



ZENworks®

Patch Management

User Guide

ZENworks Patch Management Server v6.4

Novell®

02_012N_6.4.2.19

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
Phone: 800.858.4000
www.novell.com

Copyright © 1997-2007 PatchLink® Corporation. ALL RIGHTS RESERVED. U.S. Patent No. 6,990,660, Other Patents Pending. This manual, as well as the software described in it, is furnished under license. No part of this manual may be reproduced, stored in a retrieval system, or transmitted in any form—electronic, mechanical, recording, or otherwise—except as permitted by such license.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: PATCHLINK® CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES IN REGARDS TO THE ACCURACY OR COMPLETENESS OF THE INFORMATION PROVIDED IN THIS MANUAL. PATCHLINK® CORPORATION RESERVES THE RIGHT TO MAKE CHANGES TO THE INFORMATION DESCRIBED IN THIS MANUAL AT ANY TIME WITHOUT NOTICE AND WITHOUT OBLIGATION TO NOTIFY ANY PERSON OF SUCH CHANGES. THE INFORMATION PROVIDED IN THE MANUAL IS NOT GUARANTEED OR WARRANTED TO PRODUCE ANY PARTICULAR RESULT, AND THE ADVICE AND STRATEGIES CONTAINED MAY NOT BE SUITABLE FOR EVERY ORGANIZATION. NO WARRANTY MAY BE CREATED OR EXTENDED WITH RESPECT TO THIS MANUAL BY SALES REPRESENTATIVES OR WRITTEN SALES MATERIALS. PATCHLINK® CORPORATION SHALL NOT BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER DAMAGES ARISING FROM THE USE OF THIS MANUAL, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES

Trademarks:

PatchLink™, PatchLink.com™, securing the enterprise™, WebConsole™, PatchLink Update™, PatchLink Quarantine™, PatchLink Enterprise Reporting Services™, PatchLink Scanner Integration Module™, PatchLink Developers Kit™, and their associated logos are registered trademarks or trademarks of PatchLink® Corporation.

Novell, Novell ZENworks®, Novell ZENworks® Patch Management Server, and Novell Agent are registered trademarks or trademarks of Novell, Inc.

RSA Secured® is a registered trademark of RSA Security Inc.

Apache is a trademark of the Apache Software Foundation

In addition, other companies' names and products mentioned in this document, if any, may be either registered trademarks or trademarks of their respective owners.

Feedback:

Your feedback lets us know if we are meeting your documentation needs. E-mail the Novell Technical Publications department at techpubs@patchlink.com to tell us what you like best, what you like least, and to report any inaccuracies.



Table of Contents

Table of Contents	iii
--------------------------	------------

Preface	xiii
----------------	-------------

About This Guide	xiii
Document Conventions	xiv

Chapter 1: Novell ZENworks Patch Management Overview	1
---	----------

Product Overview	1
ZENworks Patch Management Server and Agent Process	2
System Requirements	3
Minimum Hardware Requirements	3
Supported Operating Systems	3
Other Software Requirements	3
Supported Database Servers	4
Recommended Configuration	4
Agent Supported Operating Systems	5
Agent Supported Languages	6

Chapter 2: Using Novell ZENworks Patch Management	7
--	----------

Getting Started with Novell ZENworks Patch Management	7
Accessing ZENworks Patch Management	8
Common Functions within ZENworks Patch Management Server	11
Defining Browser Conventions	11
Using Search	11
Using Tabbed Pages	12
Expanding and Collapsing Folders and Outlines	13
Advancing Through Pages	14
Using the Action Menu	14
Using Help	14
Exporting Data	15
Viewing the ZENworks Patch Management Server Home Page	16
Using the Navigation Menu	17
Viewing Latest News	19
Viewing the Documentation Links	20
Viewing Server Information	21
Viewing the Graph Dashboard	22
License Expiration	25



Chapter 3: Using Vulnerabilities and Packages 27

- About Vulnerabilities 28
 - Defining Vulnerability Structure 29
 - Vulnerabilities 29
 - Signatures 29
 - Fingerprints 29
 - Pre-requisites 30
 - Packages 30
- The Vulnerabilities Page 30
 - Viewing Vulnerabilities 31
 - Viewing Vulnerability Details 31
 - Vulnerability Status & Types 32
 - Vulnerability Package Cache Status & Type 33
 - Vulnerability Name 34
 - Vulnerability Impacts 34
 - Vulnerability Statistics 35
 - Searching, Filtering, and Saving Views 35
- Working with Vulnerabilities 36
 - Vulnerability Status Tabs 36
 - Column Definitions 37
 - Device Status 38
 - Deploying Vulnerabilities 39
 - Disabling and Enabling Vulnerabilities 39
 - Using the Scan Now Feature 40
 - Updating the Cache 42
- About Packages 43
- Using the Packages Tab 44
 - Package Information Tab 46
 - Package Statuses & Types 48
 - Package Column Definitions 49
 - Searching, Filtering, and Saving Views 49
- Working with Packages 50
 - Deploying a Package 50
 - Deleting a Package 50
 - Updating the Package Cache 51
 - Editing a Package 51
 - Creating a Package 51
- Using the Package Editor 52
 - Including Deployment Options in a Package 61
 - Package Flag Descriptions 61
 - Adding Files and Directories to a Package 63
 - Adding a Directory to a Package 64
 - Adding a New Macro to a Package 64



Creating a Drive for a Package	65
Creating a Folder for a Package	66
Adding a File to a Package	66
Deleting a File from a Package	67
Renaming a File within a Package	67
File Properties for a Package	68
Creating Scripts for a Package	69

Chapter 4: Working With Deployments 71

About Deployments	71
Viewing Deployments	71
Deployment Types	74
Standard and Chained Deployments	74
Using the Deployment Pages	76
Deployment Status and Type	77
Deployment Statistics	79
Deployment Details Summary	81
Working with Deployments	82
Deployments Page	82
Viewing the Deployment Details	83
Viewing Deployment Details by Device	85
Viewing Deployment Details by Device Group	86
Viewing Deployment Results	88
Explaining Deployment Distribution Order	89
Aborting Deployments	89
Disabling Deployments	90
Enabling Deployments	90
Modifying Deployments	90
Deleting Deployments	91
Explaining Deployment Deadlines	91
Using the Deployment Wizard	92
Introduction Page	93
Device/Device Groups Selection Page	94
Package Selection Page	96
Associated Vulnerability Analysis	98
Licenses Page	99
Deployment Options Page	100
Schedule Configuration Page	102
To Schedule a Recurring Deployment	103
Package Deployment Order and Behavior Page	106



- Package Deployment Behavior Options Page 110
 - Behavior Options 111
 - Optional Package Flags 112
 - Package Flag Descriptions 113
 - Package Display Options 114
- Notification Options Page 114
- Deployment Confirmation Page 117
- Associated Vulnerability Analysis Page 119
- Deployment Summary Page 120

Chapter 5: Using Devices and Inventory _____ 123

- About Devices 123
 - Viewing Devices 124
 - Using the Devices Page 125
 - Action Menu Functions 126
 - Device Status Icons 127
 - Using the Details by Device Page 128
 - Device Information Tab 128
 - Device Information Action Menu Items 132
 - Device Vulnerabilities 132
 - Action Menu Functions 133
 - Device Inventory 133
 - Action Menu Functions 134
 - Device Deployments 134
 - Action Menu Functions 134
- Working with Devices 135
 - Installing an Agent 136
 - Viewing Device Details 137
 - Disabling and Deleting a Device 138
 - Enabling a Device 138
 - Deploying a Vulnerability 139
 - Exporting Device Information 139
 - Scanning Devices 139
 - Rebooting Devices 139
- About Inventory 141
 - Viewing Inventory 141
- Using the Inventory Tab 142
 - Inventory Types 142
 - Operating Systems View 142
 - Software View 143
 - Hardware View 143
 - Services View 143
 - Action Menu Functions 143



Scanning Inventory	143
Manually Scheduling the DAU Task	144
Using Custom Inventory	144
Guidelines for Microsoft Windows based Operating Systems	145
Literal	145
Registry	145
Environment	145
WMI	146
Text_File	147
XML_file	147
Example XML File	148
Guidelines for Linux/Unix/Mac/Netware based Operating Systems	149
Literal	149
Dynamic	150
Example XML File	151

Chapter 6: Using Groups **153**

Groups and the Directory Tree	155
Parent and Child Groups	155
Defining Groups	155
Group Information	156
Group Information Settings	157
Assigned Email Notification Addresses	158
Assigned Child Groups	158
Assigned Mandatory Baseline Items	158
Assigned Policy Sets	159
Resultant Policy Information	159
Assigned Roles	160
Group Membership	160
Creating a Group	162
Moving a Group	162
Deleting Groups	164
Editing Groups	164
Device Membership	165
Managing Device Members	166
Enabling and Disabling Devices within a Group	168
Mandatory Baseline	169
Managing Mandatory Baselines	173
Removing Deployments Created By Mandatory Baselines	177
Device Group Vulnerabilities	178
Enabling Vulnerabilities within a Group	179
Disabling Vulnerabilities within a Group	180
Group Inventory	180



Device Group Deployments 181

 Deploying to a Group 182

Policies 183

 Adding a Policy to a Group 183

 Removing a Policy from a Group 184

Roles 185

 Adding a Role to a Group 185

 Removing a Role from a Group 186

Dashboard 187

Settings 190

 Working with the Group Settings 190

 Working with Source Groups 192

Chapter 7: Reporting **195**

About Reports 195

 Available Reports Page 195

 Report Parameters Page 196

 Report Parameters List 196

 Reports Results Page 197

 Viewing Reports 198

Working with Reports 199

 Searching Within Reports 199

 Displaying Time and Date in Reports 200

 Exporting Reports 200

 Viewing Printable Data in Reports 200

Available Reports 201

 Agent Policy Report 201

 Device Duplicate Report 202

 Device Status Report 202

 Detection Results Not Found Report 203

 Deployment Detail Report 203

 Deployment Error Report 204

 Deployment In-Progress Report 206

 Deployment Summary Report 207

 Mandatory Baseline Detail Report 208

 Mandatory Baseline Summary Report 209

 Package Compliance Detail Report 210

 Package Compliance Summary Report 211

 Vulnerability Analysis Report 212

 Hardware Inventory Detail Report 213

 Hardware Inventory Summary Report 213

 Operating System Inventory Detail Report 213

 Operating System Inventory Summary Report 214



Software Inventory Detail Report	214
Software Inventory Summary Report	214
Services Inventory Detail Report	215
Services Inventory Summary Report	215

Chapter 8: Managing Users and Roles 217

About User Management	217
Viewing Users	217
Defining User Access	218
Defining Users	218
Defining Roles	219
Exploring the Predefined System Roles	219
Defining Custom Roles	220
Defining Access Rights	220
Defining Accessible Device Groups	223
Defining Accessible Devices	224
Working with Users	224
Creating New Users	224
Adding Existing Users	226
Editing User Profiles	228
Removing ZENworks Patch Management Users	229
Deleting ZENworks Patch Management Users	229
Changing a User's Password	230
Exporting User Data	231
Working with User Roles	232
Creating User Roles	232
Editing User Roles	235
Assigning User Roles	238
Disabling and Enabling User Roles	239
Deleting User Roles	241
Exporting User Role Data	241

Chapter 9: Configuring Default Behavior 243

About the Options Page	243
Viewing Subscription Service Information	244
Subscription Service Information	245
Subscription Service History	246
Subscription Service Configuration	246
Subscription Service Status	247
Subscription Service Proxy Configuration	248
Subscription Service Communication Settings	248
Verifying Subscription Licenses	250



Table of Contents

Product Information	251
Novell ZENworks Patch Management Default Configuration	252
Configuring Deployment Defaults	253
Configuring Agent Defaults	255
Agent defaults allows for establishing default behavior for the deployment agent. Communication	255
Notification Defaults	256
Absentee Agent Management	256
Setting the User Interface Defaults	257
Customizing Row Values	258
Configuring ISAPI Communication Settings	259
Concurrent Agent Limit	259
Connection Timeout	259
Command Timeout	260
Customizing and Administering Agent Policy Sets	260
Viewing Agent Policy Summary Information	262
Creating a Policy Set	265
Editing a Policy Set	269
Deleting an Agent Policy Set	270
Defining Inventory Collection Options	271
Editing Agent Hours of Operation	274
Configuring Fastpath Servers	275
Defining Agent Policy Conflict Resolution	277
Using E-Mail Notification	279
Configuring E-Mail Notification	280
Defining E-Mail Alert Thresholds	281
Technical Support Information	282
Server Information	283
Component Version Information	284
Novell Support Information	284

Chapter 10: Using the ZENworks Patch Management Agent _____ 285

About the ZENworks Patch Management Agent for Pre Windows Vista	285
Viewing the Agent	285
Agent Components	285
Deployment Tab	286
Detection Tab	289
Proxies Tab	292
About Tab	294
User Interaction During a Deployment	295
User Interaction During a Reboot	297
About the ZENworks Patch Management Agent for Linux/Unix/Mac/Netware	298
About ZENworks Patch Management Agent for Windows Vista	299



Viewing the Agent	299
Agent Components	299
Home Page	300
Tools and Settings	301
Proxy Settings	302
Logging	303
Notification Manager	304
Management Server	305
User Interaction During a Deployment	306
User Interaction During a Reboot	307

Appendix A: Patch Management Server Reference _____ 309

Patch Management Server Security	309
ZENworks Patch Management Server Error Pages	310
WinInet Error Codes	311
HTTP Status Codes	311
ZENworks Patch Management Agent (Device) Status Icons	312

Appendix B: Securing Your ZENworks Patch Management Server _____ 315

Install Your Server With SSL	315
Use Secure Passwords	315
Turn Off File and Printer Sharing	316
Put Your ZENworks Patch Management Server Behind a Firewall	317
Turn Off Non-Critical Services	317
Lock Down Unused TCP and UDP Ports	317
Apply All Microsoft Security Patches	320

Appendix C: Using the Content Update Tool _____ 321

Content Update Tool System Requirements	321
Supported Operating Systems	321
Hardware Requirements	321
Other Requirements	321
Installing the Content Update Tool	322
Using the Content Update Tool	327
Configuration Page	328
Vulnerability Selection Page	330
Package Selection Page	332
Summary Report	336

Appendix D: Creating a Disaster Recovery Solution _____ 337

Preparing Your Database	337
Creating an Automated Solution	340



Table of Contents

Creating a Manual Solution 355

 Creating a Database Backup 355

 Restoring Your Backup 358

Appendix E: Using the Distribution Point 365

 Distribution Point Installation Requirements 365

 Supported Operating Systems 365

 Hardware and Software Requirements 365

 Installing the Distribution Point 366

 Configuring the Distribution Point 373

Appendix F: Glossary 375

Appendix G: Index 391



Preface

This ZENworks Patch Management Server v6.4 User Guide is a resource written for all users of ZENworks Patch Management Server v6.4. This guide defines the concepts and procedures for installing, configuring, implementing, and using Novell ZENworks Patch Management.

About This Guide

This guide contains the following chapters and appendices:

- Chapter 1, “Novell ZENworks Patch Management Overview”
- Chapter 2, “Using Novell ZENworks Patch Management”
- Chapter 3, “Using Vulnerabilities and Packages”
- Chapter 4, “Working With Deployments”
- Chapter 5, “Using Devices and Inventory”
- Chapter 6, “Using Groups”
- Chapter 7, “Reporting”
- Chapter 8, “Managing Users and Roles”
- Chapter 9, “Configuring Default Behavior”
- Chapter 10, “Using the ZENworks Patch Management Agent”
- Appendix A, “Patch Management Server Reference”
- Appendix B, “Securing Your ZENworks Patch Management Server”
- Appendix C, “Using the Content Update Tool”
- Appendix D, “Creating a Disaster Recovery Solution”
- Appendix E, “Using the Distribution Point”
- Appendix F, “Glossary”
- Appendix G, “Index”



Tip: This document is updated on a regular basis. To acquire the latest version of this document, please refer to the Novell Support Web site (www.novell.com/support).



Document Conventions




The following conventions are used throughout this document to help you identify various information types:

Table 1.1 Document Conventions

Convention	Usage
bold	Command names, database names, options, wizard names, window and screen objects (i.e. Click the OK button)
<i>italics</i>	New terms, variables, and window and page names
UPPERCASE	SQL commands and keyboard keys
monospace	File names, path names, programs, executables, command syntax, and property names

The icons used throughout this document identify the following types of information:

Table 1.2 Icons Used

Icon	Alert Label	Description
	Note:	Identifies paragraphs that contain notes or recommendations.
	Tip:	Identifies paragraphs that contain tips, shortcuts, or other helpful product information.
	Warning:	Identifies paragraphs that contain vital instructions, cautions or critical information.



1 Novell ZENworks Patch Management Overview

Novell Update is a tool to audit the current state of a network and install updates to the various devices within that company's network. The ZENworks Patch Management Server retrieves available vendor patches collected by Novell and bundled with scripts that use an Update Agent as a detection and installation tool.

A vulnerability includes information that is used by the agents to identify the requirements for the devices. This testing uses prerequisite profiles to determine if a patch is applicable to a computer. If the prerequisite profile matches then the agent will use detailed patch identifiers, called fingerprints, to verify the device has all the vulnerabilities installed and activated.

In This Chapter

- “Product Overview”
- “System Requirements”
- “Agent Supported Operating Systems”
- “Agent Supported Languages”

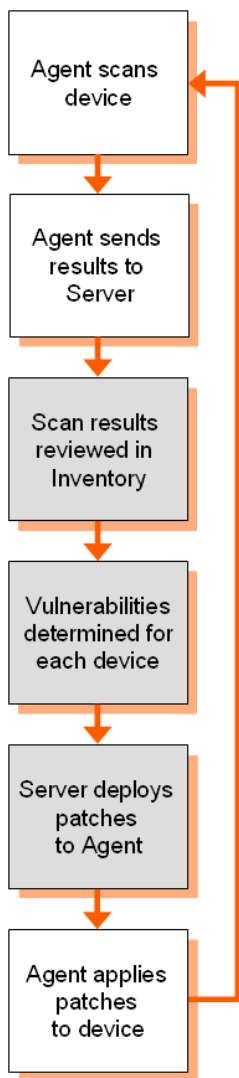
Product Overview

ZENworks Patch Management is an agent-based patch, vulnerability and compliance management system. The core component of the system is the ZENworks Patch Management Server, which monitors and maintains patch compliance throughout the entire enterprise through a centralized Web-interface. ZENworks Patch Management provides a means for an administrator to install a ZENworks Patch Management Agent on every client system in the target network ensuring all systems are protected.



ZENworks Patch Management Server and Agent Process

The following process map demonstrates how patch information is communicated between the ZENworks Patch Management Server and the Agent.



1. The Agent scans the host device and compiles information on operating system, software, hardware, and services on that device via the Discover Applicable Updates (DAU) task.
2. The DAU runs an inventory scan on the agent and sends the results back to the Server, which compares it with the list of known vulnerabilities. Based on this information, vulnerabilities are determined to be applicable for each device.
3. The results of the scan are returned to the ZENworks Patch Management Server and can be viewed at any time in the Inventory section of the product. If applicable, the ZENworks Patch Management Agent performs another scan using the patch fingerprints incorporated into each vulnerability to determine the device's patch status in relation to that vulnerability.
4. Once patch status is established, the Novell Patch Management Server Administrator creates deployments to patch the devices on the network. The deployments are then sent to the selected agents.
5. Once patch status is established, the Novell Administrator can deploy the desired vulnerability to each applicable device on the network.
6. After the agent receives the patch from the server, it applies the patches by installing them to the device. The device is now protected.



System Requirements

Minimum Hardware Requirements

The hardware requirements for Novell ZENworks Patch Management Server 6.4 vary depending upon the number of devices you manage. As the device count increases, so do the requirements. The following, minimum hardware requirements, will support up to 250 devices:

- A single 1.4 GHz Pentium or equivalent processor
- 512 MB RAM
- 36 GB of available disk space
- A single 100 Mbps network connection (with access to the Internet)



Note: For optimal performance please refer to the settings defined under “**Recommended Configuration**”.

Supported Operating Systems

Novell ZENworks Patch Management Server 6.4 is supported on the following Operating Systems:

- Microsoft Windows Server™ 2003, Web Edition with SP1 or later
- Windows Server 2003, Standard Edition with SP1 or later
- Windows Server 2003, Enterprise Edition with SP1 or later
- Windows Server 2003 R2, Standard Edition (SP2 optional but recommended)
- Windows Server 2003 R2, Enterprise Edition (SP2 optional but recommended)



Warning: Novell ZENworks Patch Management must be installed on an Operating System that is not a domain controller and uses any English locale (en-US, en-UK, en-CA, etc.) in its default configuration.

Other Software Requirements

Novell ZENworks Patch Management Server 6.4 requires the following software:

- Microsoft® Internet Information Services (IIS) 6.0
- Microsoft® .NET Framework version 1.1 SP1 and 2.0 (both versions are required)
- Microsoft Internet Explorer 6.x or higher
- Microsoft SQL Server (any version) must not be installed unless installed by a previous version of ZENworks Patch Management Server



Supported Database Servers

Novell ZENworks Patch Management Server 6.4 is supported on the following database servers:

- Microsoft® SQL Server 2005 Express Edition with SP2
- SQL Server 2005 Standard Edition with SP2
- SQL Server 2005 Enterprise Edition with SP2



Note: Novell ZENworks Patch Management Server installs SQL Server 2005 Express Edition with SP2 during installation. Therefore, you must not have any database server installed prior to the installation of Novell ZENworks Patch Management.

Recommended Configuration

Novell ZENworks Patch Management Server 6.4 recommends the following hardware:

Table 1.1 Novell ZENworks Patch Management Recommended Configuration

Number of Nodes	< 1000	<2,500	<5,000	<10,000	> 10,000
Operating System	Windows Server 2003, Web Edition with SP2	Windows Server 2003, Web Edition with SP2	Windows Server 2003, Web Edition with SP2	Windows Server 2003, Standard Edition with SP2	Contact Novell Professional Services
Database Server	SQL 2005 Express	SQL 2005 Express	SQL 2005 Express	SQL 2005 Express	
Processor	1 - 2.4 GHz	1 - Pentium 4	1 - Dual Core, Non-Xeon	2 - Dual Core Xeon	
RAM	1 GB	2 GB	2 GB	4 GB	
Storage	1 - 36 GB Hard Drive	1 - 72 GB Hard Drive	2 - 144 GB Hard Drives	4 - 144 GB Hard Drives	



Note: Refer to the [Novell Support](http://www.novell.com/support) Web site (www.novell.com/support) for additional configuration recommendations.



Agent Supported Operating Systems

The following table lists the supported platforms on which the ZENworks Patch Management Agent 6.4 is supported.

Table 1.2 ZENworks Patch Management Agent 6.4 Supported Platforms

Operating System	OS Versions	OS Edition	OS Data Width	Processor Family	Processor Data Width	Min. JRE
Apple Mac OS X	10.2.8 - 10.4.10	All	32/64 bit	x86(Intel)/PowerPC	32/64 bit	1.4.0+
HP-UX	11.00 - 11.23	All	64 bit	PA-RISC	64 bit	1.4.0+
IBM AIX	5.1 - 5.3	All	32/64 bit	PowerPC	32/64 bit	1.4.0+
Microsoft Windows 9x	98 Second Edition	All	32 bit	x86	32 bit	N/A
Microsoft Windows NT	4.0 SP6A - 2003 R2	All ⁽¹⁾	32/64 bit	x86	32/64 bit	N/A
Microsoft Windows XP	All	Professional ⁽²⁾	32/64 bit	x86	32/64 bit	N/A
Microsoft Windows Vista ⁽³⁾	All	All	32/64 bit	x86	32/64 bit	N/A
Novell Netware	6.5	All	32 bit	x86	32 bit	1.3.0+
Novell SUSE Linux	9 - 10	Enterprise	32/64 bit	x86	32/64 bit	1.4.0+
Red Hat Linux	2.1 - 4	Enterprise AS, ES, WS	32/64 bit	x86	32/64 bit	1.4.0+
Sun Solaris	2.6 - 10	All	32/64 bit	SPARC/x86	32/64 bit	1.4.0+
(1) Datacenter edition is not supported (2) Home, Media Center and Tablet PC editions are not supported (3) Windows Vista support requires .NET 3.0						



Agent Supported Languages

ZENworks Patch Management Agent 6.4 is supported on the following languages:

- en-AU: English (Australia)
- en-BZ: English (Belize)
- en-CA: English (Canada)
- en-JM: English (Jamaica)
- en-NZ: English (New Zealand)
- en-ZA: English (South Africa)
- en-GB: English (United Kingdom)
- en-US: English (United States)
- es-ES: Spanish (Spain)
- fi-FI: Finnish (Finland)
- fr-FR: French (France)
- de-DE: German (Germany)
- it-IT: Italian (Italy)
- ja-JP: Japanese (Japan)
- ko-KR: Korean (Korea)
- nl-NL: Dutch (Netherlands)
- pt-BE: Portuguese (Brazil)
- sv-SE: Swedish (Sweden)
- zh-CN: Chinese (Simplified)
- zh-CHS: Chinese (Simplified)
- zh-TW: Chinese (Traditional)
- zh-CHT: Chinese (Traditional)



2 Using Novell ZENworks Patch Management

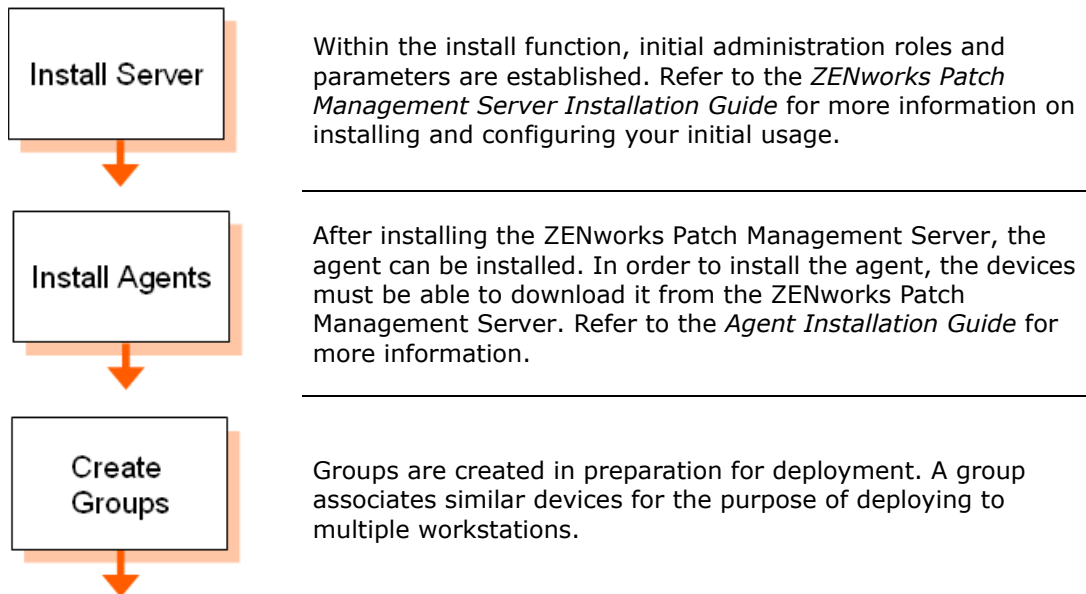
Novell Update monitors and sends patches to workstations and servers across a network. ZENworks Patch Management Server consists of a Web-based management console providing direct access to system management, configuration, reporting, and deployment options.

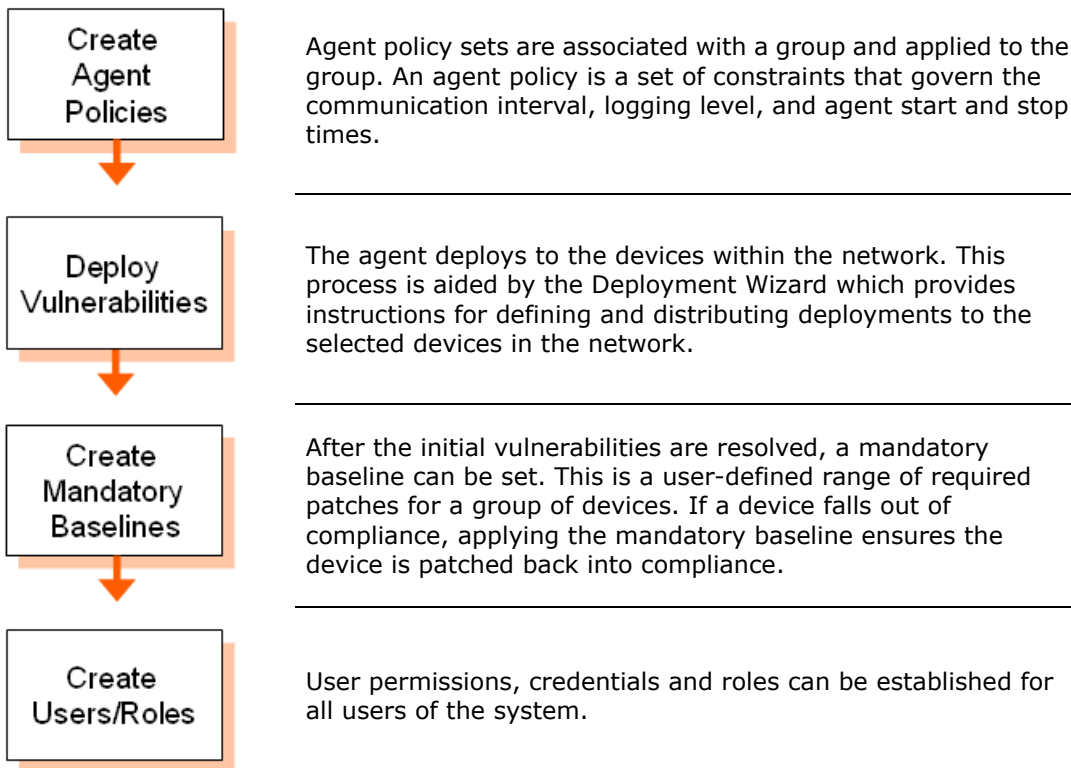
In this Chapter

- “Getting Started with Novell ZENworks Patch Management”
- “Accessing ZENworks Patch Management”
- “Common Functions within ZENworks Patch Management Server”
- “Viewing the ZENworks Patch Management Server Home Page”
- “Viewing the Graph Dashboard”
- “License Expiration”

Getting Started with Novell ZENworks Patch Management

Refer to the following process to determine tasks when using Novell ZENworks Patch Management.





Accessing ZENworks Patch Management

Novell ZENworks Patch Management is an internet application that conforms to standard web conventions. You can access the application from an internet browser. From the main screen, you navigate through the system with menu bars, scroll bars, icons, checkboxes, and hyperlinks.

Logging On to ZENworks Patch Management

1. Launch your web browser.
2. Type the ZENworks Patch Management Server URL in your web browser's **Location** field.



3. Press **Enter**.

The system displays the *Connect to Patch Management Server* dialog box.

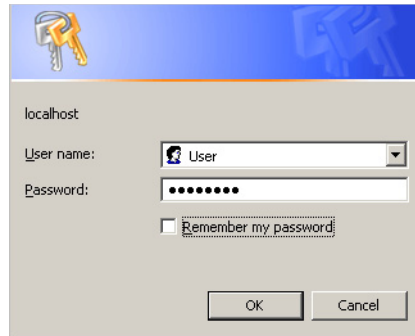


Figure 2.1 Log on dialog box

4. Type your user name in the *Username* field.

5. Type your password in the *Password* field.

6. Click **OK**.

The *ZENworks Patch Management Home* page opens.

Logging Out of ZENworks Patch Management

1. In the Navigation Menu, select **Log Out**. ZENworks Patch Management logs you out of the system and displays the *Novell Log Out* confirmation screen.

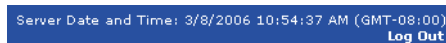


Figure 2.2 Log Out Menu Item



2. To reconnect to the system, click the **here** link.



Figure 2.3 Novell Logout Screen

Common Functions within ZENworks Patch Management Server

The following section describes standard browser conventions used and the navigational functions specific to ZENworks Patch Management. From the main screen, you can access all features of ZENworks Patch Management Server for which you are authorized. The screen is organized by function. Use the menu items at the top to navigate through the administrative options.

Defining Browser Conventions

ZENworks Patch Management supports the following browser conventions:

Table 2.1 Browser Conventions

Screen Feature	Function
Entry Fields	Type data into these fields, which allow the system to retrieve matching criteria or to enter new information.
Drop-Down Menus	Displays a list to select pre-configured values.
Command Buttons	Perform specific actions when selected.
Check Boxes	A check box is selected or cleared to enable or disable a feature. Lists also include a <i>Select All</i> check box that lets you select all the available listed items on that page.
Radio Buttons	Select the button to select an item.
Display Screens	Shows areas that are part of a window or an entire window. The data on display screens can be viewed, but not changed.
Sort	Data presented in tables can be sorted by ascending (default) or descending order within a respective column by clicking on a (enabled) column heading.
Mouseovers	Additional information may be displayed by hovering your mouse pointer over an item.
Auto Refresh	Where present and when selected, the Auto Refresh function automatically refreshes the page every 15 seconds.



Warning: The Groups page supports the right-click function, however in some areas of ZENworks Patch Management, it is not supported.

Using Search

Using the search feature, you can filter information retrieved from the database and the GSS. The search parameters differ within each function in ZENworks Patch Management.



Use the drop down lists to select the parameters you need for your search.

Name/CVE No:

Status:

Not Patched

Results for Groups:

My Devices

Impact:

--- All ---

Include Child Groups:

☐

Show results on Page Load:

☐

Save as Default View:

☐

Update View

Figure 2.4 Search feature for Vulnerabilities example

You can save frequently used search settings as your default. The checkboxes allow you to save your search and filter criteria. The following table describes these options.

Table 2.2 Search Settings

Select	To
Save as Default View	Save the active search and filter criteria as the default view for the page. The default view displays each time the page is accessed. You can change this setting at any time.
Show results automatically	Automatically retrieves and displays results from the database when the module is selected from the Navigation Menu.



Note: Your search and filter criteria will remain applicable, even after browsing to a different page, until you perform a new search or log out of ZENworks Patch Management.

Using Tabbed Pages

Tabs are labeled groups of options used for similar settings within a page. Select each tab to view the available options.

Users

Roles

<input type="checkbox"/> Action	User Role Name	Type	Access Rights	Users	Groups	Devices
<input type="checkbox"/>	Administrator	System	46	3	7	0
<input type="checkbox"/>	Guest	System	17	1	7	0
<input type="checkbox"/>	Manager	System	40	0	7	0
<input type="checkbox"/>	Operator	System	28	0	7	0

Figure 2.5 Tabbed Page Example



Expanding and Collapsing Folders and Outlines

Patch Management Server uses plus and minus sign options that allow you to expand and collapse folders, outlines, and other data sources on the page. The information is refreshed each time it is displayed.

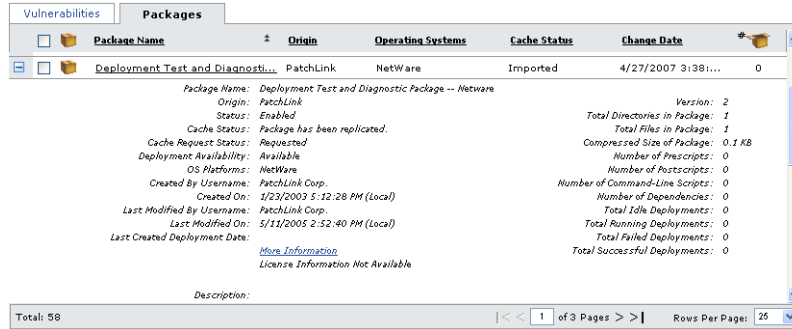


Figure 2.6 Show/Hide Row Option



Advancing Through Pages

Each page in Patch Management Server provides page-through options at the bottom of each tabbed page. The amount of items available for display and the specific page you are viewing determines how the options are presented.

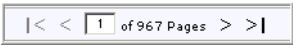


Figure 2.7 Pagination Feature

Table 2.3

Function	Use To
Next	Advance to the next page of entries or to the last page of entries by clicking the next page (>) or last page (>) links.
Previous	Return to the previous page of entries or to the first page of entries by clicking the previous page (<) or first page (<) links.
Current Page	Go to a specific page by entering the page number in the Current Page field.
Rows Per Page	Modify the number of entries displayed on a single page by selecting the desired number of records to display.



Note: When using the browser forward and back buttons, search selections do not get saved. A new search must be conducted.

Using the Action Menu

The Action menu displays at the bottom of each page and provides access to all actions available for each page and displays the logged in user in the left corner of the menu. The available commands vary depending where you are in the application. The action menu functionality depends on the role assigned to the user.



Figure 2.8 Action Menu

Using Help

Online Help is designed to provide users with the information they need to properly patch and manage a network.



Access to context sensitive help is available by clicking **Help** located in the navigation menu.

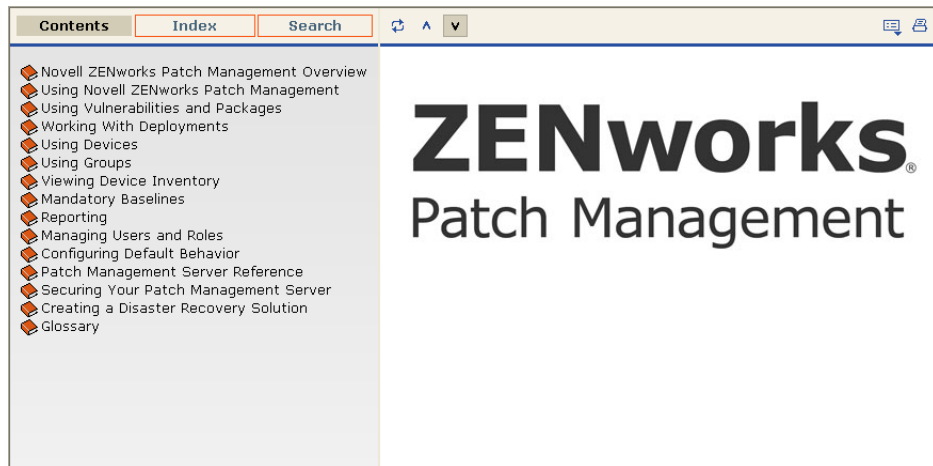


Figure 2.9 Example Help Screen

Exporting Data

Information presented in Patch Management Server can be exported into a comma-separated value (CSV) file. You may elect to save the file in a different file format *after* opening it from the download option.

To Export Data

1. If necessary, populate the page by clicking **Update View**.



Note: All data results will export, not just the selected results. However, some data may not import or translate into **.csv** format in a readable format.

2. Click **Export**.
3. In the *File Download* dialog box, select from the available options: **Open**, **Save**, **Cancel**.
 - **Open** - creates the file and opens it in your Web browser. From the browser you can save to a variety of file formats including; CSV, XML, text, and numerous spreadsheet applications.
 - **Save** - creates the file and saves it to a local folder. The file is saved to your My Documents folder in Microsoft Office Excel CSV format.



- **Cancel** - does not create or save the report.

	A	B	C	D	E
1	Device Class	Hardware	Device	OS info	Status
2	BIOS	A M I - 80003	WTP_EMERALD	Win2K3-Service Pack 1	Offline
3	Computer	Advanced Cor	WTP_EMERALD	Win2K3-Service Pack 1	Offline
4	Computer	Last Reboot =	WTP_EMERALD	Win2K3-Service Pack 1	Offline
5	Computer	Manufacturer	WTP_EMERALD	Win2K3-Service Pack 1	Offline
6	Computer	OS Serial Nur	WTP_EMERALD	Win2K3-Service Pack 1	Offline
7	Computer	Serial Number	WTP_EMERALD	Win2K3-Service Pack 1	Offline
8	Computer	Virtualization	WTP_EMERALD	Win2K3-Service Pack 1	Offline
9	Disk drives	Virtual HD	WTP_EMERALD	Win2K3-Service Pack 1	Offline
10	Display adapters	VM Additions	WTP_EMERALD	Win2K3-Service Pack 1	Offline
11	DVD/CD-ROM drives	MS C/DVD-R	WTP_EMERALD	Win2K3-Service Pack 1	Offline
12	Floppy disk controllers	Standard flopp	WTP_EMERALD	Win2K3-Service Pack 1	Offline
13	Floppy disk drives	Floppy disk d	WTP_EMERALD	Win2K3-Service Pack 1	Offline
14	IDE ATA/ATAPI controllers	Intel(R) 82371	WTP_EMERALD	Win2K3-Service Pack 1	Offline
15	IDE ATA/ATAPI controllers	Primary IDE C	WTP_EMERALD	Win2K3-Service Pack 1	Offline
16	IDE ATA/ATAPI controllers	Secondary ID	WTP_EMERALD	Win2K3-Service Pack 1	Offline

Figure 2.10 Exported Inventory Data

The file is named `<filename>Export.csv`, with the exported file containing data based on each type.

Viewing the ZENworks Patch Management Server Home Page

The entry point to Novell ZENworks Patch Management is the *Home* page. From this page, you can view patch management activity and retrieve system status reports for your ZENworks Patch Management Server.

From the Home page, you can access all features of the ZENworks Patch Management Server for which you are authorized. The Home page provides links to documentation, support resources, status information, patch-related news, and charts.

The screen is divided into four areas.

- **“Using the Navigation Menu”** - accesses the administrative options
- **“Viewing Latest News”** - provides a scrolling window with current information regarding patches
- **“Viewing the Documentation Links”** - provide user support and server status information
- **“Viewing Server Information”** - displays the status of your subscription



- “Viewing the Graph Dashboard” - displays group, agent, and patch status with interactive graphs

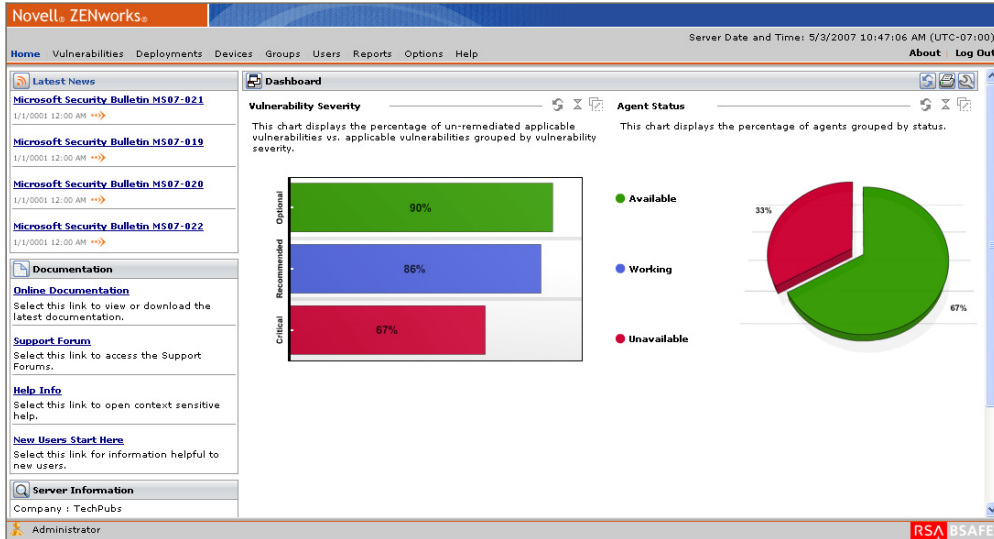


Figure 2.11 ZENworks Patch Management Server Home Page

Using the Navigation Menu

The ZENworks Patch Management Server Navigation menu displays product features based on functionality. Use the menu to navigate through the administrative options within the system. You can access all features of the system from this menu. When a menu item is selected, the system opens a series of tabbed folders.



Figure 2.12 Navigation Menu



The following table describes the navigation menu items and their functions within the system:

Table 2.4 ZENworks Patch Management Navigation Menu and Descriptions

Menu Item	Description
Home	Provides an overview of patch management activities and the Patch Management Server environment.
Vulnerabilities	Manages the vulnerabilities and packages used in deployments.
Deployments	Displays all current deployments.
Devices	Manages the devices registered to Patch Management Server and displays a comprehensive inventory of all registered devices.
Users	Manages users and roles including the assignment of access rights.
Reports	Generates full reports (Opens in a new browser window).
Options	Performs activities related to subscription, product information, default configuration settings, policy definitions, e-mail notifications, and support-related features.
Help	Accesses the online help system.
Log Out	Disconnects from ZENworks Patch Management.



Note: Certain installations may include additional modules that provide additional functionality such as enhanced reporting. Once installed, the component is included in the main navigation menu.



Viewing Latest News

The Latest News area displays important announcements and other information regarding the ZENworks Patch Management system. You can select any links within the news window. When a link is selected, a new window opens to display the news item in more detail.

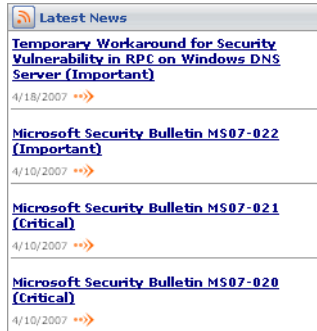


Figure 2.13 Latest News Window



Viewing the Documentation Links

The Documentation links provide access to obtaining information about ZENworks Patch Management. The links provide access to help, user documentation, and support regarding your Patch Management Server status.

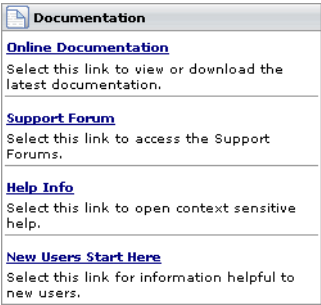


Figure 2.14 General Information links

The following table provides a description of the General Information links on the Home page.

Table 2.5 General Information Links

General Information Link	Description
Online Documentation	Provides a direct link to the latest Novell ZENworks Patch Management Server documentation.
Support Forum	Provides a location where the latest information and technical support about ZENworks Patch Management, its processes, functions and features are displayed.
Help Info	Provides comprehensive online help for ZENworks Patch Management.
New Users Start Here	Displays help information for new ZENworks Patch Management users.



Viewing Server Information

The Home page displays a *Server Information* area at the bottom of the page providing the serial number, number of licenses available, number of licenses in use, and information about current license usage and availability.

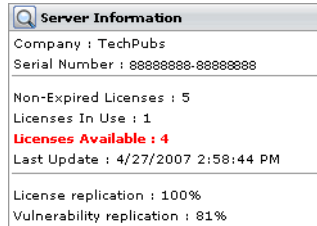


Figure 2.15 Patch Management Server Current Status

Table 2.6 ZENworks Patch Management Current Status Items

Status Item	Definition
Company	Name of the company that ZENworks Patch Management is registered to (defined during the installation process)
Serial Number	ZENworks Patch Management license number (serial number)
Non-Expired Licenses	Total number of active licenses Each registered device requires one license
Licenses in Use	Number of active licenses being used by registered devices as determined by agent registration
Licenses Available	Number of licenses that can be used to register devices and bring them into the protected ZENworks Patch Management network
Last Update	Most recent date and time ZENworks Patch Management received an update from the Global Subscription Server
License replication	Subscription Status between the local Patch Management Server server and the Global Subscription Server.
Vulnerability replication	Replication Status between the local Patch Management Server server and the Global Subscription Server patch repository.





Note: A License Expiration notice displays if all available licenses are in use. See “[License Expiration](#)” for more information.

Viewing the Graph Dashboard

The Dashboard consists of graphs providing a current view of activity on the protected network. These graphs are generated based on the latest data available and include all devices, groups, vulnerabilities, and packages.

The following table describes all of the available charts.














Table 2.7 Dashboard Charts

Chart	Description
Vulnerability Severity	This chart displays the percentage of un-remediated applicable vulnerabilities vs. applicable vulnerabilities grouped by vulnerability severity.
Vulnerability Severity by Device	This chart displays the percentage of un-remediated devices vs. applicable devices grouped by vulnerability severity.
Scheduled Remediation	This chart displays the percentage of un-remediated devices with a scheduled remediation vs. un-remediated devices grouped by vulnerability severity.
Mandatory Baseline Compliance	This chart displays the percentage of devices grouped by mandatory baseline compliance.
Incomplete Deployments	This chart displays the percentage of incomplete deployments grouped by the deployments percentage complete.
Agent Status	This chart displays the percentage of agents grouped by status.
Time since last DAU	This chart displays the percentage of available or working devices grouped by time since the last successful Discover Applicable Updates task.
Offline Agents	This chart displays the percentage of offline agents grouped by the time offline.



Use the following table to define your settings when viewing the graphs dashboard.

Table 2.8 Dashboard Settings and Behavior Icons

Icon	Function
	Opens the dashboard settings window.
	Opens a printable version of the currently displayed charts.
	Refresh all of the displayed charts.
	Display the chart descriptions on the dashboard.
	Do not display the chart descriptions on the dashboard.
	View the charts in one column.
	View the charts in two columns.
	Save the dashboard settings
	Move the selected chart up one level.
	Move the selected chart down one level.
	Refresh the selected chart.
	Minimize the chart.
	Hide the chart from view.



To Add a Graph to the Dashboard

1. Click the **Dashboard Settings** icon.
The *Dashboard Settings* drop-down list opens.

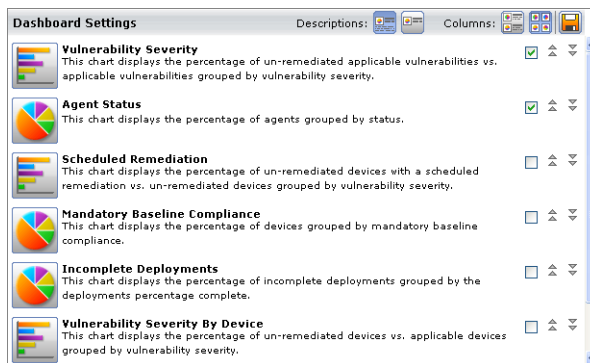


Figure 2.16 Dashboard Settings Window

2. Select the graphs you want to view by checking the box next to the graphs you want to add.
3. Move the graphs up or down according to your priorities.
4. Select a one or two column width view from *Columns*.
5. Using the *Descriptions* buttons, choose to *Show* or *Hide* the Chart Descriptions.
6. Click **Save**.
Your graph setting selections are saved and displayed in the Dashboard.

To Remove a Graph from the Dashboard

1. Click the **Dashboard Settings** icon.
The *Dashboard Settings* drop-down list opens.
2. Deselect the checkbox next to the graph(s) you want to remove. Click *Save Dashboard Settings*.
Click **Save** and the graph(s) is removed from the Dashboard window.

License Expiration

When the balance of licenses for your ZENworks Patch Management Server expire, the agent associated with an expired license is disabled and is not recognized by Patch Management Server. As a result, the agent ceases to communicate and cannot perform any tasks.



Tip: You can view the Subscription Service History and license checking by clicking **Subscription Service** in the Options page.

The *License Expiration* notice supersedes the home page and displays when you log on to Patch Management Server, and only occurs if the license is expired.

To proceed, select **Update License Data**. The license verification process begins and connects to the Global Subscription Server, retrieving updated license information. The page refreshes to the home page once your updated licenses have been saved.

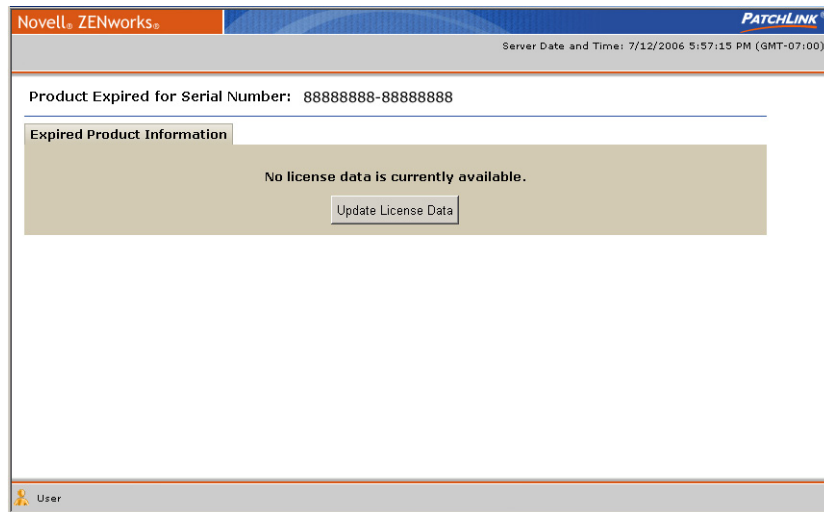


Figure 2.17 License Expiration Page



Note: If you need to renew licenses or add new licenses, contact your Novell representative at 800.858.4000.





3 Using Vulnerabilities and Packages

The *Vulnerabilities* page consists of two tabs where the majority of patch management activities are performed.

Vulnerabilities list all patch-related security issues across all devices registered to the ZENworks Patch Management Server. Within **ZENworks Patch Management Server**, a vulnerability consists of:

- The vulnerability description
- Signatures and fingerprints required to determine whether the vulnerability is patched or not patched
- Associated package or packages for performing the patch

Packages contain all vendor-supplied updates and executable code used to correct or patch security issues.

The following graphic illustrates the relationship between vulnerabilities and packages. Typically, a single vulnerability is shared by multiple products on multiple operating system platforms. There may be a series of separate patches to mediate the same vulnerability in different environments. The separate patches are grouped in packages identified by their respective product or OS. As a result, a series of packages are included for one vulnerability.

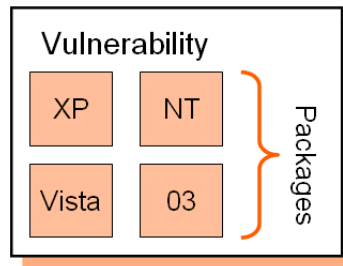


Figure 3.1 Vulnerability and Package relationship

In this Chapter

- “About Vulnerabilities”
- “The Vulnerabilities Page”
- “Working with Vulnerabilities”
- “About Packages”
- “Using the Packages Tab”
- “Working with Packages”



About Vulnerabilities

The vulnerabilities tab displays a complete listing of known patches and updates. Once reported and analyzed, the vulnerabilities are distributed to your ZENworks Patch Management Server through the Global Subscription Server.

The ZENworks Patch Management Agent installed on each device checks for known vulnerabilities using the Discover Applicable Updates (DAU) task. The DAU runs an inventory scan and sends the results back to ZENworks Patch Management Server, which compares it with the list of known vulnerabilities. If the device is found to have vulnerabilities, a deployment can be set up to remedy the issues.

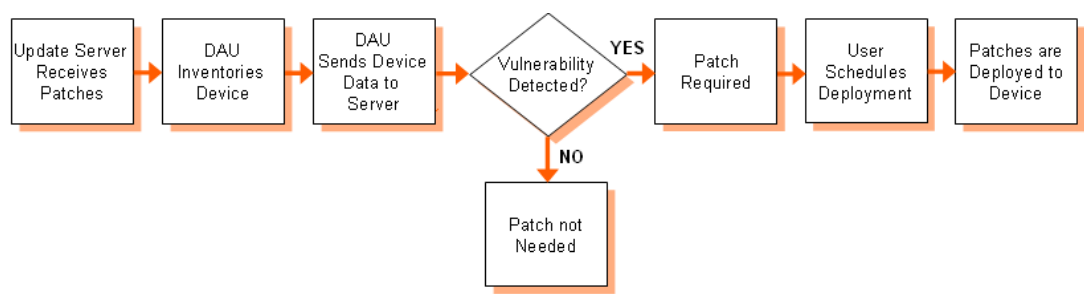


Figure 3.2 Discover Applicable Updates



Defining Vulnerability Structure

The structure of a Vulnerability allows the ability to create one patch applicable for many different operating systems and software versions. This allows for different packages and signatures capable of identifying the presence of patch files within a device.

As depicted in the following diagram, for each vulnerability you can have more than one signature. For each signature, you can have multiple fingerprints and pre-requisites. However, you can only have one package assigned per signature.

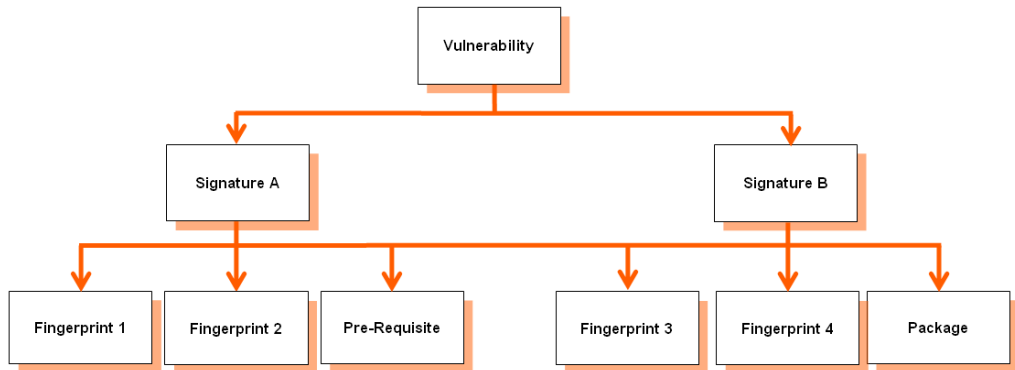


Figure 3.3 Patch Structure

Vulnerabilities

A vulnerability is the container for the entire object. All properties set for the vulnerability are viewed in the *Vulnerabilities* page of ZENworks Patch Management Server. Each vulnerability can have one or more signatures.

Signatures

Signatures recognize specific combinations of installed software in an operating system. Vulnerabilities usually contain multiple signatures to compensate for variances within applications. Frequently, a patch will require different executables, dynamic-link libraries, and switches in order to run or detect the patch within different operating systems.

Fingerprints

A fingerprint can represent a unique file, folder, registry key, or other data value somewhere within a system. Each signature can contain one or more fingerprints detecting if a patch is present in the system.



Pre-requisites

A pre-requisite is a signature belonging to another vulnerability with its own fingerprints. Adding a pre-requisite to a signature requires the pre-requisite be met before analyzing the signature for the current patch. If that signature's pre-requisite is met, the agent will analyze the fingerprints of the current signature, otherwise they will be ignored and the patch will not be applied to the device.

Packages

The package contains the actual files used to update or install software on the system. Each package contains the script commands for installing the package files or running the executable that installs the patch.

The Vulnerabilities Page

Vulnerabilities display in a table which outlines their impact and deployment status. The total number of vulnerabilities displays below the table in the bottom left corner.

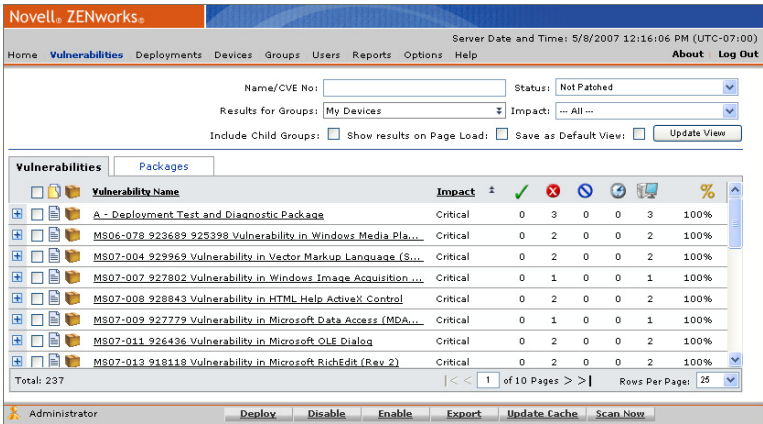


Figure 3.4 Vulnerabilities Page



Viewing Vulnerabilities

View details of a specific vulnerability by selecting the desired vulnerability and clicking the **vulnerability name**. The *Vulnerability Details* page (status page) represents the results of the vulnerability analysis and displays detailed data regarding the vulnerability.

A - Deployment Test and Diagnostic Package

Not Patched	Patched	Error	Detecting	Information
<input type="checkbox"/> Device Name	± DNS Name	Operating System	OS Service Pack	Analysis Date
<input type="checkbox"/> \\TP-MYSERVER	tp-myserver.techpubs.com	Win2K3	Service Pack 1	4/29/2007 5:45:28 PM

Figure 3.5 Vulnerability Details

To View a Vulnerability

1. In the *Vulnerabilities* list, select a vulnerability. You can only view the details of one vulnerability at a time.
2. Click the **Vulnerability name**.
The *Vulnerability Details* page for the selected vulnerability opens.

A - Deployment Test and Diagnostic Package

Not Patched	Patched	Error	Detecting	Information
<input type="checkbox"/> Device Name	± DNS Name	Operating System	OS Service Pack	Analysis Date
<input type="checkbox"/> \\TP-MYSERVER	tp-myserver.techpubs.com	Win2K3	Service Pack 1	4/29/2007 5:45:28 PM

Figure 3.6 Vulnerability Details

Viewing Vulnerability Details

Selecting the plus sign next to a vulnerability will display detailed information about the vulnerability. You can view this same detailed information on the *Vulnerability Details* page.

Vulnerabilities Packages

☐ Vulnerability Name
 Impact ±

☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

A - Deployment Test and Diagnostic Package

Type: Active Vulnerability Analysis

Impact: Critical

Status: Enabled

Downloaded On: 4/12/2007 10:45:32 AM (UTC-07:00)

Vulnerability Results: Current

Associated Packages: 1

Packages Status: Cached and ready for deployment.

Vendor: PatchLink Corporation

Released On: 11/18/2001 4:00:00 PM (UTC-07:00)

Vendor Product ID: PLDemo

Description: This is a demonstration for the package deployment feature in PatchLink Update. When you schedule this package deployment, your PatchLink Update Server (PLUS) will first download the package from PatchLink. Afterwards PatchLink Agent checks PLUS to determine if there are any task for the Agent computer. When the schedule time is reached, the PatchLink Agent will download the file PatchLink_deploy_demo.txt and store it in the system temp directory. [More Information](#)

Total: 171

<

1

>

of 7 Pages

Rows Per Page: 25

Figure 3.7 Vulnerability Details



Vulnerability Status & Types







The status of a vulnerability is indicated by an icon in the status column. The displayed vulnerabilities are determined by the filter criteria defined in the search section. The filter may be set to display vulnerabilities of a certain status type.

Table 3.1 Status and Description

Status	Description
New	Downloaded from the Global Subscription Server since the last session.
Current	Present vulnerabilities residing on ZENworks Patch Management Server.
Tasks	System task package.
Local	Locally created package.
Beta	Released to the Novell BETA community.

The following table includes descriptions of the Vulnerability status icons.

Table 3.2 Vulnerability Status Icons and Descriptions

New	Current	Beta	Status Description
			Active vulnerability.
			Vulnerability has been disabled.



Vulnerability Package Cache Status & Type

A vulnerability may have any number of packages associated with it. A package contains the patch to fix the vulnerability. Each package may be cached (downloaded) from the Global Subscription Server.

The downloading of packages can occur automatically if the vulnerability impact is rated as critical or if a deployment has been created for a particular package or vulnerability. Selecting the Package Cache Status icon, displays a list of the individual packages associated with the vulnerability. The following table describes the status descriptions.

Table 3.3 Status and Description

Status	Description
New	Downloaded from the Global Subscription Server since the last session.
Current	Present vulnerabilities residing on ZENworks Patch Management Server.
Tasks	System task package.
Local	Locally created package.
Beta	Released to the Novell BETA community.

The icons and their status are classified as follows:

Table 3.4 Package Status Icons and Descriptions






















New	Current	Tasks	Local	Description
				The package is not cached.
				The package has been scheduled to be cached or is in the process of being cached.
				An error occurred while trying to cache the package.
				The package is cached and ready for deployment.



Table 3.4 Package Status Icons and Descriptions

New	Current	Tasks	Local	Description
				The package is currently deploying (animated icon).
				The package is disabled.

Vulnerability Name

Vulnerability names typically include the vendor (manufacturer of the vulnerability) and specific application and version information.

Vulnerability Impacts

The following list describes each level of need for a device to have the vulnerability deployed and installed. Impacts can be viewed in Ascending or Descending order by clicking the icon (up or down arrows respectively) to the right of *Impact*.







- **Critical** - Novell or the product manufacturer has determined that this patch is critical and should be installed as soon as possible. Most of the recent security updates fall in to this category. The patches for this category are automatically downloaded and stored on your ZENworks Patch Management Server.
- **Critical - 01** - Novell or the product manufacturer has determined that this patch is critical and should be installed as soon as possible. This patch is older than 30 days and has not been superseded.
- **Critical - 05** - Novell or the product manufacturer has determined that this patch is critical and should be installed as soon as possible. These patches have been superseded.
- **Critical - Intl** - An international patch, where Novell or the product manufacturer has determined that this patch is critical and should be installed as soon as possible. Most of the recent international security updates fall in to this category. After 30 days international patches in this category will be moved to Critical - 01.
- **Detection** - These vulnerabilities contain signatures that are common to multiple vulnerabilities. They contain no associated patches and are only used in the detection process.
- **Informational** - These vulnerabilities detect a condition that Novell or the product manufacturer has determined as informational. If the report has an associated package, you may want to install it at your discretion.
- **Recommended** - Novell or the product manufacturer has determined that this patch, while not critical or security related is useful and should be applied to maintain the health of your computers.
- **Software** - These vulnerabilities are software applications. Typically, this includes software installers. The vulnerabilities will show not patched if the application has not been installed on a machine.
- **Task** - This category contains tasks which administrators may use to run various detection or deployment tasks across their network.
- **Virus Removal** - This category contains packages which administrators may use to run various virus detections across their network. Anti-Virus tools and updates are included in this category.



Vulnerability Statistics

The right-hand side of the vulnerability table contains columns which illustrate current statistics for the devices which have been scanned or will be scanned for that particular vulnerability. These statistics show the relationship between the vulnerability and the number of devices (or groups) that meet each status.

Table 3.5 Column Icon Definitions

Icon	Definition
	Total number of devices that are <i>Patched</i> .
	Total number of devices that are Not Patched .
	Total number of devices which returned an error.
	Total number of devices that are in the process of detecting. [whether the device is <i>Patched</i> or Not Patched]
	Total number of assigned or impacted devices.
	Percentage of the devices that have completed the detection. = [(Total Patched + Total Not Patched) / Total Assigned devices]

Searching, Filtering, and Saving Views

ZENworks Patch Management offers search and data filtering options that allow you to search for specific items and filter result sets. Searching and filtering can be performed independent of each other or can be combined to provide drill-down capabilities. Search and filter settings can be saved as the default view displayed on subsequent visits to the page.

Refer to “[Using Search](#)” for instructions on how to use the search and filter functions.



Working with Vulnerabilities

There are several tasks in vulnerabilities designed to assist with management and deployment. These are available from buttons located within the *Action* menu at the bottom of the Vulnerabilities page. These tasks include:

- “Deploying Vulnerabilities”
- “Viewing Vulnerabilities”
- “Disabling and Enabling Vulnerabilities”
- “Updating the Cache”
- “Using the Scan Now Feature”

Vulnerability Status Tabs

The results of the vulnerability analysis are detailed and separated into four tabs representing the status of devices applicable to the displayed vulnerability.

Table 3.6 Tabs and Descriptions

Status	Description
Not Patched	Devices detected as requiring the vulnerability patch.
Patched	Devices detected as being patched for that particular vulnerability.
Error	Devices that generated an error during the deployment of the vulnerability or subsequent DAU.
Detecting	Devices running or waiting for the DAU to begin.
Information	Displays detailed information about the vulnerability.



Column Definitions

Each tab in the details page displays basic device (agent) information in five columns. The following table includes descriptions of the Vulnerability column definitions.

