agent Security

You can configure whether or not to allow users to uninstall the ZENworks Adaptive Agent. In addition, you can require a password for the uninstall, define an override password to provide access to restricted administrative features in the agent, and enable self-defense to protect agent files from being removed.

The following sections explain how to configure the security settings both before the Adaptive Agent is deployed and after:

- ♦ [Section 10.3.1, “Customizing Security before Deployment,”](#) on page 97
- ♦ [Section 10.3.2, “Customizing Security after Deployment,”](#) on page 101

### 10.3.1 Customizing Security before Deployment

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

Configuration	Registration	System Information	Asset Inventory	Asset Management	System Updates	Locations	Subscriptions
<b>Management Zone Settings</b>							
<b>Content</b>							
<b>Device Management</b>							
<b>Category</b>		<b>Description</b>					
<a href="#">Local Device Logging</a>		Enable and configure local logging of warnings and errors encountered by managed devices.					
<a href="#">Device Refresh and Removal Schedule</a>		Configure the device refresh interval.					
<a href="#">ZENworks Agent</a>		ZENworks Agent Configuration.					
<a href="#">System Update Agent</a>		Configure system update behavior on ZENworks Agents.					
<a href="#">Registration</a>		Configure registration settings.					
<a href="#">ZENworks Explorer Configuration</a>		Configure the behavior of the ZENworks Explorer on managed devices.					
<a href="#">System Variables</a>		Configure system variables.					
<a href="#">Preboot Services</a>		Configure Preboot Services.					
<a href="#">Primary User</a>		Configure the setting for how the primary user is determined.					
<a href="#">Primary Workstation</a>		Configure the setting for how the primary workstation is determined.					
<a href="#">Dynamic Group Refresh Schedule</a>		Configure dynamic group refresh schedule.					
<a href="#">Wake-on-LAN</a>		Configure the Wake-on-LAN settings					
<a href="#">Power Management Settings</a>		Configure the schedule for the power management of Intel AMT devices.					
<a href="#">Remote Management</a>		Enable and configure remote management.					
<b>Discovery and Deployment</b>							
<b>Event and Messaging</b>							
<b>Infrastructure Management</b>							
<b>Inventory</b>							
<b>Reporting Services</b>							
<b>Endpoint Security Management</b>							
<b>Asset Management</b>							
<b>Patch Management</b>							

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

**ZENworks Agent**  
ZENworks Agent Configuration.

---

**Agent Security**

Allow users to uninstall the ZENworks Adaptive Agent

The following settings are not currently saved. Configure the settings as desired (either enabled or disabled), then click OK to save the settings. After they are saved, the settings override the agent's default security settings and any assigned Security Settings policies.

Require an uninstall password for the ZENworks Adaptive Agent

    Password:  [Change...](#)

Enable an override password for the ZENworks Adaptive Agent

    Password:  [Change...](#)

Enable self defense for the ZENworks Adaptive Agent

---

**Agent Features**

Asset Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Patch Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
User Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Image Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Remote Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Bundle Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Full Disk Encryption	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Endpoint Security Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Policy Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled

Choose the Reboot Behavior (if needed):

Prompt user to reboot (Default)

Do not reboot device

Force device to reboot

---

**General**

Cache life:  hour(s)

Cache orphaning threshold:  day(s)

Times to retry requests to a busy server:

Initial retry request wait (each subsequent request incremented by 1 second):  second(s)

Maximum retry request wait:  second(s)

### 3 In the Agent Security panel:

The following setting applies to all ZENworks 11 versions of the Adaptive Agent (version 11, version 11 SP1, and version 11 SP2):

- ◆ **Allow Users to Uninstall the ZENworks Adaptive Agent:** Enable this option to allow users to perform a local uninstall of the ZENworks Adaptive Agent. If this option is disabled, the agent can only be uninstalled through the ZENworks Control Center.

The following settings apply only to the ZENworks 11 SP2 and newer versions of the Adaptive Agent. For older versions of the agent, use the Security Settings policy (one of the Windows Endpoint Security policies) to configure these settings.

- ◆ **Require an Uninstall Password for the ZENworks Adaptive Agent:** Enable this option to require users to enter a password in order to uninstall the ZENworks Adaptive Agent. Click *Change* to set the password.

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

You access the Password Key Generator utility in the *Configuration Tasks* list in the left navigation pane.

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

To enable an override password, select the check box, then click *Change* to set the password.

To avoid distributing the override password to users, we recommend that you use the Password Key Generator utility to generate a key for the override password. The key, which is based on the override password, functions the same as the override password but can be tied to a single device or user and can have a usage or time limit.

You access the Password Key Generator utility in the *Configuration Tasks* list in the left navigation pane

- ◆ **Enable Self Defense for the ZENworks Adaptive Agent** Currently, self-defense functionality protects only the ZENworks Endpoint Security Agent. It does not protect the other ZENworks Adaptive Agent modules.

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

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

Select the check box to enable self defense.

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

## 10.3.2 Customizing Security after Deployment

The ZENworks Adaptive Agent is deployed with the features selected at the Management Zone level. After deploying the agent to a device, you can do any of the, following:

- ♦ Change the agent settings configured at the Management Zone level
- ♦ Override the Management Zone settings at the device folder or device level

The new settings are applied to the agent on a device refresh.

For more information on how to override and configure the settings for an existing agent, see [“Configuring Adaptive Agent Settings after Deployment”](#) in the *ZENworks 11 SP3 Adaptive Agent Reference*.

## 10.4 Changing the Target Installation Directory

### On Windows

By default, the ZENworks Adaptive Agent is installed to the following locations:

- ♦ **On a Windows 32-bit device:** `Windows_drive:\Program Files\Novell\ZENworks`
- ♦ **On a Windows 64-bit device:** `Windows_drive:\Program Files(x86)\Novell\ZENworks`

To install the agent to a different location, you can create a ZENWORKS\_HOME system environment variable on the device prior to deployment and set the variable to the new target installation directory. Some examples of acceptable paths are:

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

### On Linux

You cannot change the target installation directory.

## 10.5 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.

This form of deployment is only supported on Windows and Linux devices.

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 10.5.1, “Prerequisites for Deploying to Windows Devices,” on page 102](#)
- ♦ [Section 10.5.2, “Prerequisites for Deploying to Linux Devices,” on page 106](#)

- ♦ [Section 10.5.3, “Deploying to a Discovered Device,” on page 107](#)
- ♦ [Section 10.5.4, “Deploying to a Non-Discovered Device,” on page 117](#)

## 10.5.1 Prerequisites for Deploying to Windows Devices

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 for Microsoft Networks” on page 102](#)
- ♦ [“Enabling File and Printer Sharing through Windows Firewall” on page 103](#)
- ♦ [“Enabling Classic File Sharing” on page 104](#)
- ♦ [“Enabling the .NET Framework” on page 105](#)

In addition to these requirements, ensure that the date and time are correct on both the ZENworks Server and on managed devices.

### Enabling File and Printer Sharing for Microsoft Networks

You need to enable the *File and Printer Sharing for Microsoft Networks* option to allow other computers on a network to access resources on your computer by using a Microsoft network.

#### Windows 2003, and Windows XP

- 1 Right-click *My Network Places > Properties*.  
The Networks Connections window is displayed.
- 2 Right-click *Local Area Connection > Properties*.  
The Local Area Connection Properties dialog box is displayed.
- 3 In the *General* tab, ensure that the *File and Printer Sharing for Microsoft Networks* option is selected.
- 4 Click *OK*.

For more information, see [File and Printer Sharing for Microsoft Networks \(http://technet.microsoft.com/en-us/library/cc779133.aspx\)](http://technet.microsoft.com/en-us/library/cc779133.aspx).

#### Windows Vista and Windows Server 2008

- 1 Right-click *Network > Properties*.  
The Network and Sharing Center window is displayed.
- 2 In the left pane, click *Manage network connections*.
- 3 Right-click *Local Area Connection > Properties*.  
The Local Area Connection Properties dialog box is displayed.
- 4 In the *Networking* tab, ensure that the *File and Printer Sharing for Microsoft Networks* option is selected.
- 5 Click *OK*.

#### Windows 7, Windows 8, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2

- 1 Right-click *Network > Properties*.

- The Network and Sharing Center window is displayed.
- 2 Right-click *Local Area Connection > Properties*.
- The Local Area Connection Properties dialog box is displayed.
- 3 In the *Networking* tab, ensure that the *File and Printer Sharing for Microsoft Networks* option is selected.
  - 4 Click *OK*.

## 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 a 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 to the Windows Firewall along with the local subnet.

### Windows Vista, Windows Server 2008

- 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*.

### Windows 7, Windows 8, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2

- 1 From the desktop *Start* menu, click *Settings > Control Panel*.
  - 2 Double-click *Windows Firewall*.
- The Windows Firewall window is displayed.
- 3 In the left pane, click *Allow a program or feature through Windows Firewall*.
  - 4 In the *Allowed Programs and Features* list, select *File and Printer Sharing*.
  - 5 Click *OK*.

### Windows 2003 and Windows XP

You can allow WMI through Windows firewall.

- 1 At the command prompt, run the following command:  

```
netsh firewall set service RemoteAdmin enable
```
- For more information on WMI, see [Connecting Through Windows Firewall \(http://msdn.microsoft.com/en-us/library/aa389286%28v=VS.85%29.aspx\)](http://msdn.microsoft.com/en-us/library/aa389286%28v=VS.85%29.aspx).

## Enabling Classic File Sharing

The ZENworks Server needs classic file sharing access to the administrative share (displayed as Admin\$) on target devices.

- ♦ [“Windows 2003” on page 104](#)
- ♦ [“Windows XP” on page 104](#)
- ♦ [“Windows Vista” on page 104](#)
- ♦ [“Windows Server 2008” on page 105](#)
- ♦ [“Windows 7, Windows 8, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2” on page 105](#)

To know in detail about the ports that are opened when you enable Classic File sharing, see [IP Discovery Technologies](#).

### 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*.
- 5 Click *OK*.

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 On 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 the Remote Registry service to start automatically, then start it.
- 5 Click *Start > Settings > Control Panel*.
- 6 Double-click *Network and Sharing Center*.
- 7 Select *Turn on File Sharing*, then click *Apply*.

## Windows Server 2008

- 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 the Remote Registry service to start automatically, then start it.
- 5 Click the desktop *Start* menu > *Settings > Control Panel*.
- 6 Double-click *Network and Sharing Center*.
- 7 Select *Turn on File Sharing*, then click *Apply*.

## Windows 7, Windows 8, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2

- 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 the Remote Registry service to start automatically, then start it.
- 5 Click the desktop *Start* menu > *Settings > Control Panel*.
- 6 Double-click *Network and Sharing Center*.
- 7 In the left pane, click *Change advanced sharing settings*.
- 8 Select *Turn on file and printer sharing*, then click *Save Changes*.

## Enabling the .NET Framework

- ♦ [“Windows 7, Windows 8” on page 106](#)
- ♦ [“Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2” on page 106](#)

The .NET 3.5 SP1 Framework is bundled with ZENworks 11 SP2. However, on the Windows 7 and Windows Server 2008 R2 devices, the .NET Framework is available by default. Therefore, before deploying the agent on the Windows 7 and Windows Server 2008 R2 devices, it is recommended to enable the .NET Framework.

You do not need to enable the .NET Framework on devices other than Windows 7 and Windows Server 2008 R2.

### Windows 7, Windows 8

- 1 Click *Start > Settings > Control Panel*.
- 2 Click *Programs and Features > Turn Windows features on and off*.  
The Windows Features dialog box is displayed.
- 3 Ensure that the *Microsoft .NET Framework 3.5.1* option is selected, then click *OK*.

### Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2

- 1 Click the desktop *Start* menu > *Settings > Control Panel*.
- 2 Click *Server Management > Features > Add Features*.
- 3 Select *.Net 3.5.1 Framework*, then click *Install*.

## 10.5.2 Prerequisites for Deploying to Linux Devices

Before the ZENworks Server can deploy the ZENworks Adaptive Agent to a Linux device, make sure that SSH Port 22 is open. To open SSH port 22 use the following procedures to add SSH as an allowed service on the target device.

To add SSH as an allowed service on Red Hat Enterprise Linux (RHEL):

- 1 Edit `vi/etc/sysconfig/iptables` to append the following rule:  

```
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
```
- 2 Save the iptables file.
- 3 Restart the ip tables service by running either the service iptables restart command or the `/etc/init.d/iptables restart` command.

To add SSH as an allowed service on SUSE Linux Enterprise Server (SLES) and SUSE Linux Enterprise Desktop (SLED):

- 1 Edit the following file:  
`/etc/sysconfig/SuSEfirewall2`
- 2 Add SSH to the list of ports under `FW_SERVICES_<Firewall Zone>_TCP`.  
For example, for an external zone, add SSH under `FW_SERVICES_EXT_TCP="ssh"`.
- 3 Run the following command:  
`/sbin/SuSEfirewall2`.

## Prerequisites for Agent install on a Red Hat 4 device

Java Runtime Environment (JRE) 1.6 is a prerequisite for agent install on a Red Hat 4 device. Perform the following steps to install JRE 1.6:

- 1 Run the `mkdir -p /opt/novell/zenworks/share/zmd` command to create a folder structure `/opt/novell/zenworks/share/zmd`
- 2 Install Java Runtime Environment (JRE) 1.6 by using one of the following methods:
  1. In this location `/opt/novell/zenworks/share/zmd` create a folder called `java`.
  2. Install JRE 1.6 within `java` folder.

Or

1. Install JRE 1.6 in any location.
2. Create a symbolic link called `java` under `/opt/novell/zenworks/share/zmd` which points to the JRE 1.6 install location. For example, if JRE 1.6 is installed in `/usr/java/jre1.6.0_40`, then the symbolic link must be created by using `ln -s /usr/java/jre1.6.0_40 /opt/novell/zenworks/share/zmd/java` command.

