



ZENworks®

Patch Management

User Guide

ZENworks Patch Management Server v6.3

Novell®

02_012N_6.3m

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

Copyright © 1997-2006 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 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	4
Supported Database Servers	4
Recommended Configuration	5
Agent Supported Operating Systems	6

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

Accessing ZENworks Patch Management	7
Getting Started with Novell ZENworks Patch Management	10
Navigating within ZENworks Patch Management	11
Defining Browser Conventions	11
Using Search	12
Using Tabbed Pages	13
Expanding and Collapsing Folders and Outlines	14
Advancing through Patch Information Pages	14
Using the Action Menu	15
Using Help	15
Exporting Data	16
Using the ZENworks Patch Management Home Page	17
Using the ZENworks Patch Management Navigation Menu	18
Viewing the General Information Links	19
Viewing Latest News	20
Viewing Current Status Information	21
Using the ZENworks Patch Management Status Page	22
Viewing the Comprehensive Graphical Assessments	23
License Expiration	27



Chapter 3: Using Vulnerabilities and Packages _____ 29

- About Vulnerabilities 29
 - Viewing Vulnerabilities 30
- Using the Vulnerabilities Page 31
 - Vulnerability Status & Types 32
 - Vulnerability Package Cache Status & Type 32
 - Vulnerability Name 33
 - Vulnerability Impacts 34
 - Vulnerability Statistics 34
 - Searching, Filtering, and Saving Views 35
- Working with Vulnerabilities 36
 - Vulnerability Status (tabs) 36
 - Column Definitions 36
 - Device Status 37
 - Deploying Vulnerabilities 39
 - Disabling and Enabling Vulnerabilities 39
 - Scanning for Vulnerabilities 40
 - Updating the Vulnerability Cache 42
- About Packages 43
- Using the Packages Tab 45
 - Package Information Tab 47
 - Package Statuses & Types 48
 - Column Definitions 50
 - Searching, Filtering, and Saving Views 50
- Working with Packages 51
 - Deploying a Package 51
 - Deleting a Package 52
 - Updating Package Cache 52
 - Editing a Package 53
 - Creating a Package 53
- Using the Package Editor 54
 - Including Deployment Options in a Package 63
 - Package Flags 63
 - Adding Files to a Package 64
 - Using Macros 65
 - Creating Scripts for a Package 66
 - Using the Script Editor 66
 - Working with License Agreements 67



Chapter 4: Working With Deployments 69

About Deployments	69
Viewing Deployments	70
Deployment Types	71
Standard and Chained Deployments	72
<i>Dirty State</i> Deployments	72
Reboot Deployments	73
Using the Deployment Pages	74
Deployment Column Definitions	74
Deployment Details Summary	76
Working with Deployments	77
Viewing the Deployment Details	77
Viewing Deployment Details by Device	79
Viewing Deployment Details by Device Group	79
Viewing Deployment Results	80
Explaining Deployment Distribution Order	81
Aborting Deployments	82
Disabling Deployments	82
Enabling Deployments	83
Modifying Deployments	83
Deleting Deployments	83
Explaining Deployment Deadlines	84
Using the Deployment Wizard	84
Introduction Page	84
Device/Device Groups Selection Page	86
Package Selection Page	88
Associated Vulnerability Analysis Page	90
Licenses Page	91
Deployment Options Page	92
Schedule Configuration Page	93
Package Deployment Order and Behavior Page	98
Package Deployment Behavior Options Page	102
Notification Options Page	106
Deployment Notification Options	106
Reboot Notification Options	107
Deployment Confirmation Page	109
Package Applicability Page	111
Deployment Summary Page	112
Changing Deployments	113



Chapter 5: Using Devices 115

- About Devices 115
 - Viewing Devices 116
 - Using the Devices Page 116
 - Device Status Icons 116
 - Using the Device Details Page 119
 - Device Information 119
 - Device Vulnerabilities 122
 - Device Inventory 122
 - Device Deployments 123
- Working with Devices 124
 - Installing an Agent 125
 - Viewing Device Details 126
 - Disabling a Device 126
 - Enabling a Device 127
 - Deploying a Vulnerability 127
 - Exporting Device Information 128
 - Scanning Devices 128
 - Rebooting Devices 130

Chapter 6: Using Groups 133

- Using the Groups Page 134
- Using the Group Details (Information) Page 136
 - Device Group Information 136
 - Information Section 137
 - Device Group Vulnerabilities 138
 - Device Group Inventory 139
 - Device Group Membership 139
 - Device Group Mandatory Baselines 140
 - Device Group Deployments 140
- Working with Groups 140
 - Defining Groups 141
 - Additional Group Type Definitions 141
 - Using the Create Group Wizard 142
 - Deploying a Group 149
 - Disabling Groups 150
 - Enabling Groups 152
 - Editing Groups 153
 - Deleting Groups 153
 - Viewing Group Properties 154
 - Exporting Group Data 154
 - Scanning Groups 155
 - Rebooting Groups 157



Chapter 7: Viewing Device Inventory _____ 159

About Inventory	159
Viewing Inventory	159
Using the Inventory Page	160
Inventory Types	160
Operating Systems View	161
Software View	161
Hardware View	161
Services View	161
Scanning Inventory	162
About Inventory Scanning	163
The Detection Process	163
Detection Results	164
Using Custom Inventory	165
Guidelines for Microsoft Windows based Operating Systems	165
Valid XML Options	165
Example XML File	168
Guidelines for Linux/Unix/Mac based Operating Systems	169
Valid XML Options	169
XML Schema Definition	170
Example XML File	172
Exporting Inventory	173

Chapter 8: Mandatory Baselines _____ 175

About Mandatory Baselines	175
Viewing Mandatory Baselines	175
Using the Mandatory Baseline Page	176
Mandatory Baseline Column Definitions	177
Working with Mandatory Baselines	179
Managing a Mandatory Baseline	179
Removing Deployments Created By Mandatory Baselines	184
Exporting Baseline Information	185
Scanning Data	185
Using Update Cache	187



Chapter 9: Reporting 189

About Reports 189

 Viewing Reports 191

Available Reports 192

 Report Descriptions 192

 Agent Policy Report 192

 Device Duplicate Report 193

 Device Status Report 193

 Detection Results Not Found Report 194

 Deployment Detail Report 194

 Deployment Error Report 195

 Deployment In-Progress Report 195

 Deployment Summary Report 196

 Mandatory Baseline Detail Report 197

 Mandatory Baseline Summary Report 197

 Package Compliance Detail Report 198

 Package Compliance Summary Report 199

 Vulnerability Analysis Report 200

 Report Parameters 201

Working with Reports 202

 Searching and Updating Reports 202

 Displaying Time and Date in Reports 202

 Exporting Reports 203

 Viewing Printable Data in Reports 203

Chapter 10: Managing Users and Roles 205

About User Management 205

 Viewing Users 206

Defining User Access 206

 Windows-based Authentication 206

 ZENworks Patch Management Access Rights 206

Defining Users 206

 Creating New Users 207

 Adding Existing Windows Users 207

Defining Roles 207

 Exploring the Predefined System Roles 208

 Defining Custom Roles 208

Defining Access Rights 209

Defining Accessible Device Groups 213

Defining Accessible Devices 213

Working with Users 214

 Creating New Users 214

 Adding Existing Users 215



Editing User Profiles	216
Removing ZENworks Patch Management Users	217
Deleting ZENworks Patch Management Users	218
Changing a Users Password	219
Exporting User Data	220
Working with User Roles	221
Creating User Roles	221
Editing User Roles	223
Assigning User Roles	225
Disabling and Enabling User Roles	226
Deleting User Roles	228
Exporting User Role Data	228

Chapter 11: Configuring Default Behavior 229

About the Options Page	229
Viewing Options	230
Viewing Subscription Service Information	230
Subscription Service Information	231
Subscription Service History	232
Subscription Service Configuration	233
Subscription Service Status	234
Subscription Service Proxy Configuration	234
Subscription Service Communication Settings	234
Verifying Subscription Licenses	235
Product Information	236
Novell ZENworks Patch Management Default Configuration	237
Viewing Patch Management Server Information	238
Configuring Deployment Defaults	239
Configuring Agent Defaults	240
Defining Agent Default Settings	240
Defining Bandwidth Throttling Settings	245
Defining Deployment Notification Settings	246
Defining the Discover Applicable Updates (DAU) Settings	247
Configuring Fastpath Servers	248
Absentee Agent Management	249
Configuring ISAPI Communication Settings	250
Setting the User Interface Defaults	251
Customizing Row Values	252
Customizing and Administering Agent Policy Sets	253
Viewing Agent Policy Summary Information	254
Creating a New Policy	256
Editing a Policy	260
Deleting a Policy	261



Defining Agent Policy Conflict Resolution 262

Using E-Mail Notification 263

 Configuring E-Mail Notification 264

 Defining E-Mail Alert Thresholds 265

Technical Support Information 266

 Server Information 267

 Component Version Information 268

 Novell Support Information 268

Chapter 12: Using the ZENworks Patch Management Agent _____ 269

About the ZENworks Patch Management Agent 269

 Viewing the Agent 269

Agent Components 270

 Deployment Tab 270

 Server Information and Status 270

 Agent Information 271

 Log Operations 271

 Agent Operations 272

 Detection Tab 273

 Server Information and Status 273

 Agent Information 274

 Log Operations 274

 Agent Operations 275

 Proxies Tab 276

 Server Information and Status 276

 Proxy Information 277

 About Tab 278

 Server Information and Status 278

 Version Information 279

User Interaction During a Deployment 279

User Interaction During a Reboot 281

Appendix A: Patch Management Server Reference _____ 283

Patch Management Server Security 283

ZENworks Patch Management Server Error Pages 284

HTTP Status Codes 285

WinInet Error Codes 286

Device (ZENworks Patch Management Agent) Status Icons 286



Appendix B: Securing Your ZENworks Patch Management Server _____ 289

Install Your Server With SSL	289
Use Secure Passwords	289
Turn Off Windows Networking	290
Put ZENworks Patch Management Behind a Firewall	291
Turn Off Non-Critical Services	291
Lock Down Unused TCP and UDP Ports	292
Turn Off File and Printer Sharing	295
Apply All Microsoft Security Patches	296

Appendix C: Creating a Disaster Recovery Solution _____ 297

Preparing Your Database	297
Creating an Automated Solution	300
Creating a Manual Solution	315
Creating a Database Backup	315
Restoring Your Backup	318

Appendix D: Using the Distribution Point _____ 325

Distribution Point Installation Requirements	325
Supported Operating Systems	325
Hardware and Software Requirements	325
Installing the Distribution Point	326
Configuring the Distribution Point	333

Appendix E: Glossary _____ 335**Appendix F: Index _____ 351**



Preface

This ZENworks Patch Management Server v6.3 User Guide is a resource written for all users of ZENworks Patch Management Server v6.3. 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”
- Chapter 6, “Using Groups”
- Chapter 7, “Viewing Device Inventory”
- Chapter 8, “Mandatory Baselines”
- Chapter 9, “Reporting”
- Chapter 10, “Managing Users and Roles”
- Chapter 11, “Configuring Default Behavior”
- Chapter 12, “Using the ZENworks Patch Management Agent”
- Appendix A, “Patch Management Server Reference”
- Appendix B, “Securing Your ZENworks Patch Management Server”
- Appendix C, “Creating a Disaster Recovery Solution”
- Appendix D, “Using the Distribution Point”
- Appendix E, “Glossary”
- Appendix F, “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 ZENworks Patch Management is the core product of the leading patch and vulnerability management solution for medium and large enterprise networks. ZENworks Patch Management enables customers to easily translate security policies into automated and continuous protection against over 90% of vulnerabilities that threaten today's enterprise networks. By providing the most accurate and timely vulnerability assessment and patch management available ZENworks Patch Management ensures that policy measurement and security audits are a true representation of network security posture.

In This Chapter

- “Product Overview” on page 1
- “System Requirements” on page 3
- “Agent Supported Operating Systems” on page 6

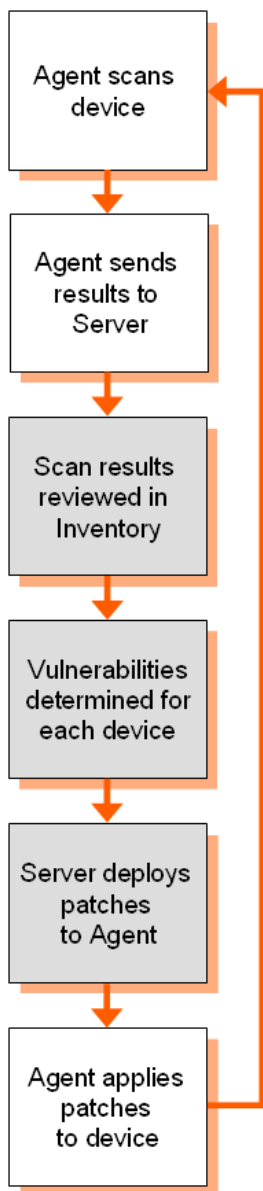
Product Overview

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 installs a ZENworks Patch Management Agent on every client system in the target network that ensures that 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.



The Agent scans the host device and compiles information on operating system, software, hardware, and services on that device.

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, even if a workstation is disconnected from your network.

Based on this information, vulnerabilities are determined to be applicable, or not, for each device. 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.

Once patch status is established, the Novell Administrator can deploy the desired vulnerability to each applicable device on the network.

Once installed, the ZENworks Patch Management Server stays current with the latest patches and fixes by daily communication with the Global Subscription Server service through a secure connection.

When a newly released patch matches the defined stored network profile, Patch Management Server administrators receive a proactive e-mail notification and the new vulnerability opens on the ZENworks Patch Management Server interface with the description and business impact as well as the list of devices that require the deployment.

At this time you can choose to deploy the patch to devices or disregard the patch.



System Requirements

Minimum Hardware Requirements

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

- 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**” on page 5.

Supported Operating Systems

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

- Microsoft Windows Server™ 2003, Web Edition with SP1
- Windows Server 2003, Standard Edition with SP1
- Windows Server 2003, Enterprise Edition with SP1
- Windows Server 2003 R2, Standard Edition
- Windows Server 2003 R2, Enterprise Edition



Warning: Do not install the server software on a Primary Domain Controller (PDC). Installation onto a PDC is not supported in this release of Novell ZENworks Patch Management.



Other Software Requirements

Your Novell ZENworks Patch Management Server **must be a clean OS installation** with *only* the following software installed:

Table 1.1 ZENworks Patch Management Server Software Requirements

Internet Server	Microsoft® Internet Information Services (IIS) 6.0
.NET Framework	1.1 SP1 and 2.0 (both versions are required)
Internet Browser	Microsoft Internet Explorer 6.x

Supported Database Servers

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

- Microsoft® SQL Server 2005 Express Edition with SP1
- SQL Server 2005 Standard Edition with SP1
- SQL Server 2005 Enterprise Edition with SP1
- MSDE 2000 with SP4 (Upgrade only)
- SQL Server 2000 with SP4 (Upgrade only)



Note: Novell ZENworks Patch Management Server installs *SQL Server 2005 Express Edition with SP1* during installation. Therefore, you must not have any database server installed prior to the installation of Novell ZENworks Patch Management.

Recommended Configuration

Table 1.2 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 SP1	Windows Server 2003, Web Edition with SP1	Windows Server 2003, Standard Edition with SP1	Windows Server 2003, Standard Edition with SP1	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 6.3 is supported.

Table 1.3 ZENworks Patch Management Agent 6.3 Supported Platforms

Operating System	OS Versions	OS Edition	OS Data Width	Processor Family	Processor Data Width	Min. JRE	JRE Data Width
Apple Mac OS X	10.2.8 - 10.4.7	All	32/64 bit	x386(Intel)/PowerPC	32/64 bit	1.4.0+	32 bit
HP-UX	11.00 - 11.23	All	64 bit	PA-RISC	64 bit	1.4.0+	32/64 bit
IBM AIX	5.1 - 5.3	All	32/64 bit	PowerPC/POWER	32/64 bit	1.4.0+	32/64 bit
Microsoft Windows 9x	98 Second Edition	All	32 bit	x86	32 bit	NA	NA
Microsoft Windows NT	4.0 SP6A - 2003 R2	All	32/64 bit	x86	32/64 bit	NA	NA
Microsoft Windows XP	XP - XP SP2	Professional *	32/64 bit	x86	32/64 bit	NA	NA
Novell Netware	6.5	All	32 bit	x86	32 bit	1.3.0+	32 bit
Novell SUSE Linux	9 - 10	Enterprise	32 bit	x86	32 bit	1.4.0+	32 bit
Red Hat Linux	2.1 - 4	Enterprise AS, ES, WS	32 bit	x86	32 bit	1.4.0+	32 bit
Sun Solaris	2.6 - 10	All	32/64 bit	SPACR	32/64 bit	1.4.0+	32/64 bit
* (excludes Home, Media Center and Tablet PC)							



2 Using Novell ZENworks Patch Management

Novell ZENworks Patch Management provides the ability to detect and patch workstations, mobile devices, and servers across a network. ZENworks Patch Management Server includes a Web-based management console providing direct access to system management, configuration, reporting, and deployment options.

In this Chapter

- “Accessing ZENworks Patch Management” on page 7
- “Getting Started with Novell ZENworks Patch Management” on page 10
- “Navigating within ZENworks Patch Management” on page 11
- “Using the ZENworks Patch Management Home Page” on page 17
- “Using the ZENworks Patch Management Status Page” on page 22
- “Viewing the Comprehensive Graphical Assessments” on page 23
- “License Expiration” on page 27

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. Depending on your security level, you can navigate through your assigned part(s) of the system at any time.

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

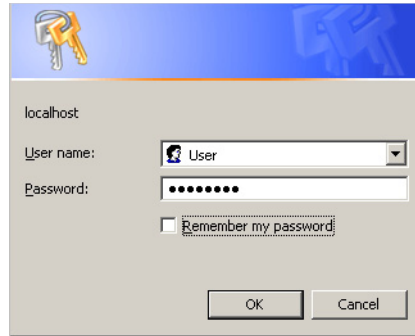


Figure 2.1 Log on dialog box

3. Type your user name in the *Username* field
4. Type your password in the *Password* field
5. 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.

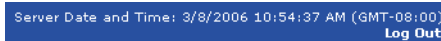


Figure 2.2 Log Out Menu Item



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

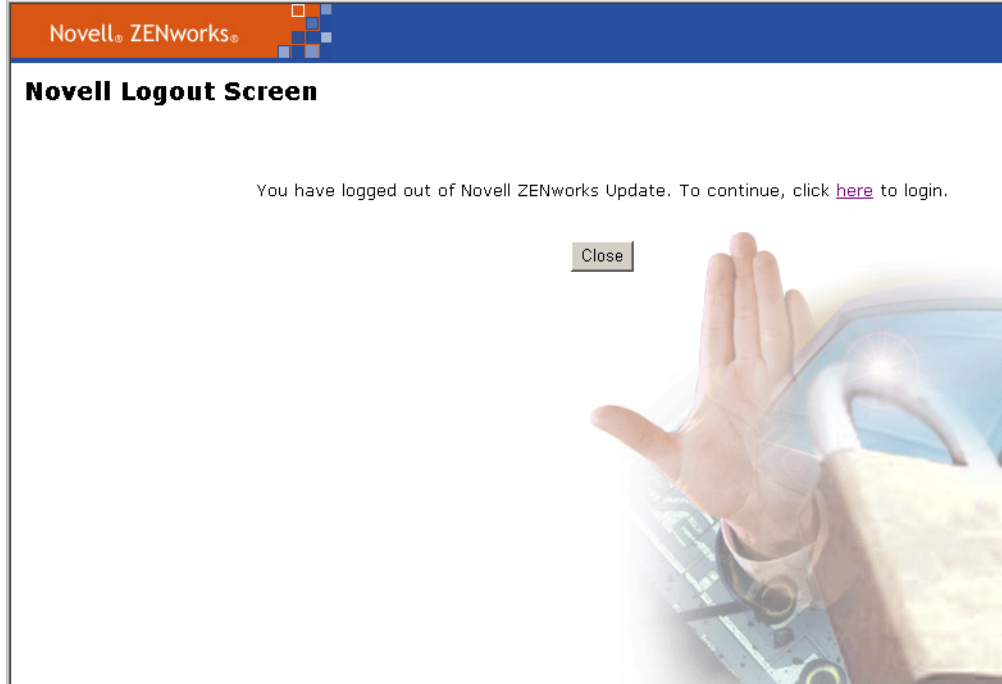
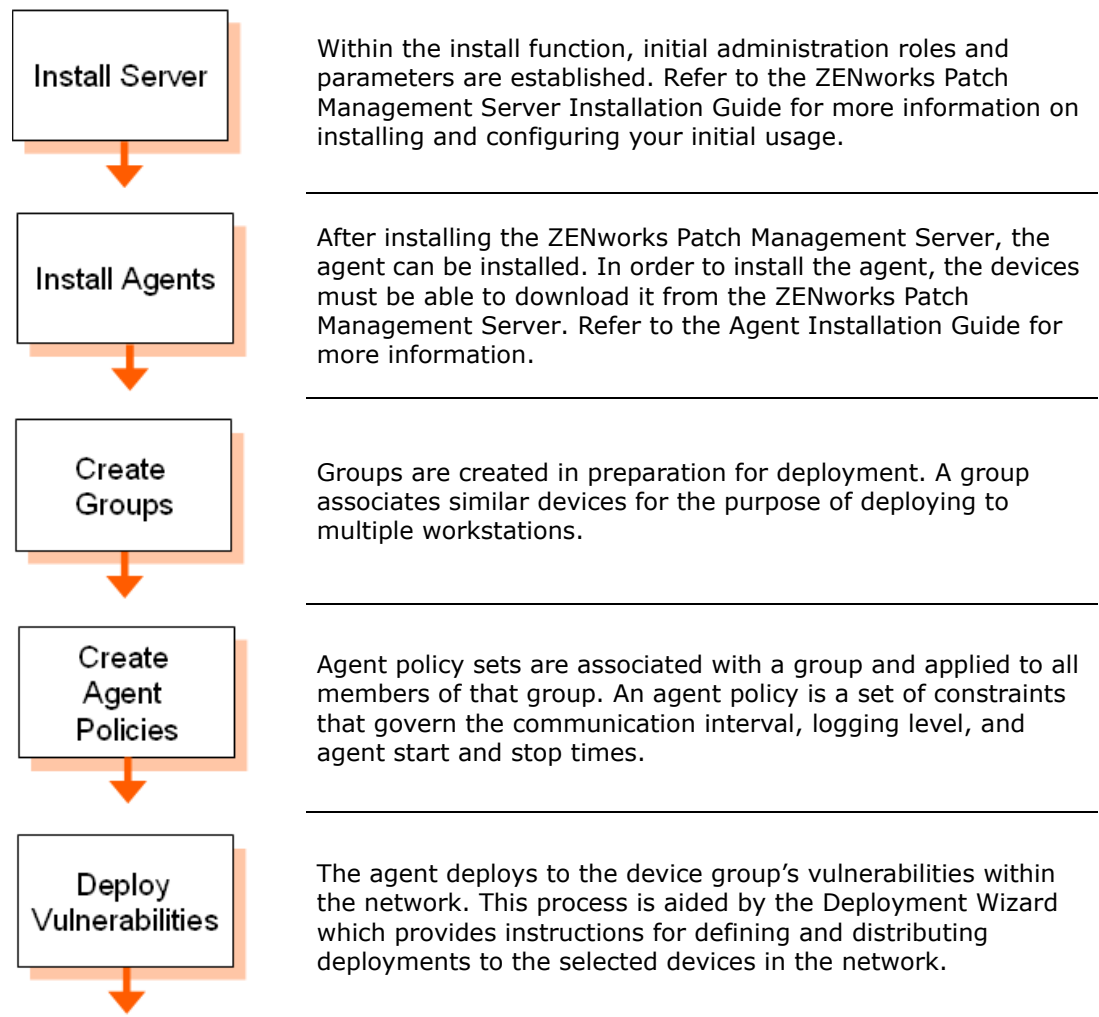


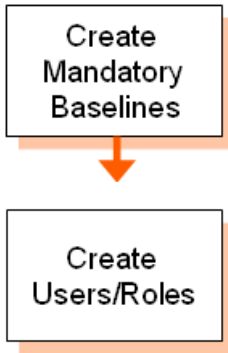
Figure 2.3 Novell Logout Screen



Getting Started with Novell ZENworks Patch Management

Refer to the following process to determine your needs in using Novell ZENworks Patch Management.





After the initial vulnerabilities are resolved, a mandatory baseline can be set. This is a user-defined range of configuration settings for a group of devices. If a device falls out of compliance, applying the mandatory baseline ensures the device is patched back into compliance.

User permissions, credentials and roles can be established for all users of the system.

Navigating within ZENworks Patch Management

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 the ZENworks Patch Management 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	Display a list from which the user can select pre-configured values
Command Buttons	Perform specific actions when they select a command button
Check Boxes	A check box is selected or cleared to enable or disable a feature. Lists also include a Select All check box that lets you select all the available listed items on that page.
Radio Buttons	Select the button to select an item
Display Areas	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



Table 2.1 Browser Conventions

Screen Feature	Function
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: In some areas of ZENworks Patch Management, the *right-click* function is not supported.

Using Search

Using the search feature, you can filter information retrieved from the database and the subscription server. 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...

Search (vulnerability name/CVE no.):

Status: Not Patched

Results for Groups: ... All ...

Impact: ... All ...

Show results automatically: ☐

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 sort 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 <i>Vulnerabilities</i> page is accessed. You can change (reset) 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		Total: 3		
<input type="checkbox"/>	Action	User Name	Role	Full Name	First Logged On	Last Logged On
<input type="checkbox"/>		Administrator	Administrator			
<input type="checkbox"/>		PatchLink	Administrator	PatchLink	6/7/2006 12:22:34 PM	6/23/2006 12:07:36 PM
<input type="checkbox"/>		TechPubs	Technical Publications User	Technical Publications User		

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.

VulnerabilitiesPackagesTotal: 51

	Vulnerability Name	Impact							
+	A - Deployment Test and Diagnostic Package	Critical	0	1	0	1	0	100%	
+	MS03-023 823559 Buffer Overrun in HTML Converter Could Allow Code Execution	Critical - 01	0	1	0	1	0	100%	
+	MS03-041 823182 Vulnerability in Authenticode Verification Could Allow Remote Code Execution (SEE NOTES)	Critical - 01	0	1	0	1	0	100%	
-	MS03-043 828035 Buffer Overrun in Messenger Service Could Allow Code Execution (re-released 10/29/03)	Critical - 01	0	1	0	1	0	100%	
<div>Type: Active Vulnerability AnalysisAssociated Distribution Packages: 7 Impact: Critical - 01Distribution Packages Status: Cached and ready for deployment. Status: EnabledVendor: Microsoft Corp. Downloaded On: 7/9/2004 6:12:38 PM (GMT-08:00)Released On: 10/14/2003 5:00:00 PM (GMT-08:00) Vulnerability Results: CurrentVendor Product ID: CAN-2003-0717 Common Vulnerability Exploit (CVE): CAN-2003-0717 Vulnerability Code Description: The Messenger Service for Windows NT through Server 2003 does not properly verify the length of the message, which allows remote attackers to execute arbitrary code via a buffer overflow attack. Reference Text: MS:MS03-043 URL:http://www.microsoft.com/technet/security/bulletin/ms03-043.asp CERT:CA-2003-27 URL:http://www.cirt.org/advisories/CA-2003-27.html BUGTRAQ:20031016 MS03-043 Popup Messenger Service buffer-overflow URL:http://lma Description: A security vulnerability exists in the Messenger Service that could allow arbitrary code execution on an affected system. The vulnerability results because the Messenger Service does not properly validate the length of a message before passing it to the allocated buffer. More Information</div>									
+	MS03-044 825119 Buffer Overrun in Windows Help and Support Center Could Lead to System Compromise	Critical - 01	0	1	0	1	0	100%	
+	MS04-011 835732 Security Update for Microsoft Windows (SEE NOTES)	Critical - 01	0	1	0	1	0	100%	

< > 1 of 2 Pages > | Rows Per Page: 50

Figure 2.6 Show/Hide Row Option

Advancing through Patch Information 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

- **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.

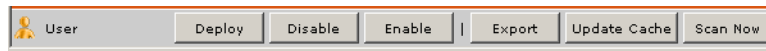


Figure 2.8 Action Menu

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.

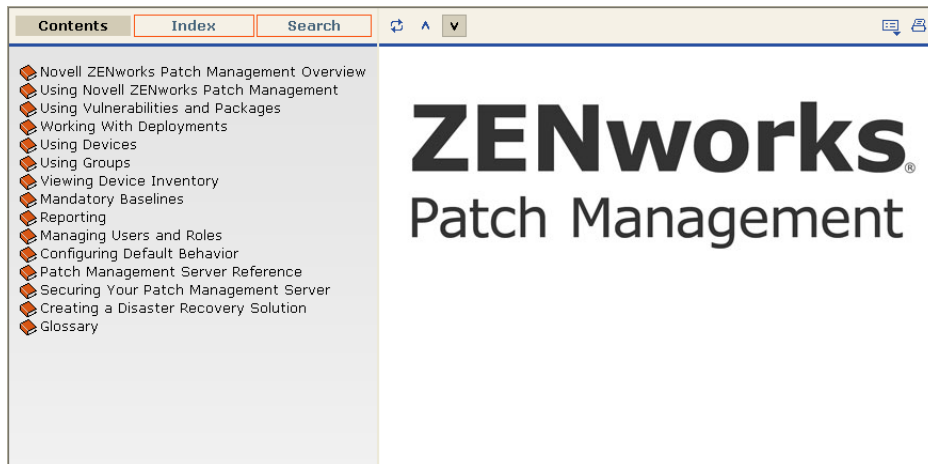


Figure 2.9 Example Help Screen



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 selected results. However, some data may not import or not 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 floppy	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 IDI	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. The file name used varies based upon the data exported.



Using the ZENworks Patch Management Home Page

The entry point to Novell ZENworks Patch Management is the *Home* page. This is where 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 ZENworks Patch Management Navigation Menu” - accesses the administrative options
- “Viewing the General Information Links” - provide user support and server status information
- “Viewing Latest News” - provides a scrolling window with current information regarding patches
- “Viewing Current Status Information” - displays the status of your subscription

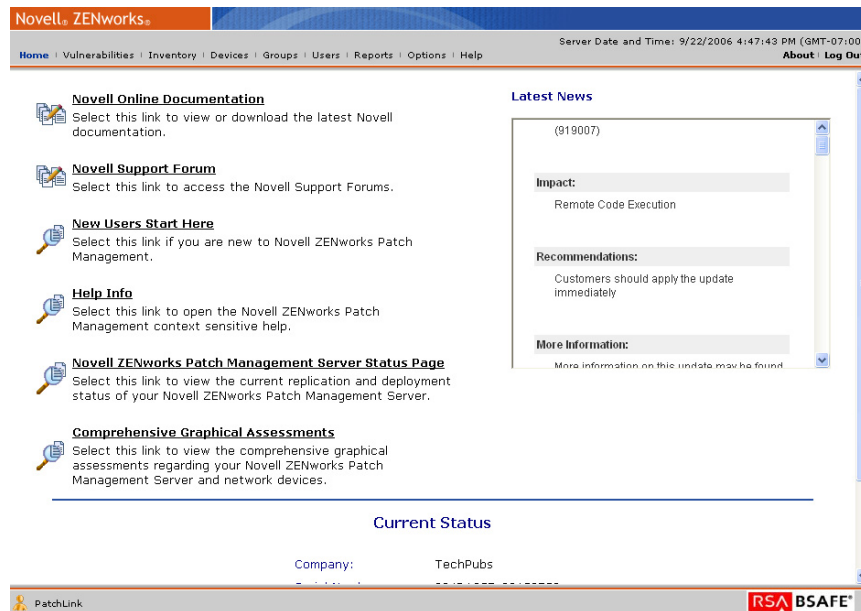


Figure 2.11 ZENworks Patch Management Server Home Page



Using the ZENworks Patch Management Navigation Menu

The ZENworks Patch Management 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.

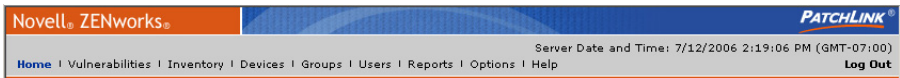


Figure 2.12 Navigation Menu

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

Table 2.3 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
Inventory	Displays a comprehensive inventory of all registered products
Devices	Manages the devices registered to Patch Management Server
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 scanner integration and enhanced reporting. Once installed, the component is included in the main navigation menu.

Viewing the General Information Links

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

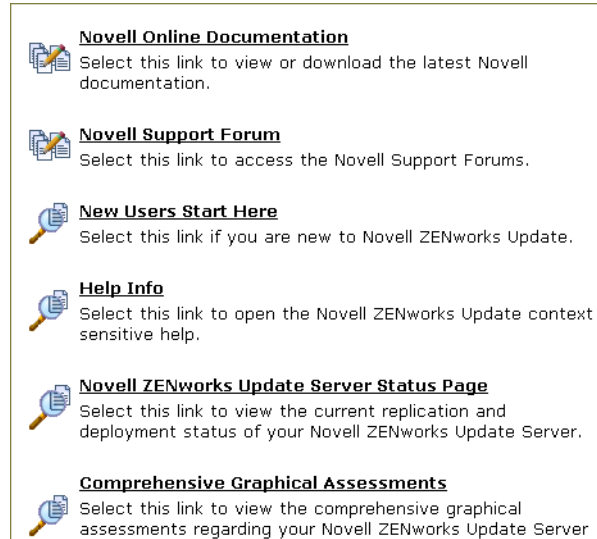


Figure 2.13 General Information Links

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

Table 2.4 General Information Links

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



Table 2.4 General Information Links

General Information Link	Description
ZENworks Patch Management Server Status Page	Displays the Replication Status between the Patch Management Server server and the Global Subscription Server patch repository. See "Using the ZENworks Patch Management Status Page" on page 22 for more information
Comprehensive Graphical Assessments	Illustrates the status of various patch elements of your ZENworks Patch Management environment. See "Viewing the Comprehensive Graphical Assessments" on page 23 for more information

Viewing Latest News

The Latest News area is a scrolling window that displays important announcements and other information regarding the ZENworks Patch Management system. You can select any links within the news window or navigate topics by using the scroll bar. Moving your mouse over the Latest News area stops the scrolling window.



Figure 2.14 Latest News Window



Viewing Current Status Information

The Home page displays a *Current Status* area at the bottom of the page providing registered user information, Patch Management Server license key (serial number), and information about current license usage and availability.

Current Status	
Company:	TechPubs
Serial Number:	88888888-88888888
Non-Expired Licenses:	10
Licenses In Use:	1
Licenses Available:	9
Last Update:	Not connected yet

Figure 2.15 Patch Management Server Current Status

Table 2.5 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



Note: A License Expiration notice displays if all available Patch Management Server licenses have been registered. See “[License Expiration](#)” on page 27 for more information.



Using the ZENworks Patch Management Status Page

The status page displays information about three primary functions of the ZENworks Patch Management Server.

- Replication Status
- Discovery and Analysis Status
- Deployment Status
- Cache Status

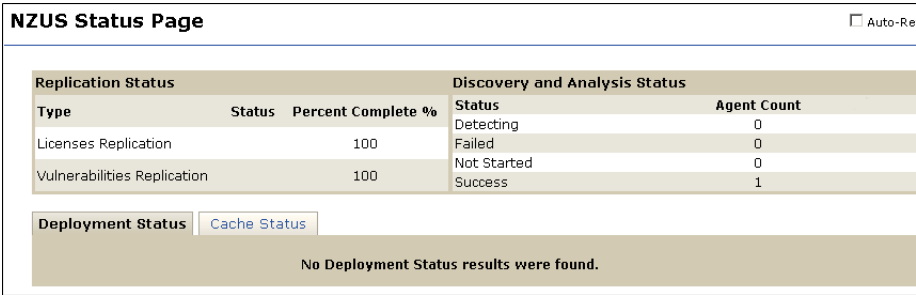


Figure 2.16 Patch Management Server Status Page

Replication Status

The ZENworks Patch Management Server Status page displays the Replication Status between the ZENworks Patch Management Server and the main Novell Subscription Service. The replication type, status and the percent complete of the replication is displayed in the window.

Discovery and Analysis Status

The *Discovery and Analysis* area displays data regarding the most current patch deployment. The area shows whether a patch is detecting, has failed, has not started or was successful.





Deployment Status

The Deployment Status area shows all deployments so you can confirm a package was deployed. Results in each column can be sorted to present in ascending or descending order by clicking the respective heading in each column. Select the **Deployment** to open the *Deployments by Package* page.



The following table defines the deployment statuses.

Table 2.6 Deployment Status Icons

Icon	Description
	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 are in the process of executing the deployment
	Percentage of the devices or groups that finished the deployment = [Total Finished Devices / Total Assigned Devices]

Cache Status

Cache Status is a chronological detailed list of the packages downloaded to the Patch Management Server cache. Each package is identified by name and the associated status, request date, start and finish dates, impact, and related operating systems.