Table 3.7 Vulnerability Column Definitions























Name	Definition
Device Name	The name of the device.
DNS Name	The DNS name for the device or its IP address if it does not have an assigned DNS name.
Operating System	The operating system (abbreviated) running the device.
OS Service Pack	Additional operating system version information.
Analysis Date	The date the agent on the device last ran the Discover Applicable Updates system task.



Device Status

Also displayed in the Vulnerability Details page is the status of the agent installed on the device. The following table defines agent (device) status and associated icons.

Table 3.8 Device Status Icons

Active	Pending	Description
	N/A	The agent is currently working on a deployment (animated icon).
		The agent is idle, and has pending deployments.
		The agent is offline.
		The agent is sleeping due to its Hours of Operation settings.
		This agent has been disabled.
		The agent is offline and is in a QChain status (can accept chained deployments only after reboot).
		The agent is offline and is in a Reboot status (can accept no more deployments until after it reboots).
		The agent is in a QChain status (the agent can accept chained deployments only until after a reboot).
		The agent is in a Reboot status (the agent can accept no more deployments until after it reboots).
		The agent is in a QChain status (the agent can accept chained deployments only until after a reboot) and is sleeping due to its Hours of Operation settings.
		The agent is in a Reboot status (the agent can accept no more deployments until after it reboots) and is sleeping due to its Hours of Operation settings.
	N/A	Unable to identify the agent status.



Deploying Vulnerabilities

Deploying a vulnerability to selected devices is a key function of the ZENworks Patch Management Server. Deployments are initiated by selecting **Deploy** and completing the *Deployment Wizard*. The *Deployment Wizard* provides step-by-step instructions for defining and distributing vulnerabilities to the protected devices in the network. Refer to [Chapter 4, “Working With Deployments”](#) for additional information.

Disabling and Enabling Vulnerabilities

Enabled vulnerabilities are included in the scanning activity of the DAU system task. All vulnerabilities are initially enabled. When a vulnerability is disabled, it is not included in the list for the *DAU* system task.

Once disabled, the vulnerability may not appear in the Vulnerabilities list based on your filter settings. To include disabled vulnerabilities in the list, select **Disabled Vulnerabilities** or **All** in the Status filter.

To Disable a Vulnerability

1. In the *Vulnerabilities* list, select one or multiple vulnerabilities.
2. In the action menu, click **Disable**.
The vulnerability displays with the *disabled* icon in the status column.

To Enable a Vulnerability

1. In the *Vulnerabilities* list, select a disabled vulnerability.
2. In the action menu, click **Enable**.
The vulnerability displays with the *enabled* icon in the status column.



Using the Scan Now Feature

Complete the following steps to use the Scan Now Action Menu item.

To Use Scan Now

1. Select one or more devices or device groups (if you do not select a device or device group, the DAU will be scheduled for all devices).
2. Click **Scan Now**.
The *Scan Now* window opens.



Figure 3.8 Scan Devices

3. Select **Yes, scan the selected device** and click **Schedule**.

The *Scan Now - Success* dialog box appears informing you that the scan has been scheduled and providing a link to view the scheduled deployment.

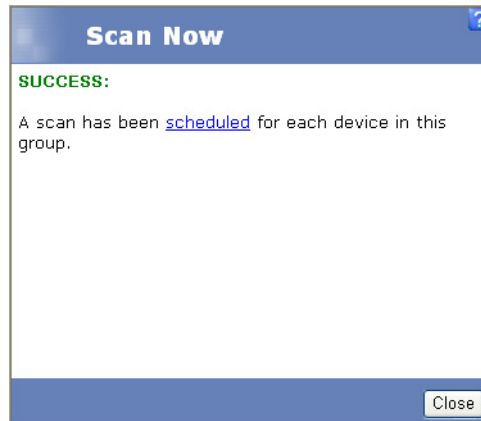


Figure 3.9 Scan Group Scheduled



Note: As with all deployments, although the DAU is scheduled for immediate execution, it will not actually occur until the next time the agent checks in.

4. Click **Close**.
The window closes.



Updating the Cache

Update Cache initiates a process that gathers the packages associated with the selected vulnerability and copies those packages to your ZENworks Patch Management Server.

To Cache Data

1. On a Vulnerability page, tab, or view, click **Update View** to display the vulnerabilities that match your filter criteria.
2. Select the vulnerabilities to cache.
3. In the *Action* menu, click **Update Cache**.
The *Warning* dialog box opens informing you that the update request and this action may take an extended period of time.
4. Click **OK**.

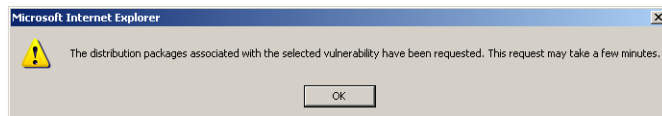


Figure 3.10 Update Cache - Warning dialog box

About Packages

A package is an archive containing the patch software and executable code required to deploy and install a patch. The process of sending a package to a device is called a package deployment.

Packages can run tasks, scripts, install software applications, send files to a specified location, and change the configuration of an application or service.

To View Packages

1. In the Patch Management Server main toolbar, select **Vulnerabilities**.
2. In the *Vulnerabilities* page, select the **Packages** tab.
3. If needed, select criteria from the *Groups*, *Status*, or *Impact* drop-down lists.
4. Select **Update View**.
The system displays the existing package list in the *Packages* tab.

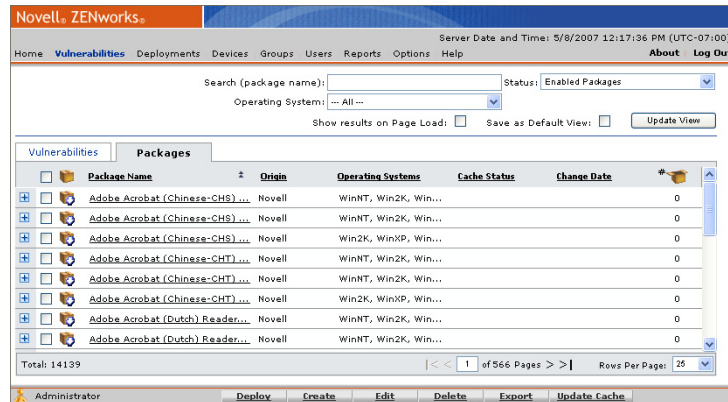


Figure 3.11 Packages View



Using the Packages Tab

Click expand to display detailed package information. Select the package name to display the package details. This includes the package deployment information and the package information tabs.

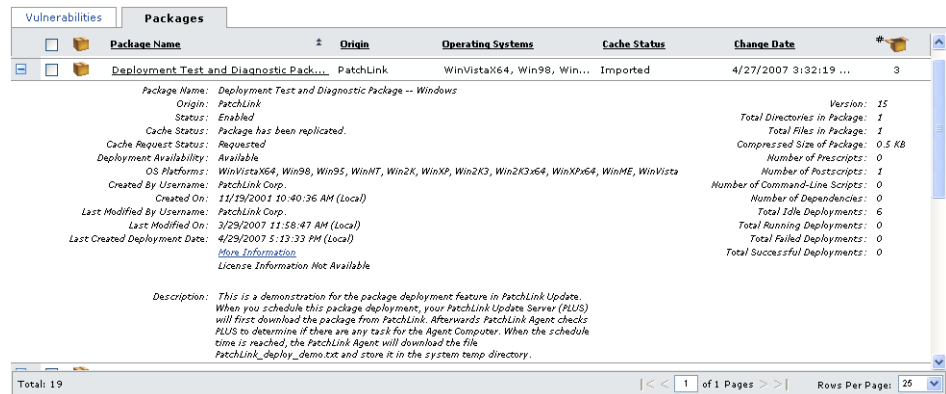


Figure 3.12 Package Details

The package summary includes the following information:

Table 3.9 Package Summary Definitions

Status	Description
Package Name	Title of the package.
Origin	Point of origin of the package. An origin of Novell or System refers to packages created by Novell.
Status	The current status of the package, stating if the package is enabled and ready to be requested from the Global Subscription Server
Cache Status	The current cache status of the package. A package is considered cached when it has been downloaded from the Global Subscription Server and actually resides on the local server.
Cache Request Status	Indicates if the package has been requested from the Global Subscription Server.
Deployment Availability	Indicates if the package has completed caching, and is available for deployment.
OS Platforms	The operating systems and platforms that the package supports and may be deployed to.



Table 3.9 Package Summary Definitions

Status	Description
Created By Username	The user who created the package.
Created On	The date and time the package was created.
Last Modified By Username	The user who last modified the package.
Last Modified On	The date and time of the last change to the package.
Last Created Deployment Date	The date and time a deployment was last created using this package.
More Information	If available, presents a link to detailed package information. This might be an article or other resource from a third-party.
License Information	If available, presents a link to detailed license information.
Description	Narrative description of the distribution package. Also includes links to any relevant Novell knowledge base articles.
Version	The package version.
Total Directories in Package	The number of directories contained in the package.
Total Files in Package	The number of files contained in the package.
Compressed Size of Package	The file size of the compressed package (in KB).
Number of Prescripts	The total number of prescripts contained in the package.
Number of Postscripts	The number of postscripts contained in the package.
Number of Command-line Scripts	The number of command-line scripts contained in the package.
Number of Dependencies	The number of dependencies associated with the distribution package.
Total Idle Deployments	The number of idle deployments.
Total Running Deployments	The number of running deployments.
Total Failed Deployments	The number of failed deployments.
Total Successful Deployments	The number of successful deployments.



Package Information Tab

Access similar information in the *Package Details* page by clicking the *package name* and selecting the *Information* tab.

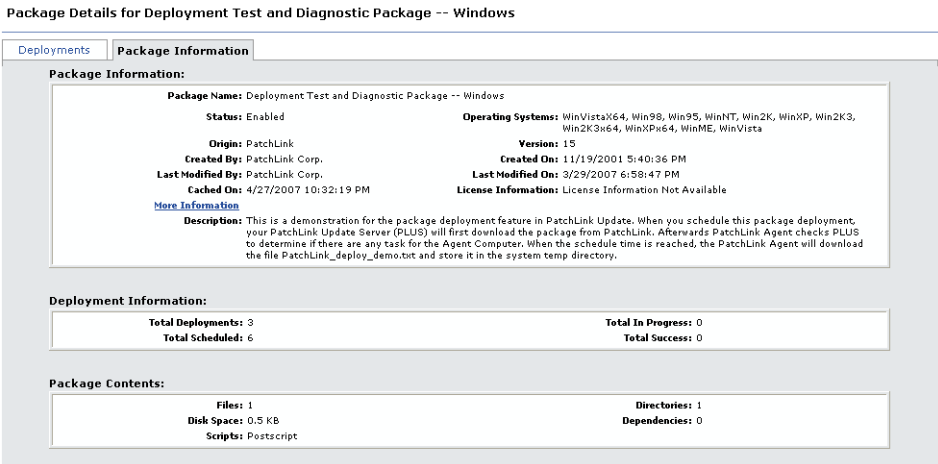


Figure 3.13 Package Details - Package Information tab

Table 3.10 Package Information Definitions

Status	Description
Package Information	
Package Name	Title of the package.
Status	The current status of the package, stating if the package is enabled and ready to be requested from the Global Subscription Server
Origin	The origin of the task or which company created the package.
Operating Systems	The operating systems and platforms that the package supports and may be deployed to.
Created By	The user who created the package.
Last Modified By	The user who last modified the package.
Cached On	The date and time the distribution package was last cached.
More Information	If available, presents a link to detailed package information. This might be an article or other resource from a third-party.



Table 3.10 Package Information Definitions

Status	Description
Description	Narrative description of the distribution package. Also includes links to any relevant Novell knowledge base articles.
Version	The package version.
Created On	The date and time the package was created.
Last Modified On	The date and time of the last change to the package.
License Information	If available, presents a link to detailed license information.
Deployment Information	
Total Deployments	The total number deployments.
Total Scheduled	The number of scheduled deployments.
Total In Progress	The number of running deployments.
Total Success	The number of successful deployments.
Package Contents	
Files	The number of files contained in the package.
Disk Space	The file size of the compressed package (in KB).
Scripts	The total number of scripts (includes Prescripts, Postscripts, and Command-line scripts) contained in the package.
Directories	The number of directories contained in the package.
Dependencies	The number of dependencies associated with the distribution package.



Package Statuses & Types

The Package status is indicated by an icon in the status column. The filter may be set to display packages according to status.

Vulnerabilities		Packages						
<input type="checkbox"/>		Package Name	Origin	Operating Systems	Cache Status	Change Date	#	
		Deployment Test and Diagnostic Pack...	PatchLink	WinVistaX64, Win98, Win...	Imported	4/27/2007 3:32:19 ...	3	
		MS_935964 Temporary Workaround fo...	PatchLink	Win2K, Win2K3	Imported	4/27/2007 3:38:40 ...	0	
		MS06-078 923689 925398 (32bit) Vul...	PatchLink	Win2K, WinXP, Win2K3	Imported	4/27/2007 3:34:48 ...	0	
		MS07-002 927198 925524 Vulnerabilit...	PatchLink	Win98, WinNT, Win2K, W...	Imported	4/27/2007 3:39:51 ...	0	
		MS07-002 927198 925524 Vulnerabilit...	PatchLink	Win98, WinNT, Win2K, W...	Imported	4/27/2007 3:32:39 ...	0	
		MS07-003 925938 921593 Vulnerabilit...	PatchLink	WinNT, Win2K, WinXP, W...	Imported	4/27/2007 3:45:18 ...	0	
		MS07-003 925938 924085 Vulnerabilit...	PatchLink	Win2K, WinXP, Win2K3	Imported	4/27/2007 3:45:39 ...	0	
		MS07-004 929969 (2K3 SP1) Vulnera...	PatchLink	Win2K3	Imported	4/27/2007 3:38:54 ...	0	
		MS07-004 929969 (2K3) Vulnerability ...	PatchLink	Win2K3	Imported	4/27/2007 3:32:14 ...	0	
		MS07-012 924667 927696 Vulnerabilit...	PatchLink	Win2K, WinXP, Win2K3	Imported	4/27/2007 3:36:57 ...	0	
		MS07-013 918118 (2K3) Vulnerability ...	PatchLink	Win2K3	Imported	4/27/2007 3:40:52 ...	0	
		MS07-013 918118 920813 Vulnerabilit...	PatchLink	Win2K, WinXP, Win2K3	Imported	4/27/2007 3:45:11 ...	0	
		MS07-013 918118 920816 (x86) Vuln...	PatchLink	Win98, WinNT, Win2K, W...	Imported	4/27/2007 3:38:50 ...	0	
		MS07-013 918118 920816 Vulnerabilit...	PatchLink	Win2K, WinXP, Win2K3	Imported	4/27/2007 3:39:07 ...	0	
Total: 19		< < 1 of 1 Pages > > Rows Per Page: 25						

Figure 3.14 Package Status

The following table describes the status of the package and the description.

Table 3.11 Status and Descriptions

Status	Description
New	Downloaded from the Global Subscription Server since the last session.
Current	Present vulnerabilities residing on ZENworks Patch Management Server.
Tasks	System task distribution package.
Local	The locally created distribution package.
















The icons and their status are classified as follows:

Table 3.12 Package Status Icons and Descriptions

New	Current	Tasks	Local	Description
				The package is not cached.
				The package has been scheduled to be cached or is in the process of being cached.



Table 3.12 Package Status Icons and Descriptions

New	Current	Tasks	Local	Description
				An error occurred while trying to cache the package.
				The package is cached and ready for deployment.
				The package is currently deploying (animated icon).
				The package is disabled.

Package Column Definitions

The following table includes descriptions of the package column definitions.

Table 3.13 Package Column Definitions

Name	Definition
Package Name	Name includes vendor, application, and version information.
Package Origin	The origin of the task or which company created the package.
Package Operating Systems	Which platforms are supported by the package.
Package Deployment Associations	Number of deployments associated with the package.

Searching, Filtering, and Saving Views

ZENworks Patch Management offers extensive search and data filtering options that allow you to search for specific items and filter result sets. Searching and filtering can be performed independent of each other or can be combined to provide extensive drill-down capabilities. Results can then be saved as a view that is displayed on subsequent visits to the page.

Refer to [“Using Search”](#) for instructions on how to use the search and filter functions.



Working with Packages

There are several tasks associated with packages designed to assist you in the management and deployment of packages. These are available from commands located in the *Action* menu at the bottom on the *Packages* page. These tasks include:

- “Deploying a Package”
- “Creating a Package”
- “Editing a Package”
- “Deleting a Package”
- “Updating the Package Cache”

Deploying a Package

Deploying a package is performed similarly to deploying a vulnerability. Deployments are initiated by clicking **Deploy** and completing the *Deployment Wizard*. The *Deployment Wizard* provides step-by-step instructions for defining and pushing deployments out to the protected devices in the network. See [Chapter 4, “Working With Deployments”](#) for more information.



Tip: Deploying via the Packages page will allow you to deploy inapplicable packages such as the custom packages that you have created.

Deleting a Package

Deleting a package removes the package from the list of available packages and all records of the package from the database (system-task packages cannot be removed).



Note: Package metadata for Novell-provided packages that are deleted will be re-downloaded from the Global Subscription Server. However, the package will not be cached unless it is associated with a critical vulnerability or included in a deployment.

To Delete a Package

1. In the *Packages* list, select one or multiple packages.
2. In the action menu, click **Delete**.
The *Warning* dialog box opens, informing you of the expected processing time for the action.
3. Confirm the request to delete the package(s).
4. The package(s) is deleted from the packages list.

Updating the Package Cache

Updating the system cache initiates the process to cache (or re-cache) the selected packages.

To Cache Package Data

1. In the *Packages* list, select one or multiple packages.
2. In the *Action* menu, click **Update Cache**.
The *Warning* dialog box opens, informing you of the expected processing time for the action.
3. Click **OK**.
The Package Data is cached.

Editing a Package

Changing a package is restricted to custom packages created by you or another Novell Patch Management Server administrator.



Note: Packages with an origin of PatchLink or System cannot be modified.

To Edit a Package

1. In the *Packages* list, select a package.
2. In the action menu, click **Edit**.
The package is displayed in the *Edit Packages* dialog box.
3. Make the desired edits and click **OK**.
4. Refer to the “[Creating a Package](#)” for details on changing packages through the Package Editor Wizard.

Creating a Package

Complete the following steps to create a package.

To Create a Package

1. In the *Packages* list, click **Create**.
The *Welcome to the Package Editor* screen opens.
2. Refer to the “[Using the Package Editor](#)” for details on changing packages through the Package Editor wizard.



Using the Package Editor

Creating distribution packages is performed using the Package Editor wizard.

To Create a Package

1. In the *Packages* list, click **Create**.
The *Welcome to the Package Editor* screen opens.

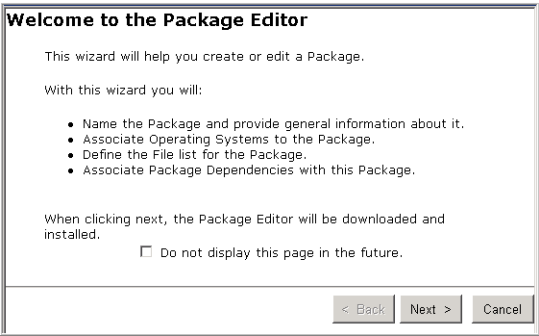


Figure 3.15 Package Editor Welcome Screen

2. Click **Next**.



Note: The Package Editor requires the installation of an ActiveX control.



3. In the *Package Editor*, type the **name**, **description** (optional), and an **Informational URL** (optional).

Figure 3.16 Package Editor - Name Package

- **Name** - A name or title for the package. Ensure package names are descriptive and short. Packages of the same name are permitted and names can be changed later.
- **Description** - An optional description allows you to specify details about the package. A good practice would be to add additional information as the package is modified, or to provide cautions and/or warnings to the potential user.
- **Information URL** - Link to additional information on the contents and usage of the package. The information URL will be displayed when viewing package information and allows the user to link to extended package information.



Note: Deployment options for manual installations of a patch can be included in the Description field. See [“Including Deployment Options in a Package”](#) for more information about using deployment options.

4. Click **Next**.



- 5. In the **Operating Systems** page, select the target operating systems from the list. These are the platforms running devices that are the target of the package deployment.

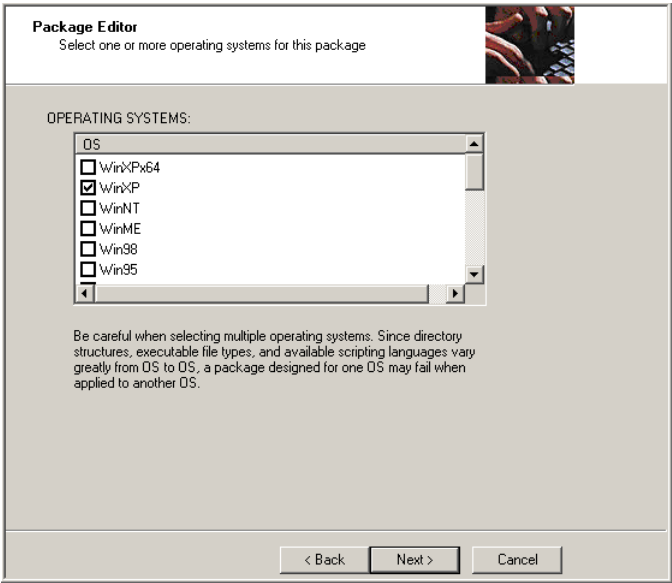


Figure 3.17 Package Editor - Select Operating System



Note: Since directory structures, executable file types, and available scripting languages vary greatly within Operating Systems, a package designed for one Operating System may fail when applied to another Operating System.

- 6. Click **Next**.



7. In the **Add Files** page, include any files to be included in the package.

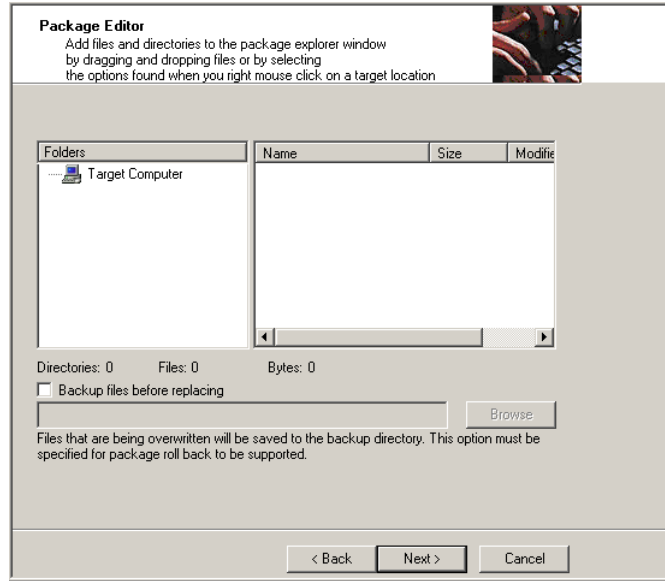


Figure 3.18 Package Editor - Add Files

Refer to [“Adding Files and Directories to a Package”](#) for additional details regarding adding Files to a package.

8. Click **Next**.



9. In the **Create Scripts** page, add a script to run on the target device during the deployment process, if needed.

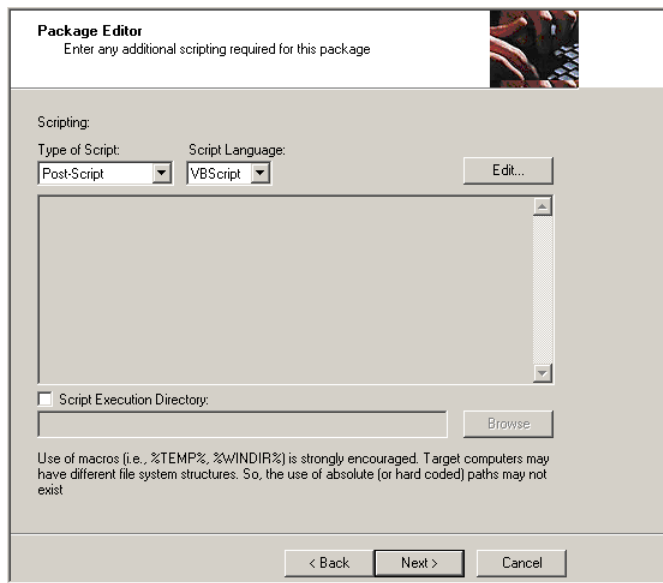


Figure 3.19 Package Editor - Create Script

Refer to [“Creating Scripts for a Package”](#) for additional details regarding Package scripts.

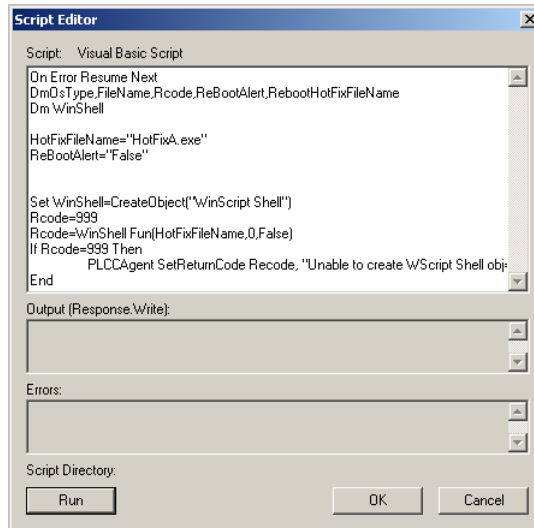


Figure 3.20 Script Editor

10. Click Next.



11. In the **License Agreement** page, select the *License Agreement* check box and enter the appropriate URL in the destination address of the **License URL** field.

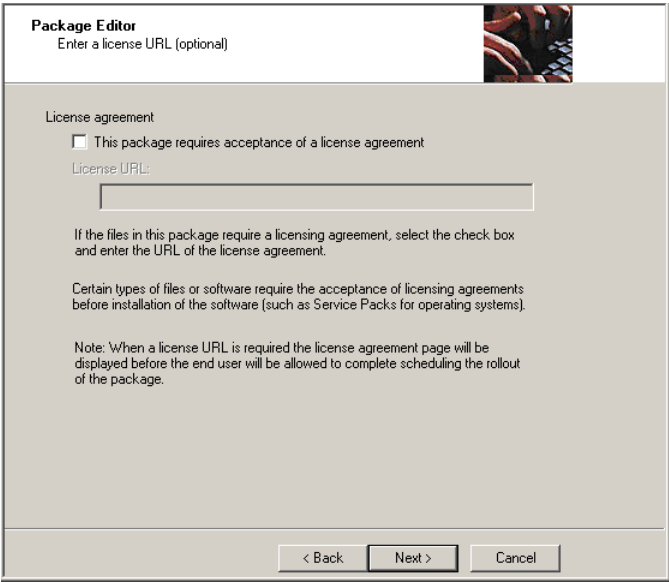


Figure 3.21 Package Editor - License URL

The License Agreement screen allows you to enter in an optional *License URL*, which can link to licensing information for the contents of the package. This option primarily is for packages containing items such as operating system service packs, device drivers, etc. The License URL will display when viewing package information and will allow the user to link to the license information.

12. Click **Next**.



13. In the **Summary** page, review the summary of the package to be deployed.

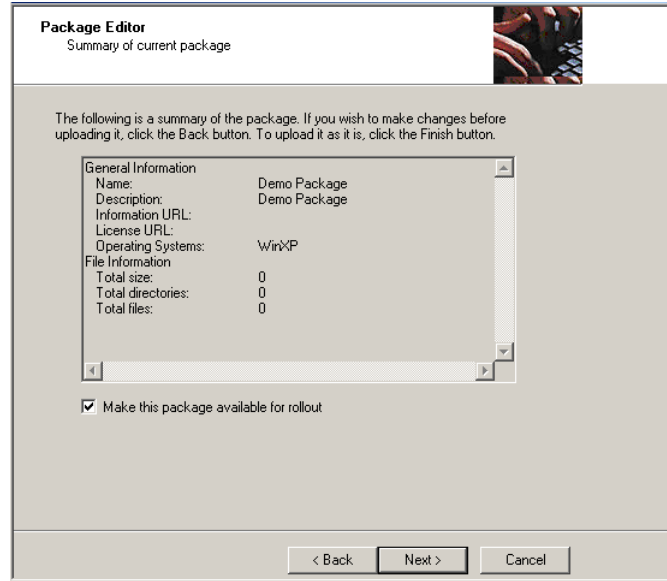


Figure 3.22 Package Editor - Summary

14. Click **Next**.



Note: Selecting the **Make this package available for rollout** checkbox enables the package to display in the list of available packages. You may wish to deselect this option if you are creating a package that will have additional files or details added at a later date or do not want to deploy the package at this time.

15. The **Upload Status** page verifies that the data is unpacking and uploading. Once all files are uploaded, click **Next**.
The *Upload Summary* page opens.



16. Click **Finish**.
The screen refreshes and the Package page opens with the custom package.

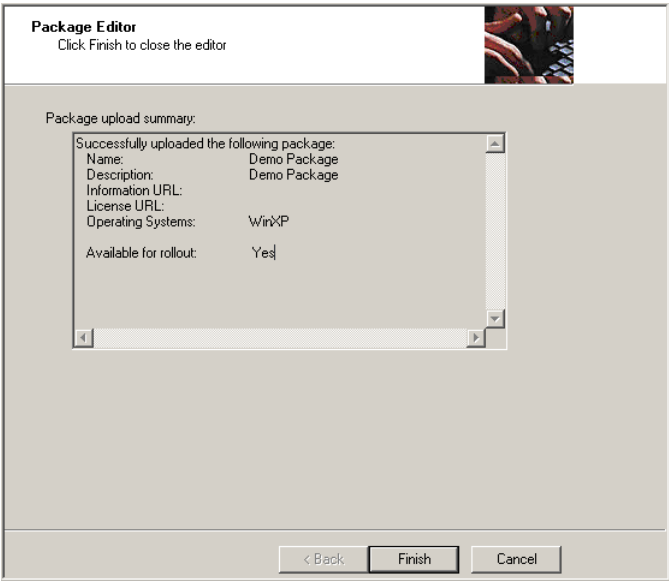


Figure 3.23 Package Editor - Upload Summary

Upon refreshing of the Packages page, you can view the package by the name you gave it, and view the operating systems that you chose to deploy to during the patch building process.

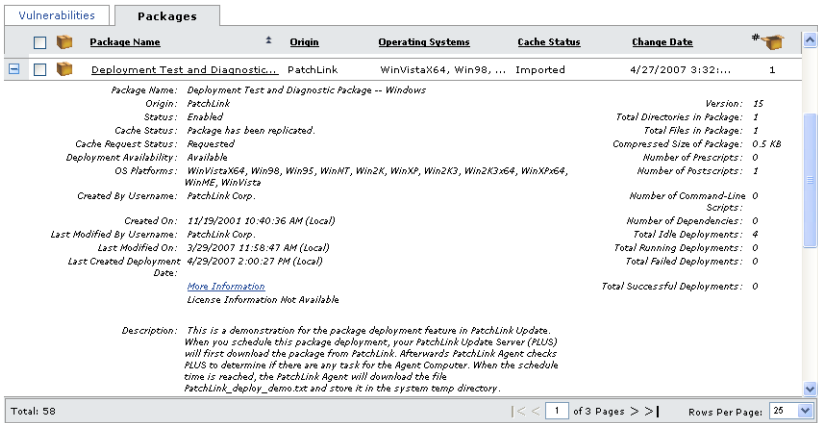


Figure 3.24 Packages Page - Custom Package



Including Deployment Options in a Package

The following tags indicate a manual installation of the patch is required. To use this option, type (manual install) in the description field.

A number of additional deployment options are available by including them in with the flags delimiter. To add these, enter (PLFlags: <Your Flags>) to the description field.

Package Flag Descriptions

The following table defines the flag behavior and their descriptions:

Table 3.14 Package Flag Descriptions and Behavior

Description (flag behavior)	Display Flag	Select Flag
Perform an uninstall; can be used with -m or -q	-yd	-y
Force other applications to close at shutdown	-fd	-f
Do not back up files for uninstall	-nd	-n
Do not restart the computer when the installation is done	-zd	-z
Use quiet mode, no user interaction is required	-qd	-q
Use unattended Setup mode	-md	-m
Install in multi-user mode (UNIX, Linux only)	-dmu	-mu
Install in single-user mode (UNIX, Linux only)	-dsu	-su
Restart service after installation (UNIX, Linux only)	-drestart	-restart
Do not restart service after installation (UNIX, Linux only)	-dnorestart	-norestart
Reconfigure after installation (UNIX, Linux only)	-dreconfig	-reconfig
Do not reconfigure after installation (UNIX, Linux only)	-dnoreconfig	-noreconfig
This package is chainable and will run Qchain.exe (windows) or (UNIX/Linux)	-dc	-c
Suppress the final chained reboot	-dc	-sc
Repair permissions	-dr	-r
Deploy Only	-PLD1	-PLD0
No Pop-up	-PLN1	-PLNP
Debug	-PLDG	-PLDEBUG
Suppress Repair	-dsr	-sr



Table 3.14 Package Flag Descriptions and Behavior

Description (flag behavior)	Display Flag	Select Flag
Force the script to reboot when the installation is done	-1d	-1
Reboot is required	Not Applicable	-2
Reboot may occur	Not Applicable	-3
Reboot is required, and MAY occur	Not Applicable	-4



Note: If you are creating multiple packages requiring custom tags, each package has to be customized with its own set of tags.



Adding Files and Directories to a Package

Files and directories can be added to the package by right-clicking the **Package Content** window, and selecting one of the following options:

- “Adding a Directory to a Package”
- “Creating a Drive for a Package”
- “Adding a New Macro to a Package”
- “Creating a Folder for a Package”
- “Adding a File to a Package”
- “Deleting a File from a Package”
- “Renaming a File within a Package”
- “File Properties for a Package”

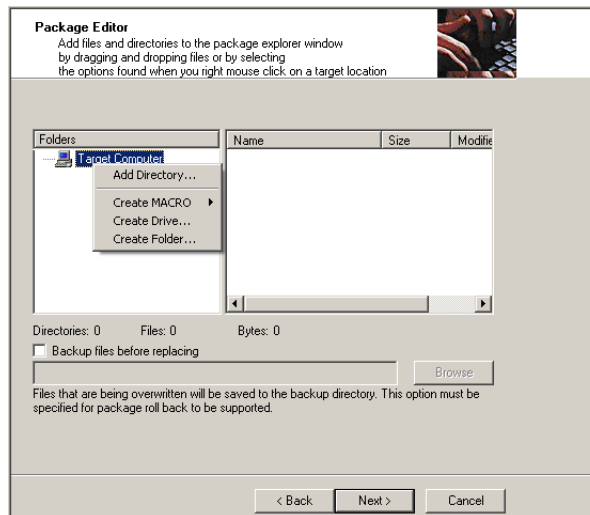


Figure 3.25 Package Content



Adding a Directory to a Package

Once a folder, directory, or macro has been created, a directory can be added. A file system window is opened where you can locate and select an existing directory to add to the Package.

To Add a Directory

1. Right-click the directory, folder, or macro associated with the *Target Computer*.
The *Add* pop-up window opens.
2. Select **Add Directory**.
The *Browse for Folder* window opens.
3. Select the directory to add to the directory, folder, or macro.
4. Click **Open**.
The directory is added to the directory, folder, or macro.
5. Click **Next** to continue with the *Package Editor*.

Adding a New Macro to a Package

Macros access existing system directories. A macro can be either an environment variable, as defined by the operating system, or a macro that only the Agent can expand.

The following pre-defined macros are available under the **New Macro** menu:



Note: Not all macros are available on all Operating Systems. Choose only the macros that are compatible with the operating systems and configurations you are using.

- **%TEMP%** - The operating system temp directory location. Expands to C:\Windows\Temp, C:\Temp, C:\WinNT\Temp, or /tmp depending on operating system and configuration.
- **%WINDIR%** - The operating system windows directory location. %WINDIR% typically expands to C:\Windows.
- **%BOOTDIR%** - The operating system boot directory location. Typically expands to C:\.
- **%ROOTDIR%** - The operating system root directory location. Typically expands to C:\.
- **%PROGRAM FILES%** - The operating system program files location. Typically expands to C:\Program Files.
- **%COMMON FILES%** - The operating system common files location. Typically expands to C:\.

To Create a Macro

1. Right-click inside the *Target Computer* window.
The *Add* pop-up window opens.

2. Select **Create Macro** and the macro required for the package.
The selected macro displays in the *Target Computer* window.

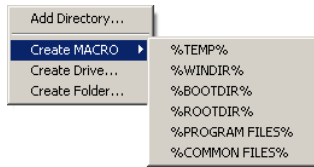


Figure 3.26 Macro Menu

3. Click **Next** to continue with the *Package Editor*.

Creating a Drive for a Package

Use the *New Drive* option to deploy a package to a drive other than the C : \ or %TEMP% drives.

To Create a New Drive

1. Right-click inside the *Target Computer* window.
2. Select **Create Drive** from the pop-up menu.
The *Create Drive* window opens.

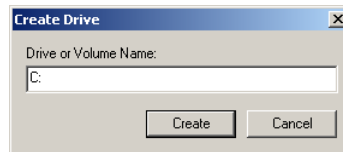


Figure 3.27 Create Drive

3. In the **Drive or Volume Name** field, type the letter you require for the drive name, followed by a colon in X : format.
4. Click **OK**.
The drive is added to the *Target Computer* window.
5. Click **Next** to continue with the *Package Editor*.



Creating a Folder for a Package

The Create Folder window allows for creating a folder within the Package Content directory.

To Create a New Folder

1. Right-click inside the *Target Computer* window.
2. Select **Create Folder**.
The *Create Folder* window opens.

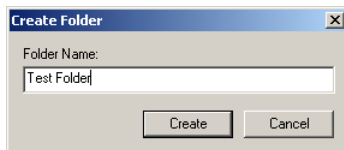


Figure 3.28 Create Folder

3. In the **Folder Name** field, type the name of the new folder.
4. Click **OK**.
The folder is added to the *Target Computer* window.
5. Click **Next** to continue with the *Package Editor*.

Adding a File to a Package

Once a folder, directory, or macro has been created, a file can be added. A file system window is opened where you can locate and select an existing file to add to the Package.

To Add a File

1. Right-click the directory, folder, or macro associated with the *Target Computer*.
The *Add* pop-up window opens.
2. Select **Add File**.
The *Open* window opens.
3. Select the file to add to the directory, folder, or macro.
4. Click **Open**.
The file is added to the directory, folder, or macro.
5. Click **Next** to continue with the *Package Editor*.

Deleting a File from a Package

Deletes the selected directory or file. This option is available only for files added to the *Target Computer* window.

To Delete a Directory or File

1. Right-click the directory, folder, or macro associated with the *Target Computer* that you want to delete.
The *Add* pop-up window opens.
2. Select **Delete**.
The file is deleted from the package.
3. Click **Next** to continue with the *Package Editor*.

Renaming a File within a Package

The Rename option allows for renaming of a previously created drive or macro within the Package.

To Rename a Directory or File

1. In the *Target Computer* directory tree, select the directory where the file is to be renamed
The file is highlighted and the cursor becomes active.
2. Type the new name of the file.
3. Click **OK**.
The folder name is changed and displays in the *Target Computer*.
4. Click **Next** to continue with the *Package Editor*.



File Properties for a Package

Brings up the *properties page* for the selected item. Only available when you right click on a file that has previously been added to the *Target Computer* window.

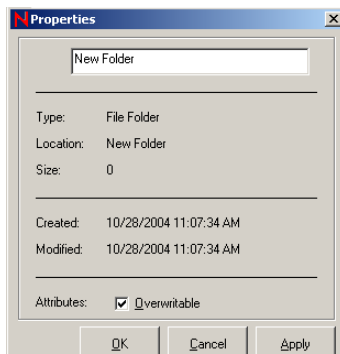


Figure 3.29 Properties

To Change the Overwrite Properties

1. In the *Target Computer* directory tree, select the directory where the file is located.
2. Select the file needed.
3. Right-click the selected file.
4. Select **Properties**.
The *Properties* window opens.
5. In the **Attribute** field, select or deselect the **Overwritable** checkbox.



Warning: Removing the check-mark from the **Overwritable** attribute will prevent subsequent patches that contain the same file from overwriting that file.

6. Click **Apply**.
The folder properties are changed.

Creating Scripts for a Package

There are three types of scripts. These scripts can be written in *Microsoft Visual Basic Script* or *Microsoft Jscript*. Documentation regarding these languages can be found at the Microsoft scripting web site: <http://msdn.microsoft.com/scripting>.

The following scripts are listed by the order in which they execute within the package:

1. **Pre-Script** - Used to test for a machine condition or shutdown a service. For example you can stop the package rollout in the pre-script by using the `SetReturnCode` in the `PLCCAgent` script object.
2. **Command Line Script** - Used to launch executables. The format is the same as a standard `.CMD` or `.BAT` file.
3. **Post-Script** - Used for any clean-up operations such as the deletion of files, starting services, or running an installed file.

A software package can have a maximum of one of each type of script. When all three scripts are present, they will be executed in the order listed above.



Note: Unless the **Execution Directory** option is selected and a valid directory is defined, all scripts run in the **ROOT** directory.

To Use the Script Editor

1. Select the type of script to execute from the **Type of Script** drop-down list.
2. Select the scripting type from the **Script Language** drop-down list.
3. Click **Edit**.
This *Script Editor* window opens.
4. Type or copy the script to be added in the Script field.
5. Click **Run**.
The script is checked and the *Errors* box displays **Success** when the script is validated.
6. Click **OK**.
The Script Editor window closes and returns to the *Package Editor* wizard.
7. If needed, select **Script Execution Directory** if a different directory location is required.
The *Script Execution Directory* field becomes active.
8. Type the backup directory path, or click **Browse**.
The location displays in the *Script Execution Directory* field.
9. Click **Next** to continue with the *Package Editor*.





4 Working With Deployments

A *Deployment* initiates the downloading of a patch by the agent to a device for installation. It is the instruction set for a package that supplies the agent the rules and conditions for deployment.

A deployment comprises all the necessary information, files, and scripts required to perform the task(s) associated with the vulnerability, whether installing a patch executable, stopping a service, validating a system condition, changing a database entry, etc. The Deployment is the mechanism that carries and supports a package.

In this Chapter

- “About Deployments”
- “Using the Deployment Pages”
- “Working with Deployments”
- “Using the Deployment Wizard”

About Deployments

As the mechanism of defining the operation of a deployment, several key concepts and status indicators are associated with a deployment. These definitions are used to define deployment behavior.

The following sections include some of the key concepts and indicators that give definition to a deployment.

- “Explaining Deployment Distribution Order” - the order that the deployment is submitted to target devices.
- “Deployment Types” - deployments can be based on vulnerabilities, packages, or a mandatory baseline.
- “Standard and Chained Deployments” - deployments are processed as either standard or chained.

Viewing Deployments

Deployments can be viewed in the following pages:

- Deployments
- Devices
- Vulnerabilities and Packages
- Groups



To View all Deployments

- 1. Select the **Deployments** tab.
The *Manage Deployments* window opens and displays all current deployments.

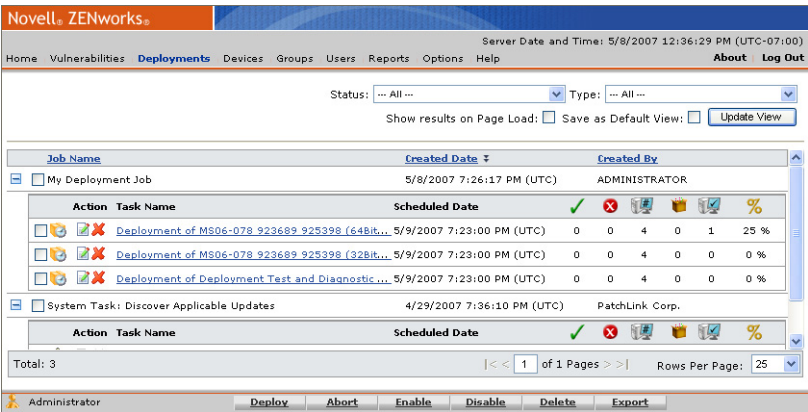


Figure 4.1 Deployments page

- 2. Click **Expand (+)** to view the Deployment details.

To View Deployments within Devices

- 1. Select the **Devices** tab, select your filter options, and click **Update View**.
The applicable devices display in the *Devices* window.
- 2. Select a device with at least one deployment to view its details.
The *Details by Device* screen opens.
- 3. Select the *Deployments* tab.
The *Deployments by Device* screen opens.

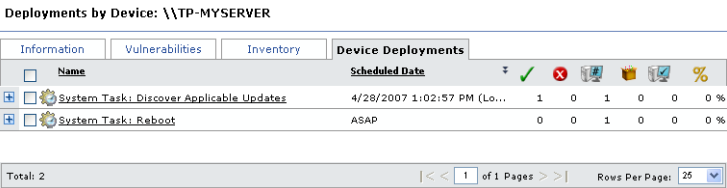


Figure 4.2 Deployments by Device



4. Select the desired deployment, and click the **plus sign (+)**.
The deployment details display.

Deployments by Device: \\TIP-MYSERVER

Information		Vulnerabilities	Inventory	Device Deployments
Name	Scheduled Date			
System Task: Discover Applicable Updates	4/26/2007 1:02:57 PM (Lo...	1	0	1
System Task: Reboot	ASAP	0	0	1

Task Name: System Task: Reboot
 Type: Deployment of a package
 Status: Enabled
 Deploy Manner: Distribute to 5 at a time, first come first serve.
 Schedule Type: One time deployment
 Start Date: ASAP

Created By: PatchLink Corp.
 Created On: 4/26/2007 11:53:11 AM (UTC-07:00)
 Last Modified By: ADMINISTRATOR
 Last Modified On: 4/26/2007 2:33:55 PM (UTC-07:00)

Deployment Notes: This is a system-wide deployment task that will reboot the Agents.

Total: 2 | << 1 of 1 Pages >> | Rows Per Page: 25

Figure 4.3 Deployment by Device expanded

To View Deployments within Groups

The Groups page displays deployments a selected group has been assigned. This view is the same as the Deployment Summary view, but displays only deployments for the selected group.

1. In the *Device Groups* page, select **Deployments** from the drop-down list.
The *Deployments* screen displays in the Groups window.
2. Select a **Group** from the directory tree.
The selected *Group* is highlighted and displays the assigned Deployments.

Novell ZENworks

Server Date and Time: 5/8/2007 12:21:00 PM (UTC-07:00)

Home Vulnerabilities Deployments Devices **Groups** Users Reports Options Help [About](#) [Log Out](#)

Group Browser: All > Custom Groups > Parent Group > Child Group View: Deployments

Name	Scheduled Date							
Deployment of MS06-078 923689...	5/9/2007 7:23:0...	0	0	4	0	1	25 %	
Deployment of MS06-078 923689...	5/9/2007 7:23:0...	0	0	4	0	0	0 %	
Deployment of Deployment Test ...	5/9/2007 7:23:0...	0	0	4	0	0	0 %	

Total: 3 | << 1 of 1 Pages >> | Rows Per Page: 25

Administrator

Abort Enable Disable Delete Deploy Export

Figure 4.4 Group Deployments



Deployment Types

Deployments are created through the *Vulnerabilities, Packages, Devices, Deployments, or Groups* pages. On each page, the **Deploy** command is presented in the *Action* menu. A different deployment type, *Mandatory Baseline*, is created by establishing a mandatory baseline for a device group. See “[Mandatory Baseline](#)” for more information on the mandatory baseline feature.

Vulnerability-based Deployments

A vulnerability contains multiple associated packages and the target packages to be deployed. As a device goes through the DAU process, it is assigned vulnerabilities to scan as the Patch Management Server determines they are applicable to the device. Based on these results, an Patch Management Server user can determine which devices should receive the patch (vulnerability fix). Behind the scenes, Patch Management Server goes through and makes sure that the devices are assigned the correct package.

Package-based Deployments

A package contains all vendor-supplied updates and executable code used to correct or patch security issues for the target devices. The majority of packages are part of specific vulnerabilities, and are deployed to multiple devices within the network. See “[About Packages](#)” for more information.

Mandatory Baseline Deployments

The *Mandatory Baseline* defines a standard level of vulnerabilities or locally-created packages that must be installed to a group membership. The mandatory baseline comprises the base set of patches and other packages required for the target device. In terms of vulnerabilities, a mandatory baseline enforces continuous checking to verify and validate that the patch identified by the baseline is installed. If the correct patch is not installed, the patch is deployed and installed.

Standard and Chained Deployments

Standard Deployments

A *standard deployment* is a deployment that has not been chained with another deployment. While not all standard deployments require a reboot, if the included package does require one and the reboot is suppressed; the computer will not accept additional deployments until it is rebooted.

Chained Deployments

A *chained deployment* is a deployment grouped with other deployments so the computer will not reboot after each one. Following the first chained deployment, the computer will accept only chained deployments until rebooted.



Reboot and Chained State

The reboot and chained states are the result of a device not performing the required reboot following a deployment.

Table 4.1 Reboot and Chained State Definitions

State	Description
Reboot State	Indicates that the device received a standard deployment requiring a reboot, yet the reboot was suppressed. While in this state, the agent will only accept one of the reboot deployments. A reboot deployment or a manual reboot will clear this state.
Chained State	Indicates that the agent received a chained deployment in which the reboot was suppressed. While in the chained state, the agent will only accept another chained deployment or a reboot deployment.

There are two deployments which will always perform a reboot:

Table 4.2 Types of Reboot Deployments

Deployment	Description
Reboot System Package	A system task that is automatically added to the end of chained deployments where the final reboot is not suppressed. Also sent to agents when you click the Reboot Now button, on the Devices page.
Task - System Reboot	A task which permits the user to schedule a reboot using the scheduling features of the Schedule Deployment Wizard .



Note: Standard packages reboot for one of three reasons:

- The deployed package required and forced the reboot (unless suppressed), during the installation.
- The package installer determined that it required a reboot.
- The reboot flag was sent to the agent. It is not necessary that the agent receive the Reboot System Package or Task, the agent will perform the reboot on its own.



Using the Deployment Pages

All scheduled deployments can be viewed by selecting the Deployments tab. The main page displays each Deployment Job and the individual deployments assigned to it. With a Deployment Job, you can schedule multiple deployments with separate instructions. With Deployment Jobs, you are able to edit and delete individual deployments without having to delete the entire deployment job.

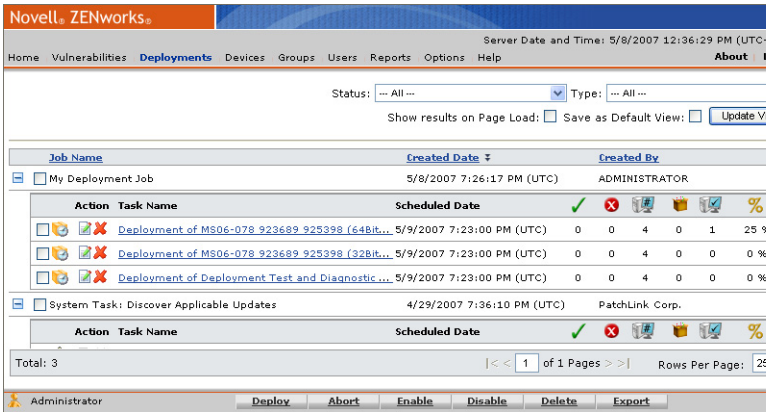


Figure 4.5 Deployments Page

The following table describes the key columns of the main Deployments page.


Table 4.3 Deployments Page Column Descriptions

Column	Description
Job Name	The name of the main unit containing a group of deployments.
Created Date	The date the initial deployment job was created.
Created by	The user who created the package.
Action	Allows you to <i>Edit</i> or <i>Delete</i> a deployment.
Task Name	The name of the deployment task. Typically, the name of the Vulnerability or Task deployed.
Scheduled Date	The date the deployment was scheduled to occur.
Deployment Statistics	Refer to “Deployment Statistics” for details regarding the Deployment Statistics icons.



Deployments also can be viewed based on an association to a specific package, or by association to a group or individual device.

Deployments by Device: \\TP-MYSERVER

Information	Vulnerabilities	Inventory	Device Deployments
Name	Scheduled Date		
 System Task: Discover Applicable Updates	4/28/2007 1:02:57 PM (Lo...	1 0 1 0 0 0 %	
 System Task: Reboot	ASAP	0 0 1 0 0 0 %	

Total: 2 | << 1 of 1 Pages >> | Rows Per Page: 25

Figure 4.6 Device Deployments page

See “[Deployment Status and Type](#)”, for information on the fields for individual deployments.

Deployment Status and Type

The deployment status is indicated by an icon in the status column. The icons vary dependent upon the deployment type and status. The deployment types are classified in the following table.

Table 4.4 Deployment Status Options

Status	Description
New	Downloaded from the Global Subscription Server since the last session.
Current	Present vulnerabilities residing on ZENworks Patch Management Server.
Local	Locally created package.
System Task	A deployment that contains a system task package.
Mandatory Baseline	A deployment is created through the mandatory baseline for a group. This deployment is automatically created and managed through the mandatory baseline process

The following table defines the Package Deployment icons:

Table 4.5 Package Deployment Icons































New	Current	Local	System Task	Mandatory Baseline	Definition
					Deployment currently has no assigned devices or device groups.
					In Progress - The device or device group has started the deployment.



Table 4.5 Package Deployment Icons

New	Current	Local	System Task	Mandatory Baseline	Definition
					Not Started - The device or device group has not started the deployment. This could be for any of the following reasons: <ul style="list-style-type: none">• The deployment start time has not elapsed.• The computer has not contacted Patch Management Server since the start of the deployment.• The deployment limit (or global deployment limit) was met the last time the computer contacted Patch Management Server. It will try again during its next communication.
					Completed - All devices or device groups have successfully completed the deployment.
					Completed with Errors - At least one device or device group failed to successfully complete the deployment.
					Disabled - The deployment has been disabled.



Deployment Statistics

The right-hand side of the deployment entry contains columns which illustrate the current result statistics for the deployment by package.

Statistics show the relationship between a specific deployment and the total number of devices (or groups) within Patch Management Server that meet a specific status.









Note: If the mandatory baseline fails to deploy more than twice, ZENworks Patch Management will record it as an error in the status column. However, this notification will only show in the Mandatory Baseline tab.



The following table defines the status icons:

Table 4.6 Column Icon Definitions

Icon	Definition
	Total number of devices or groups that finished the deployment successfully.
	Total number of devices or groups that finished the deployment unsuccessfully.
	Total number of devices or groups that are assigned the deployment.
	Total number of devices or groups that are in the process of executing the deployment.
	Total number of devices or groups that finished the deployment.
	Percentage of the devices or groups that finished the deployment. = [Total Finished devices / Total Assigned devices]



Note: All group deployments will initially show only the number of groups included within that deployment. The total number of devices assigned the deployment will equal the number of groups plus the number of devices included within those groups (as of the time of deployment). However, when the total is calculated is based upon the deployment schedule:

- **Group deployments that are scheduled for an immediate deployment** will calculate and add the number of devices, included within the assigned groups, within 5 minutes of scheduling.
- **Group deployments that are scheduled for a future deployment** will calculate and add the number of devices, included within the assigned groups, within 5 minutes prior to the deployment start time. If the deployment was scheduled to deploy based upon the UTC time, this will add all of the devices at once. However, if the deployment was scheduled to deploy based upon the agent’s local time, the devices will not be added until 5 minutes prior to their local time.



Deployment Details Summary

Expanding (by clicking the plus '+' icon) a deployment will display the deployment details as described in the following table.

Table 4.7 Deployment Details Summary Fields

Field	Description
Deployment Name	The name of the deployment as assigned, by the user, when created.
Type	The type of deployment. Options include: <i>Deployment of a package</i> or <i>Standard deployment</i> .
Status	Whether the deployment is <i>Enabled</i> , <i>Disabled</i> , or <i>Completed</i> .
Deploy Manner	The manner in which this deployment occurred. Options include: <i>Sequential</i> , <i>Parallel</i> , or <i>Distribute to # of devices at a time</i> .
Schedule Type	The frequency of the deployment. Options include: <i>Recurring</i> , or <i>One time</i> .
Start Date	The date and time this deployment was started.
Deployment Notes	Additional information about the deployment.
Created By	The user who created this deployment.
Created On	The date and time this deployment was created.
Last Modified By	The user who last modified this deployment.
Last Modified On	The date and time this deployment was last modified.
End Date	The date and time the deployment was completed.



- “Deployments Page”
- “Viewing Deployment Results”
- “Explaining Deployment Distribution Order”
- “Aborting Deployments”
- “Disabling Deployments”
- “Enabling Deployments”
- “Modifying Deployments”
- “Deleting Deployments”

Deployments Page Functions

Table 4.8 Deployments Tab - Page Functions

Menu Item	Function
Deploy	Re-deploys the selected packages. For additional information refer to "Using the Deployment Wizard" .
Abort	Cancels the deployment for any devices which have not already received the deployment package. For additional information refer to "Aborting Deployments" .
Enable	Enables the selected disabled deployment. For additional information refer to "Enabling Deployments" .
Disable	Disables the selected enabled deployment. For additional information refer to "Disabling Deployments" .
Delete	Removes the deployment from your ZENworks Patch Management Server. For additional information refer to "Deleting Deployments" .
Export	The Export button allows you to export subscription data to a comma separated value (.CSV) file.

Viewing the Deployment Details

To open the *Deployment Details* page, click the deployment name link within any *Deployments* view. This page illustrates the overall information about this particular deployment. Including the assigned devices and groups and the status of the deployment for each.

Deployment Details: System Task: Discover Applicable Updates						Auto Refresh: <input type="checkbox"/>
Devices and Groups Scheduled 9/1/2001 12:00:00 AM (Local)						
<input type="checkbox"/>	Name	2 Status	Last Run Status	Last Run Start Date	Last Run Completed Date	Next Run Date
<input type="checkbox"/>	UFD-MYSERVER	Completed	Success	4/18/2007 2:16:17 AM (Local)	4/18/2007 2:18:30 AM (Local)	
<input type="checkbox"/>	UFD-MYSERVER	Not Running				4/19/2007 4:18:30 A...
Total: 2						
<div> < < 1 of 1 Pages > > Rows Per Page: 25 </div>						

Figure 4.8 Deployment Details



Table 4.9 Deployment Details Column Definitions

Column	Description
Device Status icon	The status of the device or device group.
Name	Displays the name of the device or device group. The device group name is a link, and clicking the link will display the group membership and individual device results.
Status	The deployments current status.
Last Run Status	The deployments status when last ran. The status is a link, and clicking the link will display the Deployment Results page.
Last Run Start Date	The Date/Time the deployment began.
Last Run Complete Date	The Date/Time the deployment completed.
Next Run Date	The next scheduled start Date/Time for this deployment.



Deployment Details - Page Functions

Table 4.10 Deployment Details Tab - Page Functions

Button	Function
Enable	Enables the selected disabled deployment assignments. For additional information refer to "Enabling Deployments" .
Disable	Disables the selected enabled deployment assignments. For additional information refer to "Disabling Deployments" .
Export	The Export button allows you to export subscription data to a comma separated value (.CSV) file.

Viewing Deployment Details by Device

Another view of deployments is available through the *Devices* page. You can view deployments for devices by clicking the device name on the Devices page, or selecting the Deployments tab.

Deployments by Device: \\TP-MYSERVER

Information	Vulnerabilities	Inventory	Device Deployments
<div> <input type="checkbox"/> Name <div>Scheduled Date</div> </div>			
<div> <input checked="" type="checkbox"/> System Task: Discover Applicable Updates <div>4/28/2007 1:02:57 PM (Lo...</div> <div>1 0 1 0 0 0 %</div> </div>			
<div> <input checked="" type="checkbox"/> System Task: Reboot <div>ASAP</div> <div>0 0 1 0 0 0 %</div> </div>			
<div> Total: 2 <div>< 1 of 1 Pages ></div> Rows Per Page: 25 </div>			

Figure 4.9 Deployments Page - Devices

Device Deployments - Page Functions

Table 4.11 Device Deployments Tab - Page Functions

Menu Item	Function
Edit	Launches the deployment wizard allowing you to make modifications to the deployment. For additional information refer to "Modifying Deployments" .
Export	The Export button allows you to export subscription data to a comma separated value (.CSV) file.



Viewing Deployment Details by Device Group

Another view of deployments is available through the *Groups* page. This view displays the deployments that the selected group has been assigned. This view is the same as the Deployment Summary view, but displays only deployments for the selected group.

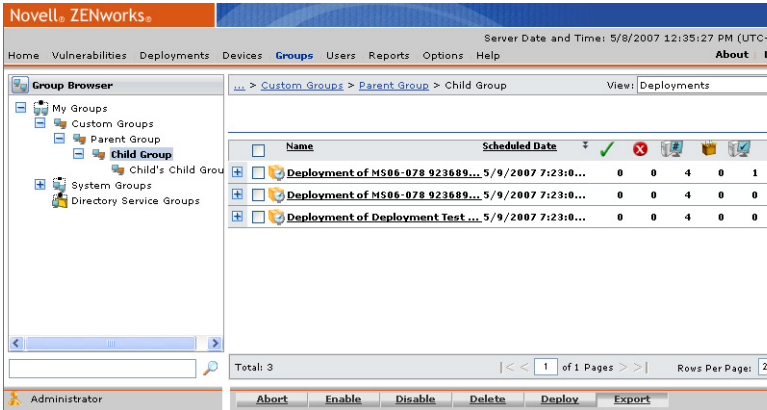


Figure 4.10 Deployments Page - Groups



Group Deployments Tab - Page Functions**Table 4.12** Group Deployments Tab - Page Functions

Button	Function
Abort	Cancels the deployment for any devices which have not already received the deployment package. For additional information refer to "Aborting Deployments" .
Enable	Enables the selected disabled deployment. For additional information refer to "Enabling Deployments" .
Disable	Disables the selected enabled deployment. For additional information refer to "Disabling Deployments" .
Delete	Removes the deployment from your ZENworks Patch Management Server. For additional information refer to "Deleting Deployments" .
Deploy	Re-deploys the selected packages. For additional information refer to "Using the Deployment Wizard" .
Export	The Export button allows you to export subscription data to a comma separated value (.CSV) file.



Viewing Deployment Results

Once the deployment has been performed, the specific results of the deployment for that device can be displayed by clicking on the status text (of the Last Run Status column).

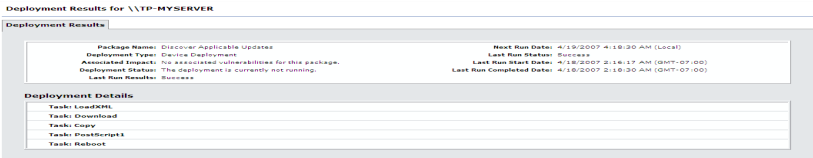


Figure 4.11 Deployment Results

The fields displayed on the *Deployment Results* tab are defined as follows:

Table 4.13 Field Descriptions

Field	Description
Package Name	Displays the name of the package that was deployed.
Deployment Type	Displays the deployment type.
Associated Impact	Displays the impact of the associated vulnerability, if the package is associated to one.
Deployment Status	Displays the overall deployment status information.
Last Run Results	Displays the results of the last time the device performed the deployment.
Next Run Date	Displays the date when the device is to perform the deployment again, if the deployment is recurring.
Last Run Status	Displays the status of the last time the device performed the deployment.
Last Run Start Date	Displays the date when the device last started the deployment.
Last Run Completed Date	Displays the date when the device last finished the deployment.



Explaining Deployment Distribution Order

When deploying more than one package to an individual device or group of devices, the deployments can be scheduled to process at different times.



Note: Each device managed by ZENworks Patch Management requires an agent. A deployment is associated to the agent installed on a particular device.

Order is also influenced by deployment type, status, and reboot requirements. Deployments proceed in the following order *prior* to regularly schedule system tasks and agent processes:

1. Chained deployments
2. Standard deployments
3. System Task: Reboot
4. Task – Reboot System
5. Discover Applicable Updates (DAU)

Although no deployment occurs before its scheduled time, a chained deployment whose time has elapsed will always precede a standard deployment whose time has also elapsed.

If multiple chained deployments are scheduled and some devices have the final reboot suppressed, while others do not, the determination of a reboot override is based on the last scheduled deployment.

Aborting Deployments

Aborting a deployment will cancel the deployment for any devices which have not already received the deployment.



Warning: The devices that have already received the deployment will not be affected, only the devices which have not yet received the deployment will have the deployment aborted.

To Abort a Deployment

1. Select the deployment you wish to Abort.
2. Click **Abort** (at the bottom of the page).
This will cancel the selected deployment.



Note: You cannot abort system task or mandatory baseline deployments.



Disabling Deployments

Disabling a deployment will pause the deployment and stop the distribution of the package(s) to devices when they have not already received a deployment.

To Disable a Deployment

1. Select the deployment you need to disable.



Note: You cannot disable deployments of System Task Packages.

2. Click **Disable**.
The selected deployment is disabled.

Enabling Deployments

Enabling a deployment will allow a disabled (or paused) deployment to continue. Scheduling the device (or device group) deployments as scheduled.

To Enable a Disabled Deployment

1. Select the disabled deployment you need to enable.
2. Click **Enable**.
The selected deployment is enabled.

Modifying Deployments

Modifying a deployment will launch the Deployment Wizard, allowing you to make modifications as needed.



Note: System Task Packages are automatically assigned to devices, so removing a device from a deployment of a System Task Package will have no effect (the device will be re-assigned to the deployment by the ZENworks Patch Management Server).

To Modify a Deployment

1. Select the deployment you need to modify.
2. Click **Edit**.
The *Deployment Wizard* opens, see “[Using the Deployment Wizard](#)” for additional information.

Deleting Deployments

Deleting a deployment will remove the deployment from your ZENworks Patch Management Server.



Note: Deleting a deployment will have no effect on devices that have already received the deployment. You cannot delete System Task deployments.

To Delete a Deployment

1. Select the *disabled* deployment you wish to delete.
2. Click **Delete**.

Explaining Deployment Deadlines

Deadlines allow you to define when a deployment or reboot should occur. A deadline can either be calculated based upon the agents Group Policy or defined by you as a specific date and time. When using deadlines you define the deadline date and time, the starting date and time and your users may snooze the deployment (or reboot), as many times as desired, up to the defined deadline.



Using the Deployment Wizard

The Deployment Wizard provides an interface to create or edit deployment schedules for multiple recipients and multiple packages. The wizard assists in device selection, scheduling the deployment, and if needed, setting recurrences.

The following table describes the scenarios for a deployment. These options are selected prior to starting the Deployment Wizard.

Table 4.14 Deployment Actions

Deployment Selection	Result
Device	The Deployment Wizard will deploy only to the selected device.
Vulnerability	The Deployment Wizard selects all the devices and packages required for this vulnerability.
Package	The Deployment Wizard will deploy the package to the selected groups or devices.
Group	The Deployment Wizard will deploy the applicable packages to the selected group members.

To use the wizard; click **Deploy** from either the *Vulnerabilities*, *Packages*, *Devices*, or *Group Deployments* page.



Note: If you have a large number of disabled devices, to deploy to only the enabled devices, filter by status and manually select the devices to which you need to deploy.



Introduction Page

The *Introduction* page of the **Deployment Wizard** describes the purpose and capabilities of the wizard.

This page can be hidden during future deployments by selecting the **Do not display this page in the future** checkbox.