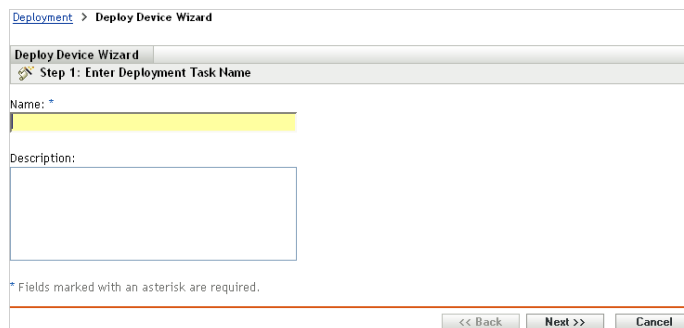
### 10.5.3 Deploying to a Discovered Device

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 10.5.4, "Deploying to a Non-Discovered Device," on page 117](#)).

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.




- 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: <code>\/ * ? : " ' &lt; &gt;   ` % ~</code>

Wizard Page	Details
Select Devices page	<p>Allows you to identify the devices to which you want to deploy the ZENworks Adaptive Agent.</p> <p>Click <i>Add</i> to display the Discovered Device Browser dialog box.</p> <p>You can deploy to the target devices by using one of the following options:</p> <ul style="list-style-type: none"> <li>◆ DNS Name</li> <li>◆ IP Address</li> </ul> <p>If you select <i>IP Address</i> and if the target device is not reachable by using the IP address, the deployment uses the DNS name. If you select <i>DNS Name</i> and if the target device is not reachable by using the DNS name, the deployment uses the IP address. If the deployment uses a proxy, the target device is only connected by using the option provided.</p>
Discovered Device Browser dialog box > <i>Source</i> > <i>IP Address</i>	<ol style="list-style-type: none"> <li>1. In the <i>Source</i> list, select <i>IP Address</i>.</li> <li>2. Fill in the <i>IP Address Range/Host Name</i> field. <p>The address can use any of the following formats:</p> <p><i>xxx.xxx.xxx.xxx</i>: Standard dotted-decimal notation for a single address. For example, 123.45.167.100.</p> <p><i>xxx.xxx.xxx.xxx - xxx.xxx.xxx.xxx</i>: Standard dotted-decimal notation for a range of addresses. For example, 123.45.167.100 - 123.45.167.125.</p> <p><i>xxx.xxx.xxx.xxx/n</i>: Standard CIDR (Classless Inter-Domain Routing) notation. For example, 123.45.167.100/24 matches all IP addresses that start with 123.45.167.</p> <p><i>hostname</i>: Standard device hostname. For example, workstation1.</p> </li> <li>3. To add the device to the <i>Selected Devices</i> list, click <i>Add</i>.</li> <li>4. When you are finished selecting devices, click <i>OK</i>.</li> </ol>

Wizard Page	Details
Discovered Device Browser dialog box > <i>Source</i> > <i>Add New CSV File</i>	<ol style="list-style-type: none"> <li>1. In the <i>Source</i> list, select <i>Add New CSV File</i> to display the Add New Source dialog box.</li> <li>2. Fill in the following fields: <ul style="list-style-type: none"> <li><b>CSV File:</b> Browse for and select the CSV file containing the devices to which you want to deploy the agent.</li> <li><b>DNS Name Column:</b> Select the number of the column that contains the DNS name information.</li> <li><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.</li> <li><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.</li> </ul> </li> <li>3. Click <b>OK</b> to display the devices in the source list.</li> <li>4. Click  to move a device to the <i>Selected Devices</i> list.</li> <li>5. When you are finished selecting devices, click <i>OK</i>.</li> </ol>
Discovered Device Browser dialog box > <i>Source</i> > existing user source	<ol style="list-style-type: none"> <li>1. 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>2. Browse the directory to find the desired device.</li> <li>3. Click  to move the device to the <i>Selected Devices</i> list.</li> <li>4. When you are finished selecting devices, click <i>OK</i>.</li> </ol>


Wizard Page	Details
Discovered Device Browser dialog box > <i>Source</i> > <i>Add New LDAP Source</i>	<ol style="list-style-type: none"> <li>1. In the <i>Source</i> list, select <i>Add New LDAP Source</i> to display the Add New Source dialog box.</li> <li>2. Fill in the following fields: <ul style="list-style-type: none"> <li><b>LDAP Source Name:</b> Provide a name for the LDAP source.</li> <li><b>LDAP Server:</b> Specify the IP address or DNS hostname of the LDAP server.</li> <li><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.</li> <li><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.</li> <li><b>Save Credentials to Data store:</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.</li> <li><b>Credentials:</b> Click Add 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.</li> </ul> <p>For Novell eDirectory access, use standard LDAP notation. For example:</p> <pre>cn=admin_read_only,ou=users,o=mycompany</pre> <p>For Microsoft Active Directory, use standard domain notation. For example:</p> <pre>AdminReadOnly@mycompany.com</pre> </li> <li>3. Click <i>OK</i> to display the LDAP directory in the source list.</li> <li>4. Browse the directory to find the desired device.</li> <li>5. Click  to move the 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 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 should 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 on Windows:</p> <ol style="list-style-type: none"> <li>1. Click <i>Add</i> to display the Enter Credential Information dialog box.</li> <li>2. In the <i>Type</i> list, select the type of operating system for which you want to enter the credential.</li> <li>3. In the <i>Username</i> field, specify the appropriate username.</li> </ol> <p>To deploy the 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>4. In the <i>Password</i> and <i>Reenter Password</i> fields, enter the user password.</li> <li>5. Click <i>OK</i> to save the credential.</li> </ol>
Select Schedule page	<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> <p>Specify only the root credential to deploy the Adaptive Agent on Linux.</p> <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 B, "Schedules," on page 161</a> or click the <i>Help</i> button for more 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>
Select or Edit a Proxy Device page	<p>The Select or Edit a Proxy Device page lets you choose whether you want to use a proxy device to perform the deployment task.</p>


Wizard Page	Details
Select or Edit a Proxy Device page > <i>Windows Proxy</i>	<p>If you want to use a Windows Proxy instead of the Primary Server to perform the deployment tasks on Windows devices, click the <i>Windows Proxy</i> option and configure the settings in the Select Windows Proxy dialog box.</p> <p>A Windows Proxy is used to perform the following actions:</p> <ul style="list-style-type: none"> <li>◆ Enable Linux Primary Servers to perform deployment tasks on Windows devices.</li> <li>◆ Deploy Windows devices that are in a different subnet than the Primary Server.</li> <li>◆ Deploy Windows devices in a network enabled for NAT.</li> </ul> <p>The connection between the ZENworks Server and the Windows Proxy is secured through SSL.</p> <p>For deployment, you need to add File and Printer Sharing as an exception in the Windows Firewall configuration settings. By default, the scope of the exception applies only to a local subnet. If the target device is in a different subnet than the Primary Server from which the deployment is run, you also need to add the IP address of the Primary Server as an exception. However, if you use a Windows Proxy in the same subnet as a target device, you do not need to change the scope of the Windows Firewall exception.</p> <p><b>Override Zone Windows Proxy Settings:</b> Select this option if you want to override the Windows Proxy settings configured at the Management Zone and configure new settings for the task.</p> <p><b>Windows Proxy:</b> Select a Windows managed device (server or workstation) to be used as a Windows Proxy for performing the deployment tasks instead of a ZENworks Server. The Windows Proxy must reside in the same network as the target devices.</p> <p><b>Windows Proxy Timeout:</b> Specify the number of seconds you want the ZENworks Server to wait for a response from the Windows Proxy.</p>



Wizard Page	Details
Select or Edit a Proxy Device page > <i>Linux Proxy</i>	<p>If you want to use a Linux Proxy instead of the Primary Server to perform the deployment tasks on Linux devices, click the <i>Linux Proxy</i> option and configure the settings in the Select Linux Proxy dialog box.</p> <p>A Linux Proxy is used to perform the following actions:</p> <ul style="list-style-type: none"> <li>◆ Enable Primary Servers to offload a deployment task to a Linux Proxy if the task includes devices in a different subnet.</li> <li>◆ Deploy Linux devices in a different subnet than the Primary Server.</li> <li>◆ Deploy Linux devices in a network enabled for NAT.</li> </ul> <p>The SSH discovery requires port 22 to be reachable in order to enable the Primary Server to connect to the target device. If the SSH port is blocked in the Network Firewall, you use a Linux managed device in the same subnet as the target device.</p> <p><b>Override Zone Linux Proxy Settings:</b> Select this option if you want to override the Linux Proxy settings configured at the Management Zone and configure new settings for the task.</p> <p><b>Linux Proxy:</b> Select a Linux managed device (server or workstation) to be used as a Linux Proxy for performing the deployment tasks instead of a ZENworks Server. The Linux Proxy must reside in the same network as the target devices.</p> <p><b>Linux Proxy Timeout:</b> Specify the number of seconds you want the ZENworks Server to wait for a response from the Linux Proxy.</p>

Wizard Page	Details
Windows Options page > <i>Reboot Option</i> field	<p>After installation of the ZENworks Adaptive Agent, a device must reboot to make the agent functional. Do the following:</p> <ol style="list-style-type: none"> <li>Select the desired reboot option. <ul style="list-style-type: none"> <li><b>Immediate:</b> To reboot immediately after installation of the Adaptive Agent, select <i>Immediate</i> to force the device</li> <li><b>Manual:</b> To allow the user to manually reboot the device at his or her convenience, select <i>Manual</i>.</li> <li><b>Scheduled:</b> To reboot the device at a specified time, select <i>Scheduled</i>. Fill in the schedule's fields. <ul style="list-style-type: none"> <li><b>Start Date:</b> Click  to display a calendar you can use to select a date for the event.</li> <li><b>Start Time:</b> Specify the time at which the event must start.</li> <li><b>Use Coordinated Universal Time (UTC):</b> 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.</li> </ul> </li> </ul> </li> <li>(Optional) Select the <i>Do Not Prompt for Reboot</i> option if you do not want the reboot prompt message to be displayed. <ul style="list-style-type: none"> <li><b>Start ZENworks Agent with limited functionality:</b> (Optional) This is enabled only if you select <i>Manual</i> reboot option. Select this option to start ZENworks Agent with limited functionality and without rebooting a device. <b>IMPORTANT:</b> If you select <i>Immediate</i> or <i>Manual</i> reboot option, and <i>Do not prompt for reboot</i> option, then <i>Cancel</i> the reboot after agent install, a prompt is displayed to start the ZENworks agent with limited functionality. If user selects <i>Yes</i>, the agent service starts with limited functionality until a reboot is done.</li> </ul> </li> </ol> <p><b>NOTE:</b> The Windows Options page is displayed only if you have provided Windows credentials on the <a href="#">Enter Credentials</a> page.</p>

Wizard Page	Details
Windows Options page > <i>Permission Prompt Options</i> fields	<p>After deployment, you can use these options to postpone the agent installation on the target machine:</p> <ul style="list-style-type: none"> <li>◆ <b>Show Permission Prompt:</b> Select <i>On</i> to display a dialog box on the agent when the installation is ready to begin. Users can cancel, postpone, or allow the installation to begin based on the Permission Prompt options configured by the Zone administrator.</li> </ul> <p><b>NOTE:</b> By default, this setting is set to <i>Off</i>, so users cannot cancel or postpone the installation. The installation begins immediately without any prompt. If you select <i>On</i>, the following options are enabled:</p> <ul style="list-style-type: none"> <li>◆ <b>Prompt Max Postpone:</b> Specify how many times a user can postpone or snooze the installation. Select <i>Unlimited</i> to let the user postpone the installation an unlimited number of times, or select <i>Limit To</i>, then specify the number of times the user can postpone the installation.</li> <li>◆ <b>Prompt Timeout:</b> Specify how long to wait for an answer before the installation begins. To display the permission prompt until the user responds, select <i>No Timeout</i>. Or, select <i>Timeout after _ mins</i> and specify the number of minutes you want an unanswered prompt to remain on the user's screen before the installation starts. By default, the user has five minutes to respond to the prompt.</li> <li>◆ <b>Prompt Nag Time:</b> Specify, in minutes, how often the prompt should appear to let a user know that an installation is waiting to start. By default, this prompt displays every 15 minutes.</li> <li>◆ <b>Prompt Max Wait Time:</b> Specify the maximum timeout for which the agent installation can be postponed. When this timeout is reached, the agent installation starts even if there are other prompt messages remaining.</li> <li>◆ <b>Agent Message Overrides:</b> Customize the text for agent installation messages that display in dialog boxes during the installation. Click <i>Add</i> to display the Edit Agent Installation Message dialog box. Select a Message Key from the drop-down list, type the desired text, then click <i>OK</i>.</li> </ul>
Windows Options page > <i>Deployment Package</i> field	<p>Depending upon the processor architecture of the managed device, select the deployment package to be used for installing ZENworks Adaptive Agent on the device.</p> <p>If you are not sure about the device's processor architecture, choose the package with target architecture as <i>All</i>, which applies to 32-bit and 64-bit platforms.</p> <p>If the selected package has been deleted from the Primary Server, then the default deployment package is deployed.</p>

Wizard Page	Details
Windows Options page > <i>Agent Installation Folder</i> field	<p>Specify the directory on the managed device where you want to install ZENworks Adaptive Agent. By default, the agent is installed to the directory specified in the <code>%ZENWORKS_HOME%</code> system environmental variable or to the <code>%ProgramFiles%\novell\zenworks</code> directory if the variable is not set on the managed device.</p> <p>Ensure that the installation path does not contain spaces.</p> <p><b>NOTE:</b> If the directory you specify cannot be created, then the agent is installed in the default location.</p>
Linux Options page	<p>The Linux Options page lets you configure the installation options to make the ZENworks Adaptive Agent functional after the installation of the agent on the Linux devices.</p> <p><b>Deployment Package:</b> Depending upon the processor architecture of the managed device, select the deployment package to be used for installing ZENworks Adaptive Agent on the device. If you are not sure about the device's processor architecture, choose the package with target architecture as All, which applies to 32-bit and 64-bit platforms. If the selected package has been deleted from the Primary Server, then the default deployment package is deployed.</p> <p><b>Installation Options:</b> Configure the following options for deploying the ZENworks Adaptive Agent:</p> <ul style="list-style-type: none"> <li>◆ <b>Do Not Install the GUI Packages:</b> Select this option if you do not want to install the RPMs that provide a GUI interface for the ZENworks Adaptive Agent such as the  icon.</li> <li>◆ <b>Disable SELinux for Red Hat Devices:</b> Select this option to disable SELinux (Security-Enhanced Linux).  SELinux provides limited access control on Linux. Select this option to disable SELinux if the agent is unable to open the ports required by ZENworks. SELinux is temporarily disabled only if the agent is unable to open the ports, and is automatically enabled again after the agent installation.</li> </ul> <p><b>NOTE:</b> The Linux Options page is displayed only if you have provided Linux credentials on the <a href="#">Enter Credentials</a> page.</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 9, "Registering Devices," on page 63</a>.</p>

Wizard Page	Details
Pre/Post Deployment page	<p>Specify commands that you want to run before and after the 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 pre-agent as part of the deployment task package. The pre-agent executes the commands in the system space, so you must specify commands that do not require user interaction.</p> <p>For more information about predeployment and post-deployment commands, click the <i>Help</i> button.</p>

When you finish the wizard, the deployment task is added to the list in the Deployment Tasks panel. You can use the panel to manage current tasks and create new tasks for deploying the ZENworks Adaptive Agent to devices. The panel includes the following information for each task:

- ◆ **Name:** Displays the name given to the task. If *Credentials Cleared* is displayed below the task name, the credentials required to perform the task on the targeted devices have been cleared from the ZENworks Server's memory and must be entered again. To avoid having credentials lost when they are cleared from memory, you must store them in the ZENworks database.
- ◆ **Schedule:** Displays the dates on which the task is scheduled to run.
- ◆ **Status:** Displays the following status information: *Scheduled, Pending, Installing, Registering, Inactive, Finished, or Error*. You can mouse over certain statuses to receive more information about the status.