Results in each column can be sorted in ascending or descending order by clicking the heading in each column. Clicking the *package name* heading opens a link to the device details page.

Viewing the Comprehensive Graphical Assessments

The Comprehensive Graphical Assessments page consists of four charts providing a current view of activity on the protected network. These charts are generated automatically based on the latest data available. The display and content of these charts cannot be edited.



Tip: You can generate a more customized view of activity in the **Reports** category.

Available charts include:

- Patch Status for all Devices
- Patch Status for all Vulnerabilities
- Devices Status for all Devices



- Baseline Status for all Device Groups.

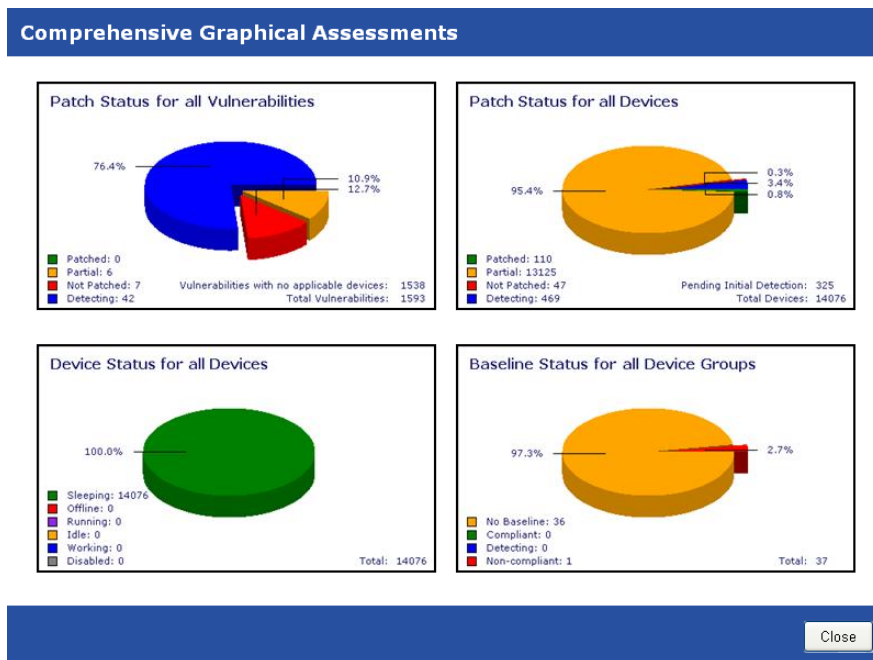


Figure 2.17 Patch Management Server Graphical Assessments

Patch Status for all Devices

Displays the patch status for all devices by category.

- **Patched** - Devices that have had all critical vulnerabilities patched
- **Partial** - Devices that have received some but not all of the available critical patches
- **Not Patched** - Devices that are not patched
- **Detecting** - Devices in process of analysis and detection

- **Pending Initial Detection** - Devices waiting for analysis and detection

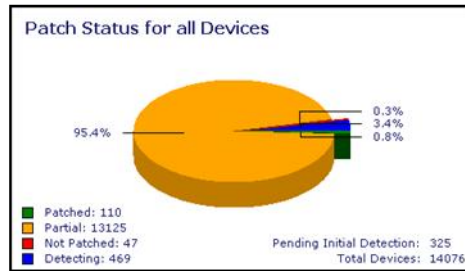


Figure 2.18 Patch Status for all Devices

Patch Status for all Vulnerabilities

Displays the patch status of all vulnerabilities by category.

- **Patched** - Vulnerabilities that are completely patched
- **Partial** - Vulnerabilities that are partially patched
- **Not Patched** - Vulnerabilities that are not patched
- **Detecting** - Vulnerabilities in process of analysis and detection
- **Vulnerabilities with no applicable devices** - Vulnerabilities not assigned to an applicable device

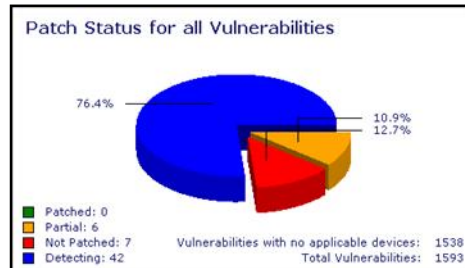


Figure 2.19 Patch Status for all Vulnerabilities

Status for all Devices

Displays the status of all devices by category.

- **Sleeping** - Devices currently outside the assigned hours of operation
In this case, the device is sleeping in regard to the agent only (the device may be in use)
- **Offline** - Devices that have not communicated with Patch Management Server in more than two intervals



- **Running** - Devices currently performing the analysis detection outside the normal means
- **Idle** - Device agent is communicating fine and currently not performing any tasks
- **Working** - Device agent currently is working on a task
- **Disabled** - Device is disabled and unable to perform any tasks

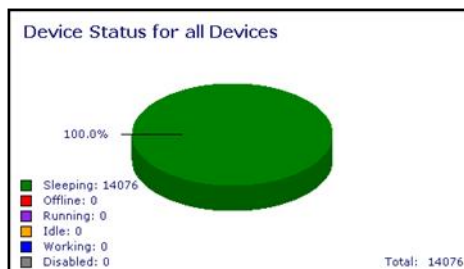


Figure 2.20 Device Status for all Devices

Baseline Status for all Groups

Displays the status of groups by category.

- **No Baseline** - Groups in which all members are fully compliant with the defined baseline
- **Compliant** - Groups in which all members are not compliant with the defined baseline
- **Detecting** - Groups in which member(s) are undergoing detection and analysis
- **Non-compliant** - Groups that do not have an associated mandatory baseline

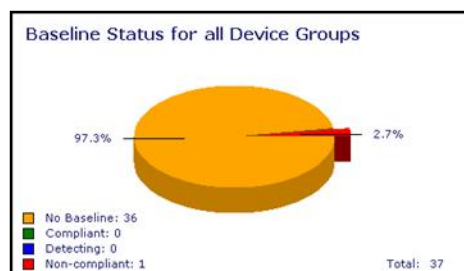


Figure 2.21 Mandatory Baseline Status for all Groups

License Expiration

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



Note: For detailed information about product licensing, in Patch Management Server, click **Options > Products** to open the *Product Licensing* page.



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. 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.

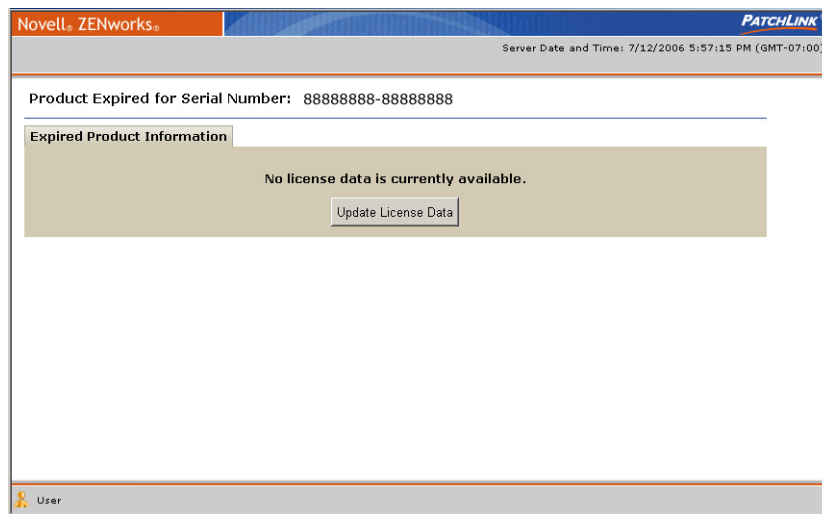


Figure 2.22 License Expiration Page



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 vulnerabilities across all systems registered to the 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 the actual patch software and executable code used to correct or patch vulnerabilities. Vulnerabilities may contain several packages that are deployed in a specific order for specific environments (different operating systems for example).

In this Chapter

- “About Vulnerabilities” on page 29
- “Working with Vulnerabilities” on page 36
- “About Packages” on page 43
- “Working with Packages” on page 51

About Vulnerabilities

The vulnerability tab displays a complete listing of all known patches and updates reported by software vendors. Once reported and analyzed, the vulnerabilities are registered for distribution to your ZENworks Patch Management Server through the Global Subscription Server. The ZENworks Patch Management Agent installed on each device checks for known vulnerabilities. Called the



Discover Applicable Updates (DAU), this task returns the results displayed on the vulnerabilities page. The results are presented in a table of vulnerability patch status. The total number of vulnerabilities displays above the table in the top right corner.

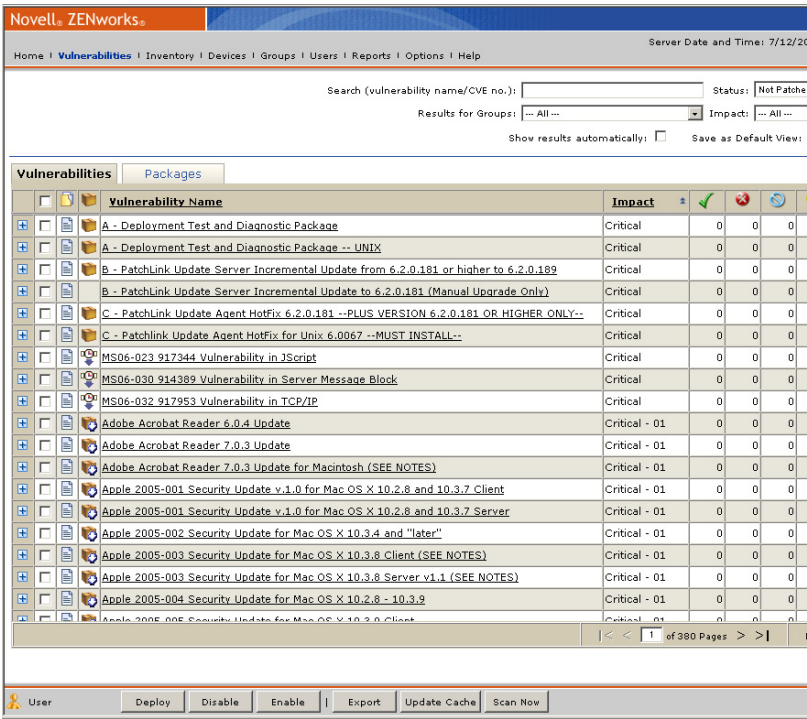


Figure 3.1 Vulnerabilities Page

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 data for the vulnerability.

Adobe Acrobat Reader 6.0				
Not Patched Patched Error Detecting				Total: 1
Device Name	Other Name	Operating System	OS Version	Analysis Date
\\TP_EMERALD	TP_Emerald.techpubs.com	Win2K3	Win2K3-Service Pack 1	3/14/2006 3:22:41 PM

Figure 3.2 Vulnerability Details



To View a Vulnerability

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

Adobe Acrobat Reader 6.0				
<div> <div>Not Patched</div> <div>Patched</div> <div>Error</div> <div>Detecting</div> </div> <div>Total: 1</div>				
<input type="checkbox"/>	Device Name	Other Name	Operating System	OS Version
<input type="checkbox"/>	\\TP_EMERALD	TP_Emerald.techpubs.com	Win2K3	Win2K3-Service Pack 1
				3/14/2006 3:22:41 PM

Figure 3.3 Vulnerability Details

Using the Vulnerabilities Page

Selecting the expand button (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		Total: 9490									
<input type="checkbox"/>	<input type="checkbox"/>	Vulnerability Name	Impact	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	A - Deployment Test and Diagnostic Package	Critical	0	0	0	0	0	0	0	0	0%	
<div> <div>Type: Active Vulnerability Analysis</div> <div>Status: Enabled</div> <div>Downloaded On: 7/7/2006 10:31:29 AM (GMT-07:00)</div> <div>Vulnerability Results: Current</div> </div> <div> <div>Associated Distribution Packages: 2</div> <div>Distribution Packages Status: Cached and ready for deployment.</div> <div>Vendor: PatchLink Corporation</div> <div>Released On: 12/18/2001 4:00:00 PM (GMT-07:00)</div> <div>Vendor Product ID: PLDemo</div> </div> <div> <div>Description: This is a demonstration for the package deployment feature in PatchLink Updates. 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.exe and store it in the system temp directory. More Information</div> </div>													
<input type="checkbox"/>	<input type="checkbox"/>	A - Deployment Test and Diagnostic Package -- UNIX	Critical	0	0	0	0	0	0	0	0	0%	
<input type="checkbox"/>	<input type="checkbox"/>	B - PatchLink Update Server Incremental Update from 6.2.0.181 or higher to 6.2.0.189	Critical	0	0	0	0	0	0	0	0	0%	
<input type="checkbox"/>	<input type="checkbox"/>	B - PatchLink Update Server Incremental Update to 6.2.0.181 (Manual Upgrade Only)	Critical	0	0	0	0	0	0	0	0	0%	
<input type="checkbox"/>	<input type="checkbox"/>	C - PatchLink Update Agent HotFix 6.2.0.181 --PLUS VERSION 6.2.0.181 OR HIGHER ONLY--	Critical	0	0	0	0	0	0	0	0	0%	
<input type="checkbox"/>	<input type="checkbox"/>	C - PatchLink Update Agent HotFix for Unix 6.0067 --MUST INSTALL--	Critical	0	0	0	0	0	0	0	0	0%	
<input type="checkbox"/>	<input type="checkbox"/>	MS06-023 917344 Vulnerability in JScript	Critical	0	0	0	0	0	0	0	0	0%	
<input type="checkbox"/>	<input type="checkbox"/>	MS06-030 914389 Vulnerability in Server Message Block	Critical	0	0	0	0	0	0	0	0	0%	
<input type="checkbox"/>	<input type="checkbox"/>	MS06-032 917953 Vulnerability in TCP/IP	Critical	0	0	0	0	0	0	0	0	0%	
<input type="checkbox"/>	<input type="checkbox"/>	Adobe Acrobat Reader 6.0.4 Update	Critical - 01	0	0	0	0	0	0	0	0	0%	
<input type="checkbox"/>	<input type="checkbox"/>	Adobe Acrobat Reader 7.0.3 Update	Critical - 01	0	0	0	0	0	0	0	0	0%	
<input type="checkbox"/>	<input type="checkbox"/>	Adobe Acrobat Reader 7.0.3 Update for Macintosh (SEE NOTES)	Critical - 01	0	0	0	0	0	0	0	0	0%	

Figure 3.4 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.

- **Beta** - Released to the Novell BETA community.
- **New** - Downloaded to the Patch Management Server, from the Global Subscription Server, since the your last session began.
- **Current** - Downloaded to the Patch Management Server, from the Global Subscription Server, prior to your previous session. The following table includes descriptions of the Vulnerability status icons.

Table 3.1 Vulnerability Status Icons and Descriptions

Beta	New	Current	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 icons and their status are classified as follows:

- **New** - This package was released and its metadata downloaded from the Global Subscription Server since your last session.
- **Current** - This package was released and its metadata downloaded from the Global Subscription Server before your last session began.
- **Tasks** - A a system task distribution package.
- **Local** - The locally created distribution package.



Table 3.2 Package Status Icons and Descriptions

New	Existing	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
				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

- **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 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 entry contains columns which illustrate the current result statistics for the computers which have been scanned in addition to the overall percentage completion of all computers which will be scanned for that particular vulnerability.

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



Table 3.3 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 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 vulnerabilities page.

Refer to “[Using Search](#)” on page 11 for instructions on how to use the search and filter functions.



Working with Vulnerabilities

There are several tasks associated with vulnerabilities designed to assist you in managing and deploying vulnerabilities. These are available from commands located in the *Action* menu at the bottom on the Vulnerabilities page. These tasks include:

- “Deploying Vulnerabilities”
- “Viewing Vulnerabilities”
- “Disabling and Enabling Vulnerabilities”
- “Updating the Vulnerability Cache”
- “Scanning for Vulnerabilities”

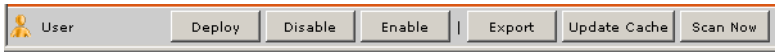


Figure 3.5 Vulnerabilities - Action Menu

Vulnerability Status (tabs)

The analysis results of the vulnerability are detailed and separated into four tabbed displays representing the status of devices in relation to the vulnerability analysis. As part of the analysis, a list of all devices requiring (or applicable) to the patch is displayed in each tabbed grouping (status-level).

- **Not Patched** - devices detected as requiring the vulnerability patch.
- **Patched** - devices detected as having a current patched for the vulnerability.
- **Error** - devices that generated an error during analysis of the patch status for the vulnerability.
- **Detecting** - devices in the process of determining patch status or waiting for the analysis process to begin.
- **Information** - displays detailed information about the vulnerability.

Column Definitions

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

Table 3.4 Vulnerability Column Definitions

Name	Definition
Device Name	The name of the device
Other 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



Table 3.4 Vulnerability Column Definitions

Name	Definition
OS Version	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 shows the available agent status icons and a description of each status

The following table defines the available device (agent) statuses and their associated icons.

Table 3.5 Device Status Icons






















Status	Description
	The agent is idle (this is a valid agent without any current or pending deployments)
	The agent is idle and has pending deployments
	The agent is currently working on a deployment (animated icon)
	The agent is offline
	The agent is offline and has pending deployments
	The agent is sleeping due to its Hours of Operation settings
	The agent is sleeping due to its Hours of Operation settings and has pending deployments
	This agent has been disabled
	This agent has been disabled, and has pending deployments
	The agent is offline and is in a QChain status (can accept chained deployments only after reboot)



Table 3.5 Device Status Icons

Status	Description
	The agent is offline, is in a QChain status (can accept chained deployments only after reboot), and it has pending deployments
	The agent is offline and is in a 'Dirty R' status (can accept no more deployments until after it reboots)
	The agent is offline, is in a 'Dirty R' status (can accept no more deployments until after it reboots), and it has pending deployments
	The agent is in a QChain status (the agent can accept chained deployments only until after a reboot)
	The agent is in a QChain status (the agent can accept chained deployments only until after a reboot) and it has pending deployments
	The agent is in a 'Dirty R' status (the agent can accept no more deployments until after it reboots)
	The agent is in a 'Dirty R' status (the agent can accept no more deployments until after it reboots) and it has pending deployments
	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 QChain status (can accept chained deployments only until after a reboot) and it has pending deployments and is sleeping due to its Hours of Operation settings.
	The agent is in a 'Dirty R' status (the agent can accept no more deployments until after it reboots) and is sleeping due to its Hours of Operation settings.
	The agent is in a 'Dirty R' status (can accept no more deployments until after it reboots) and it has pending deployments and is sleeping due to its Hours of Operation settings.

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 deployments out to the protected devices in the network. Refer to [Chapter 4, “Working With Deployments”](#) for additional information.

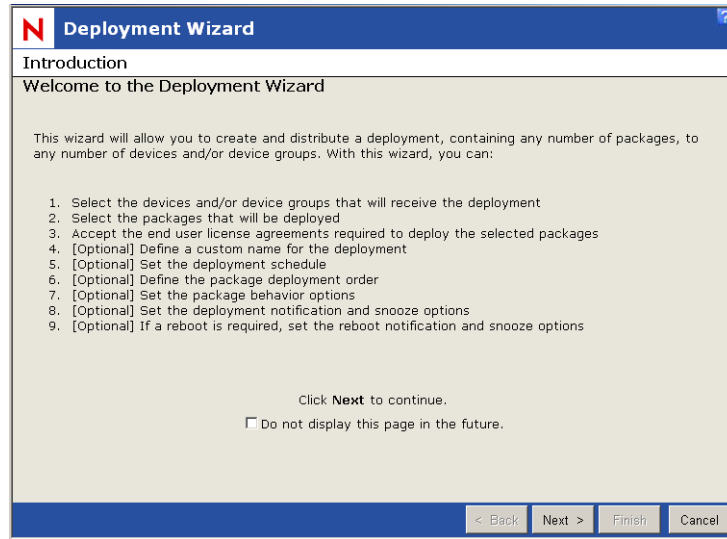


Figure 3.6 Vulnerability Details

Disabling and Enabling Vulnerabilities

Disabling a vulnerability restricts the selected vulnerability from being scanned during the *Discover Applicable Updates (DAU)* system task. The DAU task does not attempt to detect a requirement for the vulnerability on any device.

For example, you would disable a vulnerability that, while valid, you do not want to deploy because it conflicts with your overall IT strategy.

An enabled vulnerability is included in the scanning activity of the DAU system task. All vulnerabilities are initially enabled.



Note: Once disabled, the vulnerability may not appear in the Vulnerabilities list based on your *Status* 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 in the list of vulnerabilities identified with the *disabled* icon in the status column.

To Enable a Vulnerability

1. In the *Vulnerabilities* list, select the disabled vulnerability(s).
2. In the action menu, click **Enable**.
The vulnerability displays in the list of vulnerabilities identified with the *enabled* icon in the status column.

Scanning for Vulnerabilities

Scanning reschedules the Discover Applicable Updates System Task (DAU) for immediate execution. The DAU runs on a predefined interval schedule. Enacting a scan manually schedules the task for immediate execution. The **Scan Now** command results in the same action regardless of the current page.



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.

To Scan Devices

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.

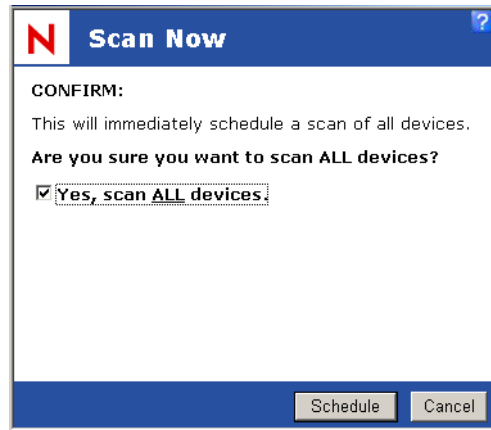


Figure 3.7 Scan Devices



Warning: Scheduling a DAU entails creating traffic for all the selected devices.

3. Select **Yes, scan the selected device** and click **Schedule**.
Scan Now - Success dialog box appears informing you that the scan has been processed and providing a link to view the results of the DAU deployment.

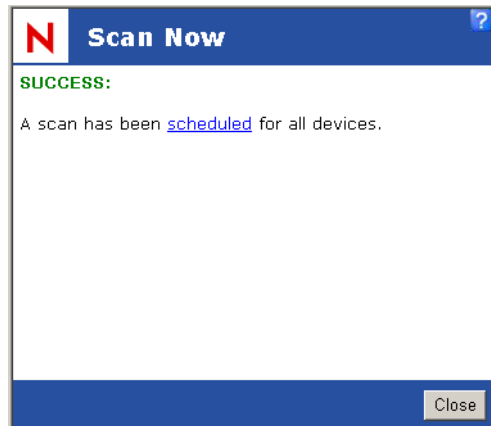


Figure 3.8 Scan Group Scheduled



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

Updating the Vulnerability Cache

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

To Cache Vulnerability Data

1. In the *Vulnerabilities* list, select one or multiple vulnerabilities.
2. In the *Action* menu, click **Update Cache**. The *Warning* dialog box opens prompting you to confirm the update request and informing you that this action may take an extended period of time.
3. Click **OK**

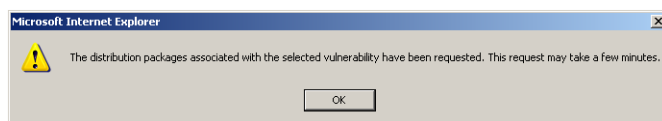


Figure 3.9 Update Cache - Warning dialog box

About Packages

A package is an archive containing all patch software and executable code required to successfully deploy and execute a patch. Packages comprise software to send to a device or group of devices.

The process of sending a package to a device(s) is called deploying a package (or simply a *deployment*).

Packages can run tasks, scripts, install software applications, place files (or directories of files) to a specified location, change the configuration of an application or service, and other programatic functions that can be performed in an unattended manner. The majority of packages comprise patches for specific vulnerabilities, defects or software bugs. A vulnerability may contain several packages that are deployed and executed in a specific order.

To View the Existing Package List

1. In the Patch Management Server main toolbar, select **Vulnerabilities**.
2. In the *Vulnerabilities* page, select the **Package** 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.

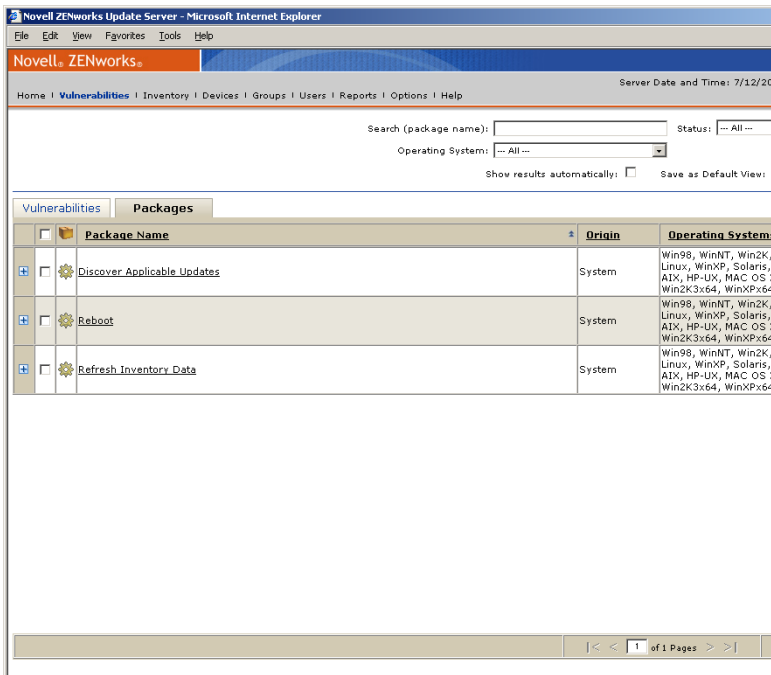


Figure 3.10 Packages View



Using the Packages Tab

Click the expand option (plus sign) to display detailed package information. Select the package name to display the package details (including the Package Deployments tab and the **Package Information Tab**).

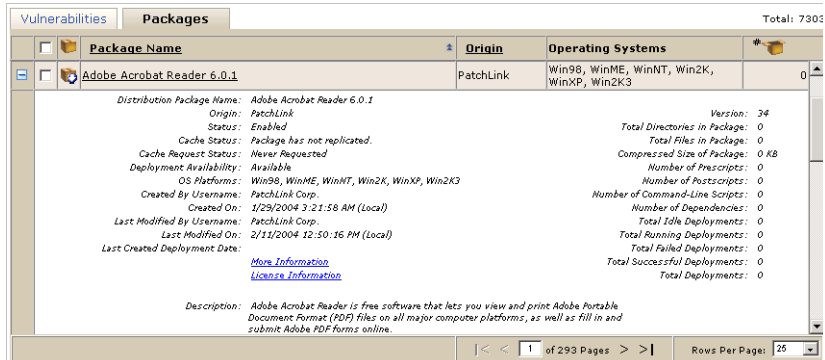


Figure 3.11 Package Details

The package summary includes the following information:

Table 3.6 Package Summary Definitions

Status	Description
Distribution Package Name	Title of the package.
Origin	Point of origin of the package. An origin of PatchLink or System refers to system tasks.
Status	The current status of the package.
Cache Status	The current cache status of the package.
Cache Request Status	Indicates if the package has been requested.
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.
Created By Username	The Patch Management Server user who created the package.
Created On	The date and time the package was created.
Last Modified By Username	The Patch Management Server user who last modified the package.
Last Modified On	The date and time of the last change to the package.



Table 3.6 Package Summary Definitions

Status	Description
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 fully successful deployments.



Package Information Tab

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

Package Details for Adobe Acrobat Reader 6.0.1

Deployments Package Information

Package Information:

Distribution Package Name: Adobe Acrobat Reader 6.0.1	Operating Systems: Win98, WinME, WinNT, Win2K, WinXP, Win2K3
Status: Enabled	
Created By: PatchLink Corp.	Created On: 1/29/2004 11:21:58 AM
Last Modified By: PatchLink Corp.	Last Modified On: 2/11/2004 8:50:16 PM
More Information	License Information
Description: Adobe Acrobat Reader is free software that lets you view and print Adobe Portable Document Format (PDF) files on all major computer platforms, as well as fill in and submit Adobe PDF forms online. This new version of the familiar Adobe Acrobat Reader provides a host of rich features that enable you to: Submit Adobe PDF forms that are created with fillable form fields. Play back a variety of embedded multimedia content, such as QuickTime and MP3 files. Activate search and accessibility capabilities built into your PDF files. Read and organize high-fidelity eBooks. 	

Package Contents:

Files: 0	Directories: 0
Disk Space: 0 KB	Dependencies: 0
Scripts:	

Figure 3.12 Package Details - Package Information tab

Table 3.7 Package Information Definitions

Status	Description
Package Information	
Distribution Package Name	Title of the package.
Status	The current status of the package.
Origin	Point of origin of the package. An origin of PatchLink or System refers to system tasks.
Created By	The Patch Management Server user who created the package.
Last Modified By	The Patch Management Server 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.
Description	Narrative description of the distribution package. Also includes links to any relevant Novell knowledge base articles.
Operating Systems	The operating systems and platforms that the package supports and may be deployed to.
Version	The package version.



Table 3.7 Package Information Definitions

Status	Description
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 fully 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	
<input type="checkbox"/>		Adobe Acrobat (Chinese-CHS) Reader 7.0.5	PatchLink	WinNT, Win2K, WinXP, Win2K3	0
<input type="checkbox"/>		Adobe Acrobat (Chinese-CHS) Reader 7.0.7	PatchLink	WinNT, Win2K, WinXP, Win2K3	0
<input type="checkbox"/>		Adobe Acrobat (Chinese-CHT) Reader 7.0.5	PatchLink	WinNT, Win2K, WinXP, Win2K3	0
<input type="checkbox"/>		Adobe Acrobat (Chinese-CHT) Reader 7.0.7	PatchLink	WinNT, Win2K, WinXP, Win2K3	0
<input type="checkbox"/>		Adobe Acrobat (Dutch) Reader 7.0.5	PatchLink	WinNT, Win2K, WinXP, Win2K3	0
<input type="checkbox"/>		Adobe Acrobat (Dutch) Reader 7.0.7	PatchLink	WinNT, Win2K, WinXP, Win2K3	0






















Figure 3.13 Package Status

The icons and their status are classified as follows:



- **New** - This package was released and its metadata downloaded from the Global Subscription Server since your last session.
- **Current** - This package was released and its metadata downloaded from the Global Subscription Server before your last session began.
- **Tasks** - A system task distribution package.
- **Local** - The locally created distribution package.

Table 3.8 Package Status Icons and Descriptions

New	Existing	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
				The package is currently deploying (animated icon)
				The package is disabled



Column Definitions

The following table includes descriptions of the package column definitions.

Table 3.9 Package Column Definitions

Name	Definition
Package Name	Package names typically include the vendor, application, and version information.
Package Origin	Novell or System are common origins meaning that package results from a system task
Package Operating Systems	The operating systems column displays the platforms that are supported by the package. That is, the package can be deployed to devices running the operating systems presented in the list. This information is based on the total number and types of operating systems detected in the ZENworks Patch Management environment.
Package Deployment Associations	Shows the 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 vulnerabilities page.

Refer to “Using Search” on page 11 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 managing packages and using packages to deploy vulnerabilities. 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 Package Cache”



Figure 3.14 Packages - Action Menu

Deploying a Package

Deploying a distribution 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.



Figure 3.15 Package Deployment Wizard





Tip: Deploying via the Packages page will allow you to deploy inapplicable vulnerabilities.

Deleting a Package

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



Note: Package metadata (and not the files or scripts) for Novell-provided packages that are deleted will be re-downloaded from the Global Subscription Server. However, the package will not be cached unless is a critical package or requested by a deployment.

To Delete a Package

1. In the *Packages* list, select one or multiple packages.
2. In the action menu, click **Delete**
3. Confirm the request to delete the package(s).
4. The package(s) is deleted from the packages list.

Updating Package Cache

Updating system cache initiates the process to cache (or re-cache) the selected packages. If no packages are selected this will re-cache all of the previously cached 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 prompting you to confirm the update request and informing you of the expected processing time for the action.
3. Click **OK**.
The Package Data is cached.

Editing a Package

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



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

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](#)” on page 53 section for details on changing packages through the Package Wizard.

Creating a Package

Creating packages is performed using the Package Wizard that takes you through the steps of creating a distribution 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](#)” on page 54 section 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.

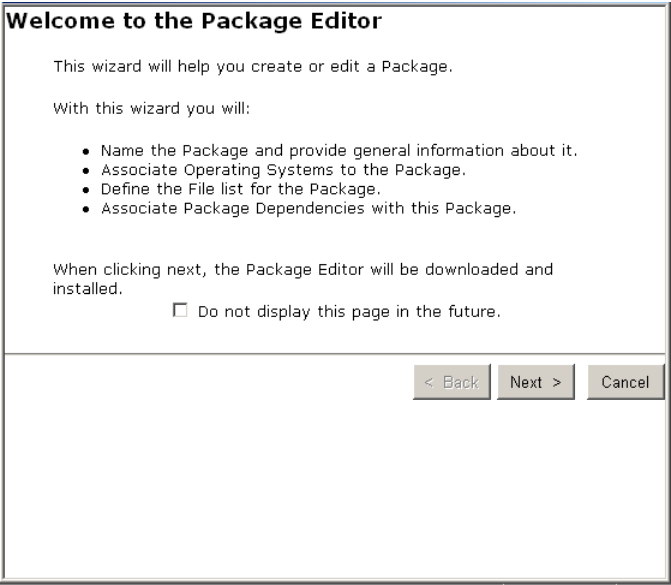


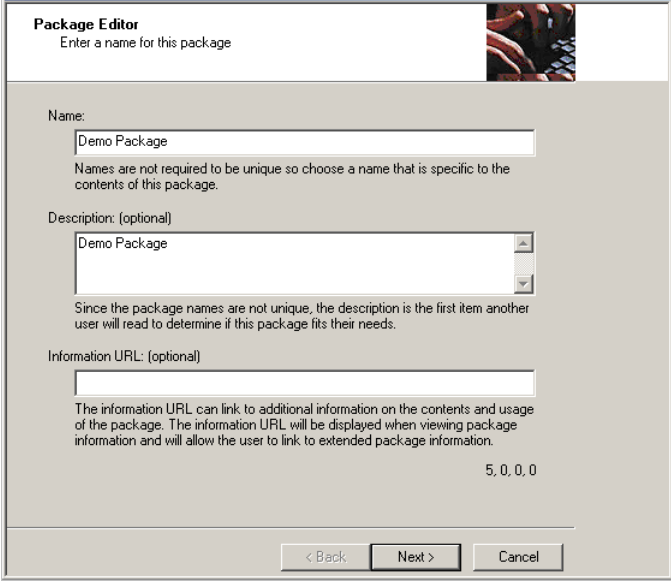
Figure 3.16 Package Editor Welcome Screen

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)



Package Editor
Enter a name for this package

Name:
Demo Package
Names are not required to be unique so choose a name that is specific to the contents of this package.

Description: (optional)
Demo Package
Since the package names are not unique, the description is the first item another user will read to determine if this package fits their needs.

Information URL: (optional)

The information URL can link to additional information on the contents and usage of the package. The information URL will be displayed when viewing package information and will allow the user to link to extended package information.
5, 0, 0, 0

< Back Next > Cancel

Figure 3.17 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”](#) on page 63 for more information about using deployment options.

4. Click **Next**.



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

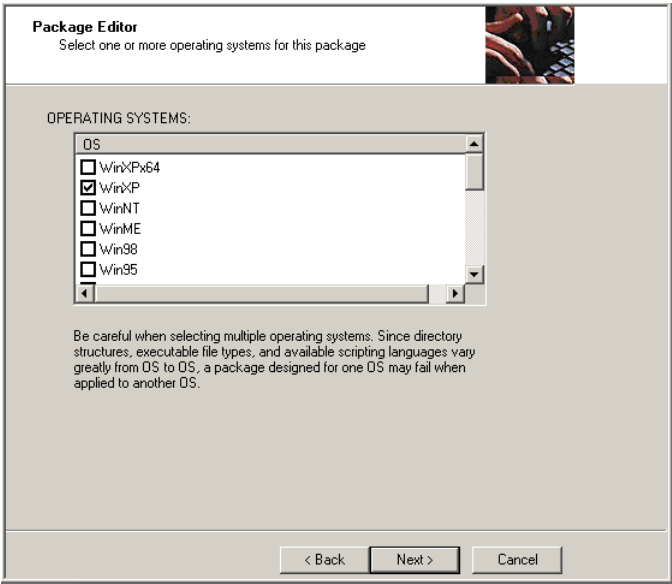


Figure 3.18 Package Editor - Select Operating System



Note: Since directory structures, executable file types, and available scripting languages vary greatly from Operating System to Operating System, 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 files to the package and describe where the files will be installed when the package is deployed to devices.