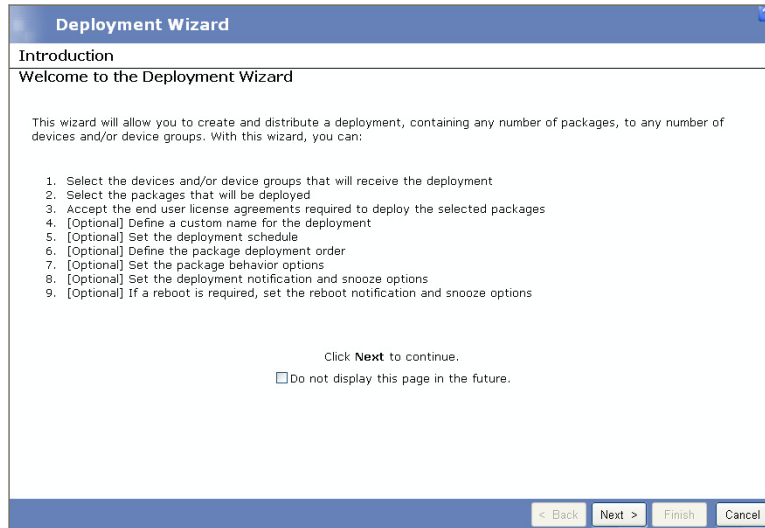


Figure 4.12 Deployment Wizard - Introduction Page

Click **Next** to proceed to the *Computers/Groups Selection* page.



Device/Device Groups Selection Page

The *Available Devices/Groups* page of the **Deployment Wizard** allows for selecting devices and groups to receive a deployment.

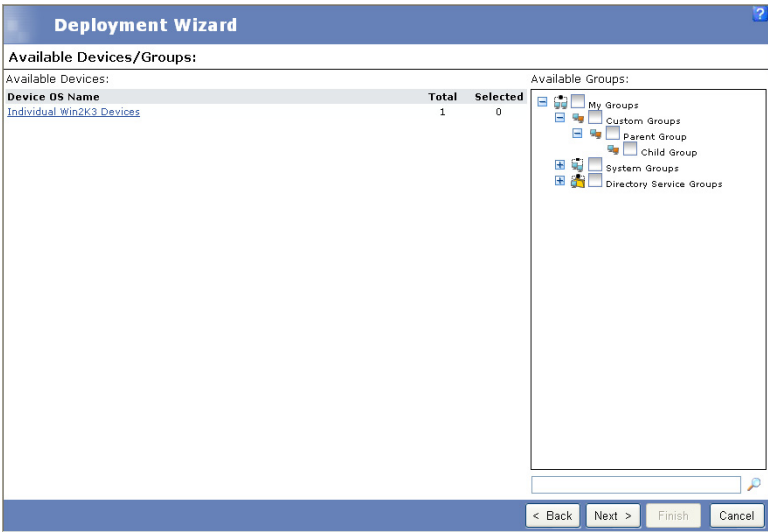


Figure 4.13 Deployment Wizard - Available Devices/Groups Selection Page

When first opened, this page displays the devices grouped by operating system, and the groups in a directory tree format by user groups, system groups, or directory service groups.

To Create a Device Deployment

- 1. From the **Available Devices** list, select the **Device OS Name** required.
The list of devices within that OS display.
- 2. Select the **Device** from the list.
The device(s) are highlighted.
- 3. Click **Next**.
The *Package Selection* window opens.

To Create a Group Deployment

- 1. From the **Available Groups** directory tree, select the group or groups requiring the deployment.



The Available Groups directory tree allows for selecting single groups, multiple groups, and group hierarchies (groups cascading down from a parent). This method enables you to select multiple groups for a deployment at the same time without having to create individual deployments for each individual group. When selecting a group from the Available Groups directory tree, the following will occur:

- When a parent group is first selected, all children groups will also be selected and the group selection is represented by a green checkmark.
- If any of the children groups are deselected, the green checkmark will change to a green square. Thus indicating that while the parent group is selected, the entire child hierarchy is not.

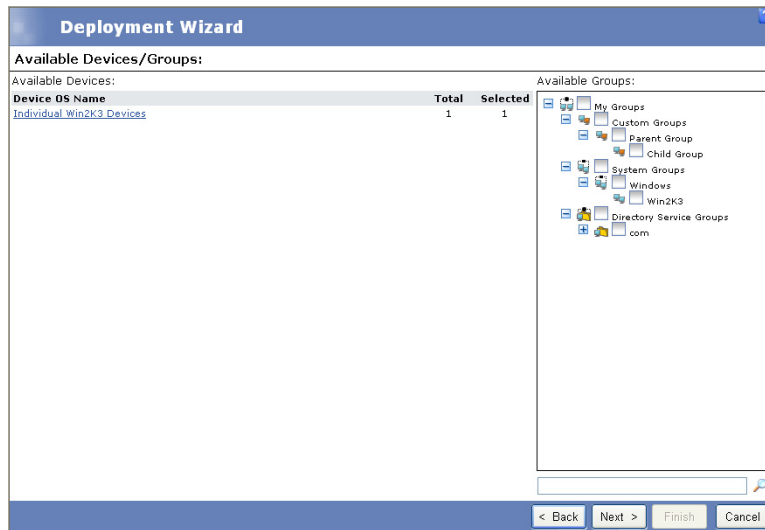


Figure 4.14 Deployment Wizard - Device/Device Groups Selection Page

2. Click **Next**.
The *Package Selection* window opens.



Package Selection Page

The *Packages Selection* page of the **Deployment Wizard** allows you to select the packages to be deployed. This page displays the packages, grouped by manufacturer, that apply to the devices selected on the *Devices/Device Groups Selection* page.

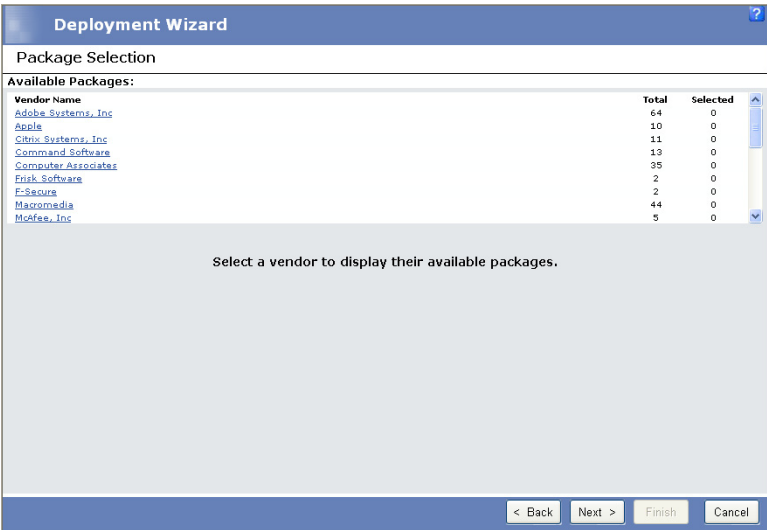


Figure 4.15 Deployment Wizard - Packages Selection Page



To Select a Package

1. Select the **Vendor** required for the deployment.
The list of associated packages displays in the Selected Packages window.

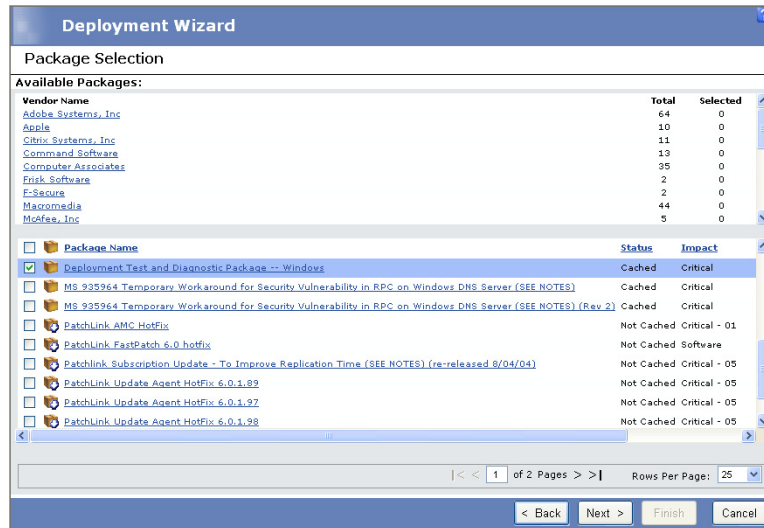


Figure 4.16 Deployment Wizard - Packages Selection Page

2. Select the packages needed. Click the **arrows** to page through the available packages, if needed.
The package is selected and highlighted.



Tip: Checking the **Package Name Box** selects all of the packages available in the list.

3. Click the **Package Name** link to open the *Associated Vulnerability Analysis* page.
4. Click **Next** to proceed to the *Licenses* page.



Note: When using the *Deployment Wizard*, the wizard will not necessarily install Service Packs first. Therefore, it is recommended that you install all relevant Service Packs prior to creating deployments through the *Deployment Wizard*.



Associated Vulnerability Analysis

The *Associated Vulnerability Analysis* page of the Deployment Wizard allows you to view the devices associated with this package and whether their status is *Patched*, *Not-Patched* or *Not-Applicable* in relation to the selected package.

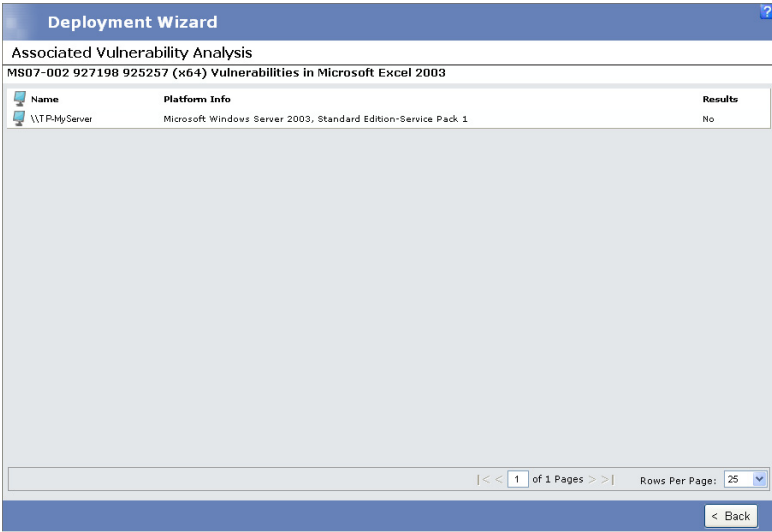


Figure 4.17 Deployment Wizard - Associated Vulnerability Analysis Page

The **Results** column of the resulting grid, will display either *Patched*, *Not-Patched* or *N/A* dependent upon the devices patch status.

Click **Back** to return to the *Packages Selection* Page.



Licenses Page

The *Licenses* page of the Deployment Wizard displays the end user license agreements associated with the vendor packages. Any license agreements displayed on the page must be agreed to prior to continuing the deployment.

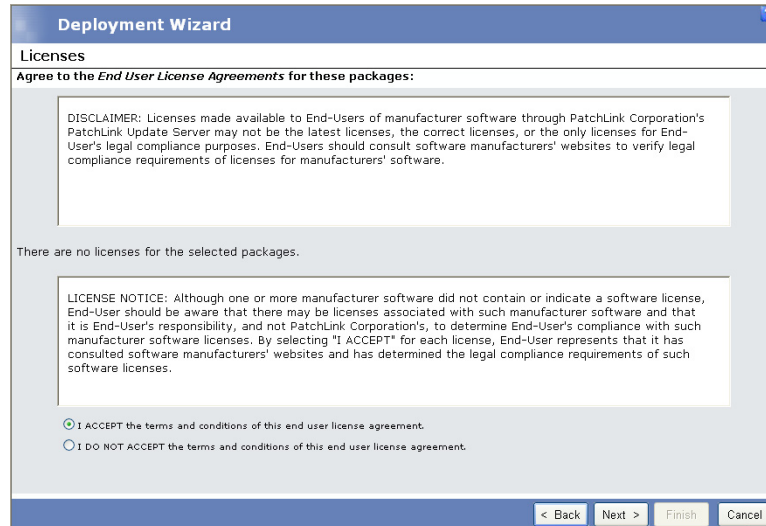


Figure 4.18 Deployment Wizard - Licenses Page

To Review and Accept the License Agreement

1. Review the agreement.
2. If you accept the agreement, select the **I ACCEPT the terms and conditions of this end user license agreement** option.
3. If there are multiple agreements, repeat steps 1-2. All agreements must be accepted before the deployment wizard can be continued.
4. Click **Next** to proceed to the *Deployment Options* page.



Deployment Options Page

The *Deployment Options* page of the Deployment Wizard, allows you to set the deployment **Job Name**, **Start Time**, **Manner**, and add any **Notes**.

Deployment Wizard

Deployment Options

Select the options for this deployment:

Job Name:

My Deployment Job

Start Time:

Local Time: 4/30/2007 11:16:03 AM
UTC Time: 4/30/2007 6:16:03 PM

Change

Deployment time zone:

☐ Agent Local Time (Deploy at local time for each individual node)

☒ Agent UTC Time (Deploy at UTC time for each individual node)

Manners:

☒ Concurrent Deploy to 500 devices at a time.

☐ Consecutive Deploy to all devices on a first come first serve basis.

☐ Suspend the deployment of this package, if it fails to deploy to one or more devices.

☐ Deploy package even if the device has been previously patched.

Notes:

Created by administrator on 4/30/2007 6:16:03 PM (UTC)

< Back

Next >

Finish

Cancel

Figure 4.19 Deployment Wizard - Deployment Options Page

Table 4.15 Deployment Options Fields

Field	Description
Job Name	The display name of the deployment job. (Note: This field must not be blank.)
Task Name	The editable display name of the deployment task. The {Package Name} variable will be replaced with the name of the Package included in the task.
Start Time	Displays the Local and UTC times the deployment is scheduled for. Click Change to open the <i>Schedule Configuration</i> page and modify time options. Deployment Time Zone <ul style="list-style-type: none">• Agent Local Time - Select to deploy based upon the local time of each device.• Agent UTC Time - Select to deploy based upon UTC (Coordinated Universal Time). When UTC is used, the deployment will be scheduled for all devices at the same time, regardless of time zone differences.



Table 4.15 Deployment Options Fields

Field	Description
Manner	<ul style="list-style-type: none"> • Concurrent - Simultaneous distribution to a specified number of devices. New deployments are distributed as agents report back as having completed the previous deployment. If a computer takes longer than four hours to complete the deployment, it is no longer counted against the Concurrent Deployment Limit. • Consecutive - Creates and distributes all deployments simultaneously. The global deployment limit will always take precedence over the defined distribution options defined. • Suspend the deployment of this package, if it fails to deploy to one or more devices - Suspends all subsequent deployments following any deployment failure. • Deploy package even if the device has been previously patched - deploys the package to all selected computers regardless of patch status.
Notes	Allows for any notes or comments.



Note: When deploying to an agent at its UTC time, if the agent's time zone is **before** the server's time zone, the local time of the **server** will be read, resulting in a possible later deployment to that agent.

Note: When using UTC, the time when the agent retrieves the deployment is dependent upon the agent's DAU Communication Interval. If the time zone of the server is before the UTC time, the deployment may be delayed until the server gets to the deployment time.

Click **Next** to proceed to the *Package Deployment Order and Behavior* page.



Schedule Configuration Page

The *Schedule Configuration* page of the Deployment Wizard, allows you to define whether a deployment is one-time or recurring, and the appropriate options for each.

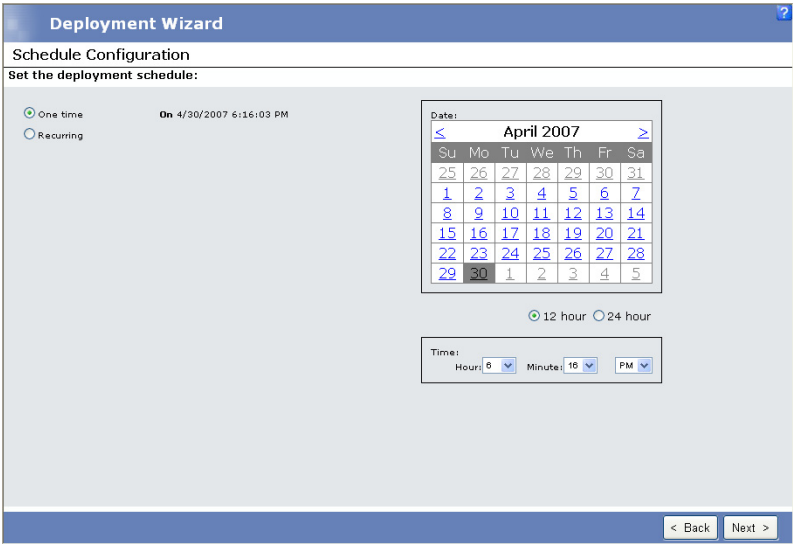


Figure 4.20 Deployment Wizard - Schedule Configuration Page

To Schedule a One Time Deployment

1. To navigate to the Deployment Wizard **Schedule Configuration** page, from the Deployment Wizard **Deployment Options** page (see previous Figure), click the **Change** button located in the *Start Time* option.
2. Select **One Time**.
The deployment will start on the selected day at the defined time. If a one time deployment is scheduled for a date and time in the past, the agents will start the deployment the next time they contact the ZENworks Patch Management Server.
3. Select **12 hour** or **24 hour** to determine 12 hour format or military 24 hour format.
4. Select the **Hour** needed using the drop-down list.
5. Select the **Minute** between 00 and 59, using the drop-down list.
6. Select **AM** or **PM** using the drop-down list.
7. Click **Next**.
The changes are saved and the *Deployment Options* screen opens.



To Schedule a Recurring Deployment

A recurring schedule will start deployments on the selected day at the selected time and repeat the deployment every day, week, or month and if defined, end on a specific date.

Deployment Wizard

Schedule Configuration

Set the deployment schedule:

☐ One time
☒ Recurring

Occurs:

☒ Daily
☐ Weekly
☐ Monthly

Daily:

Every day(s)

Daily Frequency:

☒ Occurs once a day at the scheduled start time.
☐ Occurs every: Minute(s)

Duration:

☒ 12 hour ☐ 24 hour

Start Date: End Date: ☒ No End Date

April 2007							April 2007						
Su	Mo	Tu	We	Th	Fr	Sa	Su	Mo	Tu	We	Th	Fr	Sa
25	26	27	28	29	30	31	1	2	3	4	5	6	7
1	2	3	4	5	6	7	8	9	10	11	12	13	14
15	16	17	18	19	20	21	15	16	17	18	19	20	21
22	23	24	25	26	27	28	22	23	24	25	26	27	28
29	30	1	2	3	4	5	29	30	1	2	3	4	5

Time: Hour: Minute: PM

Time: Hour: Minute: PM

< Back Next >

Figure 4.21 Deployment Wizard - Schedule Configuration Page

To Set Up a Daily Recurring Deployment

1. Select **Recurring**.
The *Recurring Deployment* window opens.
2. In the *Occurs* field, select **Daily**
The Deployment Wizard displays the *Daily Deployment Options* field.

Occurs:

☒ Daily
☐ Weekly
☐ Monthly

Daily:

Every day(s)

Figure 4.22 Daily Option

3. From the **Every X Days** drop down list, select the frequency. The valid options are: 1 through 365.
4. Select the frequency of the deployment.



- **Occurs once a day at the scheduled start time** - the deployment starts at the same time as scheduled in the X screen
 - **Occurs every** - the valid options are 1 through 60 if minutes are selected and 1 through 24 if hours are selected.
5. Continue to “**Selecting the Deployment Start and End Functions**”.

To Set Up a Weekly Recurring Deployment

1. Select **Recurring**.
The *Recurring Deployment* window opens.
2. In the *Occurs* field, select **Weekly**.
The Deployment Wizard displays the *Weekly Deployment Options* field.

Occurs:
☐ Daily
☒ Weekly
☐ Monthly

Weekly:
Every 1 week(s) on:
☐ Mon ☐ Tue ☐ Wed ☐ Thur ☐ Fri ☐ Sat ☒ Sun

Figure 4.23 Weekly Options

3. From the **Every X week(s) on: Mon, Tue, Wed, Thur, Fri, Sat, Sun** - Select the deployment to be scheduled every X weeks on the selected days.
4. Continue to “**Selecting the Deployment Start and End Functions**”.

To Set Up a Monthly Recurring Deployment

1. Select **Recurring**.
The *Recurring Deployment* window opens.
2. In the *Occurs* field, select **Monthly**.
The Deployment Wizard displays the *Monthly Deployment Options* fields.

Occurs:
☐ Daily
☐ Weekly
☒ Monthly

Monthly:
☒ Day 1 of every 1 month(s)
☐ The 1st Sunday of every 1 month(s)

Figure 4.24 Monthly Options

3. Select the frequency of the deployment.
- **Day X of every X month(s)** - allows the deployment to be scheduled on a specific date every X months. Valid date options are 1 through 31, with the ability to choose 1 through 99 months.



- **The Xth Weekday of every X month(s)** - allows the deployment to be run on a specific day every X months. The valid day options are: 1st, 2nd, 3rd, 4th, or Last, weekday options are: Sunday through Saturday, Day, Week day, or Weekend day and monthly recurrence options are: 1 through 99 months .

Duration: ☒ 12 hour ☐ 24 hour

Start Date: End Date: ☒ No End Date

Time: Hour: Minute: PM Minute: PM

Figure 4.25 Common Deployment Options

4. Continue to **“Selecting the Deployment Start and End Functions”**.

Selecting the Deployment Start and End Functions

The frequency fields allow for specific date and time deployments. Review the table to determine scheduling needs.

Table 4.16 Calendar Functions

Select	To
12 hour 24 hour	Set the schedule to either a standard 12 hour format or a military 24 hour format.
Occurs once at	Allow the deployment to occur once daily at the time defined here. Note: Agent Communication Interval and HOP settings modify the actual deployment time.
Occurs every	Allow the deployment to occur multiple times on the scheduled day, between the hours defined in the starting at: and ending at: fields with a delay of the defined hours or minutes.
Start Date	Schedule a recurring deployment to begin at a later date. Defaults to the current date.
No End Date	Continue with the defined recurrence schedule and no defined end date.
End Date	Activate the End Date Calendar function and define the date the deployment will no longer be deployed.



Click **Next** to save the changes and return to the *Deployment Options* page.

Package Deployment Order and Behavior Page

The *Package Deployment Order and Behavior* page of the Deployment Wizard, allows you to set the order and behavior for the individual package deployments.

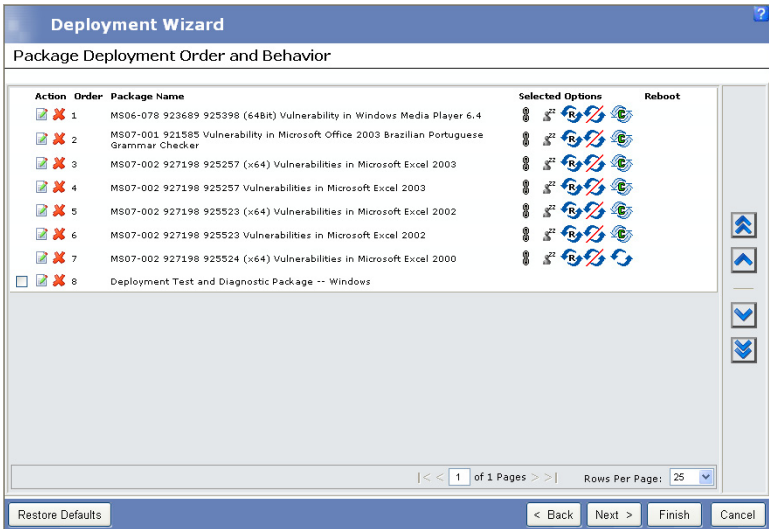


Figure 4.26 Deployment Wizard - Package Deployment Order and Behavior Page





The following tasks can be completed while using the Package Deployment Order and Behavior page:

Table 4.17 Package Order icons

Icon	Action	Use To
	Edit	Open the <i>Package Deployment Behavior Options</i> page and change the behavior options for that package.
	Delete	Remove the package from the deployment.
	Selected Options	View the behavior of each package defined in Table 4.18, "Behavior Icon Definitions" .
	Reboot	View the reboot settings of each package defined in Table 4.19, "Reboot Icon Definitions" .
	Move to top	Move the package to the top of all non-chained deployments (this will place it immediately after the chained deployments).



Table 4.17 Package Order icons

Icon	Action	Use To
	Move up one line	Move the package up one.
	Move down one line	Move the package down one.
	Move to bottom	Move the package to the bottom of the listing.
	Restore Defaults	Restore the package order and behavior back to their default settings.



Note: Chained packages cannot be moved without first removing their chained status. When a package is chained, ZENworks Patch Management determines the deployment order. However, when no longer chained, the package can be deployed at anytime following the chained deployments.

The Selected Options icons are used to identify package deployment actions.

The following table describes the Deployment Behavior icons and their descriptions:

Table 4.18 Behavior Icon Definitions






Icon	Action	Use to
	Uninstall	Uninstall the packages.
	Force Shutdown	Force all applications to close if the package causes a reboot.
	Do Not Backup	Do not backup files for uninstall.
	Suppress Reboot	Prevent a reboot after installation.
	Quiet Mode	Suppress any user interfaces during the deployment.





Table 4.18 Behavior Icon Definitions

Icon	Action	Use to
	Unattended Setup	Set up packages in unattended mode.
	List Hot Fixes	Return a listing of hot fixes installed on the target devices.
	Force Reboot	Force a reboot regardless of package requirements.
	Reboot is Required	Indicate a reboot is required prior to completing the installation.
	Chain Packages	Set the package as chainable (package must support chaining).
	Suppress Chained Reboot	Suppress the reboot, allowing other chained packages to be sent following this package. When creating multiple deployment jobs, this option is recommended.
	Repair File Permissions	Repair file permissions following the package installation.
	Download Only	Distribute the package without running the package installation script.
	Suppress Notification	Suppress any user notifications during installation.
	Debug Mode	Run the package installation in debug mode.
	Do Not Repair Permissions	Suppress the repair of file name permissions after the reboot.
	May Reboot	Allow the package to force a reboot if required.
	Multi-User Mode	Perform the installation in 'Multi-User' mode.
	Single-User Mode	Perform the installation in 'Single-User' mode.
	Restart Service	Restart the service following the deployment.
	Do Not Restart Service	Do not restart the service following the deployment.



Table 4.18 Behavior Icon Definitions






Icon	Action	Use to
	Reconfigure	Perform the system reconfigure task following deployment.
	Do Not Reconfigure	Do not perform the system reconfigure task following deployment.



Note: When using a chained deployment, reboots are suppressed whenever possible. The final deployment is represented as *May Reboot* because Patch Management Server determines if the agent is in a dirty state. If so, a *System Task - Reboot* deployment is sent before deploying the remaining packages

The following table describes the Reboot icons and their descriptions:

Table 4.19 Reboot Icon Definitions

Icon	Name	Reboot Status
	Reboot may occur	The device may be rebooted, dependent upon the package installer requirements (at the time of install).
	Reboot may occur chained	The device may be rebooted, dependent upon the package requirements. However if a reboot is required and the device is not rebooted, the device will enter a reboot state.
	Reboot required	No other (chainable or non-chainable) packages will be installed until the device reboots.
	Reboot required chained	Only chainable packages will continue to be installed until the device has been rebooted.
	Reboot will occur	The device will be rebooted following the package installation.

Click **Next** to proceed to the *Deployment Notification Options* page.

Click **Finish** to create the deployments and proceed to the *Deployments Summary* page.



Package Deployment Behavior Options Page

The *Package Deployment Behavior Options* page of the Deployment Wizard, allows you to set the behavior options for each of the packages associated with this deployment. The Package Options are active or inactive, depending on the patch selected.



Figure 4.27 Behavior Options



Note: Modification of a package’s behavior options will cause the package order to be reevaluated by the Deployment Wizard, which may result in a change in the package order.

To Modify Behavior Options

1. In the *Behavior Options* page, review the pre-selected options.
2. Select or deselect the **checkbox** next to the option to modify the Behavior Options.



3. Click **Next** to continue to the *Notification Options* page.



Note: Not all packages support all of the available behavior options.

Behavior Options












The following table describes the Deployment Behavior icons and their descriptions:

Table 4.20 Behavior Icon Definitions

Icon	Action	Use to
	Uninstall	Uninstall the packages.
	Force Shutdown	Force all applications to close if the package causes a reboot.
	Do Not Backup	Do not backup files for uninstall.
	Suppress Reboot	Prevent a reboot after installation.
	Quiet Mode	Suppress any user interfaces during the deployment.
	Unattended Setup	Set up packages in unattended mode.
	List Hot Fixes	Return a listing of hot fixes installed on the target devices.
	Force Reboot	Force a reboot regardless of package requirements.
	Reboot is Required	Indicate a reboot is required prior to completing the installation.
	Chain Packages	Set the package as chainable (package must support chaining).
	Suppress Chained Reboot	Suppress the reboot, allowing other chained packages to be sent following this package. When creating multiple deployment jobs, this option is recommended.
	Repair File Permissions	Repair file permissions following the package installation.



Table 4.20 Behavior Icon Definitions

Icon	Action	Use to
	Download Only	Distribute the package without running the package installation script.
	Suppress Notification	Suppress any user notifications during installation.
	Debug Mode	Run the package installation in debug mode.
	Do Not Repair Permissions	Suppress the repair of file name permissions after the reboot.
	May Reboot	Allow the package to force a reboot if required.
	Multi-User Mode	Perform the installation in 'Multi-User' mode.
	Single-User Mode	Perform the installation in 'Single-User' mode.
	Restart Service	Restart the service following the deployment.
	Do Not Restart Service	Do not restart the service following the deployment.
	Reconfigure	Perform the system reconfigure task following deployment.
	Do Not Reconfigure	Do not perform the system reconfigure task following deployment.

Optional Package Flags

An area for any extra package flags unique to a particular deployment. In addition to flags specific to the package being deployed, the following Novell flags are available:



Package Flag Descriptions

The following table defines the flag behavior and their descriptions:

Table 4.21 Package Flag Descriptions and Behavior

Description (flag behavior)	Display Flag	Select Flag
Perform an uninstall; can be used with -m or -q	-yd	-y
Force other applications to close at shutdown	-fd	-f
Do not back up files for uninstall	-nd	-n
Do not restart the computer when the installation is done	-zd	-z
Use quiet mode, no user interaction is required	-qd	-q
Use unattended Setup mode	-md	-m
Install in multi-user mode (UNIX, Linux only)	-dmu	-mu
Install in single-user mode (UNIX, Linux only)	-dsu	-su
Restart service after installation (UNIX, Linux only)	-drestart	-restart
Do not restart service after installation (UNIX, Linux only)	-dnorestart	-norestart
Reconfigure after installation (UNIX, Linux only)	-dreconfig	-reconfig
Do not reconfigure after installation (UNIX, Linux only)	-dnoreconfig	-noreconfig
This package is chainable and will run Qchain.exe (windows) or (UNIX/Linux)	-dc	-c
Suppress the final chained reboot	-dc	-sc
Repair permissions	-dr	-r
Deploy Only	-PLD1	-PLD0
No Pop-up	-PLN1	-PLNP
Debug	-PLDG	-PLDEBUG
Suppress Repair	-dsr	-sr
Force the script to reboot when the installation is done	-1d	-1
Reboot is required	Not Applicable	-2
Reboot may occur	Not Applicable	-3
Reboot is required, and MAY occur	Not Applicable	-4



Package Display Options

Table 4.22 Package Display Options

Option	Description
Notes	Displays the expected deployment behavior.
Description	Displays the package description

Click **Save** to save the changes and return to the *Package Deployment Order and Behavior* page.

Notification Options Page

The *Notification Options* page of the Deployment Wizard, allows you to define whether users will receive notification of these deployments and/or reboots, and if so, what the notification will contain.



Note: When an agent is installed on a server where multiple users are logged in simultaneously, the deployment manager will provide each logged in user with the ability to snooze or reject the deployment and/or reboot if snooze or reject is enabled.

Deployment Wizard														
Notification Options														
<h3>Define the Deployment Notification Options</h3> <p> <input type="radio"/> Do not notify users of this deployment <input checked="" type="radio"/> Notify users of this deployment </p> <p> Message: (Maximum 1000 characters) The download and installation of the patch: (Package Name) is ready to begin. If you require any additional information, please contact your PatchLink </p> <p>828 characters left.</p> <p> <input type="checkbox"/> Use Policies </p> <table border="0"> <thead> <tr> <th>Options</th> <th>Use Agent Policy</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>Allow user to cancel</td> <td><input type="checkbox"/></td> <td>No</td> </tr> <tr> <td>Allow user to snooze</td> <td><input type="checkbox"/></td> <td>Yes</td> </tr> <tr> <td>Notification on top</td> <td><input type="checkbox"/></td> <td>Yes</td> </tr> </tbody> </table> <p>Deploy</p> <p> <input checked="" type="radio"/> Within 60 Mins <input type="radio"/> By 4:00/2007 12:16 PM </p>			Options	Use Agent Policy	Setting	Allow user to cancel	<input type="checkbox"/>	No	Allow user to snooze	<input type="checkbox"/>	Yes	Notification on top	<input type="checkbox"/>	Yes
Options	Use Agent Policy	Setting												
Allow user to cancel	<input type="checkbox"/>	No												
Allow user to snooze	<input type="checkbox"/>	Yes												
Notification on top	<input type="checkbox"/>	Yes												
<h3>Define the Reboot Notification Options</h3> <p> <input type="radio"/> Do not notify users of the reboot <input checked="" type="radio"/> Notify users of the reboot </p> <p> Message: (Maximum 1000 characters) To complete the installation of the patch: (Package Name), it is now necessary to reboot your device. If you require any additional information, please </p> <p>884 characters left.</p> <p> <input type="checkbox"/> Use Policies </p> <table border="0"> <thead> <tr> <th>Options</th> <th>Use Agent Policy</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>Allow user to cancel</td> <td><input type="checkbox"/></td> <td>No</td> </tr> <tr> <td>Allow user to snooze</td> <td><input type="checkbox"/></td> <td>Yes</td> </tr> <tr> <td>Reboot within</td> <td><input type="checkbox"/></td> <td>60 Mins</td> </tr> </tbody> </table>			Options	Use Agent Policy	Setting	Allow user to cancel	<input type="checkbox"/>	No	Allow user to snooze	<input type="checkbox"/>	Yes	Reboot within	<input type="checkbox"/>	60 Mins
Options	Use Agent Policy	Setting												
Allow user to cancel	<input type="checkbox"/>	No												
Allow user to snooze	<input type="checkbox"/>	Yes												
Reboot within	<input type="checkbox"/>	60 Mins												

Figure 4.28 Deployment Wizard - Notification Options Page

Allows you to determine what the device users can do once they receive a deployment.

Table 4.23 Use Policies - Deployment

Option	When Used
Use Policies	The defined <i>Agent Policies</i> for each agent will be used. Selection of this option disables all other deployment notification options.
Do not notify users of this deployment	There will be no user notification of this deployment, and the deployment will occur automatically. Selection of this option disables all other (except Use Policies) deployment notification options.
Notify users of this deployment	The user will be notified prior to the installation of this deployment.
Message	This field contains the message the user will see when notified about this deployment. The <code>{%Package_Name%}</code> variable will be replaced with the Package Name, allowing you to enter custom text before or after the package name.

Deployment Permissions

When defining deployment permissions you can specify to use the Agent Policy or the custom setting.

Table 4.24 Deployment Recipient Permissions

Option	Use To
Allow User to Cancel	Define if the recipient can cancel the deployment.
Allow User to Snooze	Define if the recipient can snooze the deployment.
Notification on Top	Define if the Novell Desktop Deployment Manager (PDDM) will display on top of all other applications.
Deadline Offset	Allows you to set a custom deadline offset, or custom deadline date for the deployment. <ul style="list-style-type: none"> • From Deployment Start - Sets the deployment deadline to be X Minutes, Hours, or Days from deployment start date/time. • Specific Date - Sets the deployment deadline to a specific date and time.



Reboot Notification Options

Allows you to determine what the device users can do once they receive a reboot notification.



Note: When a deployment does not require a reboot, the following **Reboot Notification Options** are disabled.

Table 4.25 Use Policies - Reboot

Option	When Used
Use Policies	The defined Agent Policies for each agent will be used. Selection of this option disables all other reboot notification options.
Do not notify users of the reboot	There will be no user notification prior to rebooting the computer.
Notify users of the reboot	The user will be notified prior to the reboot of their computer.
Message	This field contains the message the user will see when notified about the reboot. The {%Package_Name%} variable will be replaced with the Package Name, allowing you to enter custom text before or after the package name.

Table 4.26 Reboot Recipient Permissions

Option	Use To
Allow User to Cancel	Define if the recipient can cancel the reboot.
Allow User to Snooze	Define if the recipient can snooze the reboot.
Deadline Offset	Allows you to set a custom reboot delay (in Minutes, Hours, or Days) for this deployment.

Click **Finish** to create the deployments and proceed to the *Deployments Summary* page.



Deployment Confirmation Page

The *Deployment Confirmation* page of the Deployment Wizard displays a summary of the options selected for this deployment. This information is provided for your verification prior to creating the deployment.

Deployment Wizard

Deployment Confirmation

Job Name: My Deployment Job
 Schedule: One time deployment, starting on 4/30/2007 6:16:03 PM based on Agent UTC Time.
 Manner: Concurrent; Deploying to 500 devices at a time.
 Deployment Notification: Notify and allow users to snooze the deployment.
 Reboot Notification: Notify and allow users to snooze the impending reboot.
 Total Selected Packages: 8
 Total Selected Devices/Groups: 1
 Notes: Created by administrator on 4/30/2007 6:16:03 PM (UTC)

Selected Packages

Order	Package Name	Selected Options	Reboot	Devices/Groups
1	MS06-078 922689 925298 (64bit) Vulnerability in Windows Media Player 6.4	[Icons]	[Reboot Icon]	1
2	MS07-001 921585 Vulnerability in Microsoft Office 2003 Brazilian Portuguese Grammar Checker	[Icons]	[Reboot Icon]	1
3	MS07-002 927198 925257 (x64) Vulnerabilities in Microsoft Excel 2003	[Icons]	[Reboot Icon]	1
4	MS07-002 927198 925257 Vulnerabilities in Microsoft Excel 2003	[Icons]	[Reboot Icon]	1
5	MS07-002 927198 925223 (x64) Vulnerabilities in Microsoft Excel 2002	[Icons]	[Reboot Icon]	1
6	MS07-002 927198 925223 Vulnerabilities in Microsoft Excel 2002	[Icons]	[Reboot Icon]	1
7	MS07-002 927198 925224 (x64) Vulnerabilities in Microsoft Excel 2000	[Icons]	[Reboot Icon]	1
8	Deployment Test and Diagnostic Package -- Windows	[Icons]	[Reboot Icon]	2

1 of 1 Pages Rows Per Page: 25

< Back Next > Finish Cancel

Figure 4.29 Deployment Confirmation Page

Deployment Confirmation Summary

Lists the parameters of the deployment defined in the Deployment and Notification Options.

Table 4.27 Deployment Confirmation Summary Options

Summary Item	Description
Job Name	The name given the deployment job defined in the <i>Deployment Options</i> page.
Schedule	The schedule for the deployment defined in the <i>Deployment Options</i> page.
Manner	Whether these deployments are Sequential or Parallel, and if Sequential, how many deployments will be distributed at once.
Deployment Notification	Whether or not the users will receive a deployment notification (as defined under the <i>Notification Options</i> page).
Reboot Notification	If the deployments must reboot, whether or not the users will receive a reboot notification (as defined under the <i>Notification Options</i> page).
Total Selected Packages	The total number of packages selected for deployment.



Table 4.27 Deployment Confirmation Summary Options

Summary Item	Description
Total Selected Devices/Groups	If the deployment is a group deployment, the number of groups selected. If the deployment is for individual devices, the total number of devices selected.
Notes	Who created the deployments, and when they were created.

Selected Packages

Displays the deployment order, package name, deployment options, reboot status, and the number of applicable devices for the package.

Table 4.28 Select Packages Column Descriptions

Column	Description
Order	Displays the order in which the packages will be deployed.
Package Name	Displays the name of each package that will be deployed. Click the Package Name link to open the <i>Package Applicability</i> page.
Selected Options	Displays the behavior of each package defined in the <i>Package Deployment Behavior Options</i> page.
Reboot	Displays the reboot settings of each package defined in the <i>Package Deployment Behavior Options</i> page.
Devices/Groups	Displays the number of selected devices and/or groups applicable to each package.

Click **Finish** to create the deployments and proceed to the *Deployments Summary* page.



Associated Vulnerability Analysis Page

The *Associated Vulnerability Analysis* page of the Deployment Wizard allows you to view the devices targeted for the deployment, and if they are patched for the selected vulnerabilities.

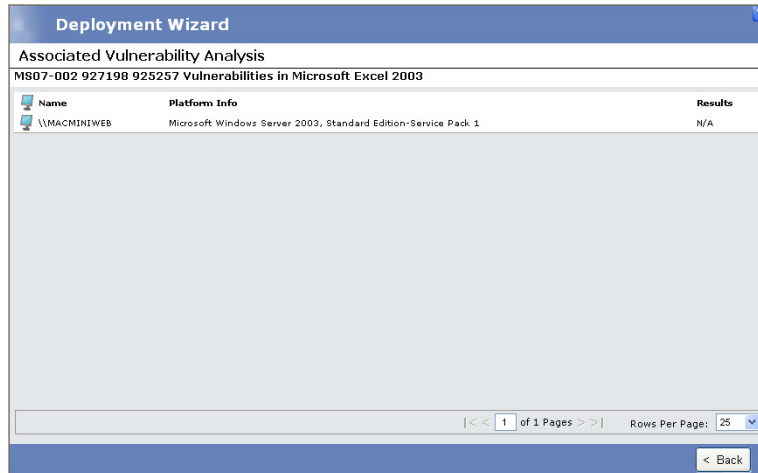


Figure 4.30 Deployment Wizard - Associated Vulnerability Analysis Page

The following table describes the fields and their descriptions.

Table 4.29 Associated Vulnerability Analysis

Name	Description
Name	Name of device receiving the deployment.
Platform Info	Applicable Operating Systems.
Results	Displays either Yes or N/A depending on whether the selected package applies to that particular device.

Click **Back** to return to the *Deployment Confirmation* Page.



Deployment Summary Page

The *Deployment Summary* page of the Deployment Wizard displays the result of the wizard.

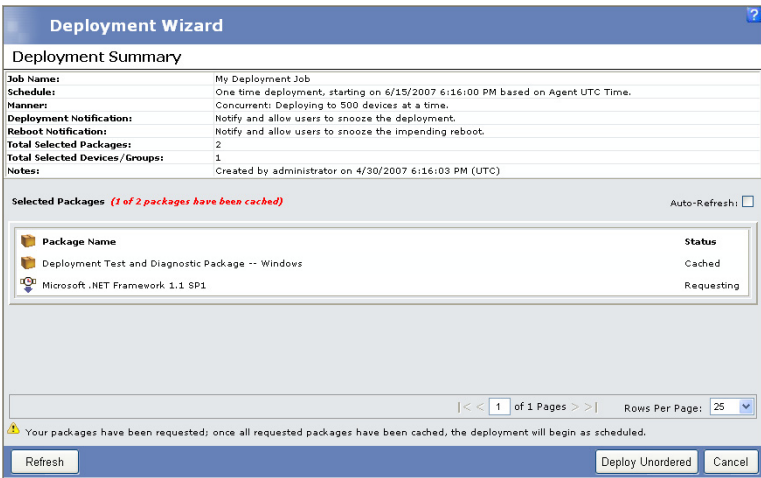


Figure 4.31 Deployment Wizard - Deployment Summary Page

Summary Section

The Deployment Summary lists all the parameters associated with the deployment.

Table 4.30 Summary Information

Summary Item	Description
Job Name	The name given the deployments defined in the <i>Deployment Options Page</i> .
Schedule	The schedule for the deployments defined in the <i>Deployment Options Page</i> .
Manner	Sequential or Parallel deployment as defined under the <i>Deployment Options Page</i> , and if Sequential, how many deployments will be distributed at once.
Deployment Notification	Whether or not the users will receive a deployment notification.
Reboot Notification	If the deployments must reboot, whether or not the users will receive a reboot notification.
Total Selected Packages	The total number of packages selected for deployment.
Total Selected Computers/Groups	If the deployment is a group deployment, the number of groups selected. If the deployment is for individual devices, the total number of devices selected.
Notes	When the deployments were created, and who created them.



Selected Packages Section

Displays the deployment order, package name, and cache status of the package in a grid format

Table 4.31 Selected Packages Options

Package	Description
Package Name	Displays the name of each package that will be deployed.
Status	Displays whether the package is already cached or currently downloading.
Cancel	Cancels all of the deployments.

If one or more of the selected packages have not been cached, **Deploy Unordered** will be available.

Table 4.32 Selected Un-cached Packages Options

Button	Description
Deploy Unordered	Creates the applicable deployments, deploying the packages in the cache order, rather than the order defined within the deployment wizard.

Click **Close** to initialize your deployment(s).





5 Using Devices and Inventory

The *Devices* page contains a listing of all devices that have an agent registered to the Patch Management Server. From this list of devices, you can access the *Device Details*. The device details include device specific information such as associated vulnerabilities, inventory information, and deployment history.

The *Inventory* page provides a means to pinpoint all the operating systems, software applications, hardware devices, and services installed and running on the devices registered to the Patch Management Server.

In this Chapter

- “About Devices”
- “Working with Devices”
- “About Inventory”
- “Using the Inventory Tab”
- “Scanning Inventory”
- “Using Custom Inventory”

About Devices

The *Devices* page contains a listing of all devices registered to the Patch Management Server. The page displays general information about the device including:

- Device Name
- IP Address
- Status
- Operating system information



■ Version

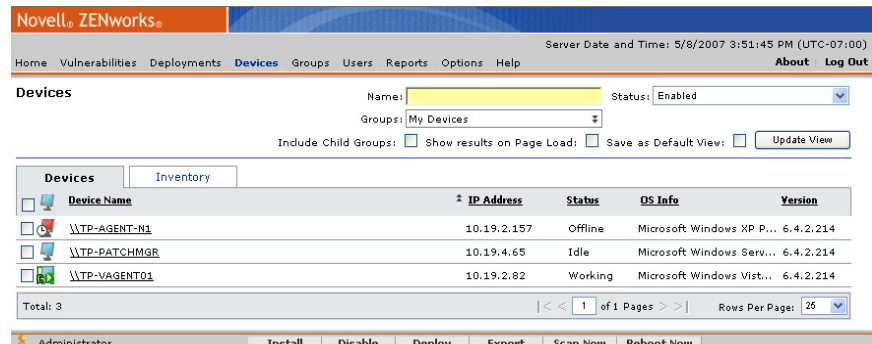


Figure 5.1 Devices page

Viewing Devices

To View Devices

- 1. Select the *Devices* tab.
- 2. Select your filter options.
- 3. Click **Update View**.
The Devices page displays the devices which match the selected filter options.



Note: To view all devices, select the **Include Child Groups** checkbox.



Using the Devices Page

To display additional information about the device, click on the name of the actual device.

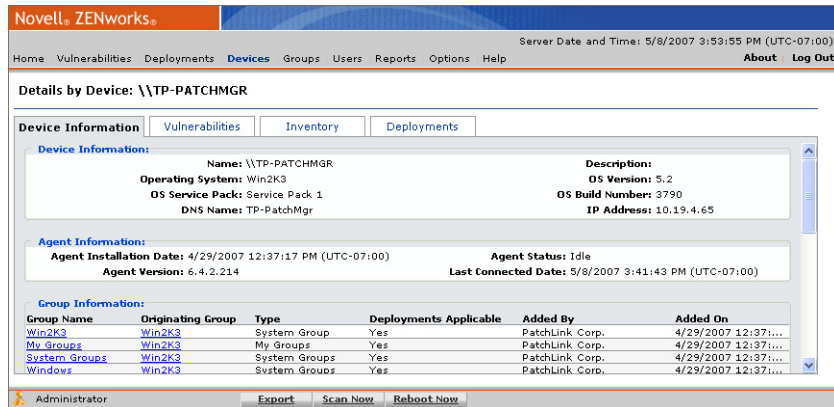


Figure 5.2 Devices page

The following table describes the fields within the Devices Page:

Table 5.1 Device Page Columns

Field	Description
Device Name	The name of the device as extracted from system data and inventory. Selecting the device name displays the Device Details page. The displayed devices can be determined by the filter criteria defined in the search section.
IP Address	The IP address of the device ascertained during the discovery and initial communication with the agent installed on the device
Status	The status of the device. Status values include: Detecting, Disabled, Idle, Offline, Sleeping, Working, and Unknown.
OS Info	Additional information about the operating system the device is running
Version	The version number of the agent installed on the device



Action Menu Functions

The following table describes the Action Menu functions used in the Devices page.

Table 5.2 Devices Action Menu

Menu Item	Description
Install	Select this option to install an agent to a device.
Enable	Select this option to enabled a disabled device.
Disable	Select this option to inactivate an agent on a device.
Delete	Select this option to delete a disabled device.
Deploy	Select this option to deploy to a selected device.
Export	Retrieves all device information and allows for saving to a .CSV file. See "Exporting Data" for more information.
Scan Now	Prompts the DAU to immediately check the device. See "Using the Scan Now Feature" for more information.
Reboot Now	Prompts the selected device to reboot. See "Rebooting Devices" for more information.

























Device Status Icons

The status of the agent installed on the registered device is indicated by an icon in the status column. The displayed devices are determined by the filter criteria defined in the search section. The filter may be set to display only a certain status type (for example, enabled or idle devices).

The following table defines agent (device) status and associated icons.

Table 5.3 Device Status Icons

Active	Pending	Description
	N/A	The agent is currently working on a deployment (animated icon).
		The agent is idle, and has pending deployments.
		The agent is offline.
		The agent is sleeping due to its Hours of Operation settings.
		This agent has been disabled.
		The agent is offline and is in a QChain status (can accept chained deployments only after reboot).
		The agent is offline and is in a Reboot status (can accept no more deployments until after it reboots).
		The agent is in a QChain status (the agent can accept chained deployments only until after a reboot).
		The agent is in a Reboot status (the agent can accept no more deployments until after it reboots).
		The agent is in a QChain status (the agent can accept chained deployments only until after a reboot) and is sleeping due to its Hours of Operation settings.
		The agent is in a Reboot status (the agent can accept no more deployments until after it reboots) and is sleeping due to its Hours of Operation settings.
	N/A	Unable to identify the agent status.



Using the Details by Device Page

To display additional information about a device; in *Devices*, click on the name of the device. The *Device Details* page provides device specific information, associated vulnerabilities, inventory information, and deployment history. The tabs access specific details about the device.

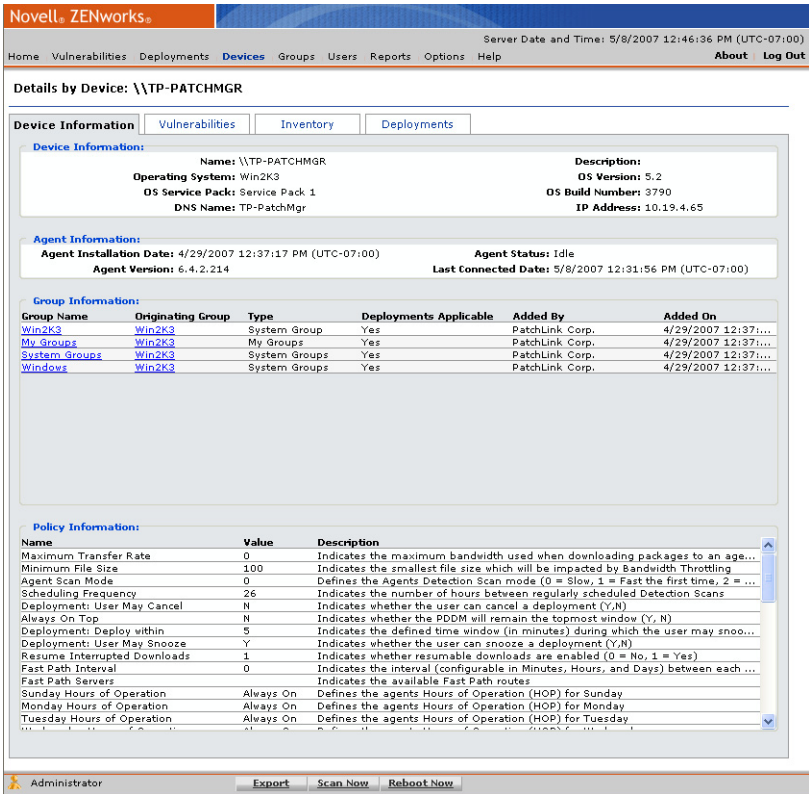


Figure 5.3 Device Details Page

Device Information Tab

The *Device Information* tab displays important information about the device. The page displays general information organized in five main categories; device, agent, group, policy, and notification settings.



Device Information Section

The **Device Information** section displays the following device data:

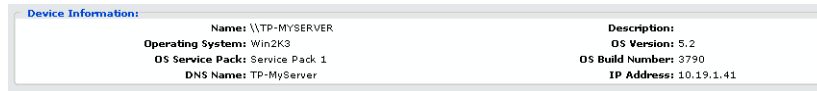


Figure 5.4 Device Information

Table 5.4 Device Information Field Descriptions

Field	Description
Name	The name of the device.
Operating System	The abbreviated name of the operating system detected on the device.
OS Service Pack	The service pack level of the device.
DNS Name	The DNS name of the device.
Description	The description of the device, if available
OS Version	The version number of the operating system running on the device.
OS Build Number	The build number of the operating system running on the device.
IP Address	The IP Address of the device.

Agent Information Section

The **Agent Information** section displays the following agent data:

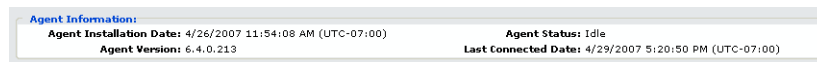


Figure 5.5 Agent Information

Table 5.5 Agent Information Field Descriptions

Field	Description
Agent Installation Date	The date the agent registered with Patch Management Server. This is typically the date the agent was installed on the device.
Agent Version	The agent version number.



Table 5.5 Agent Information Field Descriptions

Field	Description
Agent Status	The status of the agent. Also shown on the <i>Devices</i> page.
Last Connected Date	The date the agent last communicated with Patch Management Server.

Group Information Section

The *Group Information* section displays the following group data:

Group Information:					
Group Name	Originating Group	Type	Deployments Applicable	Added By	Added On
Another Child Group	Another Child Group	Custom Group	Yes	ADMINISTRATOR	4/29/2007 2:02:01...
My Child Group	My Child Group	Custom Group	Yes	PATCHLINK	4/27/2007 8:09:58...
Win2K3	Win2K3	System Group	Yes	PatchLink Corp.	4/26/2007 11:54:1...
Windows	Windows	System Groups	Yes	ADMINISTRATOR	4/29/2007 2:02:01...
Another Parent Group	Another Child Group	Custom Group	Yes	ADMINISTRATOR	4/29/2007 2:02:01...
My Groups	Windows	My Groups	Yes	ADMINISTRATOR	4/29/2007 2:02:01...
My Groups	Win2K3	My Groups	Yes	PatchLink Corp.	4/26/2007 11:54:1...
My Groups	My Child Group	My Groups	Yes	PATCHLINK	4/27/2007 8:09:58...
My Groups	Another Child Group	My Groups	Yes	ADMINISTRATOR	4/29/2007 2:02:01...
My Parent Group	My Child Group	Custom Group	Yes	PATCHLINK	4/27/2007 8:09:58...
System Groups	Windows	System Groups	Yes	ADMINISTRATOR	4/29/2007 2:02:01...
System Groups	Win2K3	System Groups	Yes	PatchLink Corp.	4/26/2007 11:54:1...
Windows	Win2K3	System Groups	Yes	PatchLink Corp.	4/26/2007 11:54:1...

Figure 5.6 Group Information

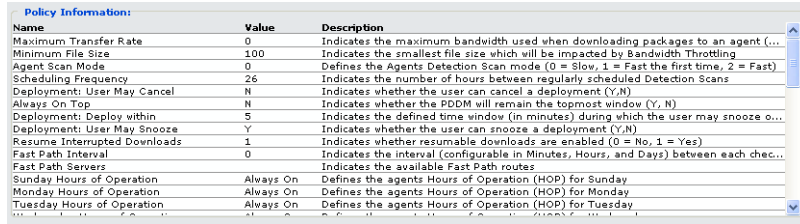
Table 5.6 Group Information Field Descriptions

Field	Description
Group Name	The name of the group(s) that the device is a member. Click the name to go to the <i>Group Information</i> page.
Originating Group	The name of the parent group that the device is a member. Click the name to go to the <i>Group Assessment</i> page.
Type	The group type. Can be a system created groups (OS), directory service, or custom group.
Deployments Applicable	Indicates if there are applicable deployments available for this device.
Added By	The Patch Management Server user who added the device to the group. System created groups indicate PatchLink Corp. in this field.
Added On	The date and time that the device was added to the group.



Policy Information Section

The Device *Policy Information* section displays the policies used by the device during a deployment. These policies are the results of applying each of the policies defined by the device's group membership (applying the conflict resolution rules when applicable) and filling in any undefined policies from the Global Policy.



Name	Value	Description
Maximum Transfer Rate	0	Indicates the maximum bandwidth used when downloading packages to an agent (...)
Minimum File Size	100	Indicates the smallest file size which will be impacted by Bandwidth Throttling
Agent Scan Mode	0	Defines the Agents Detection Scan mode (0 = Slow, 1 = Fast the first time, 2 = Fast)
Scheduling Frequency	26	Indicates the number of hours between regularly scheduled Detection Scans
Deployment: User May Cancel	N	Indicates whether the user can cancel a deployment (Y/N)
Always On Top	N	Indicates whether the PDDM will remain the topmost window (Y, N)
Deployment: Deploy within	5	Indicates the defined time window (in minutes) during which the user may snooze o...
Deployment: User May Snooze	Y	Indicates whether the user can snooze a deployment (Y/N)
Resume Interrupted Downloads	1	Indicates whether resumable downloads are enabled (0 = No, 1 = Yes)
Fast Path Interval	0	Indicates the interval (configurable in Minutes, Hours, and Days) between each chec...
Fast Path Servers		Indicates the available Fast Path routes
Sunday Hours of Operation	Always On	Defines the agents Hours of Operation (HOP) for Sunday
Monday Hours of Operation	Always On	Defines the agents Hours of Operation (HOP) for Monday
Tuesday Hours of Operation	Always On	Defines the agents Hours of Operation (HOP) for Tuesday

Figure 5.7 Policy Information

Table 5.7 Policy Information Field Descriptions

Field	Description
Name	The name of the policy assigned to the device. Because a device must have all policy values defined, every policy is listed here.
Value	The assigned value of the policy as determined by applying each of the policies defined by the device's group membership, applying conflict resolution when applicable, and filling in any undefined policies from the Global Policy. For more information go to "Customizing and Administering Agent Policy Sets" .
Description	The description of the policy assigned to the device.



Device Information Action Menu Items

The following table describes the Action Menu items available in the Device Information window.

Table 5.8 Action Menu

Menu Item	Description
Export	Retrieves all device information and allows for saving to a .CSV file. See "Exporting Data" for more information.
Scan Now	Prompts the DAU to immediately check the device. See "Using the Scan Now Feature" for more information.
Reboot Now	Prompts the selected device to reboot. See "Rebooting Devices" for more information.

Device Vulnerabilities

The *Device Vulnerabilities* tab displays vulnerability information associated with the selected device. The page displays the same information as is presented in the *Vulnerabilities* page. For details on using this page, see "Viewing Vulnerability Details" .

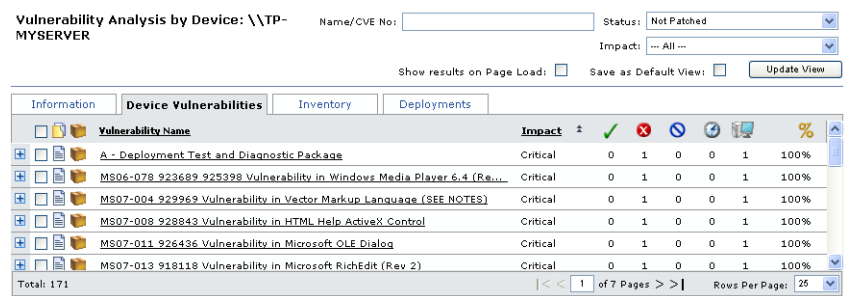


Figure 5.8 Device Vulnerabilities



Action Menu Functions

The following table describes the Action Menu functions used in the Devices Vulnerabilities page.

Table 5.9 Action Menu

Menu Item	Description
Deploy	Select this option to deploy to a selected device.
Disable	Select this option to disable a vulnerability for a device.
Enable	Select this option to enable a vulnerability for a device.
Export	Retrieves all device information and allows for saving to a .CSV file. See "Exporting Data" for more information.
Update Cache	Downloads packages and vulnerabilities required by the device. See "Updating the Cache" for more information.
Scan Now	Prompts the DAU to immediately check the device. See "Using the Scan Now Feature" for more information.
Reboot Now	Prompts the selected device to reboot. See "Rebooting Devices" for more information.

Device Inventory

The *Device Inventory* tab displays the inventory information for the selected device. The page displays the same information as is presented in the *Inventory* page. For details on using this page, see ["About Inventory"](#).



Figure 5.9 Device Inventory



Action Menu Functions

The following table describes the Action Menu functions used in the Device Inventory page.

Table 5.10 Action Menu

Menu Item	Description
Export	Retrieves all device information and allows for saving to a .CSV file. See "Exporting Data" for more information.
Scan Now	Prompts the DAU to immediately check the device. See "Using the Scan Now Feature" for more information.

Device Deployments

The *Device Deployments* page displays all of the deployments that the device has been associated with or assigned. The page displays the same information as is presented in the *Deployments* section in the *Vulnerabilities* page. For details on using this page, see "Using the Deployment Pages" .

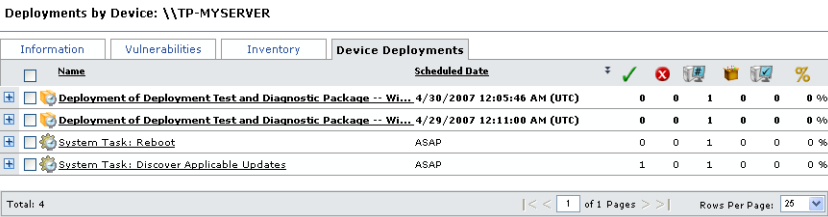


Figure 5.10 Device Inventory

Action Menu Functions

The following table describes the Action Menu functions used in the Device Deployment page.

Table 5.11 Action Menu

Menu Item	Description
Export	Retrieves all device information and allows for saving to a .CSV file. See "Exporting Data" for more information.



Working with Devices

There are several tasks associated with devices designed to assist you in managing devices and installing a ZENworks Patch Management Agent to a device. These are available from commands located in the *Action* menu at the bottom on the *Devices* page.

- “Installing an Agent”
- “Viewing Device Details”
- “Enabling a Device”
- “Disabling and Deleting a Device”
- “Deploying a Vulnerability”
- “Exporting Device Information”
- “Scanning Devices”
- “Rebooting Devices”



Installing an Agent

Click **Install** to display the list of agent installers that can be used to register devices to ZENworks Patch Management. When launching the Agent Installers dialog box, the behavior is the same whether a device is selected or not. Refer to the *ZENworks Patch Management 6.4 Agent Installation Guide* for complete instructions regarding the installation of agents.

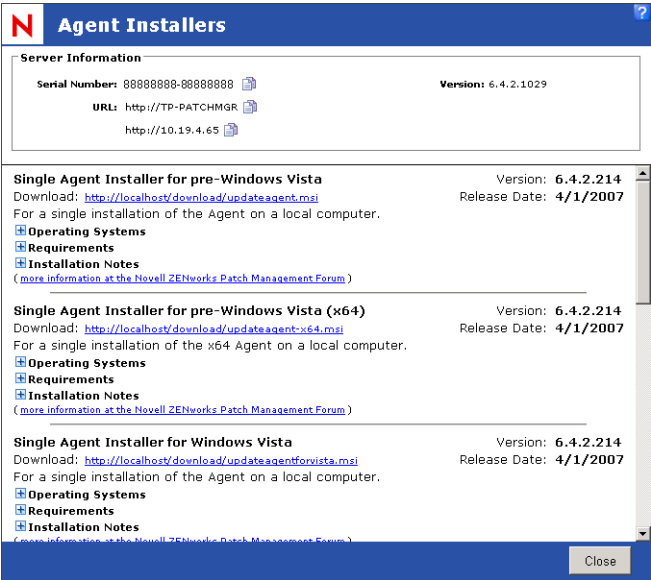


Figure 5.11 Agent Installer



Viewing Device Details

View details of a specific device by selecting the desired device and clicking the **device name**. The Device Details page is described in detail in “Using the Details by Device Page”.

Novell® ZENworks®

Server Date and Time: 5/8/2007 12:46:36 PM (UTC-07:00)

Home Vulnerabilities Deployments **Devices** Groups Users Reports Options Help [About](#) [Log Out](#)

Details by Device: \\TP-PATCHMGR

Device Information | Vulnerabilities | Inventory | Deployments

Device Information:

Name: \\TP-PATCHMGR	Description:
Operating System: Win2K3	OS Version: 5.2
OS Service Pack: Service Pack 1	OS Build Number: 3790
DNS Name: TP-PatchMgr	IP Address: 10.19.4.65

Agent Information:

Agent Installation Date: 4/29/2007 12:37:17 PM (UTC-07:00)	Agent Status: Idle
Agent Version: 6.4.2.214	Last Connected Date: 5/8/2007 12:31:56 PM (UTC-07:00)

Group Information:

Group Name	Originating Group	Type	Deployments Applicable	Added By	Added On
Win2K3	Win2K3	System Group	Yes	PatchLink Corp.	4/29/2007 12:37:17 PM
My Groups	Win2K3	My Groups	Yes	PatchLink Corp.	4/29/2007 12:37:17 PM
System Groups	Win2K3	System Groups	Yes	PatchLink Corp.	4/29/2007 12:37:17 PM
Windows	Win2K3	System Groups	Yes	PatchLink Corp.	4/29/2007 12:37:17 PM

Policy Information:

Name	Value	Description
Maximum Transfer Rate	0	Indicates the maximum bandwidth used when downloading packages to an agent.
Minimum File Size	100	Indicates the smallest file size which will be impacted by Bandwidth Throttling.
Agent Scan Mode	0	Defines the Agents Detection Scan mode (0 = Slow, 1 = Fast the first time, 2 = ...)
Scheduling Frequency	26	Indicates the number of hours between regularly scheduled Detection Scans.
Deployment: User May Cancel	N	Indicates whether the user can cancel a deployment (Y,N).
Always On Top	N	Indicates whether the PDM will remain the topmost window (Y, N).
Deployment: Deploy within	5	Indicates the defined time window (in minutes) during which the user may snooze...
Deployment: User May Snooze	Y	Indicates whether the user can snooze a deployment (Y,N).
Resume Interrupted Downloads	1	Indicates whether resumable downloads are enabled (0 = No, 1 = Yes).
Fast Path Interval	0	Indicates the interval (configurable in Minutes, Hours, and Days) between each ...
Fast Path Servers		Indicates the available Fast Path routes.
Sunday Hours of Operation	Always On	Defines the agents Hours of Operation (HOP) for Sunday.
Monday Hours of Operation	Always On	Defines the agents Hours of Operation (HOP) for Monday.
Tuesday Hours of Operation	Always On	Defines the agents Hours of Operation (HOP) for Tuesday.

Administrator [Export](#) [Scan Now](#) [Reboot Now](#)

Figure 5.12 Device Details Page



Disabling and Deleting a Device

Disabling a device releases the agent license used by the agent installed on the device and makes it available to the system. Once disabled, the agent on the device ceases communication with Patch Management Server and is no longer included in the patch management activities of the ZENworks Patch Management Server.