If an error occurred, the error is also recorded for the target device in the Deployable Devices panel. You can click the target device in the Deployable Devices panel to receive more information about the error.

## 10.5.4 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 deployment 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.


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

The screenshot shows the 'Deploy Device Wizard' window. The title bar reads 'Deployment > Deploy Device Wizard'. Below the title bar, there's a tab labeled 'Deploy Device Wizard'. The main content area is titled 'Step 1: Enter Deployment Task Name'. It contains two input fields: 'Name: \*' (with an asterisk indicating it's required) and 'Description:'. At the bottom of the window, there are three buttons: '<< Back', 'Next >>', and 'Cancel'. A small note at the bottom left states '\* 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	<p>Allows you to identify the devices to which you want to deploy the ZENworks Adaptive Agent.</p> <p>Click <i>Add</i> to display the Discovered Device Browser dialog box.</p> <p>You can deploy to the target devices by using one of the following options:</p> <ul style="list-style-type: none"> <li>◆ DNS Name</li> <li>◆ IP Address</li> </ul> <p>If you select <i>IP Address</i> and if the target device is not reachable by using the IP address, the deployment uses the DNS name. If you select <i>DNS Name</i> and if the target device is not reachable by using the DNS name, the deployment uses the IP address. If the deployment uses a proxy, the target device is only connected by using the option provided.</p>
Discovered Device Browser dialog box > <i>Source</i> > <i>IP Address</i>	<ol style="list-style-type: none"> <li>1. In the <i>Source</i> list, select <i>IP Address</i>.</li> <li>2. Fill in the <i>IP Address Range/Host Name</i> field. <p>The address can use any of the following formats:</p> <p>xxx.xxx.xxx.xxx: Standard dotted-decimal notation for a single address. For example, 123.45.167.100.</p> <p>xxx.xxx.xxx.xxx - xxx.xxx.xxx.xxx: Standard dotted-decimal notation for a range of addresses. For example, 123.45.167.100 - 123.45.167.125.</p> <p>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.</p> <p>hostname: Standard device hostname. For example, workstation1.</p> </li> <li>3. To add the device to the <i>Selected Devices</i> list, click <i>Add</i>.</li> <li>4. When you are finished selecting devices, click <i>OK</i>.</li> </ol>

Wizard Page	Details
Discovered Device Browser dialog box > <i>Source</i> > <i>Add New CSV File</i>	<ol style="list-style-type: none"> <li>1. In the <i>Source</i> list, select <i>Add New CSV File</i> to display the Add New Source dialog box.</li> <li>2. Fill in the following fields: <ul style="list-style-type: none"> <li><b>CSV File:</b> Browse for and select the CSV file containing the devices to which you want to deploy the agent.</li> <li><b>DNS Name Column:</b> Select the number of the column that contains the DNS name information.</li> <li><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.</li> <li><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.</li> </ul> </li> <li>3. Click <b>OK</b> to display the devices in the source list.</li> <li>4. Click  to move a device to the <i>Selected Devices</i> list.</li> <li>5. When you are finished selecting devices, click <i>OK</i>.</li> </ol>
Discovered Device Browser dialog box > <i>Source</i> > existing user source	<ol style="list-style-type: none"> <li>1. 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>2. Browse the directory to find the desired device.</li> <li>3. Click  to move the device to the <i>Selected Devices</i> list.</li> <li>4. When you are finished selecting devices, click <i>OK</i>.</li> </ol>

Wizard Page	Details
<p>Discovered Device Browser dialog box &gt; <i>Source</i> &gt; <i>Add New LDAP Source</i></p>	<ol style="list-style-type: none"> <li>In the <i>Source</i> list, select <i>Add New LDAP Source</i> to display the Add New Source dialog box.</li> <li>Fill in the following fields: <ul style="list-style-type: none"> <li><b>LDAP Source Name:</b> Provide a name for the LDAP source.</li> <li><b>LDAP Server:</b> Specify the IP address or DNS hostname of the LDAP server.</li> <li><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.</li> <li><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.</li> <li><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.</li> <li><b>Credentials:</b> Click Add 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.</li> </ul> <p>For Novell eDirectory access, use standard LDAP notation. For example:</p> <pre>cn=admin_read_only,ou=users,o=mycompany</pre> <p>For Microsoft Active Directory, use standard domain notation. For example:</p> <pre>AdminReadOnly@mycompany.com</pre> </li> <li>Click <i>OK</i> to display the LDAP directory in the source list.</li> <li>Browse the directory to find the desired device.</li> <li>Click  to move the device to the <i>Selected Devices</i> list.</li> <li>When you are finished selecting devices, click <i>OK</i>.</li> </ol>
<p>Enter Credentials page &gt; <i>Save Credentials to DataStore</i> field</p>	<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 should 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>1. Click <i>Add</i> to display the Enter Credential Information dialog box.</li> <li>2. In the <i>Type</i> list, select the type of operating system for which you want to enter the credential.</li> <li>3. In the <i>Username</i> field, specify the appropriate username.</li> </ol> <p>To deploy the 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>4. In the <i>Password</i> and <i>Reenter Password</i> fields, enter the user password.</li> <li>5. Click <i>OK</i> to save the credential.</li> </ol>
Select Schedule page	<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> <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 B, "Schedules," on page 161</a> or click the <i>Help</i> button for more 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>
Select or Edit a Proxy Device page	<p>The Select or Edit a Proxy Device page lets you choose whether you want to use a proxy device to perform the deployment task.</p>

Wizard Page	Details
Select or Edit a Proxy Device page > <i>Windows Proxy</i>	<p>If you want to use a Windows Proxy instead of the Primary Server to perform the deployment tasks on Windows devices, click the <i>Windows Proxy</i> option and configure the settings in the Select Windows Proxy dialog box.</p> <p>A Windows Proxy is used to perform the following actions:</p> <ul style="list-style-type: none"> <li>◆ Enable Linux Primary Servers to perform deployment tasks on Windows devices.</li> <li>◆ Deploy Windows devices that are in a different subnet than the Primary Server.</li> <li>◆ Deploy Windows devices in a network enabled for NAT.</li> </ul> <p>The connection between the ZENworks Server and Windows Proxy is secured through SSL.</p> <p>For deployment, you need to add File and Printer Sharing as an exception in the Windows Firewall configuration settings. By default, the scope of the exception applies only to a local subnet. If the target device is in a different subnet than the Primary Server from which the deployment is run, you also need to add the IP address of the Primary Server as an exception. However, if you use a Windows Proxy in the same subnet as a target device, you do not need to change the scope of the Windows Firewall exception.</p> <p><b>Override Zone Windows Proxy Settings:</b> Select this option if you want to override the Windows Proxy settings configured at the Management Zone and configure new settings for the task.</p> <p><b>Windows Proxy:</b> Select a Windows managed device (server or workstation) to be used as a Windows Proxy for performing the deployment tasks instead of a ZENworks Server. The Windows Proxy must reside in the same network as the target devices.</p> <p><b>Windows Proxy Timeout:</b> Specify the number of seconds you want the ZENworks Server to wait for a response from the Windows Proxy.</p>


---

Wizard Page	Details
Select or Edit a Proxy Device page > <i>Linux Proxy</i>	<p>If you want to use a Linux Proxy instead of the Primary Server to perform the deployment tasks on Linux devices, click the <i>Linux Proxy</i> option and configure the settings in the Select Linux Proxy dialog box.</p> <p>A Linux Proxy is primarily used for Primary Servers if you want to deploy to Linux devices in a different subnet than the Primary Server. When a Primary Server receives a deployment task that includes devices in a different subnet, it offloads the deployment tasks to the Linux Proxy. A Linux Proxy is also used for performing deployment tasks on Linux devices in a network enabled for NAT.</p> <p>The SSH discovery requires port 22 to be reachable in order to enable the Primary Server to connect to the target device. If the SSH port is blocked in the Network Firewall, you use a Linux managed device in the same subnet as the target device.</p> <p><b>Override Zone Linux Proxy Settings:</b> Select this option if you want to override the Linux Proxy settings configured at the Management Zone and configure new settings for the task.</p> <p><b>Linux Proxy:</b> Select a Linux managed device (server or workstation) to be used as a Linux Proxy for performing the deployment tasks instead of a ZENworks Server. The Linux Proxy must reside in the same network as the target devices.</p> <p><b>Linux Proxy Timeout:</b> Specify the number of seconds you want the ZENworks Server to wait for a response from the Linux Proxy.</p>

---

Wizard Page	Details
Windows Options page > <i>Reboot Option</i> field	<p>After installation of the ZENworks Adaptive Agent, a device must reboot to make the agent functional. Do the following:</p> <ol style="list-style-type: none"> <li>Select the desired reboot option. <ul style="list-style-type: none"> <li><b>Immediate:</b> To reboot immediately after installation of the Adaptive Agent, select <i>Immediate</i> to force the device</li> <li><b>Manual:</b> To allow the user to manually reboot the device at his or her convenience, select <i>Manual</i>.</li> <li><b>Scheduled:</b> To reboot the device at a specified time, select <i>Scheduled</i>. Fill in the schedule's fields. <ul style="list-style-type: none"> <li><b>Start Date:</b> Click  to display a calendar you can use to select a date for the event.</li> <li><b>Start Time:</b> Specify the time at which the event must start.</li> <li><b>Use Coordinated Universal Time (UTC):</b> 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.</li> </ul> </li> </ul> </li> <li>(Optional) Select the <i>Do Not Prompt for Reboot</i> option if you do not want the reboot prompt message to be displayed. <ul style="list-style-type: none"> <li><b>Start ZENworks Agent with limited functionality:</b> (Optional) This is enabled only if you select <i>Manual</i> reboot option. Select this option to start ZENworks Agent with limited functionality and without rebooting a device. <b>IMPORTANT:</b> If you select <i>Immediate</i> or <i>Manual</i> reboot option, and <i>Do not prompt for reboot</i> option, then <i>Cancel</i> the reboot after agent install, a prompt is displayed to start the ZENworks agent with limited functionality. If user selects <i>Yes</i>, the agent service starts with limited functionality until a reboot is done.</li> </ul> </li> </ol> <p><b>NOTE:</b> The Windows Options page is displayed only if you have provided Windows credentials on the <a href="#">Enter Credentials</a> page.</p>

Wizard Page	Details
Windows Options page > <i>Permission Prompt Options</i> fields	<p>After deployment, you can use these options to postpone the agent installation on the target machine:</p> <ul style="list-style-type: none"> <li>◆ <b>Show Permission Prompt:</b> Select <i>On</i> to display a dialog box on the agent when the installation is ready to begin. Users can cancel, postpone, or allow the installation to begin based on the Permission Prompt options configured by the Zone administrator.</li> </ul> <p><b>NOTE:</b> By default, this setting is set to <i>Off</i>, so users cannot cancel or postpone the installation. The installation begins immediately without any prompt. If you select <i>On</i>, the following options are enabled:</p> <ul style="list-style-type: none"> <li>◆ <b>Prompt Max Postpone:</b> Specify how many times a user can postpone or snooze the installation. Select <i>Unlimited</i> to let the user postpone the installation an unlimited number of times, or select <i>Limit To</i>, then specify the number of times the user can postpone the installation.</li> <li>◆ <b>Prompt Timeout:</b> Specify how long to wait for an answer before the installation begins. To display the permission prompt until the user responds, select <i>No Timeout</i>. Or, select <i>Timeout after _ mins</i> and specify the number of minutes you want an unanswered prompt to remain on the user's screen before the installation starts. By default, the user has five minutes to respond to the prompt.</li> <li>◆ <b>Prompt Nag Time:</b> Specify, in minutes, how often the prompt should appear to let a user know that an installation is waiting to start. By default, this prompt displays every 15 minutes.</li> <li>◆ <b>Prompt Max Wait Time:</b> Specify the maximum timeout for which the agent installation can be postponed. When this timeout is reached, the agent installation starts even if there are other prompt messages remaining.</li> <li>◆ <b>Agent Message Overrides:</b> Customize the text for agent installation messages that display in dialog boxes during the installation. Click <i>Add</i> to display the Edit Agent Installation Message dialog box. Select a Message Key from the drop-down list, type the desired text, then click <i>OK</i>.</li> </ul>
Windows Options page > <i>Deployment Package</i> field	<p>Depending upon the processor architecture of the managed device, select the deployment package to be used for installing ZENworks Adaptive Agent on the device.</p> <p>If you are not sure about the device's processor architecture, choose the package with target architecture as <i>All</i>, which applies to 32-bit and 64-bit platforms.</p> <p>If the selected package has been deleted from the Primary Server, then the default deployment package is deployed.</p>