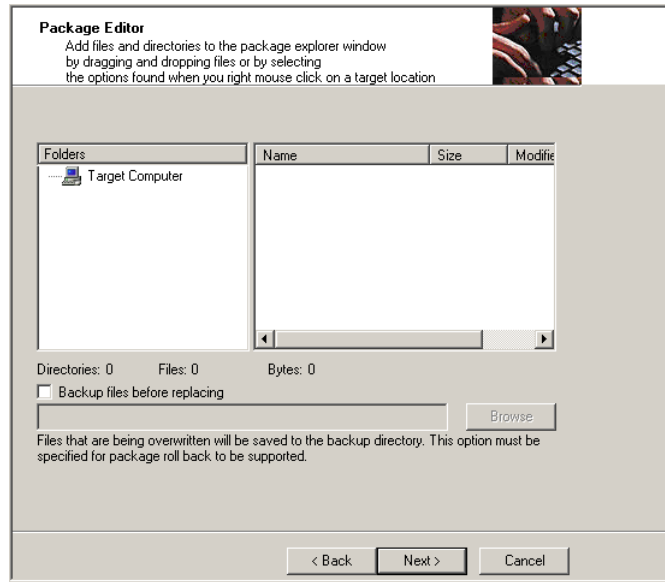


Figure 3.19 Package Editor - Add Files

Refer to **“Adding Files to a Package”** for additional details regarding adding Files to a package.

8. Click **Next**



9. In the **Create Scripts** page, you can (optionally) add and test a script to run on the target device during the deployment process.

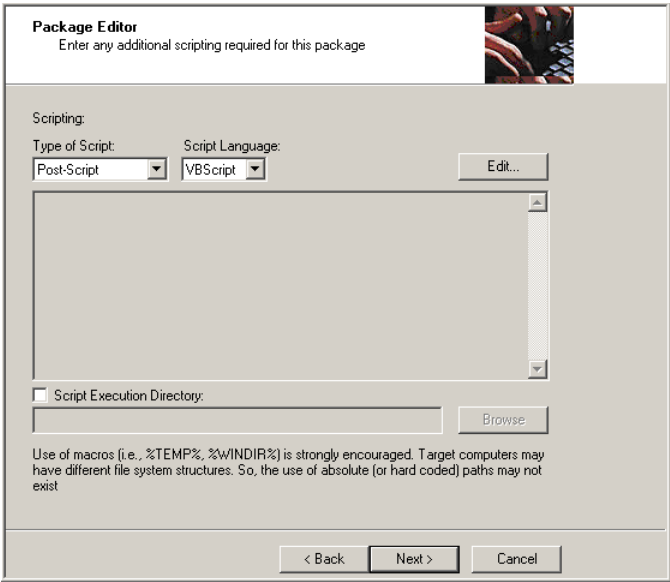


Figure 3.20 Package Editor - Create Script



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

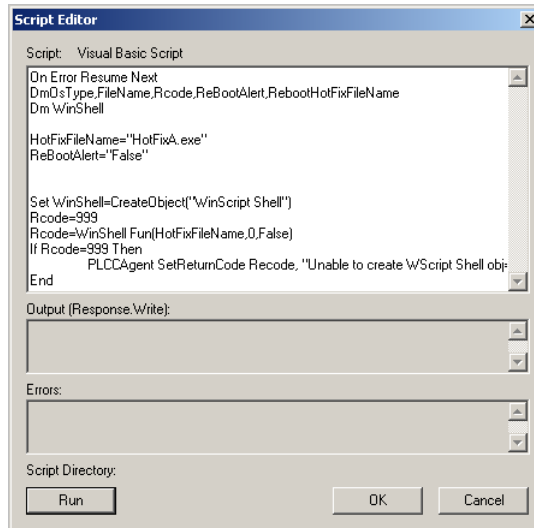


Figure 3.21 Script Editor

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 .

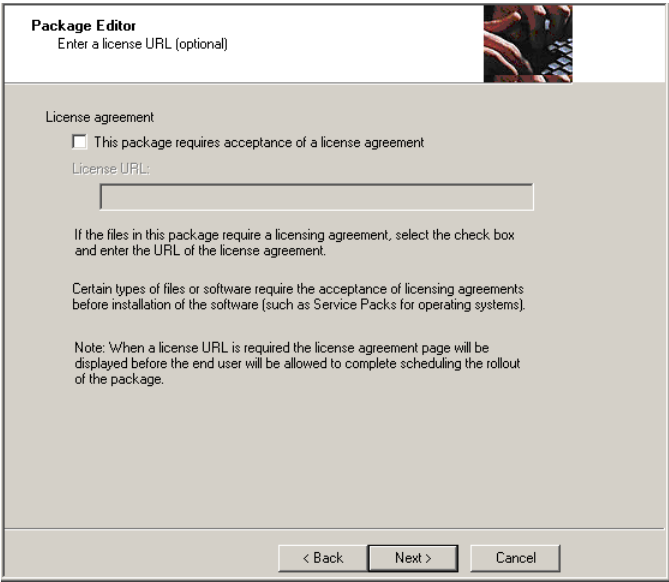


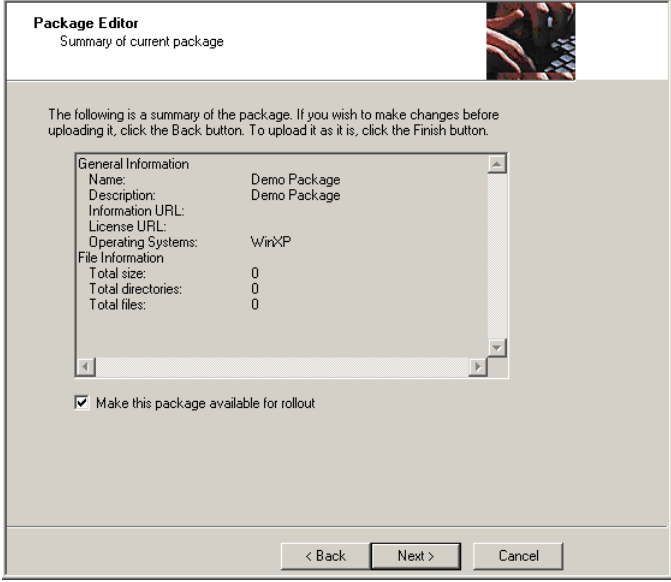
Figure 3.22 Package Editor - License URL

Refer to “[Working with License Agreements](#)” for additional details regarding licenses

12. Click **Next**



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



The screenshot shows the 'Package Editor' window with the 'Summary of current package' tab selected. The window contains a text area with the following text: 'The following is a summary of the package. If you wish to make changes before uploading it, click the Back button. To upload it as it is, click the Finish button.' Below this is a table with the following data:

General Information	
Name:	Demo Package
Description:	Demo Package
Information URL:	
License URL:	
Operating Systems:	WinXP

Below the table is a section for 'File Information' with the following data:

Total size:	0
Total directories:	0
Total files:	0

At the bottom of the window, there is a checkbox labeled 'Make this package available for rollout' which is checked. Below the checkbox are three buttons: '< Back', 'Next >', and 'Cancel'.

Figure 3.23 Package Editor - Summary

14. Click **Next**



Note: Selecting the **Make this package available for rollout checkbox**, will enable the package to show up in the list of available packages (after the package is created). You may wish to de-select this item if you are creating a skeleton package that will have additional files or details added at a later date or do not wish to enable the package deployment 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.

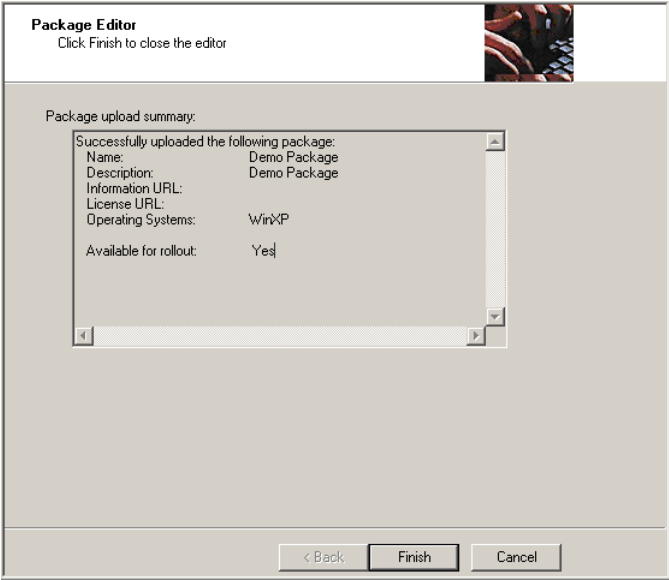


Figure 3.24 Package Editor - Upload Summary

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

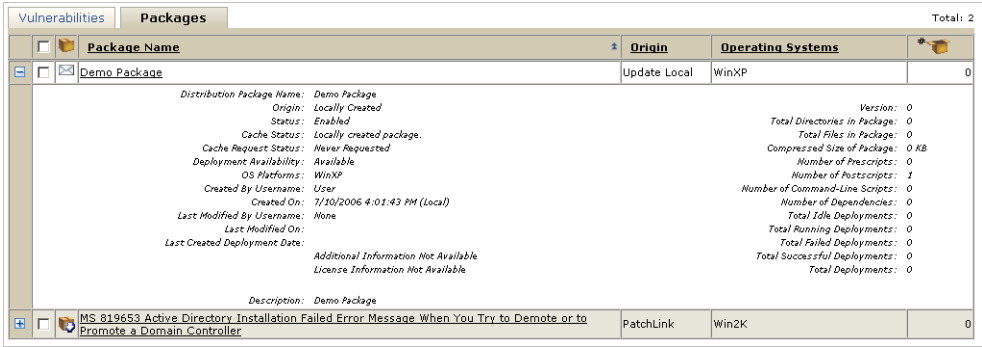


Figure 3.25 Packages Page - Custom Package



Including Deployment Options in a Package

To include a deployment option to indicate a manual installation of the patch is required, please type in (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 Flags

The following table defines the flag behavior and their descriptions:

Table 3.10 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 qchain 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	-ld	-l



Table 3.10 Package Flag Descriptions and Behavior

Description (flag behavior)	Display Flag	Select Flag
Reboot is required	Not Applicable	-2
Reboot may occur	Not Applicable	-3
Reboot is required, and MAY occur	Not Applicable	-4



Note: Many setup and installation packages are different and thus, the above flags are likely to change from package to package.

Note: To add different flags, simply type in their code. There is an input box available in the deployment wizard to allow the user to see the flags not displayed above.

Adding Files to a Package

A Windows Explorer type window initializes with a directory tree on the left starting at “Target Computer” and a file list on the right. Initially, these are both empty except for the “Target Computer” in the tree view. The Target Computer folder signifies the computer(s) on which this package will be installed. It is automatically created for you and cannot be deleted. You can begin to add files and/or directories to the package by either:

- Right-Mouse clicking on the “Target Computer” and selecting one of the options from the popup menu.
The Right-Mouse Click options are:
 - **Add Directory** - This option will bring up a file system browse window, where you can select which directory you wish to add. This option is always available.
 - **Add Files** - This option will bring up a file system browser window, where you can select which files you wish to add. This option only becomes available once there is a directory level created (or added) under Target Computer.
 - **Create MACRO** - You may create Folders from what are referred to as Macros. Any macro name can be created by placing matching percentage (%) sign's around a word when using the Create Folder option. The file editor allows you to create common macros by using the Create Macro option when right-mouse clicking on the Target Computer. Macros can be environment variables that are defined in the System Environment or special macros that only the Client Agent can expand.

Refer to “Using Macros” for more information regarding macros.

- Drag directories from a Windows Explorer or My Computer window onto the Target Computer.



- You can also drag files from a Windows Explorer or My Computer window onto any drive or directory in the tree view or into the file list.



Note: We recommend using the temp directory when delivering the package to your target computer. The files will be deployed to %systemroot%\temp directory (c:\winnt\temp on Windows 2000 Computers).

Using Macros

The following are a few examples of common macros:

Table 3.11 Macro Examples

Macro	Description
%TEMP%	The operating system temp directory location. %TEMP% is a macro that is guaranteed to exist on most systems. If it's not found in the operating system environment then it is created. %TEMP% typically expands to c:\Windows\Temp, c:\Temp, c:\WinNT\Temp, or /tmp depending on operating system and configuration.
%BOOTDIR%	The operating system boot directory location. %BOOTDIR% typically expands to c:\
%PROGRAM FILES%	The operating system program files location. %PROGRAM FILES% typically expands to c:\Program Files %WINDIR%The operating system windows directory location. %WINDIR% typically expands to c:\Windows
%ROOTDIR%	The operating system root directory location. %ROOTDIR% typically expands to c:\
%COMMON FILES%	The operating system common files location. %COMMON FILES% typically expands to c:\Program Files\Common Files



Note: Not all macros are available on all operating systems. Only select the macros available for the operating systems and configurations you are using. This option only becomes available at the directory level directly under the Target Computer option.

- Create Drive** - If your standard computer installation uses drives other C : \ or this package will be deployed to computers that use drives other than C : \, you can add drives to the package by right mouse clicking on the *Target Computer* and selecting the **Create Drive** option. Once the drive is created you can drag and drop the files or folders as needed to create the correct directory structure.
- Create Folder** - This option brings up an input window. This window allows you to type in the directory name you wish to create. This option is always available.
- Delete** - This option will delete the directory or file you have right-mouse clicked on. This option is only available on directories or files under the Target Computer.



- **Rename** - This option will rename the directory or file you have right-mouse clicked on. This option is only available on directories or files under the Target Computer. You may place files in any Drive, Folder, or Macro Folder you create. You can rename any file or folder. The package editor will keep track of where the original files were found. No changes will be made to the path names or file names on the computer on which the package editor is running as you are building a representation of where the files will be installed when the package is deployed.
- **Backup files before replacing** - This option will create a backup of the files that you are adding to the package. With a backup enabled, when the agent downloads a file it will check to see if the file already exists on the machine. If it does exist the agent will first copy the original file to the backup location then replace the file with the new version from the package. Enter the backup directory path in the text box below the option or use the Browse button to search for the path.



Note: Be sure to delete all directories that you do not want installed when the package is deployed as the empty directories will be created on the target computer

Creating Scripts for a Package

The Create Scripts screen allows you to create scripts that will be run on the computer during the deployment process. A package can have up to three scripts, one of each type (Pre-Script, Command Line, and Post-Script). Scripts are executed in the follow sequence:

1. **Pre-Script** - used to test for a condition of the machine, shutdown a service, etc. For example; you can stop the package rollout in the pre-script by using the SetReturnCode in the PLCCAgent script object. Pre-Scripts can take the form of VBScript or JScript.
2. **Command Line** - 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, delete files, start services, run a installer, etc. Post-Scripts can take the form of VBScript or JScript.

Using the Script Editor

- **Script Type** - Select the type of script you would like to execute from the Type of Script dropdown box.
- **Script Language** - Select scripting type from the Script Language dropdown box.
- **Script Execution Directory** - Select Script Execution Directory if you want your script to run somewhere other than the initial location. Enter the backup directory path in the text box below the option or use the Browse button to search for the path.
- **Edit Script** - Click the Edit button. This will display the Script Editor dialog.

Working with License Agreements

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 is not normally used for packages that are in-house file distributions. It is primarily for packages containing items such as operating system service packs, device drivers, etc. The License URL will be displayed when viewing package information and will allow the user to link to the license information.

When scheduling a deployment of the package, the license page will be displayed, and the end user will be required to click the Accept button to complete scheduling the deployment.





4 Working With Deployments

A *Deployment* initiates the downloading of a particular patch by the agent on a device for installation on the target device. It is the instruction set around a *Package* that describes to the agent the rules and conditions for deploying the package.

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

In this Chapter

- “About Deployments” on page 69
- “Using the Deployment Pages” on page 74
- “Working with Deployments” on page 77
- “Using the Deployment Wizard” on page 84

About Deployments

As the mechanism of defining the operation of a deployment (as opposed to a patch which performs the operation), several key concepts and status indicators are associated to 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 based on a mandatory baseline.
- “Standard and Chained Deployments” - deployments are processed as either standard or chained.
- “Dirty State Deployments” - deployments which are processed when a device is in a *dirty state*.
- “Reboot Deployments” - deployments may initiate a system reboot.



Viewing Deployments

To View Deployments

- 1. Select the *Devices* tab, select your variables, 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.

Details by Device: \\TP_UPDATESERVER

Device Information

Vulnerabilities

Inventory

Deployments

Device Information:

Name: \\TP_UPDATESERVER

Operating System: Win2K3

OS Service Pack: Service Pack 1

DNS Name: TP_UpdateServer.techpubs.com

Description:

OS Version: 5.2

OS Build Number: 3790

IP Address: 10.12.20.113

Agent Information:

Agent Installation Date: 7/10/2006 5:29:37 PM (GMT-07:00)

Agent Status: Idle

Agent Version: 6.3.0.310

Last Connected Date: 7/10/2006 11:26:29 PM (GMT-07:00)

Group Information:

Group Name	Type	Status	Added By	Added On
Win2K3	Computer (system created)	Enabled	PatchLink Corp.	7/10/2006 5:29:00 PM (GMT-07:00)

Policy Information:

Communication Interval	Hours of Operation	Logging Level	Agent Listener Port	Agent Scan Mode
5 Minutes	Always On	None	off	Normal

Deployment Notification Defaults:

Deployment Notification Options

Cancelable: No

Snoozable: Yes

Deploy within: 5

Use Agent UTC Time: No

Reboot Notification Options

Cancelable: Yes

Snoozable: Yes

Reboot within: 5

Figure 4.1 Details by Device

- 3. Select the *Deployments* tab.
The *Deployments by Device* screen opens.

Deployments by Device: \\TP_UPDATESERVER

Information

Vulnerabilities

Inventory

Device Deployments

Total: 3

<input type="checkbox"/>	Name	Initial Start Date							
<input type="checkbox"/>	System Task: Reboot	Not Scheduled	0	0	1	0	0	0	0 %
<input type="checkbox"/>	System Task: Refresh Inventory Data	7/15/2006 5:28:40 PM (Local)	0	0	1	0	0	0	0 %
<input type="checkbox"/>	System Task: Discover Applicable Updates	7/11/2006 5:30:52 PM (Local)	1	0	1	0	0	0	0 %

Figure 4.2 Deployments by Device



4. Select the desired deployment
The *Deployment Details* screen opens



Deployment Details: System Task: Reboot						Auto Refresh: <input type="checkbox"/>
Devices and Groups Scheduled 9/1/2005 12:00:00 AM (Local)						Total: 1
<input type="checkbox"/>		Name	Status	Last Run Status	Last Run Start Date	Last Run Completed Date
<input type="checkbox"/>		\\TP_UPDATESERVER	Not Started			
						Next Run Date
						Not Scheduled

Figure 4.3 Deployment Details screen

Deployment Types

Deployments are created through either the *Vulnerabilities* or *Packages* page. 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 [Chapter 8](#), “*Mandatory Baselines*” for more information on the mandatory baseline feature.

Vulnerability-based Deployments

A vulnerability contains multiple associated packages and the target package to be deployed depends on the assigned devices. 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 is assigned a single operating system, only those devices running a common operating system are able to perform the deployment. Package-based deployments are the easiest to create, though they do not give you the granularity to tell the user which devices apply to the patch (or package).

Mandatory Baseline

A group contains a feature called the *Mandatory Baseline* that assists in defining a standard level of vulnerabilities or locally-created packages that must be installed on the group membership. The package 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 by the necessary package 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 a reboot, and the reboot is suppressed; the computer will enter a *dirty state “R”*, and not accept additional deployments until rebooted.

Chained Deployments

A *chained deployment* is a deployment which is chained with other deployments preventing the need for the computer to reboot between each deployment. Following the first chained deployment, the computer will enter a *dirty state “C”*, accepting only chained deployments until rebooted.



Note: If the deployment (standard or chained) requires a reboot, the deployment will not be considered complete until following the reboot.

Dirty State Deployments

Dirty State is the term given to a deployment where the computer did not perform the required reboot following that deployment. There are two different dirty states.

Table 4.1 Dirty State Definitions

Dirty State	Description
Dirty State R	Indicates that the computer received a standard deployment requiring a reboot, yet the reboot was suppressed. While in the R state, the agent will only accept one of the reboot deployments. A reboot deployment or a manual reboot will clear the dirty state.
Dirty State C	Indicates that the agent received a chained deployment in which the reboot was suppressed. While in the C state, the agent will only accept another chained deployment or a reboot deployment.



Reboot Deployments

There are two deployments which will always perform a reboot:

Table 4.2 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 Computers 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

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

Deployments by Device: \\TP_UPDATESERVER									
Information		Vulnerabilities	Inventory	Device Deployments				Total: 3	
<input type="checkbox"/>	Name	Initial Start Date							
	System Task: Reboot	Not Scheduled		0	0	1	0	0	0 %
	System Task: Refresh Inventory Data	7/15/2006 5:28:40 PM (Local)		0	0	1	0	0	0 %
	System Task: Discover Applicable Updates	7/11/2006 5:30:52 PM (Local)		1	0	1	0	0	0 %

Figure 4.4 Device Deployments page

Deployment Column Definitions

- **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 as follows:
 - **New** - A deployment that has been created since you logged on to your current session
 - **Existing** - A deployment that was created before you logged on to your current session
 - **Local** - A deployment is of a locally created package
 - **System Task** - A deployment that contains a system task package to perform various tasks. These deployments may include automated schedules in which the membership of the deployment may not be modified, though the schedule may
 - **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 4.3 Package Deployment Icons

New	Existing	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 4.3 Package Deployment Icons

New	Existing	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 - At least one device or device group failed to successfully completed the deployment
					Disabled - The deployment has been disabled

- **Deployment Name** - Deployment names typically include the vendor, application, and version information or a brief system task description
- **Deployment Initial Start Date** - The schedule date the deployment is to begin. For recurring deployments this is the first scheduled date of the deployment
- **Deployment Statistics** - The right-hand side of the vulnerability 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 4.4 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]

Deployment Details Summary

Expanding (by clicking the plus ‘+’ icon) a deployment will display the following deployment details:

- **Deployment Name** - The name of the deployment as assigned, by the user, when created
- **Type** - Options include: *Deployment of a package* or *Standard deployment*
- **Status** - Whether the deployment is *Enabled*, *Disabled*, or *Completed*
- **Deploy Manner** - The manner in which this deployment occurred. Options include: *Sequential*, *Parallel*, *First come first serve*, or *Distribute to # of computers at a time*.
- **Schedule Type** - Options include: *Recurring*, or *One time*
- **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



Working with Deployments

There are several tasks associated with vulnerabilities designed to assist you in managing and deploying vulnerabilities. These are available from commands located in the *Action* menu at the bottom on the Vulnerabilities page.

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

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 computers and groups and the status of the deployment for each.

Deployment Details: System Task: Reboot						Auto Refresh: <input type="checkbox"/>
Devices and Groups Scheduled 9/1/2005 12:00:00 AM (Local)						Total: 1
<input type="checkbox"/>	Name	Status	Last Run Status	Last Run Start Date	Last Run Completed Date	Next Run Date
<input type="checkbox"/>	\\WTP_UPDATESERVER	Not Started				Not Scheduled

Figure 4.5 Deployment Details

Table 4.5 Deployment Details Column Definitions

Column	Description
Device Status	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.
Refer to Appendix A, “Update Server Reference” for a complete definition of all available computer status icons.	



Table 4.5 Deployment Details Column Definitions

Column	Description
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
Refer to Appendix A, “Update Server Reference” for a complete definition of all available computer status icons.	

Deployment Details Page - Page Functions

Table 4.6 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.

Deployments by Device: \\TP_UPDATESERVER

Information		Vulnerabilities	Inventory	Device Deployments	Total: 3
Name	Initial Start Date				
System Task: Reboot	Not Scheduled	0	0	1	0 %
System Task: Refresh Inventory Data	7/15/2006 5:28:40 PM (Local)	0	0	1	0 %
System Task: Discover Applicable Updates	7/11/2006 5:30:52 PM (Local)	1	0	1	0 %

Figure 4.6 Deployments Page - Devices

Device Deployments Tab - Page Functions

Table 4.7 Device Deployments Tab - Page Functions

Button	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 *Device Groups* page. You can view deployments for device groups by clicking the group name on the *Device Groups* page. The *Deployments by Device Group* page opens.

Information		Vulnerabilities	Inventory	Membership	Mandatory	Group Deployments	Total: 1
Name	Initial Start Date						
Deployment of Adobe Acrobat Reader 6.0.1	ASAP	0	0	1	0	0 %	

User Abort Enable Disable Delete Edit Deploy Export

Figure 4.7 Deployments Page - Groups



Group Deployments Tab - Page Functions

Table 4.8 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 assignments For additional information refer to "Enabling Deployments"
Disable	Disables the selected enabled deployment assignments For additional information refer to "Disabling Deployments"
Delete	Removes the deployment from your ZENworks Patch Management Server For additional information refer to "Deleting Deployments"
Edit	Launches the deployment wizard allowing you to make modifications to the deployment For additional information refer to "Modifying 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 computer can be displayed by clicking on the status text (of the Last Run Status column) .

Deployment Results

Deployment Status for \\TECHPUBS-PLUS

Package Name: MS05-020 890923 (2K3) Cumulative Security Update for IE 6.0

Deployment Type: Computer Deployment

Associated Impact: Critical

Deployment Status: The deployment completed successfully.

Last Run Results:

Next Run Date:

Last Run Status: Success

Last Run Start Date: 4/28/2005 4:56:17 PM (GMT-08:00)

Last Run Completed Date: 4/28/2005 4:57:03 PM (GMT-08:00)

Figure 4.8 Last Run Status



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

Table 4.9 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 computer performed the deployment.
Next Run Date	Displays the date when the computer is to perform the deployment again, if the deployment is recurring.
Last Run Status	Displays the status of the last time the computer performed the deployment.
Last Run Start Date	Displays the date when the computer last started the deployment.
Last Run Completed Date	Displays the date when the computer 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. Refresh Inventory Data (RID)
6. 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.



Note: If multiple chained deployments are scheduled and some have the final reboot suppressed, while others do not, the determination of whether a final reboot occurs is based upon the last scheduled deployment.

Aborting Deployments

Aborting a deployment will cancel the deployment for any devices which have not already received the deployment package(s).



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



Note: You cannot abort deployments of System Task Packages.

2. Click **Abort** (at the bottom of the page)
This will cancel (delete) the selected deployment

Disabling Deployments

Disabling a deployment will pause the deployment and stop the distribution of the package(s) to devices.



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 paused.

To Disable a Deployment

1. Select the deployment you need to disable



Note: You cannot allowed to 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 computers, so removing a computer from a deployment of a System Task Package will have no effect (the computer 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 computers 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 computer selection, scheduling the deployment, and if needed, setting recurrences.

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



Note: Using the Deployment wizard, you can select multiple vulnerabilities, and the wizard will automatically select all of the devices and packages required and if Devices are selected, the wizard will automatically select all vulnerabilities.

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 you need to deploy to.

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.

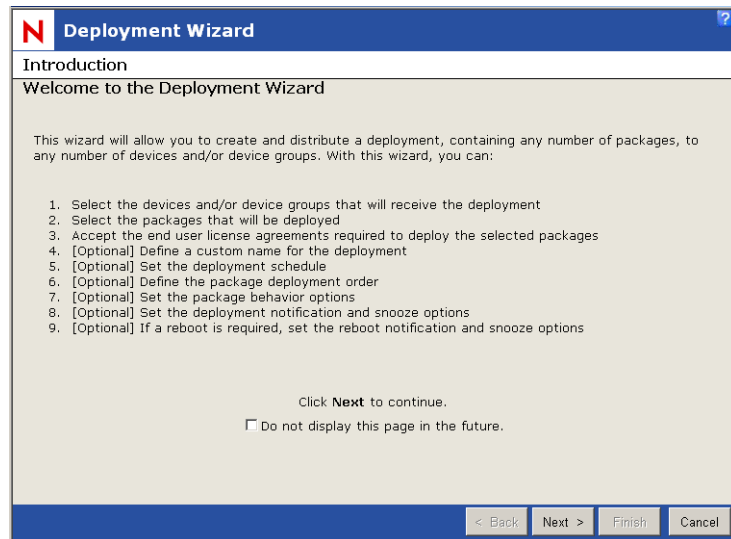


Figure 4.9 Deployment Wizard - Introduction Page

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

Click **Cancel** to abort the wizard.



Device/Device Groups Selection Page

The *Device/Device Groups Selection* page of the **Deployment Wizard** allows you to select one or more devices and/or device groups to receive this deployment.

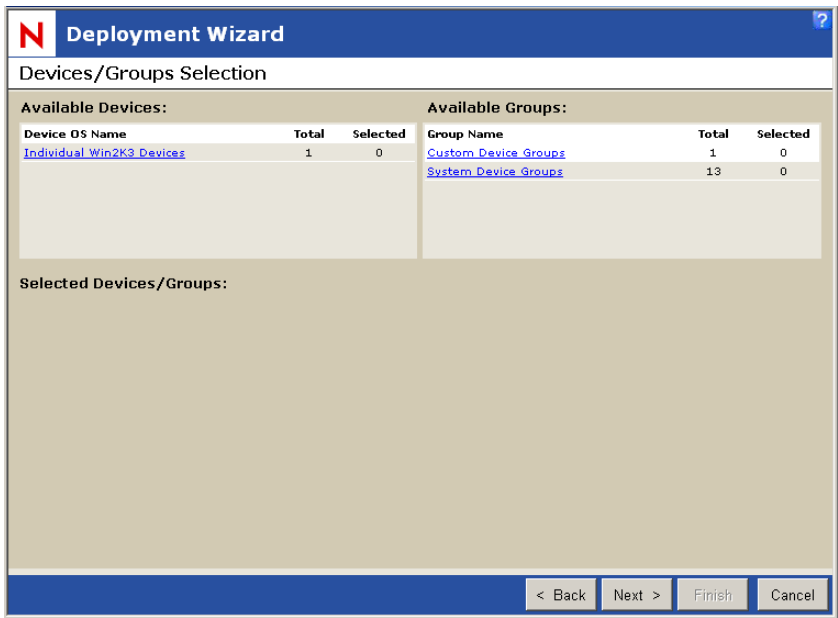


Figure 4.10 Deployment Wizard - Devices/Device Groups Selection Page

When first opened, this page displays the individual devices, grouped by operating system, and the device groups grouped by whether they are user groups or system groups.

To Select Individual Devices

- 1. Click the appropriate operating system link
- 2. For each device to be included in the deployment, select its associated checkbox

To Select a Group of Devices

- 1. Click the appropriate device group link
- 2. For each group to be included in the deployment, select its associated checkbox



Note: If a device, group of devices, and/or vulnerability was selected prior to opening the deployment wizard, those devices (or group) will be selected here by default. However, it may be necessary to expand the groupings to see the selected devices.

Deployment Wizard

Devices/Groups Selection

Available Devices:

Device OS Name	Total	Selected
Individual Win2K3 Devices	1	1

Available Groups:

Group Name	Total	Selected
Custom Device Groups	1	0
System Device Groups	13	0

Selected Devices/Groups:

<input checked="" type="checkbox"/> Device Name	Status	Platform Info	DNS Name	IP Address
<input checked="" type="checkbox"/> \\MATS01-PLUS2	Idle	Microsoft Windows Server 2003, Enterprise Edition-Service Pack 1	MATS01-PLUS2	10.12.11.67

Navigation: < Back Next > Finish Cancel

Figure 4.11 Deployment Wizard - Device/Device Groups Selection Page

When a device group is selected for deployment; only the devices in the group when the ZENworks Patch Management Server reaches the deployment's defined start time will be included in the deployment. Devices added to the group (either manually or dynamically) after the deployment begins will not be included.



Tip: If you have a large number of disabled devices within your group and only want to deploy to the enabled ones, select **Filter by status** and *manually select* the devices to be deployed.

Click **Back** to return to the previous page.

Click **Next** to proceed to the *Packages Selection* page.

Click **Cancel** to abort the wizard.



Package Selection Page

The *Packages Selection* page of the **Deployment Wizard** allows you to select the packages to be deployed.

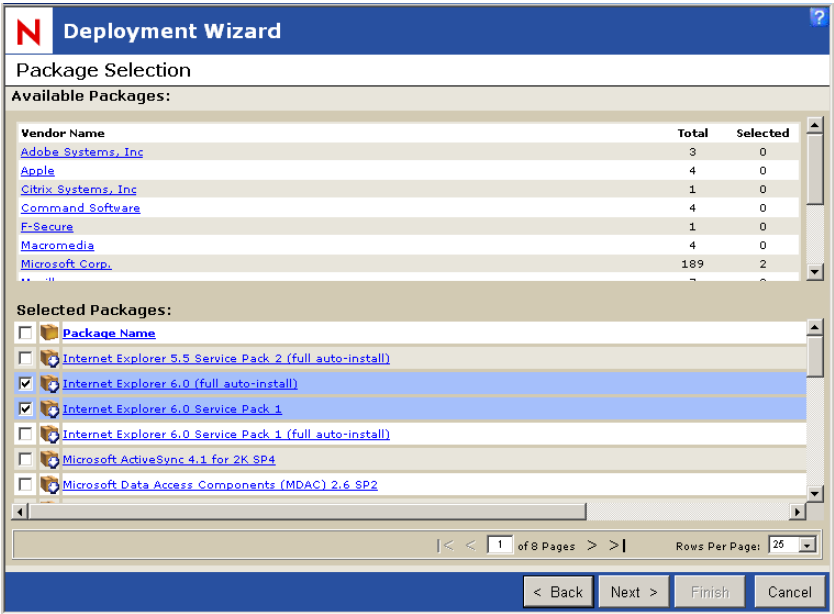


Figure 4.12 Deployment Wizard - Packages Selection Page

When opened this page displays the packages, grouped by manufacturer, that apply to the devices selected on the *Devices/Device Groups Selection* page. To view and select the individual packages or entire grouping, you must click the group **Name** link.



Note: If a package, group of packages, or vulnerability was selected prior to opening the deployment wizard, those packages will be selected here by default. However, it may be necessary to expand the groupings to see the selected packages.

Deployment Wizard

Package Selection

Available Packages:

Vendor Name	Total	Selected
Adobe Systems, Inc	5	2
Apple	5	0
Citrix Systems, Inc	1	0
Command Software	4	0
E-Secure	1	0
Macromedia	4	0
Microsoft Corp.	152	0

Selected Packages:

<input type="checkbox"/> Package Name	Status	Impact	Platforms	CVE list
<input type="checkbox"/> Adobe Acrobat Reader 6.0	Not Cached	Software		
<input type="checkbox"/> Adobe Acrobat Reader 6.0.1	Not Cached	Software		
<input type="checkbox"/> Adobe Acrobat Reader 7.0.5	Not Cached	Software		CVE-2005-2470
<input checked="" type="checkbox"/> Adobe Acrobat Reader 7.0.7	Not Cached	Software		
<input checked="" type="checkbox"/> Adobe Acrobat Reader 7.0.8	Not Cached	Software		

Navigation: < Back Next > Finish Cancel

Page: 1 of 1 Pages Rows Per Page: 25

Figure 4.13 Deployment Wizard - Packages Selection Page

To Select a Package

1. Select the **Package** or **Packages**.
2. Click the **arrows** to page through the available packages.
3. Click the **Package Name** link to open the *Associated Vulnerability Analysis* page.

To limit the number of packages displayed on each page, change the value in the **Display __ Packages per page** field.



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*.

Click **Back** to return to the previous page.

Click **Next** to proceed to the *Licenses* page.

Click **Cancel** to abort the wizard.



Associated Vulnerability Analysis Page

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



Figure 4.14 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 computers patch status.

To limit the number of computers displayed on each page, change the value in the **Display __ Results per page** field.

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



Licenses Page

The *Licenses* page of the Deployment Wizard is where any licensing information associated with the selected packages will be displayed. Any license agreements displayed here must be agreed to prior to your continuing the deployment.

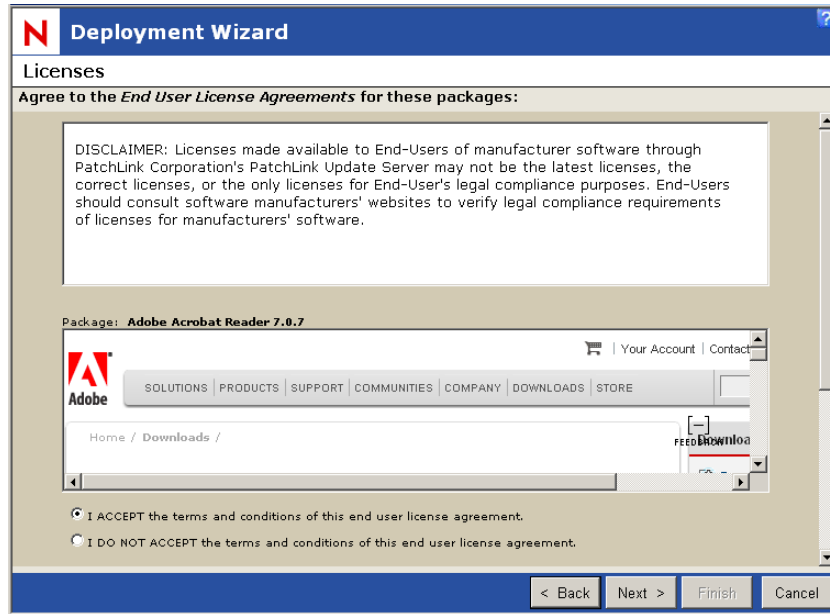


Figure 4.15 Deployment Wizard - Licenses Page

If you accept the terms and conditions, select the **I ACCEPT the terms and conditions of this end user license agreement** option for ***EACH*** license agreement



Note: You must accept ***ALL*** of the license agreements individually before you will be able to continue with a deployment. If the **target device** has stricter browser security settings, you will get multiple prompts while running the deployment wizard.