Note: Once disabled, the device may not appear in the devices list based on the *Status* filter settings. To include disabled devices in the list, ensure you select **Disabled** or **All** in the *Status* filter.

To Disable a Device

1. In the *Devices* list, select one or multiple devices.
2. In the *Action* menu, click **Disable**.
A *Disable Confirmation* dialog displays.
3. In the *Confirmation* dialog box, click **OK**.
The device is displayed in the list of devices identified with the *disabled* icon in the status column.

After disabling a device, the device can be deleted from ZENworks Patch Management.

To Delete a Device

1. In the *Devices* list, select one or multiple disabled devices.
2. In the *Action* menu, click **Delete**.
A *Delete Confirmation* dialog displays.
3. Click **OK** confirming the deletion.
The device is deleted from the *Devices* list.

Enabling a Device

An enabled device consumes an agent license and is included in the patch management activities of the ZENworks Patch Management Server.

To Enable a Device

1. In the *Devices* list, select one or multiple disabled devices.
2. In the *Action* menu, click **Enable**.
An *Enable Confirmation* dialog displays.
3. In the *Confirmation* dialog box, click **OK**.
The device is enabled.



Deploying a Vulnerability

Deploying a vulnerability to selected devices is a key function of the ZENworks Patch Management Server. Deployments are initiated by clicking **Deploy**. For more information on the Deployment Wizard, see “[Using the Deployment Wizard](#)”.



Note: The Deploy command is not exclusive to a selected device and results in the same action whether selected from the Devices or Vulnerabilities page. For detailed information on deploying patches, refer to [Chapter 4, “Working With Deployments”](#).

Exporting Device Information

The export utility lets you export device information to a comma-separated value (.CSV) file format. For more information on exporting, see “[Exporting Data](#)”.

Scanning Devices

The Scan Now utility lets you scan a device immediately via the DAU task. See “[Using the Scan Now Feature](#)” for more information.

Rebooting Devices

The *Reboot Now* command lets you initiate the Reboot system task to all or selected devices.

To Reboot Devices

1. In the *Devices* page, select one or multiple devices.
2. Click **Reboot Now**.
The *Reboot Device Warning* dialog box opens.

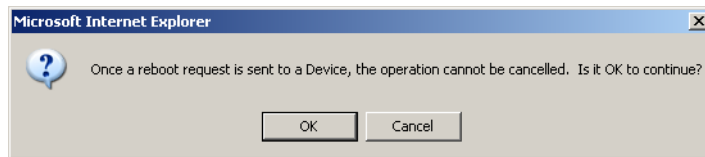


Figure 5.13 Reboot Device Warning



- 3. In the *Reboot Warning* dialog box, click **OK**.
The *Reboot Now* window opens.

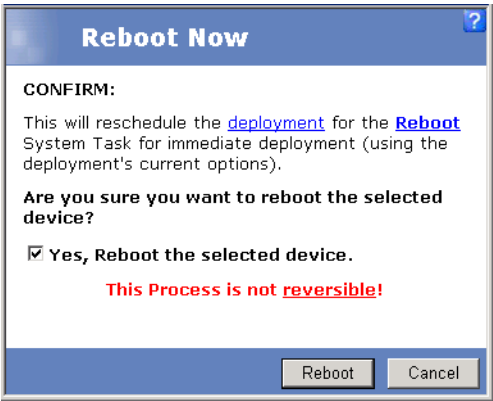


Figure 5.14 Reboot Device

- 4. Confirm the reboot, and select **Yes, Reboot the selected device**.
- 5. Click **Reboot**.
The system schedules the reboot and the *Reboot Success* window opens.
- 6. Click **Close**.
The window closes.



Figure 5.15 Reboot Device Success Screen



About Inventory

Inventory captures a comprehensive view of the functional components of each agent. An inventory list of software, hardware, operating systems, and services installed on a device can be retrieved. The inventory list displays items by *Inventory Type*.

In addition to viewing the list of inventory items, the inventory results can be exported to a file (.CSV). Inventory information is also available at the device and group level.



Note: Novell ZENworks Patch Management only captures inventory data for devices that have the ZENworks Patch Management Agent installed.

Viewing Inventory

To View Inventory

1. Select **Devices**.
The *Devices* page displays.
2. Select the *Inventory* tab.
3. Select your filter options.
4. Click **Update View**.
The Inventory results display on the *Inventory* tab.
5. Click the expand icon (plus icon) to view the details of a particular Inventory class.



Using the Inventory Tab

The *Inventory* tab displays a list of each *Inventory Type* and the associated devices. The devices that have the selected operating systems, hardware, software, and services installed can be viewed by clicking the expand icon (+).

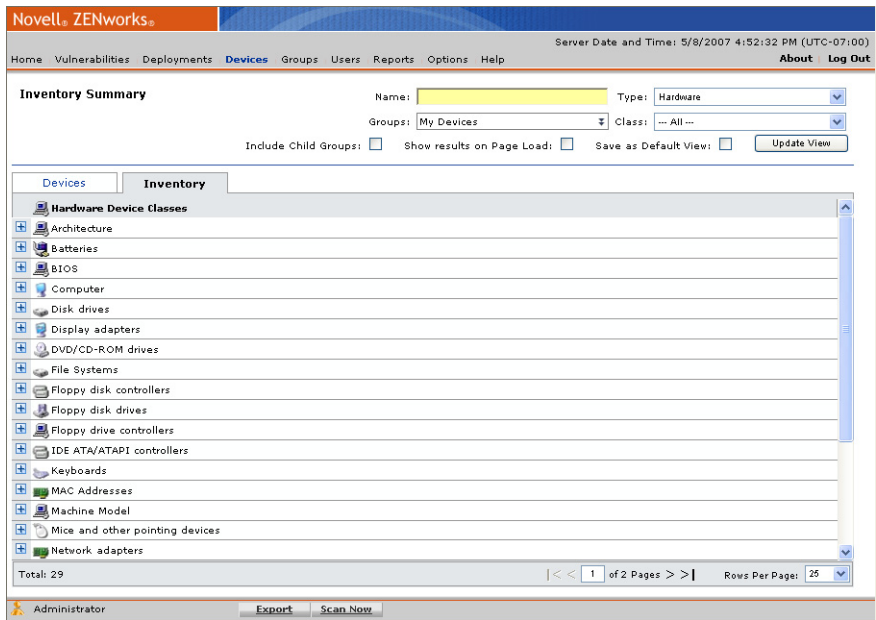


Figure 5.16 Inventory tab

Inventory Types

ZENworks Patch Management supports filtering by the following views:

- “Operating Systems View”
- “Software View”
- “Hardware View”
- “Services View”

Operating Systems View

Displays the full operating system (OS) platform names and the number of *instances the operating system was detected*. Instances refer to the number of times the operating system platform was detected. This value is always one if the display is based on a single device.



Software View

Displays the software applications detected on agents. This view displays the name of the software application and the number of instances detected.

Hardware View

Displays the hardware devices found on agents. Hardware is organized into device classes such as disk drives, processors, network adapters, etc. A Hardware Device Class is a grouping of hardware based upon type and a Hardware Device is a specific item.



Note: Windows NT reports some software as hardware resulting in displaying within the hardware inventory.

Services View

Displays the services detected on agents. The list includes all services detected, running or not. Each service also includes the number of detected instances.

Action Menu Functions

The following table describes the Action Menu functions used in the Inventory page.

Table 5.12 Action Menu

Menu Item	Description
Export	Retrieves all device information and allows for saving to a .CSV file. See "Exporting Data" for more information.
Scan Now	Prompts the DAU to immediately check the device. See "Using the Scan Now Feature" for more information.

Scanning Inventory

In addition to determining security risks and other vulnerabilities, the Discover Applicable Updates (DAU) task also identifies the device inventory. Each time the DAU runs, the current inventory is compared against the <Program Files>\Novell\ZENworks Patch



Management Agent\
localprofile.txt file. If any changes exist, a differential report is uploaded to the Patch Management Server. The following is an example local profile file (localprofile.txt).

```
<systemprofile>
  <computer>
    <BuildNumber>2600</BuildNumber>
    <Caption>Microsoft Windows XP Professional</Caption>
    <CSDVersion>Service Pack 2</CSDVersion>
    <Version>5.1.2600</Version>
    <computername>\\USER</computername>
    <DAversion>6.4.x.xxx</DAversion>
    <type>information</type>
    <agentid>XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX</agentid>
  </computer>
  <services>
    <caption svcName="Fax" State="Stopped" Startup="Automatic">Fax</caption>
  </services>
  <devices>
    <caption class="Monitors">Plug and Play Monitor</caption>
  </devices>
  <software>
    <package>Novell ZENworks Patch Management Agent</package>
  </software>
</systemprofile>
```

The Discover Applicable Updates task occurs at least once daily and following successful deployments.

Manually Scheduling the DAU Task

The Discover Applicable Updates task can be scheduled for immediate execution by selecting the *Scan Now* option. For more information on the Scan Now task, see [“Using the Scan Now Feature”](#).



Note: Clicking **Scan Now** from the *Inventory* page runs the DAU task for all enabled devices, not a specific device or device group. To schedule the DAU for a specific device or device group, click **Scan Now** from the *Devices* or *Device Groups* page.

Using Custom Inventory

To use a custom inventory file (see [“Defining Inventory Collection Options”](#)), you must create the custom inventory file in XML and distribute it to each agent. There is no automated distribution method for custom inventory.



Each agent must have a local file named `CustomInventory.xml` in `C:\Program Files\Novell\Update Agent (for Windows Agents)` or `patchagent/update/conf.d` (for Linux/Unix/Mac Agents). The XML inventory options can be customized as follows:

Guidelines for Microsoft Windows based Operating Systems

The following section defines the XML guidelines for setting up custom inventory scripts for Windows based Operating Systems. In each case, the item will be added to the hardware inventory under the *Default* device class unless a specific device class (`item class=""`) is defined.

Literal

Allows the user to assign an actual text value type into XML.

The string added will be of the form "**name = value**" where **name** is the tag name, and value is the literal typed between the open and close tags.

Example XML: (This example will return the string value defined between the open and close tags)

```
<item class="User Defined" name="Example Name" type="Literal">Novell 6.4  
Custom Inventory</item>
```

Returns:

```
"Example Name = Novell 6.4 Custom Inventory"
```

Registry

Allows the user to retrieve the registry key value.

The string added will be of the form "**name = value**" where **name** is the tag name and **value** is the value stored under the identified registry key.

Example XML (This example will return, from the Registry, the location and name of the custom inventory file):

```
<item name="Registry Example" type="registry">HKEY_LOCAL_MACHINE\Software\Novell.com\  
Discovery Agent\InventoryInputFile</item>
```

Returns:

```
"Registry Example= C:\Program Files\Novell\CustomInventory.xml"
```

Environment

Allows the user to return the value of an environment value.



The string added will be of the form "**name = value**" where **name** is the tag name and **value** is the expanded environment variable defined.

Example XML: (This example will return the value of the defined environment variable)

```
<item name="Environment Example" Class="User Defined" type="Environment">
    %PROCESSOR_ARCHITECTURE%</item>
```

Returns:

```
"Environment Example = i386"
```

WMI

Windows Management Instrumentation (WMI) allows the user to use scripting to use the WMI component, and tends to focus on operating system settings.

In the case of a WMI item, two additional attributes, *namespace* and *query* are used. If the namespace attribute is not specified, the default value of ROOT\CIMV2 is used. The query attribute must be defined as a valid WQL query. The string added will be of the form "**name = value**" where **name** is the tag name and **value** is the actual value for the specified WMI property.

Example XML (This example will return the Serial Number property from the Operating System):

```
<item name="Windows SN" type="wmi" query=" SELECT * FROM Win32_OperatingSystem">
    SerialNumber</item>
```

Returns:

```
"Windows SN = ABCD-EFGH-IJKL"
```

Example XML (This example will retrieve the Manufacturer property of the device):

```
<item name="Device Manufacturer" type="wmi" query=" SELECT * FROM Win32_OperatingSystem">
    Manufacturer</item>
```

Returns:

```
"Device Manufacturer = Computer Manufacturer A"
```



Text_File

Allows the user to retrieve text data from a file.

The string added will be of the form "***name*** = ***value***" where each line of the text file contains a Name/Value pair separated with a delimiter (defined with the ***delimiter*** attribute). For each valid line, in the text file, an entry will be added to inventory. When specifying a file name an environment variable, such as %WINDIR% can be used.

Example XML (This example will return the Name/Value pairs from a TXTSample.txt file in the Windows directory):

```
<item name="ti" type="text_file" delimiter="=">%WINDIR%\TXTSample.txt</item>
```

Returns:

```
"Line 1 = This is line one"
```

```
"Line 2 = This is line two"
```

XML_file

Allows the user to retrieve text data from a file.

An external XML file will be referenced. The XML file structure must be defined by the XPath string. When specifying an XML file name an environment variable, such as %WINDIR% can be used.

Example XML (This example will return the value of the Asset Number tag from the SampleXML.xml file in the Windows directory):

```
<item name="Asset" type="xml_file" xpath="/Top/Inventory/AssetNumber">
  %WINDIR%\SampleXML.xml</item>
```

Returns:

```
"Asset = PLA001"
```

Example XML (This example will return the value of the Location tag from the SampleXML.xml file in the Windows directory):

```
<item name="Building" type="xml_file" xpath="/Top/Inventory/Location">
  %WINDIR%\SampleXML.xml</item>
```

Returns:

```
"Building = Scottsdale-Main"
```



Where the *SampleXML.xml* file is as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<Top>
  <Inventory>
    <AssetNumber>PLA001</AssetNumber>
    <Location>Scottsdale-Main</Location>
  </Inventory>
</Top>
```

Example XML File

An example XML file, using the valid Windows agent inventory options, is provided below:

```
<?xml version="1.0" encoding="utf-8"?>
<customInventory>
  <items>
    <item name="l1" class="User Defined" type="literal">value1</item>
    <item name="l2" class="User Defined" type="literal">value2</item>
    <item name="l3" class="User Defined" type="literal">value3</item>
    <item name="l4" class="User Defined" type="literal">value4</item>
    <item name="r1" class="My New Class" type="registry">
      HKEY_LOCAL_MACHINE\Software\Novell.com
      \Discovery Agent\InventoryInputFile</item>
    <item name="e1" class="My New Class" type="environment">
      %PROCESSOR_ARCHITECTURE%</item>
    <item name="w1" class="My New Class" type="wmi" namespace="ROOT\CIMV2"
      query="SELECT * FROM Win32_OperatingSystem">SerialNumber</item>
    <item name="t1" class="My New Class" type="text_file"
      delimiter="=">c:\sampleInventoryText.txt</item>
    <item name="x1" class="My New Class" type="xml_file"
      xpath="//inventory/AssetTag">c:\sampleInventoryXML.xml</item>
  </items>
</customInventory>
```

Where the C:\SampleInventory.txt file is as follows:

```
Building = Main
Location = Scottsdale, AZ
Division = Corporate
```



And the C:\SampleInventoryXML.xml file is as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<inventory>
  <AssetTag>PLA00012</AssetTag>
</inventory>
```

Guidelines for Linux/Unix/Mac/Netware based Operating Systems

The following section defines the valid XML guidelines for setting up custom inventory scripts for Linux/Unix/Mac/Netware based Operating Systems. In each case, the item will be added to the hardware inventory under the *Default* device class unless a specific device class (`item class=""`) is defined.

Literal

Allows the user to assign an actual text value type into XML.

The string added will be of the form "**name = value**" where **name** is the tag name, and **value** is the literal typed between the open and close tags.

Example XML: (This example will return the string value defined between the open and close tags)

```
<item class="User Defined" name="Example Name" type="Literal">Novell 6.4
  Custom Inventory</item>
```

Returns:

```
"Example Name = Novell 6.4 Custom Inventory"
```



Dynamic

Allows the user to search using a script.

The string added will be of the form "**name = value**" where **name** is the tag name, and **value** is the result of the script.

Example XML:

```
<item class="System" name="Novell Disk Usage" type="dynamic">
  <command>
    <!-- Define shell -->
    <shell><![CDATA[/bin/sh]]></shell>
    <!-- Define execution directory -->
    <dir><![CDATA[/tmp]]></dir>
    <envs>
      <env>
        <!-- Define the JAVA HOME environment variable -->
        <EnvName><![CDATA[JAVA HOME]]></EnvName>
        <EnvValue><![CDATA[/usr/local]]></EnvValue>
      </env>
    </envs>
    <!-- Script -->
    <content><![CDATA[echo -n `du -ks /usr/local/work/Novell \ (in kb)`]]>
    </content>
  </command>
</item>
```