Wizard Page	Details
Windows Options page > <i>Agent Installation Folder</i> field	<p>Specify the directory on the managed device where you want to install ZENworks Adaptive Agent. By default, the agent is installed to the directory specified in the <code>%ZENWORKS_HOME%</code> system environmental variable or to the <code>%ProgramFiles%\novell\zenworks</code> directory if the variable is not set on the managed device.</p> <p>Ensure that the installation path does not contain spaces.</p> <p><b>NOTE:</b> If the directory you specify cannot be created, then the agent is installed in the default location.</p>
Linux Options page	<p>The Linux Options page lets you configure the installation options to make the ZENworks Adaptive Agent functional after the installation of the agent on the Linux devices.</p> <p><b>Deployment Package:</b> Depending upon the processor architecture of the managed device, select the deployment package to be used for installing ZENworks Adaptive Agent on the device. If you are not sure about the device's processor architecture, choose the package with target architecture as All, which applies to 32-bit and 64-bit platforms. If the selected package has been deleted from the Primary Server, then the default deployment package is deployed.</p> <p><b>Installation Options:</b> Configure the following options for deploying the ZENworks Adaptive Agent:</p> <ul style="list-style-type: none"> <li>◆ <b>Do Not Install the GUI Packages:</b> Select this option if you do not want to install the RPMs that provide a GUI interface for the ZENworks Adaptive Agent such as the  icon.</li> <li>◆ <b>Disable SELinux for Red Hat Devices:</b> Select this option to disable SELinux (Security-Enhanced Linux).  SELinux provides limited access control on Linux. Select this option to disable SELinux if the agent is unable to open the ports required by ZENworks. SELinux is temporarily disabled only if the agent is unable to open the ports, and is automatically enabled again after the agent installation.</li> </ul> <p><b>NOTE:</b> The Linux Options page is displayed only if you have provided Linux credentials on the <a href="#">Enter Credentials</a> page.</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 9, "Registering Devices," on page 63</a>.</p>

Wizard Page	Details
Pre/Post Deployment page	<p>Specify commands that you want to run before and after the 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 pre-agent as part of the deployment task package. The pre-agent executes the commands in the system space, so you must specify commands that do not require user interaction.</p> <p>For more information about predeployment and post-deployment commands, click the <i>Help</i> button.</p>

When you finish the wizard, the deployment task is added to the list in the Deployment Tasks panel. You can use the panel to manage current tasks and create new tasks for deploying the ZENworks Adaptive Agent to devices. The panel includes the following information for each task:

- ◆ **Name:** Displays the name given to the task. If *Credentials Cleared* is displayed below the task name, the credentials required to perform the task on the targeted devices have been cleared from the ZENworks Server's memory and must be entered again. To avoid having credentials lost when they are cleared from memory, you must store them in the ZENworks database.
- ◆ **Schedule:** Displays the dates on which the task is scheduled to run.
- ◆ **Status:** Displays the following status information: *Scheduled*, *Pending*, *Installing*, *Registering*, *Inactive*, *Finished*, or *Error*. You can mouse over certain statuses to receive more information about the status.

If an error occurred, the error is also recorded for the target device in the Deployable Devices panel. You can click the target device in the Deployable Devices panel to receive more information about the error.

## 10.6 Manually Deploying the Agent on Windows

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. For details see "Managed Device Requirements" in the [ZENworks 11 SP3 System Requirements](#).
- 2 On the target device, open a Web browser to the following address:

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

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

**Novell. ZENworks**  
Zone: DOC\_Aug14\_ZEN11

**Welcome to the ZENworks download page**

Here you can download specific ZENworks components and tools. To view the listing of available tools, click the desired menu item to the left.

The ZENworks Adaptive Agent can be downloaded from the list below by clicking on the link entitled "Default". Please note that the "Network" install type requires Microsoft .NET be installed prior to running the installation.

Package Name	Target Platform	Target Architecture	Install Type	Size
<a href="#">Default Agent (x86_Network)</a>	Microsoft Windows	x86 Architecture (32 bit)	Network (.NET required)	0.9 MB
<a href="#">Default Agent (x86_Complete)</a>	Microsoft Windows	x86 Architecture (32 bit)	Standalone (.NET required)	78 MB
<a href="#">Default Agent (x86_Complete)</a>	Microsoft Windows	x86 Architecture (32 bit)	Standalone	309.5 MB
<a href="#">Default Agent (x86_64_Network)</a>	Microsoft Windows	x86_64 Architecture (64 bit)	Network (.NET required)	0.9 MB
<a href="#">Default Agent (x86_64_Complete)</a>	Microsoft Windows	x86_64 Architecture (64 bit)	Standalone (.NET required)	79.6 MB
<a href="#">Default Agent (x86_64_Complete)</a>	Microsoft Windows	x86_64 Architecture (64 bit)	Standalone	311.1 MB
<a href="#">Default Agent (x86_Network)</a>	Linux	x86 Architecture (32 bit)	Network (JRE required)	1 MB
<a href="#">Default Agent (x86_Complete)</a>	Linux	x86 Architecture (32 bit)	Standalone	136 MB
<a href="#">Default Agent (x86_64_Network)</a>	Linux	x86_64 Architecture (64 bit)	Network (JRE required)	1 MB
<a href="#">Default Agent (x86_64_Complete)</a>	Linux	x86_64 Architecture (64 bit)	Standalone	136.1 MB

1 - 10 of 10 items    show 25 items

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

**Network (.NET required):** The network (.NET required) package installs only the pre-agent on the target device; the pre-agent then downloads and installs the ZENworks Adaptive Agent from the ZENworks Server. The network (.NET required) package requires that Microsoft .NET 3.5 SP1 or later is installed on the device prior to the deployment of the agent to the device.

**Standalone (.NET required):** The standalone (.NET required) package requires that Microsoft .NET 3.5 SP1 or later is installed on the device prior to the deployment of the agent to the device. This package contains all the executables files required for Adaptive Agent installation except the Microsoft .NET installer.

**Standalone:** The standalone package installs the pre-agent and extracts all executable files required for Adaptive Agent installation, including Microsoft .NET installer on the target device. The pre-agent then installs the Adaptive Agent from the local device. The standalone package is useful when you need to install the ZENworks Adaptive Agent to a device that is currently disconnected from the network. You can save the package to removable media (CD, USB flash drive, and so on) and have the standalone device run the package from the media. The Adaptive Agent is installed on the device, but no registration or management occurs until the device connects to the network.

**Custom:** The package name, Default Agent, refers to the predefined deployment packages. The custom deployment packages created through *Deployment > Edit Deployment Package* are shown with the name given during the creation of the package.

- 3 Click the name of the deployment package you want to use, then save the package to the local drive of the device or run it from the ZENworks Server.
- 4 If you downloaded the package, launch the package on the device.

For information about the options you can use with the package, see [Package Options for Windows, Linux, and Macintosh \(page 133\)](#).

**IMPORTANT:** If you choose to install a complete package, the installation of Windows Installer or .NET Framework might require a reboot after you launch the package. If you did not select a reboot option during agent deployment, a message is displayed showing various options on the reboot. Select one of the following options:

- ◆ Do nothing. Auto-reboot will occur after 5 minutes.
- ◆ Click *Cancel*. You will need to reboot later.
- ◆ Click *OK* to reboot immediately.



When the device reboots, the installation automatically resumes.

If you selected the *Manual* and the *Do not prompt for reboot* option during the agent installation, and if .NET or Windows Installer requires a reboot, then you need to manually reboot the device to resume the agent installation.

---

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

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

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

## 10.7 Reboot-less Agent

When ZENworks 11 SP3 Adaptive Agent is installed or an existing managed device is updated to ZENworks 11 SP3, the administrator can select an option not to reboot the device after completing the installation. Additionally, the administrator can select to start the Adaptive Agent services on the managed device. If the services are selected to be started without a reboot, the adaptive agent works with limited functionality until a reboot is performed by user.

**The following does not work without Reboot:**

- ♦ **Agent Fresh Install:** ZENworks Endpoint Security Management (ZESM) and ZENworks Full Disk Encryption (ZFDE) policies including the locations will not be functional until a reboot is performed. Alternatively location lite can be used to detect locations on the managed devices with out reboot.

Dynamic Local User (with and without Novell Client) and Roaming profile policies are not effective on Windows XP devices.

- ♦ **Agent System Update:** New ZESM and FDE Policies and Newly assigned locations does not work, while the previous policies assigned works. After agent is updated it goes to the last known location, which was detected by the agent before the update started. It stays at this location until the device is rebooted.
- ♦ **Start ZENworks Services:** This option starts ZENworks services incase reboot is supressed while deploying the update to the device. It is not applicable for Primary Servers.
- ♦ ZENworks Explorer Configuration Policy (ZECF) with "Name of the root folder" setting will not be effective.

## 10.8 Manually Deploying the Agent on Linux

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

---

**IMPORTANT:** For Red Hat 4 devices, there are prerequisite steps to be followed. For more information, see ["Prerequisites for Agent install on a Red Hat 4 device" on page 107](#).

---

- 1 Make sure the device meets the necessary requirements. For details, see "Managed Device Requirements" in the [ZENworks 11 SP3 System Requirements](#).
- 2 On the target device, open a Web browser and access the following address:  
`http://server:port/zenworks-setup`

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

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

**Network (JRE required):** The network (JRE required) package installs only the pre-agent on the target device; the pre-agent then downloads and installs the ZENworks Adaptive Agent from the ZENworks Server. The network (JRE required) package requires that JRE 1.6 or later is installed on the device prior to the deployment of the agent on the device.

---

**NOTE:** It is required to install only Sun's Java Runtime Environment (JRE) on the Linux managed devices for the ZENworks Adaptive Agent to work.

---

**Standalone:** The standalone package installs the pre-agent and extracts all executable files required for Adaptive Agent installation, including the JRE installer on the target device. The pre-agent then installs the Adaptive Agent from the local device. The standalone package is useful when you need to install the ZENworks Adaptive Agent on a device that is currently disconnected from the network. You can save the package to removable media (CD, USB flash drive, and so on) and have the standalone device run the package from the media. The Adaptive Agent is installed on the device, but no registration or management occurs until the device connects to the network.

**Custom:** The package name, Default Agent, refers to predefined deployment packages. The custom deployment packages created through *Deployment > Edit Deployment Package* are shown with the name assigned during the creation of the package.

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

For information on the options that you can use with the package, see [“Package Options for Windows, Linux, and Macintosh” on page 133](#).

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

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

- 5 In the terminal window, go to the directory where you have downloaded the package, then launch the package on the device by running the command `./filename`, where *filename* is the name of the package you downloaded in [Step 3](#).

---

**NOTE:** A root user has to run the agent installer.

---

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

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

---

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

- ◆ Relogin to the device.
- ◆ Specify the complete path to access the command.

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

---

## 10.9 Manually Deploying the Agent on a Macintosh Device

You can deploy the ZENworks Adaptive Agent to a Macintosh device by downloading the deployment package from the ZENworks download page. Ensure that you have installed Java 1.6 on the Macintosh device.

---

**NOTE:** It is required to install only Apple's Java Runtime Environment (JRE) on the Macintosh devices for the ZENworks Adaptive Agent to work.

---

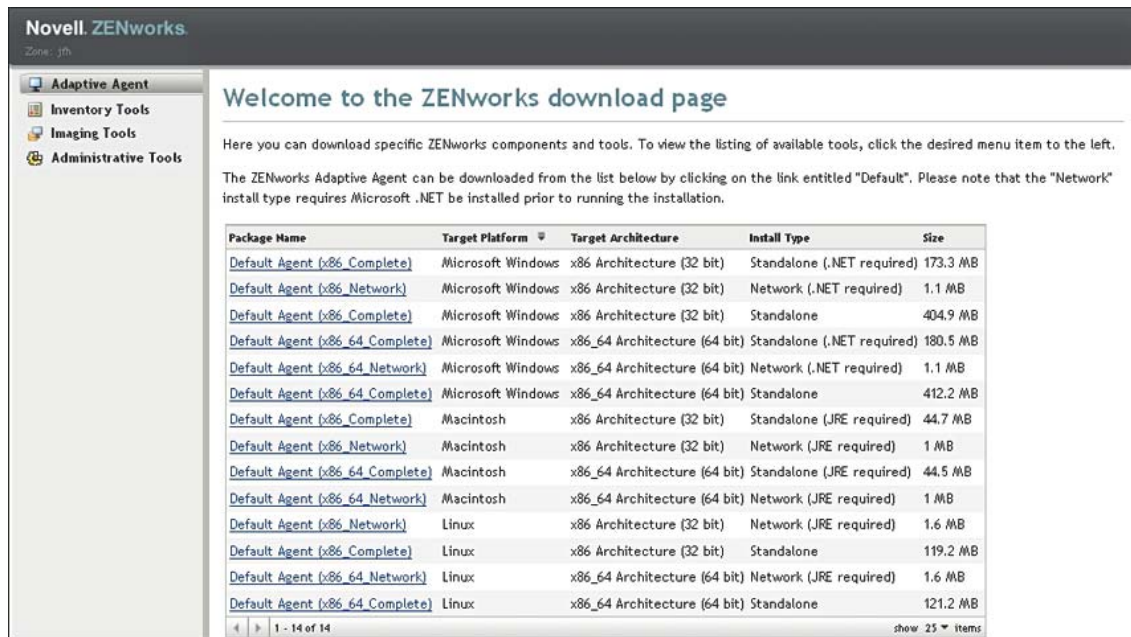
For Macintosh devices that have been upgraded to 10.7, Java 1.6 might not have been installed on the device. You can install Java 1.6 by using Apple Software Update. To know the version of the Java installed on your device, run the following command:

```
java -version
```

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

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

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



The screenshot shows the Novell ZENworks download page. The page title is "Welcome to the ZENworks download page". Below the title, there is a navigation menu on the left with items: Adaptive Agent, Inventory Tools, Imaging Tools, and Administrative Tools. The main content area contains a table of available packages. The table has columns for Package Name, Target Platform, Target Architecture, Install Type, and Size. The table lists 14 packages, including those for Macintosh (x86 and x86\_64) and Linux (x86 and x86\_64). The packages are categorized by architecture and install type (Standalone or Network).