Click **Back** to return to the previous page.

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

Click **Cancel** to abort the wizard.



Deployment Options Page

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

Figure 4.16 Deployment Wizard - Deployment Options Page

- **Deployment Name Prefix** - The display name of the deployment. The *{Package Name}* variable will be replaced with the Package Name. Allowing you to enter custom text before or after the package name.
By removing the *{Package Name}* variable, you can leave the package name out of the notification.
- **Start Time** - Click the **Change** button to open the *Schedule Configuration* page of the Deployment Wizard. From this page you can select either a **One time** or **Recurring** deployment and set the appropriate options for each.
- **One time deployment starting at:**
 - **Agent Local Time** - The Agent Local time will vary depending on the time zone of your location (daylight savings time may apply).
 - **Agent UTC Time** - *Coordinated Universal Time (UTC)*, also known as *World Time*, *Z Time*, or *Zulu Time* is a standardized measurement of time that is not dependent upon the local time zone. When UTC is used, the deployment will be scheduled for all agents at the same time, regardless of time zone differences.
- **Manner**
 - **Concurrent** - limits the simultaneous distribution of the deployment to only the specified number of computers at one time. The order of distribution is based upon a first-come first-serve basis, and new deployments are distributed as agents report back as having completed the 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 (the *Concurrent Deployment Limit* setting on the *Configuration* page) will always take precedence over the distribution options defined here.
- **Suspend the deployment of this package, if it fails to deploy to one or more computers** - Selection of this checkbox will suspend all subsequent deployments following any deployment failure.
- **Deploy package even if computer has been previously patched** - This option will deploy the package to all selected computers regardless of their patch status.
- **Notes** - This is a simple notes field, allowing you to enter any desired notes such as the expected deployment results, etc.



Note: Although the agent's local time is selected, a group deployment will never occur prior to the Patch Management Server reaching the scheduled time. Therefore, in the case where an agent's time zone is prior to the Patch Management Server's time zone, the local time of the Patch Management Server not the agents will be used. This is due to the fact that the Patch Management Server does not create the individual deployments prior to the scheduled distribution time, allowing group members to be added or removed from the deployment up to the time of distribution.

Note: Even when using UTC, the exact time when the agent retrieves the deployment is dependent upon the agent's communication interval and if the agent's (and Patch Management Server) time and time zone settings are correct.

Click **Back** to return to the previous page.

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

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

Click **Cancel** to abort the wizard.

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.



- **One Time** - One time (as the default selection) will start the deployments 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.

Deployment Wizard

Schedule Configuration

Set the deployment schedule:

☒ One time On 11/16/2004 5:23:09 PM
☐ Recurring

Date: November 2004

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

☒ 12 hour ☐ 24 hour

Time:
Hour: 5 Minute: 23 PM

Save Cancel

Figure 4.17 Deployment Wizard - Schedule Configuration Page

- **12 hour** or **24 hour** option - allows you to set the schedule to either a standard 12 hour format or a military 24 hour format.
- **Hour** - select a starting hour between 1 and 12 (1 and 24 if 24 hour format)
- **Minute** - Select a minute between 00 and 59
- **AM/PM** - Select AM or PM designation



- **Recurring** - 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 1 day(s)

Daily Frequency:

☒ 12 hour ☐ 24 hour
☒ Occurs once at: Hour: 5 Minute: 23 PM
☐ Occurs every: 1 Minute(s)
 starting at: Hour: 12 Minute: 00 AM
 ending at: Hour: 11 Minute: 59 PM

Duration:

Start Date: End Date:

< November 2004 > < November 2004 >
 Su Mo Tu We Th Fr Sa Su Mo Tu We Th Fr Sa
 31 1 2 3 4 5 6 31 1 2 3 4 5 6
 7 8 9 10 11 12 13 7 8 9 10 11 12 13
 14 15 16 17 18 19 20 14 15 16 17 18 19 20
 21 22 23 24 25 26 27 21 22 23 24 25 26 27
 28 29 30 1 2 3 4 28 29 30 1 2 3 4
 5 6 7 8 9 10 11 5 6 7 8 9 10 11

☒ No End Date

Figure 4.18 Deployment Wizard - Schedule Configuration Page

■ Daily Deployment Options

Occurs:

☒ Daily
☐ Weekly
☐ Monthly

Daily:

Every 1 day(s)

Figure 4.19

- **Every X day(s)** - Allows the deployment to be scheduled every X days. The valid options are: 1 through 366



■ Weekly Deployment Options

Occurs:
☐ Daily
☒ Weekly
☐ Monthly

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

Figure 4.20

- **Every X week(s) on: Mon, Tue, Wed, Thur, Fri, Sat, Sun** - Allows the deployment to be scheduled every X weeks on the selected days.
- Monthly Deployment Options

Occurs:
☐ Daily
☐ Weekly
☒ Monthly

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

Figure 4.21 Schedule Configuration Page - Monthly Options

- **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.



■ Common Deployment Options

Daily Frequency:

☒ 12 hour ☐ 24 hour

☒ Occurs once at: Hour: 5 Minute: 23 PM

☐ Occurs every: 1 Minute(s)

Starting at: Hour: 12 Minute: 00 AM

Ending at: Hour: 11 Minute: 59 PM

Duration:

Start Date: End Date:

< November 2004 > < November 2004 >

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

☒ No End Date

Figure 4.22 Schedule Configuration Page - Common Deployment Options

- **12 hour** or **24 hour** option - allows you to set the schedule to either a standard 12 hour format or a military 24 hour format.
- **Occurs once at** - allows the deployment to occur once daily at the time defined here.
- **Occurs every** - allows 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** - defaults to the current date. Allows schedule a recurring deployment to begin at a later date.
- **No End Date** - if selected, deployment will continue with the defined recurrence schedule and no defined end date.
- **End Date** - if the No End Date checkbox is deselected, the date defined here will be the date after which this deployment will no longer be deployed.

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

Click **Cancel** to abort 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.

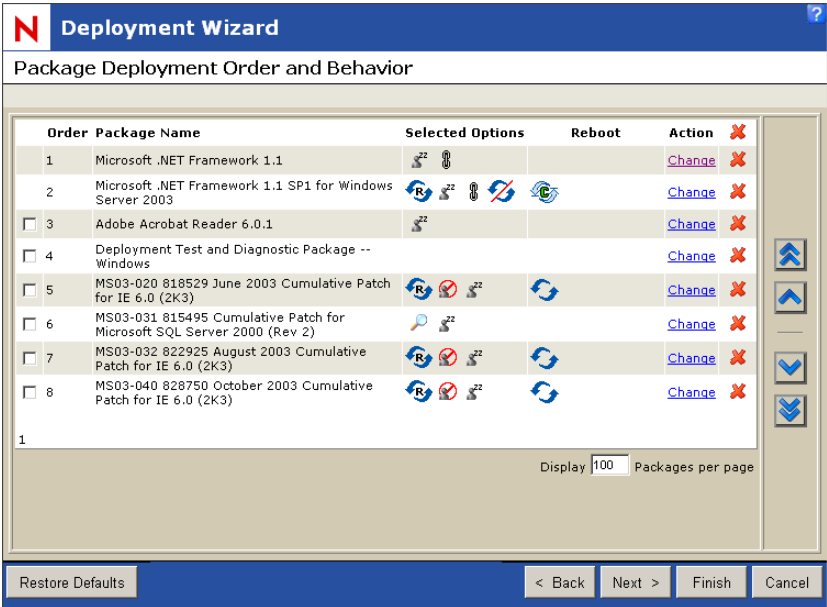


Figure 4.23 Deployment Wizard - Package Deployment Order and Behavior Page

- **Action Column**
 - **Edit** - Click the **Edit** icon, to open the *Package Deployment Behavior Options* page and change the behavior options for that package.
 - **Delete** - Click the **Delete** icon to remove the package from the deployment.
- **Selected Options Column** - Graphically displays the behavior of each package (as defined on the “*Package Deployment Behavior Options Page*”) using the following behavior icons

Table 4.10 Behavior Icon Definitions

	Uninstall - instead of an installation, this option will uninstall the packages.
	Force Shutdown - forces all applications to close if the package causes a reboot.
	Do Not Backup - will not backup files for uninstall



Table 4.10 Behavior Icon Definitions





















	Suppress Reboot - prevents the computer from rebooting after installation of the package.
	Quiet Mode - sets the installer to function in quiet mode. Quiet mode suppresses any user interfaces (in the event a user is logged in) during the deployment.
	Unattended Setup - uses the packages unattended setup mode.
	List Hot Fixes - returns a listing of the hot fixes installed on the target computers.
	Force Reboot - forces the computer to reboot regardless of package requirements.
	Reboot is Required - indicates that this package requires a reboot prior to completing the installation.
	Chain Packages - sets the package as chainable (package must support chaining).
	Suppress Chained Reboot - suppress the reboot, allowing other chained packages to be sent following this package. Tip: It is recommended that you suppress the final reboot for all chained packages, then send a reboot deployment when all packages are finished.
	Repair File Permissions - following the package installation, file permissions will be repaired.
	Download Only - distributes the package without running the package installation script.
	Suppress Notification - suppresses any user notifications during installation.
	Debug Mode - runs the package installation in debug mode.
	Do Not Repair Permissions - suppresses the repair of file name permissions after the reboot.
	May Reboot - allows the package to force a reboot if required.



Table 4.10 Behavior Icon Definitions

	Multi-User Mode - performs the installation in 'Multi-User' mode.
	Single-User Mode - performs the installation in 'Single-User' mode.
	Restart Service - restarts the service following the deployment.
	Do Not Restart Service - does not restart the service following the deployment.
	Reconfigure - performs the system reconfigure task following the deployment.
	Do Not Reconfigure - does not perform the system reconfigure task following the deployment.



Note: When deploying chained deployments reboots are suppressed, whenever possible, including the final (chained) deployment. That final deployment will be represented as *May Reboot* because the Patch Management Server will perform a check to determine if the agent is in a *dirty state*, and if so, send a *System Task - Reboot* deployment, prior to deploying the remaining packages.

- **Reboot Column** - The reboot column graphically displays the reboot settings of each package (as defined on the “[Package Deployment Behavior Options Page](#)”) using the following icons

Table 4.11 Reboot Icon Definitions






	Reboot may occur - following the installation of this package, the computer may be rebooted, dependent upon the package installer requirements (at the time of install).
	Reboot may occur dirty - following the installation of this package, the computer may be rebooted, dependent upon the package requirements. However if a reboot is required and the computer is not rebooted, the computer will enter a dirty state.
	Reboot required (Dirty State) - following the installation of this package, no other (chainable or non-chainable) packages will be installed until the computer reboots







Table 4.11 Reboot Icon Definitions

	Reboot required chain - following the installation of this package, only chainable packages will continue to be installed until the computer has been rebooted.
	Reboot will occur - the computer will be rebooted following the package installation

To move a package first select its corresponding checkbox then select a move button as defined below.

Table 4.12 Button Definitions

	Click this button to move the package to the top of all non-chained deployments (this will place it immediately after the chained deployments).
	Click this button to move the package up one.
	Click this button to move the package down one.
	Click this button to move the package to the bottom of the listing.



Note: Chained packages cannot be moved without first removing their chained status.

- **Restore Defaults** - Click the **Restore Defaults** button to restore the package order and behavior back to their default settings.

Click **Back** to return to the previous page.

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

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

Click **Cancel** to abort the wizard.




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.

Deployment Wizard

Package Deployment Behavior Options

Behavior Options for MS04-038 834707 Cumulative Security Update for IE 6.0 SP1-a

Behavior	Description
 <input type="checkbox"/> Uninstall	Uninstall the package.
 <input type="checkbox"/> ForceShutdown	If the package triggers a reboot, close all open applications.
 <input type="checkbox"/> NoBackUp	Do not create backup files for uninstall.
 <input checked="" type="checkbox"/> SuppressReboot	Do not reboot after package installation.
 <input checked="" type="checkbox"/> QuietMode	Use 'quiet mode' (no user interaction required).
 <input checked="" type="checkbox"/> UnattendedSetup	Perform an unattended setup.
 <input type="checkbox"/> ListHotFixes	Generate a list of installed hot fixes.
 <input type="checkbox"/> ForceReboot	Force a reboot after package installation.
 <input checked="" type="checkbox"/> RebootIsRequired	A reboot is required to complete package installation.
 <input checked="" type="checkbox"/> Chainable	This package is chainable; therefore Q-Chain will run following the installation of this package (windows only).
 <input type="checkbox"/> SuppressChainReboot	Following the installation of the chainable deployments; Do Not reboot. Note: A reboot is required before any non-chained deployments will be deployed.
 <input type="checkbox"/> RepairPermissions	Following the installation, repair the file permissions.
 <input type="checkbox"/> DeployOnly	Download only, do not install the package.
 <input type="checkbox"/> NoPopUp	Do not display pop-up messages during installation.
 <input type="checkbox"/> Debug	Run the installation in 'debug mode'.
 <input type="checkbox"/> SuppressRepair	Do not repair file permissions after package installation.
 <input type="checkbox"/> RebootMayOccur	To complete installation, a reboot may occur.

Optional Flags: -2

Display:
☒ Notes
☐ Description

This deployment will Do not reboot after package installation., Use 'quiet mode' (no user interaction required)., Perform an unattended setup., This package is chainable; therefore Q-Chain will run following the installation of this package (windows only).. **This installation requires a reboot in order to complete.**

SaveCancel

Figure 4.24 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.

- **Behavior Options** - The following table defines the available behavior options and their associated icons.



Table 4.13 Behavior Icon Definitions














	Uninstall - instead of an installation, this option will uninstall the packages.
	Force Shutdown - forces all applications to close if the package causes a reboot.
	Do Not Backup - will not backup files for uninstall
	Suppress Reboot - prevents the computer from rebooting after installation of the package.
	Quiet Mode - sets the installer to function in quiet mode. Quiet mode suppresses any user interfaces (in the event a user is logged in) during the deployment.
	Unattended Setup - uses the packages unattended setup mode.
	List Hot Fixes - returns a listing of the hot fixes installed on the target computers.
	Force Reboot - forces the computer to reboot regardless of package requirements.
	Reboot is Required - indicates that this package requires a reboot prior to completing the installation.
	Chain Packages - sets the package as chainable (package must support chaining).
	<p>Suppress Chained Reboot - suppress the reboot, allowing other chained packages to be sent following this package.</p> <p>Tip: It is recommended that you suppress the final reboot for all chained packages, then send a reboot deployment when all packages are finished.</p>
	Repair File Permissions - following the package installation, file permissions will be repaired.
	Download Only - distributes the package without running the package installation script.



Table 4.13 Behavior Icon Definitions

	Suppress Notification - suppresses any user notifications during installation.
	Debug Mode - runs the package installation in debug mode.
	Do Not Repair Permissions - suppresses the repair of file name permissions after the reboot.
	May Reboot - allows the package to force a reboot if required.
	Multi-User Mode - performs the installation in 'Multi-User' mode.
	Single-User Mode - performs the installation in 'Single-User' mode.
	Restart Service - restarts the service following the deployment.
	Do Not Restart Service - does not restart the service following the deployment.
	Reconfigure - performs the system reconfigure task following the deployment.
	Do Not Reconfigure - does not perform the system reconfigure task following the deployment.

- **Optional Flags** - Provides an area for the entry of any extra flags. Generally the flags entered here are unique to a particular deployment or special scenario. In addition to flags specific to the package being deployed, the following Novell flags are available:



The following table defines the flag behavior and their descriptions:

Table 4.14 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 qchain 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

- **Notes** - Displays the expected deployment behavior.
- **Description** - Displays the package description



- **Do not notify users of this deployment** - When selected, 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** - If selected, the user will be notified prior to the installation of this deployment. The user message and available options will be as defined here.
 - **Message** - This field contains the message the user will see when notified about this deployment. The `{%Package_Name%}` variable will be replaced with the Package Name, allowing you to enter custom text before or after the package name.



Note: By removing the `{%Package_Name%}` variable, you can leave the package name out of the notification.

- **Deployment Options** - When defining deployment options you can specify, for each option, whether to use the values defined in the *Agent Policy* (by selecting the **Use Agent Policy** checkbox) or the custom setting defined here
 - **Agent Time** - Informational only.
Displays the value of **UTC** or **Local** dependent upon the **Start Time** option selected (on the *Deployment Options* page)
 - **Allow User to Cancel** - Defines whether the user has the ability to cancel the deployment
 - **Allow User to Snooze** - Defines whether the user can snooze the deployment
 - **Notification on Top** - Defines whether the Novell Desktop Deployment Manager (PDDM) will be displayed on top of all other applications
 - **Deadline Offset** - Allows you to set a custom deadline offset, or custom deadline date for this deployment
 - ◆ **From Deployment Start** - Sets the deployment deadline to be *X* Minutes, Hours, or Days from deployment start date/time
 - ◆ **Specific Date** - Allows you to set the deployment deadline to a specific date and time

Reboot Notification Options

- **Use Policies** - When selected 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** - When selected, there will be no user notification prior to rebooting the computer.
 - **Notify users of the reboot** - If selected, 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.



Note: By removing the `{%Package_Name%}` variable, you can leave the package name out of the notification.

- **Reboot Options** - When defining reboot options you can specify, for each option, whether to use the values defined in the *Agent Policy* (by selecting the **Use Agent Policy** checkbox) or the custom setting defined here
 - **Allow User to Cancel** - Defines whether the user has the ability to cancel the reboot
 - **Allow User to Snooze** - Defines whether the user can snooze the reboot
 - **Reboot Delay Offset** - Allows you to set a custom reboot delay (in *Minutes*, *Hours*, or *Days*) for this deployment

Click **Back** to return to the previous page.

Click **Next** to proceed to the *Deployment Confirmation* page.

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

Click **Cancel** to abort the wizard.



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

Deployment Name Prefix: Deploying {Package Name}

Schedule: One time deployment, starting on 9/20/2005 4:49:19 PM based on Agent UTC Time.

Manner: Sequential: Deploying to 10 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: 76

Total Selected Devices/Groups: 1

Notes: Created by patchlink on 9/20/2005 4:49:19 PM

Selected Packages

Order	Package Name	Selected Options	Reboot	Devices
1	Microsoft .NET Framework 1.0	⚙️		1
2	Microsoft .NET Framework 1.1	⚙️		1
3	Microsoft .NET Framework 1.1 SP1 for Windows Server 2003	⚙️		1
4	MS 831464 IIS 6.0 Compression Corruption Causes Access Violations	⚙️		1
5	MS 870669 Disable the ADOB.Stream object from Internet Explorer-a (SEE NOTES)	⚙️		1
6	MS 898060 (2K3 SP1) Network connectivity failure between clients and servers	⚙️		1
7	MS02-008 317244 XMLHTTP Control Allows Local Access for MSXML 4.0-a	⚙️		1

< Back Next > Finish Close

Figure 4.26 Deployment Confirmation Page

- **Summary section**
 - **Deployment Name Prefix** - The name given the deployments (as defined under the *Deployment Options* page)
 - **Schedule** - The schedule for the deployments (as defined under the *Deployment Options* page)
 - **Manner** - Whether these deployments are Sequential or Parallel (as defined under the *Deployment Options* page), and if Sequential, how many deployments will be distributed at once
 - **Deployment Notification** - Whether or not the users will received a deployment notification (as defined under the *Notification Options* page)
 - **Reboot Notification** - If the deployments must reboot, whether or not the users will receive a reboot notification (as defined under the *Notification Options* page)
 - **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 computers, the total number of computers selected
 - **Notes** - When the deployments were created, and who created them



- **Selected Packages** section - Displays the deployment order, package name, deployment options, reboot status, and the number of applicable computers for the package, in a grid format
 - **Order** column - Displays the order in which the packages will be deployed
 - **Package Name** column - Displays the name of each package that will be deployed



Note: Click the Package Name link to open the *Package Applicability* page.

- **Selected Options** column - Graphically displays the behavior of each package, (as defined on the *Package Deployment Behavior Options* page) using the behavior icons
- **Reboot Column** - Graphically displays the reboot settings of each package, (as defined on the *Package Deployment Behavior Options* page) using the reboot icons.
- **Computers Column** - Graphically displays the number of (selected) computers that are applicable to each package.

Click **Back** to return to the previous page.

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

Click **Cancel** to abort the wizard.



Package Applicability Page

The *Package Applicability* page of the Deployment Wizard allows you to view the computers associated with this package, and whether they are applicable to the selected packaged.

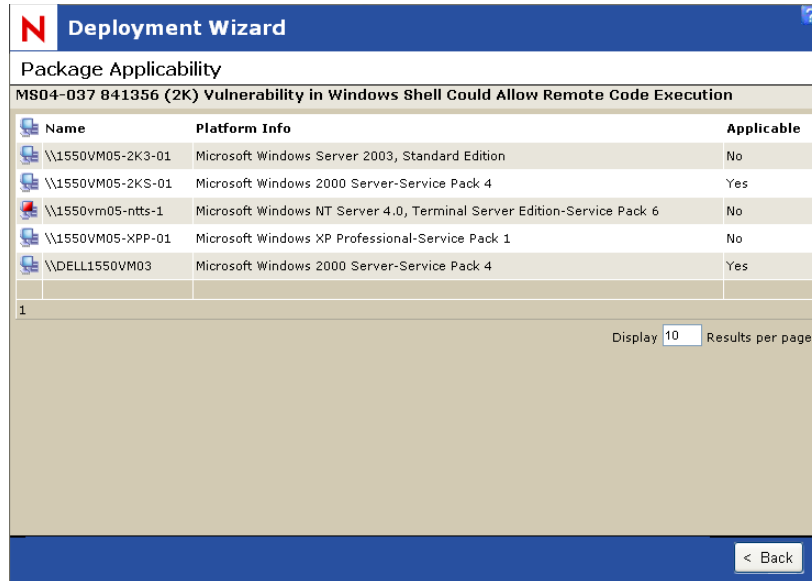


Figure 4.27 Deployment Wizard - Package Applicability Page

The **Applicable** column will display either *Applicable* or *N/A* dependent upon whether the selected package applies to that particular computer.

To limit the results displayed on each page, change the value in the **Display __ Results per page** field.

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.

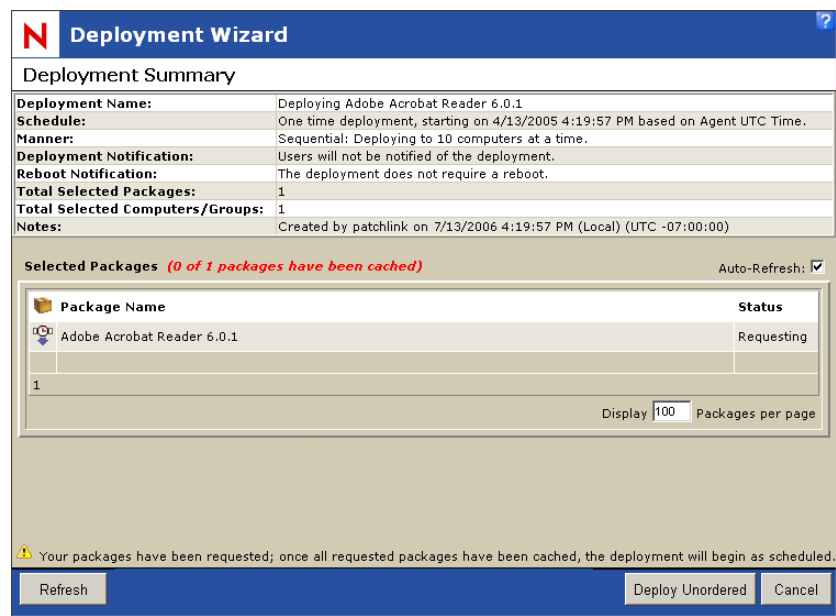


Figure 4.28 Deployment Wizard - Deployment Summary Page

- **Summary Section**
 - **Deployment Name** - The name given the deployments (as defined under the *Deployment Options Page*)
 - **Schedule** - The schedule for the deployments (as defined under the *Deployment Options Page*)
 - **Manner** - Whether these deployments are Sequential or Parallel (as defined under the *Deployment Options Page*), and if Sequential, how many deployments will be distributed at once
 - **Deployment Notification** - Whether or not the users will received a deployment notification (as defined under the *Notification Options Page*)
 - **Reboot Notification** - If the deployments must reboot, whether or not the users will receive a reboot notification (as defined under the *Notification Options Page*)
 - **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 computers, the total number of computers 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
 - **Package Name Column** - Displays the name of each package that will be deployed
 - **Status Column** - Displays whether the package is already cached or currently downloading (Requesting)

If one or more of the selected packages have not been cached the Deploy Unordered and Cancel buttons will be available

- **Deploy Unordered** - Creates the applicable deployments, deploying the packages in the order which they cache, rather than the order defined within the deployment wizard
- **Cancel** - Cancels all of the deployments

Click **Close** to exit the wizard



Note: The deployments created have been individually added to the appropriate deployment pages of the selected groups and/or computers. After closing this wizard page, there is no function that will redisplay **just** the deployments created during this wizard session.

Changing Deployments

The **Change** button, on either the *Computer Deployments* or *Group Deployments* page, launches the Deployment Wizard with the selected deployment's details pre-populated in the wizard. The function of the wizard is the same as when the deployment was created.



Note: **Change** only modifies the deployment for the selected package and its associated computers. Although when you created the deployment using the Deployment Wizard, you were able to select multiple computers and multiple packages, **Change** only supports multiple computers. To modify the deployments for other packages, those deployments must be selected individually.





5 Using Devices

The *Devices* page is where the Patch Management Server administrator organizes the protected devices. 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.

In this Chapter

- “About Devices” on page 115
- “Working with Devices” on page 124

About Devices

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

- Status
- Platform
- Operating system information
- Version
- Group association

Novell. ZENworks.						
Home Vulnerabilities Inventory Devices Groups Users Reports Options Help						
Server Date and Time: 9/22/2006 5:54:14 PM (GMT-07:00)						
About Log Out						
Devices						
Search (device name):		Status: Enabled				
Groups: --- All ---						
Show results on Page Load: <input type="checkbox"/>		Save as Default View: <input type="checkbox"/>		Update View		
Total: 1						
Device Name	IP Address	Status	OS Info	Version	Group List	
\\TP-NOVELL	10.19.2.158	Idle	Microsoft Windows Server 2003, Standard Edition-Service Pack 1	6.3.2.611	Win2K3	

Figure 5.1 Devices Page



Viewing Devices

To View Devices

- 1. Select the *Devices* tab, select your filter options, and click **Update View**.

Using the Devices Page

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


Devices							Total: 1
<input type="checkbox"/>		Device Name	IP Address	Status	OS Info	Version	Group List
<input type="checkbox"/>		\\TP_EMERALD	10.12.20.113	Idle	Microsoft Windows Server 2003, Standard Edition-Service Pack 1	6.3.0.160	Win2K3

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. The same data as indicated by the "Device Status Icons".
OS Info	Additional information about the operating system the device is running
Version	The version number of the agent installed on the device
Group List	The groups that the device is a member. Displayed devices can be filtered according to group membership in the search section.

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 the available device (agent) statuses and their associated icons.

Table 5.2 Device Status Icons





















Status	Description
	The agent is idle (this is a valid agent without any current or pending deployments)
	The agent is idle and has pending deployments
	The agent is currently working on a deployment (animated icon)
	The agent is offline
	The agent is offline and has pending deployments
	The agent is sleeping due to its Hours of Operation settings
	The agent is sleeping due to its Hours of Operation settings and has pending deployments
	This agent has been disabled
	This agent has been disabled, and has pending deployments
	The agent is offline and is in a QChain status (can accept chained deployments only after reboot)
	The agent is offline, is in a QChain status (can accept chained deployments only after reboot), and it has pending deployments
	The agent is offline and is in a 'Dirty R' status (can accept no more deployments until after it reboots)
	The agent is offline, is in a 'Dirty R' status (can accept no more deployments until after it reboots), and it has pending deployments
	The agent is in a QChain status (the agent can accept chained deployments only until after a reboot)
	The agent is in a QChain status (the agent can accept chained deployments only until after a reboot) and it has pending deployments



Table 5.2 Device Status Icons

Status	Description
	The agent is in a 'Dirty R' status (the agent can accept no more deployments until after it reboots)
	The agent is in a 'Dirty R' status (the agent can accept no more deployments until after it reboots) and it has pending deployments
	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 QChain status (can accept chained deployments only until after a reboot) and it has pending deployments and is sleeping due to its Hours of Operation settings.
	The agent is in a 'Dirty R' status (the agent can accept no more deployments until after it reboots) and is sleeping due to its Hours of Operation settings.
	The agent is in a 'Dirty R' status (can accept no more deployments until after it reboots) and it has pending deployments and is sleeping due to its Hours of Operation settings.



Using the Device Details 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.

Details by Device: \\TP-AGENT-02

Device Information | Vulnerabilities | Inventory | Deployments

Device Information:

Name: \\TP-AGENT-02	Description:
Operating System: WinXP	OS Version: 5.1
OS Service Pack: Service Pack 2	OS Build Number: 2600
DNS Name: TP-AGENT-02	IP Address: 10.19.2.157

Agent Information:

Agent Installation Date: 9/12/2006 8:54:53 PM (GMT-07:00)	Agent Status: Idle
Agent Version: 6.3.0.563	Last Connected Date: 9/13/2006 12:29:28 AM (GMT-07:00)

Group Information:

Group Name	Type	Status	Added By	Added On
WinXP	Computer (system created)	Enabled	PatchLink Corp.	9/12/2006 8:54:00 PM (GMT-07:00)

Policy Information:

Communication Interval	Hours of Operation	Logging Level	Agent Listener Port	Agent Scan Mode
15 Minutes	Always On	None	off	Normal

Deployment Notification Defaults:

Deployment Notification Options	Reboot Notification Options
Cancelable: No	Cancelable: Yes
Snoozable: Yes	Snoozable: Yes
Deploy within: 5	Reboot within: 5

Figure 5.3 Device Details Page

Device Information

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:

Device Information:

Name: \\TP_EMERALD	Description:
Operating System: Win2K3	OS Version: 5.2
OS Service Pack: Service Pack 1	OS Build Number: 3790
DNS Name: TP_Emerald.techpubs.com	IP Address: 10.12.20.25

Figure 5.4 Device Information

- **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

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

Agent Information:	
Agent Installation Date: 3/23/2006 8:46:39 PM (GMT-08:00)	Agent Status: Idle
Agent Version: 6.3.0.66	Last Connected Date: 3/29/2006 10:15:10 PM (GMT-08:00)

Figure 5.5 Agent Information

- **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
- **Agent Status** - the status of the agent. Also shown on the *Devices* page
- **Last Connected Date** - the date the agent last communicated with Patch Management Server

Group Information

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

Group Information:				
Group Name	Type	Status	Added By	Added On
Win2K3	Computer (system created)	Enabled	Novell Corp.	8/23/2006 8:46:00 PM (GMT-08:00)

Figure 5.6 Group Information

- **Group Name** - the name of the group(s) that the device is a member. Click the name to go to the *Group Information* page
- **Type** - the group type. Can be a system created groups (OS) or custom group
- **Status** - the status of the group
- **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

The **Policy Information** section displays the following Policy data:

Policy Information:				
Communication Interval	Hours of Operation	Logging Level	Agent Listener Port	Agent Scan Mode
5 Minutes	Always Run	None	off	Normal

Figure 5.7 Policy Information

- **Communication Interval** - the frequency of agent communication with Patch Management Server
- **Hours of Operation** - the hours of operation in which the agent is permitted to communicate with Patch Management Server
- **Logging Level** - logging level determines how much data the agent will log while it performs its tasks
- **Agent Listener Port** - defines the port on which the agents listen. Upon receiving a ping on the defined port, the agent responds by sending current version information and contacts ZENworks Patch Management.
- **Agent Scan Mode** - the mode in which the discovery agent runs

Deployment Notification Defaults

The **Deployment Notification Defaults** section displays the following deployment data:

Deployment Notification Defaults:	
Deployment Notification Options	Reboot Notification Options
Cancelable: No	Cancelable: Yes
Snoozable: Yes	Snoozable: Yes
Deploy within: 5	Reboot within: 5

Figure 5.8 Interactive Agent Information

- **Deployment Notification Options** - the notification options assigned to deployments related to the group. These are defined under “[PatchLink Update Default Configuration](#)” on page 235
- **Reboot Notification Options** - the notification options assigned to reboot commands initiated from a deployment related to the group. These are defined under “[PatchLink Update Default Configuration](#)” on page 235



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 “Using the Vulnerabilities Page” on page 29.

Information Device Vulnerabilities Inventory Deployments										Total: 21
		Vulnerability Name	Impact							
		A - Deployment Test and Diagnostic Package	Critical	0	1	0	0	1	100%	
		MS-870669 Disable the ADOB.Stream object from Internet Explorer (SEE NOTES)	Critical - 01	0	1	0	0	1	100%	
		Patchlink Subscription Update - To Improve Replication Time (SEE NOTES) (re-released 8/04/04)	Critical - 01	0	1	0	0	1	100%	
		MS-898060 Network connectivity failure between clients and servers	Recommended	0	1	0	0	1	100%	
		Adobe Acrobat Reader 6.0	Software	0	1	0	0	1	100%	

Figure 5.9 Device Vulnerabilities

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 “Using the Inventory Page” on page 114.

Information Vulnerabilities Device Inventory Deployments										Total: 24
Hardware Device Classes										
		Architecture								
		BIOS								
		Computer								
		Disk drives								
		Display adapters								
		DVD/CD-ROM drives								
		File Systems								
		Floppy disk controllers								

Figure 5.10 Device Inventory



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.

Deployments by Device: \\TP_EMERALD

Information		Vulnerabilities	Inventory	Device Deployments	Total: 3					
<input type="checkbox"/>	Name	Initial Start Date								
	System Task: Reboot	Not Scheduled	0	0	1	0	0	0	0 %	
	System Task: Refresh Inventory Data	4/1/2006 6:00:00 AM (Local)	1	0	1	0	0	0	0 %	
	System Task: Discover Applicable Updates	3/30/2006 4:51:40 AM (Local)	1	0	1	0	0	0	0 %	

Figure 5.11 Device Inventory



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 a Device”
- “Deploying a Vulnerability”
- “Exporting Device Information”
- “Scanning Devices”
- “Rebooting Devices”



Figure 5.12 Devices - Action Menu

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.

Agent Installers

Server Information

Serial Number: 934DA35F-93153753 Version: 6.3.2.611

URL: <http://TP-NOVELL>

<http://10.19.2.158>

Single Agent Windows MSI Installer Version: **6.3.2.611**
 Download: <http://tp-novell.lab.patchlink.com/download/updateagent.msi> Release Date: **9/22/2006**
 For a single installation of the Agent on a local computer.

Operating Systems

Requirements

Installation Notes
 ([more information at the Novell ZENworks Patch Management Forum](#))

Single Agent Windows x64 MSI Installer Version: **6.3.2.611**
 Download: <http://tp-novell.lab.patchlink.com/download/updateagent-x64.msi> Release Date: **9/22/2006**
 For a single installation of the x64 Agent on a local computer.

Operating Systems

Requirements

Installation Notes
 ([more information at the Novell ZENworks Patch Management Forum](#))

Single Agent Installer for Linux/Unix/Mac/Netware Version: **6.3237**
 Download: <http://tp-novell.lab.patchlink.com/download/unixupdateagent.tar> Release Date: **9/22/2006**
 For a single installation of the JAVA-based Agent on a local computer.

Operating Systems

Figure 5.13 Agent Installer



Viewing Device Details

View details of a specific device by selecting the desired device and clicking the **device name**.

Details by Device: \\TP-AGENT-02

Device Information

Vulnerabilities

Inventory

Deployments

Device Information:

Name: \\TP-AGENT-02

Operating System: WinXP

OS Service Pack: Service Pack 2

DNS Name: TP-AGENT-02

Description:

OS Version: 5.1

OS Build Number: 2600

IP Address: 10.19.2.157

Agent Information:

Agent Installation Date: 9/12/2006 8:54:53 PM (GMT-07:00)

Agent Version: 6.3.0.563

Agent Status: Idle

Last Connected Date: 9/13/2006 12:29:28 AM (GM

Group Information:

Group Name	Type	Status	Added By	Added On
WinXP	Computer (system created)	Enabled	PatchLink Corp.	9/12/2006 8:54:00 PM (GMT-07:00)

Policy Information:

Communication Interval	Hours of Operation	Logging Level	Agent Listener Port	Agent Scan Mode
15 Minutes	Always On	None	off	Normal

Deployment Notification Defaults:

Deployment Notification Options	Reboot Notification Options
Cancelable: No	Cancelable: Yes
Snoozable: Yes	Snoozable: Yes
Deploy within: 5	Reboot within: 5

Figure 5.14 Device Details Page

Disabling 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**
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



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**
3. In the *Confirmation* dialog box, click **OK**

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** 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.