Returns:

```
"Novell Disk Usage = 18.1 (in kb)"
```



Example XML File

An example XML file, using valid Linux/Unix/Mac/Netware inventory options, is provided below:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- <!DOCTYPE customInventory SYSTEM "/home/user/testcode/custominventory.dtd" > -->
<customInventory xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xsi:schemaLocation="file://custominventory.xsd">
  <items>
    <item class="custom" name="Location" type="literal">Hardware Lab II</item>
    <item class="custom" name="Asset Tag" type="literal">ASDS3452-4545</item>
    <item class="custom" name="All users accounts" type="dynamic">
      <command>
        <shell><![CDATA[/bin/sh]]></shell>
        <dir><![CDATA[/tmp]]></dir>
        <envs>
          <env>
            <EnvName><![CDATA[JAVA_HOME]]></EnvName>
            <EnvValue><![CDATA[/usr/local]]></EnvValue>
          </env>
        </envs>
        <content><![CDATA[cat /etc/passwd]]></content>
      </command>
    </item>
    <item class="custom" name="PATH" type="dynamic">
      <command>
        <content><![CDATA[echo $PATH]]></content>
      </command>
    </item>
  </items>
</customInventory>
```





6 Using Groups

A group is a collection of devices organized for managing activities within ZENworks Patch Management Server and contains a listing of all groups registered to it. Within the ZENworks Patch Management Server, groups are organized into nested groups. These related groups, called parent and child groups, allow you to maintain your ZENworks Patch Management Server with minimum maintenance.

The Groups browser lists the names of each custom parent group, the child groups, system groups, and custom groups. From this page you can access group information by expanding the group in the directory tree, or proceed to the *Group Information* page by clicking a group name.

The *Groups Page* displays information about a specific group. This information is classified into the following views:

- “Group Information”
- “Group Membership”
- “Device Membership”
- “Mandatory Baseline”
- “Device Group Vulnerabilities”
- “Group Inventory”
- “Device Group Deployments”
- “Policies”
- “Roles”
- “Dashboard”
- “Settings”



The *Groups* page is available by selecting Groups in the main navigation menu.



Figure 6.1 Groups Page

To View Groups

- 1. Select the **Groups** tab.
The *Groups* main page displays in the window.
- 2. In the directory tree select a **group type**.
The selected group’s information displays in the *Groups* window.
- 3. Select the function you need from the *View* drop-down list.
The applicable function displays in the *Groups* window.

To Search for a Group

The **Search** field can be used to search for groups by name, using a ‘Contains’ search condition. Wildcards are not supported.

- 1. Select the **Groups** tab.
The *Groups* main page displays in the window.
- 2. In the *Search* field, type your **search criteria**.
The directory tree automatically displays the results of the search.



Groups and the Directory Tree

You can view the list of groups using the directory tree. Click the expand icon to view **Custom** groups, **System** groups and **Directory Service** groups. By continuing to expand the tree, you can view the parent group and each child group associated with it. To display detailed group information, select the Group name. Use the **View** drop-down list to access the functions within the Groups page.

Parent and Child Groups

The nesting of groups enables the creation of hierarchical relationships that can be used to define inherited group membership. Using the policy inheritance feature, you can use parent groups to apply the same policies to multiple child groups.

A Parent and Child group relationship refers to a group that contains one or more group hierarchies underneath it. Each group must have one, and only one parent, however a parent group can have multiple children groups.

As a result of the parent-child relationship, there are hierarchies within groups:

- **Group Hierarchy** - Refers to the entire group hierarchy from the original to the deepest child group.
- **Parent Hierarchy** - Refers to the entire group hierarchy above a specific group.
- **Child Hierarchy** - Refers to the entire subordinate group hierarchy below a specific group
- **Inheritance** - Refers to the permissions a group has set. A group must have their inheritance settings set to **True** in order to inherit the settings of its parent.



Note: System and Directory Service group hierarchies cannot be modified.

Defining Groups

Groups can be categorized into the following classifications.

Table 6.1 Group Definitions






Icon	Group Type	Definition
	Parent System Groups	Devices identified in your network are automatically assigned a group membership based on their operating system. Not all operating systems may be present in your network. You cannot modify System Groups or their hierarchies.
	System Groups	



Table 6.1 Group Definitions

Icon	Group Type	Definition
	Parent Directory Service Groups	Created when an Agent submits a Directory Service Hierarchy that does not already exist on the Server. You cannot modify Directory Service groups or their hierarchies.
	Directory Service Groups	
	Custom Groups (Parent & Child)	Custom groups are created and managed by the user.

Group Information

Information displays general group-related information concerning the group's membership, hierarchy, policies, roles, mandatory baselines, and other settings.

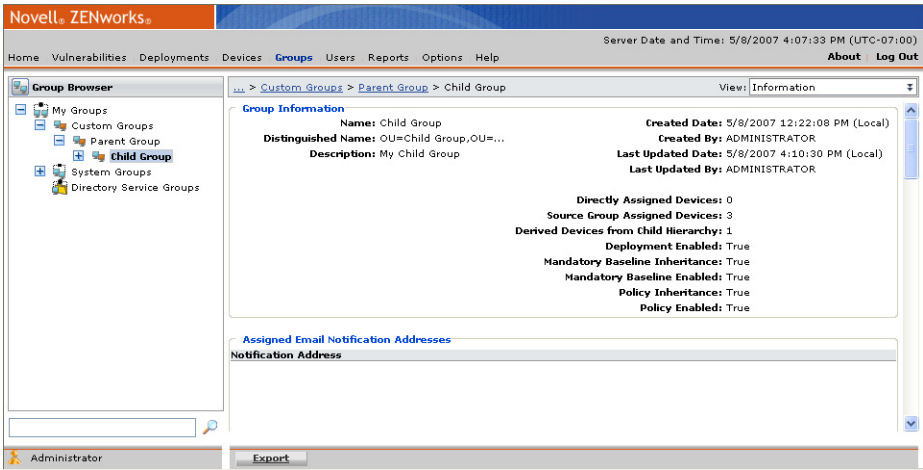


Figure 6.2 Group Information



The following table describes the Action Menu functions of the Information page.

Table 6.2 Group Information Action Menu

Action	Description
Export	Retrieves all page information and allows for saving to a.CSV file. See "Exporting Data" for more information.

Group Information Settings

The Information section of the Group Information view provides the following data:

Table 6.3 Information Fields

Field	Description
Name	The name of the group.
Distinguished Name	System-created name based upon the group's parent hierarchy.
Description	Description of the group.
Created Date	The date and time the group was created.
Created By	The user who created the group.
Last Updated Date	The date and time the group was last modified.
Last Updated By	The user who last modified the group.
Directly Assigned Devices	Number of devices assigned to the group. Does not include inherited devices.
Source Group Assigned Devices	The number of devices assigned to the source group. See "Working with Source Groups" for more information on Source Groups.
Derived Devices from Child Hierarchy	The number of devices inherited from child groups.
Deployment Enabled	When set to True, deployments can be created for the group.
Mandatory Baseline Inheritance	When set to True, Mandatory Baseline settings are inherited from the group's parent.
Mandatory Baseline Enabled:	When set to True, Mandatory Baseline deployments are created based upon the group's Mandatory Baseline configuration.
Policy Inheritance	When set to True, policy sets are inherited from the group's parent.
Policy Enabled	When set to True, policy sets can be assigned to the group.



Assigned Email Notification Addresses

The Email Notification settings of the Group Information tab provides the following data:

- **Notification Address** - The email addresses that will receive group specific notifications.

Assigned Child Groups

The *Group Section* lists the group’s direct children groups.

Table 6.4 Group Section

Field	Description
Type	Indicates whether a custom or system group.
Group Name	The name of the child group.
Distinguished Name	System-created name based upon the group’s parent hierarchy.
Group Description	Description of the Group.

Assigned Mandatory Baseline Items

The *Assigned Mandatory Baseline Items* lists the vulnerabilities defined in the group’s mandatory baseline.

Table 6.5 Mandatory Baseline Section

Field	Description
Name	The name of the vulnerability.
Impact	The vulnerability impact.
OS List	The list of applicable operating systems.



Note: The Mandatory Baseline items shown in the *Assigned Mandatory Baseline Items* section are only those baseline items that have been directly assigned to the group. The inherited Mandatory Baseline Items are shown under the *Groups - Mandatory Baseline* view.



Assigned Policy Sets

The *Assigned Policy Sets* section lists the policy sets assigned or inherited by the group.

Table 6.6 Assigned Policy Sets Section

Field	Description
Policy Set Name	The name of the policy set.
Assigned	Indicates if the policy set is assigned to or inherited by the group. A value of True indicates the policy is assigned directly to the group.

Resultant Policy Information

The *Resultant Policy Information* section displays the results of the assigned or inherited policy sets and provides the following data:

Table 6.7 Resultant Policy Section

Field	Description
Name	The name of the Policy.
Value	Indicates the policy value. When determining the policy value, inherited policies are overridden by the directly assigned policies, and conflict resolution rules are applied to the directly assigned (and conflicting policies).
Description	The description of the Policy.



Note: Only those policies that are directly assigned or inherited are displayed in the Group's Resultant Policy section. To see a complete listing of all policies assigned to an agent, refer to the "[Device Information Tab](#)".



Assigned Roles

The *Assigned Roles* section displays all the roles that have access to the group.

Table 6.8 Roles Information Section

Field	Description
Role Name	The name of the User Role that can access the group.
Source Group	The Name of the group assigned the role. If the Role Source does not contain a value, the role is assigned to the current group.
Assigned	Indicates if the role is assigned to or inherited by the group. A value of True indicates the role is assigned directly to the group.
Show or Hide Inherited	Lists or Hides Administrator, Guest, Manager, or Operator Role Group Names.

Group Membership

The Group Membership view allows the user to view the group’s direct child groups. The number of direct child groups display in the window.

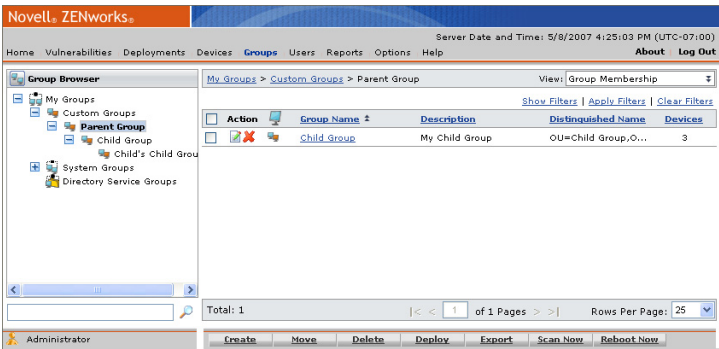


Figure 6.3 Group Membership



The *Group Membership* view displays the following group details.

Table 6.9 Group Membership View

Field	Description
Type	An Icon that indicates the group type. Refer to “Defining Groups” for details regarding the different group types.
Group Name	The name of the child group.
Description	Description of the Group.
Distinguished Name	System-created name based upon the group’s parent hierarchy.
Device	The number of devices assigned to this group.



Note: System and Directory Service groups cannot have their child group or device memberships modified. However, while the membership within System or Directory Service groups cannot be changed, their policies can.

The *Group Membership* page includes the following Action Menu functions. Some functions are common throughout the Groups page.

Table 6.10 Group Membership Action Menu

Button	Use to
Create	Create a new group. See “Creating a Group” for more information.
Move	Assigns a group to a new Parent Group. See “Moving a Group” for more information.
Delete	Remove a group. See “Deleting Groups” for more information.
Deploy	Deploy vulnerabilities to a device. See “Using the Deployment Wizard” for more information.
Export	Retrieves all page information and allows for saving to a CSV file. See “Exporting Data” for more information.
Scan Now	The Scan Now command prompts the DAU to immediately launch and check a group for vulnerabilities. See “Using the Scan Now Feature” for more information.
Reboot Now	The <i>Reboot Now</i> command lets you initiate the Reboot system task to all members of the selected group or groups. See “Rebooting Devices” for more information.



Creating a Group

Complete the following procedures to create a group.

To Create a Group

1. In the *Device Groups* page, select **Group Membership** from the drop-down list.
The *Group Membership* screen displays in the *Groups* window.
2. Click **Create**.
The *Group details* field displays in the *Group Membership* screen and auto-generates the Distinguished Name.
3. Type the **Group Name** for the Group.
4. [Optional] In the *Description* field, type a brief **description** about the group.
5. Click the **Save** icon next to the new Group.
The *Group* is saved to the list and is added to the Directory Tree.

Moving a Group

Complete the following steps to move a group to a new Parent Group.



Note: When moving a group, if the group is configured to inherit its policies, roles, or baseline settings, the group will inherit those values from the new parent group.

To Move a Group

1. Select a **Group** from the directory tree.
The selected Group is highlighted.
2. In the *Device Groups* page, select **Group Membership** from the drop-down list.
The *Group Membership* screen displays in the Groups window.

3. Click **Move**.
The *Move Groups* window opens.

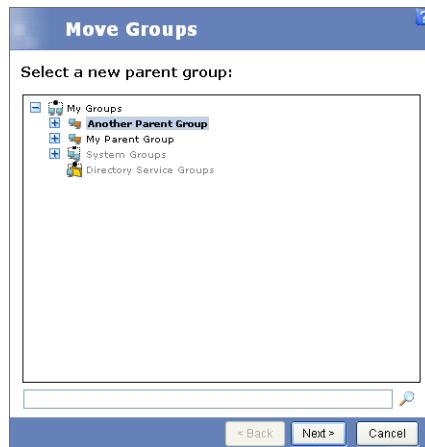


Figure 6.4 Move Groups window

4. Select a new **Parent Group**.
The *Parent Group* is highlighted.
5. Click **Next**.
The *Move Confirmation* window opens.



Figure 6.5 Move Confirmation window



6. Click **Finish**.
The Group is moved to the new Parent Group.

Deleting Groups

Complete the following steps to delete a single or multiple groups.



Note: Deleting a group does not prevent a device within that group from deploying, rebooting or scanning due to these tasks working at the device level.

To Delete a Group

1. In the *Device Groups* page, select **Group Membership** from the drop-down list.
The Group Membership screen displays in the Groups window.
2. Select a **Group** from the directory tree.
The selected Group is highlighted.
3. Click the **Delete** icon (next to the group to be deleted)
or
Select the checkbox to the left of the group(s) and click Delete on the Action Menu.
4. When the delete confirmation dialog displays, click **OK**.
The selected groups are deleted.



Warning: When a group is deleted, all of it's associated children are also deleted.

Editing Groups

Complete the following steps to edit a group.

To Edit a Group

1. Select a **Group** from the directory tree.
The selected Group and its Child Groups are listed in the Groups window.
2. In the *Device Groups* page, select **Group Membership** from the drop-down list.
The *Group Membership* screen displays in the Groups window.
3. From the list, select the **Group** to edit.
The Group is highlighted.
4. Click the **Edit** icon.
The fields become activated.
5. Edit the fields as needed.

6. Click **Save**.

The changes are saved to the group.



Note: You can only edit the group name and description within Group Membership. You must go to the Roles, Policies, Membership, Baseline, or Settings sections to make other edits.

Device Membership

The *Device Membership* view provides an interface for managing the devices assigned to a group.

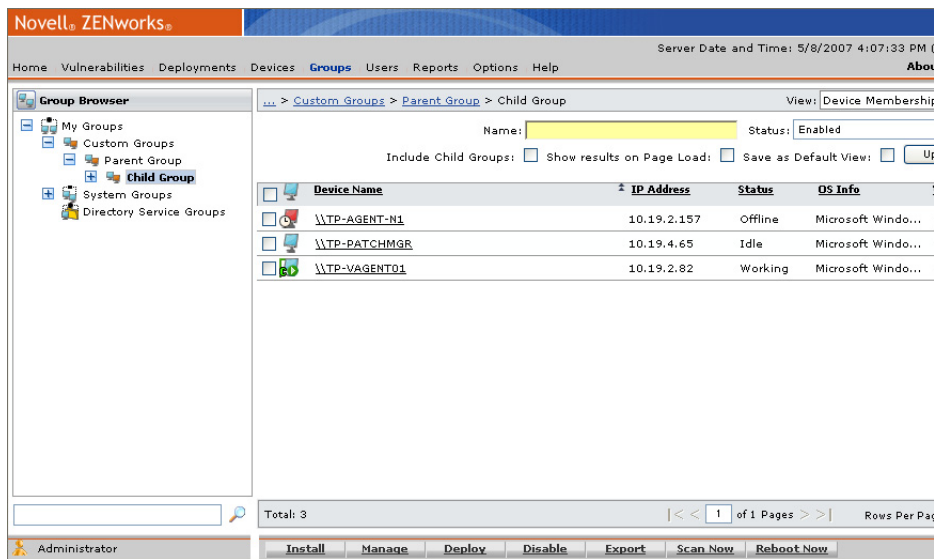


Figure 6.6 Device Membership

The Device Membership view displays the following device details.

Table 6.11 Device Membership View

Column	Description
Device Name	The name of the device as extracted from system data and inventory. Selecting the device name displays the Device Information page.
IP Address	The IP address of the device.



Table 6.11 Device Membership View

Column	Description
Status	The status of the device. Status values include: Detecting, Disabled, Idle, Offline, Sleeping, Working, and Unknown.
OS Info	Information about the operating system the device is running.
Version	The version number of the agent installed on the device.

The following table describes the functions of the Device Membership page.

Table 6.12 Device Membership Action Menu

Button	Use To
Install	Install an agent to a device. See "Installing an Agent" for more information.
Manage	Add or remove devices from a group. See "Managing Device Members" for more information.
Deploy	Deploy vulnerabilities to a device. See "Using the Deployment Wizard" for more information.
Disable	Disable a device within a group. See "To Disable a Device" for more information.
Export	Retrieves all page information and allows for saving to a CSV file. See "Exporting Data" for more information.
Scan Now	The Scan Now command prompts the DAU to immediately launch and check a group for vulnerabilities. See "Using the Scan Now Feature" for more information.
Reboot Now	The <i>Reboot Now</i> command lets you initiate the Reboot system task to all members of the selected group or groups. See "Rebooting Devices" for more information.

Managing Device Members

Complete the following steps to manage Devices within the Groups window.

Adding or Removing Device Members

- 1. In the *Device Groups* page, select **Device Membership** from the drop-down list.
The *Device Membership* screen displays in the Groups window
- 2. Select a **Group** from the directory tree.
The selected Group is highlighted.



3. Click **Manage** in the *Action Menu*.
ZENworks Patch Management Server displays the *Manage Devices* window.

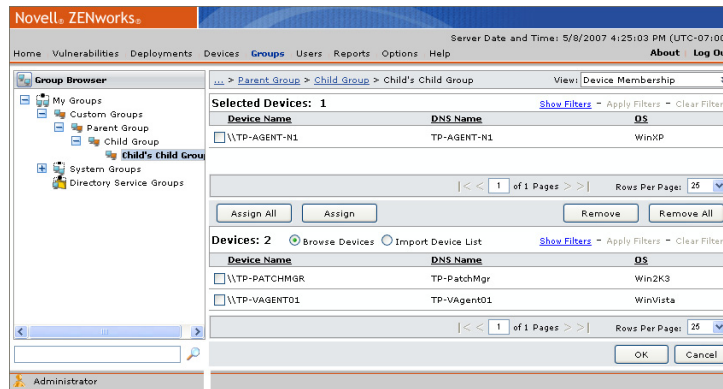


Figure 6.7 Manage Devices

4. To add devices:
 - a. Select the device or devices to include in the group from the *Devices* area.
 - b. Click **Assign**.
The selected devices move to the *Selected Devices* area.
 - c. Page to the next screen, if needed. If any more devices are selected, you must click **Assign** after each new page.
 - d. To assign all available devices, click **Assign All**.
The system displays the devices in the *Selected Devices* area.
 - e. Click **OK**.
The devices are saved to that group.
5. To remove devices:
 - a. Select the device or devices to remove from the *Selected Devices* area.
 - b. Click **Remove**.
The selected devices move to the *Devices* area.
 - c. Page to the next screen, if needed. If any more devices are selected, you must click **Remove** after each new page.
 - d. To remove all available devices, click **Remove All**.
The system displays the devices in the *Devices* area.



- e. Click **OK**.
The devices are removed from the group.
6. Click **Update View** to review the device assignment.

Enabling and Disabling Devices within a Group

Complete the following steps to enable or disable devices in a group.

To Disable a Device

1. Select a **Group** from the directory tree.
The selected Group is highlighted.
2. In the *Device Groups* page, select **Device Membership** from the drop-down list.
The *Device Membership* screen displays in the Groups window.
3. Select the options for the search, and click **Update View**.
The Devices that belong to the group display in the Groups window.
4. Locate and select the Device you want to disable.
5. In the *Action Menu*, click **Disable**.
The system disables the Device and displays it accordingly.



Warning: Disabling a device within a group is not group specific, and will disable the device everywhere.

Enabling a Device

1. Select a **Group** from the directory tree.
The selected *Group* is highlighted.
2. In the *Device Groups* page, select **Device Membership** from the drop-down list.
The *Device Membership* screen displays in the Groups window.
3. Select the options for the search, and click **Update View**.
The Devices that belong to the group display in the Groups window.
4. Locate and select the disabled device you want to enable.
5. In the *Action Menu*, click **Enable**.
ZENworks Patch Management Server enables the device.



Mandatory Baseline

A mandatory baseline is a minimum patch standard set by the administrator which all agents assigned the baseline under that ZENworks Patch Management Server must comply. If a device falls out of that minimum patched status, the mandatory baseline will automatically send out the patches necessary to keep the device secure.



Warning: Unless stringent *Hours of Operation* policies are in effect, **do not** apply mandatory baselines to groups of mission critical servers or other devices where unscheduled reboots would disrupt daily operations.

When a mandatory baseline is created or modified:

- ZENworks Patch Management Server automatically schedules a DAU task for all machines in that group
- Patch Management Server determines which devices are out of compliance following the DAU task
- Necessary packages are deployed as soon as possible for each machine.



Note: Some patches require both reboots **and** an Administrator level login to complete. If these or similar patches are added to a baseline, the deployment will stop until the login occurs.

This view provides an interface for managing Mandatory Baselines within a group.

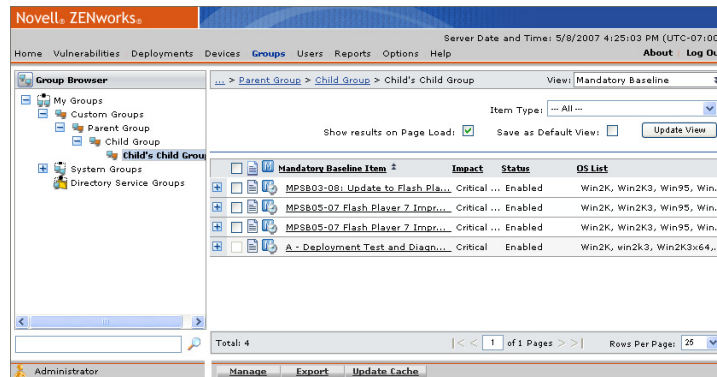


Figure 6.8 Mandatory Baseline



The following table includes descriptions of the Mandatory Baseline column definitions.

Table 6.13 Mandatory Baseline Column Definitions

Name	Definition
Expand (+)	Expanding, allows you to view the devices, their Operating System, and their mandatory baseline compliance.
Vulnerability Status	The status of a mandatory baseline is indicated by an icon. This column displays the status/type of each vulnerability assigned to the baseline. See "Vulnerability Status Icons" for a description of the Vulnerability Status icons.
Mandatory Baseline Compliance	Mandatory Baseline compliance is indicated by an icon. This column displays the compliance status of each vulnerability assigned to the baseline. See "Mandatory Baseline Item Compliance Icons" for a description of the compliance icons. Note: If the mandatory baseline fails to deploy more than twice, ZENworks Patch Management will record it as an error in the status column. However, this notification will only show in the Mandatory Baseline tab.
Mandatory Baseline Item	The name of a mandatory baseline item is presented in the <i>Mandatory Baseline Item</i> column. The mandatory baseline item is the same as the vulnerability name.
Impact	The impacts listed here mirror the impacts of the vulnerability.
OS List	The operating systems listed here mirror the operating systems that apply to the vulnerability (or package).



Note: You must keep the following rules in mind when working with Mandatory Baselines:

- Mandatory baseline inheritance indicates that a group’s devices (both inherited and assigned) are included by the parent group when evaluating it’s own baseline items and inheritance.
- If devices receive a mandatory baseline item via inheritance, the mandatory baseline item will also be displayed on the child group’s *Mandatory Baseline* page. However, the baseline items will be grayed-out to represent that the actual mandatory baseline assignment is done by a parent group.
- Disabling mandatory baseline deployments only applies to the mandatory baseline items that are directly assigned to the group, and will prevent those directly assigned items from being inherited by the group’s child hierarchy.
- Disabling mandatory baseline deployments does not disable the deployments created through mandatory baseline inheritance. Nor will disabling the baseline deployments, remove the baseline items from the group’s *Mandatory Baseline* view.









Viewing a Group Mandatory Baseline

1. Select a **Group** from the directory tree.
The selected Group is highlighted.
2. In the *Device Groups* page, select **Mandatory Baseline** from the drop-down list.
The *Mandatory Baseline* screen displays in the Groups window.
3. In the *Item Type* field, select the **Item Type**.
4. Click **Update View**.
The *Groups* page displays the associated Mandatory Baselines.

Vulnerability Status Icons

The following table includes descriptions of the Vulnerability status icons.

Table 6.14 Vulnerability Status Icons and Descriptions

New	Current	Beta	Status Description
			Active vulnerability.
			Vulnerability has been disabled.

Mandatory Baseline Item Compliance Icons

Compliance status for the mandatory baseline item relative to groups include:

Table 6.15 Mandatory Baseline Item Compliance Icons and Descriptions






Status	Description
	At least one member of this group is either detecting, obtaining the Package, Waiting on detection, or in a Deployment not started state
	At least one member of this group is deploying the package
	All of the applicable members of this group are disabled.



Table 6.15 Mandatory Baseline Item Compliance Icons and Descriptions

Status	Description
	All of the members of this group are either not applicable or in compliance for this package (Some can also be disabled)
	At least one member of this group is out of compliance and has had an error when attempting to deploy. Specific information about the type of error will display in the mouse over text.

The following table describes the functions available on the Mandatory Baseline Action Menu.

Table 6.16 Mandatory Baseline Action Menu

Button	Use To
Manage	Add or remove vulnerabilities from the Mandatory Baseline.
Export	Retrieves all page information and allows for saving to a.CSV file. See "Exporting Data" for more information.
Update Cache	Downloads packages and vulnerabilities required by the device. See "Updating the Cache" for more information.



Managing Mandatory Baselines

Complete the following steps to manage Mandatory Baselines within a group.

To Manage a Mandatory Baseline

1. Click **Manage**.

ZENworks Patch Management Server retrieves all known vulnerabilities and displays them in the Groups window.

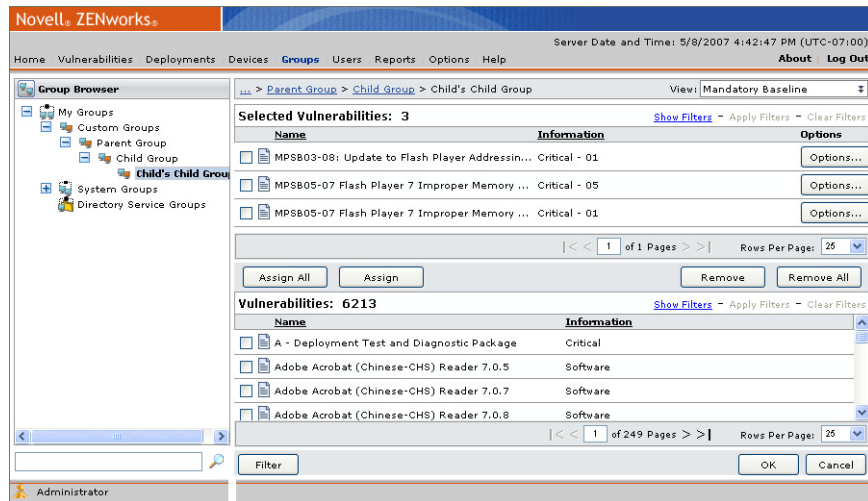


Figure 6.9 Assign Vulnerabilities

2. To add vulnerabilities to the Mandatory Baseline:

a. Select the vulnerabilities to include in the baseline from the *Vulnerabilities* area.

b. Click **Assign**.

The selected vulnerabilities move to the *Selected Vulnerabilities* area.

c. Page to the next screen, if needed. If any more vulnerabilities are selected, you must click **Assign** after each new page.

d. To assign all available vulnerabilities, click **Assign All**.

The system displays the vulnerabilities in the *Selected Vulnerabilities* area.

3. To remove vulnerabilities from the Mandatory Baseline:

a. Select the vulnerabilities to remove from the *Selected Vulnerabilities* area.

b. Click **Remove**.

The selected vulnerabilities move to the *Vulnerabilities* area.



- c. Page to the next screen, if needed. If any more vulnerabilities are selected, you must click **Remove** after each new page.
 - d. To remove all vulnerabilities, click **Remove All**.
The system displays the vulnerabilities in the *Vulnerabilities* area.
4. Click **OK**.
The vulnerabilities are added (or removed) to the mandatory baseline.

Using the Filter Functions to Select Vulnerabilities

1. In the *Vulnerabilities* or *Selected Vulnerabilities* area, select **Show Filters**.
The filters display in the window.
2. Type the **filter criteria** in the *Name* and/or the *Information* fields.
3. Click **Apply Filters**.
The Vulnerabilities are filtered and the results display.
4. Select **Clear Filters** to start another search.

Showing Only the Required Vulnerabilities

1. Click **Filter**.
The *Needed Detection Vulnerabilities* window opens.
2. Select the vulnerabilities as needed.



Note: Only patch vulnerabilities, that are both applicable and un-patched (based upon the current group membership), display in the *Needed Detection Vulnerabilities* window. However, the *Mandatory Baseline Management* window displays all vulnerabilities, that do not require a manual installation, regardless of applicability or patch status.

3. Click **OK**.
The *Needed Detection Vulnerabilities* screen closes and the patches display in the *Selected Vulnerabilities* window
4. Selecting Mandatory Baseline Deployment Options
5. In the list of selected vulnerabilities, select **Options**.

6. The *Package Deployment Options* window opens.

Figure 6.10 Package Deployment Options screen

7. In the *Deployment Options For* field, confirm the operating system selection.



Note: If the Deployment Options For field has multiple Operating System groupings, you must set the Package Deployment Options for each OS grouping.

8. In *Distribution Options*, select **Concurrent** and the **device amount** or **Consecutive**.
9. If needed, type additional **Deployment Flags**.
10. Set the desired **Deployment Options**.

Table 6.17 Deployment Options

Select	To
Do not notify users of this deployment	Deploy the mandatory baseline package without notifying the users of the device.
Notify Users of this deployment	Deploy the mandatory baseline package and notify the users of the device. When this option is selected the remaining options in Deployment Options become active.



Table 6.17 Deployment Options

Select	To
Message	Display a message to notify the users regarding the deployment.
Use Policies	Selecting this option indicates that deployments will use the agent policies to define deployment notification settings.
Allow user to cancel	Permits the recipient of the deployment to cancel.
Allow user to snooze	Permits the recipient of the deployment to delay the deployment.
Notification on top	Displays the Agent Deployment window on top when notifying of a deployment.
Deploy within	Sets the time frame for the deployment. If snooze is enabled, this value is also maximum deployment snooze duration.

11. Set the desired **Reboot Options**.

Table 6.18 Reboot Options

Select	To
Do not notify users of this reboot	Reboot the mandatory baseline package without notifying the users of the device.
Notify Users of this reboot	Reboot the mandatory baseline package and notify the users of the reboot. When this option is selected the remaining options in Deployment Options become active.
Message	Display a message to notify the users regarding the reboot.
Use Policies	Selecting this option indicates that deployments will use the agent policies to define reboot notification settings.
Allow user to cancel	Permits the recipient of the deployment to cancel the reboot.
Allow user to snooze	Permits the recipient of the deployment to delay the reboot.
Notification on top	Displays the Agent Deployment window on top when notifying of a deployment requiring a reboot.
Deploy within	Sets the time frame for the reboot after a deployment. If snooze is enabled, this value is also maximum deployment snooze duration.

12. Click **OK**.
The *Package Deployment Options* screen closes.



Removing Deployments Created By Mandatory Baselines

The following section describes the two different methods for stopping a Mandatory Baseline deployment.



Note: If the Mandatory Baseline is still applied the deployment(s) will be recreated.

To Remove a Mandatory Baseline Deployment from a Group

1. In the *Groups* page, select the group from the Directory Tree.
2. Select **Deployments** from the drop-down list.
3. Select the mandatory baseline deployment to delete.
4. Click **Delete**.

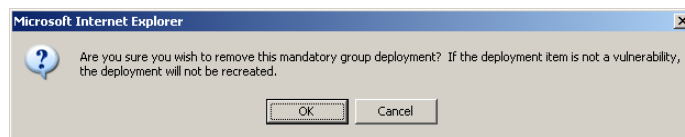


Figure 6.11 Remove Deployment

5. Click **OK** to acknowledge the warning message and remove the deployment(s).

To Stop Deployment for Specific Devices

1. In the *Groups* page, select the group to disable from the Directory Tree.
2. Select **Deployments** from the drop-down list.
3. Click the appropriate **Name** link, opening the **Deployment Details** page.
4. Click **Disable** to disable the deployment for the selected computer.



Device Group Vulnerabilities

The *Vulnerabilities menu item* displays the vulnerabilities that have been assigned to the members of the group and the status of each vulnerability for the devices. This view is the same as the Vulnerability Summary view, but only displays the vulnerabilities applicable to the member devices of the selected group.

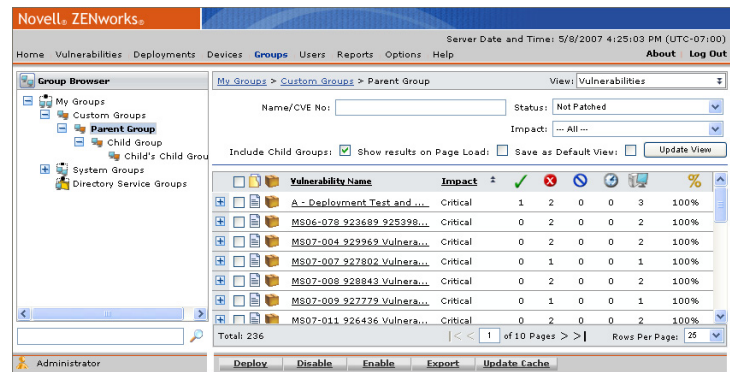


Figure 6.12 Vulnerabilities

The *Vulnerabilities* view displays the following group details.

Table 6.19 Vulnerabilities View Columns

Column	Description
Vulnerability Status and Type Icons	Refer to “ Vulnerability Status & Types ” for a description of the icons.
Vulnerability Package Cache Status and Type Icon	Refer to “ Vulnerability Package Cache Status & Type ” for a description of the icons.
Vulnerability Name	The name of the vulnerability. Typically includes the vendor, specific application, and version information.
Impact	Describes the level of requirement for the vulnerability. Refer to “ Vulnerability Impacts ” for additional details.
Vulnerability Statistics Icons	Refer to “ Vulnerability Statistics ” for a description of the icons.



The following table describes the functions of the Vulnerabilities Action Menu

Table 6.20 Groups Vulnerabilities Action Menu

Select	To
Deploy	Create a group deployment using the deployment wizard. See "Using the Deployment Wizard" for additional information
Disable	Disable a vulnerability. See "To Disable a Vulnerability" for more information.
Enable	Enable a vulnerability. See "Disabling and Enabling Vulnerabilities" for more information.
Export	Retrieves all page information and allows for saving to a.CSV file. See "Exporting Data" for more information.
Update Cache	Downloads (or re-downloads) the selected packages and vulnerabilities. See "Updating the Cache" for more information.

Enabling Vulnerabilities within a Group

You can enable vulnerabilities. Enabled vulnerabilities are noted with the enabled status icon.

Enabling Vulnerabilities in a Group

1. Select a **Group** from the directory tree.
The selected *Group* is highlighted.
2. In the *Groups* page, select **Vulnerabilities** from the drop-down list.
The *Vulnerabilities* screen displays in the Groups window.
3. Select the required parameters, and click **Update View**.
The available *Vulnerabilities* display in the *Groups* window.
4. Select a disabled vulnerability.
5. Click **Enable** in the *Action Menu*.
ZENworks Patch Management Server enables the vulnerability for the selected group.



Disabling Vulnerabilities within a Group

You can disable all vulnerabilities. Disabled vulnerabilities move to the bottom of the list and are noted with the disabled status icon.

Disabling Vulnerabilities in a Group

1. Select a **Group** from the directory tree.
The selected *Group* is highlighted.
2. In the *Groups* page, select **Vulnerabilities** from the drop-down list.
The *Vulnerabilities* screen displays in the *Groups* window.
3. Select the required parameters, and click **Update View**.
The available *Vulnerabilities* display in the *Groups* window.
4. Click **Disable** in the *Action Menu*.
ZENworks Patch Management Server disables the vulnerability for the selected group.

Group Inventory

This view displays the software, hardware, operating systems and services that were detected on the devices in the group. This view is the same as the Inventory Summary view, but only displays the inventory of the selected group. See “Using the Inventory Tab” for additional details.

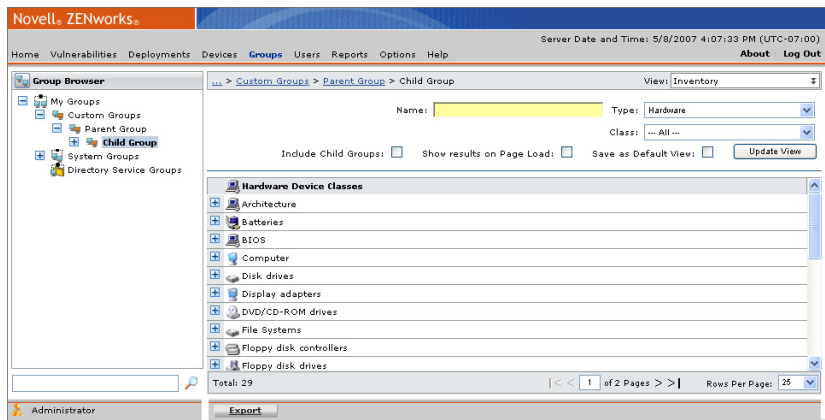


Figure 6.13 Inventory (software)



The following table describes the functions of the Inventory page

Table 6.21 Group Inventory Action Menu

Action	Description
Export	Retrieves all page information and allows for saving to a.CSV file. See “Exporting Data” for more information.

Device Group Deployments

This view displays the deployments that the selected group has been assigned. This view is the same as the Deployment Summary view, but displays only deployments for the selected group. See [“Using the Deployment Pages”](#) for additional details.

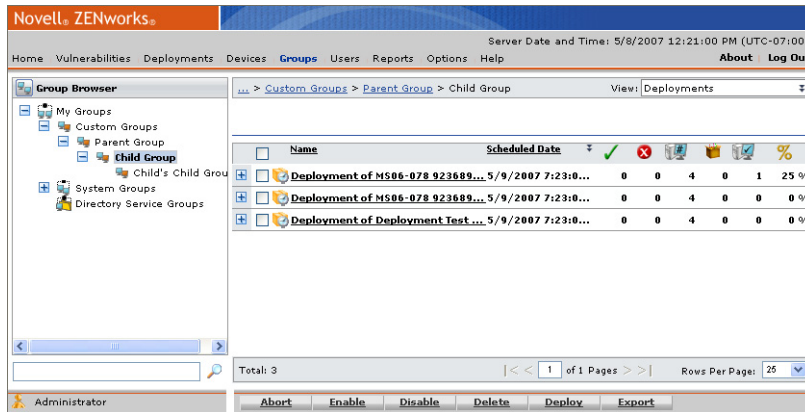


Figure 6.14 Group Deployments



Note: This view does not display the deployments for each member, only the deployments that the group has been assigned.



The following table describes the functions of the Deployments page

Table 6.22 Group Deployments Tab - Page Functions

Button	Function
Abort	Cancels the deployment for any devices which have not already received the deployment package. For additional information refer to "Aborting Deployments".
Enable	Enables the selected disabled deployment. For additional information refer to "Enabling Deployments".
Disable	Disables the selected enabled deployment. For additional information refer to "Disabling Deployments".
Delete	Removes the deployment from your ZENworks Patch Management Server. For additional information refer to "Deleting Deployments".
Deploy	Re-deploys the selected packages. For additional information refer to "Using the Deployment Wizard".
Export	The Export button allows you to export subscription data to a comma separated value (.CSV) file.

Deploying to a Group

Deploying to a group of selected devices is a key function of the ZENworks Patch Management Server. Deployments are initiated by clicking **Deploy** and completing the *Deployment Wizard*. The *Deployment Wizard* provides step-by-step instructions for defining and pushing deployments out to the protected devices in the network. Refer to "Using the Deployment Wizard" for additional information



Policies

This view displays the policy sets that the selected group has been assigned. For more information on policy sets and policy conflict resolution, see [“Customizing and Administering Agent Policy Sets”](#).

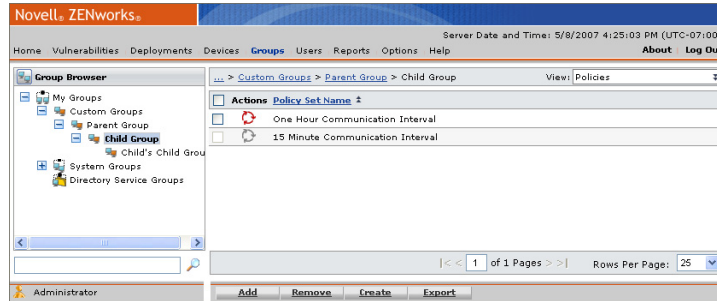


Figure 6.15 Policies page

Adding a Policy to a Group

Complete the following steps to add an already established policy set to a group.

To Add a Policy

1. Select a **Group** from the directory tree.
The selected *Group* is highlighted and displays any associated policies.
2. In the *Groups* page, select **Policies** from the drop-down list.
The *Policies* screen displays in the Groups window.
3. Click **Add**.
The *Policy Set Name* drop-down list displays in the Groups window.

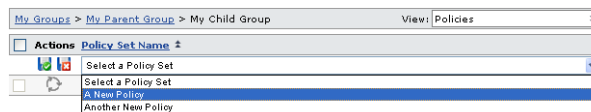


Figure 6.16 Add a Policy Set



- 4. Select a **Policy** from the drop-down list.
- 5. Click the **Save** icon.
The *Policy Set* is saved and associated with the group.

Removing a Policy from a Group

Complete the following steps to remove an already established policy set from a group.



Note: You cannot remove inherited policy sets, you must change the group’s policy inheritance setting. See “[Working with the Group Settings](#)” for additional details regarding the modification of group inheritance.

To Remove a Policy Set from a Group

- 1. Select a **Group** from the directory tree.
The selected *Group* is highlighted and displays any associated policies.
- 2. In the *Groups* page, select **Policies** from the drop-down list.
The *Policies* screen displays in the Groups window.

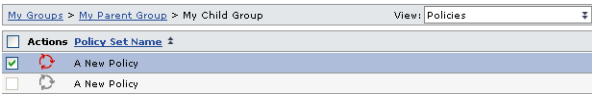


Figure 6.17 Remove a Policy Set

- 3. Select a **Policy** to remove.
- 4. Click **Remove** in the *Action Menu* or click the **Remove** icon.
A confirmation window displays prompting the removal.
- 5. Click **OK**.
The *Policy Set* is no longer associated with the group.

The following table describes the functions of the Policies page.

Table 6.23 Group Policy Action Menu

Action	Use To
Add	Select and add an already established policy set to a group.
Remove	Remove a policy set from a group.
Create	Create a new policy. See “ Creating a Policy Set ” for more information.
Export	Retrieves all page information and allows for saving to a.CSV file. See “ Exporting Data ” .



Roles

This view displays the roles that have been assigned to the selected group.



Figure 6.18 Roles page

The Roles view displays the following role details.

Table 6.24 Roles View Columns

Column	Description
Role Name	The name of the User Role.
Source Group	The name of the group assigned the User Role.

The following table describes the functions of the Roles page.

Table 6.25 Group Roles Action Menu

Action	Use To
Add	Select to add an already established role to the group.
Remove	Remove a role from the group.
Create	Create a new role. See "Creating User Roles" .
Export	Retrieves all page information and allows for saving to a CSV file. See "Exporting Data" .

Adding a Role to a Group

Complete the following steps to add an established role to a group.



To Add a Role

- 1. Select a **Group** from the directory tree.
The selected Group is highlighted and displays any associated policies.
- 2. In the *Groups* page, select **Roles** from the drop-down list.
The *Roles* screen displays in the Groups window.
- 3. Click **Add**.
The *Select a Role* drop-down list displays in the Groups window.

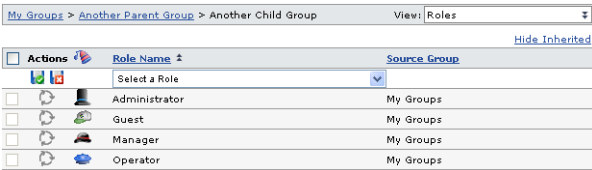


Figure 6.19 Add a Role

- 4. Select a **Role** from the drop-down list.
- 5. Click **Save**.
The Role is saved and associated with the group.

Removing a Role from a Group

Complete the following steps to remove an established role from a group.

To Remove a Role

- 1. Select a **Group** from the directory tree.
The selected Group is highlighted
- 2. In the *Groups* page, select **Roles** from the drop-down list.
The *Roles* screen displays in the Groups window and displays the group’s associated roles.

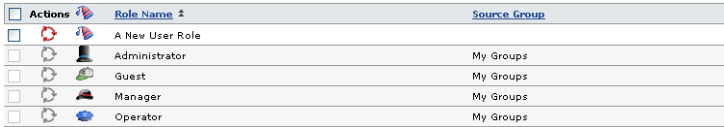


Figure 6.20 Remove a Role

- 3. Select a **Role** to remove.
- 4. Click **Remove** or the **Remove icon**.
A confirmation window displays prompting the removal.



5. Click **OK**.

The Role is removed and no longer associated with the group.

Dashboard

The Group *Dashboard* view consists of a series of charts providing a current view of the selected group. These charts are generated based on the latest data available and include only those devices that are members of the current group, its child hierarchy, and their applicable vulnerabilities and packages.

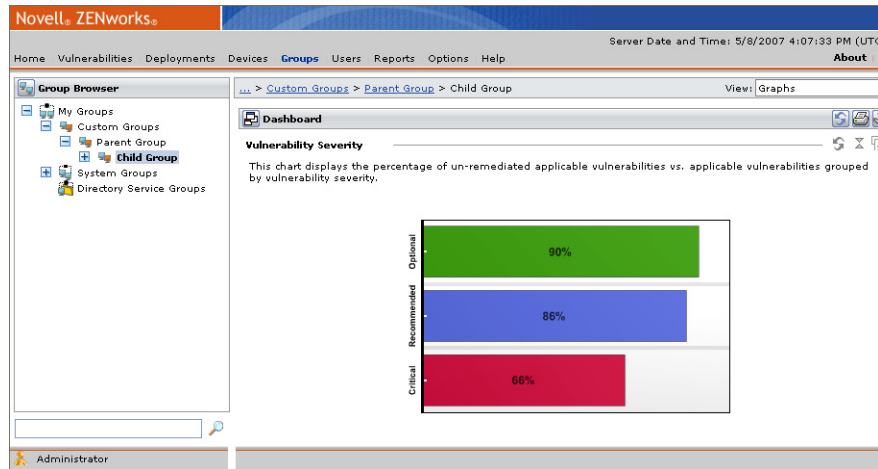


Figure 6.21 Graphs page



Note: The charts displayed on the *Group Dashboard* view include data from the selected group's child hierarchy. Modifications to the visible charts and their display settings will apply to all groups.

The following table describes all of the available charts.

Table 6.26 Dashboard Charts

Chart	Description
Vulnerability Severity	This chart displays the percentage of un-remediated applicable vulnerabilities vs. applicable vulnerabilities grouped by vulnerability severity.
Vulnerability Severity by Device	This chart displays the percentage of un-remediated devices vs. applicable devices grouped by vulnerability severity.



Table 6.26 Dashboard Charts

Chart	Description
Scheduled Remediation	This chart displays the percentage of un-remediated devices with a scheduled remediation vs. un-remediated devices grouped by vulnerability severity.
Mandatory Baseline Compliance	This chart displays the percentage of devices grouped by mandatory baseline compliance.
Incomplete Deployments	This chart displays the percentage of incomplete deployments grouped by the deployments percentage complete.
Agent Status	This chart displays the percentage of agents grouped by status.
Time since last DAU	This chart displays the percentage of available or working devices grouped by time since the last successful Discover Applicable Updates task.
Offline Agents	This chart displays the percentage of offline agents grouped by the time offline.

Use the following table to define your settings when viewing the graphs dashboard.

Table 6.27 Dashboard Settings and Behavior Icons














Icon	Function
	Opens the dashboard settings window.
	Opens a printable version of the currently displayed charts.
	Refresh all of the displayed charts.
	Display the chart descriptions on the dashboard.
	Do not display the chart descriptions on the dashboard.
	View the charts in one column.
	View the charts in two columns.
	Save the dashboard settings

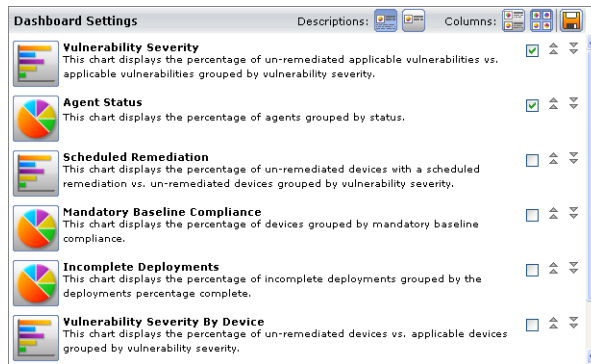


Table 6.27 Dashboard Settings and Behavior Icons

Icon	Function
	Move the selected chart up one level.
	Move the selected chart down one level.
	Refresh the selected chart.
	Minimize the chart.
	Hide the chart from view.

To Add a Graph to the Dashboard

1. Click the **Dashboard Settings** icon.
The *Dashboard Settings* drop-down list opens.

**Figure 6.22** Dashboard Settings Window

2. Select the graphs you want to view by checking the box next to the graphs you want to add.
3. Move the graphs up or down according to your priorities.
4. Select a one or two column width view from *Columns*.
5. Using the *Descriptions* buttons, choose to *Show* or *Hide* the Chart Descriptions.
6. Click **Save**.
Your graph setting selections are saved and displayed in the Dashboard.



To Remove a Graph from the Dashboard

- 1. Click the **Dashboard Settings** icon.
The *Dashboard Settings* drop-down list opens.
- 2. Deselect the checkbox next to the graph(s) you want to remove. Click *Save Dashboard Settings*.
Click **Save** and the graph(s) is removed from the Dashboard window.

Settings

The Settings page displays the default group settings.

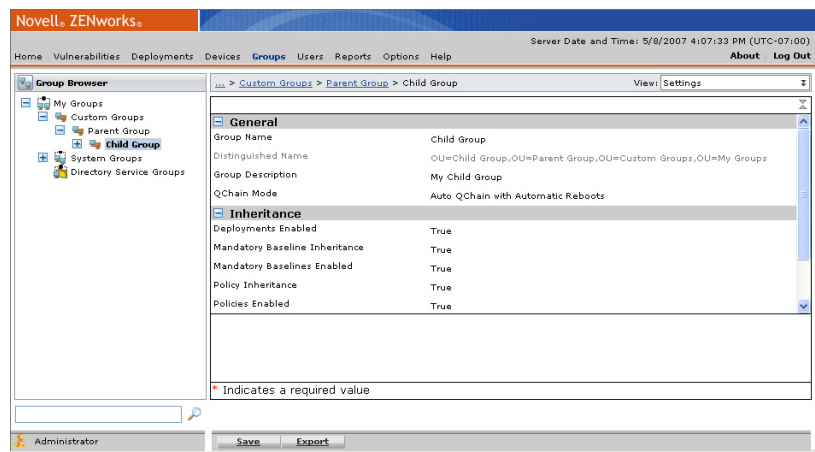


Figure 6.23 Group Settings

The following table describes the functions of the Settings page.

Table 6.28 Settings Action Menu

Action	Use To
Save	Saves the settings defined in the page.
Export	Retrieves all page information and allows for saving to a.CSV file. Go to "Exporting Data" for more information.

Working with the Group Settings

If different settings are required, you can edit the default settings for a group.



To Edit Group Settings

1. In the **General** area, edit the following fields as necessary.

Table 6.29 General

Field	Description
Group Name	The user-defined group name.
Distinguished Name	A system-defined group name that represents the group's parent hierarchy.
Group Description	The user-defined description of the group.
Chain Mode	A user-defined setting indicating chain behavior during Mandatory Baseline Deployments.
Deployments Enabled	A user-defined setting indicating whether deployments may be created for the group. A True value will allow users to create deployments for the group.



Note: The **Deployments Enabled** field only impacts the ability to **create** deployments for a group. Deployments created prior to disabling group deployments will still occur as scheduled. Additionally, any deployments created for the device will occur as scheduled.

2. In the *Mandatory Baseline* Area, edit the following fields as necessary.

Table 6.30 Mandatory Baseline Settings

Field	Description
Mandatory Baseline Inheritance	A user-defined setting indicating whether the group inherits the policies assigned to the group's parent hierarchy. A True value will set the group to inherit its parent hierarchy's Mandatory Baseline settings.
Mandatory Baseline Enabled	A user-defined setting indicating whether Mandatory Baselines may be assigned to the group. A True value will allow users to create Mandatory Baseline deployments for the group.



3. In the *Policy* Area, edit the following fields as necessary.

Table 6.31 Policy Settings

Field	Description
Policy Inheritance	A user-defined setting indicating whether the group inherits the policies assigned to the group's parent hierarchy. A True value will set the group to inherit it's parent hierarchy's policy settings.
Policies Enabled	A user-defined setting indicating whether policies may be assigned to the group. A True value will allow users to assign policies directly to the group.

4. In the *Other* area, edit the following fields as necessary.

Table 6.32 Other Settings

Field	Use To
Email Address	A user-defined email addresses to which notifications are sent regarding events impacting the group.
Source Groups	A user-defined group or groups whose agents are dynamically assigned to the group. See "Working with Source Groups" for additional details regarding Source Groups.

5. Click **Save**.
The new settings are saved and applied to the group.

Working with Source Groups

When a custom group is created, you can assign it a source group. When the source group is modified, your custom group is automatically updated as well.



Note: Source groups can only be assigned to custom groups.

To Assign a Source Group to a Custom Group

1. Select a **Custom Group** from the directory tree.
The selected Group is highlighted and displays its settings.
2. In the *Groups* page, select **Settings** from the drop-down list.
The *Settings* screen displays in the Groups window.



3. In the *Other* area, select **Modify** in the *Source Groups* field.
The *Edit Source Groups* window opens.

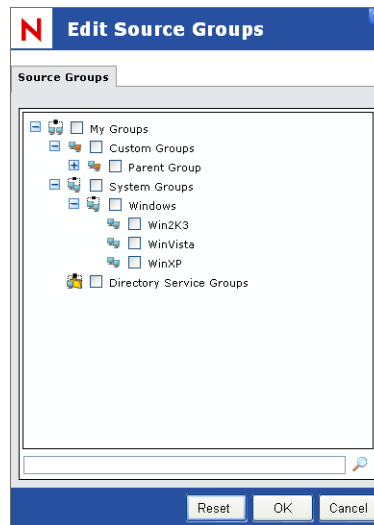


Figure 6.24 Edit Source Groups

4. Expand the **Source Group tree** or use **Search** to locate the group you require as a source.
5. Select the groups you require as a source.



Note: A Source Group's inherited devices will always be included regardless of whether you select the Source Group's child groups. Additionally, if the Source Group (or any of its child groups) has a Source Group, those devices will also be included.

6. Click **Save**.
The custom group now will use the selected groups as its source. As new agents are added to (or removed from) the source group, they will also be added to the custom group.





7 Reporting

This chapter provides information on defining and generating reports in ZENworks Patch Management. Reports provide a way to view the current patch status and network vulnerabilities for internal reporting, and briefing management.

In this Chapter

- “About Reports”
- “Available Reports”
- “Working with Reports”

About Reports

Reports cover a range of indicators and can be customized to cover a general category (devices, packages) or focus on specific elements of your network (for example, vulnerabilities specific to a particular vendor). Targeted reporting is done through selecting an appropriate report type, defining the parameters of a report, and by customizing report criteria through the Search feature.

Available Reports Page

The main page from which you select which report to display from a list of available reports.

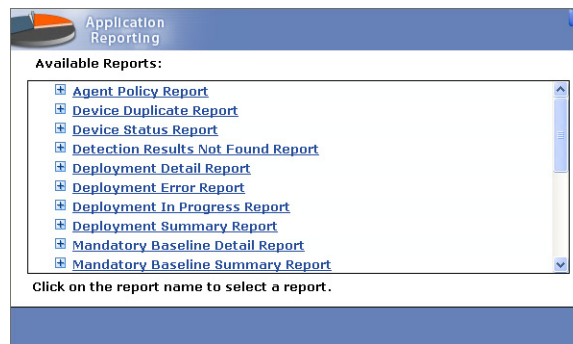


Figure 7.1 Available Reports



Report Parameters Page

From the Available Reports List, selecting **Device Status Report** displays the *Application Reporting Device Status Report Parameters* page. The report definition page where you define the data to include in the report.

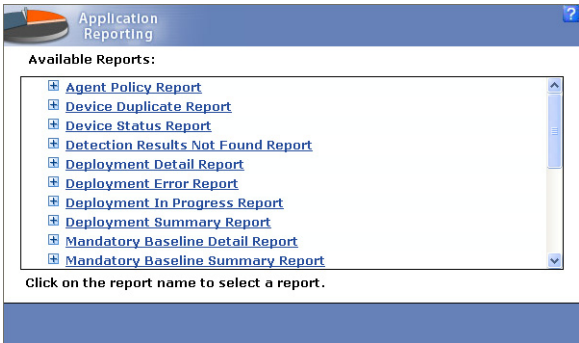


Figure 7.2 Report Parameters Page

Report Parameters List

The following table describes the parameters used when using reports. Each report includes at least one parameter.

Table 7.1 Report Parameters

Select	To
Devices	Choose from a list of all available devices that you have permission to view. All available devices are shown in the <i>Available Devices</i> list. Click a single device or use the CTRL and SHIFT keys to select multiple devices. Note: All access is limited to users with access to all Devices or with the Enable Administrative Reports access rights.
Groups	Choose from a list of all available groups within Patch Management Server that you have permission to view. All groups are shown in the <i>Available Groups</i> list and all of the devices belonging to the selected group and it's child groups are included in the report. Click a single group or use the CTRL and SHIFT keys to select multiple groups. Note: All access is limited to users with access to all Groups or with the Enable Administrative Reports access rights.
Deployments	Choose a deployment from a list of all available deployment names. All available deployments are shown in the <i>Available Deployments</i> list. Click a single deployment or use the CTRL and SHIFT keys to select multiple deployments.




Table 7.1 Report Parameters

Select	To
Packages	Choose from a list of all available packages. All available packages are shown in the <i>Available Packages</i> list. Click a package name or use the CTRL and SHIFT keys to select multiple packages.
Vulnerabilities	Choose from a list of all available vulnerabilities identified by Patch Management Server. All vulnerabilities are shown in the <i>Available Vulnerabilities</i> list. Click a vulnerability name or use the CTRL and SHIFT keys to select multiple vulnerabilities.
Date Range	Choose from a list of all deployments that occur within the selected dates. You can also display the time in 12 or 24 hour format and as Patch Management Server local time or UTC time.

Reports Results Page

Make your selection(s) and click **Generate**. This page presents the results of the report once it is generated.



Application
Reporting

Device Status Report

Report created: 4/29/2007 1:12:32 PM

Device Name	DNS Name	IP Address	OS Name	OS Build No	OS Service Pack	Agent Version	Last Contact Date	Patchable Status	Group List
\\TP-MYSERVER	TP-MyServer	10.19.1.41	Microsoft Windows Server 2003, Standard Edition	3790	Service Pack 1	6.4.0.213	4/29/2007 1:05:30 PM	0	My Child Group, My Groups, My Parent Group, System Groups, Win2K3, Windows

< < 1 of 1 Pages > >

Rows Per Page: 25

Display dates as:

☒ Local Time ☐ UTC Time

Export

Comma-separated values (CSV)

Printer-Friendly

Close

Figure 7.3 Report Page example

Viewing Reports

ZENworks Patch Management provides several pre-defined reports designed to provide a comprehensive view of your computing environment in respect to patch management activities.

To Generate a Report

- 1. In the *Main Menu*, select **Reports**.
ZENworks Patch Management opens the **Available Reports** screen in a new browser window.

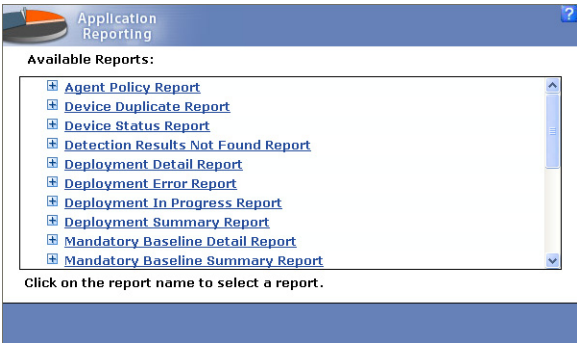


Figure 7.4 Available Reports

- 2. Select the report to generate in the *Available Reports* page.
The corresponding *Report Parameters* page opens.

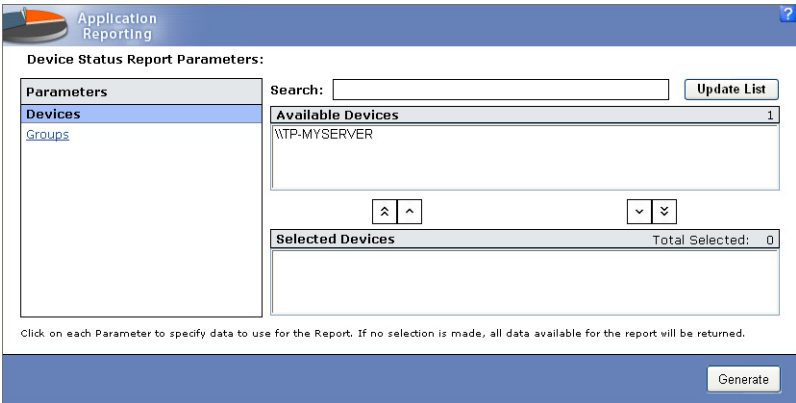


Figure 7.5 Report Parameters



3. In the *Report Parameters* page, define the report contents and organization by selecting parameters.
 - a. In the *Parameters* box, select the parameter to use in defining the report contents from the list of available parameters. This is the left-side pane of the page.
 - b. In the *Available Devices* (or *Available Options*) box, select from the list of available parameters to include (Devices, Groups, Vulnerabilities) by selecting with your cursor. Select multiple items using the **CTRL** or **SHIFT** keys.



Note: You may choose not to define any Parameters; in this case, all applicable data for the report Parameters will be returned.

4. With the desired items selected, click the **Include** arrow.
5. To include all available items, click the **Include All** arrow.
6. Verify the contents of the *Selected Options* box.
7. Remove items by clicking the **Remove** arrow.
8. Or, to include all available items, click the **Remove All** arrow.
9. Click **Generate** to create the report.
The *Report Results* screen opens with the retrieved information.

Working with Reports

The following section explains how to use the functions to create, view, and use report data.

- “Searching Within Reports”
- “Displaying Time and Date in Reports”
- “Exporting Reports”
- “Viewing Printable Data in Reports”

Searching Within Reports

The search feature provides standard searching on a word matching basis (exact and partial matching). The search is conducted against the Patch Management Server database. Some general rules include:

- Search does not support the use of Boolean search commands (AND, OR, NOT, nesting (), etc.)
- Search terms are **not** case sensitive. All letters are treated as lower case. For example, the search term *WIN* is treated the same as *win* and will generate the same results
- To show all results, remove any content from the *Search* text box (leave blank).
- To search, enter the search term in the *Search* text box and click **Update List**. To return to the pre-search results, click from the list of available options in the *Parameters* list box.



Displaying Time and Date in Reports

For reports that generate date range data, you have two options for displaying date/time information;

- Use the Patch Management Server Local time (this is the date and time established by the ZENworks Patch Management Server).
- Use the ZENworks Patch Management Server UTC (Coordinated Universal Time) time



Note: Coordinated Universal Time or UTC, is often referred to as Universal Time, Zulu time or Greenwich Mean Time (GMT).

Exporting Reports

Once the report is created, you have the option of switching to a printable view for printing, or exporting the report into another file format.

Reports are presented in standard HTML and can be exported into several file formats for your convenience.

- Comma Separated Values (CSV)
- Microsoft Excel Worksheet (XLS)
- XML Document

The Export command and drop-down list is presented at the bottom of the page.



Note: All data results will export, not just selected results. However, some of the data may not import into a readable format.

Viewing Printable Data in Reports

An HTML version of the generated report can be previewed for printing.

To Print a Report

1. Generate a report.
The completed report page displays in the window.
2. Select **Printer Friendly**.
The Report's results page refreshes with the data in print preview mode.
3. Select **Send to Printer**.
The file is sent to your installed printer.



Note: If you have not established printer connectivity, click *Yes* when the Print dialog box appears and use the *Add Printer Wizard* to select and connect your printer.

Available Reports

ZENworks Patch Management Server provides several pre-defined reports designed to provide a comprehensive view of the application environment in respect to patch management activities. In many cases there is a detail and summary report for each specific function.

The following reports are available:

- "Agent Policy Report"
- "Device Status Report"
- "Deployment Detail Report"
- "Deployment In-Progress Report"
- "Mandatory Baseline Detail Report"
- "Package Compliance Detail Report"
- "Vulnerability Analysis Report"
- "Hardware Inventory Summary Report"
- "Operating System Inventory Summary Report"
- "Software Inventory Summary Report"
- "Services Inventory Summary Report"
- "Device Duplicate Report"
- "Detection Results Not Found Report"
- "Deployment Error Report"
- "Deployment Summary Report"
- "Mandatory Baseline Summary Report"
- "Package Compliance Summary Report"
- "Hardware Inventory Detail Report"
- "Operating System Inventory Detail Report"
- "Software Inventory Detail Report"
- "Services Inventory Detail Report"

Agent Policy Report

Available Parameters: Device, Group

The *Agent Policy Report* shows the policies that are the resolution of all policies assigned to the device. In the report, each policy value is listed in the *Policy Name* column. When using groups as a parameter, it is only a method to select multiple devices, the group policies are not part of the actual results. The following table describes the columns included in the report.

Table 7.2 Agent Policy Report Column Definitions

Column	Definition
Device Name	Name of device.
Policy Name	Name of agent policy.
Current Value	The policy setting.
Policy Desc	Describes the agent policy.



Device Duplicate Report

Available Parameters: Date Range

The *Device Duplicate Report* returns a list of duplicate devices registered with the Server. Duplicate devices are usually the result of applying the *Agent Uniqueness* feature that permits an agent installed on ghost images to register multiple times with Patch Management Server. The following table describes the columns included in the report.

Table 7.3 Device Duplicate Report Column Definitions

Column	Definition
Device Name	Name of device.
Status	Current status of device.
Install Date	Date agent was installed on device.

Device Status Report

Available Parameters: Device, Group

The *Device Status Report* returns the current status of the selected devices (or devices in the selected groups). In the report, each device is listed in the *Device Name* column. The report then provides information about the particular device. The following table describes the columns included in the report.

Table 7.4 Device Status Report Column Definitions

Column	Definition
Device Name	Name of device.
DNS Name	Name used by the Domain Name System (DNS) to identify the device.
IP Address	Internet Protocol address.
OS Name	The device's operating system.
OS Build No.	Build number of operating system.
OS Service Pack	Latest service pack applied to the operating system (if applicable).
Agent Version	Version of the ZENworks Patch Management Agent.
Last Contact Date	Last date the ZENworks Patch Management Server has contact with the agent.



Table 7.4 Device Status Report Column Definitions

Column	Definition
Patchable Status	Reboot /chained status of the agent.
Group List	A listing of the groups that the device belongs to, using the group's Distinguished Name.

Detection Results Not Found Report

Available Parameters: Device, Group

The *Detection Results Not Found Report* returns a list of devices that have not completed a DAU task with the server. The report lists each agent name, the installation date of the agent, and information required to identify and locate the device. The following table describes the columns included in the report.

Table 7.5 Detection Results Not Found Report Column Definitions

Column	Definition
Agent Name	Name of agent.
OS Abbr Name	The device's operating system.
Agent Version	Version of the ZENworks Patch Management Agent.
Last Contact Date	Last date the ZENworks Patch Management Server has contact with the agent.
Installation Date	Date agent was installed on device.
IP Address	Internet Protocol address.
DNS Name	Name used by the Domain Name System (DNS) to identify the device.
OS Info	A description of operating system.

Deployment Detail Report

Available Parameters: Deployments, Vulnerabilities, Date Range



The *Deployment Detail Report* provides information about a selected list of deployments. In the report, each deployment name is listed in the *Deployment Name* column. The report provides information as to the status of the particular deployment activity. The following table describes the columns included in the report.

Table 7.6 Deployment Detail Report Column Definitions

Column	Definition
Deployment Name	Name of deployment.
Package Name	Name of package.
Device Name	Name of device.
Deployment Status	Indicates the deployment status or stage.
Deployment Date	Date deployment was sent.
Install Date	Date agent was installed on device.
Vulnerability Status	Patch status of the vulnerability.
Date Last Verified	Date of the last DAU scan.



Note: If a selected Vulnerability does not have an associated deployment, it will not appear in the report.

Deployment Error Report

Available Parameters: Deployments, Packages, Devices, Date Range

The *Deployment Error Report* provides information about deployments which have returned an error. The following table describes the columns included in the report.

Table 7.7 Deployment Error Report Column Definitions

Column	Definition
Deployment Status	Indicates the deployment status or stage.
Status Code	Reference code for support identification. When contacting support, this code is used to help identify the deployment issue.
Error Message	Actual error text returned by the deployment.
Install Date	Date agent was installed on device.
Package Name	Name of package.



Table 7.7 Deployment Error Report Column Definitions

Column	Definition
Deployment Name	Name of deployment.
Device Name	Name of device.



Deployment In-Progress Report

Available Parameters: Deployments, Packages, Devices, Groups

The *Deployment In-Progress Report* provides information about deployments that have not completed. Reports can be generated for each deployment, package, or device. The report provides the status of the deployment. The following table describes the columns included in the report.

Table 7.8 Deployment In-Progress Report Column Definitions

Column	Definition
Deployment Name	Name of deployment.
Package Name	Name of package.
Total Deployed	Number of devices that were assigned the deployment.
Already Patched	Number of devices that are already patched.
Not Applicable	Number of devices where the deployment does not apply.
Total Successful	Number of devices successfully patched.
Total In-Progress	Number of devices currently receiving the deployment.
Not Started	Number of devices yet to receive the deployments.
Caching Package	Indicates whether the deployment is still caching the package. 1 = Caching, 0 = Complete
Total Failed	Total number of deployments that have failed.
Total Disabled	Total number of devices that are disabled and cannot receive the deployment.
Percent Success	Percentage of devices that have successfully received the deployment.
Percent Failure	Percentage of devices on which the deployment has failed.



Deployment Summary Report

Available Parameters: Deployments, Vulnerabilities, Date Range

The *Deployment Summary Report* provides information about a selected list of deployments. The report provides a summary of the particular deployment activity. The following table describes the columns included in the report

Table 7.9 Deployment Summary Report Column Definitions

Column	Definition
Deployment Name	Name of deployment.
Package Name	Name of package.
Total Deployed	Number of devices that were assigned the deployment.
Already Patched	Number of devices that are already patched.
Not Applicable	Number of devices where the deployment does not apply.
Total Successful	Number of devices successfully patched.
Total In-Progress	Number of devices currently receiving the deployment.
Not Started	Number of devices yet to receive the deployments.
Caching Package	Indicates whether the deployment is still caching the package. 1 = Caching, 0 = Complete
Total Failed	Total number of deployments that have failed.
Total Disabled	Total number of devices that are disabled and cannot receive the deployment.
Total Patched	Total number of devices that have been patched by this deployment.
Percent Success	Percentage of devices that have successfully received the deployment.
Percent Failure	Percentage of devices on which the deployment has failed.



Note: If a selected Vulnerability has no associated deployment, it will not appear in the report.



Mandatory Baseline Detail Report

Available Parameters: Devices, Groups

The *Mandatory Baseline Detail Report* provides information about the mandatory baseline status associated with a device. The following table describes the columns included in the report.

Table 7.10 Mandatory Baseline Detail Report Column Definitions

Column	Definition
Device Name	Name of device.
Assigned By Group	The distinguished name of the group that assigned the mandatory baseline.
Package Name	Name of the package.
Mandatory Baseline Enabled	Indicates whether the <i>Assigned By Group</i> has Mandatory Baselines enabled.
Package Enabled	Indicates whether the package is enabled. If the package is disabled, it cannot be deployed to the device.
Mandatory Status	Identifies whether the device is applicable, patched, or needs patched by the mandatory baseline.
Deployment Status	Indicates the deployment status or stage.
Package Release Date	Date the associated package was released.
Date Deployed	Date the mandatory baseline package was deployed.
Date Installed	Date the mandatory baseline package was installed on the device.
Date Last Verified	Date of the last DAU scan.
Assigned	A value of 1 indicates the Mandatory Baseline has been assigned to the device.



Mandatory Baseline Summary Report

Available Parameters: Devices, Groups

The *Mandatory Baseline Summary Report* returns a summary list of patch and deployment information for all mandatory baseline packages and vulnerabilities associated with the selected list of devices. The following table describes the columns included in the report.

Table 7.11 Mandatory Baseline Summary Report Column Definitions

Column	Definition
Mandatory Baseline Item Name	Name of the mandatory baseline vulnerability.
Total Devices	Total number of devices receiving the deployment.
Total Patched	Total number of devices that have been patched by this deployment.
Total Not Applicable	Total number of devices where the deployment does not apply.
Total In-Progress	Number of devices currently receiving the deployment.
Total Disabled	Total number of devices that are disabled and cannot receive the deployment.
Total Error Condition	Total number of devices on which the deployment has failed.
Percent Patched	The percentage of devices successfully patched.



Package Compliance Detail Report

Available Parameters: Devices, Groups, Packages

The *Package Compliance Detail Report* provides information about patch and deployment status for a specific package or device. The report lists each package associated with the selected device(s) or group(s). In the report, each package is listed in the *Package Name* column. The report then provides details for the vulnerability status for each package; and the associated device, status, and deployment details. The following table describes the columns included in the report.

Table 7.12 Package Compliance Detail Report Column Definitions

Column	Definition
Package Name	Name of package.
Device Name	Name of device.
Vulnerability Status	Patch status of the vulnerability.
Last DAU Run	Date of the last DAU scan.
Last DAU Status	Status of the last DAU scan.
Date Last Verified	Date of the last DAU scan.
Deployment Name	Name of deployment.
Deployment Status	Indicates the deployment status or stage.
Package Release Date	Date the associated package was released.
Date Deployed	Date the package was deployed.
Date Installed	Date the package was installed on the device.
Date Scheduled	Date the package was scheduled for deployment to the device.



Note: If a selected Package has no associated deployment, it will not appear in the report.



Package Compliance Summary Report

Available Parameters: Devices, Groups, Packages

The *Package Compliance Summary Report* returns a summary list of patch and deployment information by package name for all applicable devices. The following table describes the columns included in the report.

Table 7.13 Package Compliance Summary Report Column Definitions

Column	Definition
Package Name	Name of package.
Total Devices	Total number of devices.
Applicable Devices	Total number of devices applicable to the package.
Devices Detecting	Number of devices currently running a DAU.
Devices Patched	Number of devices already patched.
Not Patched/Not Scheduled	Number of devices that are not patched, and do not have a deployment scheduled.
Not Patched/Scheduled	Number of devices that are not patched, but have a deployment scheduled.
Deployments Completed	Number of deployments that have successful completed.
Deployments Failed	Number of failed deployments.
Deployments In Progress	Number of devices currently receiving the deployment.



Note: If a selected Package has no associated deployment, it will not appear in the report.



Vulnerability Analysis Report

Available Parameters: Devices, Groups, Vulnerabilities

The *Vulnerability Analysis Report* provides a summary of the remediation status for the selected vulnerabilities. The report lists each vulnerability affecting the selected device or group. The report also can be generated for a single vulnerability or group of vulnerabilities. In the report, each vulnerability is listed in the *Vulnerability Name* column. The report then provides patch status details for each vulnerability and if a deployment is required. The following table describes the columns included in the report.

Table 7.14 Vulnerability Analysis Report Column Definitions

Column	Definition
Vulnerability Name	Name of the vulnerability.
Vulnerability Release Date	Date the vulnerability was released.
Total Devices	Total number of devices receiving the deployment.
Applicable Devices	Number of devices applicable to the vulnerability.
Devices Detecting	Number of devices currently running a DAU.
Devices Patched	Number of devices already patched.
Not Patched	Number of devices not patched.
Percent Patched	The percentage of applicable devices that are patched.



Note: If a selected Vulnerability has no associated deployment, it will not appear in the report.



Hardware Inventory Detail Report

Available Parameters: Devices, Groups

The *Hardware Inventory Detail Report* provides information about hardware associated with a device and device status. The following table describes the columns included in the report.

Table 7.15 Hardware Inventory Detail Report Column Definitions

Column	Definition
Hardware Device Class	The type of hardware.
Hardware Device Name	Name of the hardware device.
Device Name	Name of device.
Device OS Info	A description of operating system.

Hardware Inventory Summary Report

Available Parameters: Devices, Groups

The *Hardware Inventory Summary Report* provides a summary of reported hardware and the devices associated with them. The following table describes the columns included in the report.

Table 7.16 Hardware Inventory Summary Report Column Definitions

Column	Definition
Hardware Device Class	The type of hardware.
Hardware Device Name	Name of the hardware device.
Instances	The number of times this device occurs. (Within the parameters of the report.)

Operating System Inventory Detail Report

Available Parameters: Devices, Groups

The *Operating System Inventory Detail Report* provides information about the operating system associated with a device and the device status. The following table describes the columns included in the report.

Table 7.17 Operating System Inventory Detail Report Column Definitions

Column	Definition
Operating System	The operating system name and description.
Device Name	Name of the device.



Operating System Inventory Summary Report

Available Parameters: Devices, Groups

The *Operating System Inventory Summary Report* provides a summary about the operating system associated with a device and the device status. The following table describes the columns included in the report.

Table 7.18 Operating System Inventory Detail Report Column Definitions

Column	Definition
Operating System	The operating system name and description.
Instances	The number of times this operating system occurs. (Within the parameters of the report.)

Software Inventory Detail Report

Available Parameters: Devices, Groups

The *Software Inventory Detail Report* provides information about the software associated with a device and the device status. The following table describes the columns included in the report.

Table 7.19 Software Inventory Detail Report Column Definitions

Column	Definition
Software Program	The name of the software installed on the device.
Device Name	Name of the device.

Software Inventory Summary Report

Available Parameters: Devices, Groups

The *Software Inventory Summary Report* provides information about the software associated with a device and the device status. The following table describes the columns included in the report.

Table 7.20 Software Inventory Summary Report Column Definitions

Column	Definition
Software Program	The name of the installed software.
Instances	The number of times this software program occurs. (Within the parameters of the report.)



Services Inventory Detail Report

Available Parameters: Devices, Groups

The *Services Inventory Detail Report* provides information about the service associated with a device and the device status. The following table describes the columns included in the report.

Table 7.21 Services Inventory Detail Report Column Definitions

Column	Definition
Service Name	The name of the service.
Device Name	The name of the device.
Service Startup State	The state the service should enter upon device boot.
Service Current State	The current state of the service.

Services Inventory Summary Report

Available Parameters: Devices, Groups

The *Services Inventory Summary Report* provides summary information about the service associated with a device and the device status. The following table describes the columns included in the report.

Table 7.22 Services Inventory Summary Report Column Definitions

Column	Definition
Service Name	The name of the service.
Instances	The number of times this service occurs. (Within the parameters of the report.)





8 Managing Users and Roles

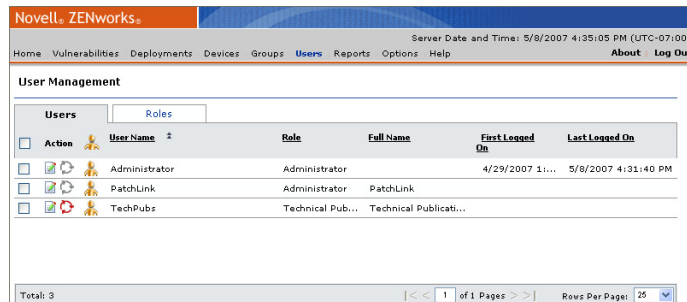
This chapter provides information on managing ZENworks Patch Management Server users. The user management features allow you to create users and define their permissions and access rights.

In this Chapter

- “About User Management”
- “Defining User Access”
- “Defining Users”
- “Working with Users”
- “Working with User Roles”

About User Management

The *User Management* page allows the system administrator to define which users can access ZENworks Patch Management Server and the role each user has within the system. Roles define the permissions and access rights for each user.



Action	User Name	Role	Full Name	First Logged On	Last Logged On
	Administrator	Administrator		4/29/2007 1:...	5/8/2007 4:31:40 PM
	PatchLink	Administrator	PatchLink		
	TechPubs	Technical Pub...	Technical Publicati...		

Total: 3 | < 1 of 1 Pages > Rows Per Page: 25

Figure 8.1 User Management View

Viewing Users

To View Users

1. From the *Main menu*, select the **Users** tab.
The users display in the *Users* window.



Defining User Access

ZENworks Patch Management allows for establishing security policies in accordance with your company needs. Security access is determined by a combination of two mechanisms: Windows-based authentication and ZENworks Patch Management access rights.

Windows-based Authentication

ZENworks Patch Management authentication is controlled by the Windows operating system. Users who have access to ZENworks Patch Management are members of the local Windows group *PLUS Admins*.

Update Access Rights

Once a user has logged into ZENworks Patch Management, their assigned user role is authenticated by the system. If a user does not have access to a given section, an access denied error message will display.

In the Users Section, the Roles tab is where these roles are defined, while the Users tab is where you can add or remove users and assign them a user role.

Defining Users

Users can be defined as individuals (John Smith) or conceptual users (Quality Assurance Manager). The user profile includes access credentials and the role assigned to the user. While a user only can be assigned one role, there can be many users assigned to a certain role

There are two methods of bringing users into the system: creating users and adding users.

- **Creating New Users**

When a user is created, the user is added to both ZENworks Patch Management Server and Windows. Additionally, if the new user is given permission to *Manage Users* within ZENworks Patch Management, they will also be added to the Windows Administrators group. Without addition to the Windows Administrators group, the user would be unable to modify other users.

- **Adding Existing Windows Users**

An existing Windows user can be added and granted access to ZENworks Patch Management. Using this method, existing users are searched and can be added to ZENworks Patch Management. Additionally, if the newly added users are given permissions to manage users



within ZENworks Patch Management, they will also be added to the Windows Administrators group. Without addition to the Windows Administrators group, the user would be unable to modify other users.



Note: The Microsoft IIS Web server software does not support the entering of user names or passwords in languages (Korean, Kanji, etc.) that require Unicode characters. Since the ZENworks Patch Management Server software uses a Microsoft IIS Web server, Patch Management Server usernames and passwords cannot be created in unicode and authentication does not support some native languages.

Defining Roles

The ZENworks Patch Management Server permits system and custom roles. System roles are roles native to every installation and cannot be edited or disabled. They allow control over all device groups and devices. Custom roles are created by the administrator and allow for combining access rights and selected devices or groups for a particular user.



Note: See “[Defining Access Rights](#)” for detailed description of the available access rights for each role.

Roles are defined by a combination of three attributes; access rights, groups and devices.

- **Access rights** define the application pages and functionality available to the user.
- **Groups** and **Devices** define the specific machines or group of machines the user has permission to access.

Exploring the Predefined System Roles

Predefined system roles are provided to assist you in defining the roles that newly created users should inherit. The Patch Management Server administrator can assign these defined roles to the user, or may use a predefined role as a model in defining a new role.



Note: System roles provide access to all groups and devices. A user assigned a system role has access to all devices and groups.



There are four system roles: Administrator, Manager, Operator and Guest.

Table 8.1 Predefined System Roles

Role	Description
Administrator	Any user assigned this role is permitted full access to all areas and functionality of the product. Users assigned this role are the only users who can delegate newly installed devices to other user roles. The administrator role includes all available access rights. Administrators can view <i>all</i> devices/groups and perform any function within the ZENworks Patch Management Server environment. There must be at least one user assigned the administrator user role.
Manager	Users assigned this role can manage every section of the ZENworks Patch Management Server system with the exception of <i>Advanced Configuration</i> and <i>User Management</i> options.
Operator	This user role is permitted to perform all routine operations (deploy, detect, export). Operators can only perform typical daily functions.
Guest	This role provides access to the system but restricts the user from performing any patch management tasks. The role allows view-only access.

Defining Custom Roles

Custom roles are created by the ZENworks Patch Management Server administrator. Custom roles are based on a system role and then can be altered to fit a particular need. Creating a custom role involves selecting a predefined role as a model, or template. Unlike system roles which cannot be disabled, you can disable a custom role at any time.

Defining Access Rights

Every page, feature, function, and individual action within the application is constrained to a series of access rights. The application pages (views) and functionality available to the user are based on the access rights associated to the role assigned the user. The four predefined roles have a default set of access rights assigned to each role. Users inherit the access rights of the role they are assigned.

Access rights begin at permitting read-only (view) access to system data followed by offering the ability to export data. At the administration level, users can be assigned rights to fully manage the various system components and to initiate deployments.



Note: If additional modules are installed and running in the Patch Management Server environment, access rights pertaining to the installed module may be added by the system to the access rights list.



The following table identifies the default set of access rights, describes the functionality of each, and illustrates the system role assigned to each access right.

Table 8.2 User Role Access Rights

Access Right Name	Description	Administrator	Manager	Operator	Guest
Enable Update Cache Button	Ability to cache (download) packages from the Global Subscription Server.	X	X		
View Devices	Access the <i>Devices</i> section.	X	X	X	X
Export Device Data	Enable the export of device data.	X	X	X	
Install Agents	Access to the <i>Agent Installers</i> page.	X	X		
Manage Devices	Ability to enable, disable, and delete devices.	X	X		
View Deployments	Access the <i>Deployments</i> section.	X	X	X	X
Manage Deployments	Ability to enable, disable, abort, change and delete deployments.	X	X	X	
Export Deployment Data	Enable the export of deployment data.	X	X	X	
View Device Groups	Access the <i>Device Groups</i> section.	X	X	X	X
Export Device Group Data	Enable the export of Device Group data.	X	X	X	
Manage Device Groups	Ability to add, edit, disable, enable, and delete device groups.	X	X		
View Home Page	Access the <i>Home</i> page.	X	X	X	X
View Current Status	Display the server status (on the <i>Home</i> page).	X	X	X	X
View Inventory	Access the <i>Inventory</i> data.	X	X	X	X
Export Inventory Data	Enable the export of Inventory data.	X	X	X	
Manage Product Licenses	Manage the product licenses.	X			
View Support Options	Access the <i>Options > Support</i> tab.	X	X	X	X
Export Support Data	Enable the export of support data.	X	X	X	
View Agent Policies	Access the <i>Options > Policies</i> tab.	X	X	X	X
Export Agent Policy Data	Enable the export of agent policy data.	X	X		
View Default Configuration	Access the <i>Options > Configuration</i> tab.	X	X	X	X
Export Configuration Data	Enable the export of configuration data.	X	X		



Table 8.2 User Role Access Rights

Access Right Name	Description	Administrator	Manager	Operator	Guest
View E-mail Notifications	Access the <i>Options > E-Mail Notifications</i> tab.	X	X	X	X
Export E-mail Notification Data	Enable the export of e-mail notification data.	X	X		
View Product Licenses	Access the <i>Options > Products</i> tab.	X	X	X	X
Export Product License Data	Enable the export of product license data.	X	X		
Manage Options	Manage subscription, product licenses, configuration, agent policies, e-mail notifications, and support options.	X			
View Subscription Information	Access the <i>Options > Subscription</i> tab.	X	X	X	X
Export Subscription Data	Enable the export of subscription data.	X	X		
View Packages	Access the <i>Packages</i> section.	X	X	X	X
Create Deployments	Ability to create deployments.	X	X	X	
Export Package Data	Enable the export of package data.	X	X	X	
Manage Packages	Ability to add, change, disable, enable, and delete packages.	X	X		
Enable Reboot Now Button	Ability to reboot devices using the reboot now button.	X			
View Vulnerabilities	Access the <i>Vulnerability</i> section.	X	X	X	X
View Vulnerability Details	Access the vulnerability details.	X	X	X	X
Export Vulnerability Data	Enable the export of vulnerability data.	X	X	X	
Manage Vulnerabilities	Ability to disable and enable vulnerabilities.	X	X		
Enable Administrative Reports	Ability to run reports that return data for all devices and device groups regardless of user role, device, or group assignments.	X			
Export Reports	Ability to export application reports.	X	X	X	
Enable User Reports	Ability to run reports returning data for only the devices and device groups to which the user has access.	X	X	X	X



Table 8.2 User Role Access Rights

Access Right Name	Description	Administrator	Manager	Operator	Guest
Enable Scan Now Button	Ability to deploy the Discover Applicable Updates (DAU) Task using the Scan Now button.	X	X	X	
View Users	Access to the <i>Users</i> tabs.	X	X	X	X
Change Password	Ability to change the password for a user.	X			
Export User Data	Enable the export of user data.	X	X		
Manage Users	Ability to create, add, edit, remove, delete, enable, and disable users or user roles.	X			

Defining Accessible Device Groups

Accessible device groups are groups of devices associated with a particular role. This option is used to achieve a level of granularity in the assignment of roles to system users.

As mentioned, roles are defined primarily by the access rights associated to the role. In the case of the default system roles, the entire network monitored by the Patch Management Server is available to users if they have the appropriate role-based access rights.