Package Name	Target Platform	Target Architecture	Install Type	Size
<a href="#">Default Agent (x86_Complete)</a>	Microsoft Windows	x86 Architecture (32 bit)	Standalone (.NET required)	173.3 MB
<a href="#">Default Agent (x86_Network)</a>	Microsoft Windows	x86 Architecture (32 bit)	Network (.NET required)	1.1 MB
<a href="#">Default Agent (x86_Complete)</a>	Microsoft Windows	x86 Architecture (32 bit)	Standalone	404.9 MB
<a href="#">Default Agent (x86_64_Complete)</a>	Microsoft Windows	x86_64 Architecture (64 bit)	Standalone (.NET required)	180.5 MB
<a href="#">Default Agent (x86_64_Network)</a>	Microsoft Windows	x86_64 Architecture (64 bit)	Network (.NET required)	1.1 MB
<a href="#">Default Agent (x86_64_Complete)</a>	Microsoft Windows	x86_64 Architecture (64 bit)	Standalone	412.2 MB
<a href="#">Default Agent (x86_Complete)</a>	Macintosh	x86 Architecture (32 bit)	Standalone (JRE required)	44.7 MB
<a href="#">Default Agent (x86_Network)</a>	Macintosh	x86 Architecture (32 bit)	Network (JRE required)	1 MB
<a href="#">Default Agent (x86_64_Complete)</a>	Macintosh	x86_64 Architecture (64 bit)	Standalone (JRE required)	44.5 MB
<a href="#">Default Agent (x86_64_Network)</a>	Macintosh	x86_64 Architecture (64 bit)	Network (JRE required)	1 MB
<a href="#">Default Agent (x86_Network)</a>	Linux	x86 Architecture (32 bit)	Network (JRE required)	1.6 MB
<a href="#">Default Agent (x86_Complete)</a>	Linux	x86 Architecture (32 bit)	Standalone	119.2 MB
<a href="#">Default Agent (x86_64_Network)</a>	Linux	x86_64 Architecture (64 bit)	Network (JRE required)	1.6 MB
<a href="#">Default Agent (x86_64_Complete)</a>	Linux	x86_64 Architecture (64 bit)	Standalone	121.2 MB

- 2 Click the appropriate Macintosh package to download

---

**NOTE:** There are two types of packages for each architecture (32-bit and 64-bit):

- ♦ **Network (JRE required):** This package requires Java 1.6 to be installed on the device prior to the installation of the deployment package. It also requires network access to the ZENworks Server to download the necessary PKG files.
  - ♦ **Standalone (JRE required):** This package requires Java 1.6 to be installed on the device prior to the installation of the deployment package. However, access to the ZENworks Server is not required to install the agent.
-

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

For more information on the options that you can use with the package, see [Section 10.12, “Package Options for Windows, Linux, and Macintosh,”](#) on page 133.

---

**NOTE:** X11 is no longer included as a default install in OS X Mountain Lion 10.8.3 and onwards. Hence before installing OS X Mountain Lion 10.8.3, you need to install the X11 application. For details, see the [support information \(http://support.apple.com/kb/HT5293\)](http://support.apple.com/kb/HT5293).

---

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

```
sudo -i /Users/novell/Downloads/PreAgentPkg_AgentMacComplete.bin
```

The `filename` is the name of the package you downloaded in [Step 2 on page 131](#).

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

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

---

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

- ◆ Login to the device again.
- ◆ Specify the complete path to access the command.

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

---

## 10.10 Agent Deployment in VDI environment

Perform the following steps to prepare Master image:

- 1 Install the Agent manually.

For more information, see [Section 10.6, “Manually Deploying the Agent on Windows,”](#) on page 127.

- 2 Backup the `initial-web-service` file from the `%ZENworks_Home%\conf` location.

- 3 If you want to add a registration key, you can add in the `initial-web-service` file.

The first line of the `initial-web-service` file contains the list of IP addresses and host names of the server to which this device has registered. Add the registration key in the second line.

- 4 Unregister the device by using the `zac unr` command.

- 5 Clear the Workstation GUID by using `zac fsg -d` command.

- 6 Open the command prompt as an administrator, go to `%ZENworks_Home%\bin\preboot` folder, then run the `ZISWIN.exe -w` command to clear Image-safe Data.

- 7 Clear the cache by using the `zac cc` command.

- 8 Copy the backed up `initial-web-service` file to `%ZENworks_Home%\conf` location.

---

**IMPORTANT:** Enable the below Reconcile settings to ensure that the agent registration and reconciliation works in VDI environment:

Serial number + Mac address + Hostname - with Differentiation Enabled.

For more information, see [Section 9.5.2, “Reconciling the Devices,”](#) on page 79.

---

## 10.11 Agent Deployment on Citrix Server

On a Citrix server, after deploying the ZENworks agent, you need to perform certain tasks. For details, see “[Tasks to be Performed after Deploying the Agent on Citrix Servers](#)” in the *ZENworks Configuration Management - Best Practices Guide*.

## 10.12 Package Options for Windows, Linux, and Macintosh

You can use the following options when launching a deployment package from the command line on Windows, Linux, and Macintosh. The syntax is:

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

An example for Windows:

```
PreAgentPkg_Agent.exe -q -v -k regkey1
```

An example for Linux:

```
PreAgentPkg_AgentLinux.bin -S -k regkey1
```

An example for Macintosh:

```
PreAgentPkg_AgentMAC.bin -k regkey1
```

The command accepts the following options:

### On Linux

- G:** Do not install packages which require X or GUI.
- S:** Disable SELinux if the agent is unable to open the ports required by ZENworks.
- k:** The registration key used to register the device in the management zone.

### On Windows

- x:** Do not reboot after installation.
- q:** Suppress the reboot prompt.
- Z:** Log the ZESM installation information.
- U:** Force uninstall of older ZENworks Desktop Management Agent.

### On Linux, Macintosh, and Windows

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

The default target path for Linux and Macintosh is `/opt/novell/zenworks/stage`.

- h: Display help information.
- k: The registration key used to register the device in the management zone.
- 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.
- 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.

## 10.13 Installing the Agent as an Add-on Product in SLES/SLED

You can install the ZENworks Adaptive Agent on SUSE Linux Enterprise Server (SLES) and Desktop (SLED) devices by using YaST. The ZENworks Server hosts a repository, which is used as add-on media by YaST to install the Adaptive Agent at the following URL:

```
http://<server_ip>/zenworks-agent-addon/zenworks-agent-addon-sle10/
```

```
http://<server_ip>/zenworks-agent-addon/zenworks-agent-addon-sle11/
```

Replace *server\_ip* with the DNS name or IP address of a ZENworks Server.

The agent installed is automatically registered with the ZENworks Server that is used as a repository.

---

### NOTE

- ♦ The ZENworks Agent cannot be installed by using the Auto YaST installation process.
- ♦ When a ZENworks 11SP3 server is added as a YaST2 repository in a SLED or SLES machine, you will see a warning message: *Cannot assess installation media. Check whether the server is accessible.*

Ignore the warning and proceed with adding the repository.

---

### 10.13.1 Installing the ZENworks Agent on SLES/SLED 10

To install the agent as an add-on product in SLES/SLED 10, perform the following tasks in the order listed:

1. [Adding the Repository as an Installation Source](#)
2. [Installing the ZENworks Agent](#)

#### Adding the Repository as an Installation Source

To add the repository hosted on the ZENworks Server as the Installation Source:

- 1 Launch YaST Control Center.
- 2 Click the *Software* tab, then click *Installation Source*.
- 3 Click *Add*.
- 4 Select the *Media Type* as *HTTP*, then click *Next*.

- 5 Provide the necessary repository and server details for the selected media, then click *Next*.
- 6 Accept the *License Agreement*, then click *Finish*.

## Installing the ZENworks Agent

You can install the ZENworks Adaptive Agent by using one of the following methods:

### Method 1

- 1 Launch YaST Control Center.
- 2 Click the *Software* tab, then click *Software Management*.
- 3 In the *Filter* drop-down list, select *Patterns*.  
In the Patterns panel under *Add-on*, select *ZENworks Agent All*.
- 4 Click *Accept* to install the ZENworks Agent.

### Method 2

- 1 Launch YaST Control Center.
- 2 Click the *Software* tab, then click *Add-on Products*.
- 3 Select the *Add-on Product* media as *HTTP*.
- 4 Provide the necessary repository and server details for the selected media, then click *OK*.
- 5 Accept *License Agreement*.  
The Agent package is downloaded from the specific repository, and the *Software Selection and System Tasks* window is displayed.
- 6 Select *ZENworks Agent All* under *Add-on*.
- 7 Click *Accept* to install the ZENworks Agent.

## 10.13.2 Installing the ZENworks Agent on SLES/SLED 11

You can install the ZENworks Adaptive Agent on SLES/SLED 11 by using YaST:

- 1 Launch Yast Control Center.
- 2 Click the *Software* tab, then click *Add-on Products*.
- 3 In the Installed Add-on Products window, click *Add*.
- 4 Select the *Media Type* as *HTTP*, then click *Next*.
- 5 Provide the necessary repository and server details for the selected media, then click *Next*.
- 6 Accept the *License Agreement*.  
The Software Management wizard is displayed.
- 7 In the *Filter* drop-down list, select *Patterns*.  
In the Patterns panel under *Add-on*, select *ZENworks Agent All*.
- 8 Click *Accept* to install the ZENworks Agent.

## 10.14 Installing the Agent by Using YUM on RHEL

You can install the ZENworks Adaptive Agent on Red Hat Enterprise Linux (RHEL) devices by using YUM.

---

**IMPORTANT:** Currently installing the agent by using YUM is not supported for Scientific Linux.

---

The ZENworks Server hosts a repository, which is used by YUM to install the Adaptive Agent at the following URL:

```
http://<server_ip>/zenworks-agent-addon/zenworks-agent-yum-repo-rhel4/
```

```
http://<server_ip>/zenworks-agent-addon/zenworks-agent-yum-repo-rhel5/
```

```
http://<server_ip>/zenworks-agent-addon/zenworks-agent-yum-repo-rhel6/
```

The agent installed is automatically registered with the ZENworks Server that is used as a repository.

---

**IMPORTANT:** For Red Hat 4 devices, there are prerequisite steps to be followed. For more information, see [“Prerequisites for Agent install on a Red Hat 4 device” on page 107](#).

---

To install the ZENworks Adaptive Agent on RHEL, perform the following steps:

- 1 Add a new repository file named `zenworks.repo` to the `/etc/yum.repos.d/` directory with the following content:

For a 32-bit device:

```
[zenworks-agent-addon]
name=zenworks-agent-addon
baseurl=http://<server_ip>/zenworks-agent-addon/<repo_url>/
gpgcheck=0
```

For a 64-bit device:

```
[zenworks-agent-addon]
name=zenworks-agent-addon
exclude=*.i386 novell-zenworks-zislnx*.i586 xinetd*.i386 xinetd*.i686 novell-
zenworks-xplat-zennotifyicon*.i586 novell-zenworks-xplat-jsvc*.i586 novell-
zenworks-xplat-imaging-native*.i586 jre*.i586 novell-zenworks-zmg*.i586
baseurl=http://<server_ip>/zenworks-agent-addon/<repo_url>/
gpgcheck=0
```

Replace `server_ip` with the DNS name or IP address of a ZENworks Server and `repo_url` with `zenworks-agent-yum-repo-rhel4` for RHEL 4, `zenworks-agent-yum-repo-rhel5` for RHEL 5 and `zenworks-agent-yum-repo-rhel6` for RHEL 6.

---

**NOTE:** By default, YUM installs 32-bit RPMs on 64-bit devices. If multiple architectures for the same RPM are available in the YUM repository, both the 32-bit and 64-bit RPMs are installed on 64-bit devices. The `exclude` attribute ensures that conflicting 32-bit RPMs are not installed on the 64-bit devices.

---

- 2 Ensure you disable selinux before installing the agent. To install the agent, run the `yum groupinstall zenworks-agent-addon` command.



---

**NOTE:** On RHEL devices, if the Adaptive agent is installed using the `yum groupinstall`, to uninstall it, you need to use the `novell-zenworks-xplat uninstall` located at `/opt/novell/zenworks/bin`. The `yum groupremove` is not supported.

---



---

# 11 Uninstalling the Agent

For information on how to uninstall the ZENworks Adaptive Agent, see:

- ♦ **Windows:** “Uninstalling ZENworks Software from Windows Devices” in the *ZENworks 11 SP3 Uninstall Guide*.
- ♦ **Linux:** “Uninstalling ZENworks Software from Linux Devices” in the *ZENworks 11 SP3 Uninstall Guide*.
- ♦ **Macintosh:** “Uninstalling ZENworks Software from Macintosh Devices” in the *ZENworks 11 SP3 Uninstall Guide*.



# 12 Deploying the Inventory-Only Module

If a Windows device does not meet the requirements for deploying the Adaptive Agent, or if you want to inventory a Windows, Linux, NetWare, or Macintosh OS X device, you can deploy the Inventory-Only module. See “[System Requirements](#)” in the *ZENworks 11 SP3 Server Installation Guide* for information about the platform versions on which the Inventory-Only module is supported.