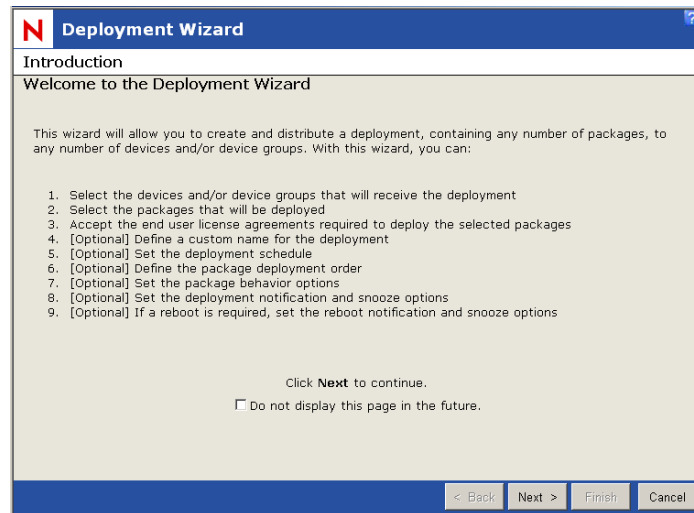


Figure 5.15 Deployment Wizard



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 capture device information and save it in comma-separated value (.CSV) file format. Exported files are saved in .csv format as a Microsoft Excel Worksheet. You also can save the exported file to another format from Excel.

For more information on exporting, see “Exporting Data” on page 14.

Scanning Devices

Scanning reschedules the Discover Applicable Updates System Task (DAU) for immediate execution. The DAU runs on a predefined interval schedule. Enacting a scan manually schedules the task for immediate execution. The **Scan Now** command results in the same action regardless of the current page.



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.

To Scan Devices

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.

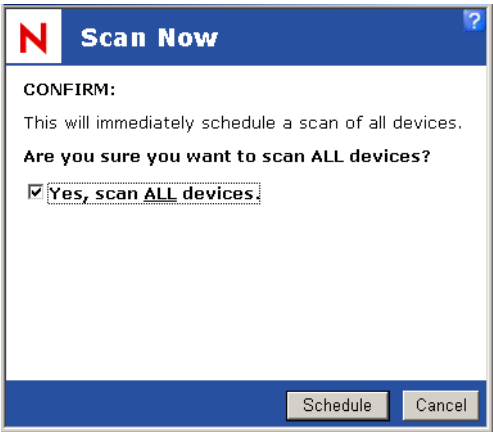


Figure 5.16 Scan Devices





Warning: Scheduling a DAU entails creating traffic for all the selected devices.

3. Select **Yes, scan the selected device** and click **Schedule**.
Scan Now - Success dialog box appears informing you that the scan has been processed and providing a link to view the results of the DAU deployment.

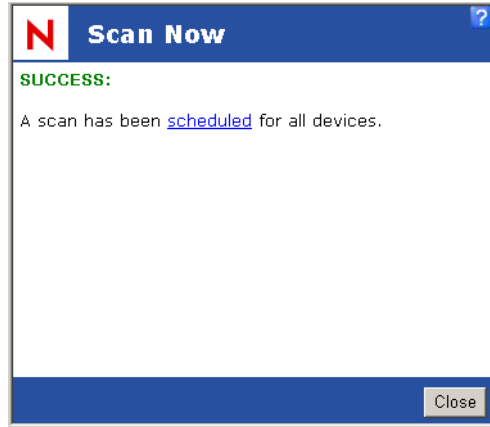


Figure 5.17 Scan Group Scheduled

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



Rebooting Devices

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

To Reboot Device Membership

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

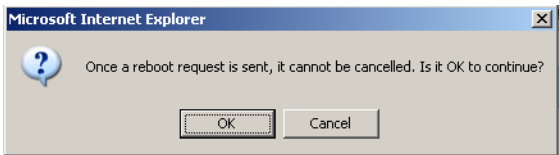


Figure 5.18 Reboot Device Group Members

The *Reboot Now* window opens.



Figure 5.19 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.

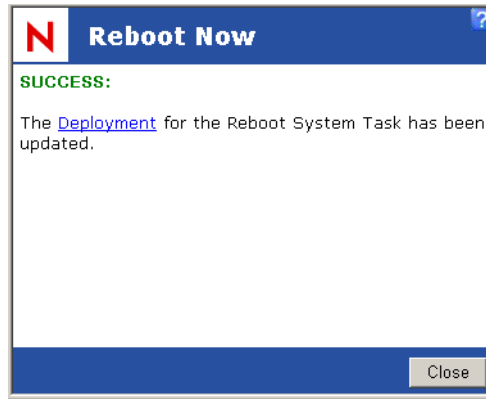


Figure 5.20 Reboot Device Success Screen





6 Using Groups

A group is a collection of devices organized for the purpose of simplifying management activities. The *Groups* page contains a listing of all groups registered to the Patch Management Server. The page lists the names of each group and displays both system groups and custom groups. From this page you can access group information by expanding the group or proceed to the *Group Information* page by clicking a group name.

In this Chapter

- “Using the Groups Page”
- “Using the Group Details (Information) Page”
- “Working with Groups”

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

Action	Group Name	Devices
	AIX	0
	HP-UX	0
	Linux	0
	Mac OS X	0
	NetWare	0
	Solaris	0
	Win2K	2
	Win2K3	3
	Win2K3x64	0
	Win98	1
	WinNT	0
	WinXP	2
	WinXPx64	0

Figure 6.1 Groups Page

To View Groups

1. Select the *Groups* tab, select your filter options, and click **Update View**.
The applicable hardware displays in the *Groups* window.



Using the Groups Page

You can manipulate the list of groups using the search and filter options. Click the expand icon to view a summary of each group. To display detailed group information, select the group name. The total number of groups, for each view, is displayed at the top of the *Groups* page.

- Group Status** - device group status is indicated by an icon in the status column. The displayed groups are determined by the filter criteria defined in the search section. Group status includes system and custom groups.

























































Device Groups					Total: 14
	<input type="checkbox"/>	Action	Group Name	Devices	
	<input type="checkbox"/>	  	 AIX	0	
	<input type="checkbox"/>	  	 HP-UX	0	
	<input type="checkbox"/>	  	 Linux	0	
	<input type="checkbox"/>	  	 Mac OS X	0	
	<input type="checkbox"/>	  	 NetWare	0	
	<input type="checkbox"/>	  	 Solaris	0	
	<input type="checkbox"/>	  	 Testv	0	
	<input type="checkbox"/>	  	 Win2K	1	
	<input type="checkbox"/>	  	 Win2K3	1	
	<input type="checkbox"/>	  	 Win2K3x64	1	
	<input type="checkbox"/>	  	 Win98	1	
	<input type="checkbox"/>	  	 WinNT	1	
	<input type="checkbox"/>	  	 WinXP	0	
	<input type="checkbox"/>	  	 WinXPx64	0	
< < 1 of 1 Pages > >					Rows Per Page: 25

Figure 6.2 Groups Status

The following table defines the available device group status and associated status icons.

Table 6.1 Device Group Status Icons





Icon	Status	Description
	Enabled System Group	By default, one system group is formed automatically corresponding to each operating system in the network.
	Disabled System Group	Vulnerabilities cannot be deployed to computers in this group.



Table 6.1 Device Group Status Icons

Icon	Status	Description
	Enabled Custom Group	These are groups created by the administrator. Either one agent or multiple agents belonging to multiple operating systems can be added to a group.
	Disabled Custom Group	These are the groups created by the administrator and disabled. Either one agent or multiple agents belonging to multiple operating systems can be added to a group. Vulnerabilities cannot be deployed to computers in this group.

- **Group Name** - displays the *Device Group Details* page when selected. The displayed groups are filtered by the filter criteria defined in the search section.
- **Devices** - shows the number of devices assigned to a particular group.
- **Device Group Summary Information** - the summary information is accessed by selecting the expand icon in the group list.



Device Groups			
	Action	Group Name	
		AIX	
<div> <div> Group State: Enabled Group Type: Computer (System) Agent Policy Set: No Policy Total Device Members: 0 Total Mandatory Patches: 0 Description: PatchLink Update Server Operating System Group. System Groups can not be deleted. </div> <div> Created On: 7/29/2003 4:54:13 PM (GMT-07:00) Created By: PatchLink Corp. Last Modified On: Last Modified By: None </div> </div>			

Figure 6.3

- **Group State** - current status of the group (enabled or disabled)
- **Group Type** - the group type (custom or system defined group)
- **Agent Policy Set** - the policy associated to and applied to the group
- **Total number of Member Devices** - the number of unique devices assigned to a group
- **Total number of Mandatory Patches** - the number of mandatory patches associated to the group
- **Description of the Group** - a description of the group as defined by the individual that created the group
- **Created By** - the user who created the group
- **Created On** - the date the group was created
- **Last Modified By** - the last user to have modified any settings for the group
- **Last Modified On** - the date the group was last modified
- **Last Connected Date** - the date when an agent, in this group, last connected to the ZENworks Patch Management Server



Using the Group Details (Information) Page

The *Device Group Details* page displays information about a specific device group. The page comprises the following sections: Information, Vulnerabilities, Inventory, Membership, and Mandatory baselines.



Note: Each tabbed page is associated with access rights depending on your security settings. These are in addition to the core access rights associated to the *Devices* page. See “[Defining Access Rights](#)” for details.

Device Group Information

The *Device Group Information* tab displays general group-related information and assessment graphs concerning the group's membership. The *Group Assessment* feature lets you display a record of patch activity and status information based on a variety of filter criteria.

Information for Group: WinXP

Information

Vulnerabilities

Inventory

Membership

Mandatory

Deployments

Details:

Name: WinXP

Status: Enabled

Type: System Computer Group

Agent Policy Set Name: [No Policy](#)

Membership Total: 2

Description: Novell ZENworks Patch Management Operating System Group. System Groups can not be deleted.

Created By: PatchLink Corp.

Created On: 5/29/2002 10:08:15 AM

Last Modified By: None

Last Modified On: 8/6/2002 1:49:12 PM

Mandatory Baseline Total: 0

Graphical Assessments:

Group Assessment

Filter on:

Platform: WinXP

Vendor:

All Vendors

access-remote-pc.com

Adobe

Adobe Systems, Inc

Apple

Impact:

All Impacts

Critical

Critical - 01

Critical - 05

Detection

Device Assessment

Perspective:

☒ By Agent

☐ By Patch

Perspective:

☐ By Agent

☐ By Status

GO

Figure 6.4 Group Information tab

- 136 -

Information Section

The Information section of the Device Group Information tab provides the following data:

- **Name** - the name of the group
- **Status** - the current status of the group
- **Type** - the type of the group (system or custom)
- **Agent Policy Set Name** - the assigned policy and link to the policy set information
- **Membership Total** - the total number of devices which are a member of the group
- **Description** - the group description
- **Created By** - the user who created the group
- **Created On** - the date and time the group was created
- **Last Modified By** - the user who last modified the group
- **Last Modified On** - the date and time the group was last modified
- **Mandatory Baseline Total** - the total number of patches that form the group's baseline

Device Group Assessment

Performing a group assessment creates and displays a graph representing various filtered group information. There are three basic graphs that display status information about the group membership. Selecting any one of the three options and selecting **Go** displays a graph illustrating the assessment. Additionally there are three filters that can define down to obtain more precise status information. The filters are:

- Platform
- Vendor
- Vulnerability Impact
- The graphs display the following information
 - **Group Patch Status by Agent** - displays how many agents are in each of the following patch statuses:
 - ◆ **Fully Patched** - the device requires no additional patches at this time
 - ◆ **Partially Patched** - the device is not fully patched, but some patches are installed
 - ◆ **Not Patched** - The device is not patched at all
 - ◆ **Detecting** - In process of running the Discovery and Analysis Process
 - ◆ **Pending** - The initial Discovery and Analysis process has not started so there is no data on which to determine the status
 - **Group Patch Status by Patch** - displays the how many applicable patches are in each of the following patch statuses:
 - ◆ **Fully Patched** - the device requires no additional patches at this time
 - ◆ **Partially Patched** - the device is not fully patched, but some patches are installed
 - ◆ **Not Patched** - The device is not patched at all



- ◆ **Detecting** - In process of running the Discovery and Analysis Process
- ◆ **Non-applicable** - The number of devices which have no applicable vulnerabilities
- **Agent Status** - displays the number of devices in each of the various agent states. The various states are:
 - ◆ **Sleeping** - these devices are outside their defined hours of operation
 - ◆ **Offline** - these devices haven't contacted the ZENworks Patch Management Server in over two communication intervals (15 minutes minimum for intervals smaller than 10 minutes)
 - ◆ **Running** - these devices are currently running the DAU
 - ◆ **Idle** - these devices are active yet not performing any deployments
 - ◆ **Working** - these devices are working on some deployments
 - ◆ **Disabled** - these devices are disabled

Device Group Vulnerabilities

The *Vulnerabilities* tab 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.

Information Vulnerabilities Inventory Membership Mandatory Deployments									
Vulnerability Name				Impact					
				Adobe Acrobat Reader 6.0.1	Software	0	1	0	100%
				Command AntiVirus for Windows 4.80.5 (Full-install)	Software	0	1	0	100%
				Command AntiVirus for Windows 4.90 (Full-install)	Software	0	1	0	100%
				Command AntiVirus for Windows 4.91 (Full-install)	Software	0	1	0	100%
				Command AntiVirus for Windows 4.92.1 (Full-install)	Software	0	1	0	100%
				Macromedia Flash Player 7.0.r19 for IE	Software	0	1	0	100%
				Microsoft .NET Framework 1.0	Software	0	1	0	100%
Page 1 of 1				Rows Per Page: 50					

Figure 6.5 Vulnerabilities



Device Group Inventory

This view will display 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.

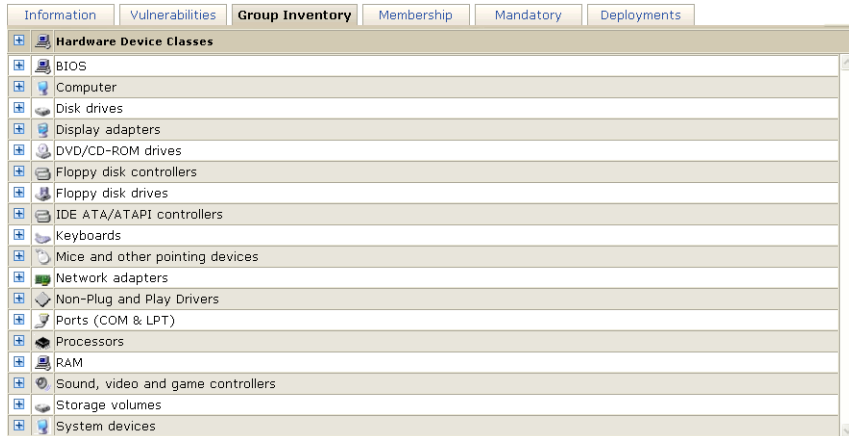


Figure 6.6 Inventory (hardware)

Device Group Membership

This view will provide a interface for management of device membership in a given custom device group.

The Device Group Membership Page allows the user to view the devices in a group.



Figure 6.7 Membership



Note: System-defined groups cannot be changed.



Device Group Mandatory Baselines

This view will display the mandatory packages (as defined by the user), for the selected device group. Refer to [Chapter 8, “Mandatory Baselines”](#) for additional details regarding Mandatory Baselines.

Information		Vulnerabilities		Inventory		Membership		Mandatory Baseline		Deployments	
				Mandatory Baseline Item		Impact	OS List				
				Adobe Acrobat Reader 6.0.1		Software	Win2K, Win2K3, Win98, WinMe, WinNT, WinXP				
				Adobe Acrobat Reader 6.0.2 update		Critical - 01	Win2K, Win2K3, Win98, WinMe, WinNT, WinXP				
				Adobe Acrobat Reader 6.0.3 Update		Critical - 01	Win2K, Win2K3, Win98, WinMe, WinNT, WinXP				

Figure 6.8 Mandatory Baseline

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.

Information		Vulnerabilities		Inventory		Membership		Mandatory		Group Deployments		Total: 1
<input type="checkbox"/>	Name	Initial Start Date										
<input checked="" type="checkbox"/>	Deployment of Adobe Acrobat Reader 6.0.1	ASAP	0	0	1	0	0	0	0	0	0	0 %

Figure 6.9 Group Deployments Tab



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

Working with Groups

Effective use of groups provide a way to manage devices by letting you apply the same deployment rules to multiple devices with similar needs.

- “Using the Create Group Wizard”
- “Deploying a Group”
- “Disabling Groups”
- “Enabling Groups”
- “Editing Groups”

- “Deleting Groups”
- “Viewing Group Properties”
- “Exporting Group Data”
- “Scanning Groups”
- “Rebooting Groups”

Defining Groups

System groups are organized by operating system to provide an easier way to manage the entire group rather than managing each device individually

You can define groups into System or Custom groups, depending on your organizational needs.

Table 6.2 Group Definitions

Group Type	Definition
System	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.
Custom	Devices grouped using the Create a Group wizard. Custom groups associate a collection of devices as defined by the user.

Additional Group Type Definitions

You can create some or all of the following group types, depending on your organizational needs:

Table 6.3 Special Group Definitions

Group Type	Purpose
Critical	Devices grouped by priority such as mission critical, production, and development. These groups contain the computers which must be accessible during business hours
Functional	Devices grouped by function such as web servers, SQL servers, file servers, and print servers
Geographical	Devices grouped by geographical limitations. They are generally unique physical locations such as remote offices, different campuses, countries, and other geographical criteria
Operational	Devices grouped by user function
Reporting	Devices grouped for management and auditing reports



Using the Create Group Wizard

Use a wizard to create and define groups. The wizard comprises three tabbed pages: group information, device members, and mandatory baseline.

The wizard includes three main commands:

Table 6.4 Device Group Wizard Functions

Button	Function
Reset	Clears the page back to its initial state
OK	Saves the group and closes the wizard.
Cancel	Closes wizard without saving the group

To Create a Group

1. In the *Device Groups* page, select **Create**
The Create a Group wizard opens and displays the *Group Information* tab.
2. In the *Name* field, type the name of the new group. The name can be up to 255 characters
3. In the Description field, type a brief description about the group.
4. Select an **Agent Policy Set** from the drop-down list.



5. Select an e-mail address(es) to serve as the recipient(s) of group-related system messages and notifications.

Create a Group

Group Information | Members | Mandatory

Enter the Group Information:

* Name:

Description:

Agent Policy Set:

E-Mail: ☐ techpubs@patchlink.com

Number of Device Members: 0 Number Assigned to the Mandatory Baseline: 0

* Indicates a required field.

OK Cancel

Figure 6.10 Create a Group Wizard - Group Information



Note: Additional e-mail addresses can be added from the **Options > E-Mail notification** settings.

6. Click **OK** or continue to the *Members* tab.

Group Members Are Created By

- “Manually Selecting Device Members”
- “Importing a Device List”

Manually Selecting Device Members

1. Select the **Members** tab.
The *Select Member Devices* tab opens.
2. In the *Devices* section, select **Browse Devices**. To import a Device list, continue to *Importing a Device List*.
3. Select the device or devices to include in the group.



- 4. Click **Assign**.
The selected devices move to the Selected Devices area.
- 5. Page to the next screen, if needed. If any more devices are selected, you must click **Assign** after each new page.
- 6. To assign all available devices, click **Assign All**

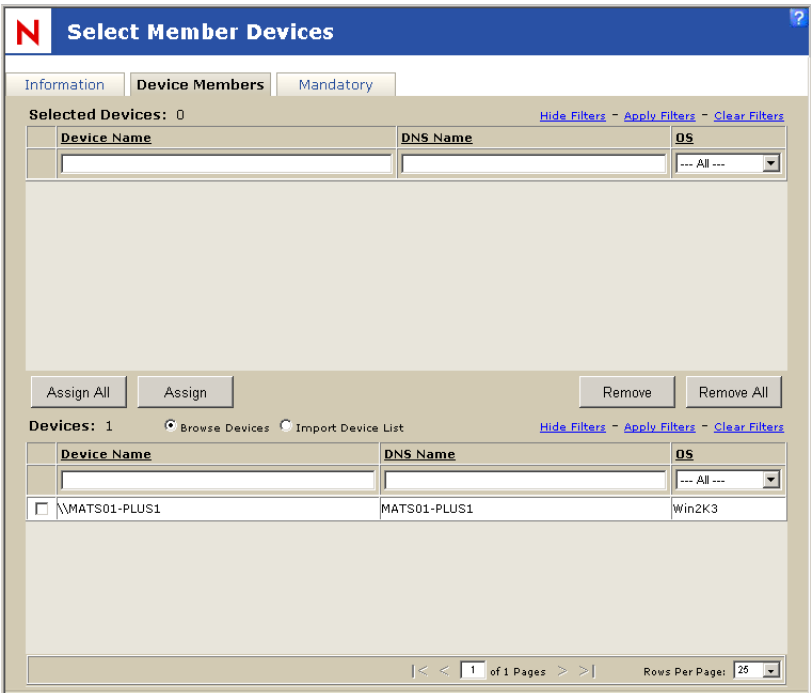


Figure 6.11 Create a Group - Device Members

- The system displays the selected device in the *Selected Devices* window.
- 7. Click **OK** or select the *Mandatory* Tab.

Using the Filter Functions to Select Devices

- 1. In the *Devices* area, select **Show Filters**.
The filters display in the window.
- 2. Type the **filter criteria** in the *Device Name* and/or the *DNS Name* fields. Use the drop-down list box for the *OS* filter.
- 3. Click **Apply Filters**.
The *Devices* are filtered and the results display in the *Device* area.
- 4. Select **Clear Filters** to start another search.



Importing a Device List

1. In the *Device Members* tab, select **Import Device List**.
The **Comma-delimited list of devices to add to the group** field opens.

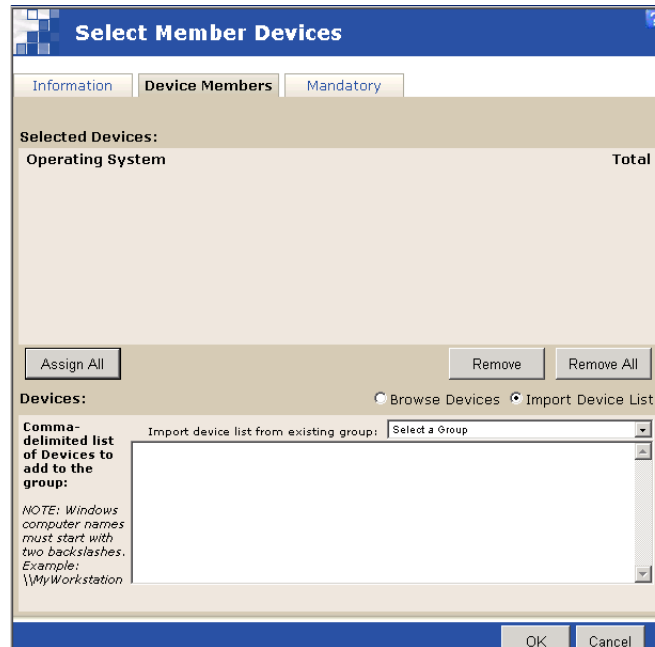


Figure 6.12 Import Device List

2. Select a device from the **Import device list from an existing group** drop-down list.
The selected device displays in the field.
3. Continue to add devices as needed.
The system separates each additional device by a comma.
4. Click **OK** or continue to the *Mandatory* tab.

Setting a Mandatory Baseline



Note: Assigning a Mandatory Baseline to a group is optional. If you do not want to assign a baseline, or will do it later, click **OK**. The group is created and opens in the Groups list.

1. Select the **Mandatory** tab



- 2. In the *Vulnerabilities* field, select the desired vulnerabilities



Note: This listing of vulnerabilities includes ALL known vulnerabilities, not just the applicable vulnerabilities for the members of this group.

- 3. Click **Assign**. To assign all available vulnerabilities, click **Assign All**
- 4. Page to the next screen, if needed. If any more devices are selected, you must click **Assign** after each new page.

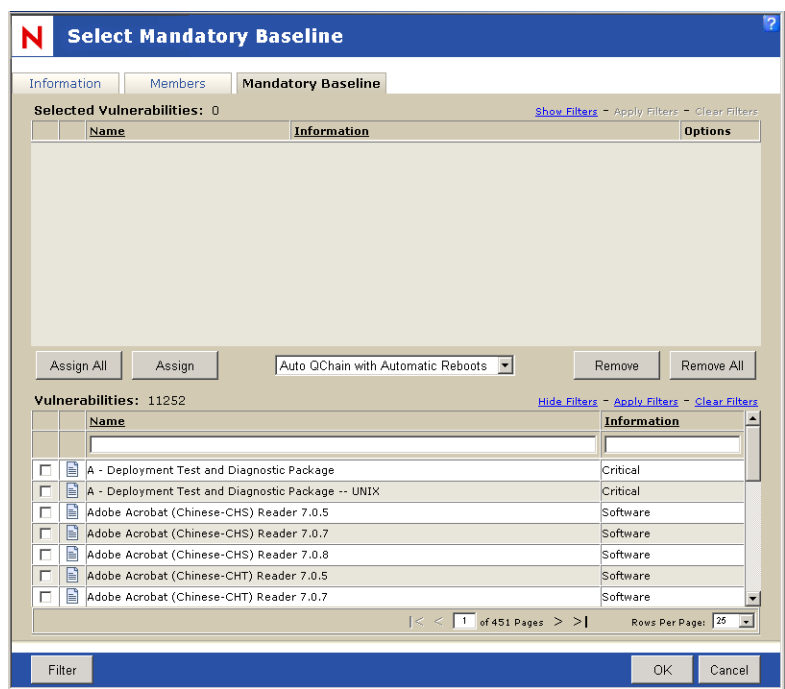


Figure 6.13 Create a Group - Mandatory Baseline

- 5. Click the **Filter** button to search for mandatory patches for any devices on the system. The *Needed Detection Vulnerabilities* screen opens and displays all required patches.

Using the Filter Functions to Select Vulnerabilities

- 1. In the *Devices* 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 Devices are filtered and the results display in the Device area.
4. Select **Clear Filters** to start another search.
5. Select the patches and click **OK**.
The *Needed Detection Vulnerabilities* screen closes and the patches display in the *Selected Vulnerabilities* window.

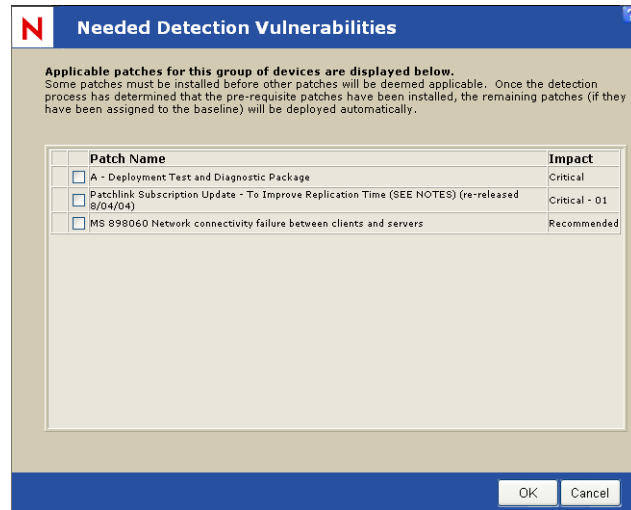


Figure 6.14 Create a Group - Needed Detection Vulnerabilities

6. In the **Deployment Options** drop-down list, select a deployment type
 - **Auto QChain with Manual Reboots** - Automatically sets all possible vulnerabilities to deploy with QChain enabled. When a reboot is required the agent will remain in a 'dirty state' until you perform a reboot
 - **Auto QChain with Automatic Reboots** - Automatically sets all possible vulnerabilities to deploy with QChain enabled. All necessary reboots are performed automatically
 - **Standard - Set Individually** - Uses the QChain and reboot settings as defined for each vulnerability
7. Click **OK**.
The new group information is saved and the system opens the *Group Details* page.

Go to **Selecting Deployment Options** for more information on customizing package deployment options.



Selecting Mandatory Baseline Deployment Options

- 1. In the list of selected vulnerabilities, select **Options**
- 2. The *Package Deployment Options* window opens.

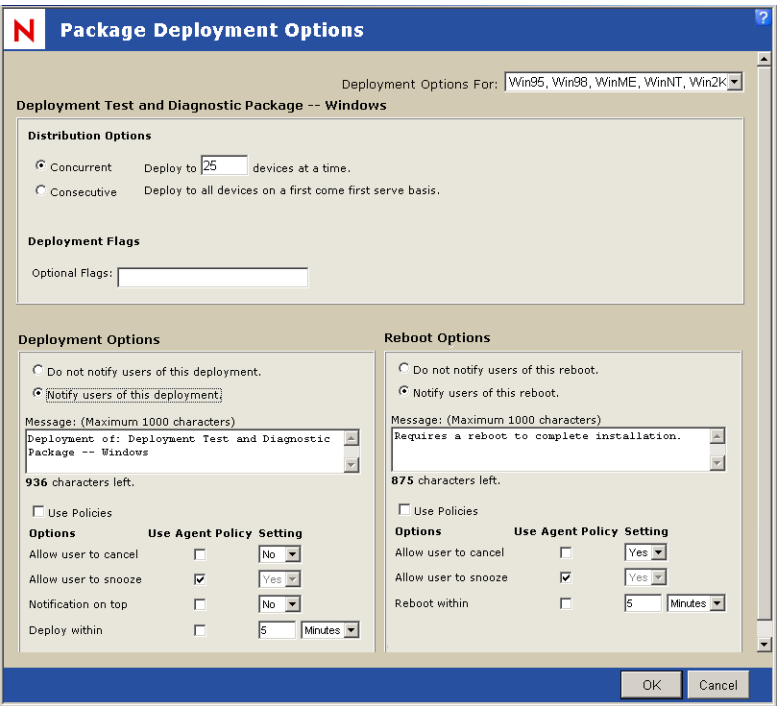


Figure 6.15 Package Deployment Options screen

- 3. In the *Deployment Options* drop-down list, confirm the operating system selection.
- 4. In *Distribution Options*, select **Concurrent** and the **device amount** or **Consecutive**.
- 5. If needed, type the **Deployment Flags** if the system has not added any.
- 6. Set the desired **Deployment Options**.
 - **Use Agent Policies** - uses the current settings. The other options become inactive when selecting this option
 - **Custom Behavior** - allows you to set notification, and recipient options
- 7. Set the desired **Reboot Options**



- **Use Agent Policies** - uses the current settings. The other options become inactive when selecting this option
 - **Custom Behavior** - allows you to set notification, and recipient options
8. Click **OK**.
The *Package Deployment Options* screen closes.

Deploying a Group

Deploying to a group of selected devices is a key function of the ZENworks Patch Management system. 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](#)” on page 84 for additional information.

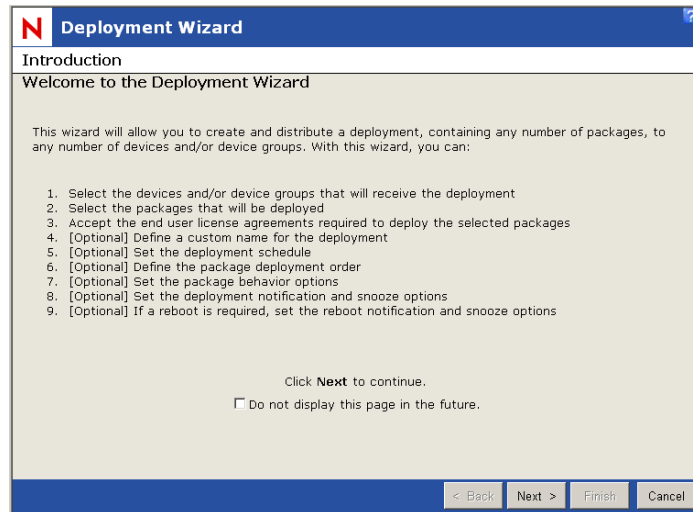


Figure 6.16 Deployment Wizard



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, see [Chapter 4, “Working With Deployments”](#) in this guide.



Disabling Groups

You can disable any group; allowing you to maintain the group within the Patch Management Server database in an inactive state. Disabled groups are not included in deployments.



Note: If you disable a group, the devices associated to the group are **not** disabled.

You can view, enable and delete all disabled groups. Disabled groups move to the bottom of the list and are noted with the disabled status icon.

Device Groups				Total: 13
	Action	Group Name	# Devices	
		AIX	0	
		HP-UX	0	
		Linux	0	
		Mac OS X	0	
		NetWare	0	
		Solaris	0	
		Win2K	0	
		Win2K3	1	
		Win2K3x64	0	
		Win98	0	
		WinNT	0	
		WinXP	2	
		WinXPx64	0	
< 1 of 1 Pages >				Rows Per Page: 25
Administrator Create Enable Disable Delete Deploy Export Scan Now Reboot Now				

Figure 6.17 Groups List



To Disable a Group

1. In the Patch Management Server main menu, select **Groups**
2. In the *Groups* page, select a group or groups to disable
3. In the *Action Menu*, click **Disable**
The system disables the Group and displays it accordingly.











































Device Groups				Total: 14
<input type="checkbox"/>	Action	Group Name	Devices	
<input checked="" type="checkbox"/>	  	AIX	0	
<input checked="" type="checkbox"/>	  	HP-UX	0	
<input checked="" type="checkbox"/>	  	linux	0	
<input checked="" type="checkbox"/>	  	Mac OS X	0	
<input checked="" type="checkbox"/>	  	NetWare	0	
<input checked="" type="checkbox"/>	  	Solaris	0	
<input checked="" type="checkbox"/>	  	Win2K	0	
<input checked="" type="checkbox"/>	  	Win2K3	1	
<input checked="" type="checkbox"/>	  	Win2K3x64	0	
<input checked="" type="checkbox"/>	  	Win98	0	
<input checked="" type="checkbox"/>	  	WinNT	0	
<input checked="" type="checkbox"/>	  	WinXP	2	
<input checked="" type="checkbox"/>	  	WinXPx64	0	
<input checked="" type="checkbox"/>	  	Test Group	0	

Figure 6.18 Disabled Group



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



Enabling Groups

You can re-enable any disabled group. A group must be enabled to create deployments for that group.

Device Groups				Total: 14
	Action	Group Name	Devices	
		AIX	0	
		HP-UX	0	
		Linux	0	
		Mac OS X	0	
		NetWare	0	
		Solaris	0	
		Win2K	0	
		Win2K3	1	
		Win2K3x64	0	
		Win98	0	
		WinNT	0	
		WinXP	2	
		WinXPx64	0	
		Test Group	0	

1

of 1 Pages

Rows Per Page: 25

Administrator

Create

Enable

Disable

Delete

Deploy

Export

Scan Now

Reboot Now

Figure 6.19 Groups List

To Enable a Group

- 1. In the Patch Management Server main menu, select **Groups**
- 2. In the *Groups* page, select the disabled group or groups to enable
 - Ensure the page filter is set to *All* or *Disabled*



3. In the *Action Menu*, click **Enable**

Device Groups			Total: 14
<input type="checkbox"/>	Action	Group Name	Devices
<input type="checkbox"/>		AIX	0
<input type="checkbox"/>		HP-UX	0
<input type="checkbox"/>		Linux	0
<input type="checkbox"/>		Mac OS X	0
<input type="checkbox"/>		NetWare	0
<input type="checkbox"/>		Solaris	0
<input type="checkbox"/>		Test Group	0
<input type="checkbox"/>		Win2K	0
<input type="checkbox"/>		Win2K3	1
<input type="checkbox"/>		Win2K3x64	0
<input type="checkbox"/>		Win98	0
<input type="checkbox"/>		WinNT	0
<input type="checkbox"/>		WinXP	2
<input type="checkbox"/>		WinXPx64	0

1 of 1 Pages Rows Per Page: 25

Administrator Create Enable Disable Delete Deploy Export Scan Now Reboot Now

Figure 6.20 Enabled Group

The Group is enabled and now can be used for deployment.

Editing Groups

All group can be edited at any time. Editing is performed in the Edit a Group wizard. The *Edit a Group* wizard has the same features and functionality as the *Create a Group* wizard.

To Edit a Group

1. In the *Groups* page, select the group to edit
2. In the Edit a Group wizard, perform the desired edits
3. Click **OK**

Deleting Groups

In order to delete a group, it must first be disabled. Ensure the filter is set to **All** or **Disabled Groups**.

To Delete a Group

1. In the Patch Management Server main menu, select **Groups**
2. In the *Groups* page, select the group or groups to delete.
3. In the *Action Menu*, click **Delete**



Viewing Group Properties

Selecting a group and clicking Properties opens the Information for Group page. This page was discussed earlier in the section “[Using the Group Details \(Information\) Page](#)”.

To View Group Properties

1. In the Patch Management Server main menu, select **Groups**
2. In the *Groups* page, select the group to view
3. In the *Action Menu*, select **Properties**

Exporting Group Data

The export utility lets you capture device information and save it in comma-separated value (.CSV) file format. Exported files are saved in .csv format as a Microsoft Excel Worksheet. You may, of course, save the exported file to another format from Excel.