Note: The *accessible groups* option is disabled when working with a predefined system role.

The accessible groups option allows you to restrict a user to specified groups. For example, a user assigned the access rights to manage deployments can be limited to managing deployments for select groups.

The accessible groups option is available in the Add/Edit Role Wizard.

- **Selected Groups** - Lists the groups of devices assigned to the role
- **Groups** - Lists the available groups of devices that can be assigned to the role



Defining Accessible Devices

Accessible devices are individual devices associated with a particular role. This option works in the same manner as the accessible groups option by allowing you to achieve a level of granularity in the assignment of roles to system users.

The accessible devices option allows you to limit a user's permissions to specified devices. For example, a user assigned access rights to manage devices can be limited to managing only a single device using this option.



Note: The accessible devices option is disabled when working with a predefined system role.

The accessible devices option is available in the *Add/Edit Role Wizard*.

- **Selected Devices** - Lists the devices assigned to the role
- **Devices** - Lists the available devices that can be assigned to the role

Working with Users

This section describes the user-based tasks available from the *User Management* page. The available user-based tasks are:

- “Creating New Users”
- “Adding Existing Users”
- “Editing User Profiles”
- “Removing ZENworks Patch Management Users”
- “Deleting ZENworks Patch Management Users”
- “Changing a User's Password”

Creating New Users

When creating users, you have two options: Create a new local user, or Add an existing local or domain user.

To Create a New User

1. In the *User Management* page, click **Create**.
The *Create User Wizard* opens.
2. Select the **Creating a new local user** option.



3. Click **Next**.
The *Create User* page opens.



Figure 8.2 Create User Wizard - Create or Add User page

4. Enter the user credentials, and contact information for the new user.



Warning: **User Name**, **Password**, **Confirm Password**, and **Role** are required fields.

The **User Name** may be between 1-20 characters in length and cannot include any of the following characters:

` \ " @ ^ % & { } () [] ; < > ! # : ? ` / * = |

The **Password** may be between 7-20 characters in length and can include alpha, numeric, or special characters. The password is case sensitive and must meet password the rules defined by local and/or domain password policies. Note that a **Password Strength Indicator** is provided to display the strength or weakness of your password selection while it's being typed.

The **Full Name**, **Office Phone**, **Cell Phone**, **Pager**, **E-mail**, and **Description** fields are not validated and apply no formatting rules other than maximum length of 25 characters.

5. Select a **Role** (Administrator, Manager, Operator, or Guest) for the user from the pull-down window list.
6. Click **Next**.
The *Confirm User* page opens.
7. Confirm the user information and click **Close**.
The *Verify User* page opens.



- 8. Verify the status information and click **Close**.
The **Create User** wizard closes.

Adding Existing Users

Adding a user imports an existing Windows user into the Patch Management Server database and access group, and can import a user from an existing domain by logging into that domain as a domain user.

To Add a User to ZENworks Patch Management

- 1. In the *User Management* page, click **Create**.
The *Create User Wizard* opens.
- 2. Select the **Adding existing local or domain users** option.
- 3. Click **Next**.
The *Search for the following users* page opens.

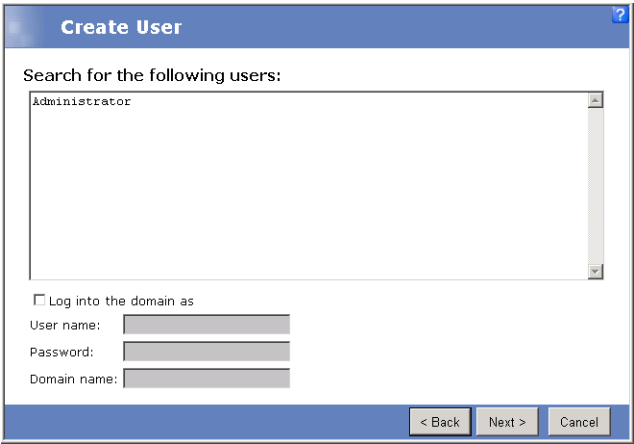


Figure 8.3 Search for Users

- 4. In the **Search for the following users** field type a user name, or the beginning characters of one or more user names. Use semicolons to separate user names. To search for users within a specific domain, prefix the user name with the domain (DOMAINNAME\UserName).

If searching using the domain, select **Log into the domain as**. *Enter the User name, Password, and Domain name.*





Note: There must be a secure connection between the domain and the Patch Management Server's domain, or the users will be unable to access the Server.

5. Click **Next**.
The *Users Found* page opens.

User Name	Full Name	Current Role	User Role
Administrator		Administrator	No Action

< Back Finish Cancel

Figure 8.4 Add User Wizard - Assign Role page

6. Select a **User Role** for each of the users found.
The *No Action* value indicates that the user will not be added to ZENworks Patch Management, or if the user already exists as a ZENworks Patch Management User, no changes are made to the user.
7. Confirm the user information and click **Finish**.
The *Summary* page opens.
8. Verify the Summary data and click **Close**.
The *Create User* wizard closes.



Editing User Profiles

Editing user profile information allows you to change the role assigned to a user as well as update contact information. If you have the Change Password access right, you can edit other user’s passwords using the procedure defined under “Changing a User’s Password” .

To Edit User Profile Information

- 1. From the *Users* grid located under *Action*, click the **Edit user details** icon associated with the user profile.
The *Edit User Wizard* opens.

The image shows a software window titled "Edit User" with a blue header bar. Below the header, the text "Edit User TechPubs:" is displayed. The form contains several input fields: "Full Name:" with the value "Technical Publications User", "Office Phone:" with "555.555.1234", "Cell Phone:" with "555.555.4321", "Pager:" with "555.555.5678", "E-mail:" with "techpubs@techpubs.com", "Description:" with "Technical Publications User", and "Role:" with a dropdown menu showing "Administrator". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

Figure 8.5 Edit User Wizard - User Information page

- 2. Make the necessary modifications as defined in “Creating New Users” , and click **Finish** to exit the wizard when complete.



Removing ZENworks Patch Management Users

Removing a user from ZENworks Patch Management disables their access to the ZENworks Patch Management Server without deleting the user's Windows account. Once removed, the user is deleted from the Patch Management Server database and access device groups and is removed from the user list in the *User Management* page.



Note: You **cannot** remove or delete a user that has been assigned the **Administrator** role, or a **Custom** role that has been given the **Manage Users** access right. You must first edit the user, change the user's role, then remove or delete the user.

To Remove a User

1. Click **Users** to open the *Users* page.
2. On the *Users* page, select the checkbox for the users to remove.
3. Click **Remove**.
A Remove User warning displays.
4. Acknowledge the *Warning* by clicking **OK**.
The User is removed.

Deleting ZENworks Patch Management Users

Deleting a user from ZENworks Patch Management disables their access to the ZENworks Patch Management Server and deletes the Windows account for that particular user.



Warning: Deleting a user deletes not only the users access to ZENworks Patch Management, but also from the device or Active Directory.

To Delete a User

1. Click **Users** to open the *Users* page.
2. On the *Users* page, select the checkbox for the users delete.
3. Click **Delete**.
A *Delete User* warning displays.
4. Acknowledge the *Warning* by clicking **OK**.
A *Delete User* confirmation displays.
5. In the *Confirmation* dialog box, click **OK**.
The User is deleted.



Changing a User's Password

Changing a User's Password in ZENworks Patch Management also changes the user's Windows password on the [physical] ZENworks Patch Management Server.

To Change a User's Password

1. Click **Users** to open the *Users* page.
2. Select the user requiring the password change.
3. Click **Change Password**.
The **Change Password Wizard** opens.
4. Type the **new password** in the *New Password* field.
The *Password Strength* indicator displays the effectiveness of the password you select and displays the *Weak* indicator when the first character is typed in the *New Password* field.



Figure 8.6 Weak Password Indicator



5. When the *Password Strength* indicator displays the acceptable password strength, retype the password in the *Confirm Password* field.

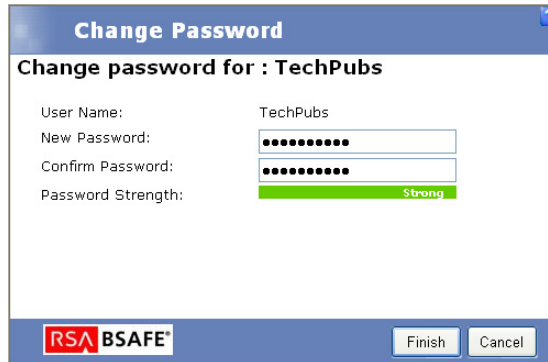


Figure 8.7 Confirm for Strong Password

The *Password Strength Meter* monitors factors such as the password length, complexity, variety of characters, and resemblance to common words.

Strong passwords usually contain more than eight characters, and combine capital and lower case letters, numbers and symbols. Also, they do not resemble common words or names including words with numbers in place of letters.

6. Click **Finish**.
The password is changed.

Exporting User Data

Information presented in ZENworks Patch Management Server can be exported into a comma-separated value (.csv) file. You may elect to save the file in a different file format after opening it from the download option.

For more information on exporting data, see “[Exporting Data](#)”.



Working with User Roles

This section describes the role-based tasks available from the *User Management* page.

- “Creating User Roles”
- “Editing User Roles”
- “Assigning User Roles”
- “Disabling and Enabling User Roles”
- “Deleting User Roles”



Note: When sorting user roles, regardless of the requested sort column or order, the system defined user roles (Administrator, Manager, Operator, and Guest) will remain as the first four items.

Creating User Roles

Creating custom-defined roles is an effective means to delegate patch management responsibilities to stakeholders throughout the organization. Custom roles are based on a template created from one of the system roles. Once you define the template, you can then modify access rights and modify group and device access levels.

To Create a User Role

- 1. In the *Users* page, select the **Roles** tab.

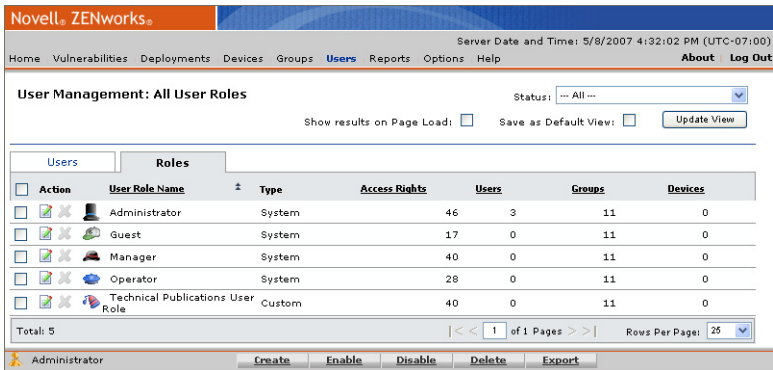


Figure 8.8 User Management - Roles tab



2. Click **Create**.
The *Create a Role* wizard opens.

The screenshot shows the 'Create a Role' wizard with the 'Role Information' tab selected. The form contains the following elements:

- Role Information** tab (selected), with other tabs: Access Rights, Groups, Devices.
- Enter the Role Information:** section.
 - Name:** A text input field with a red asterisk indicating it is required.
 - Description:** A larger text input area.
 - Role Template:** A dropdown menu with the text 'Please select a role template.' and a red asterisk indicating it is required.
- A legend at the bottom left: *** Indicates a required field.**
- OK** and **Cancel** buttons at the bottom right.

Figure 8.9 User Role Wizard - Role Information tab

3. On the *Role Information* tab:
 - a. Type a **Name** for the Role.
 - b. Type a **Description** for the role.
 - c. Select a **Role Template** (*Administrator, Manager, Operator, or Guest*)
The template selected, will determine what access rights the user role will start with. You can add or remove access right regardless of which role was selected as the template.
4. Select the *Access Rights* tab, to define which rights the users assigned this role will have.

To Assign Access Rights:

 - a. Select the checkbox to the left of each of the desired access rights.
 - b. Click **Assign** to move the selected access rights to the *Selected Access Rights* table or click **Assign All** to move all of the access rights to the *Selected Access Rights* table.

To Remove Access Rights:

 - a. Select the checkbox to the left of each of the desired access rights.
 - b. Click **Remove** to remove the selected access rights from the *Selected Access Rights* table or click **Remove All** to remove all of the access rights from the *Selected Access Rights* table.
5. Select the *Accessible Groups* tab, to define which groups the users assigned this role will be able to access.



To Assign Group Access:

- a. Select the checkbox to the left of each of the desired groups.
- b. Click **Assign** to move the selected groups to the *Selected Groups* table or click **Assign All** to move all of the groups to the *Selected Groups* table.

To Remove Group Access:

- a. Select the checkbox to the left of each of the desired groups.
- b. Click **Remove** to remove the selected groups from the *Selected Groups* table or click **Remove All** to remove all of the groups from the *Selected Groups* table.



Note: Granting access to a *Device Group* gives permission to all devices within that group, regardless of the options selected within the *Devices* tab.

6. Select the *Devices* tab, to define which devices the users assigned this role will be able to access.

To Assign Device Access:

- a. Select the checkbox to the left of each of the desired devices.
- b. Click **Assign** to move the selected devices to the *Selected Devices* table or click **Assign All** to move all of the devices to the *Selected Devices* table.

To Remove Device Access:

- a. Select the checkbox to the left of each of the desired devices.
 - b. Click **Remove** to remove the selected devices from the *Selected Devices* table or click **Remove All** to remove all of the devices from the *Selected Devices* table.
7. Click **OK**.
The wizard saves your changes and closes.



Editing User Roles

The editing feature is available only to custom-defined roles (system-defined roles cannot be edited) and is performed within the *Edit a Role Wizard*.

To Edit a User Role

1. In the *Users* page, select the **Roles** tab.

Novell ZENworks

Server Date and Time: 5/8/2007 4:32:02 PM (UTC-07:00)

Home Vulnerabilities Deployments Devices Groups **Users** Reports Options Help [About](#) [Log Out](#)

User Management: All User Roles Status:

Show results on Page Load: ☐ Save as Default View: ☐ [Update View](#)

Users **Roles**

Action	User Role Name	Type	Access Rights	Users	Groups	Devices
	Administrator	System		46	3	11
	Guest	System		17	0	11
	Manager	System		40	0	11
	Operator	System		28	0	11
	Technical Publications User Role	Custom		40	0	11

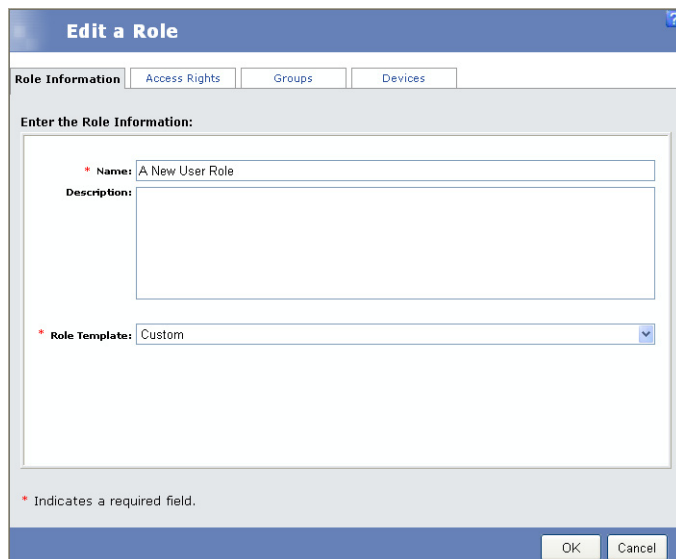
Total: 5 | < 1 of 1 Pages > | Rows Per Page: 25

Administrator [Create](#) [Enable](#) [Disable](#) [Delete](#) [Export](#)

Figure 8.10 User Management - Roles tab



2. Click the **Edit** icon to the left of the Role you wish to edit.
The *Edit a Role* wizard opens.



The screenshot shows the 'Edit a Role' wizard with the 'Basic Information' tab selected. The wizard has a title bar with a question mark icon. Below the title bar are four tabs: 'Role Information' (selected), 'Access Rights', 'Groups', and 'Devices'. The main area is titled 'Enter the Role Information:' and contains three fields: 'Name' (with the value 'A New User Role'), 'Description' (a large text area), and 'Role Template' (a dropdown menu with 'Custom' selected). A legend at the bottom left states '* Indicates a required field.' At the bottom right are 'OK' and 'Cancel' buttons.

Figure 8.11 User Role Wizard - Basic Information tab

3. On the *Role Information* tab, Edit the **Name** or **Description** as desired.
4. Select the *Access Rights* tab, to define which rights the users assigned this role will have.

To Assign Access Rights:

- a. Select the checkbox to the left of each of the desired access rights.
- b. Click **Assign** to move the selected access rights to the *Selected Access Rights* table or click **Assign All** to move all of the access rights to the *Selected Access Rights* table.

To Remove Access Rights:

- a. Select the checkbox to the left of each of the desired access rights.
- b. Click **Remove** to remove the selected access rights from the *Selected Access Rights* table or click **Remove All** to remove all of the access rights from the *Selected Access Rights* table.

5. Select the *Accessible Groups* tab, to define which groups the users assigned this role will be able to access.

To Assign Group Access:

- a. Select the checkbox to the left of each of the desired groups.

- b. Click **Assign** to move the selected groups to the *Selected Groups* table or click **Assign All** to move all of the groups to the *Selected Groups* table.

To Remove Group Access:

- a. Select the checkbox to the left of each of the desired groups.
- b. Click **Remove** to remove the selected groups from the *Selected Groups* table or click **Remove All** to remove all of the groups from the *Selected Groups* table.



Note: Granting access to a *Device Group* gives permission to all devices within that group, regardless of the options selected within the *Devices* tab.

- 6. Select the *Devices* tab, to define which devices the users assigned this role will be able to access.

To Assign Device Access:

- a. Select the checkbox to the left of each of the desired devices.
- b. Click **Assign** to move the selected devices to the *Selected Devices* table or click **Assign All** to move all of the devices to the *Selected Devices* table.

To Remove Device Access:

- a. Select the checkbox to the left of each of the desired devices.
- b. Click **Remove** to remove the selected devices from the *Selected Devices* table or click **Remove All** to remove all of the devices from the *Selected Devices* table.

- 7. Click **OK**.
The wizard saves your changes and closes.



Assigning User Roles

User Roles are assigned to individual users or conceptual user groups (IT support) when you create or add a user.



Note: At any given time, ZENworks Patch Management must have at least one user assigned the *Administrator* role.

To Assign a User Role to an Existing User

- 1. In the *Users* tab, select the user profile that will be assigned the user role.

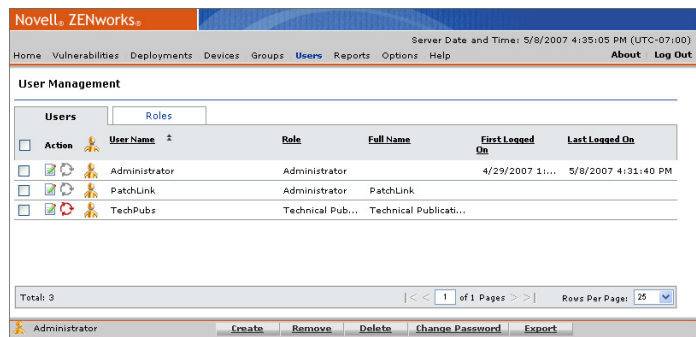


Figure 8.12 User Management - Users tab

- 2. Click **Edit User details**.
The *Edit User* wizard opens.
- 3. Edit the user as defined in “Editing User Profiles” , changing the role as desired.
Click **Finish** to save your selections. Click **Close** to exit the *Edit User* wizard.



Disabling and Enabling User Roles

You can disable any *non-system* role, allowing you to continue maintaining the role within ZENworks Patch Management but restricting its assignment to any users. You can *enable*, *edit*, and *delete* disabled roles. Disabled user roles appear with a gray background in the list of user roles in the *User Management* page.



Note: You cannot disable the system defined User Roles (*Administrator*, *Manager*, *Operator*, and *Guest*).

To Disable a User Role

1. From the *Users* page, select the **Roles** tab.

Action	User Role Name	Type	Access Rights	Users	Groups	Devices
	Administrator	System	46	3	11	0
	Guest	System	17	0	11	0
	Manager	System	40	0	11	0
	Operator	System	28	0	11	0
	Technical Publications User Role	Custom	40	0	11	0

Total: 5 | < 1 of 1 Pages > | Rows Per Page: 25

Buttons: Create, Enable, Disable, Delete, Export

Figure 8.13 User Management - User Roles tab

2. Ensure the page filter (Status) is not set to **Disabled**.
3. Click **Update View** to populate the tab.
4. Select the role or roles to disable.
5. Click **Disable**.
The role is disabled.



Warning: If you disable a role that is assigned to a user, the user will be able to log on to ZENworks Patch Management, but will be unable to view any pages.



To Re-Enable a User Role

- 1. From the Users view, select the **Roles** tab.

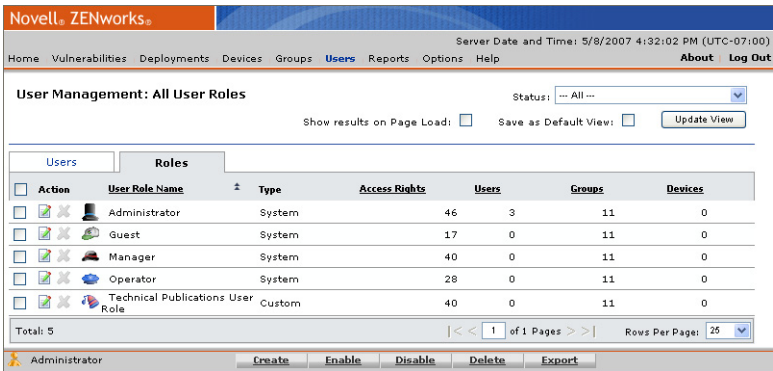


Figure 8.14 User Management - User Roles tab

- 2. Ensure the page filter (Status) is set to *All* or *Disabled*.
- 3. Click **Update View** to populate the tab.
- 4. Select the role or roles to enable.
- 5. Click **Enable**.
The roles are re-enabled.



Deleting User Roles

Removing a role deletes the role and its data from the Patch Management Server database. In order to remove a role, it must first be disabled. As well, you cannot remove a system role.

To Delete a User Role

1. From the *Users* view, select the **Roles** tab.

Action		User Role Name	Type	Access Rights	Users	Groups	Devices
<input type="checkbox"/>		Administrator	System	46	3	11	0
<input type="checkbox"/>		Guest	System	17	0	11	0
<input type="checkbox"/>		Manager	System	40	0	11	0
<input type="checkbox"/>		Operator	System	28	0	11	0
<input type="checkbox"/>		Technical Publications User Role	Custom	40	0	11	0

Total: 5 | < < 1 of 1 Pages > > | Rows Per Page: 25

Administrator [Create] [Enable] [Disable] [Delete] [Export]

Figure 8.15 User Management - User Roles tab

2. Ensure the status filter is set to *All* or *Disabled*.
3. Click **Update View** to populate the tab.
4. Select the role or roles to delete.
You cannot delete *Enabled* User Roles or the system defined User Roles (*Administrator*, *Manager*, *Operator*, and *Guest*).
5. Click **Delete**.
The role is deleted.



Warning: If you delete a role that is assigned to a user, the user will be able to log on to ZENworks Patch Management, but will be unable to view any pages.

Exporting User Role Data

Information presented in ZENworks Patch Management Server can be exported into a comma-separated value (.csv) file. You may elect to save the file in a different file format after opening it from the download option.

For more information on exporting data, see “[Exporting Data](#)”.





9 Configuring Default Behavior

Configuration options provide you a means to define the default behavior and administer the ZENworks Patch Management Server. This chapter provides information on configuring and managing ZENworks Patch Management.

In this Chapter

- “About the Options Page”
- “Viewing Subscription Service Information”
- “Verifying Subscription Licenses”
- “Novell ZENworks Patch Management Default Configuration”
- “Customizing and Administering Agent Policy Sets”
- “Using E-Mail Notification”
- “Technical Support Information”

About the Options Page

The *Options* page is available by clicking **Options** on the main toolbar. The page comprises six management and configuration views as individual tabs.

To View Configuration Options

1. From the *Main menu*, select **Options**.
The *Options* pages displays with the *Subscription Service* tab as the default view.
2. Select a tab to view ZENworks Patch Management Server details.



Viewing Subscription Service Information

The *Subscription Service* page allows you to modify the Subscription Communication interval, initiate a standard or full replication, configure the subscription service, and view Subscription Service history and status information.

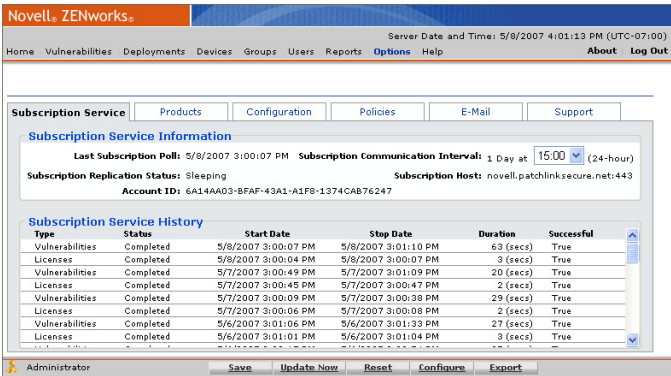


Figure 9.1 Subscription Service Tab

ZENworks Patch Management Agents gather a list of software, hardware, services and patches installed on each agent within the network. With this detailed information, the ZENworks Patch Management Server generates a complete analysis of your network to identify the patches, hot fixes, service packs and updates of importance to your network.

The ZENworks Patch Management Server connects to the Global Subscription Server (GSS) once daily to download a series of vulnerability definitions and packages.

Table 9.1 Page Functions

Button	Function
Save	Saves changes made to the Subscription communication interval.
Update Now	Initiates replication of the ZENworks Patch Management Server with the Global Subscription Server. This option retrieves the changes made since your last replication.
Reset	Resets the replication status and initiates a complete replication with the Global Subscription Server. Note: Once you click Reset , a confirmation window opens stating the replication status has been reset and you can choose whether to initiate the replication process by clicking OK , or wait until a later time, by clicking Cancel .



Table 9.1 Page Functions

Button	Function
Configure	Opens the "Subscription Service Configuration" page.
Export	The Export button allows you to export subscription data to a comma separated value (.csv) file. For more information on exporting data, see "Exporting Data" .

Subscription Service Information

The Subscription Service Information section provides a summary of the configuration settings and status of the subscription service.

Table 9.2 Subscription Service Information

Information	Description
Last Subscription Poll	Date and time of the last successful contact with ZENworks Patch Management Server.
Subscription Replication Status	Current replication status. Replication ensures that the ZENworks Patch Management Server remains current with the latest vulnerability, package, and license information.
Account ID	Passed to the Global Subscription Server and validates the update request. The account ID is created by the ZENworks Patch Management Server when it registers with the Global Subscription Server.
Subscription Communication Interval	Time frame for connecting to the Global Subscription Server and retrieving updates.
Subscription Host	URL and port of the Global Subscription Server.



Note: If you modify the *Subscription Communication Interval* you must save the changes by clicking **Save** on the *Action Menu*.



Subscription Service History

The Subscription Service History section displays a list of subscription activity and update records.

Table 9.3 Subscription Service History Field Descriptions

Field Name	Description
Type	Defines the type of task, the available types include: <ul style="list-style-type: none">• Licenses - Verifies the validity of your ZENworks Patch Management Server license.• Vulnerabilities - Downloads the current vulnerabilities according to the subscription type defined for the account .• Packages - Downloads the current packages, based upon the vulnerabilities selected for deployment.
Status	The status of the task. While the task is active, the process begins with a status of <i>Initializing Replication</i> , followed by downloads. When the task is finished, the status is <i>Completed</i> .
Start Date	The date and time the task started.
Stop Date	The date and time the task completed.
Duration	Indicates the duration of the task. This is shown in seconds or minutes. For example; <i>19 (secs)</i> , <i>1.22 (mins)</i> .
Successful	Confirms communication settings between your ZENworks Patch Management Server and the Global Subscription Server.

Subscription Service Configuration

The Subscription Service Configuration page allows you to view the current status and define your Proxy, and Communication settings.

To Access the Configuration Page

1. Select the **Options** tab.
- The *Configuration Options* window opens with the *Subscription Service* tab displaying as the default.



- In the *Action* menu, click **Configure**.
The *Subscription Service Configuration* window opens.

Figure 9.2 Subscription Service Configuration page

Subscription Service Status

The following table describes the fields within the *Status* area of the *Subscription Service Configuration* window.

Table 9.4 Subscription Service Status Field Descriptions

Field Name	Description
Service Status	The current status of the local Subscription Service's communication with the Global Subscription Server.
Last Checked	The last date and time the local Subscription Service contacted the Global Subscription Server.
Next Check	The next scheduled date and time for the local Subscription Service to contact the Global Subscription Server.



Subscription Service Proxy Configuration

The following table describes the fields within the *Proxy* area of the *Subscription Service Configuration* window.

Table 9.5 Subscription Service Proxy Field Descriptions

Field Name	Description
Address	Uses the defined proxy address when connecting to the Global Subscription Server.
Port	Uses the defined proxy port when connecting to the Global Subscription Server.
Authenticated	Enables the User Name and Password fields for use with an authenticated proxy.
User Name	When using an authenticated proxy, you must provide a valid user name.
Password Confirm Password	The password associated with the defined proxy user.

Subscription Service Communication Settings

The following table describes the fields within the *Communication* area of the *Subscription Service Configuration* window.

Table 9.6 Subscription Service Communication Field Descriptions

Field Name	Description
Logging Level	The level of detail recorded to the Subscription Service Log. Options include: <i>Debug</i> , <i>Info</i> , <i>Warn</i> , <i>Error</i> , and <i>Fatal</i> .
Use SSL	Enable SSL for use when communicating with the Global Subscription Server.
Enable Bandwidth Throttling	Enables the Kilobytes per second field, allowing you to set the maximum bandwidth used when communicating with the Global Subscription Server.
__ Kbytes per second	The maximum Kbytes per second used when communicating with the Global Subscription Server.
Retry Limit	The number of times ZENworks Patch Management attempts to establish a connection with the Global Subscription Server.
Retry Wait	The number of seconds between retries.



Table 9.6 Subscription Service Communication Field Descriptions

Field Name	Description
Connect Timeout	The number of seconds before a connection will be considered unsuccessful (when the connection timeouts, it will be retried based upon the retry limit and retry wait values).
Command Timeout	The seconds of inactivity before a command will be considered unsuccessful.

Subscription Service Configuration Page Action Menu

The following table describes the Action Menu functions in the Subscription Service Configuration window.

Table 9.7 Action Menu Functions

Button	Function
Restart	Stops and restarts the Global Subscription Server.
Save	Saves any changes to the database, then closes the Subscription Service Configuration window.
Cancel	Closes the Subscription Service Configuration window without saving changes.
Apply	Saves changes to the database, without closing the Subscription Service Configuration window.



Verifying Subscription Licenses

The *Products* page allows you to view, validate and export license information. The page provides a summary of all product, third-party software, and plug-in component licenses that are part of your patch management activities. This information is updated as part of the daily replication with the Global Subscription Server.

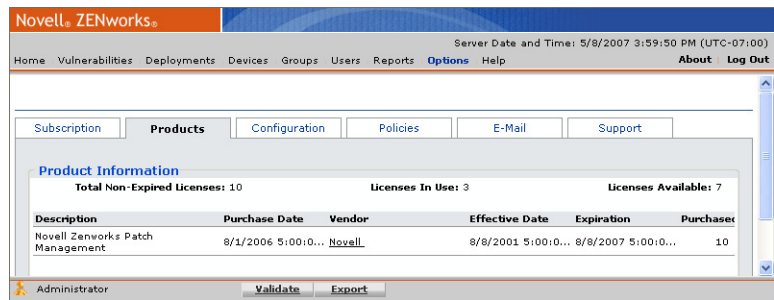


Figure 9.3 Products Tab

Table 9.8 Page Functions

Button	Function
Validate	Initiates a license replication that searches for any changes to your license data.
Export	Exports license data to a comma separated value (.csv) file. For more information on exporting data, see "Exporting Data" .



Product Information

The Product Information section provides a summary of license availability and usage.

Table 9.9 License Availability

License	Description
Licenses In Use	The total number of licenses in use by registered agents.
Licenses Available	The total number of licenses available for use.
Total Non-Expired Licenses	The total number of licenses active and available for use. This number represents a sum of available licenses.

License summary information is presented according to license group. A license group is defined as a block of licenses purchased at a time. For example, you may have 3 license groups comprising 500 total licenses with a group of 300 licenses purchased initially, and two additional groups of 100 licenses each added during subsequent quarters.

The license group information includes the following:

Table 9.10 License Group Information

Field	Description
Description	The license name or description.
Purchase Date	The date the license group was purchased.
Vendor	The source of the license. Click the vendor name to open a Web browser to the vendor's home page.
Effective Date	The date the license(s) went into effect. This is the first day that the licenses were valid, not necessarily the installation date.
Expiration	The date the license(s) expires.
Purchased	The number of licenses in this group.



Novell ZENworks Patch Management Default Configuration

The *Patch Management Server Configuration* page lets you establish, modify and export the Deployment Defaults, Agent Defaults (*Default Agent Policy*), ISAPI Communication, and User Interface settings.

SubscriptionProducts**Configuration**PoliciesE-MailSupport

Deployment DefaultsSet your deployment defaults

Concurrent

Maximum number of Deployments that can run simultaneously (Deployment Limit) 500

Maximum number of Discover Applicable Update System tasks that can be run simultaneously (DAU) 500

Maximum number of Reboot tasks that can be run simultaneously 5

Maximum number of Simultaneous mandatory baseline deployments 50

Consecutive

Maximum number of times a deployment will be consecutively attempted 2

Agent DefaultsSet your Agent defaults

Communication

Agents should be shown Offline when inactive for 3 Hours Set to 0 (zero) to disable

Agent Uniqueness Based On: Device Name

Notification Defaults

☐ User Notification window should always be on top

Manual Installation (Max 256 Chars):
This package will be downloaded
and made available for your
administrator to install.
171 characters left.

May Reboot (Max 256 Chars):
This deployment MAY need to
reboot your computer, dependent
upon various configuration
118 characters left.

Legacy Agents have a Notification Timeout of 2 min(s)

Legacy Agents have a Snooze Duration of 60 min(s)

☒ DAU (Discover Applicable Updates) should be run after Subscription Replication

DAU (Discover Applicable Updates) should be run every 28 Hours

Absentee Agent Deletion

Delete Absentee Agent after 0 Days. Set to 0 (zero) to disable

User InterfaceSet the Default behavior of your User Interface Elements

Display 25 Rows Per Page Modify

Password Expiration Notification should be displayed in 0 Days. Set to 0 (zero) to disable

Cache Timeout: 5 Minutes (values 5-99)

How should Deployment Wizard Start Times be displayed?

☐ Agent Local Time (Deploy at local time for each individual node)

☒ Agent UTC Time (Deploy at UTC time for each individual node)

ISAPI CommunicationThese settings determine how the Agent communicates with the Server

Concurrent Agent Limit

☒ SQL Default (64 threads)

☐ Custom Setting (5 to 256 threads) 64 threads

Connection Timeout

☒ Default (30 seconds)

☐ Custom Setting (5 to 300 seconds) 30 sec(s)

Command Timeout

☒ Default (60 seconds)

☐ Custom Setting (5 to 900 seconds) 60 sec(s)

Figure 9.4 Patch Management Server Configuration Tab



Table 9.11 Action Menu Functions

Button	Function
Save	Saves any changes made on this page. Warning: If you have made ANY changes, you must click Save . If you do not click Save , the system will return to the last saved settings when you navigate off of the <i>Configuration</i> page.
Export	Allows you to export Patch Management Server information to a comma separated value (.CSV) file. For more information on exporting data, see "Exporting Data" .

Configuring Deployment Defaults

The Deployment Defaults area establishes global deployment limitations.

Deployment Defaults	Set your deployment defaults
Concurrent	Maximum number of Deployments that can run simultaneously (Deployment Limit) <input type="text" value="500"/> Maximum number of Discover Applicable Update System tasks that can be run simultaneously (DAU) <input type="text" value="500"/> Maximum number of Reboot tasks that can be run simultaneously <input type="text" value="5"/> Maximum number of Simultaneous mandatory baseline deployments <input type="text" value="50"/>
Consecutive	Maximum number of times a deployment will be consecutively attempted <input type="text" value="2"/>

Figure 9.5 Patch Management Server Configuration Tab - Deployment Defaults section

Table 9.12 Deployment Defaults

Deployment Setting	Description
Concurrent	
Maximum number of Deployments that can run simultaneously (Deployment Limit)	The maximum amount of agents that can receive simultaneous deployments.
Maximum number of Discover Applicable Update System tasks that can be run simultaneously (DAU)	The maximum number of agents that can receive the DAU System Task at the same time.
Maximum number of Reboot tasks that can be run simultaneously	The maximum number of agents that can receive a simultaneous deployment requiring a reboot.
Maximum number of Simultaneous mandatory baseline deployments	The maximum number of agents that can receive simultaneous mandator baseline deployments.
Consecutive	
Maximum number of times a deployment will be consecutively attempted	The number of failed deployment attempts permitted before ZENworks Patch Management Server disables the deployment. However, this does not apply to mandatory baseline deployments.



Note: You can define deployment notification recipients on the *E-Mail Notification* tab.



Configuring Agent Defaults

Agent defaults allows for establishing default behavior for the deployment agent.

Figure 9.6 ZENworks Patch Management Server Configuration Tab - Agent Communication Defaults

Communication

Agent communications to devices are defined in the Communication section of the Configuration page. The following table describes the fields within this section.

Table 9.13 Communication settings

Field	Description
Agents should be shown Offline when inactive	Configures a time interval (defined in minutes, hours or days) that must elapse before an agent is considered to be offline. Agents are noted as being offline when they have not communicated with Patch Management Server for the defined period of time. If an agent is disabled or uninstalled it does not appear as offline. When Use Offline Threshold is not enabled, an agent is considered offline after failing to connect to Patch Management Server after two of its communication intervals.
Agent Uniqueness Based On	Defines the Agent Uniqueness method used to identify agents. Options are: <ul style="list-style-type: none"> Instance - Validates using instanced validation. Instanced validation, when determining agent uniqueness, uses logic which does not rely upon the device name Device Name - Validates based on the device name



Notification Defaults

Applies to deployments where a notification is required. The behavior defined in this section may be overridden within a Agent Policy or on a per-deployment basis using the Deployment Wizard.

Table 9.14 Deployment Messages

Option	Use To
User Notification window should always be on top	Selection of this option will force all notification windows to display on top of other windows
Manual Installation	Edit and display a message advising the user that the package still requires installation (maximum of 256 characters).
May Reboot	Edit and display a message advising the user that the computer MAY be rebooted (maximum of 256 characters).
Legacy Agents have a Notification Timeout	Time allotment for the notification window to display for pre-6.3 agents.
Legacy Agents have a Snooze Duration	Maximum time allotment the agent can be set to snooze for pre-6.3 agents.
DAU should be run every after Subscription Replication	Select this option if you want the DAU task to run after your local subscription server communicates with the Global Subscription Server.
DAU should be run every X hours	Default time frame for DAU system check.

Absentee Agent Management

The Absentee Agent option allows for removing an agent that has failed to communicate with the server.

Table 9.15 Absentee Agent settings

Field	Description
Delete Absentee Agent after	Removes an uncommunicative agent after the set time frame. If set to zero, this function is disabled.



Setting the User Interface Defaults

The User Interface default settings allow you to define the initial user experience for your users.

User Interface Set the Default behavior of your User Interface Elements

Display **25** Rows Per Page Modify

Password Expiration Notification should be displayed in Days. Set to 0 (zero) to disable

Cache Timeout: Minutes (values 5-99)

How should Deployment Wizard Start Times be displayed?

☐ Agent Local Time (Deploy at local time for each individual node)

☒ Agent UTC Time (Deploy at UTC time for each individual node)

Figure 9.7 User Interface Defaults

Table 9.16 User Interface Defaults

UI Default	Description
Display __ Rows Per Page	Allows you to set the default number of rows [25, 50, 100, 200, 500, or 1000] displayed within ZENworks Patch Management Server. The setting applies to users who have not set their own parameters.
Password Expiration Notification should be displayed in _ days	Allows you to define when users will start receiving warnings regarding when their password will expire.
Cache Timeout	Allows you to define the maximum amount of time in minutes before the data grid will refresh (updated from the database).
How should Deployment Wizard Start Times be displayed?	<ul style="list-style-type: none"> • Agent Local Time - Sets the deployment wizard to default to the agent local time. • Agent UTC Time - Sets the deployment wizard to default to UTC time.

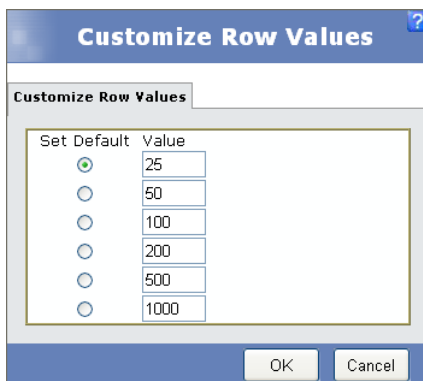


Note: ZENworks Patch Management Server default security settings prohibit the use of any browser other than Internet Explorer 6 SP 1 and above. If you need to remove this restriction, **and disable the enhanced security settings** available with IE 6 SP1, refer to the [Novell Knowledgebase](#)



Customizing Row Values

The *Customize Row Values* page allows you to define the amount of rows you want to display when using ZENworks Patch Management Server,



Set Default	Value
<input checked="" type="radio"/>	25
<input type="radio"/>	50
<input type="radio"/>	100
<input type="radio"/>	200
<input type="radio"/>	500
<input type="radio"/>	1000

Figure 9.8 Customize Row Values

To Customize Row Values

1. In the *Configuration* window, click the **Modify** button.
The *Customize Row Values* window opens.
2. If needed, type a new value in the *Value* field.
3. If needed, select the desired radio button in the *Set Default* field.
4. Click **OK**.
The Customized Row Values are saved and the window closes.

Configuring ISAPI Communication Settings

ZENworks Patch Management supports the Internet Server API (ISAPI) communication settings for the Internet Information Server (IIS).

ISAPI Communication	These settings determine how the Agent communicates with the Server
Concurrent Agent Limit <input checked="" type="radio"/> SQL Default (64 threads) <input type="radio"/> Custom Setting (5 to 256 threads) <input type="text" value="64"/> threads	
Connection Timeout <input checked="" type="radio"/> Default (30 seconds) <input type="radio"/> Custom Setting (5 to 300 seconds) <input type="text" value="30"/> sec(s)	
Command Timeout <input checked="" type="radio"/> Default (60 seconds) <input type="radio"/> Custom Setting (5 to 900 seconds) <input type="text" value="60"/> sec(s)	

Figure 9.9 Patch Management Server Configuration Tab - ISAPI Communication Settings

Concurrent Agent Limit

Defines the maximum number of threads used by ZENworks Patch Management.

Table 9.17 Concurrent Agent Limit

Field	Description
SQL Default (64 threads)	Select to enable the recommended thread count for a SQL Server implementation.
Custom Setting	Select to define a custom (between 5 and 256) thread count.

Connection Timeout

Time (seconds) before an ISAPI thread expires (times out).

Table 9.18 Connection Timeout

Field	Description
Default	Select to set the Connection timeout to the default value of 30 seconds.
Custom Setting	Select to define a custom (between 5 and 300 seconds) timeout setting.



Command Timeout

Time (seconds) before an ISAPI command expires (times out).

Table 9.19

Field	Description
Use Default	Select to set the Command timeout to the default value of 30 seconds.
Custom Setting	Select to define a custom (between 5 and 900 seconds) timeout setting.

Customizing and Administering Agent Policy Sets

Agent Policies are the key element in defining agent behavior. Agent Policies consist of the rules for communicating with the ZENworks Patch Management Server and define settings such as communication interval, deployment notification options, reboot notification options, logging levels, discovery mode, and hours of operation.

Agent policies are assigned to agents by assigning Agent Policy Sets to Device Groups. The policy values are then assigned to the agents based upon their group membership. When agents or groups are assigned conflicting policies, the conflict resolution rules found under “[Defining Agent Policy Conflict Resolution](#)” are applied. Any agent that does not have all of the policies defined by it’s various group memberships will have any missing policy values defined by the Global System Policy.

The *Agent Policies Sets* page allows you to define the behavior of the ZENworks Patch Management Agent. Click **Options** in the tool bar and then click the **Policies** tab.

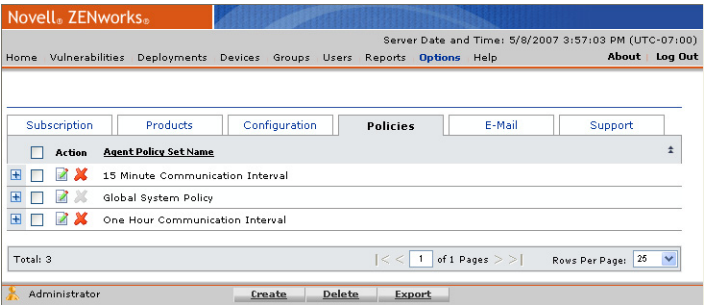


Figure 9.10 Agent Policy Set Tab





The following functions are available when using Policy Sets.

Table 9.20 Action Menu Page Functions

Button	Function
Create	Creates a new Agent Policy Set.
Delete	Deletes an Agent Policy Set.
Export	Exports policy data to a comma separated value (.csv) file. For more information on exporting data, see "Exporting Data" .

Table 9.21 Action Column Functions

Icon	Name	Function
	Edit	Allows you to Edit an existing Agent Policy.
	Delete	Deletes an Agent Policy.



Viewing Agent Policy Summary Information

Expanding an Agent Policy Set listing displays the following information regarding each policy as illustrated in the following figure:

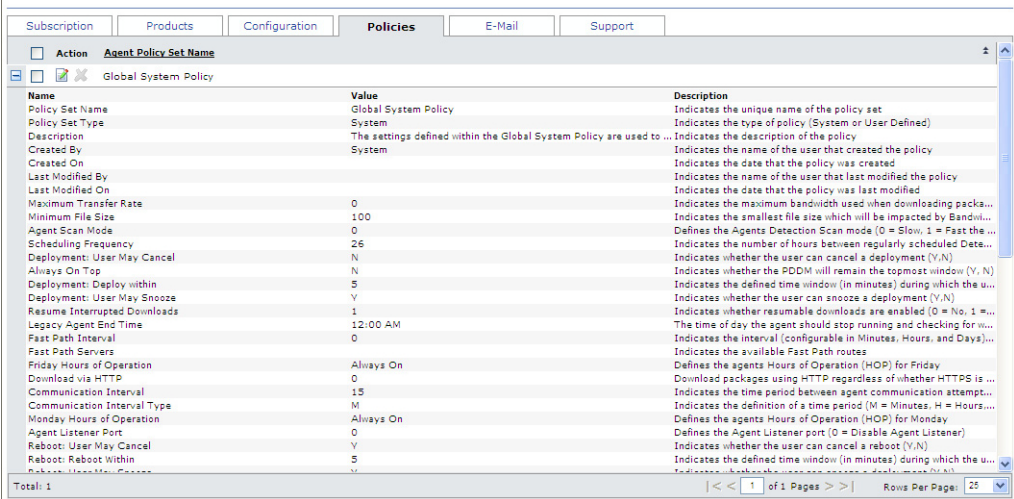


Figure 9.11 Agent Policies

The following table lists and describes the Agent Policy Set fields.

Table 9.22 Agent Policy Set Definitions

Value	Description
Policy Set Name	The name designated to the policy. Policies are named by the user when the policy is created and can be edited at any time. Limited to 256 characters.
Policy Set Type	There are two types of policies: System and User.
Logging Level	The agent logging level. Levels include: <ul style="list-style-type: none">• None - Only errors are logged and recorded• Basic Information - Captures all errors and basic system and usage information• Detailed - Captures all errors and the major system actions• Debug - Captures all errors and system actions
Start Time	Relates to Hours of Operation settings. Identifies when the agent can begin communication.



Table 9.22 Agent Policy Set Definitions

Value	Description
Stop Time	Relates to Hours of Operation settings. Identifies when the agent must suspend communication.
Created On	The date and time the policy was created.
Created By	The user who created the policy. System policies have a created by value of PatchLink.
Last Modified On	The date and time the policy was last modified.
Last Modified By	The user who last modified the policy.
Communication Interval	The interval (in minutes, hours or days) between each communication between the agent and Patch Management Server.
Download via HTTP:	Download packages using HTTP regardless of whether HTTPS is used for agent to server communication.
Description	The description attributed to the policy. Policy descriptions can be edited at any time.
Bandwidth Throttling	
Maximum Transfer Rate	Defines the maximum amount of bandwidth used when downloading packages to an Agent. A setting of zero (0) will disable Bandwidth Throttling.
Minimum File Size	The smallest file size which will be impacted by Bandwidth Throttling.
Agent Scan Mode	The mode in which the Discover Applicable Updates task runs. Levels include: <ul style="list-style-type: none"> • Fast Scan - Always run in Fast mode, performs the discovery faster but uses more resources • Initial Only - Performs the first discovery scan in Fast mode and subsequent scans in Normal mode • Normal - Always run in normal mode, performs the scan using the least amount of resources
Agent Listener Port	When contacted on this port, the agent will respond with the current version and initiate communication with Patch Management Server. A value of 0 (zero) turns the agent listener off.
Deployment Notification Options	
Cancelable	Cancel the deployment.
Snoozable	Snooze the deployment.
Deploy within	Snooze or cancel the deployment time window, in minutes. When the defined Offset has elapsed, the deployment will automatically occur.



Table 9.22 Agent Policy Set Definitions

Value	Description
Window always on top	Selection of this option keeps this window on top of all other windows until the recipient acknowledges the notification by selecting a valid option (Snooze, Cancel, Deploy, or Reboot).
Reboot Notification Options	
Cancelable	Cancel the reboot.
Snoozable	Snooze the reboot.
Reboot within	Snooze or cancel the reboot time window, in minutes. When the defined Offset has elapsed, the reboot will automatically occur.
Fastpath Servers	Provides a listing of the Fastpath servers the agents can use when communicating with ZENworks Patch Management Server.
Discover Applicable Updates Schedule	Defines how often the agent must perform a Discover Applicable Updates (DAU). The value here indicates the maximum amount of time between scans.
Hours of Operation	Sunday-Monday-Tuesday-Wednesday-Thursday-Friday (Always on): Launches the Agent Policy Set page. HOP is based on Agent local time and allows for further definition of the Agent start and end times. This page may contain a Legacy Agent Hours of Operation if the appropriate box was checked in the Configuration Defaults Communications Section.



Creating a Policy Set

The Create a Policy Wizard allows you to create and add a policy to the ZENworks Patch Management Server.

To Create a Policy Set

1. In ZENworks Patch Management Server, open the *Agent Policy Sets* page (**Options > Policies**)
2. Click **Create**
The *Create a Policy Set* window opens

Policy Set Information	
Policy Set Details	
* Policy Set Name	Another New Policy
Policy Set Description	Another new Policy Set
Communication	
Logging Level	None
Agent Scan Mode	Normal
Communication Interval	15 minute(s)
Agent Listener Port	0
Inventory Collection Options	Define
Resume Interrupted Downloads	True
Hours of Operation	Define
Legacy Agent Start Time	12:00 AM
Legacy Agent End Time	12:00 AM
Deployment Notification Defaults	
User May Cancel	True
User May Snooze	True
Deploy within	45 Minutes
Always On Top	False
Reboot Notification Defaults	
User May Cancel	True
User May Snooze	True
Reboot Within	5 Minutes
Discover Applicable Updates (DAU)	
Scheduling Frequency	26 Hours
FastPath Servers	
Fast Path Interval	0 minute(s)
Servers	Define
Bandwidth Throttling	
Maximum Transfer Rate	0 KBps
Minimum File Size	100 KB
* Indicates a required value	

Figure 9.12 Create a Policy Set

3. In the *Policy Set Information* tab, click **within the fields** to activate the options.



The following table lists and describes the available Agent Policies.

Table 9.23 Agent Policy Descriptions

Policy	Description
Policy Set Details	
Policy Set Name	The name of the policy set. Limited to 255 characters.
Policy Set Description	The policy set description.
Communication	
Logging Level	<p>The agent logging level. Levels include:</p> <ul style="list-style-type: none"> • None - Only errors are logged and recorded • Basic Information - Captures all errors and basic system and usage information • Detailed - Captures all errors and the major system actions • Debug - Captures all errors and system actions
Agent Scan Mode	<p>The mode in which the Discover Applicable Updates task runs. Levels include:</p> <ul style="list-style-type: none"> • Fast Scan - Always run in Fast mode, performs the discovery faster but uses more resources • Initial Only - Performs the first discovery scan in Fast mode and subsequent scans in Normal mode • Normal - Always run in normal mode, performs the scan using the least amount of resources
Communication Interval	The interval (in minutes, hours or days) between each communication between the agent and Patch Management Server.
Agent Listener Port	<p>When contacted on this port, the agent will respond with the current version and initiate communication with Patch Management Server.</p> <p>A value of 0 (zero) turns the agent listener off.</p>
Inventory Collection Options	Launches the <i>Select Inventory Collection</i> page, allowing selection of which inventory values to record during collection.
Resume Interrupted Downloads	When enabled, the agent will resume interrupted downloads at the point of interruption.
Hours of Operation	Launches the <i>Edit Agent Hours of Operation</i> page. HOP is based on Agent local time, and allows for further definition of the Agent start and end times. This page may contain a Legacy Agent Hours of Operation if the appropriate box was checked in the Configuration Defaults Communication Section.
Download via HTTP:	Download packages using HTTP regardless of whether HTTPS is used for agent to server communication.



Table 9.23 Agent Policy Descriptions

Policy	Description
Legacy Agent Start Time	Relates to Hours of Operation settings. Identifies when the agent can begin communication.
Legacy Agent End Time	Relates to Hours of Operation settings. Identifies when the agent must suspend communication.
<i>Deployment Notification Defaults</i>	
User May Cancel	Selection of this option will permit the recipient to cancel the deployment.
User May Snooze	Selection of this option will permit the recipient to snooze the deployment.
Deploy within	Default time (in minutes), between the creation of the deployment and the deployment deadline.
Always on Top	Selection of this option keep the Deployment (or Reboot) notification window on top of all other windows until the recipient acknowledges the notification by selecting a valid option (Snooze, Cancel, Deploy, or Reboot).
<i>Reboot Notification Defaults</i>	
User May Cancel	Selection of this option will permit the recipient to cancel the reboot.
User May Snooze	Selection of this option will permit the recipient to snooze the reboot.
Reboot within	Default time (in minutes), between the creation of the deployment and the reboot deadline.
<i>Discover Applicable Updates (DAU)</i>	
Scheduling Frequency	Configures the frequency of the DAU system task.
<i>FastPath Servers</i>	
FastPath Interval	Time interval between agent and ZENworks Patch Management Server communication. Interval can be defined in minutes, hours, or days.
Servers	Allows for the redirection of an agent via a FastPath server (caching proxy server) based upon the fastest route.
<i>Bandwidth Throttling</i>	



Table 9.23 Agent Policy Descriptions

Policy	Description
Maximum Transfer Rate	Defines the maximum amount of network bandwidth (in Kbps), per device, which can be used, by the agent, for package download. Entering a value of zero (0) will disable Bandwidth Throttling.
Minimum File Size	Defines the threshold (in KB) at which a file will be managed by Bandwidth Throttling. Any file that is smaller than the defined Minimum File Size will not be managed by Bandwidth Throttling.

4. Click **Save** to save the agent policy set as defined.



Editing a Policy Set

The *Edit a Policy Set* Wizard allows you to modify an agent policy and its behavior.

To Edit an Agent Policy Set

1. Select the **Agent Policy Set** requiring editing.
2. Select the **Edit** icon to the left of the policy.
The Edit A Policy Set window opens.

The screenshot shows the 'Policy Set Information' window with the following sections and settings:

- Policy Set Details**
 - Policy Set Name: Another New Policy
 - Policy Set Description: Another new Policy Set
- Communication**
 - Logging Level: None
 - Agent Scan Mode: Normal
 - Communication Interval: 15 minute(s)
 - Agent Listener Port: 0
 - Inventory Collection Options: [Define](#)
 - Resume Interrupted Downloads: True
 - Hours of Operation: [Define](#)
 - Legacy Agent Start Time: 12:00 AM
 - Legacy Agent End Time: 12:00 AM
- Deployment Notification Defaults**
 - User May Cancel: True
 - User May Snooze: True
 - Deploy within: 45 Minutes
 - Always On Top: False
- Reboot Notification Defaults**
 - User May Cancel: True
 - User May Snooze: True
 - Reboot Within: 5 Minutes
- Discover Applicable Updates (DAU)**
 - Scheduling Frequency: 26 Hours
- FastPath Servers**
 - Fast Path Interval: 0 minute(s)
 - Servers: [Define](#)
- Bandwidth Throttling**
 - Maximum Transfer Rate: 0 KBps
 - Minimum File Size: 100 KB

* Indicates a required value

Figure 9.13 Editing Policies

3. In the *Edit a Policy* window, edit the policy as necessary.
 - Refer to “[Creating a Policy Set](#)” for details regarding the available policy options.



- 4. Click **Save** to save your changes.



Note: The new policy settings take effect immediately and will be applied to the target agent(s) during their next communication with Patch Management Server.

Deleting an Agent Policy Set

You can delete a policy at any time. Deleting a policy will delete the policy from the database and any groups associated to the policy are automatically associated to the default policy.

To Delete an Agent Policy Set



Note: System-defined Agent Policy Sets cannot be deleted.

- 1. In ZENworks Patch Management Server, click **Options**
- 2. In the *Options* page, click **Policies**.
The list of policies displays in the *Policies* tab.

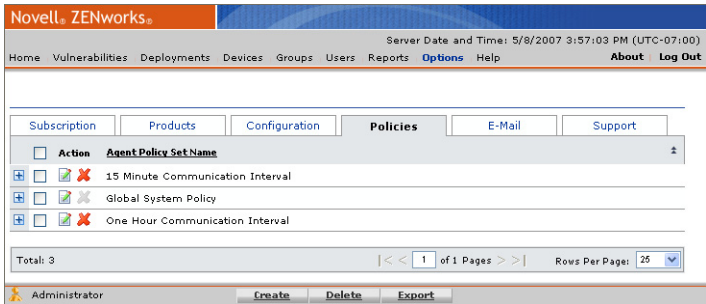


Figure 9.14 Removing a Policy

- 3. Select the policy to remove by selecting the checkbox to the left of the policy.
- 4. In the *Action Menu*, click **Delete**.
The *Delete Confirmation* window opens.
- 5. Click **Yes**
The policy is deleted from the system.



Defining Inventory Collection Options

The Select Inventory Collection page allows you to choose the inventory the DAU checks.

Figure 9.15 Inventory Collection Options

Table 9.24 Page Functions

Button	Function
Reset	Resets the previous settings.
OK	Closes the page (maintaining changes).
Cancel	Cancels all changes and closes the page.

To Define the Inventory Collection Options

1. Select the desired inventory collection options

Table 9.25 Inventory Collection Options

Inventory Option	Description
Inventory Collection Options	Deselecting this option will deselect all inventory collection options.
Allow use of WMI during inventory collection	Required if WMI data will be gathered, deselecting this option will deselect all inventory options which require WMI.



Table 9.25 Inventory Collection Options

Inventory Option	Description
Hardware	Deselecting this option will deselect all <i>Hardware</i> inventory options.
USB controllers	Scans for data regarding USB device inventory (from ...\\Enum\\USB).
IDE ATA/ATAPI controllers	Scans for data regarding IDE ATA/ATAPI controllers.
Other Hardware devices	Scans for system device data.
Processors	Scans for processor data.
USB storage devices	Scans for data regarding USB device inventory (from ...\\Enum\\USBSTOR).
Network adapters and MAC address (may use WMI)	Scans for data regarding network adapters.
Physical RAM - amount	Scans for the device's total physical RAM.
System Devices	Scan the Windows registry for additional hardware information.
Non-Plug and Play drivers	Scans for data regarding non-Plug and Play drivers.
Locally attached drives, total & free space	Scan for data regarding the disk drives.
USB devices	Scans for data regarding USB controllers.
BIOS information	Scans for BIOS data.
Sound, video, and game controllers	Scans for data regarding sound, video, and game controllers.
OS serial number (requires WMI)	Scans for the OS serial number (Requires WMI).
Virtual Machines	Scans to determine if the device is a virtual machine.
Device serial number (requires WMI)	Scans for the device's serial number (Requires WMI).
Device Manufacturer and Model (may use WMI)	Scans for the computer manufacturer and model.
Device asset tag (requires WMI)	Scans for the device's asset tag (Requires WMI).
User - last logged on	Scans for last logged in user and time.



Table 9.25 Inventory Collection Options

Inventory Option	Description
System uptime (may use WMI)	Scans for and return the time since last reboot (system uptime).
Custom import from file (may use WMI)	Scan for file containing custom inventory data (refer to "Using Custom Inventory" for additional details).
Services	Scans for a listing of Windows services (not applicable for Windows 9x or ME).
Software	Scans for a listing of installed software.

2. Click **OK** to close the page maintaining your changes



Warning: Changes made to the *Inventory Collection Options* will not be saved until you have selected **Save** on the *Configuration* page.



Editing Agent Hours of Operation

Agent communication can be enabled or disabled to restrict agent communication with ZENworks Patch Management to a specific time range only.



Note: Hours of Operation (HOP) is based on the Agent’s local time.

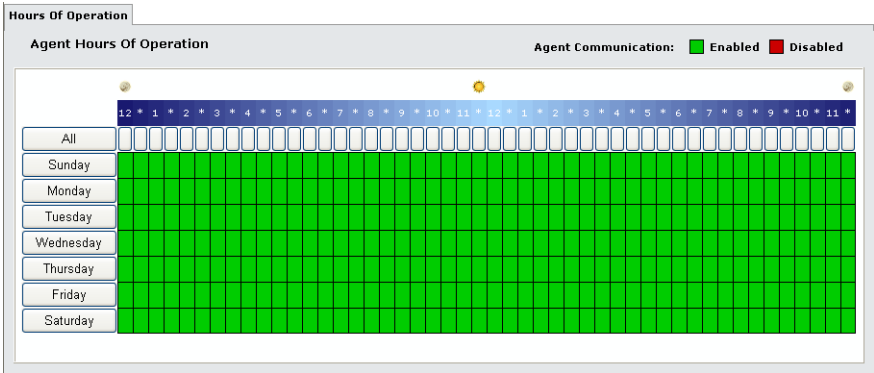


Figure 9.16 Edit Agent Hours of Operation

Table 9.26 Page Functions

Button	Function
Reset	Resets the previous Hours of Operation settings leaving the page open for edit.
OK	Closes the page (maintaining the changes made).
Cancel	Cancels all changes and closes the page.

To Set an Hours of Operation Policy

- Click the Day and Hour combinations during which you want to restrict agent communication.
 - ALL** toggles all agent communication
 - day** toggles entire day
 - time** unit toggles 30 minute increment across all days
- Click **OK**



Warning: Changes made to the *Hours of Operation* schedule will not be saved until you have selected **Save** on the *Patch Management Server Configuration* page.



Configuring Fastpath Servers

The Fastpath functionality will allow for the redirection of an agent from the ZENworks Patch Management Server to a Fastpath Server (or any caching proxy server) based upon the fastest route.

Table 9.27 FastPath Server fields

Field	Description
Communication Interval	The time interval between each check by fastpath to determine the fastest communication path back to the ZENworks Patch Management Server. A setting of zero (0) will disable the use of Fastpath Servers.
Servers	A listing of the available Fastpath servers.

To Add/Edit FastPath Servers

1. Open **Create/Edit Policy Set**.
The *Create/Edit a Policy Set* window opens.
2. Scroll to the *FastPath Servers* area, and click **Modify**.
The *Edit FastPath Servers* window opens.



Figure 9.17 Edit FastPath Servers



3. Click the **Add** link (or **Edit** icon) to open the *Add Fastpath Server* dialog.



Figure 9.18 Add Fastpath Server

4. Provide the following data about your FastPath server.
 - **Url** - The Url should be added in the `http://servername` format.
 - **Port** - The port on which your FastPath server operates.
 - **Authenticated** - Select this option if the FastPath server requires authentication. Enables the **User Name** and **Password** fields.
 - **User name** - If your FastPath server requires authentication, provide a valid user name.
 - **Password / Confirm Password** - The password associated with the defined user.
5. Click **OK**.
The FastPath Server data is saved and the *Add FastPath Server* window closes.
6. Click **Save**.
The *Edit FastPath Servers* window closes.

Defining Agent Policy Conflict Resolution

When a group is assigned conflicting policies, those policies must be validated, and any conflicting policies resolved. The policies are resolved in the following order:

1. **Group Policies** - The conflicting policy sets assigned to a group are resolved prior to attempting to resolve the agent policies. The following rules apply:
 - If a group has *inherit policies* turned **off**:
 - a. It will **not** receive the policy sets that are assigned to its parent. Therefore, only those policy sets that are directly assigned are considered.
 - b. Any conflicting values are resolved as defined in [Table 9.28](#).
 - If a group has *inherit policies* turned **on**:
 - a. It **will** receive the resultant (after conflict resolution) policies assigned to its parent.
 - b. Any directly assigned conflicting values are resolved as defined in [Table 9.28](#).
 - c. Finally, any policy values that are not directly assigned to the group, but are inherited from the group's parent, are assigned to the group.
2. **Agent Policies** - After resolving the group policies, the conflicting policies assigned to an agent (via it's group membership) are resolved. The following rules apply:
 - a. The resultant policies of all groups to which the agent is a member are resolved as defined in [Table 9.28](#).
 - b. Any policy values that have **not** been defined via the agent's group membership are populated based upon the policy settings defined in the *Global Policy Set*.



Note: The policy settings defined in the *Global Policy Set* are only used to fill the empty agent policy values. Therefore, conflict resolution rules do not apply to the Global Policy Set.

The following table defines the rules used when resolving conflicting policy settings:

Table 9.28 Agent Policy Conflict Resolution

Policy Setting	Resolution
Logging Level	The agent will use the most verbose Logging Level. (Debug > Detailed > Basic Information > None).
Agent Scan Mode	The agent will use the fastest Agent Scan Mode. (Fast Scan > Initial Scan > Normal Scan).
Communication Interval	The agent will use the shortest Communication Interval.
Agent Listener Port	If any group has an Agent Listener port defined (not zero), the agent listens on the highest defined port value.



Table 9.28 Agent Policy Conflict Resolution

Policy Setting	Resolution
Inventory Collection Options	The agent will use an all inclusive set of Inventory Collection options.
Resumable Downloads	If any group is not using Resumable Downloads, the agent will not use Resumable Downloads.
Hours Of Operation	If any group is not using Hours of Operation, the agent will not use Hours of Operation. However, if all groups are using Hours of Operation, the agent will use an all inclusive setting. The on value takes precedence during this operation.
User May Cancel Deployment	The agent will use True .
User May Snooze Deployment	The agent will use True .
Deployment Within n minutes	The agent will use the smallest Deploy Within value.
Always On Top	The agent will use True .
User May Cancel Reboot	The agent will use True .
User May Snooze Reboot	The agent will use True .
Reboot Within n minutes	The agent will use the smallest Reboot Within value.
Discover Applicable Updates (DAU) Scheduling Frequency	The agent will use the longest possible DAU frequency.
FastPath Interval	The agent will use the shortest FastPath Interval.
FastPath Servers	The agent will use all of the defined FastPath Servers.
Maximum Transfer Rate	The agent will use the smallest Transfer Rate.
Minimum File Size	The agent will use the smallest File Size.



Using E-Mail Notification

The *E-Mail Notification* page lets you configure system alerts to help in monitoring your ZENworks Patch Management Server. You can enter any number of e-mail addresses and then assign the particular alert types that you want each recipient to receive. This page also allows you to define the trigger levels for individual alerts.

The screenshot shows the 'E-Mail Notifications' configuration window. It features a tabbed interface with 'E-Mail Notification' selected. The main area is divided into two sections: 'E-Mail Notifications' and 'Alert Thresholds'. The 'E-Mail Notifications' section contains a table with columns for various alert types and a 'Notification Address' field. The 'Alert Thresholds' section contains four sub-sections: 'Low System Disk Space', 'Low Storage Disk Space', 'Low Available License Count', and 'Upcoming License Expiration'. Each sub-section has input fields for 'Alert When Below' and 'Check Disk Space Every' (or 'Alert When Days Remaining Are Below'). The 'Outgoing Mail Server (SMTP)' is set to 'mail.TechPubs.com'.

Alert Type	Notification Address
<input type="checkbox"/> New Vulnerabilities	Technical.Publications@TechPubs.com
<input checked="" type="checkbox"/> New Agent Registrations	
<input checked="" type="checkbox"/> Subscription Failure	
<input checked="" type="checkbox"/> Deployment Failure	
<input checked="" type="checkbox"/> Low System Disk Space	
<input checked="" type="checkbox"/> Low Storage Disk Space	
<input checked="" type="checkbox"/> Low Available License Count	
<input checked="" type="checkbox"/> Up-Coming License Expiration	
<input checked="" type="checkbox"/> License Expiration	

Alert Thresholds

Outgoing Mail Server (SMTP): mail.TechPubs.com

Low System Disk Space: Alert When Below 1025 MB. Check Disk Space Every 1 Days

Low Storage Disk Space: Alert When Below 1000 MB. Check Disk Space Every 1 Days

Low Available License Count: Alert When Below 25 Licenses.

Upcoming License Expiration: Alert When Days Remaining Are Below 90

Figure 9.19 E-Mail Notifications Tab

The following table describes the Action Menu functions of the *E-Mail Notification* window.

Table 9.29 Page Functionality

Button	Function
Create	Creates a new e-mail notification.
Save	Saves the changes made to e-mail notification. Warning: Be sure to click Save after making any changes. If you do not click Save , the system will revert to the last saved settings when you navigate off of the <i>E-Mail</i> page.
Delete	Deletes the selected e-mail address from the notification list. Once deleted, the entry cannot be restored.
Export	Exports a list of e-mail notification addresses and settings to comma separated value (.csv) file format. For more information on exporting data, see "Exporting Data" .
Test	Sends a test e-mail message to the selected e-mail address(es).



Configuring E-Mail Notification

The following options can be defined for each e-mail address included in the notification address column. Notification trigger levels (default values) for disk space, checking intervals, and license data are defined in the *Alert Thresholds* section.

Table 9.30 E-mail Notification Column Descriptions

Column Name	Description
New Vulnerabilities	Alerts when a new vulnerability becomes available for deployment.
New Agent Registrations	Alerts when an agent registers with the ZENworks Patch Management Server.
Subscription Failure	Alerts when any subscription task (download) fails.
Deployment Failure	Alerts when a deployment fails.
Low System Disk Space	Alerts when the free disk space, on the ZENworks Patch Management Server, falls below the defined minimums.
Low Storage Disk Space	Alerts when the available storage space, on the ZENworks Patch Management Server, falls below the defined minimums.
Low Available License Count	Alerts when the number of licenses available to the ZENworks Patch Management Server falls defined minimums.
Up-Coming License Expiration	Alerts when licenses will expire within the defined time frame.
License Expiration	Alerts when a license expires.
Notification Address	The e-mail address that receives notifications. Must be a validly formatted e-mail address (name@domain.tld); the system does not, however, validate the actual address.
Outgoing Mail Server (SMTP)	The mail host used by your ZENworks Patch Management Server for sending e-mail messages.



Defining E-Mail Alert Thresholds

Alert thresholds allow you to define the limits that trigger various alerts (notifications). Trigger limits are available for system disk space, storage disk space and license information.

Table 9.31 E-Mail Notification Alert Definitions

Alert Threshold	Definition
Low System Disk Space	Alert is generated if the system disk space on the ZENworks Patch Management Server drops below the defined level. The level is measured in Megabytes (MB) and must be a whole number between 1 and 9,999 MB (9.765 GB).
Low Storage Disk Space	Alert is generated if the storage drive disk space on the ZENworks Patch Management Server drops below the defined level. The level is measured in Megabytes (MB) and must be a whole number between 1 and 9,999 MB (9.765 GB).
Check Disk Space Every... Interval	Represents the schedule that the thresholds are checked. This is defined in units of minutes, hours or days. The interval must be defined as a whole number between 1 and 99.
Low Available License Count	Alert is generated if the number of available licenses drops below the defined level. The level is measured in units of available licenses, and must be a whole number between 1 and 999.
Up-Coming License Expiration	Alert is generated if licenses will expire within the defined days. The level is measured in units of days to expiration, and must be defined as a whole number between 1 and 99.

To Send a Test E-mail

1. On the *Options* page, click **E-Mail**.
2. In the *Current E-Mail Notifications* section, select the e-mail address(es) to receive the test message.
3. In the *Action Menu*, click **Test**.
4. A confirmation message informs you that the test message was sent.



Technical Support Information

Clicking on the **Support** tab causes the *Technical Support* page to be displayed. The *Technical Support* page is a view-only page that provides a variety of system data pertaining to the ZENworks Patch Management Server environment. It also provides links to contacting support.

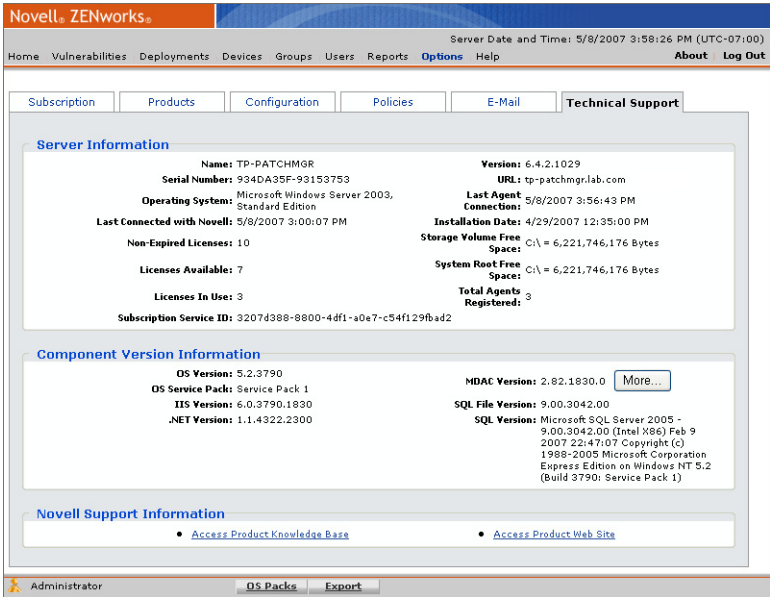


Figure 9.20 Technical Support Tab

The following table describes the Action Menu functions of the *Technical Support* page.

Table 9.32 Page Functionality

Button	Function
OS Packs	Regenerates and synchronize the relevant information for each of the Operating Systems supported by your ZENworks Patch Management Server.
Export	Exports a list of e-mail notification addresses and settings to comma separated value (.CSV) file format. For more information on exporting data, see "Exporting Data" .



Server Information

This section provides general notes regarding the ZENworks Patch Management Server. The information is not editable.

Table 9.33 Novell ZENworks Patch Management Server Information Field Descriptions

Field Name	Description
Name	The name of the computer on which ZENworks Patch Management Server is installed.
Serial Number	The serial number used by this server.
Operating System	The operating system installed and running on the ZENworks Patch Management Server machine.
Last Connected with Novell	The date and time the system last made a connection with the Global Subscription Server.
Non-Expired Licenses	Total number of active licenses.
Licenses Available	Number of licenses that can be used to register devices with this ZENworks Patch Management Server.
Licenses in Use	Number of licenses being used by agents.
Subscription Service ID	The ID assigned to the ZENworks Patch Management Server upon its registration with the Global Subscription Server.
Version	The version number of the ZENworks Patch Management Server installed.
URL	The URL assigned to this ZENworks Patch Management Server.
Last Agent Connection	The date and time an Agent last made a connection to the ZENworks Patch Management Server.
Installation Date	The date ZENworks Patch Management Server was installed.
Storage Volume Free Space	The amount of free disk space on your storage volume.
System Root Free Space	The amount of free disk space on your system volume.
Total Agents Registered	The total number of agents registered with this ZENworks Patch Management Server.



Component Version Information

This section identifies the basic component software and services running on the ZENworks Patch Management Server. The information is not editable.

Table 9.34 Component Version Information Field Descriptions

Field Name	Description
OS Version	Additional operating system information (typically the version number).
OS Service Pack	Service pack information, if available, regarding your operating system.
IIS Version	The version of Internet Information Server (IIS) running on the system.
.NET Version	The .NET Framework version(s) installed on the server.
MDAC Version	The Microsoft Data Access Components (MDAC) version. Click More... to view a detailed list of MDAC product and file versions.
SQL File Version	The SQL Server version installed on the server.
SQL Version	Detailed SQL Server version information.

Novell Support Information

This section provides links to Novell Support.

Table 9.35 Novell Support Information Link Descriptions

Field Name	Description
Access Product Knowledge Base	Accesses the Novell Knowledge Base.
Access Product Web Site	Accesses the Novell Web site.



10 Using the ZENworks Patch Management Agent

When installed on a device, the Agent scans that device for vulnerabilities and communicates the results of the scan to your ZENworks Patch Management Server. The results returned to ZENworks Patch Management can be viewed at any time, even if the workstation is disconnected from your network. The scan results are used, by ZENworks Patch Management, to determine a vulnerability's applicability for each device. If a vulnerability is applicable, ZENworks Patch Management will display the device as Not Patched.

After installing the ZENworks Patch Management Agent, there is generally, no additional user interaction required at the device.

In this Chapter

- “About the ZENworks Patch Management Agent for Pre Windows Vista”
- “About the ZENworks Patch Management Agent for Linux/Unix/Mac/Netware”
- “About ZENworks Patch Management Agent for Windows Vista”

About the ZENworks Patch Management Agent for Pre Windows Vista

The agent is responsible for retrieving device data, uploading the device data to ZENworks Patch Management Server, and deploying vulnerabilities to the device.

Viewing the Agent

To Access the Update Agent

1. Go to **Start > Settings > Control Panel**.
2. Select **Novell ZENworks Patch Management**.
The *Novell Agent Control Panel* opens. The *Deployment* tab is the default.



Note: When opening the ZENworks Patch Management Agent, the *Control Panel* must be displayed in the *Windows Classic View*. Viewing the *Control Panel* in *Category View* will not display the Agent.

Agent Components

The following section describes the components of the ZENworks Patch Management Agent and their functions.



Deployment Tab

The Deployment tab is comprised of four functional areas.

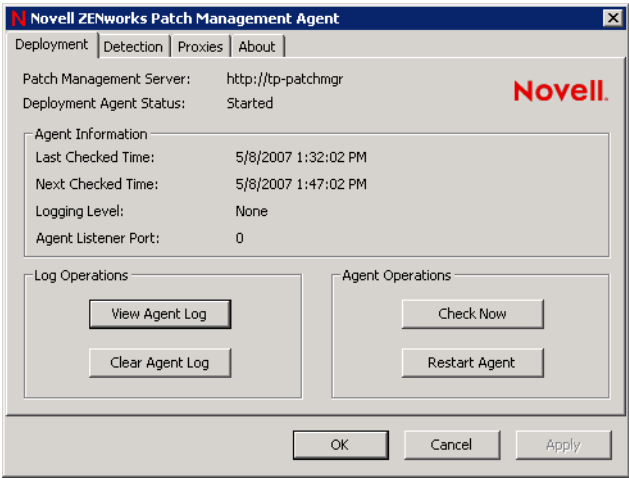


Figure 10.1 Agent initial screen

Server Information and Status

The following table displays the ZENworks Patch Management Server location and the communication status:

Table 10.1 Server Information

Field	Description
Patch Management Server	The URL of the ZENworks Patch Management Server the agent is registered against.
Deployment Agent Status	Indicates the current status (started, stopped, working, waiting, or restarting) of the <i>Novell ZENworks Patch Management Update service</i> on the local device.



Agent Information

The following table describes the information in the Agent Information area of the Deployment tab:

Table 10.2 Agent Information

Field	Description
Last Checked Time	When the agent last communicated with the ZENworks Patch Management Server.
Next Checked Time	Next scheduled time when the agent will contact the ZENworks Patch Management Server.
Logging Level	The agent's current logging level. As defined in "Customizing and Administering Agent Policy Sets" .
Agent Listener Port	The port on which the agent will listen for communication. 0 = Disabled. Defined in "Customizing and Administering Agent Policy Sets" .

Log Operations

The following table describes the log operations:

Table 10.3 Log Operations

Use	To
View Agent Log	View the Agent's activity log.
Clear Agent Log	Clear the contents of the agent log.

To View the Agent Log

1. Click **View Agent Log**.

The Agent Log (ZENworks Patch Management Agent.log) opens

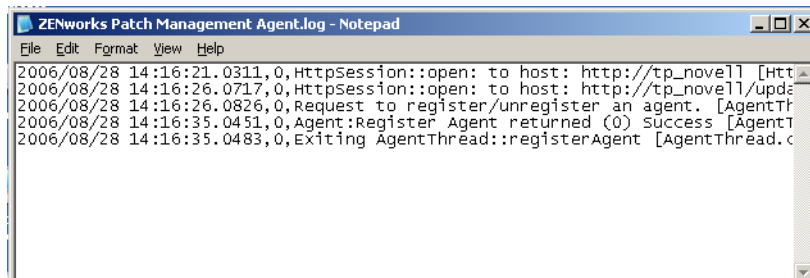


Figure 10.2 View Agent Log



To Clear the Agent Log

- 1. Click **Clear Agent Log**.
The Clear confirmation message dialog box opens.

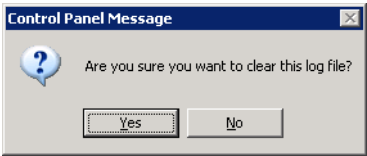


Figure 10.3 Clear Agent Log Message

- 2. Click **Yes**.
The system clears the Agent Log.

Agent Operations

The following table describes the Agent Operations area:

Table 10.4 Agent Operations

Use	To
Check Now	Cause the Agent to contact the ZENworks Patch Management Server.
Restart Agent	Restarts the ZENworks Patch Management Update service.

To Initiate Communication Between the Agent and the ZENworks Patch Management Server

- 1. Click **Check Now**.
- 2. The Agent initiates communication with the ZENworks Patch Management Server and checks for any pending tasks or deployments.
The *Last Checked Time* field reflects the current time.

To Restart the Agent

- 1. Click **Restart Agent**.
- 2. The Agent restarts.
The *Deployment Agent Status* field confirms that the Agent is restarting by displaying *Restarting*, and then *Started* when complete.



Detection Tab

The Detection tab is comprised of four functional areas.

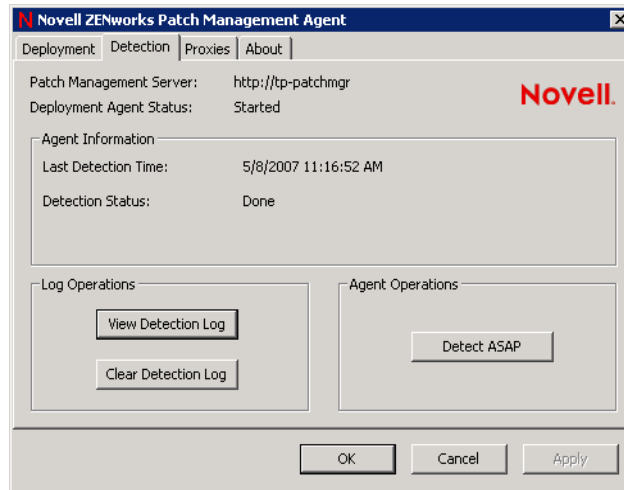


Figure 10.4 Detection Tab

Server Information and Status

The following table displays the ZENworks Patch Management Server location and the communication status:

Table 10.5 Server Information

Field	Description
Patch Management Server	The URL of the ZENworks Patch Management Server the agent is registered against.
Deployment Agent Status	Indicates the current status (started, stopped, working, waiting, or restarting) of the <i>Novell ZENworks Patch Management Update service</i> on the local device.



Agent Information

The following table describes the information in the Agent Information area of the Deployment tab:

Table 10.6 Agent Information

Field	Description
Last Detection Time	The last time the Discover Applicable Updates (DAU) task ran.
Detection Status	The status of the DAU task.

Log Operations

The following table describes the Log Operations area:

Table 10.7 Log Operations

Use	To
View Agent Log	View the Detection log.
Clear Agent Log	Clear the Detection log.

To View the Detection Log

- 1. Click **View Detection Log**
The *Detection Log* (ZENworks Patch Management Detection Agent.log) opens.

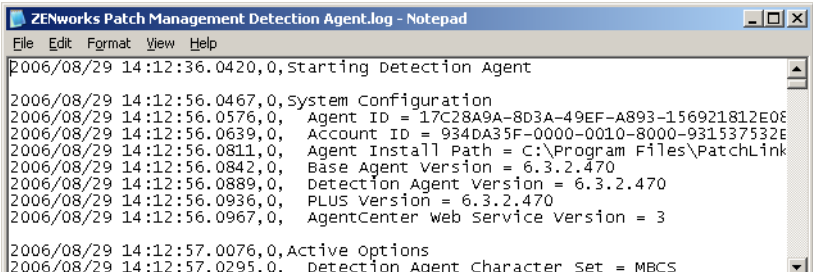


Figure 10.5 View Detection Log



To Clear the Detection Log

1. Click **Clear Detection Log**.
The Clear confirmation message dialog box opens.

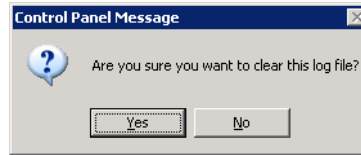


Figure 10.6 Clear Agent Log Message

2. Click **Yes**.
The system clears the Detection Log.

Agent Operations

The following table describes the Agent Operations area:

Table 10.8 Agent Operations

Use	To
Detect ASAP	Causes the agent to start a DAU as soon as possible.

To Prompt the Agent to Detect Vulnerabilities Immediately

1. Click **Detect ASAP**.
The Agent starts the DAU task.
The *Last Detection Time* field reflects the current time.



Proxies Tab

The Proxies tab allows you to configure proxy settings for communication with the ZENworks Patch Management Server.

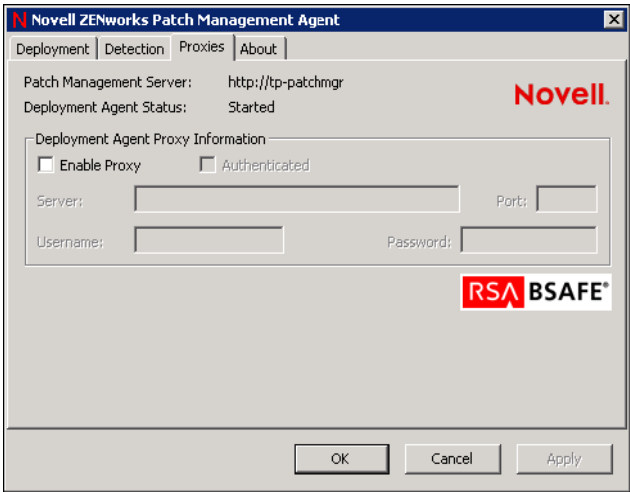


Figure 10.7 Proxies Tab

Server Information and Status

The following table displays the ZENworks Patch Management Server location and the communication status:

Table 10.9 Server Information

Field	Description
Patch Management Server	The URL of the ZENworks Patch Management Server the agent is registered against.
Deployment Agent Status	Indicates the current status (started, stopped, working, waiting, or restarting) of the <i>Novell ZENworks Patch Management Update service</i> on the local device.



Proxy Information

To Configure the Proxy Settings

1. Select **Enable Proxy**.
The **Server** and **Port** fields become active.
2. Type the *server's URL address* in the **Server** field.
3. Type the *Port* in the **Port** field.
4. If you are using an Authenticated proxy, select **Authenticated**.
The **Username** and **Password** fields become active.

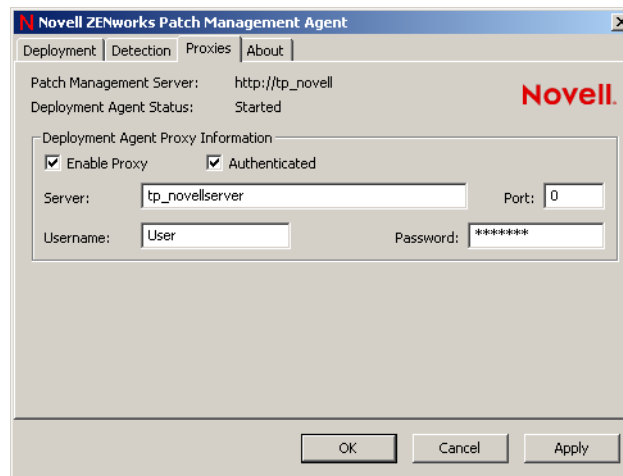


Figure 10.8 Proxy tab with both options activated

5. Type the *Username* in the **Username** field.
6. Type the *Password* in the **Password** field.
7. Click **OK**.
The confirmation dialog box opens.

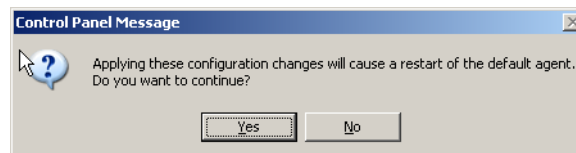


Figure 10.9 Proxy change confirmation



- 8. Click **Yes**.
The proxy information is saved.

About Tab

The About Tab displays information regarding the Agent and its associated ZENworks Patch Management Server.

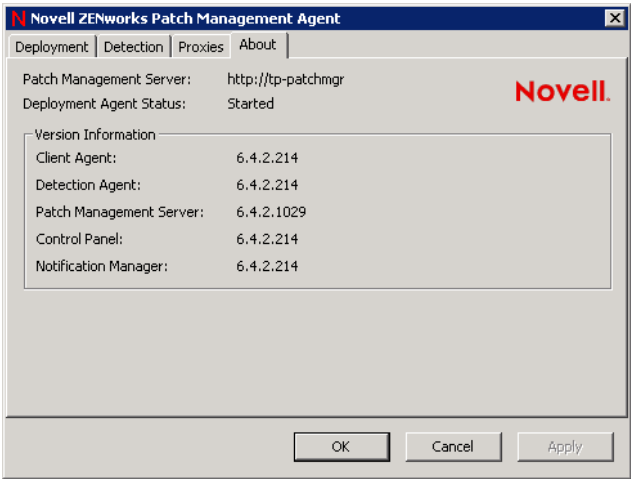


Figure 10.10 Proxies tab

Server Information and Status

The following table displays the ZENworks Patch Management Server location and the communication status:

Table 10.10 Server Information

Field	Description
Patch Management Server	The URL of the ZENworks Patch Management Server the agent is registered against.
Deployment Agent Status	Indicates the current status (started, stopped, working, waiting, or restarting) of the <i>Novell ZENworks Patch Management Update</i> service on the local device.



Version Information

The following table describes the Version Information area for the About tab:

Table 10.11 Version Information

Field	Description
Client Agent	Version number of the ZENworks Patch Management Agent.
Detection Agent	Version number of the Detection Agent.
Patch Management Server	Version number of the Patch Management Server.
Control Panel	Version number of the Control Panel.
Notification Manager	Version number of the Notification Manager.

User Interaction During a Deployment

After you create a deployment within ZENworks Patch Management Server, the agent can retrieve the deployment from the server. When the agent receives a deployment, if a deployment notification was enabled and a user is logged into the device, the Novell Desktop Deployment Manager displays on the Device screen.

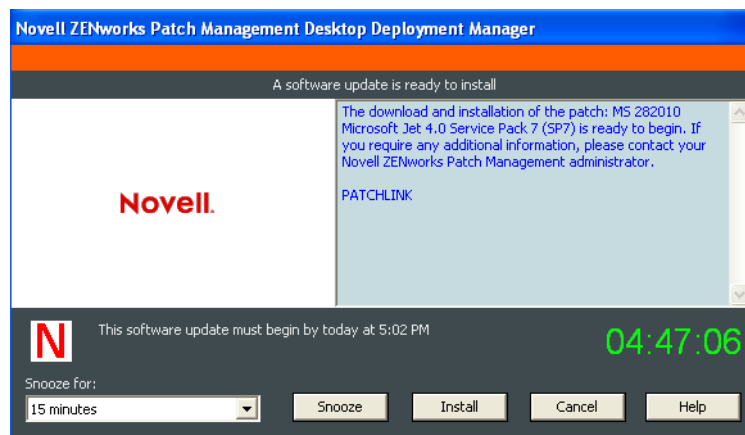


Figure 10.11 Novell Desktop Deployment Manager - Pending Deployment



An icon is also visible in the taskbar.



Figure 10.12 Install Icon

To Begin the Deployment

1. Click **Install**.
The Agent starts the deployment.

To Delay a Deployment

1. Select a *time frame* from the **Snooze for** drop-down list.
2. Click **Snooze**.
The deployment is delayed for the selected duration.

To Cancel a Deployment

1. Click **Cancel** (if Cancel is not available, your Administrator has disabled your ability to do so)
A confirmation dialog box displays, confirming your choice.
2. Click **Yes**.
The deployment is cancelled.



Note: If the deployment is part of a mandatory baseline, the Server will redeploy the patch until it is installed on the device.

User Interaction During a Reboot

If the agent must reboot the device, a user is logged into the device, and reboot notification was enabled, the Novell Desktop Deployment Manager will display on the Device screen.

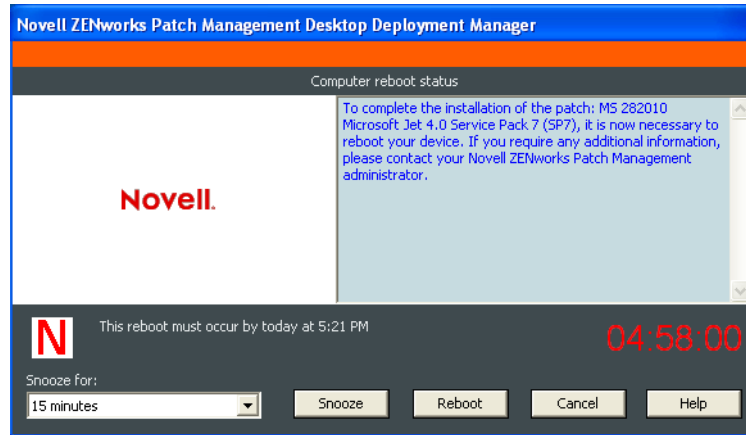


Figure 10.13 Novell Desktop Deployment Manager - Pending Reboot

An icon is also visible in the taskbar.

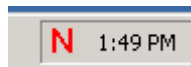


Figure 10.14 Install Icon

To Reboot Immediately

1. Click **Reboot**.
The Agent reboots the device.

To Delay the Reboot

1. Select a *time frame* from the **Snooze for** drop-down list.
2. Click **Snooze**.
The reboot is delayed for the selected duration.

To Cancel the Reboot

1. Click **Cancel** (if Cancel is not available, your Administrator has disabled your ability to do so)
A confirmation dialog box displays, confirming your choice.



- 2. Click Yes.
The reboot is cancelled.

About the ZENworks Patch Management Agent for Linux/Unix/Mac/Netware

The Linux/Unix/Mac/Netware Agent is a command line based application that does not have a user interface. While you are in the root directory, inside the Patch Service program, type:

```
user\local\patchagent\readme
```

Refer to the following commands to complete tasks within these agents:

Table 10.12 LUMN Agent Commands

Command	Description
info	General information about the Agent.
status	Status of the Agent process.
daustatus	Status of the Discover Applicable Updates task.
detect	Starts the detection task.
stop	Stop the Agent process.
restart	Stop and start the Agent process
patchdirectory	Sets the directory where patches will be temporarily downloaded.
setmacro	Specifies the macro definitions that should be used by the agent.
trimlogs	Trims the Update Agent logs.
archiveLogs	Archives the Agent logs so that they can be sent to Novell.
proxysetup	Set up your proxy server.
clearAgentLog	Clears the Update Agent error log file.
clearErrLog	Clears the Update Agent detection log file.
help	Displays the patch server script usage information.



About ZENworks Patch Management Agent for Windows Vista

The following section describes the Microsoft Vista Agent and its components.

Viewing the Agent

To Access the Update Vista Agent

1. Go to **Start > Control Panel**.
The *Control Panel* opens.
3. Select **Novell ZENworks Patch Management Agent**.
The *Agent Control Panel* opens.

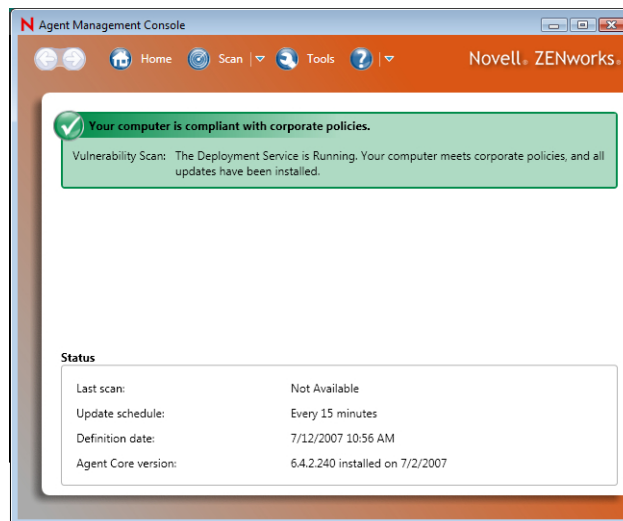


Figure 10.15 Control Panel

Agent Components

The following section describes the components of the ZENworks Patch Management Agent for Windows Vista and their functions.

- “Home Page”
- “Tools and Settings”



Home Page

The *Home* page is comprised of the following functional areas.

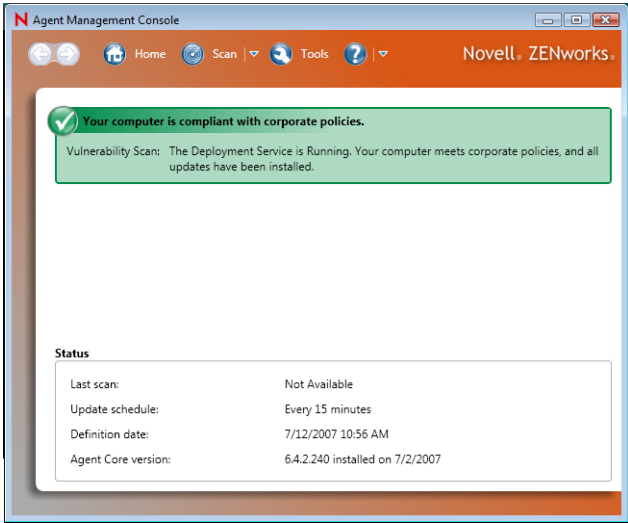


Figure 10.16 Vulnerability Detection Page

- **Compliance** - Displays whether your computer is compliant with corporate policies. The available values are as follow:

Table 10.13 Computer Compliance Status


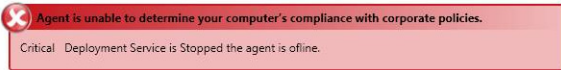


Status	Description	Displays
Compliant	Green (Service is running and the ZENworks Patch Management Agent is idle)	
Unable to Determine Compliance	Red (Service is not running)	



Table 10.13 Computer Compliance Status

Status	Description	Displays
Not Compliant	Yellow (Service is running and the ZENworks Patch Management Agent is busy)	 Your computer not is compliant with corporate policies. Vulnerability Scan: Deployment Service is Running your computer requires a reboot to finish installing updates.
Unable to Contact Server	Blue (Service is running and the ZENworks Patch Management Agent is offline or unknown)	 Your computer has not been able to contact the management server. Critical Deployment Service is Running the agent is in an unknown state.

- **Active Scan Statistics** - Only displays after clicking the **Scan** button. The *Active Scan Statistics* section will start a scan if one is not already active, and displays the **Scan Type**, **Start Time**, **Duration**, and **Status**.



Note: The scan **Start Time** and **Duration** values are only populated if you started the Scan. If the Scan was running prior to you clicking the **Scan** button, the exact start time duration are unknown.

- **Status** - Provides general Agent status values. Including the **Last Scan**, the **Update Schedule** (as defined by the Communication Interval), the scan **Definition Date**, and the **Agent Version**.

Tools and Settings

The Tools and Settings page is comprised of links to the following:

- **“Proxy Settings”** - The Proxy Settings link opens the Proxy Settings page, allowing you to view or modify the agent’s current proxy configuration.
- **“Logging”** - The Logging link opens the Log Files page, allowing you to view or clear the Agent log files.
- **“Notification Manager”** - The Notification Manager link opens the Notification Manager page, allowing you to define the Notification Manager behavior.
- **“Management Server”** - The Management Server link opens the Server Settings page.



Proxy Settings

The *Proxy Settings* page allows you to override the server provided proxy settings for communication with the ZENworks Patch Management Server.

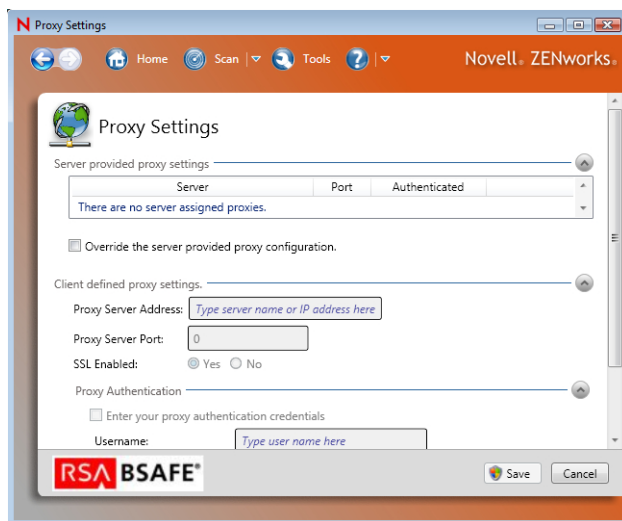


Figure 10.17 Proxy Settings

To Configure the Proxy Settings

1. Select **Override the Server Provided Proxy Settings**.
The *Proxy Server Address*, *Proxy Server Port* and *SSL Enabled* fields become active.
2. Type the *Proxy Server's Address* in the **Proxy Server Address** field.
3. Type the *Port* in the **Proxy Server Port** field.
4. If your proxy uses https, select the **SSL Enabled** field.
5. If you are using an Authenticated proxy:
 1. Select **Enter proxy authentication credentials**.
The *Username*, *Password*, and *Retype Password* fields become active.
 2. Type the *Username* in the **Username** field.
 3. Type the *Password* in the **Password** and **Retype Password** fields.
6. Click **Save**.
The proxy information is saved.

Logging

The Log Files page, provides buttons to view and clear the Agent log files.

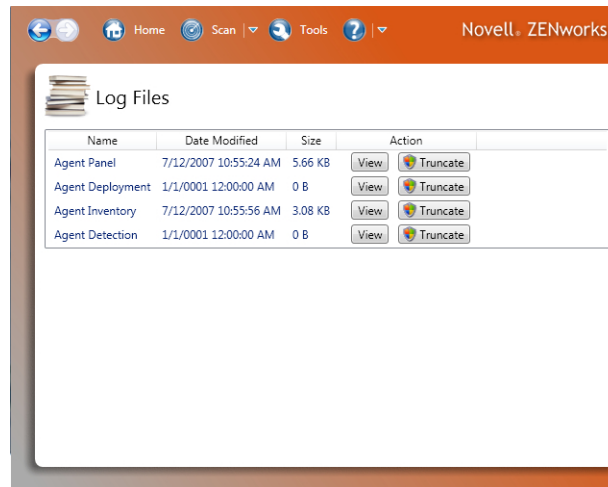


Figure 10.18 Log Files Page

To View a Log File

1. If desired, click the **Name**, **Date Modified**, or **Size** column heading to sort the log files.
2. Click the **View** button to open the **Log Detail** page.

To Clear a Log File

1. If desired, click the **Name**, **Date Modified**, or **Size** column heading to sort the log files.
2. Click the **Truncate** button to clear the log.

Log Detail Page

The Log Detail page displays the **Name**, **Size**, last **Updated** date, and log contents. From the *Log Detail* page, you can search the log contents, change to a single page, or facing pages view, and refresh.



Notification Manager

The Notification Manager page, comprised of the Notification Settings area, which provides the following information:

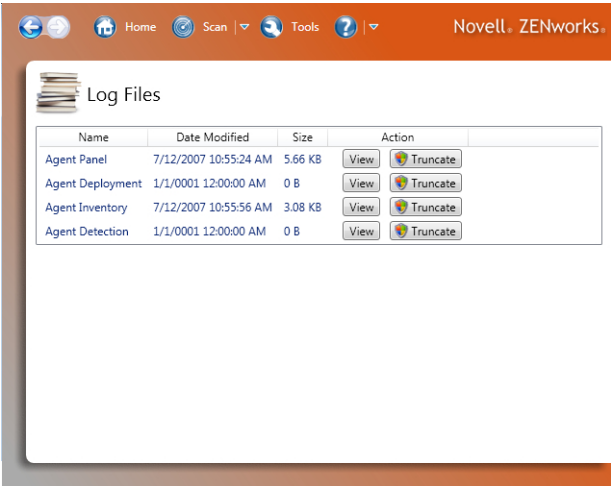


Figure 10.19 Notification Manager

- **Notification Manager Version** - Displays the version of the Notification Manager (for use by Technical Support).
- **Always Show Icon in System Tray** - When selected, will force the Novell Notification Manager icon to display in the Windows System Tray area.



Management Server

The *Server Settings* page is comprised of the *Patch Management Server Settings* area which provides the following:

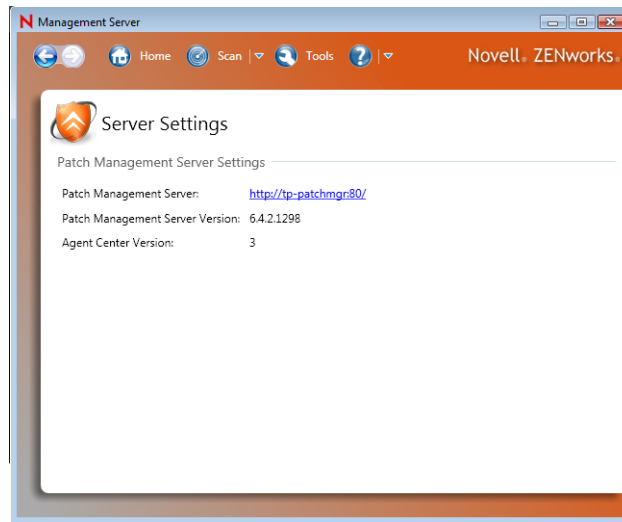


Figure 10.20 Server Settings

- **Patch Management Server Version** - Provides the version of the Patch Management Server that this agent is registered against.
- **Open Patch Management Server** - A link that, when clicked, will open the Patch Management Server in a web browser.
- **Agent Center Version** - Provides the associated Agent Center version (for use by Technical Support).



User Interaction During a Deployment

After you create a deployment within ZENworks Patch Management Server, the agent can retrieve the deployment from the server. When the agent receives a deployment, if a deployment notification was enabled and a user is logged into the device, the Novell Desktop Deployment Manager will display.

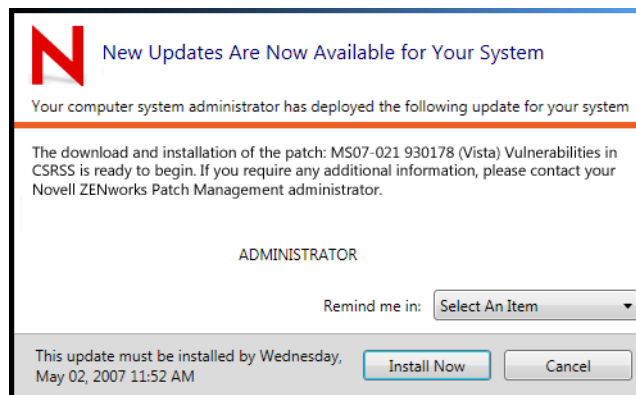


Figure 10.21 Novell Desktop Deployment Manager - Pending Deployment

When the Novell Desktop Deployment Manager displays, to indicate a pending deployment, you must select one of the following options:

- **Start the Deployment** - To begin the deployment:
 1. Click **Install Now**.
The Agent starts the deployment.
- **Snooze the Deployment** - To delay the deployment:
 1. Select a *time frame* from the **Remind me in** drop-down list.
The deployment is delayed for the selected duration.
- **Cancel the Deployment** - To cancel the deployment:
 1. Click **Cancel** (if Cancel is not available, your Administrator has disabled this function)
A confirmation dialog box displays, confirming your choice.
 2. Click **Yes**.
The deployment is cancelled.



Note: If the deployment is part of a mandatory baseline, the Server will redeploy the patch until it is installed on the device.

User Interaction During a Reboot

If the agent must reboot the device, a user is logged into the device, and reboot notification was enabled, the Novell Desktop Deployment Manager will display.

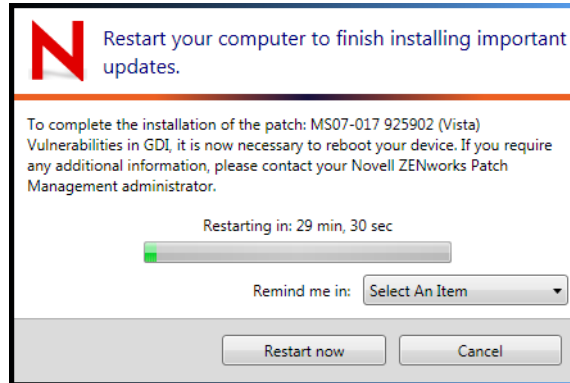


Figure 10.22 Novell Desktop Deployment Manager - Pending Reboot

When the Novell Desktop Deployment Manager displays, to indicate a pending reboot, you must select one of the following options:

- **Reboot the Device** - To reboot immediately:
 1. Click **Restart now**.
The Agent reboots the device.
- **Snooze the Reboot** - To delay the reboot:
 1. Select a *time frame* from the **Remind me in** drop-down list.
The reboot is delayed for the selected duration.
- **Cancel the Reboot** - To cancel the reboot:
 1. Click **Cancel** (if Cancel is not available, your Administrator has disabled your ability to do so)
A confirmation dialog box displays, confirming your choice.
 2. Click **Yes**.
The reboot is cancelled.





A Patch Management Server Reference

In this Appendix

- “Patch Management Server Security”
- “ZENworks Patch Management Server Error Pages”
- “WinInet Error Codes”
- “HTTP Status Codes”
- “ZENworks Patch Management Agent (Device) Status Icons”

Patch Management Server Security

There are multiple layers of security for ZENworks Patch Management:

Web Site Authentication

Internet Information Services (IIS) controls authentication in to the Patch Management Server web site, which means the operating system itself is validating users and their passwords.



Note: ZENworks Patch Management Server default security settings prohibit the use of any browser other than Internet Explorer 6 SP 1 and above. If you need to remove this restriction, **and disable the enhanced security settings** available with IE 6 SP1, refer to the [Novell Knowledgebase](#)

Web Site Encryption via SSL

SSL provides an encrypted wrapper around all web communication to and from the product. Therefore installing ZENworks Patch Management with SSL will provide another level of protection.

User (Security) Roles

Every feature, page and action throughout ZENworks Patch Management has been assigned to a series of Access Rights. These access rights combine together to form a user role. Roles also contain a list of devices and device groups. Regardless of how a user authenticated into ZENworks Patch Management, the access and permissions are defined solely by the Novell Administrator.



ZENworks Patch Management Server Error Pages

The ZENworks Patch Management Server provides several distinct error pages. These pages are:

- **Access Denied** - This page is displayed whenever a user fails to provide valid credentials when accessing ZENworks Patch Management Server or they attempt to access an area of ZENworks Patch Management to which they do not have access.
- **Internal Server Error** - This page is displayed whenever an unspecified internal error occurs. In most cases, closing the browser window and restarting your task within ZENworks Patch Management will resolve the issue.
- **Refresh User Data** - This page is displayed whenever the current session expires, such as when there has been an extended period of inactivity.
- **Requested Page Not Found** - This page is displayed whenever a user attempts to navigate to an address that does not exist on the ZENworks Patch Management Server. Links are provided to common sections of the ZENworks Patch Management Server to assist the user in returning to their desired location within ZENworks Patch Management.
- **System Component Version Conflict** - This page is displayed whenever a system component version conflict is detected. To ensure optimal behavior, the system components of the ZENworks Patch Management Server are checked every time a user logs into the site. If a conflict is detected, this page identifies the component(s) that caused the conflict. The ZENworks Patch Management Server will also send a notification e-mail to the Novell Administrator when a conflict occurs.
- **Cache Expired** - This page is displayed whenever the user session expires. Usually the result of an extended period of inactivity.
- **Unsupported Browser Version** - This page is displayed whenever a user visits the ZENworks Patch Management Server with an unsupported browser.



WinInet Error Codes

ZENworks Patch Management uses Microsoft's WinInet API for communication between the Agents and Server. When this communication fails, the error codes returned are WinInet error codes. The following table defines the most commonly seen error codes:

Table A.1 ZENworks Patch Management Agent Error Codes

PL Agent Error Description	WinInet Error Code	Description
Head failed: Head request failed. Error is 12002. . Host=1116 HTTP Error=0	12002	The internet connection timed out
Head failed: Head request failed. Error is 12031. . Host=1109 HTTP Error=0	12031	The connection with the server has been reset
Head failed: Head request failed. Error is 12007. . Host=1109 HTTP Error=0	12007	The server name could not be resolved
Refer to Microsoft knowledgebase article #193625 for additional details regarding the WinInet error codes.		

HTTP Status Codes

As a Web based application using Internet Information Services (IIS), Novell ZENworks Patch Management uses HTTP status codes. While many of the status codes are informational only, the following table defines a few of the common errors:

Table A.2 HTTP Status Codes

Code	Description
HTTP 401.1 - Logon failed	Logon attempt was unsuccessful (likely due to invalid user name or password). Note: ZENworks Patch Management Server will display a custom error page (as defined under “ZENworks Patch Management Server Error Pages”) instead of the default HTTP 401.1 - Logon failed error page
HTTP 403.4 - SSL Required	You must use HTTPS instead of HTTP when access this page.
Refer to Microsoft knowledgebase article #318380 (http://support.microsoft.com/kb/318380/) or the W3C Protocol definition (http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html) for additional details regarding HTTP Status Codes.	



Table A.2 HTTP Status Codes

Code	Description
HTTP 403.9 - Too many users	The number of connected users exceeds the defined connection limit.
HTTP 404 - Not found	The requested file cannot be found. Note: ZENworks Patch Management Server will display a custom error page (as defined under “ZENworks Patch Management Server Error Pages”) instead of the default HTTP 404 - Not Found error page
Refer to Microsoft knowledgebase article #318380 (http://support.microsoft.com/kb/318380/) or the W3C Protocol definition (http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html) for additional details regarding HTTP Status Codes.	

ZENworks Patch Management Agent (Device) Status Icons

The following table defines agent (device) status and associated icons.

Table A.3 Device Status Icons























Active	Pending	Description
	N/A	The agent is currently working on a deployment (animated icon).
		The agent is idle, and has pending deployments.
		The agent is offline.
		The agent is sleeping due to its Hours of Operation settings.
		This agent has been disabled.
		The agent is offline and is in a QChain status (can accept chained deployments only after reboot).
		The agent is offline and is in a Reboot status (can accept no more deployments until after it reboots).
		The agent is in a QChain status (the agent can accept chained deployments only until after a reboot).



Table A.3 Device Status Icons

Active	Pending	Description
		The agent is in a Reboot status (the agent can accept no more deployments until after it reboots).
		The agent is in a QChain status (the agent can accept chained deployments only until after a reboot) and is sleeping due to its Hours of Operation settings.
		The agent is in a Reboot status (the agent can accept no more deployments until after it reboots) and is sleeping due to its Hours of Operation settings.
	N/A	Unable to identify the agent status.





B Securing Your ZENworks Patch Management Server

This appendix identifies various options to secure ZENworks Patch Management Server.

In this Appendix

- “Install Your Server With SSL”
- “Use Secure Passwords”
- “Turn Off File and Printer Sharing”
- “Put Your ZENworks Patch Management Server Behind a Firewall”
- “Turn Off Non-Critical Services”
- “Lock Down Unused TCP and UDP Ports”
- “Apply All Microsoft Security Patches”

Install Your Server With SSL

Secure Sockets Layer (SSL) is a protocol used to secure data transmitted over the internet. SSL support is included in browsers, web servers, and operating systems so that any type of client and server can use authenticated and encrypted communications over private as well as public networks.

Novell ZENworks Patch Management always uses SSL when downloading vulnerability data and packages from the Global Subscription Server. Additionally, SSL can be used when transmitting data between the ZENworks Patch Management Server and ZENworks Patch Management Agents by enabling SSL during the ZENworks Patch Management Server installation. This process involves obtaining a SSL certificate (.CER), and installing the certificate during the ZENworks Patch Management Server installation. Refer to the *ZENworks Patch Management Server 6.4 Server Installation Guide* for details regarding installing with SSL enabled.

Use Secure Passwords

Worm attacks frequently try to log in with weak and commonly used passwords. For secure passwords, the Department of Defense standard of 12 characters with alpha, numeric, punctuation and mixed case characters all included in a password is recommended.



Turn Off File and Printer Sharing

An intruder can exploit a Windows networking share. Additionally, ZENworks Patch Management Server should not be used as a file or print server. Therefore, *File and Printer Sharing for Microsoft Networks* should be disabled.

To Turn Off File and Printer Sharing

1. From within the *Windows Control Panel*, select the **Network Connections** icon.
2. Open the **Local Area Connection**.
3. Click **Properties**.

The *Local Area Connection Properties* window opens.

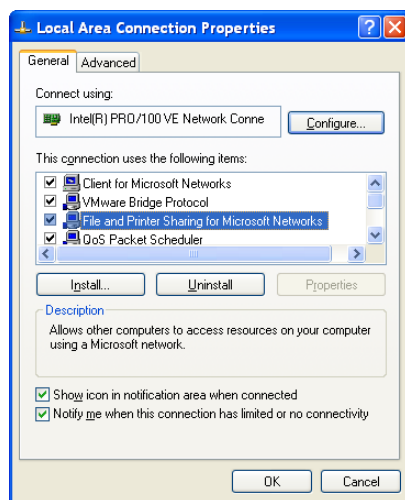


Figure B.1 Turn Off Windows Networking

4. Select **File and Printer Sharing for Microsoft Networks**.
5. Click **Uninstall**.
File and Printer Sharing for Microsoft Networks is removed.
6. Click **OK**.
The *Local Area Connection Properties* window closes.



Note: Do not uninstall *Client for Microsoft Networks* because it is required by both Microsoft SQL Server and Internet Information Server.

Put Your ZENworks Patch Management Server Behind a Firewall

Since the ZENworks Patch Management Server receives its patch updates from the Global Subscription Server, there is no need to allow access from the Internet into the Patch Management Server. However, access to the Global Subscription Server must be specified in your Firewall configuration.

Turn Off Non-Critical Services

The default installation of Microsoft Windows has most features and services active. Therefore, there are a number of services that can be turned off (e.g.: RPC, Remote Registry, etc.) to reduce the risk of outside attacks. Novell does not encourage this type of lock down, however it can be an effective method to reduce the risk of hacker attacks.

The following services are required to run ZENworks Patch Management:

- World Wide Web Publishing Service
- IIS Admin Service
- MSSQLSERVER
- ZENworks Patch Management

Lock Down Unused TCP and UDP Ports

Preventing network traffic on various unused and vulnerable TCP and UDP ports should be completed through the use of a firewall. However, if a firewall is not available or additional machine level locking is desired, TCP and UDP ports can be locked down as a function of the network connection.

To Lock Down Unused Ports

1. From within the *Windows Control Panel*, select the **Network Connections** icon.
2. Open the **Local Area Connection**.



- 3. On the *Local Area Connections Status* General tab, click **Properties**. The *Local Area Connection Properties* window opens.

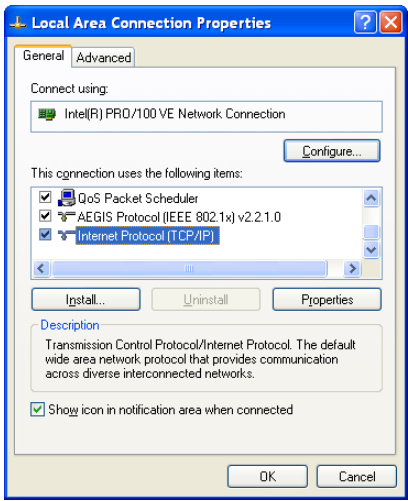


Figure B.2 Local Area Connection Properties

- 4. Select the *Internet Protocol (TCP/IP)* protocol.
- 5. Click **Properties**. The *Internet Protocol (TCP/IP) Properties* window opens.

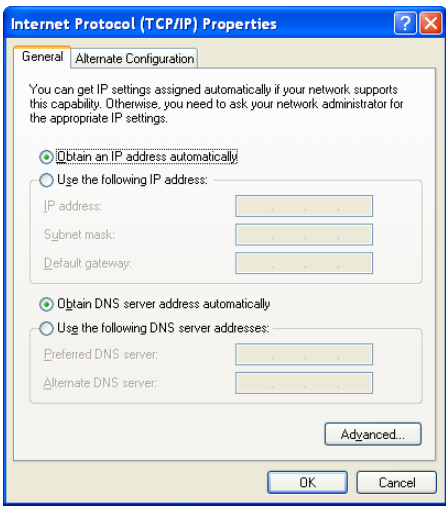


Figure B.3 General tab



6. In the *General* tab click **Advanced...**
The *Advanced TCP/IP Settings* window opens.
7. Select the **Options** tab.

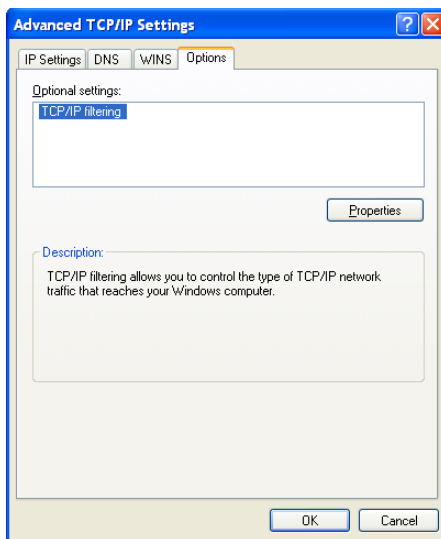


Figure B.4 Advanced TCP/IP Settings

8. Select *TCP/IP filtering*.
9. Click **Properties**
The *TCP/IP Filtering* window opens.
10. Enable the **Enable TCP/IP Filtering (All adapters)** option.



11. Select the **Permit Only TCP Ports** option.

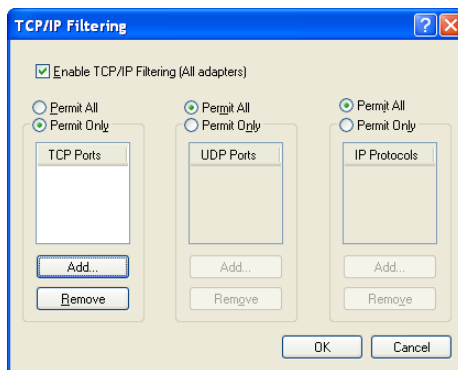


Figure B.5 TCP/IP Filtering

12. Add TCP ports 443 and 80 to the listing of permitted ports.
 - a. Click **Add...**
Add Filter window opens.
 - b. Type *443* in the **TCP Port** field.
 - c. Click **OK**.
The Filter window closes.
 - d. Repeat steps a, b, and c to add port 80.
 - ◆ No other ports are required, though you may want to allow DNS, TS, or VNC.
13. Select the **Permit Only UDP Ports** option.
 - Leave the UDP Ports window blank since no UDP ports are required.



Warning: If all ports are locked except ports 80 and 443, it will be necessary to add entries for www.novell.com, the Global Subscription Server, and your Proxy to your HOSTS file.

14. Close the open windows.

Apply All Microsoft Security Patches

Apply all applicable Microsoft Security Patches to ensure that the server remains protected against all known security threats. Be sure to apply the most recent patches for IIS, SQL Server, and Windows Server 2003.



C Using the Content Update Tool

With the advent of subscription support, some software manufacturers require a subscription to download software patches and updates. Due to this subscription model some vulnerabilities retrieved from the Global Subscription Server cannot include the vendor's patch. It is the Content Update Tool that will allow you to associate these vulnerabilities with the patches you download from the vendor. By associating these patches with the vulnerability details retrieved from the Global Subscription Server, you can continue to use the power and convenience of Novell ZENworks Patch Management when maintaining your network.

Content Update Tool System Requirements

Supported Operating Systems

The Content Update Tool is supported on the following Operating Systems:

- Microsoft Windows Server™ 2003 Standard Edition with SP1
- Windows Server 2003 Enterprise Edition with SP1

Hardware Requirements

- 512 MB of RAM *
- Minimum of 50 MB of Disk Space *
- 1 GHz Processor or higher

* The actual RAM and disk space requirements will vary depending upon the size of the imported patches.

Other Requirements

- Novell ZENworks Patch Management Server 6.4
- An active network connection to your ZENworks Patch Management Server
- Microsoft Windows Installer 3.0
- Microsoft .NET Framework 2.0
- Local / Domain Administrator or Administrator equivalent
- Administrator (Admin) rights to Novell ZENworks Patch Management
- An active Internet Connection



Installing the Content Update Tool

The Content Update Tool is available as a download from the *Agent Installers* page of your ZENworks Patch Management Server.

Downloading the Content Update Tool From ZENworks Patch Management Server

1. Log on to the target computer as the local **administrator** (or a member of the **LOCAL_ADMINS** group).
2. Launch your web browser.
3. Type your ZENworks Patch Management Server URL in your web browser's *Address* field. Press **Enter**.
4. Type your **User Name** in the *User name* field. Press **TAB**.
5. Type your **password** in the *Password* field.
6. Click **OK**.
The *ZENworks Patch Management Server Home* screen opens.
7. Select **Devices**.
8. Click **Install**.
The *Agent Installers* page opens.

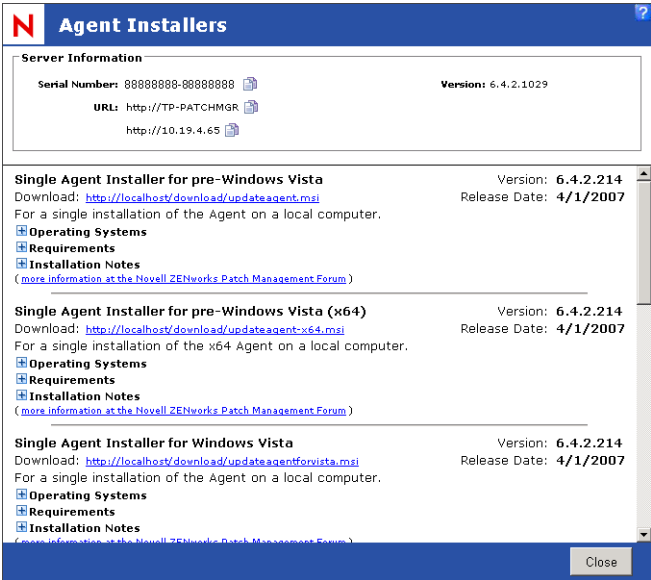


Figure C.1 Agent Installers



9. From the *Agent Installers* window, select the Content Update Tool download link.
The *File Download* dialog box opens.
10. In the *File Download* dialog box, click **Save**.
The *Save As* window opens.
11. Specify the location to save the `ContentUpdateTool.msi` file, and click **Save**.
The `ContentUpdateTool.msi` file saves to the specified location.

Installing the Content Update Tool

1. From the downloaded location, select the `contentupdatetool.msi` to extract the *Content Update Tool Installation Wizard*.
The *Content Update Tool Welcome* page opens.

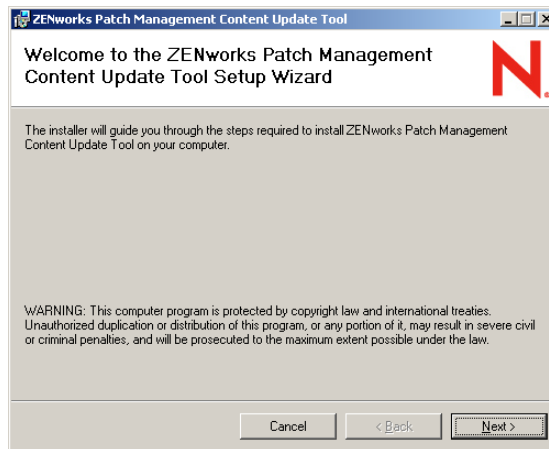


Figure C.2 Installation Wizard - Welcome



- 2. Click **Next**.
The *License Agreement* page opens.

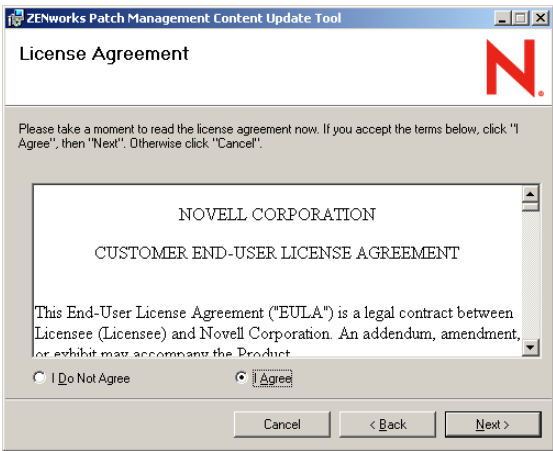


Figure C.3 Installation Wizard - License Agreement

- 3. If you agree with the license agreement select **I Agree**.
- 4. Click **Next**.
The *Select Installation Folder* page opens.

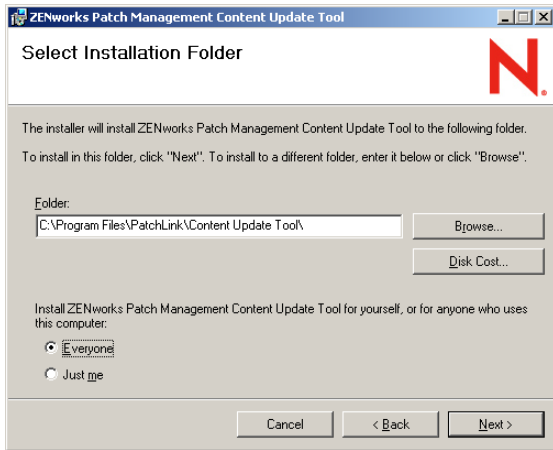


Figure C.4 Installation Wizard - Select Installation Address



5. If a different **Installation Folder** is required:
 - a. Click **Browse...**
The *Select Folder* window opens.
 - b. Select a new folder and click **Save**.
The *Select Folder* window closes, returning to the *Select Installation Address* page with the new path displayed.



Note: Clicking **Disk Cost...** will display your available installation drives and each drive name (*Volume*), *Disk Size*, *Available* space, space *Required* for installation, and the space remaining after the installation (*Difference*).

6. If you want all users of this computer to have access to the Content Update Tool select **Everyone**.
7. Click **Next**.
The *Confirm Installation* page opens.

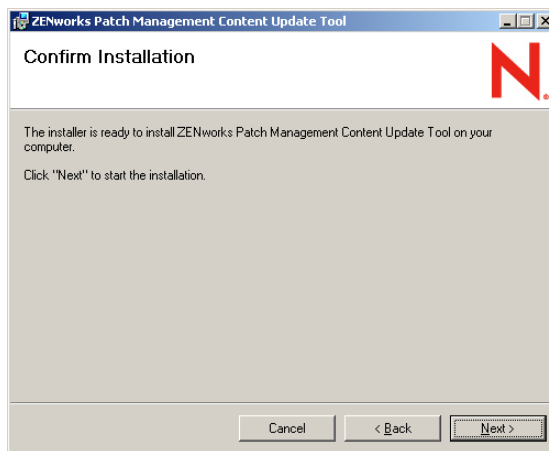


Figure C.5 Installation Wizard - Confirm Installation



8. Click **Next** to install.

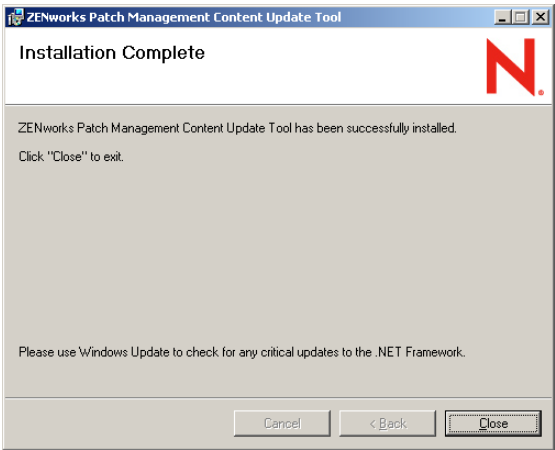


Figure C.6 Installation Wizard - Installation Complete

9. Click **Close** to exit the wizard.



Using the Content Update Tool

The Content Update Tool is a wizard-based utility that will guide you through the process of associating your vulnerability definitions with vendor supplied patches.

To Open the Content Update Tool Wizard

1. Select **Start > Programs > Novell > Novell ZENworks Patch Management Content Update Tool 6.4** to start the Content Update Tool.

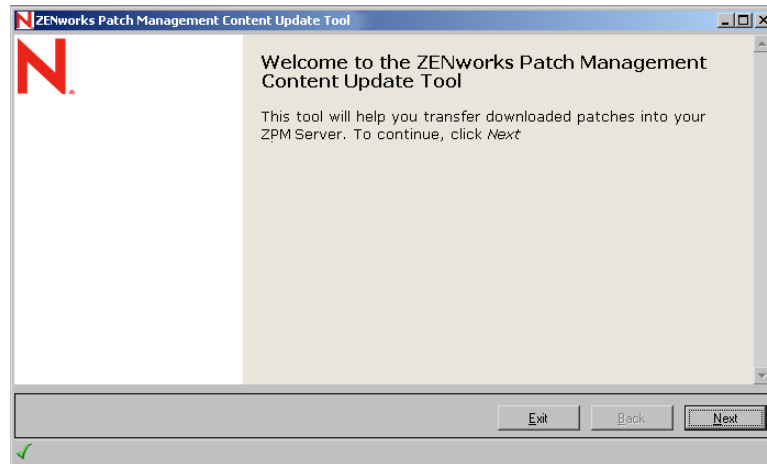


Figure C.7 Welcome page

2. Click **Next**.
The *Configuration Page* opens.



Note: Only users with the Administrator User Role will be able to use the Content Update Tool.



Configuration Page

The Configuration page contains the configuration settings required to communicate with your ZENworks Patch Management Server and the Global Subscription Server. You must provide the following configuration details before you can continue.

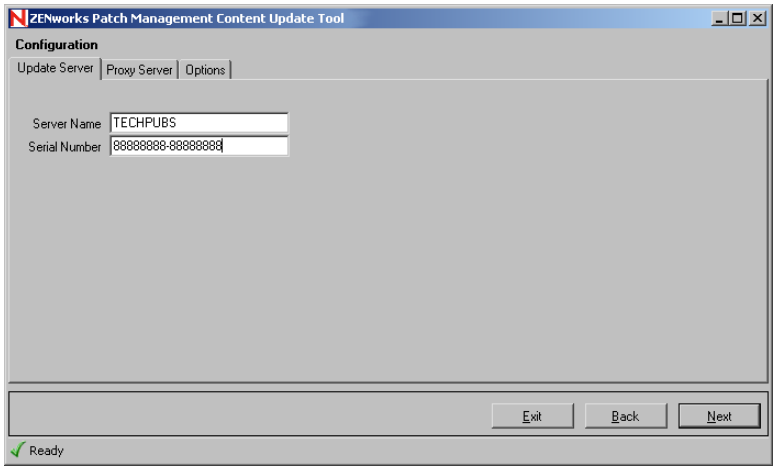


Figure C.8 Configuration page



Configuring the Content Update Tool

1. Enter the following data:

Table C.1 Configuration Field Descriptions

Field	Description
ZPM Server Tab	
Server Name	The name of your ZENworks Patch Management Server. Note: The Windows user you logged in as must also have administrator access to this ZENworks Patch Management Server.
Serial Number	The ZENworks Patch Management Server serial number. (Can be found on the Home page of your ZENworks Patch Management Server.)
Proxy Server Tab	
Use Proxy	Select if a proxy is required during the communication between the Content Update Tool and your ZENworks Patch Management Server. Selecting this option will enable the Proxy Server and Port fields.
Proxy URL	The proxy server's name. (Do not include the <code>http://</code> or <code>https://</code> prefix.)
Port	The proxy server's port.
Authenticated Proxy	Select if the defined proxy requires a User Name and Password. Selecting this option will enable the Username and Password fields.
Username	The user name used when connecting via the defined proxy.
Password	The password associated with the defined user name.
Options Tab	
Use SSL	Select to use SSL during communication with your ZENworks Patch Management Server. Note: Should only be enabled if your ZENworks Patch Management Server Web site is using SSL.
Log Errors	Select to enable Error Logging.
Product Information	Displays the Content Update Tool version and copyright information.



Note: The configuration details are saved to the **ContentUpdate.xml** file, with a default location of C:\Program Files\Novell\Content Update Tool\ContentUpdate.xml, and will be pre-populated the next time you load the Content Update Tool.

- 2. Click **Next**.
The *Vulnerability Selection* page opens.

Vulnerability Selection Page

Complete the following steps to select Vulnerabilities.

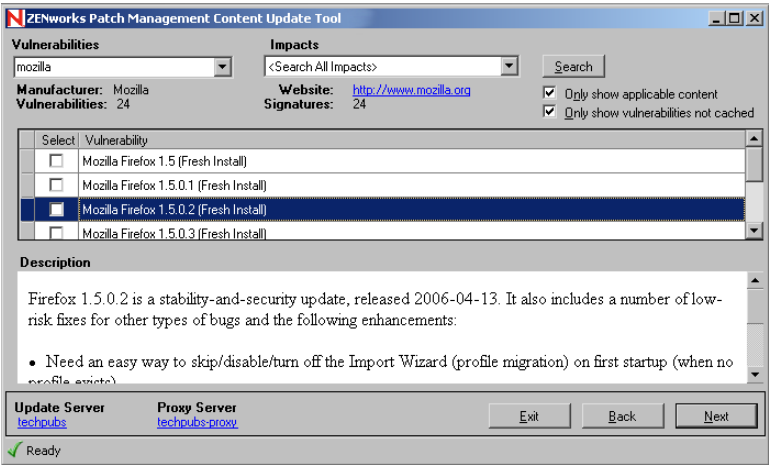


Figure C.9 Vulnerability Selection page

Selecting Vulnerabilities

- 1. Type a search string in the **Search** field (or select a vendor using the drop-down arrow).



Note: When selected the **ZENworks Patch Management Server** and **Proxy Server** links at the bottom of the page will return you to the Configuration page.

- 2. Select a vulnerability impact in the **Impacts** field.
- 3. Select the **Only show applicable content** option to limit the results to only those vulnerabilities applicable to those devices managed by your ZENworks Patch Management Server.



4. Select the **Only show vulnerabilities not cached** option to limit the results to only those vulnerabilities which have not already been cached.
5. Click **Search**.
The Vulnerabilities grid will display the results of your search.
6. Select the desired vulnerabilities by selecting (or de-selecting) the checkboxes in the Selected column.
7. When selecting vulnerabilities, the following reference fields are available:
 - **Manufacturer** - The manufacturer of the currently selected vulnerability.
 - **Website** - The manufacturer's website.
 - **Vulnerabilities** - The total number vulnerabilities from the selected manufacturer.
 - **Signatures** - The total number of signatures from the selected manufacturer.
 - **Description** - A description of the currently selected vulnerability.
8. Click **Next**.
The Vulnerability metadata will be downloaded from the Novell Global Subscription Server and the *Package Selection* page will open when complete.



Package Selection Page

When the Package Selection page first opens, the signatures associated with the vulnerabilities you selected will display. You must associate each signature with a file to continue.

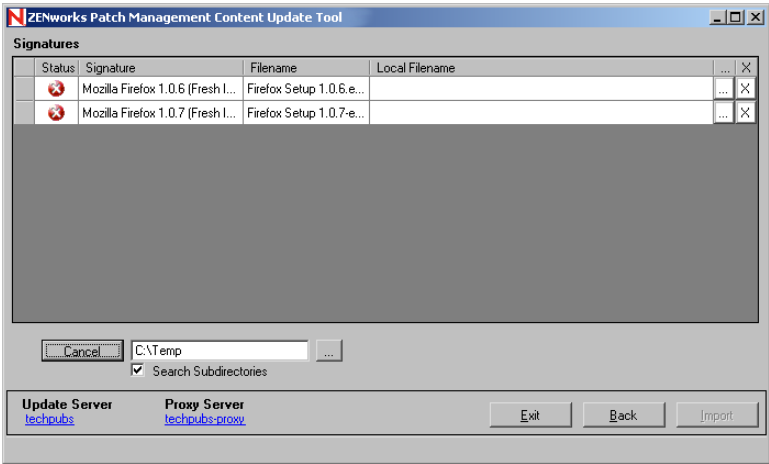


Figure C.10 Package Selection page



Note: Only signatures which include a package definition will be displayed by the Content Update Tool. If the selected vulnerability does not contain at least one package definition you cannot proceed.



Performing an Automatic Selection of the Package Components

1. Type, or browse to (using the ellipsis button), the target search directory.

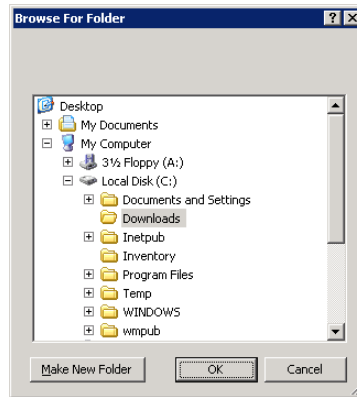


Figure C.11 Browse for folder

2. If desired, select the **Search Subdirectories** option to include any sub-folders in the search.
3. Click **Search**.



Note: When you perform an automatic selection the Content Update Tool will attempt to associate the selected vulnerabilities with files found in the defined Search directory. If the automatic selection is unable to find all of the necessary packages, you must either repeat the search using a different directory, or manually select the package components (see “[Manually Selecting the Package Components](#)”)

Note: Only files that are an exact match to the vulnerabilities metadata (including the filename, file size, checksum, etc.) will be automatically selected.



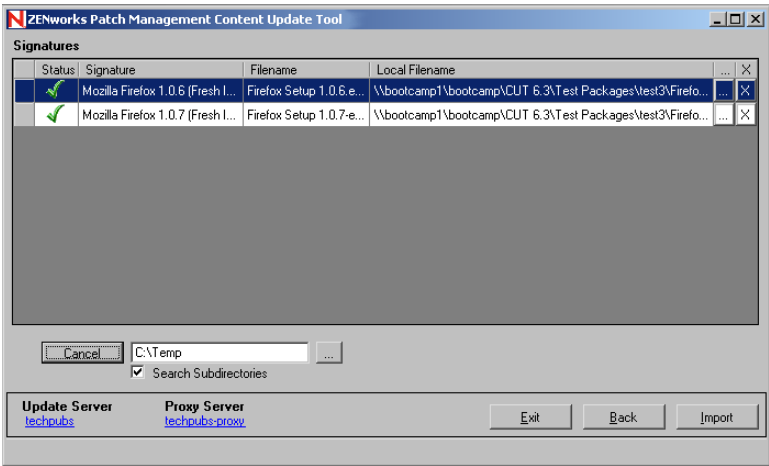


Figure C.12 Package Selection page - ready for import

- 4. Click **Import** to begin the package import.
The package components are uploaded to your ZENworks Patch Management Server and the *Summary Report* page will open when complete.



Manually Selecting the Package Components

1. Within the results grid, Select the ellipsis (...) button associated with the signature.
2. Browse to the desired file.
The name of the file you select must match the filename defined in the vulnerability metadata (as displayed in the Filename column).
3. Click **Open** to select the file and return to the Package Selection page.

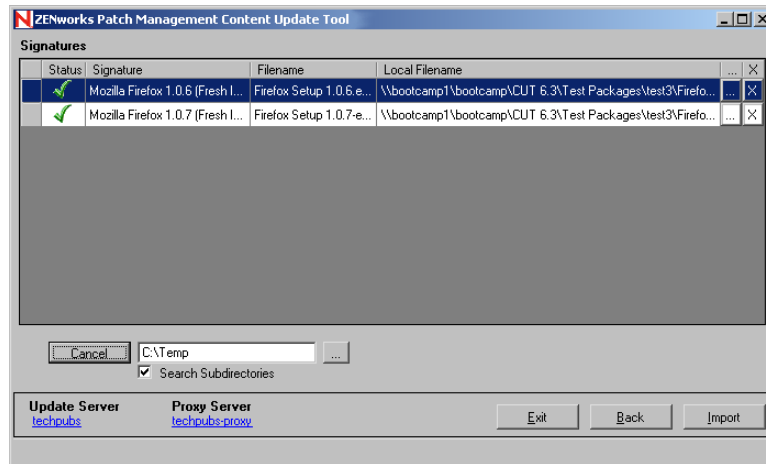





Figure C.13 Package Selection page - ready for import

The following status icons are displayed in the Status column:

Table C.2 Package Status Icons

Icon	Definition
	The green check indicates that the package component file has been found and is consistent with the vulnerability definition.
	The yellow caution indicates that the package component file has been found but it is NOT consistent with the vulnerability metadata.
	The red X indicates the package component file has not been found.

4. Click **Import** to begin the package import.
The package components are uploaded to your ZENworks Patch Management Server and the *Summary Report* page will open when complete.





Warning: Although the Content Update Tool will allow you to force an import when the package is not an exact match to the vulnerability definition , this practice is discouraged. Possible reasons for the package not matching include file corruption and tampering.

Warning: If you choose to perform the import although the package is not an exact match to the vulnerability definition, the text **User Modified** will be added as a prefix to the vulnerability name. Additionally, a listing of what properties failed to match will be added to the beginning of the vulnerability description.

Summary Report

The Summary Report page displays the results of the Content Update Tool updates to your ZENworks Patch Management Server.

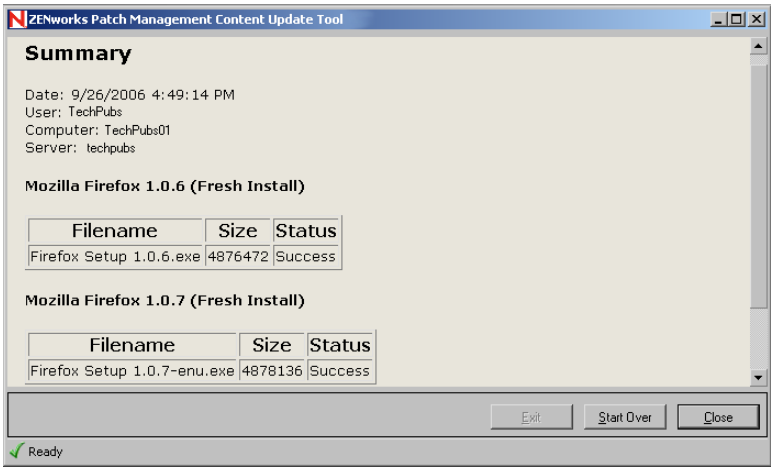


Figure C.14 Summary Report page

Following the package import you may perform another import (**Start Over**) or exit (**Close**) the wizard.



D Creating a Disaster Recovery Solution

The most important part of an effective disaster recovery solution is having a current and valid backup. You can create backups either manually or as part of a Database Maintenance Plan.

In this Appendix

- “Preparing Your Database”
- “Creating an Automated Solution”
- “Creating a Manual Solution”



Note: This appendix applies to *Microsoft SQL Server 2005* and requires the *Microsoft SQL Server Management Studio*. The Management Studio is available by upgrading to SQL Server 2005 Standard or Enterprise or as a download from the [Microsoft Download Center](http://www.microsoft.com/downloads/details.aspx?familyid=82AFBD59-57A4-455E-A2D6-1D4C98D40F6E) (<http://www.microsoft.com/downloads/details.aspx?familyid=82AFBD59-57A4-455E-A2D6-1D4C98D40F6E>).

Preparing Your Database

The installation of ZENworks Patch Management sets your database to a recovery model of *Simple*. To use *Transaction Logs*, and thus increase the quality of your disaster recovery solution, you should change the recovery model to *Full*.

Changing Your Database Recovery Model

1. Open the *Microsoft SQL Server Management Studio* (**Start > Programs > Microsoft SQL Server 2005 > SQL Server Management Studio**).
2. Log into your database server.
3. Expand your server group, server, and database folder until you see the **PLUS** database.
4. Right-click on the **PLUS** database.



- 5. Select **Properties**.
The *Database Properties* window opens.

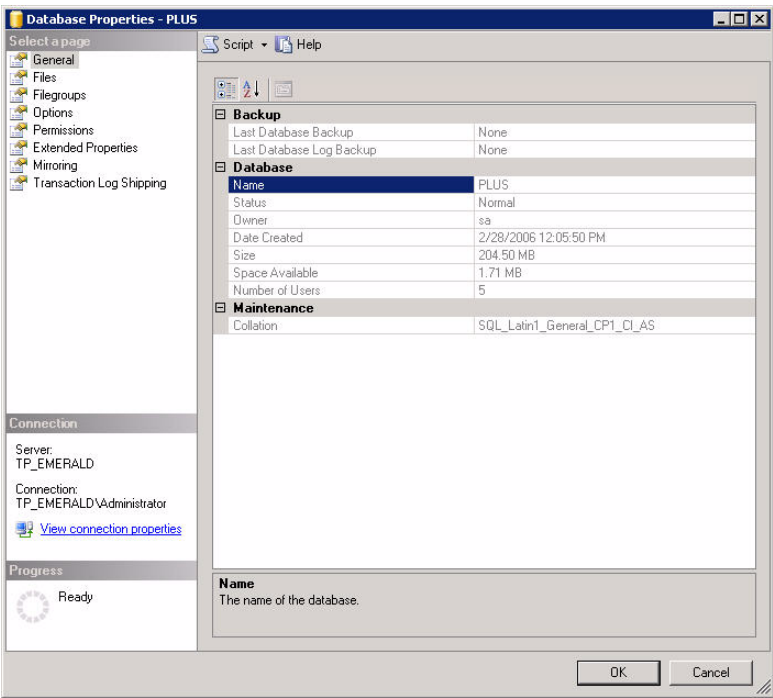


Figure D.1 Database Properties

- 6. Select *Options* within the **Select a page** field.
The Options page displays.



7. In the **Recovery model:** field select **Full**.

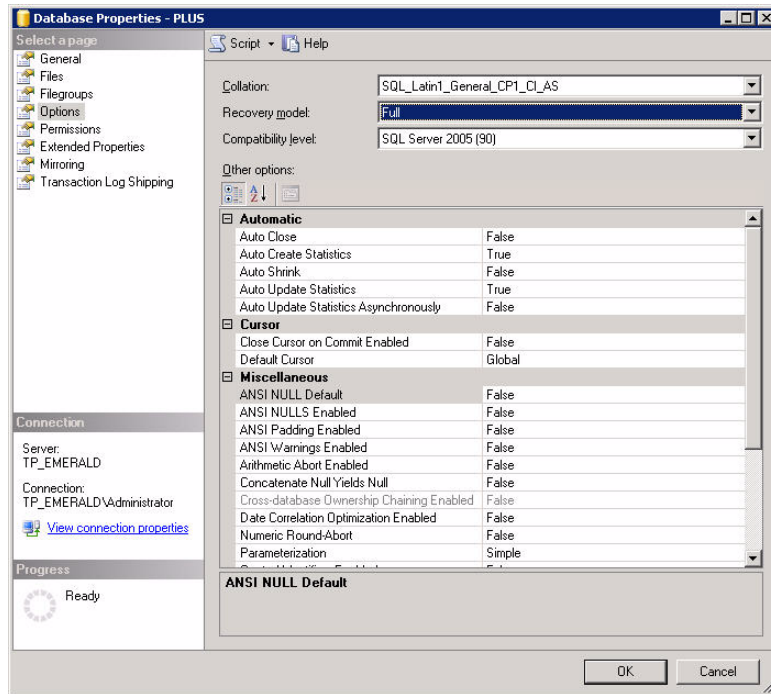


Figure D.2 Database Properties - *Options* page

8. Click **OK**.
The changes are saved the the *Database Properties* window closes.
9. Repeat steps 4 through 8 for the **PLUS_Staging** database.



Note: You must create a backup (of each database), before any *Transaction Logs* will be created. Refer to “**Creating a Database Backup**” for details on creating a one-time backup of your database.



Creating an Automated Solution

A Maintenance Plan allows you to create an automated backup and schedule the backup to occur as frequently as your organizational needs dictate. Maintenance Plans allow you to define your back up options as well as which databases and transaction logs to include.



Note: If you have not already done so, you should change your Database Recovery Model to FULL before continuing. Refer to “[Preparing Your Database](#)” for additional details.

Creating a Maintenance Plan



Warning: You can only create a Maintenance Plan if you have:

1. Upgraded to *Microsoft SQL Server 2005 Standard* or *Microsoft SQL Server 2005 Enterprise*.
2. During the Upgrade, you selected to install *SSIS (SQL Server Integration Services)*. If necessary, rerun the *SQL Server 2005* upgrade to add SSIS.
3. The *SQL Server Agent* is started with a startup type of *Automatic*.

1. Open the *Microsoft SQL Server Management Studio* (**Start > Programs > Microsoft SQL Server 2005 > SQL Server Management Studio**).
2. Log in to your database server.
3. Expand your server group, server, and the Management folder until you see the *Maintenance Plans* folder.
4. Right-click on the Maintenance Plans folder.

5. Select **Maintenance Plan Wizard**.

The *Database Maintenance Plan Wizard - Welcome* page opens.

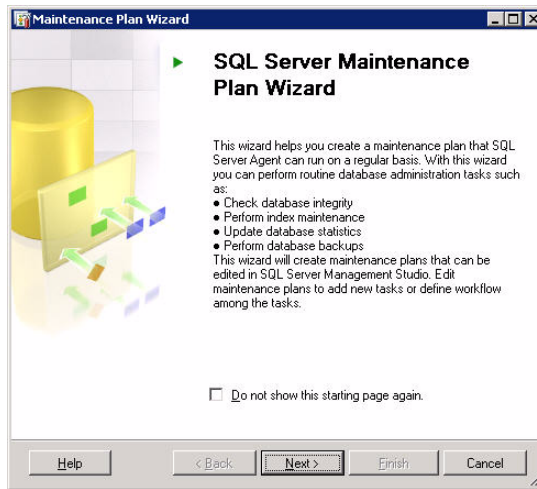


Figure D.3 Maintenance Plan Wizard - Welcome

6. Click **Next**.

The *Select a Target Server* page opens.

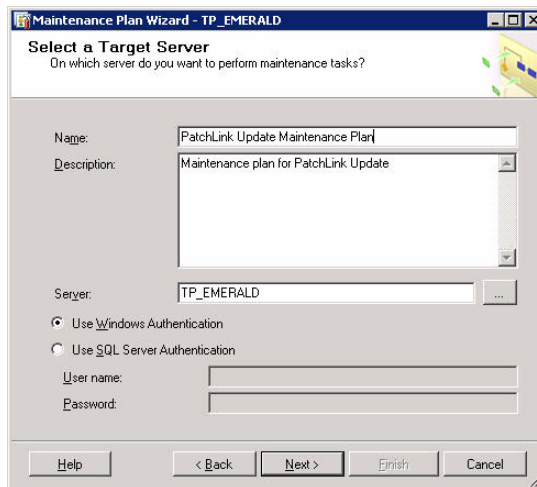


Figure D.4 Maintenance Plan Wizard - Select a Target Server



7. Define the Maintenance Plan **Name**, **Description** [optional], target **Server**, and **Authentication** method.
8. Click **Next**.
The *Select Maintenance Tasks* page opens.

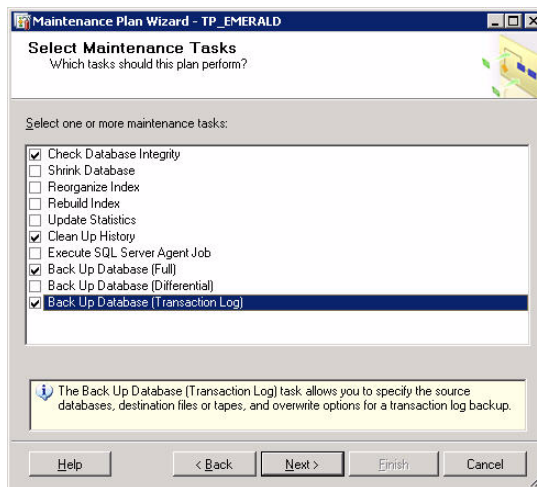


Figure D.5 Maintenance Plan Wizard - Select Maintenance Tasks

9. Select the following maintenance tasks:
 - **Check Database Integrity**
 - **Clean Up History** [optional]
 - **Back Up Database (Full)**
 - **Back Up Database (Transaction Log)**

10. Click **Next**.

The *Select Maintenance Task Order* page opens.

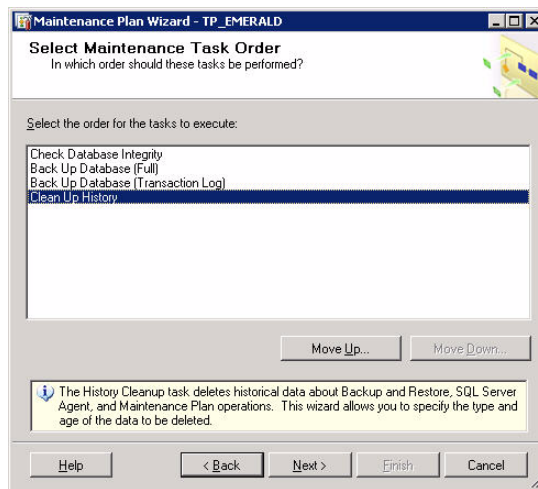


Figure D.6 Maintenance Plan Wizard - Select Maintenance Task Order

11. Set the tasks to execute in the following order:

- **Check Database Integrity**
- **Back Up Database (Full)**
- **Back Up Database (Transaction Log)**
- **Clean Up History** [optional]



- 12. Click **Next**.
The *Define Database Check Integrity Task* page opens.

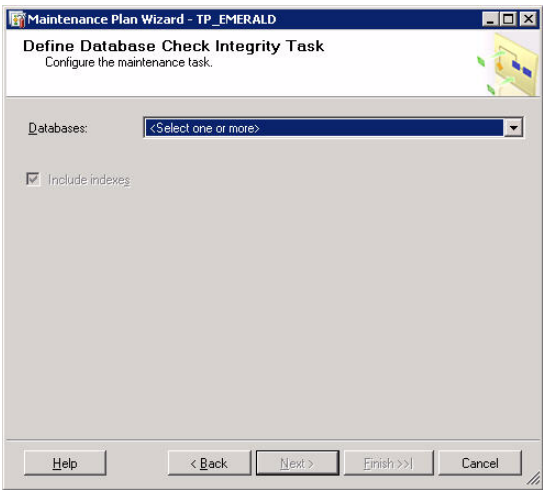


Figure D.7 Maintenance Plan Wizard - Define DB Check Integrity Task



13. Click the **Databases:** drop-down.

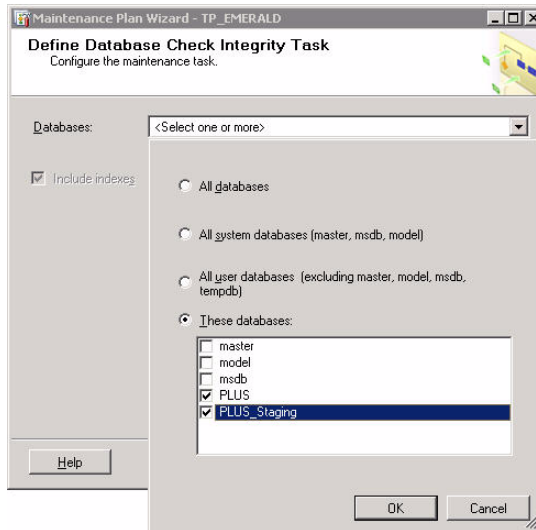


Figure D.8 Maintenance Plan Wizard - Select Databases

- a. Select the **These databases:** option.
 - b. Select the **PLUS** and **PLUS_Staging** databases.
 - c. Click **OK**.
14. Ensure that the **Include indexes** option is selected.



- 15. Click **Next**.
The *Define Back Up Database (Full) Task* page opens.

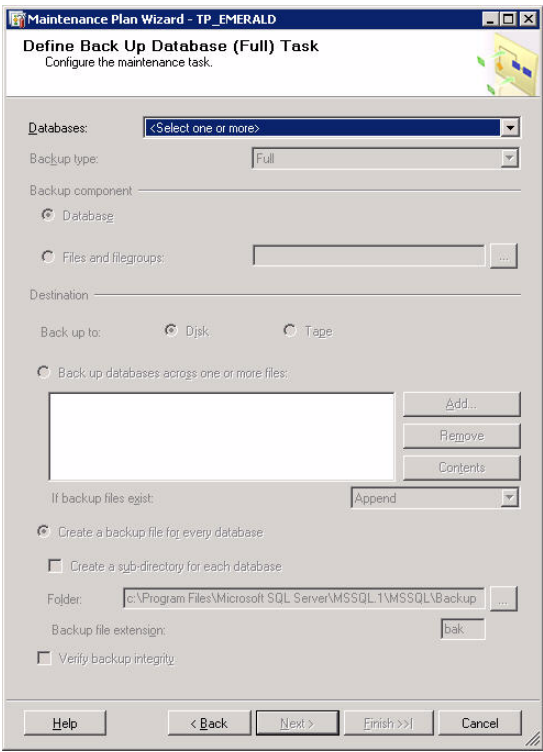


Figure D.9 Maintenance Plan Wizard - Define Back Up DB (Full) Task



16. Click the **Databases:** drop-down.

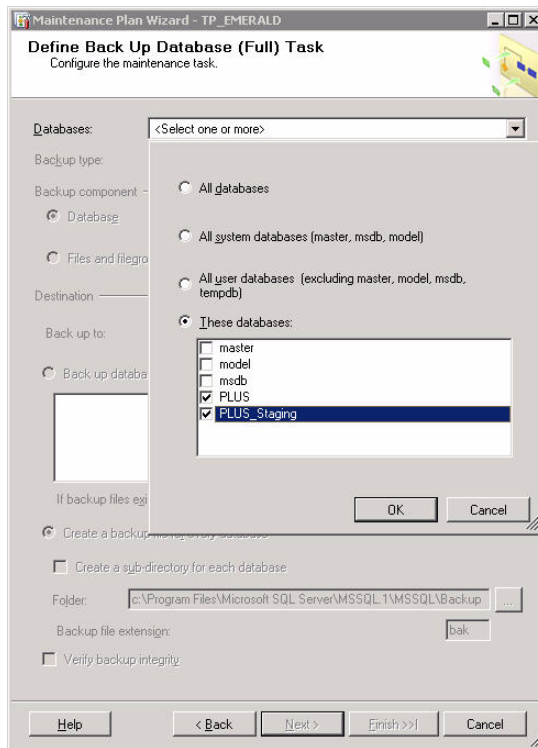


Figure D.10 Maintenance Plan Wizard - Select Databases

- Select the **These databases:** option.
- Select the **PLUS** and **PLUS_Staging** databases.



- c.** Click **OK**.

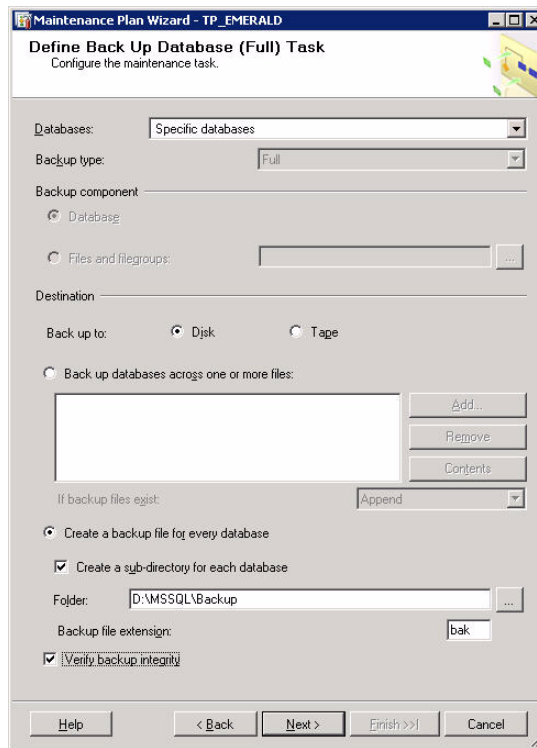


Figure D.11 Maintenance Plan Wizard - Specific Databases

17. Define your Back up *Destination* settings.
 - a. Select either the **Disk** or **Tape** option.
 - b. Select to **Create a backup file for every database**.
 - c. Select to **Create a sub-directory for each database**.
 - d. Define your destination **Folder**.



Note: For performance reasons, it is recommended that you create your database backup in a directory that is **not** on the same physical drive as your database.

- e. Ensure the **Backup file extension** is set as **bak**.
- f. Select **Verify backup integrity**.

18. Click Next.

The *Define Back Up Database (Transaction Log) Task* page opens.

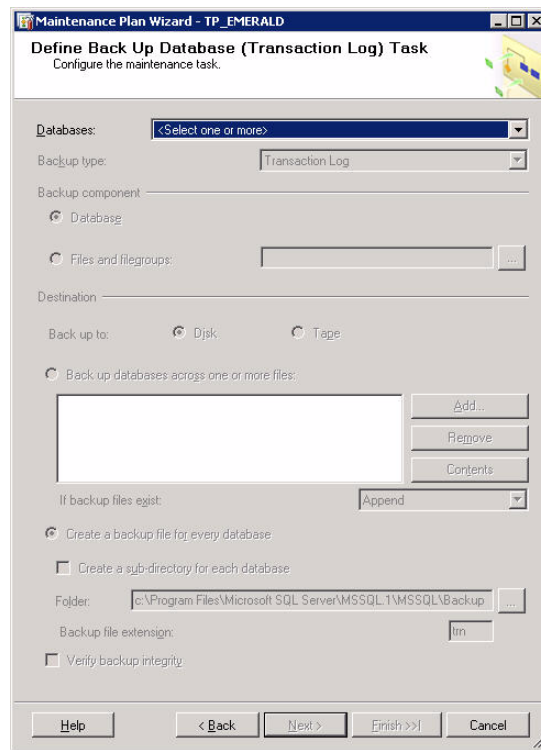


Figure D.12 Maintenance Plan Wizard - Define Back Up DB (Transaction Log) Task

19. Click the **Databases: drop-down.**

- a. Select the **These databases:** option.
- b. Select the **PLUS** and **PLUS_Staging** databases.



c. Click **OK**.

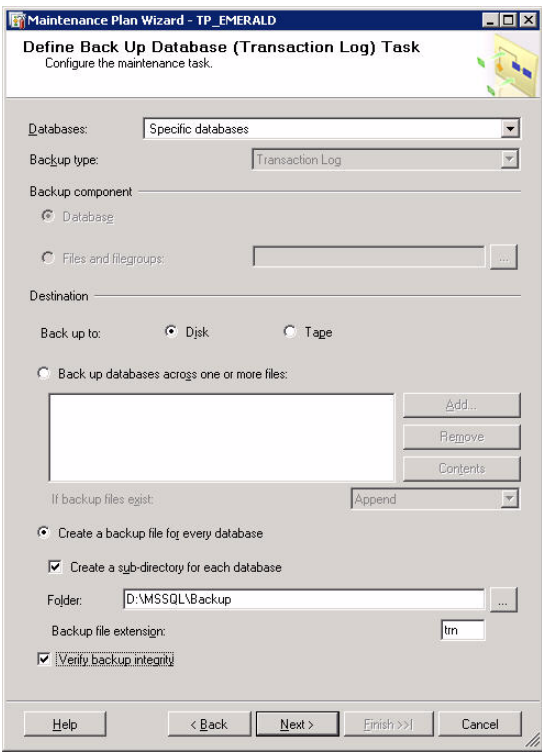


Figure D.13 Maintenance Plan Wizard - Specific Databases

20. Define your Back up *Destination* settings.
- a. Select either the **Disk** or **Tape** option.
 - b. Select to **Create a backup file for every database**.
 - c. Select to **Create a sub-directory for each database**.
 - d. Define your destination **Folder**.



Note: For performance reasons, it is recommended that you create your database backup in a directory that is NOT on the same physical drive as your database.

- e. Ensure the **Backup file extension** is set as **trn**.
- f. Select **Verify backup integrity**.



21. Click Next.

If the **Clean Up History** option was selected, the *Define Cleanup History Task* page open.

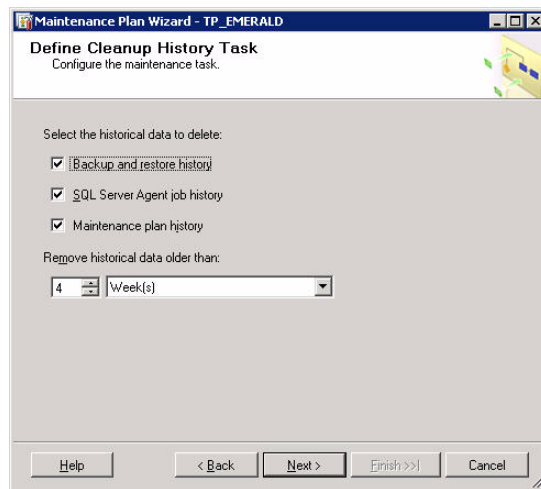


Figure D.14 Maintenance Plan Wizard - Define Cleanup History Task

- 22. Ensure that Backup and restore history is selected.**
- 23. Ensure that SQL Server Agent job history is selected.**
- 24. Ensure that Maintenance plan history is selected.**
- 25. Define the Remove historical data older than setting as appropriate for your organization.**



- 26. Click **Next**.
The *Select Plan Properties* page will open.

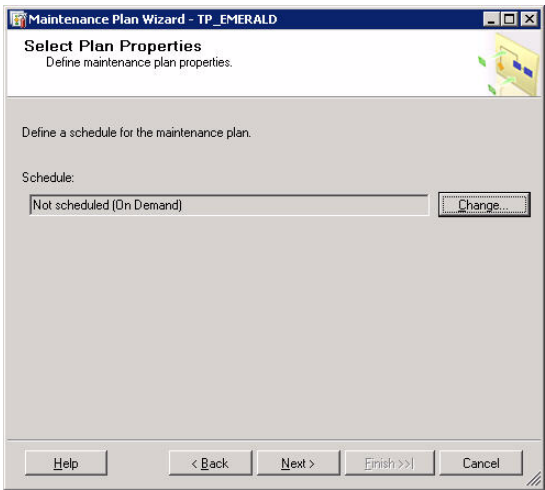


Figure D.15 Maintenance Plan Wizard - Select Plan Properties



27. [Optional] Click **Change...** to define the Maintenance plan schedule.
The *New Job Schedule* page will open.

Figure D.16 Maintenance Plan Wizard - New Job Schedule

- a. Enter a **Name** for the schedule.
- b. Select a **Schedule** type.
- c. Ensure that **Enabled** is selected.
- d. Define the **Occurrence** frequency (**Daily**, **Weekly**, or **Monthly**) and options.
- e. Define the **Daily frequency**.
- f. Define the **Duration**.
- g. Click **OK**.
The changes are saved and the *New Job Schedule* page closes.



- 28. Click **Next**.
The *Select Report Options* page opens.

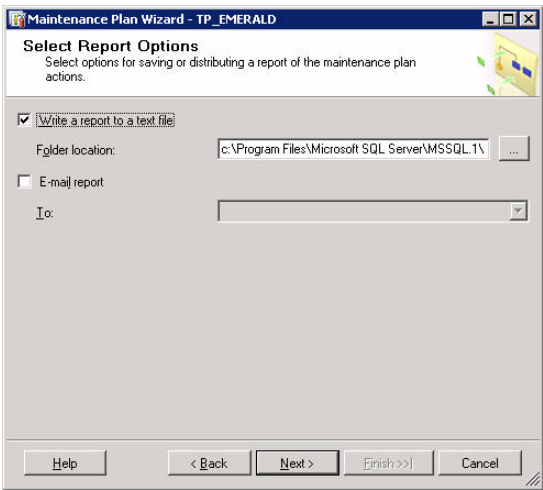


Figure D.17 Maintenance Plan Wizard - Select Report Options

- 29. Set your desired reporting options.
- 30. Click **Next**.
The *Complete the Wizard* page opens.
- 31. Click **Finish** to complete the wizard.



Warning: You must now establish a backup procedure which will archive **all** of your backup files and the contents of the `UpdateStorage` directory on a regular basis. This can be done through the use of any file backup utility.



Creating a Manual Solution

While a Maintenance Plan will allow you to automate the backup of your databases and transaction logs, you can also create and restore individual backups using the SQL Server Management Studio.

Creating a Database Backup

The most important part of an effective disaster recovery technique is having a current and valid backup.

Creating a Database Backup Using Microsoft SQL Server 2005

1. Open the *Microsoft SQL Server Management Studio* (Start > Programs > Microsoft SQL Server 2005 > SQL Server Management Studio).
2. Expand your *server group*, *server*, and *databases* folder until you see your **PLUS** database.
3. Right-click on the **PLUS** database.

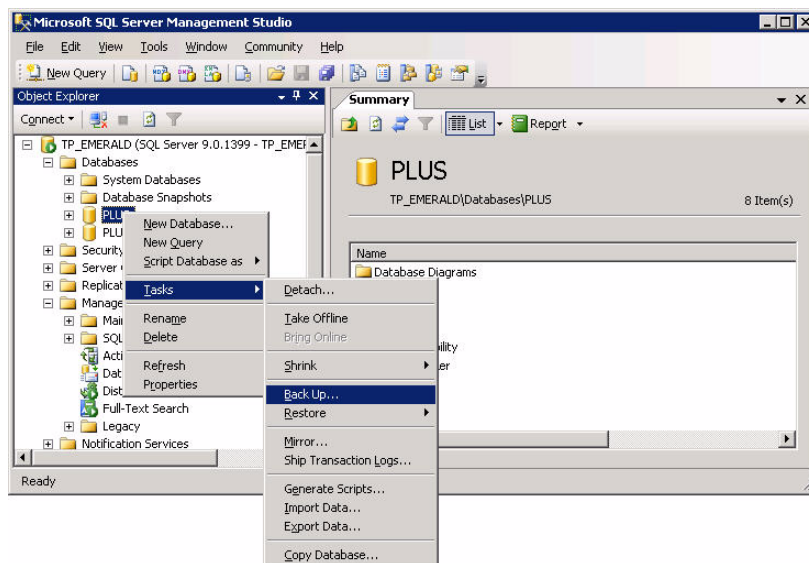


Figure D.18 SQL Server Management Studio - Database Context Menu



- 4. Select **Tasks > Back Up...**
The *Back Up Database - PLUS* window opens.

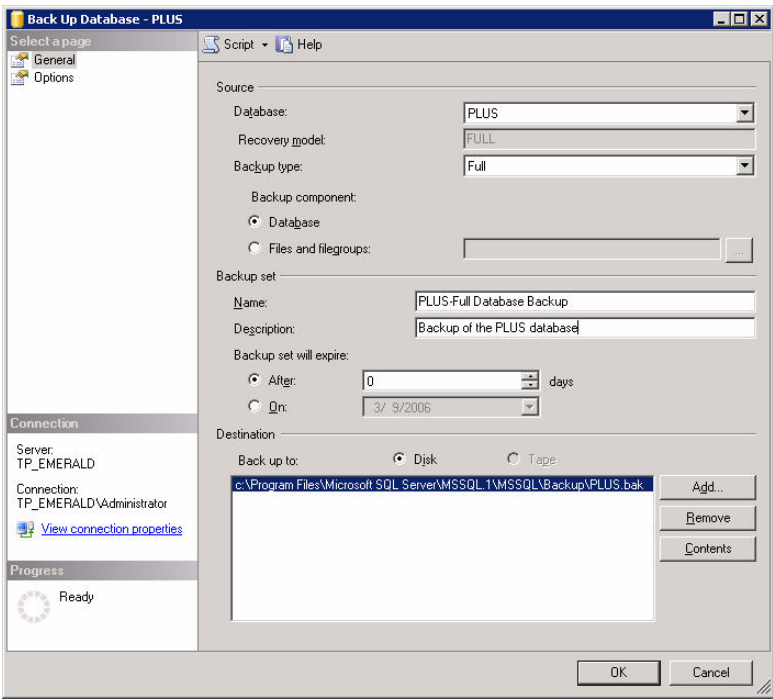


Figure D.19 *Back Up Database - PLUS - General page*

- 5. Ensure that the **Source** values are set as follows:
 - a. **Database:** *PLUS*
 - b. **Recovery model:** *FULL*



Note: If the Recovery model is not set to FULL, refer to “Preparing Your Database”.

- c. **Backup type:** *Full*
 - d. **Backup component:** *Database*
- 6. Define the Backup set **Name**, **Description**, and when the **Backup set will expire**.
- 7. Define your Back up *Destination* settings.
 - a. Select either the **Disk** or **Tape** option.



b. Define the destination **Folder**

Note: For performance reasons, it is recommended that you create your database backup in a directory that is **not** on the same physical drive as your database.

8. Select *Options* within the **Select a page** field.
The *Options* page displays.

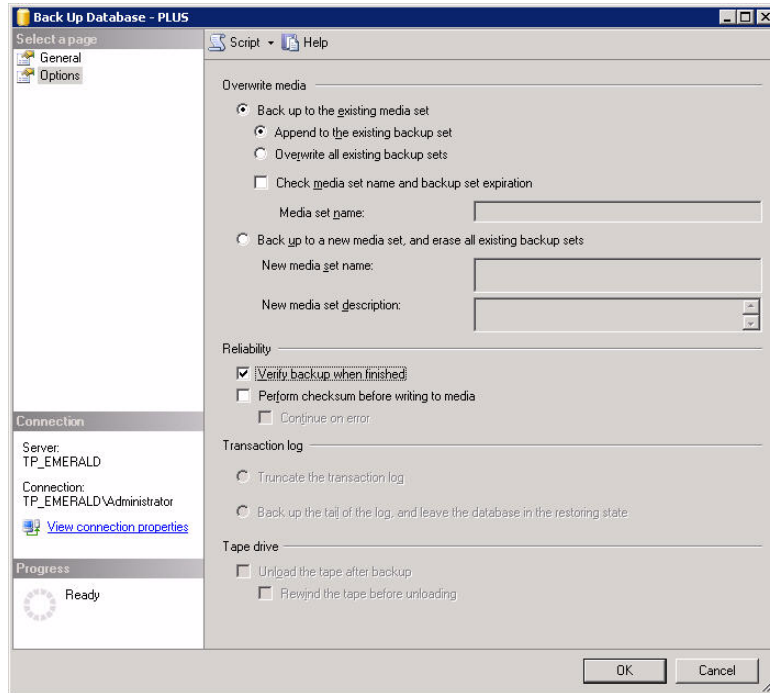


Figure D.20 *Back Up Database - PLUS - Options* page

9. Select whether to **Back up to the existing media set** or **Back up to a new media set, and erase all existing backup sets** as required for your organization.
10. Select the **Verify backup when finished** option to ensure a valid backup.
11. Click **OK**.
12. Repeat steps 3 through 11 for the **PLUS_Staging** database (and **PLAMS** and **PLUS_Reports** if they exist).



Restoring Your Backup

Another important part of an effective Disaster Recovery Solution is having a process defined in which to restore your database backup.

Restoring Your Database Backup

- 1. Open the *Services Management Console* (**Start > Settings > Control Panel > Administrative Tools > Services**).
- 2. Select and right-click on the *Novell ZENworks Patch Management* service.

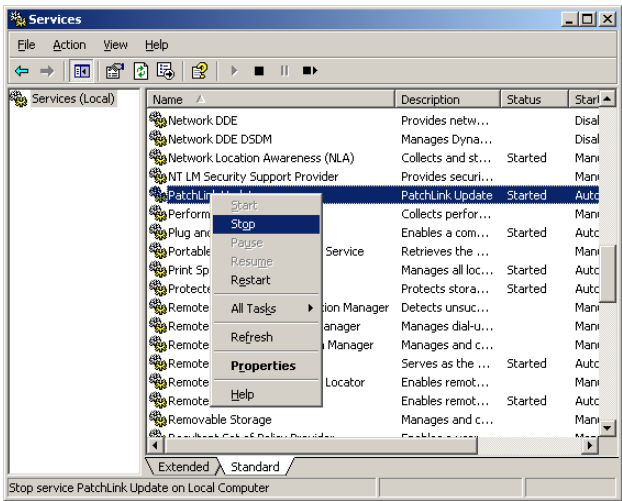


Figure D.21 Services Management Console

- 3. Select **Stop**, to stop the *Novell ZENworks Patch Management* service.
- 4. Repeat steps 2 and 3 to stop the *World Wide Web Publishing Service*.
- 5. Open the *Microsoft SQL Server Management Studio* (**Start > Programs > Microsoft SQL Server 2005 > SQL Server Management Studio**).
- 6. Expand your *server group*, *server*, and *databases* folder.



Note: If the database already exists, and you are performing a Full Restore, take the database offline, before the restore, by right-clicking on the database and selecting **Tasks > Take Offline**.

- 7. Right-click on the *Databases* folder.



8. **Select Restore Database...**
The *Restore Database* window opens.

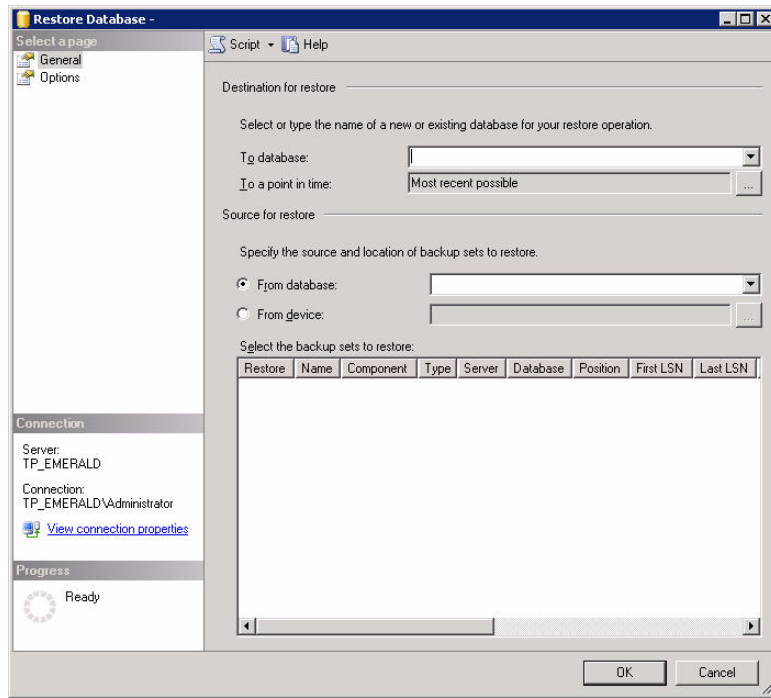


Figure D.22 Restore Database

9. In the **To database:** field, type or select the database you need.



Note: Specifying a new name for the database automatically defines the database files restored from the database backup.



10. Select **From device:** and click the ellipses [...] button.
The *Specify Backup* window opens.