The following sections provide instructions:

- ◆ [Section 12.1, “Downloading the Module from a ZENworks Server,”](#) on page 141
- ◆ [Section 12.2, “Installing on Linux,”](#) on page 142
- ◆ [Section 12.3, “Installing on NetWare,”](#) on page 143
- ◆ [Section 12.4, “Installing on Windows,”](#) on page 143
- ◆ [Section 12.5, “Installing on Macintosh OS X,”](#) on page 144
- ◆ [Section 12.6, “Uninstalling the Inventory-Only Module,”](#) on page 145
- ◆ [Section 12.7, “Upgrading Inventory-Only Agent,”](#) on page 145
- ◆ [Section 12.8, “Re-registering Inventory-Only Devices,”](#) on page 145
- ◆ [Section 12.9, “Running Scannow on an Inventory-Only Device,”](#) on page 147

## 12.1 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.

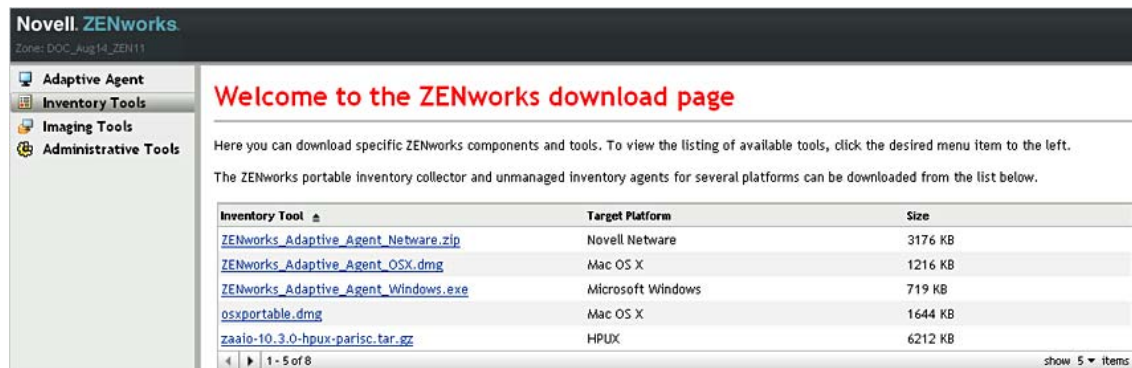
If you are downloading the NetWare module, open the Web browser on a device from which you have file copy access to the NetWare server.

---

**IMPORTANT:** The Inventory-Only module uses the default port (80 or 443) and not the customized port configured on the ZENworks Server.

---

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



Novell. ZENworks  
Code: DOC\_Aug14\_ZEN11

Adaptive Agent  
**Inventory Tools**  
Imaging Tools  
Administrative Tools

### Welcome to the ZENworks download page

Here you can download specific ZENworks components and tools. To view the listing of available tools, click the desired menu item to the left.

The ZENworks portable inventory collector and unmanaged inventory agents for several platforms can be downloaded from the list below.

Inventory Tool	Target Platform	Size
<a href="#">ZENworks_Adaptive_Agent_Netware.zip</a>	Novell Netware	3176 KB
<a href="#">ZENworks_Adaptive_Agent_OSX.dmg</a>	Mac OS X	1216 KB
<a href="#">ZENworks_Adaptive_Agent_Windows.exe</a>	Microsoft Windows	719 KB
<a href="#">osxportable.dmg</a>	Mac OS X	1644 KB
<a href="#">zaio-10.3.0-hpux-parisc.tar.gz</a>	HP/UX	6212 KB

1 - 5 of 8 show 5 items

The Inventory-Only Module for each platform is listed on

Platform	Filename
Novell NetWare	ZENworks_Adaptive_Agent_Netware.zip
Mac OS X	ZENworks_Adaptive_Agent_OSX.dmg
Microsoft Windows	ZENworks_Adaptive_Agent_Windows.exe
Linux	

- 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 12.2, “Installing on Linux,” on page 142](#)
  - ♦ [Section 12.3, “Installing on NetWare,” on page 143](#)
  - ♦ [Section 12.4, “Installing on Windows,” on page 143](#)
  - ♦ [Section 12.5, “Installing on Macintosh OS X,” on page 144](#)

## 12.2 Installing on Linux

- 1 Log in as a user with installation rights on the device.
- 2 Make sure you have downloaded the correct Inventory-Only module package to the target device. If you haven't, see [Section 12.1, “Downloading the Module from a ZENworks Server,” on page 141](#).
- 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 zaaio--linux-x86.tar.gz
```

- 7 Using the Linux package as an example, install the Inventory-Only module by running the `./zenumia-install.sh -s <server>` command, from the directory in which the file is located. Where `server` is the DNS name or IP address of a ZENworks Server.
  - ♦ If the Inventory-Only agent has a non-default port, add the default port number after the DNS name or IP address of a ZENworks Server, by running the `./zenumia-install.sh -s <server> <default port number>` command. Where `server` is the DNS name or IP address of a ZENworks server and the default port number is either 80 or 443.
  - ♦ If the server is installed on a non-default port on a Linux operating system, ensure that the `<server>` tag in the `/opt/novell/zenworks/umia/uiacconfig.xml` file points to port 81, to make sure that the file upload does not run into failure.
  - ♦ If you are installing the Inventory-Only agent on a 64-bit Linux machine where the default 32-bit libraries are not already available, then make sure you first install the following `openssl` and `libopenssl` rpms manually on the agent:
    - ♦ `libssl.so.0.9.(7-9)` or `libssl.so.1.0.0` in the `/usr/lib` or `/lib` path
    - ♦ `libcrypto.so.0.9.(7-9)` or `libcrypto.so.1.0.0` in the `/usr/lib` or `/lib` path

If you are prompted to install `curl` or `expat`, then manually install the following rpms on the agent:

- ♦ `libcurl.so.(2-9)` in the `/usr/lib` path
- ♦ `libexpat.so.0` in the `/usr/lib` path
- ♦ If you are installing the Inventory-Only agent on a 64-bit Linux machine (such as RHEL 6.3) which does not have the default gcc 32-bit library in the `/lib` path, you need to install the `libgcc_s.so.1` library manually on the agent.

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.

---

**NOTE:** Inventory-Only agents fail to install on RHEL 6.x devices because of an OpenSSL dependency. Ensure that you first install OpenSSL before installing the Inventory-Only agent on RHEL 6.x devices.

---

## 12.3 Installing on NetWare

- 1 Make sure you have downloaded `ZENworks_Adaptive_Agent_Netware.zip` to a device that has access to the target NetWare server. If you haven't, see [Section 12.1, "Downloading the Module from a ZENworks Server,"](#) on page 141.
- 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 1.1.1.1
```

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 > *Servers* folder).

## 12.4 Installing on Windows

- 1 Make sure you've downloaded `ZENworks_Adaptive_Agent_Windows.exe` to the target Windows device. If you haven't, see [Section 12.1, "Downloading the Module from a ZENworks Server,"](#) on page 141.
- 2 Make sure the location of `msiexec.exe` on the target machine is in the path variable of the target machine.
- 3 At a command prompt, run `ZENworks_Adaptive_Agent_Windows.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).

## 12.5 Installing on Macintosh OS X

- 1 Make sure you have downloaded the `ZENworks_Adaptive_Agent_OSX.dmg` disk image to the target Macintosh device.

For more information on how to download the `ZENworks_Adaptive_Agent_OSX.dmg` disk image, see [Section 12.1, “Downloading the Module from a ZENworks Server,”](#) on page 141.

- 2 Double-click the `ZENworks_Adaptive_Agent_OSX.dmg` file.
- 3 If you are using prior versions of Macintosh OS X 10.8 then double-click the `ZENworks_Adaptive_Agent_OSX` file to launch the installation package.

If you are using Macintosh OS X 10.8 then perform the following steps:

- ♦ Right-click `ZENworks_Adaptive_Agent_OSX` file and click *Open*.
  - ♦ A message appears as “ZENworks\_Adaptive\_Agent\_OSX” is from an unidentified developer. Are you sure you want to open it? then click *Open*.
- 4 If a message appears telling that a program needs to run to determine whether the package can be installed, click *Continue* to reach the Select Destination page.
  - 5 Select a destination volume, then click *Continue* to display the Installation Type page.
  - 6 Click *Install*.
  - 7 When you are prompted to authenticate, enter a username and a password for the target device, then click *OK*.

The installation begins. The `servername.txt` file opens in the text edit window, and you are prompted to enter the name of a ZENworks Server.

---

**NOTE:** If the `servername.txt` file does not open, continue with [Step 10 on page 144](#) and follow the instructions provided [Editing the Inventory Configuration File and Refreshing the zenumia Process](#).

---

- 8 In the text edit window, enter the IP address or DNS name of the ZENworks Server you want the device to communicate with.
- 9 Save the file and close the window.  
The client files are installed.
- 10 When the installation is complete, click *Close*.  
The Inventory-Only module is started, and the device is added to the Invenoried Devices page in ZENworks Control Center (*Devices* tab > *Invenoried* tab > *Workstations* folder).

### 12.5.1 Editing the Inventory Configuration File and Refreshing the zenumia Process

- 1 Locate `uiaconfig.xml` from the path `/usr/local/novell/zenworks/umia/` in the inventory config file.
- 2 Stop the zenumia service by using the `systemstarter stop zenumia` command.
- 3 Replace `col.lec.ser.ver` with the Primary Server IP address in the following line:  
`server>col.lec.ser.ver</server>`, for example, `<server>192.160.28.34</server>`
- 4 Save and close the inventory config file.
- 5 Restart the zenumia service by using the `systemstarter start zenumia` command.



## 12.6 Uninstalling the Inventory-Only Module

To uninstall the Inventory-Only module for the supported platforms, use the following instructions:

### Linux

- 1 Go to the `/opt/novell/zenworks/umia` directory.
- 2 Execute the `./zenumia-uninstall.sh` uninstall command.

### NetWare

- 1 Log in to ZENworks Control Center.
- 2 Click *Devices > Inventoried*.
- 3 Select either *Servers* or *Workstations* as the type of device.
- 4 Select the Inventory-Only device to uninstall, then click *Delete*.

### Windows

- 1 From the Windows Start menu, select *Settings > Control Panel > Add or Remove Programs*.
- 2 Select ZENworks Adaptive Agent, then click *Remove*.

### Macintosh OS X

- 1 Go to the `cd /usr/local/novell/zenworks/umia/` directory.
- 2 Execute the `./zenumia-remove.sh` uninstall command.

---

**NOTE:** To uninstall the Inventory-Only module by using ZENworks Control Center, go to ZENworks Control Center and manually delete the object.

---

## 12.7 Upgrading Inventory-Only Agent

To upgrade to a newer version of the Agent on an Inventory-Only Device:

- 1 Uninstall the existing Inventory-Only agent. For more information, see [Section 12.6, “Uninstalling the Inventory-Only Module,” on page 145](#).
- 2 Install the new Inventory-Only agent. For more information, see [Section 12.1, “Downloading the Module from a ZENworks Server,” on page 141](#).

## 12.8 Re-registering Inventory-Only Devices

There are two options you can use for re-registering Inventory-Only devices.

- ♦ [Section 12.8.1, “Re-registering Inventory-Only Devices for All Platforms,” on page 146](#)
- ♦ [Section 12.8.2, “Re-registering Inventory-Only Devices for Individual Platforms,” on page 146](#)

## 12.8.1 Re-registering Inventory-Only Devices for All Platforms

This procedure is common to re-register the Inventory-Only devices for all the supported platforms.

- 1 Uninstall the existing agent from the device by following the instructions provided for the selected platform in [Section 12.6, “Uninstalling the Inventory-Only Module,” on page 145.](#)
- 2 Download the executable agent from the latest module on the ZENworks Server.  
For more information, see [Section 12.1, “Downloading the Module from a ZENworks Server,” on page 141.](#)

## 12.8.2 Re-registering Inventory-Only Devices for Individual Platforms

This procedure can be used for re-registering Inventory-Only devices for the specified platforms.

### Linux

- 1 Go to the `/opt/novell/zenworks/umia` directory.
- 2 Stop the service by using the `"/etc/init.d/zenumia stop"` command.
- 3 Edit the `uiaconfig.xml` file.
- 4 Replace the existing Server IP address with the new ZENworks Server IP address.
- 5 Save and close the inventory config file.
- 6 Restart the service by using the `"/etc/init.d/zenumia start"` command.

### Netware

- 1 Go to the `sys:\ZENworks\zaa` directory.
- 2 To stop the service, unload the `zenaa` module by using the `unload zenaa` command.
- 3 Edit the `uiaconfig.xml` file.
- 4 Replace the existing Server IP address with the new ZENworks Server IP address.
- 5 Save and close the inventory config file.
- 6 To restart the service, load the `zenaa` module by using the `load zenaa` command.

### Windows

- 1 Go to the `C:\Program Files\Novell\ZENworks\bin` directory.
- 2 In the service manager, stop the Novell ZENworks Adaptive Agent Service.
- 3 Edit the `uiaconfig.xml` file.
- 4 Replace the existing Server IP address with the new ZENworks Server IP address.
- 5 Save and close the inventory config file.
- 6 (Conditional) If necessary modify the register key `HKLM\Software\Novell\ZCM` to change the default values for server, port, and secure port.  
By default, the server is the DNS name or IP address of the ZENworks Server and the default numbers for the port and secure port are 80 and 443.
- 7 To restart the service in the service manager, start Novell ZENworks Adaptive Agent Service.

## Macintosh OS X

- 1 Go to the `cd /usr/local/novell/zenworks/umia/` directory.
- 2 Stop the zenumia service by using the `systemstarter stop zenumia` command.
- 3 Edit the `uiaconfig.xml` file.
- 4 Replace the existing Server IP address with the new ZENworks Server IP address.
- 5 Save and close the inventory config file.
- 6 Restart the zenumia service by using the `systemstarter start zenumia` command.