Note: Some data may not import or not translate into .csv format in a readable format.

Scanning Groups

Scanning reschedules the Discover Applicable Updates System Task (DAU) for immediate execution. The DAU runs on a predefined interval schedule. Enacting a scan manually schedules the task for immediate execution. The **Scan Now** command results in the same action regardless of the current page.



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.

To Scan Devices

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.

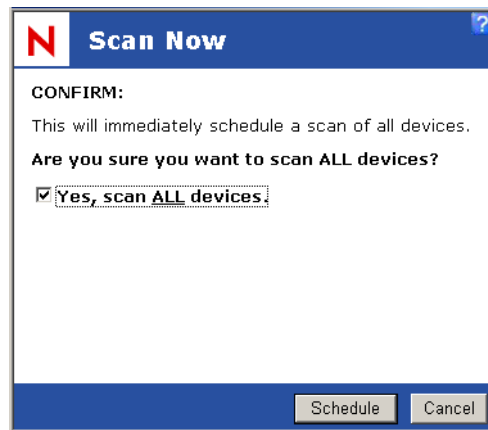


Figure 6.21 Scan Devices



Warning: Scheduling a DAU entails creating traffic for all the selected devices.



3. Select **Yes, scan the selected device** and click **Schedule**.
Scan Now - Success dialog box appears informing you that the scan has been processed and providing a link to view the results of the DAU deployment.

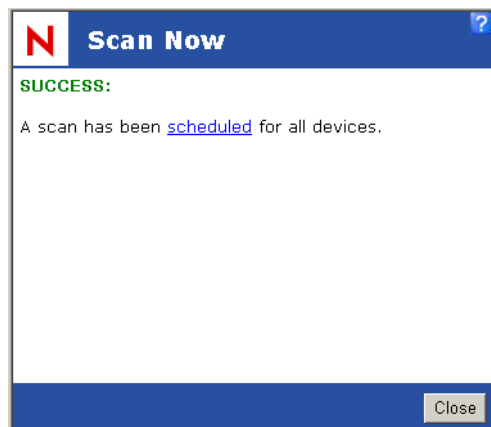


Figure 6.22 Scan Group Scheduled

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

Rebooting Groups

The *Reboot Now* command lets you initiate the Reboot system task to all members of the selected group or groups.

To Reboot Group Membership

1. In the *Groups* page, select one or multiple groups
2. Click **Reboot Now**
The Reboot Warning dialog box opens.
3. In the *Reboot Warning* dialog box, click **OK**.

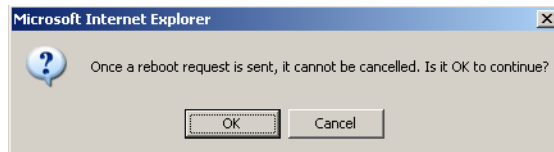


Figure 6.23 Reboot Device Group Members

The *Reboot Now* window opens.

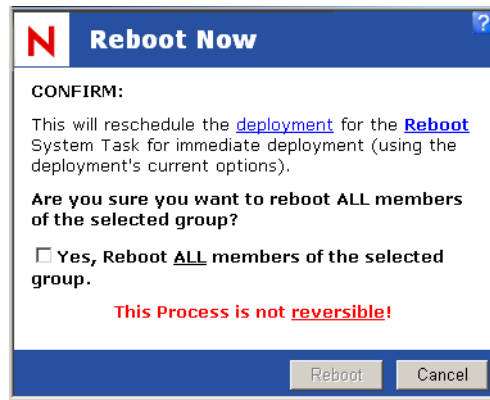


Figure 6.24 Reboot Now

4. Confirm the reboot, and select **Yes, Reboot ALL members of the selected group**.



5. Click **Reboot**.

The system schedules the reboot and the *Reboot Success* window opens.

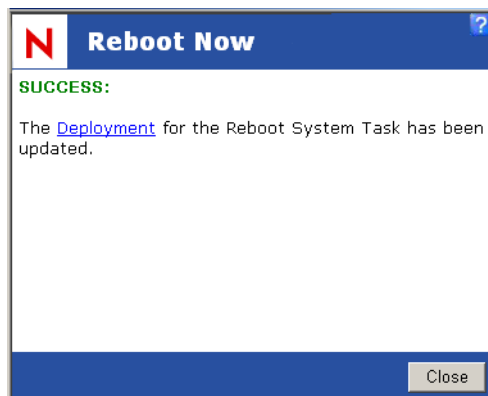


Figure 6.25 Reboot Success Screen



Note: Disabled groups still can be rebooted because this function works at the device level.

7 Viewing Device Inventory

This chapter provides information on viewing and exporting network inventory information using ZENworks Patch Management. Inventory provides you a means to pinpoint all the operating systems, software applications, hardware devices, and services installed and running on your network down to the single machine level.

In this Chapter

- “About Inventory”
- “Using the Inventory Page”
- “Scanning Inventory”
- “Using Custom Inventory”

About Inventory

Inventory captures a comprehensive view of all functional components of each agent. You can generate an inventory list for software, hardware, operating systems, and services installed on a system. Using this feature, you can determine all devices with a particular component installed.

The inventory list displays each item belonging to a specific *Inventory Type*. For example, it will display the operating systems detected on the agents. For each listed item, click the expand icon (plus icon) to view all devices installed with or running the selected component.

In addition to allowing you to generate inventory reports for various components, you can also export inventory to a file (.CSV) or initiate an inventory scan on all of your agents.

Inventory information is also available at the device and group level.

- **Devices** - Click a device name to view the details page for the selected device. In the *Device Details* page, click the **Inventory** tab
- **Groups** - Click a group name to view the information page for the selected group. In the *Information for Group* page, click the **Inventory** tab).



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

Viewing Inventory

To View Inventory

1. Select the *Inventory* tab, select your variables, and click **Update View**.
The applicable hardware displays in the *Inventory* window.
2. Click the expand icon (plus icon) to view the details of a particular Inventory class.



Using the Inventory Page

The *Inventory* page displays a listing of each *Inventory Type* and the devices that have the selected type installed. For type, click the expand icon (plus icon) to view all devices installed with or running the selected component. Clicking the collapse icon hides this list from view.

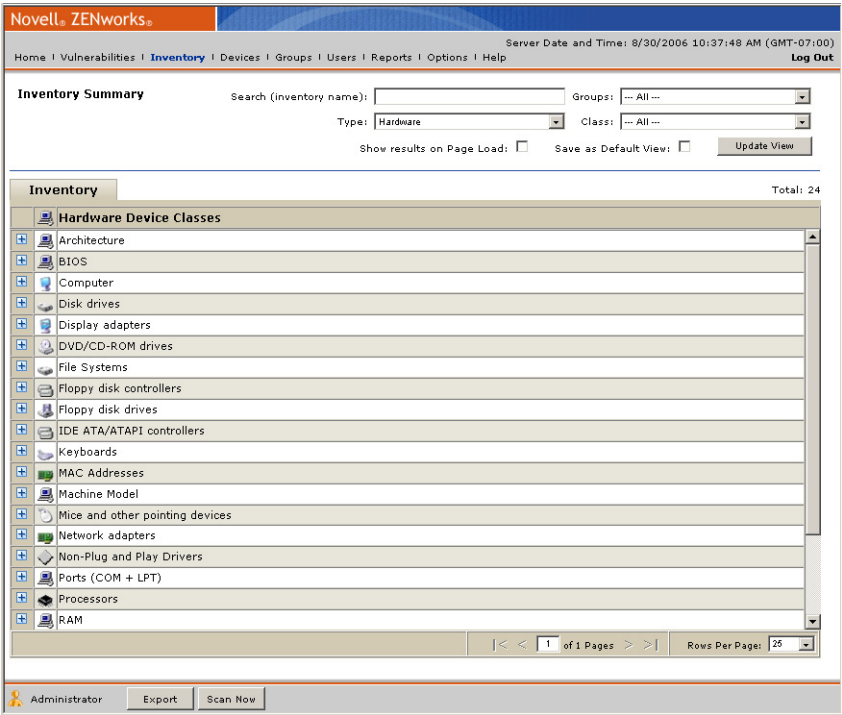


Figure 7.1 Inventory Page

Inventory Types

ZENworks Patch Management supports filtering by the following views:

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



- “Services View”



Note: The Type, Groups, Devices, and Search options are inclusive of each other. That is, you can produce a more granular filter by selecting a type and group. For very large networks, you may even consider filtering by type, group, and also use the search feature to further narrow down the potential result set.

Operating Systems View

Displays the full operating system (OS) platform names and the number of instances this operating system was detected. Instances refer to the number of times the operating system platform was detected. This value is always one (1) if the display is based on a single device.

Software View

Displays the software applications detected as being installed on your agents. This view displays the name of the software application and the number of instances the software application was detected.

Hardware View

Displays the hardware devices found on your agents. Hardware is organized into device classes such as disk drives, processors, network adapters, etc. A device is a specific piece of hardware, such as a Virtual Hard Drive or DVD/CD-ROM Drive. Each device also includes the number of instances that the device was detected.

An instance is a specifically detected device or installed driver. A device may contain multiple instances of a installed device or driver. For example, a device may contain a video graphics adapter that contains multiple video sources and destinations in which each source or destination is identified as a separate instance.



Note: The hardware view includes an additional filter option: Devices. This allows you to filter inventory by device type as well as device group.



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

Services View

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



Scanning Inventory

Scanning reschedules the Discover Applicable Updates System Task (DAU) for immediate execution. The DAU runs on a predefined interval schedule. Enacting a scan manually schedules the task for immediate execution. The **Scan Now** command results in the same action regardless of the current page.



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.

To Scan Devices

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.

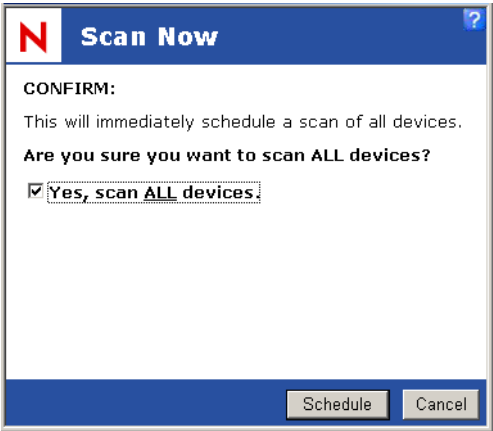


Figure 7.2 Scan Devices



Warning: Scheduling a DAU entails creating traffic for all the selected devices.



3. Select **Yes, scan the selected device** and click **Schedule**.
Scan Now - Success dialog box appears informing you that the scan has been processed and providing a link to view the results of the DAU deployment.

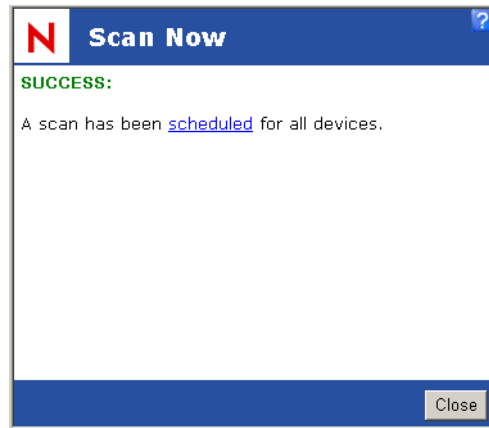


Figure 7.3 Scan Group Scheduled

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

About Inventory Scanning

The Detection Process

The detection agent process has the primary role of performing detection scans which allow the ZENworks Patch Management Server to determine security risks and other vulnerabilities present in your computing environment. This analysis determines the patches, hot fixes, service packs and updates that are significant to your network. Based on the analysis performed through the detection agent, the subscription agent automatically downloads a series of vulnerabilities.

The Discover Applicable Updates task (DAU) runs the Detection Agent. This system task is performed daily on an established schedule and also after every successful deployment. The DAU is managed through the Vulnerabilities page.



Note: Clicking **Scan Now** in the *Inventory* page runs the DAU task for all devices under management, not only a specified device.



Detection Results

If the ZENworks Patch Management Agent is in the *Pending Initial Detection* state for an usually long period of time, it is possible that the ZENworks Patch Management Server is experiencing a communication problem.

To check, determine if the *Discover Applicable Updates* and *Refresh Inventory Data* system tasks are scheduled for deployment.

To Determine If the DAU is Scheduled

1. Select **Devices**
2. Select the desired device
3. On the *Device Details* page, click the **Deployment** tab



Note: If both system tasks are scheduled for deployment, the problem is likely device specific. You can look for error codes or messages indicating why the Agent cannot upload it's discovery results to ZENworks Patch Management in the Agent's debug.log file found in C:\Program Files\Novell\Update Agent\

Using Custom Inventory

To use a custom inventory file (see “[Setting Inventory Collection Options](#)” on page 243), you must create the custom inventory (XML) file.



Note: The file must be named `CustomInventory.xml` and each agent must have a local file (in the `C:\Program Files\Novell\Update Agent` directory for Windows Agents, and the `patchagent/update/conf.d` for Linux/Unix/Mac Agents).

The XML inventory options are customizable as follows:

Guidelines for Microsoft Windows based Operating Systems

Valid XML Options

Literal

The new item will be added to the hardware inventory in the specified (or default if not specified) class. 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 6.3
  Custom Inventory</item>
```

Returns:

```
"Example Name = Novell 6.3 Custom Inventory"
```

Registry

The new item will be added to the hardware inventory in the specified (or default if not specified) class. 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\XML_Inventory.xml"
```



Environment

The new item will be added to the hardware inventory in the specified (or default if not specified) class. The string added will be of the form "***name*** = ***value***" where ***name*** is the tag name and ***value*** is the expanded (if possible) 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

The new item will be added to the hardware inventory in the specified (or default if not specified) class. 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 SerialNumber 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_ComputerSystem">
  Manufacturer</item>
```

Returns:

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



Text_File

The new item will be added to the hardware inventory in the specified (or default if not specified) class. 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 consistent delimiter (defined with the ***delimiter*** attribute). For each valid line 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 the 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

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 AssetNumber 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 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/assestTag">
      c:\sampleInventoryXML.xml</item>
  </items>
</customInventory>
```



Guidelines for Linux/Unix/Mac based Operating Systems

Valid XML Options

Literal

The new item will be added to the hardware inventory in the specified (or default if not specified) class. 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 6.3
  Custom Inventory</item>
```

Returns:

```
"Example Name = Novell 6.3 Custom Inventory"
```

Dynamic

Dynamic allows the usage of a script and will add the results of the script in the specified (or default if not specified) class. 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)"
```



XML Schema Definition

The CustomInventory.xml file should conform to the following XML schema definition:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="command">
    <xs:complexType>
      <xs:sequence>
        <xs:element maxOccurs="1" minOccurs="0" ref="shell"/></xs:element>
        <xs:element maxOccurs="1" minOccurs="0" ref="dir"/></xs:element>
        <xs:element maxOccurs="1" minOccurs="0" ref="envs"/></xs:element>
        <xs:element maxOccurs="1" minOccurs="1" ref="content"/></xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="content">
    <xs:complexType mixed="true"/></xs:complexType>
  </xs:element>
  <xs:element name="customInventory">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="items"/></xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="dir">
    <xs:complexType mixed="true"/></xs:complexType>
  </xs:element>
  <xs:element name="env">
    <xs:complexType>
      <xs:sequence>
        <xs:element maxOccurs="1" minOccurs="1" ref="EnvName"/></xs:element>
        <xs:element maxOccurs="1" minOccurs="1" ref="EnvValue"/></xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="EnvName">
    <xs:complexType mixed="true"/></xs:complexType>
  </xs:element>
```



```
<xs:element name="envs">
  <xs:complexType>
    <xs:sequence>
      <xs:element maxOccurs="unbounded" minOccurs="1" ref="env"/></xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="EnvValue">
  <xs:complexType mixed="true"></xs:complexType>
</xs:element>
<xs:element name="item">
  <xs:complexType mixed="true">
    <xs:choice>
      <xs:element ref="command"/></xs:element>
    </xs:choice>
    <xs:attribute name="xpath" type="xs:string" use="optional"/></xs:attribute>
    <xs:attribute name="delimiter" type="xs:string" use="optional"/>
    </xs:attribute>
    <xs:attribute name="name" type="xs:NMTOKEN" use="required"/></xs:attribute>
    <xs:attribute name="type" type="xs:NMTOKEN" use="required"/></xs:attribute>
    <xs:attribute name="namespace" type="xs:string" use="optional"/>
    </xs:attribute>
    <xs:attribute name="query" type="xs:string" use="optional"/></xs:attribute>
    <xs:attribute name="class" type="xs:string" use="required"/></xs:attribute>
  </xs:complexType>
</xs:element>
<xs:element name="items">
  <xs:complexType>
    <xs:sequence>
      <xs:element maxOccurs="unbounded" minOccurs="1" ref="item"/></xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="shell">
  <xs:complexType mixed="true"></xs:complexType>
</xs:element>
</xs:schema>
```



Example XML File

An example XML file is provided below:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- <!DOCTYPE customInventory SYSTEM "/home/claremonts/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="System" name="ZENworks Patch Management Disk Usage" 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[echo -n `du -ks /usr/local/work/Novell` \{(in kb\)}\]]>
          </content>
        </command>
      </item>
    <item class="custom" name="PATH" type="dynamic">
      <command>
        <content><![CDATA[echo $PATH]]></content>
      </command>
    </item>
```



```
<item class="custom" name="IP Addresses" type="dynamic">
  <command>
    <content><![CDATA[ifconfig -a | grep 'inet addr']]></content>
  </command>
</item>

<item class="custom" name="Users with exceeded disk quotas" type="dynamic">
  <command>
    <content><![CDATA[MAXDISKUSAGE=100
      for name in $(cut -d: -f1,3 /etc/passwd | awk -F: '{ $2 > 99 { print $1 } }')
      do
        echo -n "User $name exceeds disk quota. Disk usage is: "
        find /home -user $name -xdev -type f -ls | \
        awk '{ sum += $7 } END { print sum / (1024*1024) " Mbytes" }'
        done | awk "\$9 > $MAXDISKUSAGE { print \$0 }"
        exit 0]]>
    </content>
  </command>
</item>
</items>
</customInventory>
```

Exporting Inventory

Within inventory, you can export the data into an Excel comma delimited (.csv) file. Refer to [“Exporting Data”](#) on page 16 for instructions.





8 Mandatory Baselines

Establishing a mandatory baseline ensures that a group of devices is protected and that all devices in the group are patched consistently.

In this Chapter

- “About Mandatory Baselines”
- “Working with Mandatory Baselines”

About Mandatory Baselines

A mandatory baseline is a user-defined compliance level for a group of devices. If a device falls out of compliance a mandatory baseline ensures the device is patched back into compliance.



Warning: Mandatory baselines are an automatic enforcement method based on the most recent discovery scan results, and therefore there is **NO** control over the deployment time or package order for vulnerabilities resolved in this manner. Therefore, 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:

- The ZENworks Patch Management Server automatically schedules a DAU (Discover Applicable Update) task for all machines in that group.
- Patch Management Server determines which systems are applicable and out of compliance (based upon the vulnerabilities added to the baseline) following the DAU task,
- Necessary packages, as defined in the baseline, are deployed as soon as possible for each machine.



Note: Some patches like MDAC and IE 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.

Viewing Mandatory Baselines

To View the Mandatory Baseline

1. In the *Device Groups* page, select a group to go to the *Group Information* page.



2. In the *Group Information* page, select the **Mandatory** tab

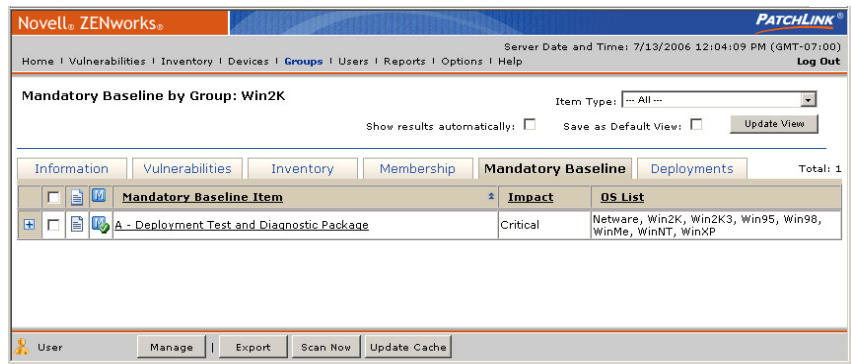


Figure 8.1 Mandatory Baseline Tab

Using the Mandatory Baseline Page

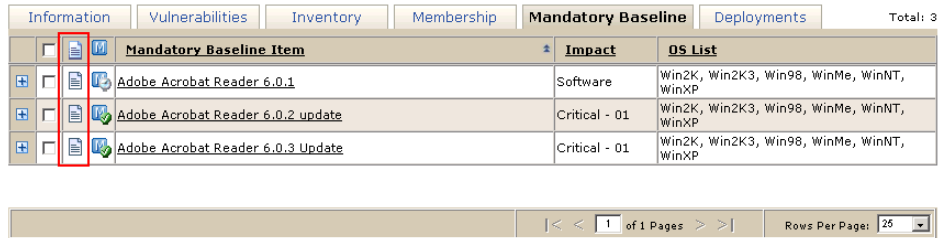
Mandatory baselines are associated to a group and can be defined in the **Add a Group** wizard when you create the group or at any time in the **Edit a Group** wizard.

When viewing the mandatory baseline for a group, you can filter the grid contents by selecting one of the following options within the *Item Type* field

- **Vulnerability Analysis** - displays only vulnerabilities associated with this baseline.
- **Distribution Packages** - displays only distribution packages associated with this baseline.
- **All** - displays both vulnerabilities and distribution packages.



Mandatory Baseline Column Definitions



Information	Vulnerabilities	Inventory	Membership	Mandatory Baseline	Deployments	Total: 3
				Mandatory Baseline Item	Impact	OS List
				Adobe Acrobat Reader 6.0.1	Software	Win2K, Win2K3, Win98, WinMe, WinNT, WinXP
				Adobe Acrobat Reader 6.0.2 update	Critical - 01	Win2K, Win2K3, Win98, WinMe, WinNT, WinXP
				Adobe Acrobat Reader 6.0.3 Update	Critical - 01	Win2K, Win2K3, Win98, WinMe, WinNT, WinXP

Rows Per Page: 25

Figure 8.2 Mandatory Baseline Columns

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

Table 8.1 Mandatory Baseline Column Definitions







Name	Definition
Mandatory Baseline Vulnerability Status	<p>The status of a mandatory baseline is indicated by an icon in the status/type column in the <i>Mandatory Baseline</i> page of the Group Details page. This column displays the status/type of each vulnerability assigned to the baseline.</p> <p>Tip: Refer to "Vulnerability Status Icons" for icon descriptions</p>
Mandatory Baseline Compliance	<p>The compliance column displays the compliance status of each vulnerability assigned to the baseline and is relative to deployment to the group membership.</p> <p>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.</p> <p>Tip: Refer to "Mandatory Baseline Item Compliance Icons" for icon descriptions</p>
Mandatory Baseline Item	<p>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.</p>
Mandatory Baseline Impact	<p>The mandatory baseline impact is presented in the <i>Impact</i> column. The impacts listed here mirror the impacts of the vulnerability (does not apply to packages).</p>
Mandatory Baseline OS List	<p>The mandatory baseline OS list is presented in the <i>OS List</i> column. The operating systems listed here mirror the operating systems that apply to the vulnerability (or package).</p>



Vulnerability Status Icons

The following table includes descriptions of the Vulnerability status icons.






Table 8.2 Vulnerability Status Icons and Descriptions

Beta	New	Current	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 8.3 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 this package (None of the members are they Detecting)
	All of the members of this group are Disabled for this package.
	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. This indicates that an error has occurred. More specific information about the type of error will appear in the mouse over text.



Working with Mandatory Baselines

There are several tasks associated with mandatory baselines designed to assist you in managing and deploying vulnerabilities in a consistent and uniform manner across groups. These are available from commands located in the *Action* menu at the bottom on the **Mandatory Baseline** page.

- “Managing a Mandatory Baseline”
- “Exporting Baseline Information”
- “Scanning Data”
- “Using Update Cache”



Figure 8.3 Mandatory Baseline - Action Menu

For information on the mandatory baseline feature when adding a new group.

Managing a Mandatory Baseline

Mandatory baselines can be applied only to groups, and each group can have only one mandatory baseline applied to it. However, a single device can be a member of multiple groups, each of which could have a different mandatory baseline.



Note: A mandatory baseline deployment always remains as *In Progress* in case a device within a group is added or altered. A fully compliant device within that Group displays as *Deployed*, despite the *In Progress* status of the Mandatory Baseline.

To Create or Manage a Mandatory Baseline

1. Select the **Groups** page
2. Select the group needed to apply a Mandatory Baseline.
3. In the *Group Details* page, select the **Mandatory** tab

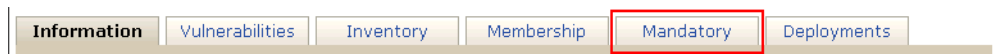


Figure 8.4 Mandatory Baseline Tab

4. Click **Update View**
The Mandatory Baseline Information populates the screen.



- 5. In the *Action Menu*, click **Manage**.
The *Add a Group* wizard opens to the *Select Mandatory Baseline* tab

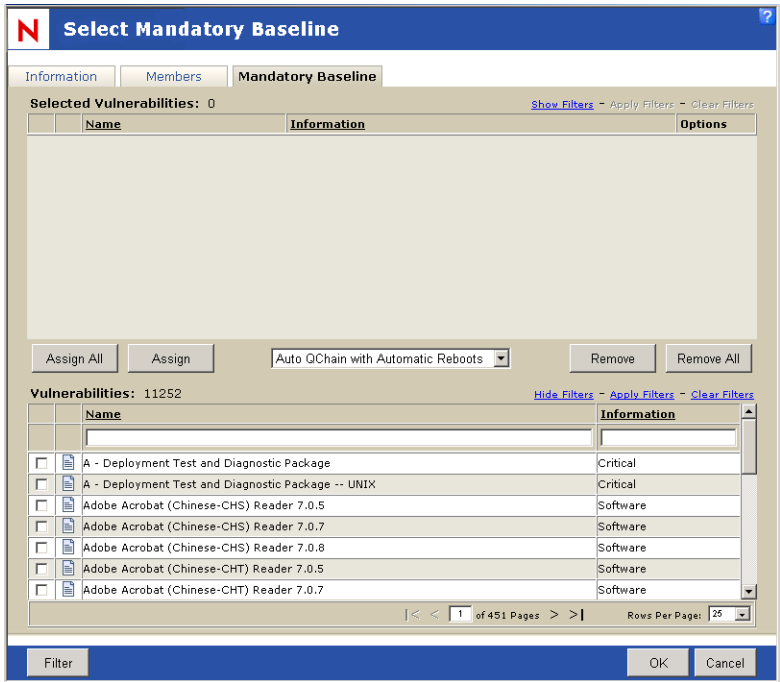


Figure 8.5 Add a Group - Mandatory Baseline

- 6. To add a vulnerability to the baseline
 - a. In the *Vulnerabilities* field, select the vulnerabilities to be patched.



Note: Manual Install vulnerabilities cannot be added to Mandatory Baselines

- b. Click **Assign**. To assign all available vulnerabilities, click **Assign All**. The selected vulnerabilities display in the *Selected Vulnerabilities* field.
 - c. If desired, click the **Filter** button to display only the vulnerabilities applicable to the group (the vulnerability is applicable to at least one device in the group).



The *Needed Detection Vulnerabilities* screen opens and displays the applicable vulnerabilities.

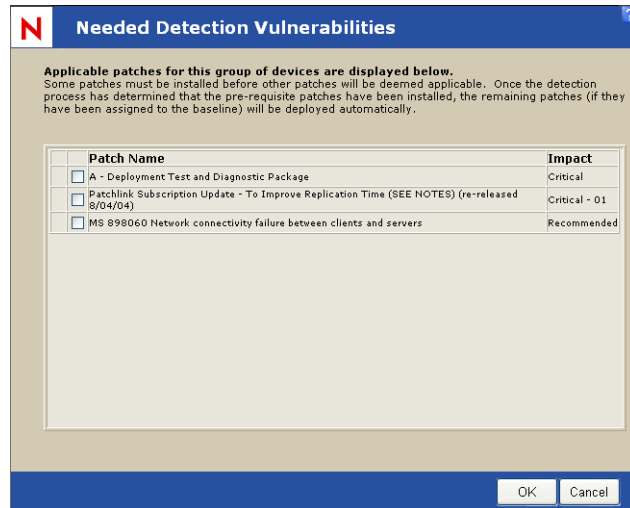


Figure 8.6 Add a Group - Needed Detection Vulnerabilities

- d. Select the vulnerabilities and click **OK**.
The *Needed Detection Vulnerabilities* screen closes returning to the *Selected Vulnerabilities* window.
7. To remove a vulnerability from the baseline
 - a. In the *Selected Vulnerabilities* field, select the vulnerabilities to be removed.
 - b. Click **Remove**. To remove all available vulnerabilities, click **Remove All**. The selected vulnerabilities are removed from the *Selected Vulnerabilities* field.
8. In the **Deployment Options** drop-down list, select a deployment type
 - **Auto QChain with Manual Reboots** - Automatically sets all possible vulnerabilities to deploy with QChain enabled. When a reboot is required the agent will remain in a 'dirty state' until you perform a reboot
 - **Auto QChain with Automatic Reboots** - Automatically sets all possible vulnerabilities to deploy with QChain enabled. All necessary reboots are performed automatically



- **Standard - Set Individually** - Uses the QChain and reboot settings as defined for each vulnerability



Note: If the Deployment is not QChainable and the reboot is suppressed then the agent will be in the *Dirty R* state. Agents in the Dirty R state will only accept one of the reboot deployments. Therefore, for uninterrupted mandatory baseline patching, be sure not to select the without reboot option. You should also ensure there are no patches in the baseline that require a login after patch installation.

9. To modify the deployment options for each individual vulnerability, click that vulnerabilities associated Options button
Refer to “[To Set Package Deployment Options](#)” for details regarding the Package Deployment Options page.
10. Click **OK**.
The new group information is saved and the system opens the *Group Details page*.

To Set Package Deployment Options

1. Select a vulnerability in the list of Selected Vulnerabilities and click **Options**. The *Package Deployment Options* page opens.

Package Deployment Options

Deployment Options For: Win95, Win98, WinME, WinNT, Win2K

Deployment Test and Diagnostic Package -- Windows

Distribution Options

☒ Concurrent Deploy to 25 devices at a time.

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

Deployment Flags

Optional Flags:

Deployment Options

☐ Do not notify users of this deployment.

☒ Notify users of this deployment.

Message: (Maximum 1000 characters)

Deployment of: Deployment Test and Diagnostic Package -- Windows

936 characters left.

☐ Use Policies

Options	Use Agent Policy	Setting
Allow user to cancel	<input type="checkbox"/>	No
Allow user to snooze	<input checked="" type="checkbox"/>	Yes
Notification on top	<input type="checkbox"/>	No
Deploy within	<input type="checkbox"/>	5 Minutes

Reboot Options

☐ Do not notify users of this reboot.

☒ Notify users of this reboot.

Message: (Maximum 1000 characters)

Requires a reboot to complete installation.

875 characters left.

☐ Use Policies

Options	Use Agent Policy	Setting
Allow user to cancel	<input type="checkbox"/>	Yes
Allow user to snooze	<input checked="" type="checkbox"/>	Yes
Reboot within	<input type="checkbox"/>	5 Minutes

OK Cancel

Figure 8.7 Package Deployment Options screen

2. In *Distribution Options*, select one of the following options:
 - **Concurrent** and the **device amount** - instructs the deployment to install patches in priority order
 - **Consecutive** - installs all patches at the same time
3. If needed, modify the existing, or add additional, **Deployment Flags**
4. Set the desired **Deployment Options** and **Reboot Options**.
 - Refer to the “[Notification Options Page](#)” on page 106 for additional details regarding the Deployment and Reboot Options



- 5. Click **OK**.
The *Package Deployment Options* screen closes
- 6. Repeat this procedure for any other vulnerabilities

Removing Deployments Created By Mandatory Baselines

To stop a patch that has been initiated by a mandatory baseline, open the *Group Details* page for the relative group and select the **Deployments** tab.

- 1. Remove the vulnerability from the mandatory baseline
Refer to “[Managing a Mandatory Baseline](#)” on page 179 for details.



Warning: You must make sure to remove the vulnerability from the mandatory baseline which created the deployment or the deployment will be recreated.

- 2. On the *Group Details* page, select the **Deployments** tab
- 3. Select the checkbox associated with the group deployment(s) you wish to stop
- 4. Click **Delete**

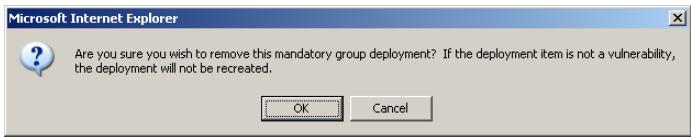


Figure 8.8 Remove Deployment

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

To Stop Deployment for Specific Devices

- 1. On the *Group Details* page, select the **Deployments** tab
- 2. Click the appropriate **Name** link, opening the **Deployment Details** page
- 3. Select the computer(s) for which you wish to stop the deployment
- 4. Click **Disable** to disable the deployment for the selected computer



Exporting Baseline Information

Mandatory baseline 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.

For more information on exporting data, see “[Exporting Data](#)”.

Scanning Data

Scanning reschedules the Discover Applicable Updates System Task (DAU) for immediate execution. The DAU runs on a predefined interval schedule. Enacting a scan manually schedules the task for immediate execution. The **Scan Now** command results in the same action regardless of the current page.



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.

To Scan Devices

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.

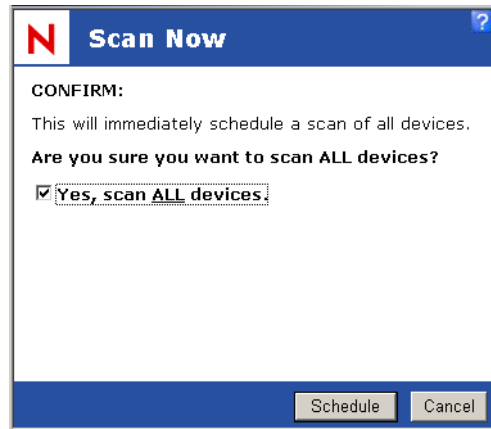


Figure 8.9 Scan Devices





Warning: Scheduling a DAU entails creating traffic for all the selected devices.

- 3. Select **Yes, scan the selected device** and click **Schedule**.
Scan Now - Success dialog box appears informing you that the scan has been processed and providing a link to view the results of the DAU deployment.

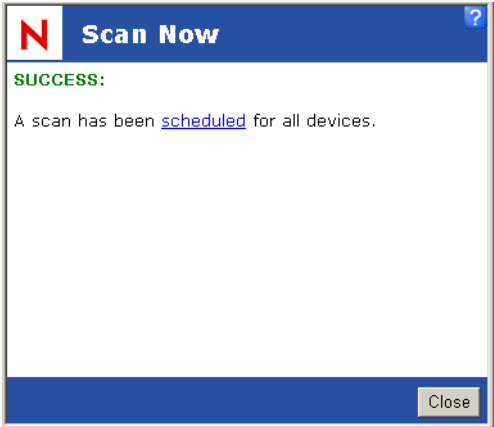


Figure 8.10 Scan Group Scheduled

- 4. Click **Close**.
The system closes the window.



Using Update Cache

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

To Cache Vulnerability Data

1. In the *Vulnerabilities* list, select one or multiple vulnerabilities.
2. In the *Action* menu, click **Update Cache**. The *Warning* dialog box opens prompting you to confirm the update request and informing you that this action may take an extended period of time.
3. Click **OK**

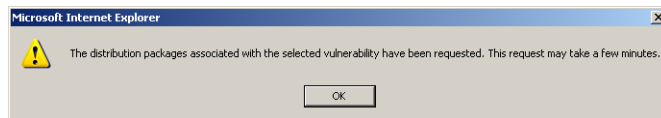


Figure 8.11 Update Cache - Warning dialog box





9 Reporting

This chapter provides information on defining and generating reports in ZENworks Patch Management. Reports provide you a means to capture the status of the organization's current patch status and network vulnerability for internal reporting and briefing management.

In this Chapter

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

About Reports

Reports cover a range of key 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. The following are the report-related Web pages in the application:

- **Available Reports Page** - the main page from which you select a report output from a list of available reports.