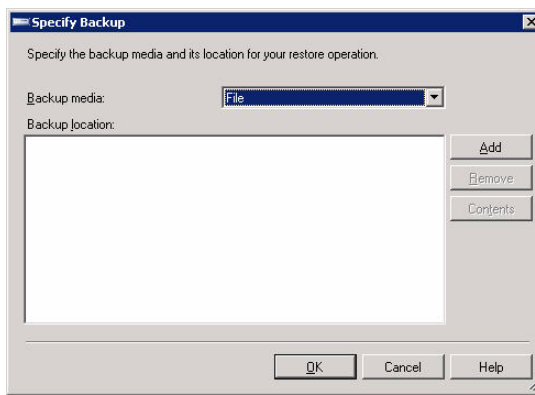


Figure D.23 Specify Backup

11. Click Add.

The *Locate Backup File* window opens.

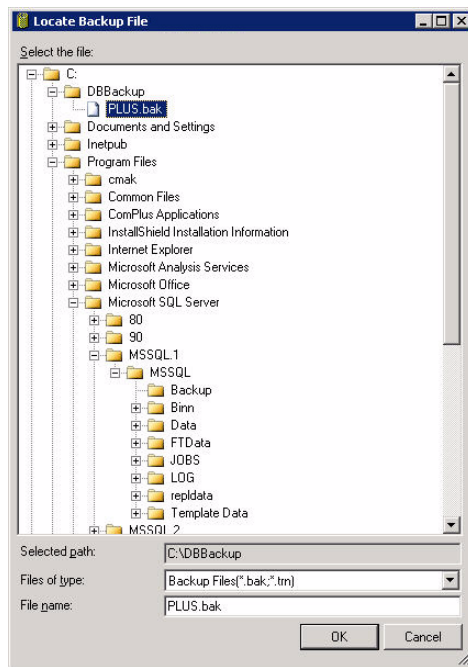


Figure D.24 Locate Backup File

12. Locate and select your backup (bak) file.**13. Click OK.****14. Click OK to return to the *Restore Database* window.**

15. Select your backup within the **Select the backup sets to restore:** field.

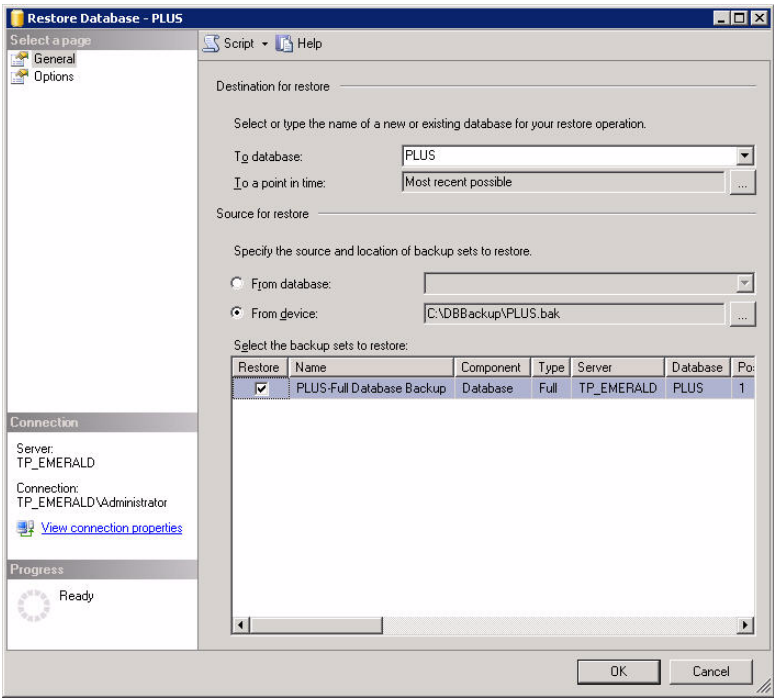


Figure D.25 Restore Database - PLUS - General page



16. Select *Options* within the **Select a page** field.
The *Options* page will display.

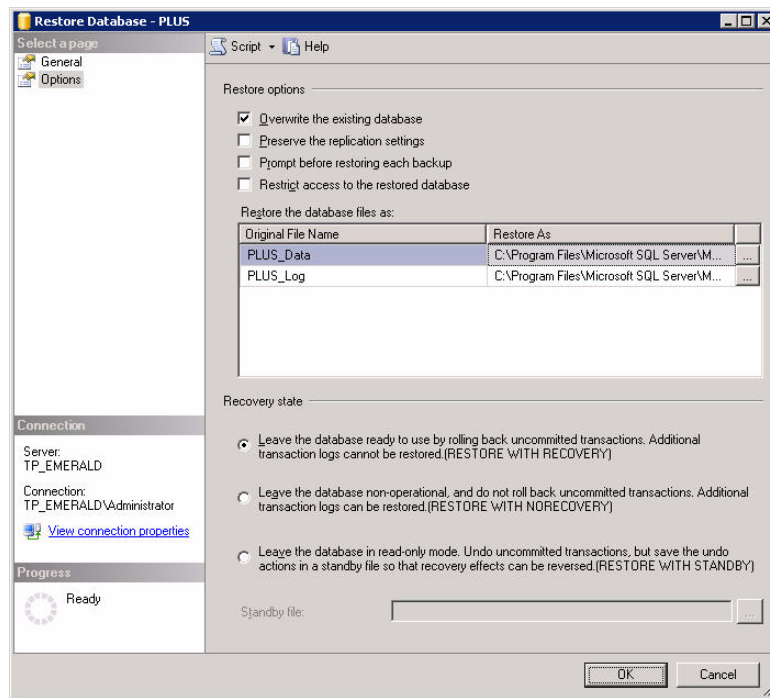


Figure D.26 Restore Database - PLUS - Options page

17. Ensure the **Overwrite the existing database** option is selected.
18. Verify, and correct if necessary, the directory path within the **Restore the database files as** field.
19. Ensure the **Leave the database ready to use...** option is selected.
20. Click **OK** to begin the database restoration.
21. Repeat steps 6 through 20 for the PLUS_Staging database.
22. Restart the and *World Wide Web Publishing Service* services.





E Using the Distribution Point

The Distribution Point, based upon the Apache HTTP Server 2.2.3 open source product, provides remote package caching to a network. Through the use of the Distribution Point, agent communication can be redirected from the primary ZENworks Patch Management Server to a local web-cache server. This appendix defines the procedures for installing, configuring, and managing the Novell Distribution Point.

In this Appendix

- “Distribution Point Installation Requirements”
- “Installing the Distribution Point”
- “Configuring the Distribution Point”

Distribution Point Installation Requirements

Supported Operating Systems

- Microsoft® Windows Server™ 2003, Standard Edition
- Windows Server 2003, Enterprise Edition
- Windows Server 2003 R2, Standard Edition
- Windows Server 2003 R2, Enterprise Edition



Note: Additional OS support details available from <http://httpd.apache.org/>

Hardware and Software Requirements

- 256 MB RAM
- 5 GB of available disk space
- A LAN connection



Note: Refer to <http://httpd.apache.org/> for additional details.



Installing the Distribution Point

The service installed by this wizard is called *Distribution Point - Apache HTTP Server*

Downloading the Distribution Point from Patch Management Server

1. Log on to the target computer as the local **administrator** (or a member of the **LOCAL_ADMINS** group).
2. Launch your web browser.
3. Type your ZENworks Patch Management Server URL in your web browser's *Address* field. Press **Enter**.
4. Type your **User Name** in the *User name* field. Press **TAB**.
5. Type your **password** in the *Password* field.
6. Click **OK**.
The *ZENworks Patch Management Server Home* screen opens.
7. Select **Devices**.
8. Click **Install**.
The *Agent Installers* page opens.

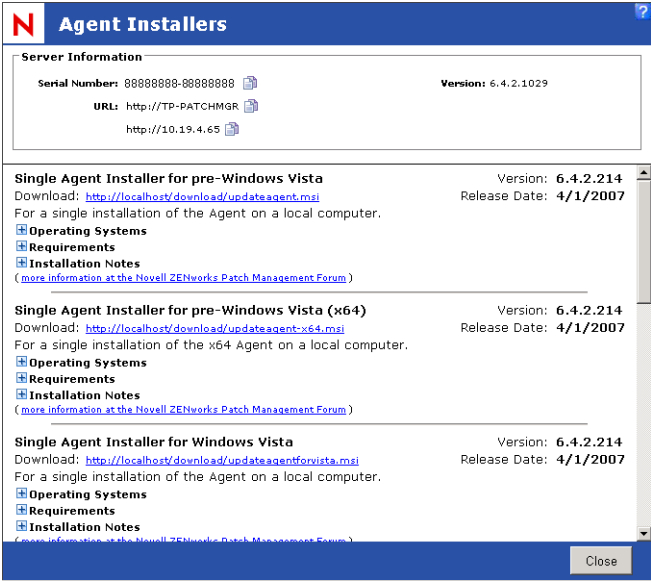


Figure E.1 Agent Installers



9. From the *Agent Installers* window, select the **Distribution Point** download link.
The *File Download* dialog box opens.
10. In the *File Download* dialog box, click **Save**.
The *Save As* window opens.
11. Specify the location to save the `distributionpoint.msi` file, and click **Save**.
The `distributionpoint.msi` file saves to the specified location.

Installing the Distribution Point

1. Select the `distributionpoint.msi` file to start the *Distribution Point Installation Wizard*.
The *Welcome* page opens.

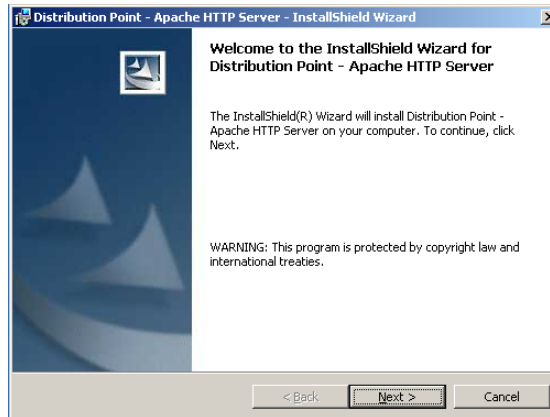


Figure E.2 Welcome page



- 2. Click **Next**.
The *License Agreement* page opens.

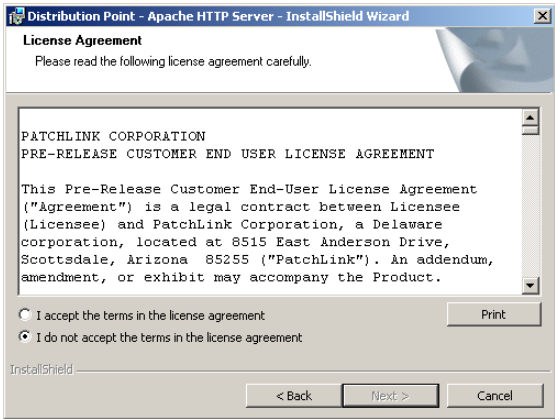


Figure E.3 License Agreement page

- 3. If you agree to the license terms, select the **I accept the terms in the license agreement** option and click **Next**.
The *Destination Folder* page opens.

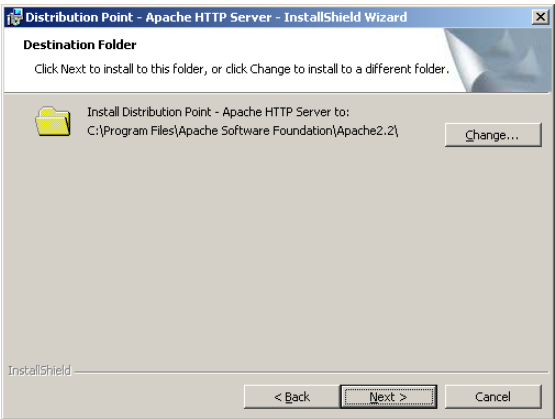


Figure E.4 Destination Folder page

- 4. If a different installation path is required:
 - a. Click **Change**.
The *Save As* window opens.



- 7. Click **Next**.
The *ZENworks Patch Management Server Information* page opens.

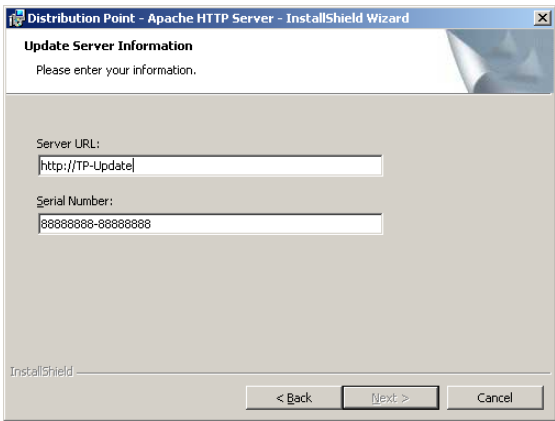


Figure E.6 Server Information page

- 8. Type the **ZENworks Patch Management Server URL** and **Serial Number** in their respective fields.
- 9. Click **Next**.
The *Server Information* page opens.

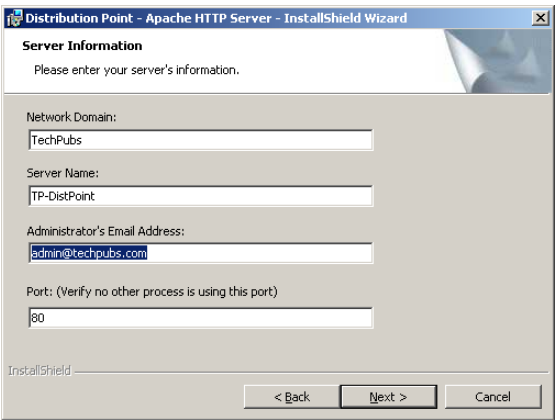


Figure E.7 Server Information page



10. Enter the following information:

Figure E.8 Server Information Field Descriptions

Field	Description
Network Domain	The DNS domain in which your Distribution Point is registered (MyDomain.com).
Server Name	The full DNS name of the server on which you are installing the Distribution Point (ServerName.MyDomain.com).
Administrator's Email Address	The Distribution Point Administrator's (or Webmaster's) e-mail address.
Port	The port on which the Distribution Point will monitor incoming traffic. (Default = 80)

11. Click **Next**.

The *Ready to Install* page opens.

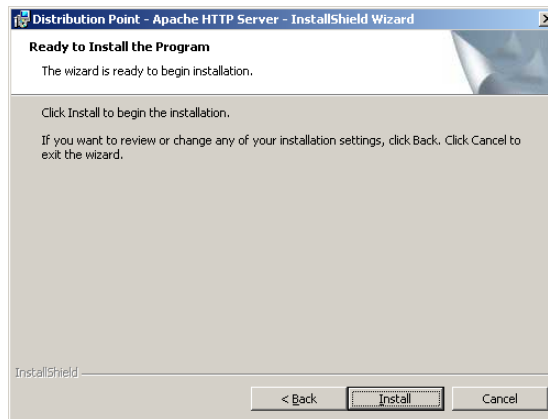


Figure E.9 Registration page



12. Click **Install** to begin the installation.

Following the Installation, the *InstallShield Wizard Completed* page opens.

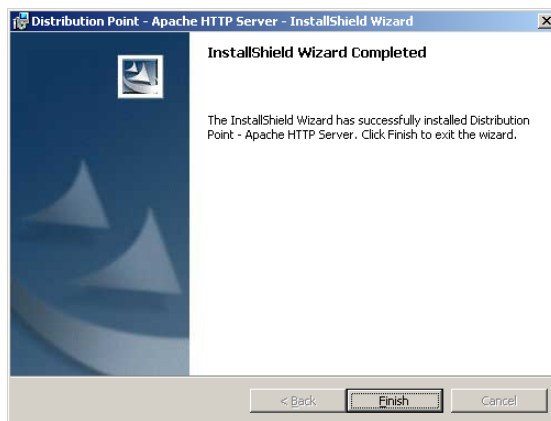


Figure E.10 InstallShield Wizard Completed

13. Click **Finish** to exit the wizard.

Configuring the Distribution Point

During the installation of the Distribution Point, the custom installer configures the files in the `conf` subdirectory, based upon your environment and responses. It is recommended that you do not alter these settings. Doing so may disable your Distribution Point and could require re-installation.



Note: Reinstallation of the Distribution Point will not overwrite any of the configuration files in the `conf` subdirectory. The new file is appended with a `.default` extension. The configuration file must be manually updated by referencing and copying the settings in the `.default` file into your `.conf` file.

Table E.1 Configurable Distribution Point Directives

Directive Name	Usage	Default Value
ThreadsPerChild <i>value</i>	The Maximum number of connections the Distribution Point can handle at one time.	100
MaxRequestsPerChild <i>value</i>	The number of requests a child process will serve before exiting. A value of 0 indicates the process will never exit (recommended).	0
ServerRoot <i>path</i>	The Distribution Point installation path. <i>Defined during installation</i>	<Program Files>\ Apache Software Foundation\ Apache2.2\
Listen <i>value</i>	The ports on which the Distribution Point monitors incoming traffic. <i>Defined during installation</i>	80
ServerAdmin <i>value</i>	The Distribution Point Administrator's e-mail address. <i>Defined during installation</i>	
ServerName <i>value</i>	The Distribution Point's Hostname (includes port if the Distribution Point was not installed on port 80). <i>Defined during installation</i>	
DocumentRoot <i>path</i>	The directory that forms the main document tree which is visible from the web. <i>Uses the install path defined during installation</i>	<Program Files>\ Apache Software Foundation\ Apache2.2\htdocs
ErrorLog <i>path</i>	The location defining the Distribution Point Error Logs.	logs/error.log †
† Due to Apache using Unix-style names internally, forward slashes must be used (/) instead of backslashes (\) when identifying filenames within a directive. Example: C:/logs/error.log not C:\logs\error.log		



Table E.1 Configurable Distribution Point Directives

Directive Name	Usage	Default Value
LogLevel <i>value</i>	The indicator that controls error logging.	Warn
ProxyRequests <i>value</i>	The indicator that defines whether forward (standard) proxy requests are enabled.	On
CacheRoot <i>path</i>	The directory root where cache files are stored. <i>Defined during installation</i>	<Program Files>\ Apache Software Foundation\ Apache2.2\cache
CacheMaxFileSize <i>value</i>	The maximum file size (in bytes) that will be cached.	1000000000000
CacheMinFileSize <i>value</i>	The minimum file size (in bytes) that will be cached.	1
CacheEnable <i>type URL</i>	The storage type and URLs to cache.	disk /disk http://patchlink-1
CacheDirLevels <i>value</i>	The number of subdirectory levels in the cache.	3
CacheDirLength <i>value</i>	The number of characters in the subdirectory names.	1
CacheDisable <i>URL</i>	The function that disables caching of the specified URLs.	http://security. update.server /update-list/
† Due to Apache using Unix-style names internally, forward slashes must be used (/) instead of backslashes (\) when identifying filenames within a directive. Example: C:/logs/error.log not C:\logs\error.log		



Tip: If additional details are required regarding the Distribution Point (Apache HTTP Server Version 2.2.3), refer to the [Directive Quick Reference](http://httpd.apache.org/docs/2.2/mod/quickreference.html) (<http://httpd.apache.org/docs/2.2/mod/quickreference.html>) and other [Online Documentation](http://httpd.apache.org/docs/2.2/) (<http://httpd.apache.org/docs/2.2/>) published by the Apache Software Foundation.



F Glossary

A

AAA Architecture

authentication, authorization and accounting architecture. In client/server networking, an architecture that combines three necessary elements of security, to make them available on one server, and able to work with each other in a coordinated fashion.

Access Control List

Access Control List (ACL). A database file that stores information regarding entities that may request access to a network, and the rights and privileges to be granted upon request.

accounting

In Network security architectures, records what users do once they are granted access to a network, or in the case of denied access, it can report how many failed attempts, and even details of the attempts.

See also [AAA Architecture](#)

Active Directory

Active Directory (AD) . Microsoft's trademarked system that centralizes the management of networked resources by making each item on a network including most applications, objects in a relational database and then enabling the administrator to manage those objects through one management center.

ActiveX Template Library

Active Template Library (ATL). Formerly called ActiveX Template Library, A Microsoft program library for use when creating ASP code and other ActiveX program components to run in a browser window.

ActiveX

A technology, built on Microsoft's Component Object Model (COM), that enables software components, regardless of the language used to create them, to interact with one another in a networked environment.

Address Resolution Protocol

Address Resolution Protocol (ARP). An OSI layer-3 protocol used to find a device's MAC address using their IP address.

agent policies

The agent rules for communicating with the server. These rules include: communication interval, deployment notification options, discovery agent mode, hours of operation, logging level, and reboot notification options. Agent policies are assigned to groups and any group that has not been explicitly assigned an agent policy will use the default system policy, as defined within Patch Management Server.



agent

A software routine that resides in background memory on a computer or other device and waits to perform an action when a specified event occurs.

ASP

Active Server Page. An HTML page that contains embedded server side scripting that is processed on a Microsoft Web Server before the page is sent to the user.

authentication

The process of identifying an user, typically through the use of credentials such as a user name and password as the originator of a message or as the end point of a channel. High level authentication can use such other tokens as the originating IP address, or an encryption key, providing evidence of the authenticity of the request.

Authenticode

A technology based on Information Technology Security industry standards that provide a method for developers to digitally sign their code. When code is signed, the company signing the code, takes responsibility for the code and guarantees that the code is safe and free from viruses.

authorization vs. authentication

Whereas authentication is the process of verifying that a user is who they say they are, like having two forms of ID from different places, or aging the paint and carbon testing the frame wood to verify authenticity of a painting, authorization is verifying the level of access available to that user, such as aisle and row seating stamped on a concert ticket, or possessing a back-stage pass.

authorization

The process of determining what level of access to grant a user, to a system or function of a software application based upon their login credentials.

Automatic Caching System

Automatic Caching System (ACS). Automatically writes packages marked critical to a memory queue allowing administrators to have the critical and security-related patches available for rapid deployment.

B

baseline

In Information Technology, it is the base set of files that comprises a system, or to which it may fall back in the case of viral infection or other loss of data, such as when a system is restored from a backup.

behavior

A specific desired outcome for any patch or package deployment, configurable by the use of deployment flags and options.



browser

Software that allows the user to find, view, hear, and interact with material on a corporate Intranet or the World Wide Web.

C**CDL**

Concurrent Deployment Limit (CDL). Defines the maximum number of ZENworks Patch Management agents that can receive active deployments at the same time. The purpose of the limit is to control the number of deployments to agents across the entire network and to reduce the chance of overloading your ZENworks Patch Management Server. If an agent takes longer than 60 minutes to finish its deployment, it is no longer counted against this limit.

This is the only value that cannot be overridden by a group's Agent Policy Set, as it limits deployments for all agents.

chained deployment

The deployment of multiple packages in sequence, flagged to prevent reboot until the last of the chain has been deployed.

client

In computer networks, a client is any user, computer, node, server, or system that is requesting files from or access to some other system, regardless of whether it also acts as a server.

code signing

The process of digitally signing programs for verification purposes.

COM

Component Object Model. Microsoft's programming architecture in the Windows family of Operating Systems that enables software components to communicate between processes and fit easily into object-oriented program design. The family of COM technologies includes COM+, Distributed COM (DCOM) and ActiveX

communication interval

Determines how much time the ZENworks Patch Management agent will sleep between communication with the ZENworks Patch Management Server. When it communicates with the ZENworks Patch Management Server it is checking for policy updates and deployments. This interval is critical since if the interval is too long, the agents will not get their tasks in a reasonable amount of time. If the interval is too short, the ZENworks Patch Management Server may constantly be busy and other agents may not be able to get their tasks.

Interval rates typically vary between 15 and 60 minutes depending on number of nodes, network architecture and bandwidth.

compliance

An expression of whether the node being evaluated, meets the Mandatory Baseline of patches to make it safe for admission to the network in a quarantine arrangement. Usually expressed by the boolean true or false, a station can either be compliant or non-compliant. If non-compliant, it is set up for remediation and under quarantine until fully patched.



context

As pertains to Microsoft's Active Directory, context refers to the exact container position in the directory tree, thus allowing for the location of resources in a tree, by use of relative rather than fully qualified identifiers

control panel applet

An application designed to be run within the Microsoft Windows control panel. Novell's Control Panel applet allows easy interaction with the ZENworks Patch Management Agent.

credentials

An object or objects presented along with a request for admission to a network or server that is used to validate the authorization of the presenter. Usually a credential is a combined username and password, but can also consist of IP address, MAC address or an encryption key to verify that the request comes from an authorized location.

cross-platform

Portable or applicable to more than one operating system.

CVE

Common Vulnerabilities and Exposures (CVE). A list of standardized names for vulnerabilities and other information exposures. CVE aims to standardize the names for all publicly known vulnerabilities and exposures.

D

DAU

Discover Applicable Updates. A pre-defined system task which will launch the ZENworks Patch Management Agent on a client machine. The DAU runs following subscription replication, five minutes after the application of a patch, after a reboot and when an agent checks in after the Scan Now button has been clicked in the ZENworks Patch Management Server interface.

DCOM

Distributed Component Object Model. An extension of the Component Object Model (COM) which extends COM's capabilities across network boundaries, and allows objects to communicate across a network, whereas COM is designed for interprocess communication on the same node or computer.

deadline

When deploying patches or packages, it is the date and time by which a package or patch absolutely must deploy, and until which, a user may snooze a deployment if inconvenient.

Decryption Key

A string of seemingly random bits of data used with cryptographic algorithms to create or verify digital signatures and unscramble cipher text back to its original clear text. Keys can be public or private and keeping at least one key private provides high security. Keys at least 128 bits long are considered more secure by modern standards, as many shorter ones have been cracked by modern computing technology.



Decryption

The process of converting cipher text, back to plain text, after traveling across a public access medium, using a previously determined decryption key so as to arrive at the original clear text message that was sent.

deployment flag

When preparing a package or patch deployment, the administrator has many options and flags that can be set to fine tune how and when the deployment occurs and what events accompany and follow the deployment. Also known as: package deployment flag

deployment script

Also known as: [package script](#)

deployment

The planned delivery of a vulnerability patch or package of patches, to any or all nodes determined to be non-compliant.

DHCP

Dynamic Host Configuration Protocol. A protocol that lets network administrators centrally manage and automate the assignment of IP addresses in an organization's network by establishing a range of IP addresses to be assigned automatically and indexed. Without DHCP, managers would have to manually assign and keep track of each host IP address on the network.

dirty "C" state

Indicates that the ZENworks Patch Management Agent received a chained deployment and the reboot is currently suppressed. While in the "C" state, the agent will only accept other chained deployments or a reboot deployment. Only a reboot deployment or manual reboot will clear this state.

dirty "R" state

Indicates that the ZENworks Patch Management Agent received a deployment which required a reboot and the reboot was suppressed. While in the "R" state, the agent will only accept a reboot deployment. Only a reboot deployment or manual reboot will clear this state.

dirty state

The term used to describe an agent that displays a C or R on the computers page of the ZENworks Patch Management Server. Agents that are in a clean state, display no such lettering.

distribution package

See [package](#)

DLL

Dynamic-Link Library file. A file that has linked and compiled, one or more functions used by a separate process, that can be loaded into the memory space of that process when the program is started, or during run-time.



DNS

Domain Name System. Is the mechanism by which computers and especially servers are named for easier location and associated with an IP address. A domain name is a meaningful and human-readable name associated with an Internet address. Domain names most often take on the format of domainname.com and the most common ones are associated with WWW locations.

domain

On a Local or Wide Area Network, a domain is a set of network resources and services available to a group of users. Domains act as containers that can be identified by a name and address and which can then provide authorized users access to any elements they contain. Domains can also share resources with each other as trust is extended by administrators to those other domains.

E

encryption

The process of converting clear readable text to apparently random strings known as cipher text before it travels on network media, so that it can only be read, or understood by a recipient with the proper decryption key. Some of the most secure encryption methods include RSA, AES, IKE, MDS, SSL and SHA-1

encryption key

A string of seemingly random bits used with cryptographic algorithms to create or verify digital signatures and scramble clear text to protect it from being intercepted and read while traveling across public networking media. Keys can be public or private and keeping at least one key private provides high security. Keys at least 128 bits long are considered more secure by modern standards, as many shorter ones have been compromised by modern computing technology.

endpoint

In a client/server network architecture, an endpoint is any node that is a destination of two way communication, whether requesting or responding.

eXtensible markup language

See [XML](#)

F

fingerprint

A group of unique identifiers used to determine the presence of a patch and/or vulnerability. Fingerprints can include unique files, file attributes, directories, registry keys or data values.

firewall

A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from unauthorized access.



FQDN

Fully Qualified Domain Name. The Domain Name is a unique identifier for any resource located within a Domain or Network. A Fully Qualified Domain Name is the full name of any network entity starting with its hostname and ending with the exact Domain Name in which it resides. example johnq.accounting.acme.com

FTP

File Transfer Protocol. A simple, clear text and thus, non-secure protocol used to exchange files between computers on a network or the internet.

G

Global Subscription Server

The Global Subscription Server is the central repository where vulnerability reports and their associated patches are stored for retrieval by the ZENworks Patch Management Server. The Global Subscription Server also serves as the ZENworks Patch Management licensing server.

group

A targeted collection of computers created and named for the purpose of deploying distribution packages, defining agent policies, setting Mandatory Baselines or reporting. Groups provide a simple way to manage computers that have similar requirements rather than managing each computer separately.

GUID

Globally Unique Identifier. A 128-bit number generated by Windows Operating System, or one of its applications, assigned to any object in a two way communication, be they user, application, or component. The algorithm used to generate GUIDs combines a few unique settings, such as IP Address, MAC Address, clock date and time, to create an even more unique identifier.

H

Host Name

The name given to identify each node of a network, usually descriptive of either the user that operates that node, or its position in a building, or function. Host Name is intended to be more human friendly than the IP Address that networks use to identify each node.

hours of operation

When enabled, this value determines when the agents start and stop communicating with ZENworks Patch Management Server. If the agent is in the middle of a deployment and the agent's hours of operation expire (exceed the designated stop time) it will finish what it is currently working on and continue the rest of the deployment at the next hours of operation interval.



HTML

HyperText Markup Language. The accepted publishing language of the World Wide Web. It is a universally accepted standard for displaying links, images, and text in a format that computers around the world can read. There are currently many advances in HTML that allow for an increasing number of different types of objects to be added to and displayed in a browser page.

HTTP

HyperText Transfer Protocol. The set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.

HTTPS

Secure HyperText Transfer Protocol. A Web protocol built into most browsers that encrypts and decrypts user page requests as well as the pages that are returned via HTTP over SSL by the web server

hyperlink

Generally a different color from the surrounding text, it is a coded reference to some other location in the document, or to some URL or network address, usually written in a form of HTML code or JAVA, and is most prevalent on web pages.

I

IANA

Internet Assigned Numbers Authority. An administrative organization that assigns internet host addresses and other numeric constants used in Internet protocols.

IIS

Internet Information Server. Microsoft's web server that provides an infrastructure for all Internet services (HTTP, FTP, Telnet and Gopher for some examples) and other capabilities for Microsoft's NT, 2000, XP, and 2003 operating systems. Usually managed from IIS Manager, allows for central control of all related information services.

IP address

The 32-bit (4 dotted divisions of 8 binary digits) numeric identifier for any device on a network that distinguishes it from other devices and allows for routers and switches to group devices and their communication packets. The 32-bit dotted format is soon to be replaced by a IPv6, to allow for and keep pace with the enormous growth of the internet in recent years. See example below

IP address 192.168.0.1 would be read by a router as 11000000.10101000.00000000.00000001

IP

Internet Protocol. The best known and main protocol in a suite of protocols known as TCP/IP that carry all traffic on the internet currently. IP is a connectionless protocol, meaning it does not wait for confirmation that it was received before sending the next packet. It is designed for long distance carriage of packets of data, as was originally the plan with Arpanet, which later became the Internet.



J**JAVA**

A programming language invented by Sun Microsystems. It can be used as a general purpose application programming language with built-in networking libraries. It can also be used to write small applications called applets.

JRE

JAVA Runtime Environment. Created by SUN Microsystems, it is the core set of files necessary to execute Java written programs in any OS environment. JAVA is used because it is cross-platform, which is increasingly necessary in the current web-based world.

L**LDAP**

Lightweight Directory Access Protocol. A software protocol that enables the use of Directory Services to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate intranet.

library

A collection of precompiled routines, sometimes called modules, that are stored in object format for reuse by a program.

localhost

The default name describing the computer address also known as the loopback address of the computer. On web servers, this loopback can be used to test the default web page, by typing `http://127.0.0.1` or `http://localhost`

localprofile.txt

An XML file found in `C:\Program Files\Novell\ZENworks Patch Management Agent`, this file is maintained by the ZENworks Patch Management agent and contains information on computer name, operating system and support pack level, services, software, and hardware. The refresh inventory data system task uses the information in this file to populate computer inventory data on the ZENworks Patch Management Server.

M**MAC address**

A 12 digit hexadecimal address, that is burned into network cards and networking devices to allow for unique reference.

macro

Within Novell ZENworks Patch Management, a macro is an environment variable that represents a series of commands, actions, or keystrokes, a directory path, or a filename that can only be executed by the ZENworks Patch Management Agent.



Mandatory Baseline

Is the absolute minimum set of vulnerability reports or locally-created distribution packages that must be installed for the group's computer members. In terms of vulnerability reports, a mandatory baseline will continually verify that the patch is actually installed, and, if it is not, it will deploy the necessary distribution packages to bring the computer into compliance.

MSDE

Microsoft SQL Desktop Edition. An enabling technology that provides local data storage and is completely compatible with the SQL Server™ version 7.0 code base. This technology transforms Access from a simple file-server database application into an extremely powerful and highly scalable client-server solution for any size organization.

MSI installer

Designed for Windows networks that use the Windows software installer mechanism. The MSI installer can be edited to include the ZENworks Patch Management Server name and serial number. In this way, the agent can be deployed through the use of group policy agents.

N

NDS

Novell Directory Services. The relational database that contains all the resources on a Novell network, and provides security, and access for all resources.

NetWare

Networking OS that has played a major role in the development of Local Area Networking over the past few decades, being an early Network OS to use the Directory Services concept.

Novell ZENworks Patch Management Server

Consists of three major components:

1. Global Subscription Server
2. ZENworks Patch Management Server
3. ZENworks Patch Management Agent

O

OSD

Open Software Description. Creates a standard way to describe software components, their versions, underlying structure, and relationships to other components. OSD is the standard language used when performing automatic software distributions and updates over the Internet.



OS Pack

Operating System Pack. Contains all vulnerability detection information needed by an agent for a given operating system. It is generated by the DS and is passed to the agent during the DAU process. When a Vulnerability replication executes, it checks to if any operating systems received new data and it will automatically schedule the DS to regenerate the OS Packs for those operating systems.

OVAL

Open Vulnerability Assessment Language. The common language for security experts to discuss and agree upon technical details about how to check for the presence of vulnerabilities on computer systems. The vulnerabilities are identified using gold-standard tests—OVAL vulnerability definitions in XML and queries in Structured Query Language (SQL)—that can be utilized by end users or implemented in scanning tools.

P

package script

The script that performs the functions required to start package installation. Can be written using Microsoft VBScript, Microsoft Jscript, or command line script For more information on these scripting languages, refer to msdn.microsoft.com/scripting

Also known as: **deployment script**

package

A package contains all the actual patch software and executable code for deployment. A package can run tasks or scripts, install software applications, place files (or directories of files) to a specified location, change the configuration of an application or service, or various other things that can be done in an unattended manner. The majority of packages contain the patches for vulnerability, defect or bug.

A combination of vendor-supplied patches and scripts created install the patches using Novell ZENworks Patch Management.

Patch Developers Kit

Patch Developers Kit (PDK). An addition to the Novell ZENworks Patch Management suite that provides the ability to define custom detection reports, deployment packages, signatures and fingerprints. It has an easy-to-use graphical interface that illustrates all associated subcomponents of the patch in a single view.

Patch Management administrator

Any user who is assigned any of the access rights which control the functionality of the ZENworks Patch Management Server or its deployments is considered a Patch Management administrator.

Patch Management user

Any user who has access to authenticate in to the ZENworks Patch Management Server is considered a Patch Management user.



patch management

The systematic deployment, installation, and auditing of applicable hotfixes, patches, and service packs to operating systems and software applications. It must incorporate the organization or people needed to administer the patches, the processes needed to ensure the proper testing, the inventorying of existing patch levels, the identification of needed patches, and the technology to deploy and apply the appropriate patches.

policies

See [agent policies](#)

policy server

In a network designed with protections against unauthorized admission, it is where the rules and policies are stored that are the standards by which admission decisions are made. Rules can then be enforced by routers or some other form of firewall protection.

port number

The port number is carried in internet transport protocols to identify which service or program is to receive an incoming packet. Certain port numbers are permanently assigned to particular protocols by the IANA. For example, e-mail uses port 25 and Web services use port 80.

posture

A term used by Cisco to refer to the state of readiness of a node requesting admission to a network, that will determine, when compared to the rules on the policy server, what degree of access if any, the node may be granted to the network. No access is usually termed as quarantine.

pre-requisite

also known as: pre-req. A requirement, such as the existence of a software package, file, and/or registry entry, that must be met prior to the deployment or installation of a patch.

proxy server

In an enterprise that uses one of the Internet protocols, a proxy server is a server that acts as an intermediary between a client and an Internet server. The proxy server allows an enterprise to ensure security and administrative control.

Q

Q-chain

Qchain (Qchain.exe) is the utility Microsoft provides to chain hotfixes on Microsoft Windows 2000, XP, or 2003.

quarantine

A state resulting from a node making a request to access a network, denied because of some non-compliance condition also known as a vulnerability, such as missing patches or old antivirus dat file. Usually this is followed by prescribed remediation.



quiet mode

When set to quiet mode, a deployment package will suppress all user interfaces during installation.

R

RARP

Reverse Address Resolution Protocol. Literally, the reverse of Address Resolution Protocol, being used to resolve an IP address from a given hardware, or MAC address.

Refresh Inventory Data

Refresh Inventory Data (RID) prevents certain log files from getting too large. RID is handled differently on the various platforms – some delete the files when they reach a certain size and others will trim the file, leaving the most recent data but shrinking the file size.

registry

The registry serves as a central data repository for system and application-specific configuration data on a Windows machine. A registry contains *keys*, which are much like directories in a Windows file system. Each key can contain *values* (the registry equivalent of a data file) or nested *subkeys* (the registry equivalent of a nested folder). Just as with files or folders, you can identify a registry key by building a full path to it.

remediation

Installing a countermeasure to reduce the risks associated with a vulnerability.

replication

The process whereby the ZENworks Patch Management Server receives daily scheduled updates of patches from the Global Subscription Server. The scheduled replication time of day can be manually overridden daily by clicking **Update Now**.

report

See [vulnerability report](#).

role

In ZENworks Patch Management, it is a basic grouping of rights and privileges, such as Administrator, Manager, Operator and Guest, which can be expanded to fit the needs of individual enterprises. Each role also allows fine tuning to add or delete certain rights.

rules

Statements of conditions that must be met or parameters that will determine some action to be taken. Rules can be positive or negative, but usually are stated simply and clearly such as ‘if member of group ADMIN, run superuser.bat’.



S

Secure File Transfer Protocol

Secure File Transfer Protocol (SFTP) is a secure version of FTP, designed to provide some encryption capabilities for file transfer over a network. Functionally similar to FTP, SFTP instead uses SSH to transfer files, and so cannot be used with a standard FTP client.

server

A server is a computer, or software application that provides data to client computers or software applications. A single computer running multiple software applications can simultaneously perform the functions of multiple servers, multiple clients, or any combination thereof.

signature

A signature is used to recognize a specific combination of installed software applications, services and operating systems. A signature typically contains multiple fingerprints.

SQL Server™

A trademark for a Microsoft database server that utilizes SQL. SQL Server is a popular database management system for Windows NT environments.

SQL

Structured Query Language. A database language used by administrators of relational databases to query, update and manage data. It enables the administrator to use clear syntax that is descriptive of whatever action is desired.

SSL Certificate

An electronic certificate consisting of a set of keys, one public, one private, exchanged between a web server and a requesting client. A session is created, and a unique session key ensures high level of encryption of any sensitive data passed between the client and server, preventing interception or unauthorized use of that data by any other entity.

SSL

Secure Sockets Layer. A security protocol that provides data encryption, message integrity, and client/server authentication for the transmission of private information and documents over the internet. SSL is available with either 40bit or 128bit encryption, however 40bit has been compromised in recent years, making 128bit the lowest level anyone should go for secure encryption.

standard deployment

The deployment of a standard, non-chainable, package, or the deployment of a chainable package in a non-chained state.



T

TCP/IP

Transmission Control Protocol/Internet Protocol. The main suite of communications protocols used to connect hosts on the Internet, and now the prevalent LAN protocol even when other protocols are available.

Trust

In Domains, a trust relationship will allow members of one Domain, when properly logged in and authenticated, to access services available on another Domain.

U

UDP

User datagram protocol (UDP). Is a communications method (protocol) that offers a limited amount of service when messages are exchanged between computers in a network that uses **IP**. It is one of the most common connection based protocols in use on the internet, the other being TCP

URL

Universal Resource Locator. The address that is the formal access name for a networked or Internet resource, usually begins with the protocol identifier, such as http or ftp, thus http://www.yahoo.com is a URL for the domain yahoo.com.

user name

The unique name used to gain access to a computer and/or network. User names, and passwords, are required in multi-user systems.

UTC

Universal Time Coordinated. An international standard that allows for synchronization of events across many geographic zones. On a ZENworks Patch Management Server, UTC might be chosen instead of local time if a scheduled event is desired to run at the same time, at all sites, dependent also upon deployment constraints.

V

VeriSign certificate

A VeriSign certificate is issued by VeriSign, Inc. to verify a company's identity, and enables the company to digitally sign programs and prove the authenticity of a web site address.

vulnerability report

A series of signatures and fingerprint designed to determine if a computer is susceptible to a vulnerability and if the computer has been patched.



vulnerability

A weakness in a system that would allow an attacker to compromise system confidentiality, integrity, or availability.

A breach from the original design, concept or intended behavior of a computer's hardware or software which leaves the computer, or any piece of it, in an exposed state. Malicious users can use this to force other unattended actions to be performed. Vulnerabilities are often caused by defects or bugs, though this is not always the case. Many times the very configuration may result in unexpected exposures. Even out of date documentation may be labeled as a vulnerability, as not informing a user of how to perform actions in the preferred manner may result in systems being widely exposed.

W - Z

web server

A program that publishes content using the HTTP protocol so that it can be viewed using any type of compliant browser from any location on the connected Intranet or Internet.

WWW

World Wide Web (WWW). The commonly used name for the Internet, and which is in fact a web of connected Domains of local computers, which can share information with authorized users who connect from anywhere else on the web. Due to the exponential growth in recent years, a good way to check on current standards at any time is to visit the World Wide Web Consortium at <http://www.w3.org/>

XML

Extensible Markup Language. A flexible way to create common information formats and share both the format and the data on the World Wide Web, intranets, and elsewhere.

ZENworks Patch Management Agent

Novell ZENworks Patch Management Agent. The ZENworks Patch Management Agent is a service that runs on each node and queries the ZENworks Patch Management Server to receive any deployments that become ready. The behavior of the agent is defined by the agent's policies, whether it is using the default agent policies for ZENworks Patch Management Server or the group's agent policies.

ZENworks Patch Management Server

Novell ZENworks Patch Management Server. The central system in ZENworks Patch Management that manages patch retrieval, detection and package deployment to all registered computers on the network. As a sophisticated, automated central repository of the most current patches available for a network, it maintains communication with the ZENworks Patch Management Agent on nodes, across many key networking platforms, on the network, and detects any vulnerabilities with the help of the agent on each node.



G Index

A

AAA Architecture	375
Access Control List.....	375
accounting.....	375
Active Directory.....	375
ActiveX	
definition of	375
template library.....	375
Address Resolution Protocol	375
agent.....	376
agent policies.....	375
ASP	376
authentication	376
vs. authorization.....	376
Authenticode.....	376
authorization.....	376
vs. authentication	376
automatic caching system.....	376

B

baseline	376
behavior.....	376
browser.....	377

C

CDL	377
chained deployment.....	377
Client.....	377
code signing	377
COM	377
communication Interval.....	377
compliance	377

Component Object Model	377
Concurrent Deployment Limit	377
context.....	378
control panel applet	378
credential	378
cross-platform.....	378
CVE	378

D

DAU.....	28, 378
DCOM	378
deadline	378
Decryption	379
Decryption Key.....	378
deployment.....	379
standard.....	388
deployment flag.....	379
deployment script	379
Deployment Wizard.....	92
DHCP	379
dirty state.....	379
dirty state 'R'	379
dirty state 'C'	379
Discover Applicable Updates.....	378
distribution package	
see package	
Distribution Point	
installing.....	366
DLL.....	379
DNS.....	380
domain.....	380



E

encryption 380

encryption key 380

endpoint 380

F

fingerprint 29, 380

firewall 380

FQDN 381

FTP 381

G

Global Subscription Server 381

group 381

GUID 381

H

host name 381

hours of operation 381

HTML 382

HTTP 382

HTTPS 382

hyperlink 382

I

IANA 382

IIS 3, 382

install

 Distribution Point 366

IP 382

IP address 382

J

JAVA 383

JRE 383

L

LDAP 383

library 383

license information 250

localhost 383

localprofile.txt 383

M

MAC address 383

macro 383

mandatory baseline 384

mandatory baselines

 removing deployments created by .

 177

Microsoft Internet Explorer 3

Microsoft Internet Information Services

 3

Microsoft Windows Server 2003 3

MSDE 384

MSI installer 384

N

NDS 384

NetWare 384

Novell Directory Services 384

Novell ZENworks Patch Management

 Server 384

O

OSD 384

OVAL 385



P

package	30, 385
content window	63
macros	64
%BOOTDIR% macro	64
%COMMON FILES% macro	64
%PROGRAM FILES% macro	64
%ROOTDIR% macro	64
%TEMP% macro	64
%WINDIR% macro	64
scripts	
command line script	69
post-script	69
pre-script	69
package deployment flag 61, 113, 379	
package script	385
Patch Developers Kit	385
Patch Management	
administrator	385
user	385
patch management	386
policies	386
policy server	386
port number	386
posture	386
pre-requisite	386
pre-requisite signature	30
Products page	250
proxy server	386

Q

Q-chain	386
quarantine	386
quiet mode	387

R

RARP	387
Refresh Inventory Data	387
registry	387
remediation	387
replication	387
report	387
RID	387
role	387
rules	387

S

Secure File Transfer Protocol	388
server	388
signature	29, 388
SQL	388
SQL Server	388
SSL	388
SSL Certificate	388

T

TCP/IP	389
--------------	-----

U

UDP	389
URL	389
user name	389
user roles	
assigning	238
creating	233
disabling	239
editing	236
enabling	240
removing	241



- users
 - adding..... 218, 226
 - changing password 230
 - creating..... 218
 - deleting..... 229
 - editing 228
 - removing..... 229
- UTC 389

V

- VeriSign certificate..... 389
- Vulnerabilities 27
- vulnerability 29, 390
- vulnerability report 389

W

- web server..... 390
- WWW..... 390

X

- XML 390

Z

- ZENworks Patch Management Agent...
390
- ZENworks Patch Management Server..
390





Novell, Inc.

1800 South Novell Place
Provo, UT 84606

www.novell.com
phone: 800.858.4000