## 12.9 Running Scannow on an Inventory-Only Device

To run a scan on an Inventory-Only device, follow the steps provided for the supported platforms:

### Linux

- 1 At the command prompt, execute the `"/etc/init.d/zenumia stop"` command.
- 2 Go to the umia directory by using the `cd "/opt/novell/zenworks/umia"` command.
- 3 Enter the `./zenumia scannow &` command.

### NetWare

- 1 To stop the service, unload the zena module by using the `unload zena` command.
- 2 In the system console, go to the `sys:\ZENworks\zaa\bin` directory.
- 3 Execute the `zennwscan.nlm` module.

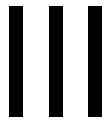
### Windows

- 1 In the service manager, stop the Novell ZENworks Adaptive Agent Service.
- 2 At the command prompt, go to the `cd "C:\Program Files\Novell\ZENworks\bin"` bin directory.
- 3 Enter the `zenumia scannow` command.

### Macintosh OS X

- 1 At the command prompt, execute the `systemstarter stop zenumia` command.
- 2 Go to the umia directory by using the `cd "/usr/local/novell/zenworks/umia"` command.
- 3 Enter the `./zenumia scannow` command.





# Device Removal and Retirement

The following sections provide information and instructions to help you delete or retire devices from your ZENworks system.

If you delete a server or workstation device, the selected device is removed from your ZENworks system.

Retiring a device is different from deleting a device. When you retire a device, its GUID is retained (as opposed to when you delete a device, which also deletes its GUID). As a result of retiring a device, all inventory information is retained and is assessable but all policy and bundle assignments are removed. A retired device is in a holding state until you unretire or delete the device. If you unretire the device in the future, its assignments are restored. You can retire both managed and inventoried devices.

- ♦ [Chapter 13, “Deleting Devices from Your ZENworks System,” on page 151](#)
- ♦ [Chapter 14, “Retiring or Unretiring Devices,” on page 153](#)



---

# 13 Deleting Devices from Your ZENworks System

If you delete a server or workstation device, the selected device is removed from your ZENworks system, its GUID is deleted, all inventory information is removed, and all policy and bundle assignments are removed.

- 1 In ZENworks Control Center, click the *Devices* tab.
- 2 Click the underlined link next to the *Servers* or *Workstations* folder to display the list of servers or workstations in your ZENworks system.
- 3 Select the check box in front of the server or workstation (you can select multiple devices).
- 4 Click *Delete*.

---

**NOTE:** In ZENworks Control Center, if you delete Windows devices, the devices are automatically registered again after the next refresh. For Linux devices, you need to manually register the device if it is deleted.

---

You cannot delete a ZENworks Primary Server from the *Devices* tab. If you select a Primary Server in [Step 3](#) and click *Delete*, then the following error message displays:

Error: The object "vm232w2k3ent" is a Primary Server and cannot be deleted. To delete a Primary Server, go to Configuration, Server Hierarchy, (select a Primary Server), Action, Delete ZENworks Server.

For more information about deleting a ZENworks Primary Server, see "[Deleting a ZENworks Primary Server](#)" in the *ZENworks 11 SP3 Primary Server and Satellite Reference*.





# 14 Retiring or Unretiring Devices

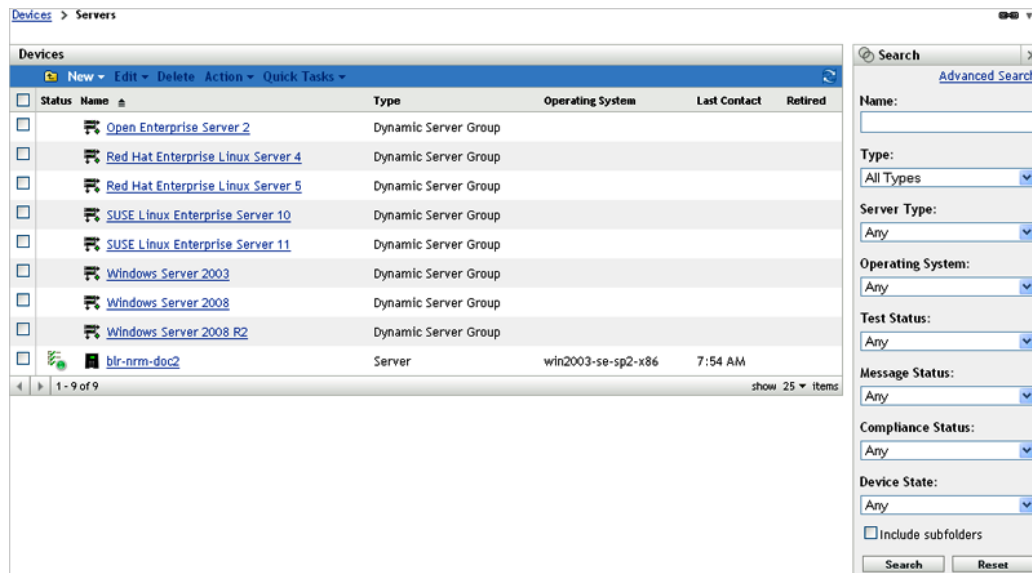
If you retire a server or workstation device, the selected device is retired from your ZENworks Zone. Retiring a device is different from deleting a device. When you retire a device, its GUID is retained (as opposed to when you delete a device, which also deletes its GUID). As a result of retiring a device, all inventory information is retained and is assessable but all policy and bundle assignments are removed. A retired device is in a holding state until you unretire or delete the device. If you unretire the device in the future, its assignments are restored. You can retire both managed and inventoried devices.

To retire or unretire a device, you must have Device Modify rights. For more information, see “[Device Rights](#)” in the *ZENworks 11 SP3 Administrator Accounts and Rights Reference*.

To retire or unretire a managed device:

- 1 In ZENworks Control Center, click the *Devices* tab.
- 2 Click the underlined link next to the *Servers* or *Workstations* folder to display the list of servers or workstations in your ZENworks system.

Figure 14-1 *Devices panel showing list of servers.*




- 3 Select the check box in front of the server or workstation (you can select multiple devices).

Before you can retire a ZENworks Primary Server, you must first demote it. For more information, see “[Changing the Parent-Child Relationships of Primary Servers](#)” in the *ZENworks 11 SP3 Primary Server and Satellite Reference*.

- 4 Click *Action* > *Retire Device* to retire the device upon its next refresh.

or

Click *Action* > *Unretire* to unretire the device upon its next refresh.

The  icon displays in the *Status* column in the *Servers* or *Workstations* list for retired devices. You can mouse over the time to see the full date and time.

---

**NOTE:** To retire a device immediately, select the check box in front of the servers or workstations, then click *Quick Tasks > Retire Device Now*.

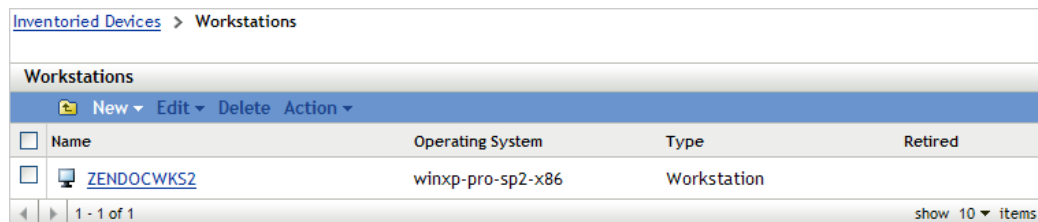
To unretire a device immediately, select the check box in front of the servers or workstations, then click *Quick Tasks > Unretire Device Now*.

---

To retire or unretire an inventoried device:


- 1 In ZENworks Control Center, click *Devices > Inventoried*.
- 2 Click the underlined link next to the *Servers* or *Workstations* folder to display the list of servers or workstations in your ZENworks system.

**Figure 14-2** *Devices panel showing list of inventoried devices.*



Inventoried Devices > Workstations			
Workstations			
New Edit Delete Action			
<input type="checkbox"/>	Name	Operating System	Type Retired
<input type="checkbox"/>	<a href="#">ZENDOCWKS2</a>	winxp-pro-sp2-x86	Workstation

- 3 Select the check box in front of the server or workstation you want to retire or unretire (you can select multiple devices).
- 4 Click *Action > Retire Device*.  
or  
Click *Action > Unretire Device*.

The  icon displays in the *Status* column in the *Servers* or *Workstations* list for retired devices. You can mouse over the time to see the full date and time.

After a device has been retired the inventory management status shows as *Disabled*. You can continue to view the inventory reports of the last inventory scan or search for all retired devices in your ZENworks system.

To search for retired servers and workstations:

- 1 In ZENworks Control Center, click the *Devices* tab.
- 2 (Conditional) To search for both retired servers and workstations, skip to [Step 3](#).  
or  
To search for only retired servers, click the underlined link next to the *Servers* folder to display the list of servers.  
or  
To search for only retired workstations, click the underlined link next to the *Workstations* folder to display the list of workstations.
- 3 In the Search box, select *Retired* from the *Device State* drop-down list.

Figure 14-3 Search box with Retired selected.

The image shows a search interface with the following fields:

- Name:** An empty text input field.
- Type:** A dropdown menu with "All Types" selected.
- Server Type:** A dropdown menu with "Any" selected.
- Operating System:** A dropdown menu with "Any" selected.
- Message Status:** A dropdown menu with "Any" selected.
- Compliance Status:** A dropdown menu with "Any" selected.
- Device State:** A dropdown menu with a list of options: "Any", "Lost", "Normal", and "Retired". The "Retired" option is highlighted in blue, indicating it is selected.

4 Click *Search*.



---

# IV Appendixes

- ◆ [Appendix A, “Viewing the Predefined Reports,” on page 159](#)
- ◆ [Appendix B, “Schedules,” on page 161](#)
- ◆ [Appendix C, “Configuring NMAP for ZENworks,” on page 165](#)
- ◆ [Appendix D, “Troubleshooting Discovery, Deployment, and Retirement,” on page 167](#)
- ◆ [Appendix E, “Documentation Updates,” on page 175](#)



---

# A Viewing the Predefined Reports

The ZENworks Reporting is a powerful, flexible, and customizable reporting tool that is installed and configured separately from the ZENworks system. For information on how to install ZENworks Reporting, see the [ZENworks Reporting 5 Installation Guide](#).

To view the predefined reports for discovered devices and ZENworks Systems:

- 1 Log in to ZENworks Reporting.
- 2 Navigate to the *View > Repository > Folders > Organization > Reports > ZENworks > Predefined Reports* folder.
- 3 Click *Discovered Devices*.

The following predefined reports are included for discover devices:

- ♦ **CISCO Routers:** Displays information on the discovered Cisco routers in the zone.
- ♦ **Deployable Devices:** Displays all the discovered devices that have been identified as types to which you can deploy the ZENworks Adaptive Agent.
- ♦ **Managed Devices by ZENworks Management Zone:** Displays all the discovered devices that have the ZENworks Adaptive Agent installed on them. It also displays the ZENworks Management Zone information of all the discovered devices.
- ♦ **Printed Page Count by Printer:** Displays the discovered printers and the number of pages printed by each printer.
- ♦ **Printer Alerts:** Displays printer alerts and the alerting units of the discovered printers.
- ♦ **Printer Supply Levels:** Displays the supply levels for units, including toner, waste toner, and fuser of the discovered printers.
- ♦ **Unmanaged Servers:** Displays all the discovered devices that have been identified as servers to which you can deploy the ZENworks Adaptive Agent.
- ♦ **Unmanaged Workstations:** Displays all the discovered devices that have been identified as workstations to which you can deploy the ZENworks Adaptive Agent.
- ♦ **Managed Device Listing:** Displays the discovered, inventoried, and managed devices in the Management Zone. This report is included in the *ZENworks System* folder (*Novell ZENworks Reports > Predefined Reports* folder).
- ♦ **Non-Compliant Devices:** Displays the number of non-compliant devices that are present in a zone. This report is included in the *ZENworks System* folder (*Novell ZENworks Reports > Predefined Reports* folder).

For more information about ZENworks Reporting, see the [ZENworks Reporting 5 System Reference](#) documentation.





---

# B Schedules

The following schedules are available for discovery and deployment tasks:

- ♦ [Section B.1, “Now,” on page 161](#)
- ♦ [Section B.2, “No Schedule,” on page 161](#)
- ♦ [Section B.3, “Date Specific,” on page 161](#)
- ♦ [Section B.4, “Recurring,” on page 162](#)

## B.1 Now

Runs the task immediately after completing the task wizard.


## B.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.

## B.3 Date Specific

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

### B.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.

### B.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.

### B.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.

## B.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.

## B.4 Recurring

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

### B.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.

### B.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.

### B.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.



---

# C Configuring NMAP for ZENworks

The following sections let you know how to configure NMAP for ZENworks:

- ♦ [“Configuring NMAP for ZENworks on Linux” on page 165](#)
- ♦ [“Configuring NMAP for ZENworks on Windows” on page 165](#)

## Configuring NMAP for ZENworks on Linux

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. Consequently, the NMAP discovery fails when it runs with the `zenworks` username. You should not run ZENloader with the `root` username. To resolve this issue, the `zenworks` user must be enabled to run NMAP for discovery with `root` privilege by configuring NMAP for ZENworks.

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

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

---

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

---

- 3 Comment the following lines by typing `#` at the beginning of the 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 Save your changes and exit the editor.

## Configuring NMAP for ZENworks on Windows

On a Windows Primary Server, the NMAP (`nmap.exe`) is installed in the `%ProgramFiles%\nmap` directory and added to the PATH variable of the user who installs it. While installing NMAP, PATH variable is added only to the user variable. You have to manually add it to system environment variable.

You must append the location of the NMAP installation directory (`%ProgramFiles%\nmap`) to the system environment variable PATH of Windows. You have to manually restart the Novell ZENworks Loader service in order to discover the devices.