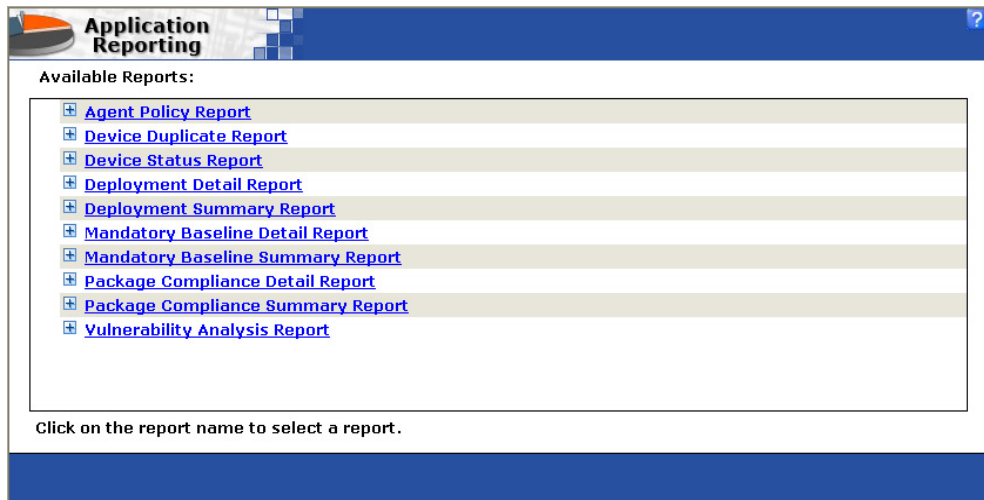



Figure 9.1 Available Reports



- **Report Parameters Page** - the report definition page where you define the data to include in the report. The ID number for the report type is represented in the Web page address (URL) and indicates the specific report type ID.

**Application Reporting**

Agent Policy Report Parameters:

Parameters

Computers

Groups

Search:

Update List

Available Groups

AIX
ALTestGroup
BAH Series 1
BAH Series 2

⬆ ⬇

⬇ ⬆


Selected Groups

Total Selected

Click on each Parameter to specify data to use for the Report. If no selection is made, all data available for the report will be returned.

Figure 9.2 Report Parameters Page

- **Reports Results Page** - this report output that presents the results of the report generation. The ID number for the report type is represented in the Web page address (URL) and indicates the specific report type ID.

**Application Reporting**

Deployment Detail Report

Report created: 4/5/2006 4:58:34

Deployment Name	Vulnerability Name	Computer Name	Deployment Status	Deployment Date	Install Date	Vulnerability Status	Date Last Verified
Deployment of MS04-040 889293 (NT) Cumulative Security Update for IE 6.0 SP1-a	MS04-040 889293 Cumulative Security Update for IE 6.0 SP1	\\CALENDAR-SPARE	Not Started	12/22/2005 11:03:27 AM	12/22/2005 11:03:27 AM	Not Patched	4/11/20 4:52:13
Deployment of MS04-040 889293 (NT) Cumulative Security Update for IE 6.0 SP1-a	MS04-040 889293 Cumulative Security Update for IE 6.0 SP1	\\JOTS99	Not Started	12/22/2005 11:03:27 AM	12/22/2005 11:03:27 AM	Not Patched	4/11/20 7:25:15
Deployment of MS04-040 889293 (NT) Cumulative Security Update for IE 6.0 SP1-a	MS04-040 889293 Cumulative Security Update for IE 6.0 SP1	\\NCILAB	Not Started	12/22/2005 11:03:27 AM	12/22/2005 11:03:27 AM	Not Patched	4/11/20 7:25:19
Deployment of MS04-040 889293 (NT) Cumulative Security Update for IE 6.0 SP1-a	MS04-040 889293 Cumulative Security Update for IE 6.0 SP1	\\BNS-NNM	Not Started	12/22/2005 11:03:27 AM	12/22/2005 11:03:27 AM	Not Patched	3/9/200 2:34:32
Deployment of MS04-040 889293 (NT) Cumulative Security Update for IE 6.0 SP1-a	MS04-040 889293 Cumulative Security Update for IE 6.0 SP1	\\KALIMANTAN	Not Started	12/22/2005 11:03:27 AM	12/22/2005 11:03:27 AM	Not Patched	4/7/200 7:37:16

Display 700 Results per page

Figure 9.3 Report Page



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.
2. Select the report to generate in the *Available Reports* page.
The corresponding *Report Parameters* page opens.
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 and organization from the list of available parameters. This is the left-side pane of the page.
 - b. In the *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. Or, to include all available items, click the **Include All** arrow.
5. Verify the contents of the *Selected Options* box. Remove items by clicking the **Remove** or **Remove All** arrows.
6. Click **Generate** to create the report.
The *Report Results* screen opens with the retrieved information.



Available 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. In many cases, you will find both a *detailed* and *summary* report for a specific activity (for example; deployment, mandatory baseline, package compliance).

The following reports are available:

- “Agent Policy Report”
- “Device Duplicate Report”
- “Device Status Report”
- “Detection Results Not Found Report”
- “Deployment Detail Report”
- “Deployment Error Report”
- “Deployment In-Progress Report”
- “Deployment Summary Report”
- “Mandatory Baseline Detail Report”
- “Mandatory Baseline Summary Report”
- “Package Compliance Detail Report”
- “Package Compliance Summary Report”
- “Vulnerability Analysis Report”

Report Descriptions

Agent Policy Report

Available Parameters: Device, Group

The Agent Policy Report returns a list of all policies associated with a selected group or devices(s) associated with a group. The report lists the current value and description of each policy associated with the selected device(s), if you selected groups, each device associated to the selected group.

In the report, each policy value is listed in the *Policy Name* column. A single device is assigned a policy set, which can comprise multiple policy values depending on the definition of the policy set. As such, a policy name is defined as a single value assigned to the policy set. The values included in the report are defined as follows:

- Device Name
- Policy Name
- Current Value
- Policy Description



Device Duplicate Report

Available Parameters: Date Range

The Device Duplicate Report returns a list of devices that are identified by an installed agent multiple times. This is usually the result of employing the *Agent Uniqueness* feature that permits an agent installed on ghost images to register multiple times with Patch Management Server.

In the report, each agent is listed in the *Agent Name* column. The report lists each agent name occurring during the selected date range and the status and installation date of the agent. The values included in the report are defined as follows:

- Agent Name
- Status
- Install Date

Device Status Report

Available Parameters: Device, Group

The Device Status Report returns the current state of remediation for a specified device, list of devices, devices in a group, or devices in a list of groups.

In the report, each device is listed in the *Device Name* column. The report then provides information about the particular device. The values included in the report are defined as follows:

- Device Name
- DNS Name
- IP Address
- Operating System Name
- OS Build No.
- Service Pack
- Agent Version
- Last Contact Date
- Patchable Status
- Group List



Detection Results Not Found Report

Available Parameters: Device, Group

The Detection Results Not Found Report returns a list of devices that have no detection (DAU) results.

In the report, each agent is listed in the *Agent Name* column. The report lists each agent name, the installation date of the agent, and information required to identify and locate the device. The values included in the report are defined as follows:

- Agent Name
- OS Abbr Name
- Agent Version
- Last Contact Date
- Installation Date
- IP Address
- DNS Name
- OS Info

Deployment Detail Report

Available Parameters: Deployments, Vulnerabilities, Date Range

The Deployment Detail Report provides information about a selected list of deployments. You can report on each deployment, vulnerability, or generate a report based on a specific date range.

In the report, each device is listed in the *Deployment Name* column. The report then provides information as to the status of the particular deployment activity. The values included in the report are defined as follows:

- Deployment Name
- Vulnerability Name
- Device Name
- Deployment Status
- Deployment Date
- Install Date
- Vulnerability Status
- Date Last Verified



Note: If a selected Vulnerability has no 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 had an error. You can report on each deployment, package, Device, or date range.

In the report, each deployment with an error is listed in the *Deployment Name* column. The report then provides information as to the status of the deployment. The values included in the report are defined as follows:

- Deployment Status
- Status Code
- Error Message
- Install Date
- Package Name
- Deployment Name
- Device Name

Deployment In-Progress Report

Available Parameters: Deployments, Packages, Devices, Groups

The Deployment In-Progress Report provides information about a deployments that have not completed. You can report on each deployment, package, device, or generate a report based on a specific date range.

In the report, each deployment is listed in the *Deployment Name* column. The report then provides information as to the status of the deployment. The values in the report are defined as follows:

- Deployment Name
- Package Name
- Total Deployed
- Already Patched
- Not Applicable
- Total Successful
- Total In-Progress
- Not Started
- Caching Package
- Total Failed
- Total Disabled
- Percent Success
- Percent Failure



Deployment Summary Report

Available Parameters: Deployments, Vulnerabilities, Date Range

The Deployment Summary Report provides information about a selected list of deployments. You can report on each deployment, vulnerability, or generate a report based on a specific date range.

In the report, each device is listed in the *Deployment Name* column. The report then provides information as to the status of the particular deployment activity. The values included in the report are defined as follows:

- Deployment Name
- Vulnerability Name
- Total Deployed
- Total Successful
- Total InProgress
- Total Failed
- Total Disabled
- Total Patched
- Percent Success
- Percent Failure



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 a selected list of devices and the status of the mandatory baseline package and deployment status associated with each device.

In the report, each device is listed in the *Device Name* column. The report then provides detailed information as to the group, package, and deployment status for each device. The values included in the report are defined as follows:

- Device Name
- Group Name
- Package Name
- Vulnerability Status
- Deployment Status
- Package Release Date
- Date Deployed
- Date Installed
- Date Last Verified

Mandatory Baseline Summary Report

Available Parameters: Devices, Groups

The Mandatory Baseline Summary Report provides information about a selected list of packages that have been designated as representing baseline packages. A mandatory baseline is the set of packages identified as representing the core package requirements for each device or group.

In the report, each package is listed in the *Package Name* column. The report then provides summary information as to the compliance status for each package; telling you the associated status, and deployment details. The values included in the report are defined as follows:

- Package Name
- Total Deployed
- Total Successful
- Total InProgress
- Total Failed
- Percent Success
- Percent Failure



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 and device. The report identifies the compliance status for the any of the specified packages, or for any package deployed to a specified device or group.

The report lists each package associated with one of the selected device(s) or group(s). As well, you can elect to generate the report based on a single package or group of packages, independent of any association to a device.

In the report, each package is listed in the *Package Name* column. The report then provides details as to the compliance status for each package; telling you the associated device, status, and deployment details. The values included in the report are defined as follows:

- Package Name
- Device Name
- Vulnerability Status
- Data Last Verified
- Deployment Name
- Deployment Status
- Package Release Date
- Date Deployed
- Date Installed
- Date Scheduled



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 provides a summary of the patch and deployment status for a specific package. The report identifies the compliance status for the any of the specified packages on any device. The report lists each package that impacts one of the selected device(s) or group(s). As well, you can elect to generate the report based on a single package or group of packages.

In the report, each package is listed in the *Package Name* column. The report then provides details as to the compliance status for each package; telling you how many devices are impacted and how many require or do not require deployment of the patch. The values included in the report are defined as follows:

- Package Name
- Total Devices
- Applicable Devices
- Devices Detecting
- Devices Patched
- Not Patched/Not Scheduled
- Not Patched/Scheduled
- Deployments Completed
- Deployments Failed
- Deployments In-Progress



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 specified vulnerabilities identified by the system. The report lists each vulnerability that impacts one of the selected device(s) or group(s). As well, you can elect to generate the report based on a single vulnerability or group of vulnerabilities (for example, from a single vendor or for a specific software program).

In the report, each vulnerability is listed in the *Vulnerability Name* column. The report then provides details as to the remediation status (patch status) for each vulnerability; telling you how many devices are impacted and how many require or do not require deployment of the patch. The values included in the report are defined as follows:

- Vulnerability Name
- Vulnerability Release Date
- Total Devices
- Applicable Devices
- Devices Detecting
- Devices Patched
- Not Patched
- Pct Patched



Note: If a selected Vulnerability has no associated deployment, it will not appear in the report.

Report Parameters

Targeted reporting is accomplished through defining the report parameters (options) that determine how to display and organize information provided in each report. This is accomplished by selecting report parameters that determine how the report is to be constructed; whether by device, package or other means, including date.

While the following parameters are available for all reports, not every report will use each parameter.

Table 9.1 Report Parameters

Parameter	Function
Devices	Select Devices to choose from a list of all available devices registered by the ZENworks Patch Management Agent. All available devices are shown in the <i>Available Data</i> list. Click a single device or use the <code>CTRL</code> and <code>SHIFT</code> keys to select multiple devices.
Groups	Select Groups to choose from a list of all available groups created in Patch Management Server. All groups are shown in the <i>Available Data</i> list and any devices belonging to the selected group are included in the report. Click a single group or use the <code>CTRL</code> and <code>SHIFT</code> keys to select multiple groups.
Deployments	Select Deployments to choose a deployment from a list of all available deployment names. All available deployments are shown in the <i>Available Data</i> list. Click a single deployment or use the <code>CTRL</code> and <code>SHIFT</code> keys to select multiple deployments.
Packages	Select Packages to choose from a list of all available packages. All available packages are shown in the <i>Available Data</i> list. Click a package name or use the <code>CTRL</code> and <code>SHIFT</code> keys to select multiple packages.
Vulnerabilities	Select Vulnerabilities to choose from a list of all available vulnerabilities identified by Patch Management Server. All vulnerabilities are shown in the <i>Available Data</i> list. Click a vulnerability name or use the <code>CTRL</code> and <code>SHIFT</code> keys to select multiple vulnerabilities.
Date Range	Select Date Range to 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.



Working with Reports

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

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

Searching and Updating Reports

The Search feature assists in reporting by providing a specific, range of items (parameters).

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 search 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).

If you want to narrow the list down to only vulnerabilities by vendor, enter the vendor name as the search term. To produce results for only machines running Linux operating system, enter Linux as the search term. You can apply this to devices, groups, vulnerability, or package name, depending on the parameter being defined in the report.

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 display 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 Update 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 options of switching to a printable view for printing, or exporting the report into another file format. As well, you can modify the time/date display for each report.



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

Viewing Printable Data in Reports

An HTML version of the generated report can be previewed for printing.

To Print a Report

1. On the *Report Results* page, select **View Printable**
The Report Results page refreshes with the data in print preview mode.
2. Select **File > Print**
The file is sent to the printer.





10 Managing Users and Roles

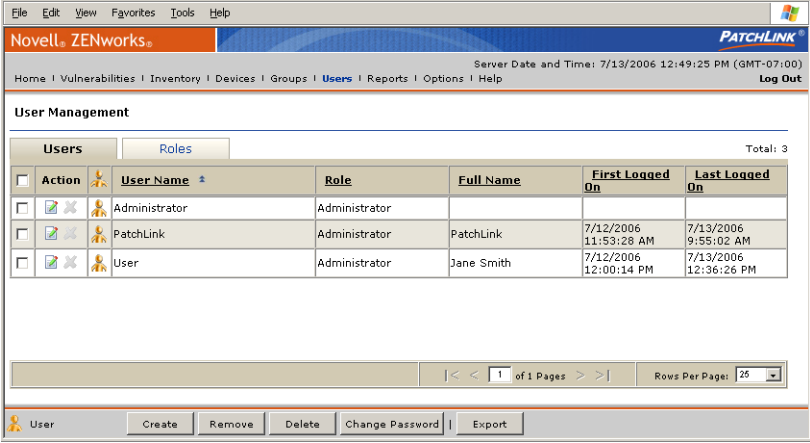
This chapter provides information on managing users of the ZENworks Patch Management Server. The user management features allow you create credentials for users of the system and define permissions for each user.

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 manage which users can access the ZENworks Patch Management Server and the role each user has within the system. Roles define the access rights that each user has as well as the device groups and devices that the user has control.



Action	User Name	Role	Full Name	First Logged On	Last Logged On
<input type="checkbox"/>	Administrator	Administrator			
<input type="checkbox"/>	PatchLink	Administrator	PatchLink	7/12/2006 11:53:28 AM	7/13/2006 9:55:02 AM
<input type="checkbox"/>	User	Administrator	Jane Smith	7/12/2006 12:00:14 PM	7/13/2006 12:36:26 PM

Total: 3

1 of 1 Pages Rows Per Page: 25

User Create Remove Delete Change Password Export

Figure 10.1 User Management View



Viewing Users

To View Users

1. 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 two mechanisms:

- “Windows-based Authentication”
- “ZENworks Patch Management Access Rights”

Windows-based Authentication

Windows-based Authentication

ZENworks Patch Management authentication is controlled by the Windows operating system. Any users who are members of the local Windows group *PLUS Admins* will have access.

ZENworks Patch Management Access Rights

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, they will be given an access denied error message.

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 are defined as individuals (John Smith) or conceptual users (Quality Assurance Manager). As you define a user profile you provide not only the credentials (user name and password) that permit the user to sign in to the system but you also define the role to associate with the user.



Note: A user can only be assigned a single role; while a role may encompass many users.

There are two methods of bringing users into the system: creating users and adding users

Creating New Users

Creating a user allows you to create a new local machine user and provide them with access to ZENworks Patch Management. The end result is that the new user is added as a Windows user and added to the ZENworks Patch Management database. Using this method, ZENworks Patch Management not only adds the user to the ZENworks Patch Management Server but also updates the Windows user accounts security database. For example, if the user was given access to a user role which has the **Manage Users** access right, they will also be added to the Windows administrators group on the local ZENworks Patch Management Server computer.

Adding Existing Windows Users

Adding a user allows you to give an existing Windows user access to ZENworks Patch Management. Using this method, Patch Management Server generates a list of Windows users and allows you to select a user from that list to be added to the ZENworks Patch Management database and access group.

If the user was given access to a user role which has the **Manage Users** access right, they will also be added to the Windows administrators group on the local ZENworks Patch Management Server computer.



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 two types of roles: system and custom. System roles are roles native to every installation and cannot be edited or disabled. Custom roles are created by the ZENworks Patch Management Server administrator. System roles allow control over all device groups and devices. Custom roles allow you to define any combination of access rights and selected devices or device groups for a particular user.



Note: See “[Defining Access Rights](#)” on page 209 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 that the user is permitted to act upon.

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 roles to the user ‘as is’ across the board, 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 10.1 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 (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 view the defined devices/groups and 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 customized. In this sense, 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 10.2 User Role Access Rights

Access Right Name	Description	Administrator	Manager	Operator	Guest
Cache Packages	Permits caching (or re-cache) of distribution packages from the Global Subscription Server.	X	X		
View Computers	Access the <i>Computers</i> page.	X	X	X	X
Export Computer Data	Save computer data to CSV file format.	X	X	X	
Install Computers	Access the <i>Agent Installers</i> page.	X	X		
Manage Computers	Conduct computer administration tasks, including: enable, disable, remove, etc.	X	X		
View Deployments	Access the <i>Deployments</i> page.	X	X	X	X
Manage Deployments	Conduct deployment administration tasks, including; enable, disable, abort, change, remove, etc.	X	X	X	
View Deployment Results	Access the <i>Deployments Results</i> page.	X	X	X	X
Export Deployment Data	Save deployment data to CSV file format.	X	X	X	
View Groups	Access the <i>Groups</i> page.	X	X	X	X
Export Group Data	Save group data to CSV file format.	X	X	X	



Table 10.2 User Role Access Rights

Access Right Name	Description	Administrator	Manager	Operator	Guest
Manage Groups	Conduct group administration tasks.	X	X		
View Home Page	Access the <i>Home</i> page.	X	X	X	X
View Patch Management Server Status	Display the current ZENworks Patch Management status on the <i>Home</i> page.	X	X	X	X
View OS Inventories	Access the <i>Inventory > OS</i> page.	X	X	X	X
Export Inventory Data	Save inventory data to CSV file format.	X	X	X	
View Hardware Inventories	Access the <i>Inventory > Hardware</i> page.	X	X	X	X
Manage Hardware Group Locks	Lock and unlock the detected hardware for selected groups. This permits the control of displayed data to only when viewing hardware inventory by group membership. Receive e-mail notifications are sent when lock goes in and out of compliance.	X	X		
View Service Inventories	Access the <i>Inventory > Services</i> page.	X	X	X	X
Manage Services Group Locks	Lock and unlock the detected services for selected groups. This permits the control of displayed data to only when viewing hardware services by group membership. Receive e-mail notifications are sent when lock goes in and out of compliance.	X	X		
View Software Inventories	Access the <i>Inventory > Software</i> page.	X	X	X	X
Manage Software Group Locks	Lock and unlock the detected software applications for selected groups. This permits the control of displayed data to only when viewing software by group membership. Receive e-mail notifications are sent when lock goes in and out of compliance.	X	X		
Manage Options: Licenses	Conduct license administration tasks.	X			
View Options: Support Info	Access the <i>Options > Support</i> page.	X	X	X	X
Export Support Data	Save support information to CSV file format.	X	X	X	
View Options: Policies	Access the <i>Options > Agent Policy Sets</i> page.	X	X	X	X



Table 10.2 User Role Access Rights

Access Right Name	Description	Administrator	Manager	Operator	Guest
Export Agent Policies Sets Data	Save agent policy data to CSV file format.	X	X		
View Options: Defaults	Access <i>Options > Patch Management Server Defaults</i> page.	X	X	X	X
Export Defaults Data	Save export defaults data to CSV file format.	X	X		
View Options: E-mail	Access the <i>Options > E-Mail Notification</i> page.	X	X	X	X
Export E-mail Notification Data	Save export e-mail notification data to CSV file format.	X	X		
View Options: Licenses	Access the <i>Options > License</i> page.	X	X	X	X
Export License Data	Save license data to CSV file format.	X	X		
Manage Options	Conduct all options administrative tasks, including: subscriptions, default policy settings, agent policy sets, alerts, and support management.	X			
View Options: Subscription	Access the <i>Options > Subscription Information</i> page.	X	X	X	X
Export Subscription Data	Export subscription data to CSV file format.	X	X		
View Packages	Access the <i>Packages</i> page.	X	X	X	X
Deploy Packages	Create deployments based on distribution packages.	X	X	X	
Export Package Data	Save export package data to CSV file format.	X	X	X	
Manage Packages	Conduct package administration, including: adding, removing, etc.	X	X		
Reboot Now	Authorization to initiate a reboot of computers (all or selected). Enables the <i>Reboot Now</i> button within the application.	X			
View Vulnerabilities	Access the <i>Vulnerability</i> page.	X	X	X	X
Deploy Vulnerabilities	Create vulnerability-based deployments.	X	X	X	
View Vulnerability Results	Access <i>Vulnerability Analysis Results</i> page.	X	X	X	X
Export Vulnerability Data	Save vulnerability data to CSV file format.	X	X	X	



Table 10.2 User Role Access Rights

Access Right Name	Description	Administrator	Manager	Operator	Guest
Change Vulnerability Filter	Modify the <i>Vulnerabilities</i> page filter settings.	X	X	X	X
Manage Group Vulnerability Locks	Lock and unlock group-based analysis results for selected vulnerabilities. This permits the control of displayed data to only when viewing vulnerabilities by group membership. Access the <i>Vulnerabilities Lock Compliance</i> page and receive e-mail notifications are sent when lock goes in and out of compliance.	X	X		
Manage Vulnerabilities	Conduct vulnerability administration for analysis results.	X	X		
Manage Vulnerability UI Locks	Lock and unlock analysis results totals for selected vulnerabilities. This permits the control of displayed data to only when viewing vulnerabilities for all computers.	X	X		
Manage Administrative Reports	Create and define reports based on data from all computers and groups regardless of user role, computer, and group assignments.	X			
Manage User Based Reports	Create and define reports based on data from computers and groups assigned to a defined user.	X	X	X	X
Manage System Tasks	Conduct ZENworks Patch Management system task administration, including: discovery and analysis process, refresh data, etc.	X	X	X	
View Users	Access the <i>Users</i> page.	X	X	X	X
Export User Data	Save user data to CSV file format.	X	X		
Manage Users	Conduct user administration, including: adding, editing, removing, and other administrative functions.	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 limit the control that a user is permitted 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 the control over the system granted a user 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 Users 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 ZENworks Patch Management 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**

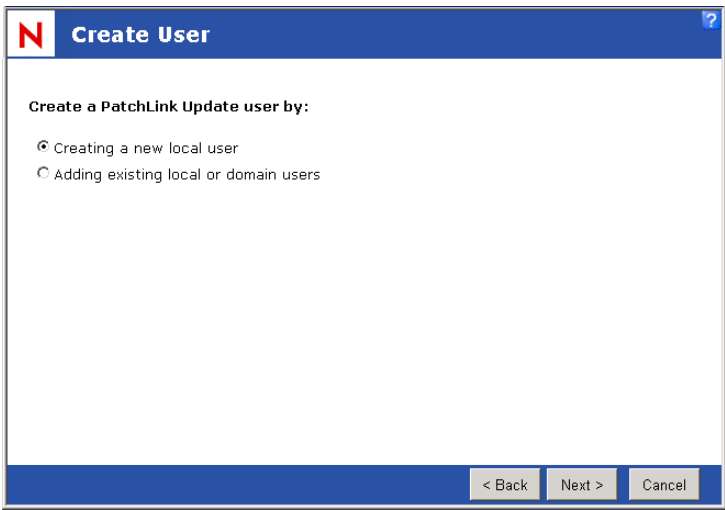


Figure 10.2 Create User Wizard - Create or Add User page



4. Enter the user credentials, contact information and select a role for the new user



Warning: **User Name**, **Password**, **Confirm Password**, and **Role** are required fields.

User Name 1-20 characters, may include any characters (spaces)

Password 7-20 characters, may include alpha, numeric, special characters; not case sensitive; must meet password rules defined by local and/or domain password policies

Office Phone, **Cell Phone**, **Pager**, and **E-mail** fields are not validated and apply no formatting rules other than max. characters (25)

5. Click **Next**
6. Confirm the user information and click **Close**
7. Verify the status information and click **Close**

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



Warning: If you add domain users to ZENworks Patch Management, there must be a trust between that domain and the ZENworks Patch Management Servers domain, or the users will be unable to access Patch Management Server.

3. Click **Next**
4. In the **Search for the following users** field type a user name, or the beginning characters of one or more user names



Note: Use semicolons to separate user names. To search for users within a specific domain, prefix the user name with the domain (DOMAINNAME\UserName). If desired, you can provide a Domain, User Name, and Password to access a domain directory.



- 5. Click **Next**
The *Users Found* page displays

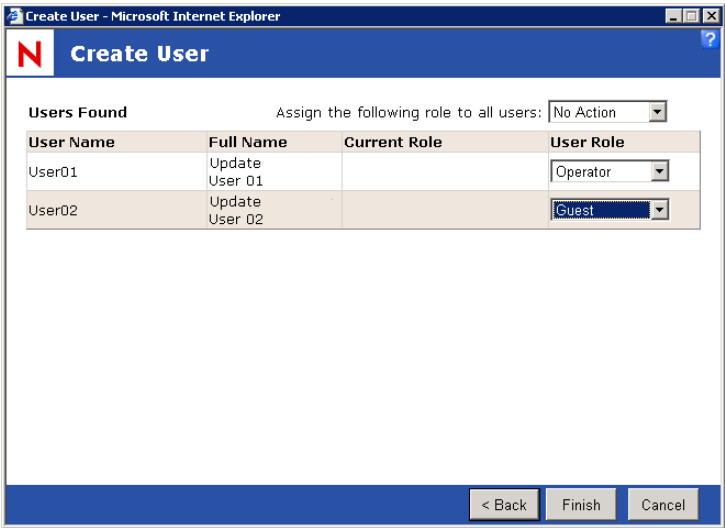


Figure 10.3 Add User Wizard - Assign Role page

- 6. Select a **User Role** for each of the users found (No action 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**
- 8. Verify the Summary data and click **Close**

Editing User Profiles

Editing user profile information allows you to change the role assigned to a user as well as update contact information. You cannot edit the user credentials (user name and password). This is because authentication in Patch Management Server is conducted through the Windows operating system (applies to both Created and Added users).



To Edit user Profile Information

1. In the *User Management* details area, click the **Edit** icon associated with the user profile to edit
The *Edit User Wizard* opens

Figure 10.4 Edit User Wizard - User Information page

2. Make the necessary modifications as defined in “[Creating New Users](#)” on page 214, exiting 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. You must edit the user, changing the users role, then remove or delete the user.

To Remove a User

1. In the Patch Management Server main menu, click **Users**
2. On the *User Management* page, select the checkbox for the user profile to remove
 - You may select multiple users for removal
3. Click **Remove**



4. Acknowledge the *Warning* by clicking **OK**

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. On the Patch Management Server main menu, click **Users**
2. On the *User Management* page, select the checkbox for the user profile to remove
 - You may select multiple users for removal
3. Click **Delete**
4. Acknowledge the *Warning* by clicking **OK**
5. In the *Confirmation* dialog box, click **OK**

Changing a Users Password

Changing a Users Password in ZENworks Patch Management also changes the password for the associated local user on the ZENworks Patch Management Server.

To Change a User Password

1. On the Patch Management Server main menu, select **Users**
The *User Management* window opens
2. Select the user requiring the password change.
3. Click **Change Password**
The **Change Password Wizard** opens.
4. In the *Welcome* dialog box, click **Next**
5. 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.



The screenshot shows a 'Change Password' dialog box. At the top, there's a blue header with a red 'N' icon and the text 'Change Password'. Below the header, it says 'Change password for : TechPubs'. There are four labeled fields: 'User Name:' with the value 'TechPubs', 'New Password:' with a masked input (dots), 'Confirm Password:' with an empty input, and 'Password Strength:' with a red bar and the word 'Weak'. At the bottom, there's a blue footer with the 'RSA BSAFE' logo on the left and 'Finish' and 'Cancel' buttons on the right.

Figure 10.5 Weak Password Indicator



- 6. When the *Password Strength* indicator displays the acceptable password strength, retype the password in the *Confirm Password* field.

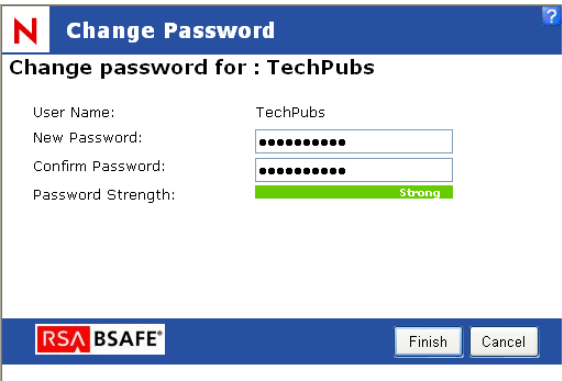


Figure 10.6 Confirm for Strong Password

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.

- 7. 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” on page 16.



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 implement group and device access levels to a role.

To Create a Role

1. In the *Users* page, select the **Roles** tab

The screenshot shows the Novell ZENworks Patch Management Server interface. The top navigation bar includes links for Home, Vulnerabilities, Inventory, Devices, Groups, Users, Reports, Options, and Help. The main content area is titled "User Management: All User Roles" and includes a status dropdown set to "All" and checkboxes for "Show results automatically" and "Save as Default View". Below this is a tabbed interface with "Users" and "Roles" tabs. The "Roles" tab is active, displaying a table with columns: Action, User Role Name, Type, Access Rights, Users, Groups, and Devices. The table lists two roles: "Administrator" (System type, 46 Access Rights, 3 Users, 13 Groups, 13 Devices) and "Manager" (System type, 40 Access Rights, 0 Users, 0 Groups, 13 Devices).

Action	User Role Name	Type	Access Rights	Users	Groups	Devices
	Administrator	System	46	3	13	13
	Manager	System	40	0	0	13

Figure 10.7 User Management - Roles tab



2. Click Create

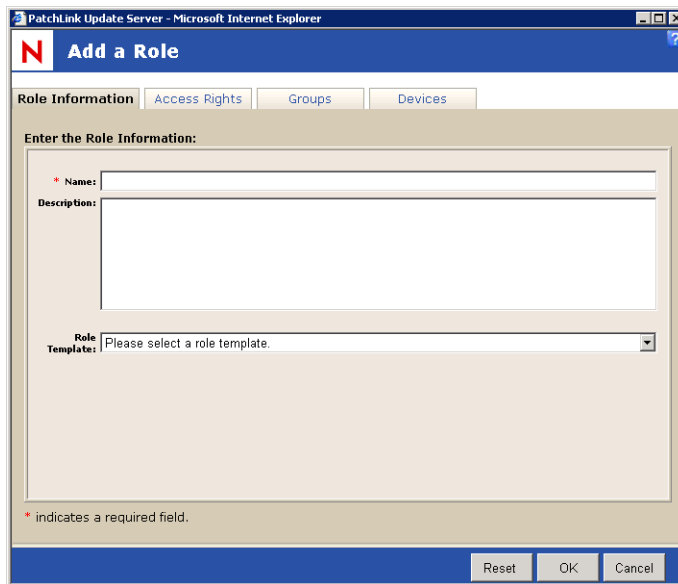
The screenshot shows a web browser window titled "PatchLink Update Server - Microsoft Internet Explorer". The main content area is a form titled "Add a Role" with a blue header bar. Below the header, there are four tabs: "Role Information" (selected), "Access Rights", "Groups", and "Devices". The "Role Information" tab contains the following fields: a text box for "Name" with a red asterisk indicating it is required, a larger text box for "Description", and a dropdown menu for "Role Template" with the text "Please select a role template." below it. At the bottom of the form, there is a note: "* indicates a required field." and three buttons: "Reset", "OK", and "Cancel".

Figure 10.8 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

- Assign access rights by selecting the checkbox to the left of each access right and clicking **Assign** to move them into the *Selected Access Rights* table (**Assign All** will move all access rights from the *Access Rights* table to the *Selected Access Rights* table)
- Remove access rights by selecting the checkbox to the left of each access right and clicking **Remove** to move them to the *Access Rights* table (**Remove All** will move all access rights from the *Selected Access Rights* table to the *Access Rights* table)

5. Select the *Groups* tab, to define which groups the users assigned this role will be able to access

- Assign group access by selecting the checkbox to the left of each group and clicking **Assign** to move them into the *Selected Groups* table (**Assign All** will move all groups from the *Groups* table to the *Selected Groups* table)

- Remove group access by selecting the checkbox to the left of each group and clicking **Remove** to move them to the *Groups* table (**Remove All** will move all groups from the *Selected Groups* table to the *Groups* table)



Note: Granting access to a *Device Group* will also grants permission to all of the devices within that group, regardless of the options selected on the *Devices* tab.

- Select the *Devices* tab, to define which Devices the users assigned this role will be able to access
 - Assign specific Device access by selecting the checkbox to the left of each Device and clicking **Assign** to move them into the *Selected Devices* table (**Assign All** will move all Devices from the *Devices* table to the *Selected Devices* table)
 - Remove specific Device access by selecting the checkbox to the left of each Device and clicking **Remove** to move them to the *Devices* table (**Remove All** will move all groups from the *Selected Devices* table to the *Devices* table)
- Click **OK**, saving your changes

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 Role

- In the *Users* page, select the **Roles** tab

Action	User Role Name	Type	Access Rights	Users	Groups	Devices
	Administrator	System	46	3	13	13
	Manager	System	40	0	13	13

Figure 10.9 User Management - Roles tab

- Select role you wish to edit



3. Click **Edit**

The screenshot shows a web-based dialog box titled "Edit a Role" with a blue header bar containing a red "N" logo and a help icon. Below the header are four tabs: "Role Information" (selected), "Access Rights", "Groups", and "Devices". The "Role Information" tab contains a section titled "Enter the Role Information:". Inside this section, there is a text field for "Name:" with the value "TechPubs Role" and an asterisk indicating it is required. Below it is a larger text area for "Description:" containing the text "Technical Publications User Role". At the bottom of the section is a dropdown menu for "Role Template:" with "Custom" selected. A legend at the bottom left states "* indicates a required field." At the bottom right are three buttons: "Reset", "OK", and "Cancel".

Figure 10.10 User Role Wizard - Basic Information tab

4. On the *Role Information* tab, Edit the **Name** or **Description** as desired
5. Select the *Access Rights* tab, to define which rights the users assigned this role will have
 - Assign access rights by selecting the checkbox to the left of each access right and clicking **Assign** to move them into the *Selected Access Rights* table (**Assign All** will move all access rights from the *Access Rights* table to the *Selected Access Rights* table)
 - Remove access rights by selecting the checkbox to the left of each access right and clicking **Remove** to move them to the *Access Rights* table (**Remove All** will move all access rights from the *Selected Access Rights* table to the *Access Rights* table)
6. Select the *Groups* tab, to define which groups the users assigned this role will be able to access
 - Assign group access by selecting the checkbox to the left of each group and clicking **Assign** to move them into the *Selected Groups* table (**Assign All** will move all groups from the *Groups* table to the *Selected Groups* table)
 - Remove group access by selecting the checkbox to the left of each group and clicking **Remove** to move them to the *Groups* table (**Remove All** will move all groups from the *Selected Groups* table to the *Groups* table)



Note: Granting access to a *Device Group* will also grants permission to all of the devices within that group, regardless of the options selected on the *Devices* tab.