---

# D Troubleshooting Discovery, Deployment, and Retirement

The following sections provide solutions to the problems you might encounter while discovering devices, deploying the Adaptive Agent to devices, and retiring devices:

- ♦ “An error occurs while installing the ZENworks Adaptive Agent through a deployment task” on page 167
- ♦ “Manual installation of the ZENworks Adaptive Agent hangs with the status as starting” on page 168
- ♦ “NMAP discovery does not run from a Windows Primary Server that has NMAP installed” on page 169
- ♦ “How do I enable debug logging?” on page 169
- ♦ “Where do I find the PreAgent log files?” on page 169
- ♦ “Refreshing the Deployment page causes the discovery tasks to be repeated” on page 169
- ♦ “Orphaned and deleted files are not cleaned up from a deployment task that uses a proxy” on page 169
- ♦ “Discovery task remains in a pending state if it has a large IP address range” on page 170
- ♦ “The device that has the ZENworks Adaptive Agent installed is not registered in the Management Zone” on page 170
- ♦ “Unable to remove or uninstall a registered Macintosh device from the Management Zone” on page 171
- ♦ “ZENworks Adaptive Agent installation fails because of a ZENPreAgent and ZPA\_lfacetype initialization exception” on page 171
- ♦ “After installing the ZENworks Adaptive Agent, you cannot find the /opt directory in the Mac OS X Finder” on page 172
- ♦ “ZENworks Adaptive Agent installation fails on a Mac OS X Lion (version 10.7) device or later” on page 172
- ♦ “Push deployment fails on a WinXP device with a generic error message” on page 172
- ♦ “Agent Installation is incomplete” on page 172
- ♦ “ZENworks Agent does not work if Macintosh device is upgraded from 10.8 to 10.9” on page 173
- ♦ “ZENworks Agent installation fails when the Windows Imaging Component is not installed on the device” on page 173
- ♦ “Duplicate Device Objects are created when Device Authentication fails during Reconciliation” on page 173
- ♦ “When a Mac patch policy bundle fails, the xauth messages that are launched are not terminated” on page 173

## **An error occurs while installing the ZENworks Adaptive Agent through a deployment task**

Source: ZENworks 11; Discovery, Deployment, and Retirement.

**Explanation:** If the ZENworks Adaptive Agent is installed through a deployment task on a managed device that has .NET Framework 3.5 SP1 installed, you might encounter the following error message:


```
An unhandled exception (System.Security.SecurityException)
occurred in
micasad.exe.
Additional Information: Ecall methods must be packaged into a
system module.
```

**Action:** On the managed device, uninstall .NET Framework 3.5 SP1 and reinstall it. For more information on how to uninstall .NET Framework 3.5 SP1 and reinstall it, see the [Microsoft .NET Framework 2.0 Solution Center Web site \(http://support.microsoft.com/ph/8291\)](http://support.microsoft.com/ph/8291).

## Manual installation of the ZENworks Adaptive Agent hangs with the status as starting

**Source:** ZENworks 11; Discovery, Deployment, and Retirement.

**Explanation:** The manual installation of ZENworks Adaptive Agent abruptly stops on the managed device after the MSI packages are downloaded. Following are the symptoms:

- ◆ The  icon displays the installation status as “Starting...” for a considerable amount of time.
- ◆ The status of Novell ZENworks PreAgent service is not *Started* in the Windows Service Control Manager.
- ◆ The `%SystemRoot%\novell\zenworks\bin\zenpreagent.installerr` file contains the following error message:

```
Exception during start: Cannot start service ZENPreAgent on
computer.
```

**Possible Cause:** The Novell ZENworks PreAgent service was terminated by the Windows Service Manager because it failed to respond to the start request in a timely fashion. This issue is likely to occur if the device is slow and heavily loaded.

**Action:** Do the following:

- 1 Start the Novell ZENworks PreAgent service:
  - 1a From the Windows desktop Start menu, click *Settings > Control Panel*.
  - 1b Double-click *Administrative Tools > Services*.
  - 1c Start the Novell ZENworks PreAgent service.  
This automatically resumes the ZENworks Adaptive Agent installation.
- 2 (Conditional) If the problem persists, do the following:
  - 2a Kill the `zenpreagent.exe` and `zpa_iface.exe` processes.
  - 2b Start the ZENworks Adaptive Agent installation. For more information, see [Section 10.6, “Manually Deploying the Agent on Windows,” on page 127](#).



## NMAP discovery does not run from a Windows Primary Server that has NMAP installed

Source: ZENworks 11; Discovery, Deployment, and Retirement.

Possible Cause: On a Windows Primary Server, the NMAP (`nmap.exe`) is installed in the `%ProgramFiles%\nmap` directory and added to the PATH variable of the user who installs it. Consequently, the ZENworks user is unable to locate `nmap.exe` by using the PATH variable.

Action: Append the location of the NMAP installation directory (`%ProgramFiles%\nmap`) to the system environment variable PATH of Windows.

## How do I enable debug logging?

Source: ZENworks 11; Discovery, Deployment, and Retirement.

Action: To enable the logs, see TID 3418069 in the [Novell Support Knowledgebase](http://support.novell.com/search/kb_index.jsp) ([http://support.novell.com/search/kb\\_index.jsp](http://support.novell.com/search/kb_index.jsp)).

## Where do I find the PreAgent log files?

Source: ZENworks 11; Discovery, Deployment, and Retirement.

Action: Following are the PreAgent log files located in `%SystemRoot%\novell\zenworks\bin\`

`zenpreagent.installerr`

`zenpreagent.installlog`

`zenpreagent.installstate`

`ZPA.status`

`cmdline.txt` (The command line executed when the managed agent package was launched.)

After the PreAgent service is installed, all logging information is available in the system application event log.

## Refreshing the Deployment page causes the discovery tasks to be repeated

Source: ZENworks 11; Discovery, Deployment, and Retirement.

Possible Cause: It is normal for a Web browser to resend information in order to refresh a page. ZENworks auto-updates the data on a Deployment page every 5 seconds, so you should not need to refresh the Deployment page after running a discovery task. If you refresh the Deployment page in ZENworks Control Center after running a discovery task, you are asked to confirm the resend in order to refresh the page. If you do so, the discovery task runs again.

Action: Do not refresh the Deployment page after running a discovery task. Instead, exit the page and return to see any changes.

## Orphaned and deleted files are not cleaned up from a deployment task that uses a proxy

Source: ZENworks 11; Discovery, Deployment, and Retirement.

**Explanation:** Orphaned or to-be-deleted files from a pre-task or post-task action during a deployment task that uses a proxy are not cleaned up.

For example, if you run the deployment task from a Linux server through a Windows Proxy, there is a folder created in the `zenworks_installation_directory\novell\zenworks\bin\_rfu_cache` directory on the Windows device that contains the pre-task or post-task command file. If you delete the task in ZENworks Control Center, the command file is left on the Windows Proxy device. However, all command files older than five days are removed when another deployment task is run by using the same Windows Proxy.

**Action:** To immediately delete the orphaned files from the `zenworks_installation_directory\novell\zenworks\bin\_rfu_cache` directory, you must manually delete it.

## Discovery task remains in a pending state if it has a large IP address range

**Source:** ZENworks 11; Discovery, Deployment, and Retirement.

**Explanation:** If a discovery task has an IP address range with more than 50,000 devices, the task is not started. The status of the task remains as *Pending*. If any other discovery or loader task is running simultaneously, it might take a considerable time to complete.

**Possible Cause:** The ZENworks Loader has insufficient memory to run a task that has a large IP address range.

**Action:** Do the following:

- 1 Stop the discovery task that has a large IP address range:
  - 1a In the Discovery Tasks panel, select the discovery task that has a large IP address range.
  - 1b Click *Action > Abort Discovery Task*.
- 2 Create multiple tasks with the IP address ranges that have fewer than 50,000 devices.
- 3 (Conditional) If any other discovery or loader task takes a considerable time to complete, restart the ZENworks Loader.
  - ◆ **On Windows:** Do the following:
    1. From the Windows desktop *Start* menu, click *Settings > Control Panel*.
    2. Double-click *Administrative Tools > Services*.
    3. Restart the *Novell ZENworks Loader Service*.
  - ◆ **On Linux:** At the console prompt, enter `/etc/init.d/novell-zenloader restart`.
- 4 Restart the ZENworks Loader.

## The device that has the ZENworks Adaptive Agent installed is not registered in the Management Zone

**Source:** ZENworks 11; Registration.

Possible Cause: The device has more than one DNS suffix configured.

Action: Do the following on the device that is not registered in the Management Zone:

- 1 Reconfigure the device with only one DNS suffix.
- 2 Manually register the device to the Management Zone.

For more information on how to manually register the device, see [Section 9.7, “Manually Registering a Device,” on page 90](#).

## Unable to remove or uninstall a registered Macintosh device from the Management Zone

Source: ZENworks 11; Discovery, Deployment, and Retirement.

Explanation: Uninstalling or removing a previously registered Macintosh agent from the Management Zone gives the following errors:

```
Permission denied.
```

or

```
Not enough privileges to perform the operation.
```

Action: A user needs to have root privileges before running the uninstall script.

- 1 Log in as `root` or use the `sudo -i` command.
- 2 Run the uninstall script.

## ZENworks Adaptive Agent installation fails because of a ZENPreAgent and ZPA\_Iface type initialization exception

Source: ZENworks 11; Discovery, Deployment, and Retirement

Explanation: When you download and install the pre-agent package, installation fails because of a `ZENPreAgent` and `ZPA_Iface` type initialization exception.

You might get the following error message in the ZENPreAgent.exe-Common Language Runtime Debugging Services window:

```
Application has generated an exception that could not be handled
```

You might get the following error message in the Visual Studio Just-In-Time Debugger window:

```
An unhandled  
exception(System.TypeInitializationException)occurred in  
ZPA_Iface.exe
```

Possible Cause: A corrupted .NET framework.

Action: To successfully install the pre- agent on the device:

- 1 Use the .NET clean up utility to uninstall the .NET framework.
- 2 Re-install the .NET framework.

## After installing the ZENworks Adaptive Agent, you cannot find the /opt directory in the Mac OS X Finder

Source: ZENworks 11; Discovery, Deployment, and Retirement

Explanation: After installing the ZENworks Adaptive Agent on a Mac OS X Lion device, you cannot find the `/opt` directory in the Mac OS X Finder.

Action: To make the `/opt` directory visible in the Mac OS X Finder, run the following command:

```
/usr/bin/chflags nohidden /opt
```

## ZENworks Adaptive Agent installation fails on a Mac OS X Lion (version 10.7) device or later

Source: ZENworks 11; Discovery, Deployment, and Retirement

Explanation: If you install the ZENworks Adaptive Agent on a Mac OS X Lion (version 10.7) device or later, the installation fails.

Possible Cause: Java 1.6 might not have been installed on the machine.

Action: To install Java 1.6, run the following command:

```
java -version
```

## Push deployment fails on a WinXP device with a generic error message

Source: ZENworks 11; Discovery, Deployment, and Retirement

Explanation: The push deployment fails on a WinXP device, with the following error message:

```
Error: Credentials invalid. Please ensure that Classic file sharing is enabled on the target device
```

Possible Cause: The failure could be because of one of the following:

- ◆ You might have entered wrong credentials and have not enabled the classic file sharing option on the target device.
- ◆ A Microsoft issue. For more information, see the CAUSE section in (<http://support.microsoft.com/?id=281308>).

Action: Do the following:

- ◆ Enter correct credentials and ensure that you have enabled classic file sharing on the target device.
- ◆ If the generic error message is displayed even after the above conditions are met, you need to add a registry key. For more information, see (<http://support.microsoft.com/?id=281308>).

## Agent Installation is incomplete

Source: ZENworks 11; Discovery, Deployment, and Retirement.

Explanation: Agent installation fails to complete when you have selected the *Manual* and the *Do not prompt for reboot* option.

Possible Cause: .NET or Windows Installer requires a reboot.

Action: Reboot the device to resume the agent installation.

## **ZENworks Agent does not work if Macintosh device is upgraded from 10.8 to 10.9**

Source: ZENworks 11; Discovery, Deployment, and Retirement.

Explanation: If ZENworks Agent is installed on Macintosh 10.8 device and Macintosh device is upgraded from 10.8 to 10.9, then ZENworks Agent does not work. Since, Apple's jdk 1.6 have been removed after upgrade.

Action: On Macintosh 10.9 device install Apple's jdk 1.6 and log in again.

## **ZENworks Agent installation fails when the Windows Imaging Component is not installed on the device**

Source: ZENworks 11; Discovery, Deployment, and Retirement

Explanation: ZENworks agent installation fails with the following error message:

Windows Imaging Component, a prerequisite for .NET 4.0 should be installed manually before the ZENworks Agent installation.

Possible Cause: The Windows Imaging Component which is a prerequisite for .NET 4.0 is not installed on the device.

Action: Install Windows Imaging Component on your device manually and restart the ZENworks agent installation.

## **Duplicate Device Objects are created when Device Authentication fails during Reconciliation**

Source: ZENworks 11; Discovery, Deployment, and Retirement

Explanation: During device registration if a device is not reconciled due to device authentication failure, duplicate device objects are created for the device in the management zone.

Action: Prevent creation of duplicate device objects for the managed device:

- ♦ Ensure that the network adapters of the managed device are connected and have a valid IP address.
- ♦ Execute the following zac command on the managed device:  

```
zac reregister <GUID of original device object>
```

## **When a Mac patch policy bundle fails, the xauth messages that are launched are not terminated**

Source: ZENworks 11; Discovery, Deployment, and Retirement

Explanation: If you launch a Mac patch policy bundle several times, the policy fails each time with a pop-up message to install xauth. These xauth messages are not terminated even after the bundle error messages disappear. This is because X11 is no longer included as a default install, starting with OS X Mountain Lion 10.8.3.

Action: Before upgrading a ZENworks agent to an OS X Mountain Lion 10.8.3 (or later) device, or before installing ZENworks agent on an OS X Mountain Lion 10.8.3 (or later) device, you need to install the X11 application.

---

# E Documentation Updates

This section summarizes the significant changes made to the *Discovery, Deployment, and Retirement Reference* since the initial release of ZENworks 11 SP3.