7. Select the *Devices* tab, to define which Devices the users assigned this role will be able to access
 - Assign specific Device access by selecting the checkbox to the left of each Device and clicking **Assign** to move them into the *Selected Devices* table (**Assign All** will move all Devices from the *Devices* table to the *Selected Devices* table)
 - Remove specific Device access by selecting the checkbox to the left of each Device and clicking **Remove** to move them to the *Devices* table (**Remove All** will move all groups from the *Selected Devices* table to the *Devices* table)
8. Click **OK**, saving your changes

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

Users		Roles		Total: 6		
<input type="checkbox"/>	Action	User Name *	Role	Full Name	First Logged On	Last Logged On
<input type="checkbox"/>		Administrator	Administrator			
<input type="checkbox"/>		PatchLink	Administrator	PatchLink	3/23/2006 1:14:11 PM	3/28/2006 10:38:36 AM
<input type="checkbox"/>		TechPubs	TechPubs Role	Technical Publications	3/23/2006 3:27:05 PM	3/30/2006 11:21:53 AM
<input type="checkbox"/>		TPublications	Manager	Technical Publications		
<input type="checkbox"/>		User01	Operator	PatchLink Update User 01		
<input type="checkbox"/>		User02	Guest	User 02		
		< 1 of 1 Pages >		Rows Per Page: 25		

Figure 10.11 User Management - Users tab

2. Click **Edit**
3. Edit the user as defined in “[Editing User Profiles](#)” on page 216, changing the role as desired



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. Select the **Roles** tab

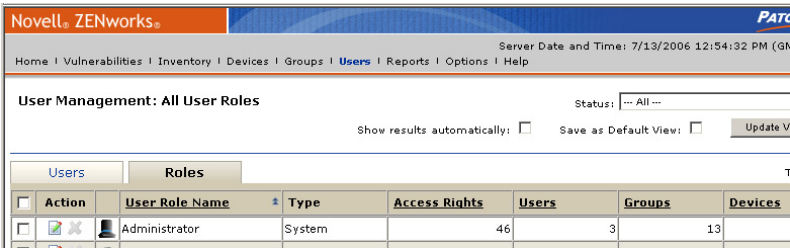


Figure 10.12 User Management - User Roles tab

- 2. Ensure the page filter is not set to *Disabled*
- 3. Click **Update View** to populate the tab
- 4. Select the role or roles to disable
- 5. Click **Disable**



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. Select the **Roles** tab

The screenshot shows the Novell ZENworks PatchLINK User Management interface. The top navigation bar includes links for Home, Vulnerabilities, Inventory, Devices, Groups, **Users**, Reports, Options, and Help. The server date and time are 7/13/2006 12:54:32 PM (GMT-07:00). The main heading is "User Management: All User Roles". Below this, there are checkboxes for "Show results automatically" and "Save as Default View", and an "Update View" button. The "Status" dropdown is set to "All".

The "Roles" tab is selected, displaying a table with the following data:

Action	User Role Name	Type	Access Rights	Users	Groups	Devices
<input type="checkbox"/>	Administrator	System	46	3	13	1
<input type="checkbox"/>	Manager	System	40	0	13	1
<input type="checkbox"/>	Operator	System	28	0	13	1
<input type="checkbox"/>	Guest	System	17	0	13	1

At the bottom of the table, there is a pagination bar showing "1 of 1 Pages" and "Rows Per Page: 25". Below the table, there are buttons for "Create", "Enable", "Disable", "Delete", and "Export".

Figure 10.13 User Management - User Roles tab

2. Ensure the page filter 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**



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. Select the **Roles** tab

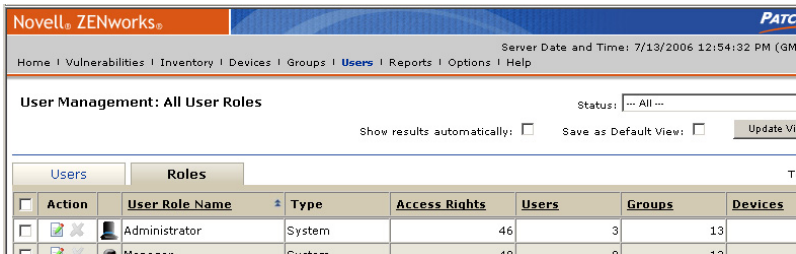


Figure 10.14 User Management - User Roles tab

- 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**



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” on page 16.



11 Configuring Default Behavior

This chapter provides information on configuring and managing ZENworks Patch Management. Configuration options provide you a means to define the default behavior and administer the ZENworks Patch Management Server.

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.

Table 11.1 Options Tabs

Tab	Description
Subscription [Service]	Provides status and a record of activity for the subscription service <ul style="list-style-type: none"> • Refer to “Viewing Subscription Service Information” for additional details regarding the <i>Subscription</i> tab
Products	View ZENworks Patch Management and Plug-In licenses and current usage <ul style="list-style-type: none"> • Refer to “Verifying Subscription Licenses” for additional details regarding the <i>Products</i> tab
[Patch Management Server] Configuration	Manage configuration settings for the ZENworks Patch Management Agents registered to the ZENworks Patch Management Server <ul style="list-style-type: none"> • Refer to “Novell ZENworks Patch Management Default Configuration” for additional details regarding the <i>Configuration</i> tab
Policies	Create custom agent policy sets to configure the ZENworks Patch Management Agents behavior <ul style="list-style-type: none"> • Refer to “Customizing and Administering Agent Policy Sets” for additional details regarding the <i>Policies</i> tab



Table 11.1 Options Tabs

Tab	Description
E-Mail [Notification]	Create, define and manage system alerts <ul style="list-style-type: none">Refer to "Using E-Mail Notification" for additional details regarding the <i>E-Mail</i> tab
[Technical] Support	Detailed system and component information and technical support contact information <ul style="list-style-type: none">Refer to "Technical Support Information" for additional details regarding the <i>Support</i> tab

Viewing Options

To View Options

- 1. Select the *Options* tab.
The *Options* pages displays with the *Subscriptions* 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 update history and status information.
Click **Options** in the tool bar and then click the **Subscription** tab.

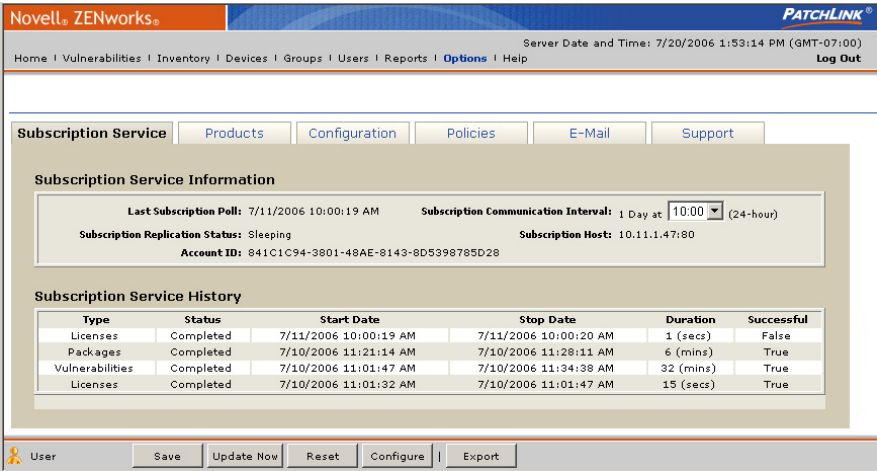


Figure 11.1 Subscription Service Tab



ZENworks Patch Management Agents gather a list of software, hardware, services and patches installed on each agent within your network. With this detailed information, the ZENworks Patch Management Server generates a complete analysis of your agents profile 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 once daily to download a series of vulnerability definitions and packages that ensure the ZENworks Patch Management environment remains current.

Table 11.2 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: There is no intermediate step allowing you to cancel resetting the replication status. Once you click Reset , you will see the dialog box that states 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 .
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" on page 16.

Subscription Service Information

The Subscription Service Information section provides a summary of the configuration settings and status of the subscription service.

- **Last Subscription Poll** - The date and time of the last successful update. The update contacts the Global Subscription Server for update retrieval for the ZENworks Patch Management Server
- **Subscription Replication Status** - The current replication status. Replication ensures that your ZENworks Patch Management Server remains current with the latest vulnerability, package, and license information. This is not the same as the status of individual updates as reported in the history section but rather the current status of the replication process.
- **Account ID** - Key passed to the Global Subscription Server and used to validate the update request. The account key is created by the ZENworks Patch Management Server when it registers with the Global Subscription Server



- **Subscription Communication Interval** - The time frame ZENworks Patch Management Server attempts to connect to the Global Subscription Server and retrieve updates. Unless you click **Update Now** on the *Action Menu*, the update is performed only once daily (at the time indicated in the drop-down list box).



Note: If you modify the *Subscription Communication Interval* you must save the changes by clicking **Save** on the *Action Menu*.

- **Subscription Host** - The URL and port of the Global Subscription Server

Subscription Service History

The Subscription Service History section displays a list of subscription activity and update records.

Table 11.3 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 license• Vulnerabilities - Downloads the current vulnerabilities according to the subscription type defined for your account• Packages - Downloads the current packages, based upon the vulnerabilities you have 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 the downloads comprising the update. When the task is finished, the status reads <i>Completed</i>
Start Date	The date and time that the task started
Stop Date	The date and time that the task completed
Duration	Indicates the duration of the task. This is shown in seconds or minutes and labeled accordingly. For example; <i>19 (secs)</i> , <i>1.22 (mins)</i>
Successful	<i>True</i> indicates the communication was a success and the request was completed. <i>False</i> indicates the request was not successfully completed



Note: To view if the package download was successful, go to the **Home** page, click **Novell ZENworks Patch Management Server Status Page**, and select the **Cache Status** tab.



Subscription Service Configuration

The Subscription Service Configuration page allows you to view the current status and define your Proxy, and Communication settings.

Figure 11.2 Subscription Service Configuration page

Table 11.4 Button Functions

Button	Function
Restart	Stops and restarts the Global Subscription Server
Apply	Saves changes to the database, without closing the Subscription Service Configuration window
Save	Saves any changes to the database, then closes the Subscription Service Configuration window
Cancel	Closes the Subscription Service Configuration window without saving changes



Subscription Service Status

Table 11.5 Subscription Service Status Field Descriptions

Field Name	Description
Service Status	The current status of the Novell Subscription Service
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
Restart	Stops and Restarts the local Novell Subscription Service

Subscription Service Proxy Configuration

Table 11.6 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

Table 11.7 Subscription Service Communication Field Descriptions

Field Name	Description
Logging Level	The level of detail recorded to the Subscription Service Log. Options include: <i>None, Fatal, Error, Warn, Info, and Debug.</i>
Use SSL	This will 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.



Table 11.7 Subscription Service Communication Field Descriptions

Field Name	Description
___ 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.
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.

Verifying Subscription Licenses

The *Products* page allows you to view, validate and export license information. As well, 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.

Click **Options** in the tool bar and then click the **Products** tab.

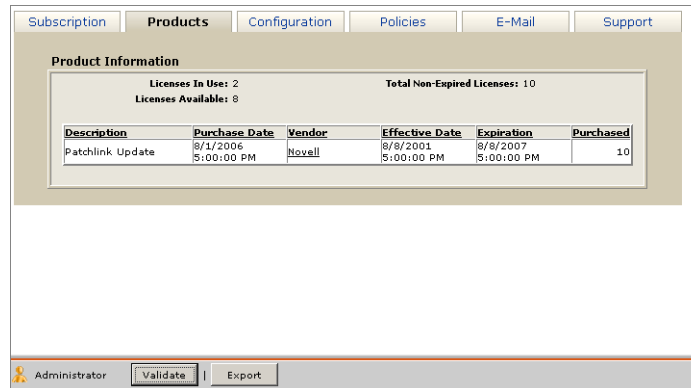
**Figure 11.3** Products Tab

Table 11.8 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" on page 16.

Product Information

The Product Information section provides a summary of license availability and usage.

- **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 that are active and available for use. This number represents a sum of the licenses in use and available

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 each subsequent quarter.

The license group information includes the following:

- **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. Licenses typically expire one calendar year after purchase
- **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.

To open the *Patch Management Server Configuration* page click **Options** in the tool bar and then click the **Configuration** tab.

The screenshot shows the 'Configuration' tab of the Novell ZENworks Patch Management Server. The interface includes a top navigation bar with tabs for Subscription, Products, Configuration (selected), Policies, E-Mail, and Support. Below the navigation bar, the 'Server Information' section displays details like Name (MATS01-RLUS2), Total Agents Registered (3), and URL (10.12.1.1:67). The 'Deployment Defaults' section includes 'Concurrent' settings for Deployment Limits (10), Reboot Processes (5), and Discover Applicable Updates System Tasks (500), as well as 'Consecutive' settings for Failure Limits (2). The 'Agent Defaults' section is divided into 'Communication' (with options for Show Logon Settings, Use Offline Threshold, Communication Interval, Inventory Collection Options, Agent Uniqueness Based On, Logging Level, Agent Scan Mode, and Agent Listener Port) and 'Bandwidth Throttling' (with Maximum Transfer Rate and Minimum File Size). The 'Deployment Notification Defaults' section includes 'Deployment Notification Options' (User May Cancel, User May Snooze), 'Reboot Notification Options' (User May Cancel, User May Snooze), and 'Deployment Messages' (Manual Installation and May Reboot). The 'Discover Applicable Updates (DAU)' section has options for Initialize after Subscription Replication and Scheduling Frequency. The 'FastPath Servers' section includes a Communication Interval and a list of servers. The 'Absentee Agent Management' section has a Delete Absentee Agent After option. The 'ISAPI Communication Settings' section includes Concurrent Agent Limit and Connection/Command Timeout settings. The 'User Interface Defaults' section includes Deployment Wizard Start Time, Display Rows Per Page, Password Expiration Notifications, and Cache Timeout.

Figure 11.4 Patch Management Server Configuration Tab



Table 11.9 Button 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	The Export button allows you to export Patch Management Server information to a comma separated value (.CSV) file. For more information on exporting data, see "Exporting Data" on page 16.

Viewing Patch Management Server Information

Summary information appears along the top of the page and provides general notes regarding the ZENworks Patch Management Server. The information is not editable and is exclusive of the default account policy settings.

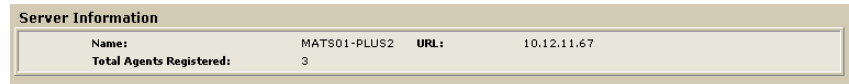


Figure 11.5 Patch Management Server Configuration Tab - Patch Management Server Information section

- **Name** - The name of the machine on which the ZENworks Patch Management Server is installed
- **Total Agents Registered** - The total number of agents registered to the ZENworks Patch Management Server
- **URL** - The URL of the ZENworks Patch Management Server



Configuring Deployment Defaults

The Deployment Defaults all you to establish global deployment limitations.

Figure 11.6 Patch Management Server Configuration Tab - Deployment Defaults section

Concurrent [Deployment Settings]

- **Deployment Limit** - The purpose of this limit is to throttle the number of concurrent deployments. The maximum number of agents that can receive active deployments at the same time. If an agent takes longer than four hours to report a successful deployment, it will no longer be counted against the deployment limit
- **Reboot Processes** - The maximum number of agents that can receive the Reboot deployment at the same time
- **Discover Applicable Updates System Tasks** - The maximum number of agents that can receive the Discover Applicable Updates (DAU) System Task at the same time

Consecutive [Deployment Settings]

- **Failure Limit** - The number of consecutive failed deployment attempts permitted before a deployment is deleted (if not a mandatory baseline deployment) or disabled (if a mandatory baseline deployment)



Note: You can define deployment notification recipients on the *E-Mail Notification* tab.



Configuring Agent Defaults

Agent defaults let you establish default behavior for the deployment agent.

Defining Agent Default Settings

The screenshot shows the 'Communication' tab in the Patch Management Server Configuration. It contains several settings:

- Hours Of Operation:** A button labeled 'Modify'.
- Logging Level:** A dropdown menu set to 'None'.
- ☒ **Show Legacy Settings**
- Use Offline Threshold:** A numeric input set to '3' and a dropdown set to 'Hours'.
- Agent Scan Mode:** A dropdown menu set to 'Normal'.
- Communication Interval:** A numeric input set to '5' and a dropdown set to 'Minutes'.
- Agent Listener Port:** A numeric input set to '0'.
- Inventory Collection Options:** A button labeled 'Modify'.
- ☒ **Resume Interrupted Downloads**
- Agent Uniqueness Based On:** A dropdown menu set to 'Device Name'.

Figure 11.7 Patch Management Server Configuration Tab - Agent Default Communication

- **Hours of Operation** - Agent communication can be limited to a defined day and time range. Click **Modify** to open the “[Editing Agent Hours of Operation](#)” window
- **Show Legacy Settings** - When selected, this option adds a Legacy Agent Time Settings section in the Hours of Operation display that caters to agents prior to version 6.3 of ZENworks Patch Management
- **Use Offline Threshold** - Select to configure 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.
- **Communication Interval** - The time interval between agent and ZENworks Patch Management communication. Interval can be defined in minutes, hours, or days
- **Inventory Collection Options** - Allows you to modify what inventory data is collected from the agents. Click **Modify** to open “[Setting Inventory Collection Options](#)”
- **Agent Uniqueness Based On** - Defines the Agent Uniqueness method used to identify agents. Options are:
 - **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
- **Logging Level** - Displays the logging level employed by the agent beyond the default error logging which occurs at all levels. Levels include; None, Basic Information, Detailed, or Debug
 - **None** - Only errors are logged and recorded, no regular system activity
 - **Basic Information** - Logs all errors and basic system and usage information

- **Detailed** - Logs all errors and the major system actions
- **Debug** - Logs all errors and all system actions
Based upon your operating system, the log files can be found in the following locations:
 - **Windows (any version)**: C:\Program Files\Novell\Update Agent\ZENworks Patch Management Agent.log
 - **NetWare**: /export/home/Novell/update/log/updateagent.log
 - **Linux**: /usr/local/Novell/update/log/updateagent.log
 - **Solaris**: PUPDATE.LOG
- **Agent Scan Mode** - The mode in which the discovery agent runs
 - **Fast Scan** - Performs the discovery faster, but uses more resources
 - **Initial Only** - Performs the first discovery scan in Fast Scan mode and all subsequent scans are performed in Normal mode
 - **Normal** - Performs the scan using less resources, causing minimal impact on the target computer
- **Agent Listener Port** - Defines the port on which the agents listen. Upon receiving a ping on the defined port, the agent replies with its current version and contacts the ZENworks Patch Management Server to identify any pending tasks. A setting of zero (0) will disable the Agent Listener
- **Resume Interrupted Download** - When selected, resumes downloads where the interruption occurred rather than starting over



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.

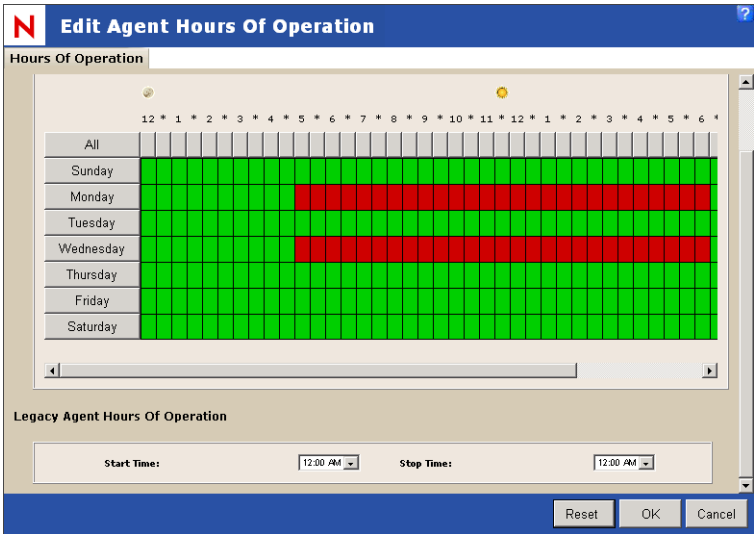


Figure 11.8 Edit Agent Hours of Operation

Table 11.10 Page Functions

Button	Function
Reset	Resets the 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
 - Clicking **ALL** will toggle all agent communication
 - Clicking the *day* will toggle that entire day
 - Clicking the *time* unit will toggle that 30 minute increment across all days
 - Legacy hours of operation are set for a specific start and stop time and apply to every day
- 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.

Setting Inventory Collection Options

Agent Inventory Collection can be modified through the Select Inventory Collection page. These options allow you to remove the inventory items about which you are not concerned.

Select Inventory Collection

- ☒ **Inventory Collection Options:**
 - ☒ **Allow use of WMI during inventory collection**
 - ☒ **Hardware**
 - ☒ USB controllers
 - ☒ IDE ATA/ATAPI controllers
 - ☒ Other hardware devices
 - ☒ Processors
 - ☒ USB storage devices
 - ☒ Network adapters and MAC address (may use WMI)
 - ☒ Physical RAM - amount
 - ☒ System devices
 - ☒ Non-Plug and Play drivers
 - ☒ Locally attached drives, total and free space
 - ☒ USB devices
 - ☒ BIOS information
 - ☒ Sound, video, and game controllers
 - ☒ **Other**
 - ☒ OS serial number (requires WMI)
 - ☒ Virtual Machines
 - ☒ Device serial number (requires WMI)
 - ☒ Device manufacturer and model (may use WMI)
 - ☒ Device asset tag (requires WMI)
 - ☒ User - last logged on
 - ☒ System uptime (may use WMI)
 - ☒ Custom import from file (may use WMI)
 - ☒ **Services**
 - ☒ **Software**

OK Cancel

Figure 11.9 Inventory Collection Options

Table 11.11 Page Functions

Button	Function
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 11.12 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
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
Other	Deselecting this option will deselect all <i>Other</i> inventory options
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)



Table 11.12 Inventory Collection Options

Inventory Option	Description
User - last logged on	Scans for last logged in user and time
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 *Patch Management Server Configuration* page.

Defining Bandwidth Throttling Settings

Bandwidth Throttling

Maximum Transfer Rate: Kbps
(0 for disabled)

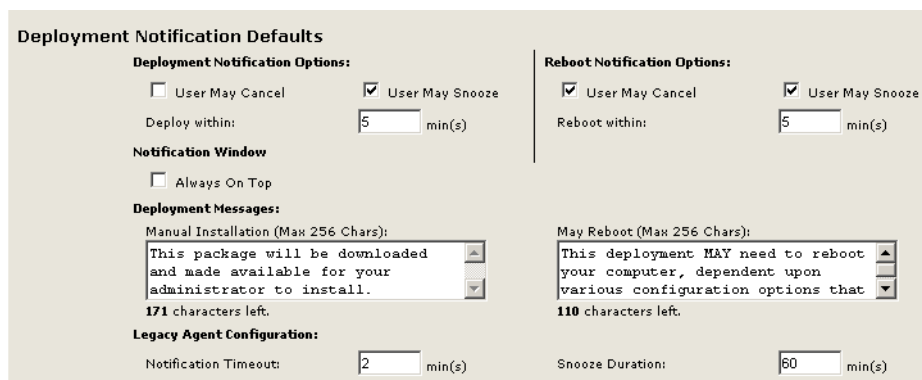
Minimum File Size: KB

Figure 11.10 Patch Management Server Configuration Tab - Bandwidth Throttling

- **Maximum Transfer Rate** - Define 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



Defining Deployment Notification Settings



Deployment Notification Defaults

Deployment Notification Options:

☐ User May Cancel ☒ User May Snooze

Deploy within: min(s)

Notification Window

☐ Always On Top

Deployment Messages:

Manual Installation (Max 256 Chars):

This package will be downloaded and made available for your administrator to install.

171 characters left.

Reboot Notification Options:

☒ User May Cancel ☒ User May Snooze

Reboot within: min(s)

May Reboot (Max 256 Chars):

This deployment MAY need to reboot your computer, dependent upon various configuration options that

110 characters left.

Legacy Agent Configuration:

Notification Timeout: min(s)

Snooze Duration: min(s)

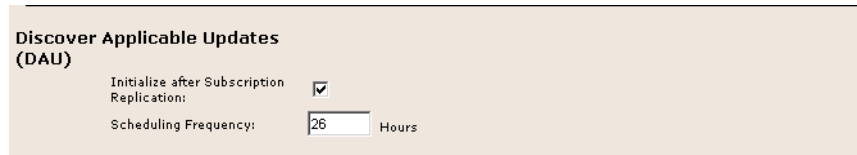
Figure 11.11 Patch Management Server Configuration Tab - Deployment Notification Defaults

- **Deployment Notification Options** - Deployment options defined in this section may be overridden within a Agent Policy or on a per-deployment basis using the Deployment Wizard
 - **User May Cancel** - Selection of this option permits the recipient to cancel the deployment
 - **User May Snooze** - Selection of this option permits the recipient to snooze the deployment
 - **Deployment Date Offset** - The time window, in minutes, during which the client user may snooze or cancel the deployment. When the defined Offset has elapsed, the deployment will automatically occur
- **Reboot Notification Options** - Reboot options apply to deployments where a reboot 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
 - **User May Cancel** - Selection of this option permits the recipient to cancel the reboot
 - **User May Snooze** - Selection of this option permits the recipient to snooze the reboot
 - **Reboot Date Offset** - The time window, in minutes, during which the client user may snooze or cancel the reboot. When the defined Offset has elapsed, the reboot will automatically occur
- **Notification Window**
 - **Always On Top** - Selection of this option will force all notification windows to display on top of other windows
- **Deployment Messages**
 - **Manual Installation** - Packages deployed with the download only flag enabled will display this message advising the user that the package still requires installation (maximum of 256 characters)

- **May Reboot** - Packages deployed with the may reboot flag enabled will display this message advising the user that the computer MAY be rebooted (maximum of 256 characters)
- **Legacy Agent Configuration** - Legacy agent configuration rules apply to legacy (pre 6.3) ZENworks Patch Management Agents
 - **Notification Timeout** - If the deployment or reboot is set to notify the user, this is how long the deployment notification window will be shown, allowing the user to snooze (delay) the deployment. If the window times out, the deployment will automatically snooze
 - **Snooze Duration** - This is the amount of time the deployment is delayed if the user decides to use the snooze option

Defining the Discover Applicable Updates (DAU) Settings

The Discover Applicable Updates settings, allow you to configure the frequency of the DAU system task.



Discover Applicable Updates (DAU)

Initialize after Subscription Replication: ☒

Scheduling Frequency: Hours

Figure 11.12 Patch Management Server Configuration Tab - Discover Applicable Updates (DAU)

Discover Applicable Updates (DAU) Options

- **Initialize after Subscription Replication** - Indicates whether a DAU should be scheduled for all agents after the ZENworks Patch Management Server replicates (and receives new vulnerabilities and/or packages) with the Global Subscription Server
- **Scheduling Frequency** - The maximum number of hours between DAU's. This value indicates that if a DAU has not run within the last __ hours, it should start



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.

Fastpath Servers

Communication Interval:
(0 for disabled)

12

Hours

Servers:

Add	Url	Port
	http://proxy.myorg.com	12345

Figure 11.13 Patch Management Server Configuration Tab - Fastpath Configuration

- **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. Click the **Add** link (or **Edit** icon) to open the *Add Fastpath Server* dialog

Add FastPath Server

Add FastPath Server

URL:

Port:

☐ Authenticated

User Name:

Password:

Confirm Password:

Figure 11.14 Add Fastpath Server

2. 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
 - **Authentication** - 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
3. Click **Save** to save the server data

Absentee Agent Management

Absentee Agent Management allows ZENworks Patch Management Server to automatically delete Agents that are unresponsive for a set number of days. A value of zero disables this function.

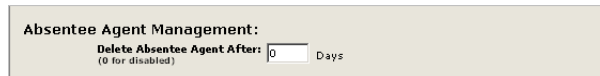
A screenshot of a configuration window titled "Absentee Agent Management:". Inside the window, there is a label "Delete Absentee Agent After:" followed by a text input field containing the number "0". Below the input field, there is a small note "(0 for disabled)". To the right of the input field, the word "Days" is displayed.

Figure 11.15 Absentee Agent Management



Configuring ISAPI Communication Settings

ZENworks Patch Management supports the Internet Server API (ISAPI) communication settings for Internet Information Server (IIS).

ISAPI Communication Settings

Concurrent Agent Limit:

- ☐ MSDE Default (5 threads)
- ☒ SQL Default (64 threads)
- ☐ Custom Setting (5 to 256 threads) threads

Connection Timeout:

Connection Timeout:

- ☒ Default
- ☐ Custom Setting (5 to 300 seconds) sec(s)

Command Timeout:

- ☒ Default
- ☐ Custom Setting (5 to 900 seconds) sec(s)


Figure 11.16 Patch Management Server Configuration Tab - ISAPI Communication Settings

- **Concurrent Agent Limit** - Defines the maximum number of threads used by ZENworks Patch Management, the options are:
 - **MSDE Default (5 threads)** - Select to enable the recommended thread count for a MSDE implementation
 - **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 Time-out** - Time (seconds) before an ISAPI thread expires (times out)
 - **Default** - Select to set the Connection time-out to the default value of 30 seconds
 - **Custom Setting** - Select to define a custom (between 5 and 300 seconds) time-out setting
- **Command Time-out** - Time (seconds) before an ISAPI command expires (times out)
 - **Use Default** - Select to set the Command time-out to the default value of 30 seconds
 - **Custom Setting** - Select to define a custom (between 5 and 900 seconds) time-out setting



Setting the User Interface Defaults

The User Interface default settings allow you to define the initial user experience for your users.



User Interface Defaults

Deployment Wizard Start Time:
☐ Agent Local Time (Deploy at local time for each individual node)
☒ Agent UTC Time (Deploy at UTC time for each individual node)

Display 25 Rows Per Page [Modify](#)

Password Expiration Notification: (0 for disabled) Days

Cache Timeout: (minimum 5-120) Minutes

Figure 11.17 User Interface Defaults

- **Deployment Wizard Start Time**
 - **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
- **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



Note: While the **Display __ Rows Per Page** is unique per user, this global setting only applies to the pages on which the user has not set the value manually.

- **Password Expiration Notification** - 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 before the data grid will refresh (updated from the database)



Note: Due to the enhanced security available when using Internet Explorer 6 SP 1, Novell ZENworks Patch Management default security settings prohibit the use of any other browsers. If you would like to remove the restriction against other browsers, **and disable the enhanced security settings** only available with IE 6 SP1, please refer to [Novell Knowledgebase Article #390](http://support.patchlink.com/scripts/rightnow.cfg/php.exe/enduser/std_adp.php?p_faqid=390) (http://support.patchlink.com/scripts/rightnow.cfg/php.exe/enduser/std_adp.php?p_faqid=390)



Customizing Row Values

The *Customize Row Values* page allows you to define six values, and define one as the default, for use when displaying pages.

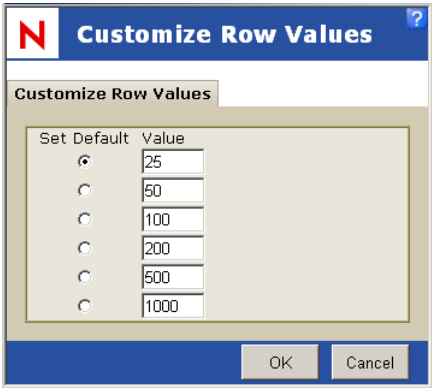


Figure 11.18 Customize Row Values

To Customize Row Values

- 1. If needed, type a new value in the *Value* field.
- 2. If needed, select the desired radio button in the *Set Default* field.



Customizing and Administering Agent Policy Sets

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 11.19 Agent Policy Set Tab

An agent policy set is the key element in defining agent deployment behavior. An agent policy set is defined as a set of constraints that govern the communication interval, logging level, and agent start and stop times. Agent policy sets are associated with a group and are applied to all the members of that group. As such, deployments inherit the behavior rules defined by the policy.



Note: If an group has not been assigned a policy, the settings defined on the Patch Management Server Configuration page are applied.

When you create an agent policy set, the values on the Configuration page are replaced with those defined in the custom policy with a couple important exceptions.



- Concurrent Deployment Limit settings and system task CDL settings
- Consecutive Deployment Failure Limits and Offline Threshold options

Table 11.13 Page Functions

Button	Function
Create	Creates a new Agent Policy
Delete	Deletes an Agent Policy
Export	Exports policy data to a comma separated value (.csv) file. For more information on exporting data, see "Exporting Data" on page 16.



Table 11.14 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 listing displays the following information regarding each policy:

Table 11.15 Agent Policy Set Definitions

Value	Description
Policy 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 Type	There are two types of policies: System and User.
Logging Level	The logging level assigned to the policy. This is determined when the policy is created and can be edited at any time. Trace levels include: None, Info, Detailed, and Debug.
Start Time	Relates to Hours of Operation settings. Identifies when the agent can begin communication.
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 Corp.
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 - measured in minutes, hours or days - of contact between the client agent and ZENworks Patch Management Server.
Description	The description attributed to the policy. Policy descriptions can be edited at any time.
Agent Scan Mode	The mode in which the discovery agent runs. The available options include: Fast Scan, Initial Only, and Normal.
Agent Listener	Defines the port on which agents listen. When pinged, the agent responds with its current version and contacts the ZENworks Patch Management Server to identify pending tasks.



Table 11.15 Agent Policy Set Definitions

Value	Description
Deployment Notification Options	The rules pertaining to how agents accept deployments. These options permit the user to avoid interruption by a deployment.
Reboot Notification Options	The rules pertaining to how agents accept reboot requests. These options permit the user to avoid interruption by a reboot.
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.



Creating a New Policy

The Create a Policy Wizard allows you to create and add a policy to the ZENworks Patch Management Server.

To Create an Agent Policy

- 1. In ZENworks Patch Management Server, open the *Agent Policy Sets* page (**Options > Policies**)
- 2. Click **Create**
The *Create a Policy* wizard opens

Create A Policy

Policy Information

Enter the Policy Information:

Policy Details

* Name:

Description:

3000 characters left.

Communication

Hours Of Operation:

Inventory Collection Options:

* Communication Interval: Minutes

Logging Level:

Agent Scan Mode:

Agent Listener Port:

☐ Resume Interrupted Downloads

Bandwidth Throttling

Maximum Transfer Rate: Kbps

Minimum File Size:

Figure 11.20 Create a Policy Wizard



Figure 11.21 Create a Policy Wizard, scrolled page

3. Configure the following options (as applicable for your organization):

Table 11.16 Agent Policy Configuration

Value	Description
Policy Details Section	
Name (required)	The name of the policy. Limited to 255 characters
Description	The policy description
Communication Section	
Hours of Operation	Button launches the <i>Edit Agent Hours of Operation</i> page, allowing 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.



Table 11.16 Agent Policy Configuration

Value	Description
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
Inventory Collection Options	Button launches the <i>Select Inventory Collection</i> page, allowing selection of which inventory values to record during collection
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
Communication Interval (required)	The interval (in minutes, hours or days) between each communication between the agent and Patch Management Server
Agent Listener Port	When pinged 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
Resume Interrupted Downloads	When enabled, the agent will resume interrupted downloads at the point of interruption
Bandwidth Throttling Section	
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
Deployment Notification Section	
<i>Deployment Deadline Options</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
Deployment Date Offset	The default time (in minutes), between the creation of the deployment and the deployment deadline
<i>Reboot Deadline Options</i>	



Table 11.16 Agent Policy Configuration

Value	Description
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 Date Offset	The default time (in minutes), between the creation of the deployment and the reboot deadline
Notification Window	
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)
FastPath Servers	Allows for the redirection of an agent via a FastPath server (caching proxy server) based upon the fastest route
Discover Applicable Updates (DAU)	Allows you to configure the frequency of the DAU system task

4. Click **Save** to save the agent policy as defined



Editing a Policy

The *Edit a Policy* Wizard allows you to modify an agent policy and its behavior.

To Edit a Policy

- 1. In ZENworks Patch Management Server, open the *Agent Policy Sets* page (**Options > Policies**)
- 2. Select the *Edit* icon to the left of the policy

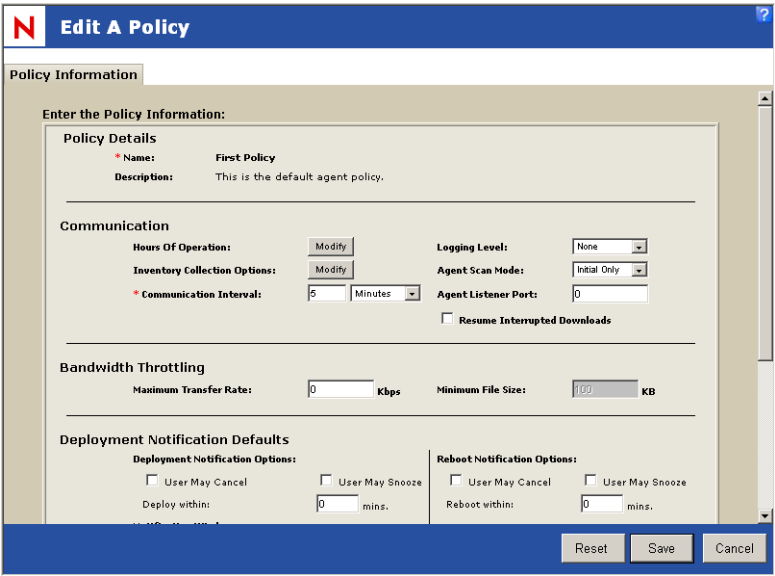


Figure 11.22 Editing Policies

- 3. In the *Edit a Policy* dialog box, edit the policy as necessary
 - Refer to “[Creating a New Policy](#)” on page 256 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 a Policy

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 a Policy

1. In ZENworks Patch Management Server, click **Options**
2. In the *Options* page, click **Policies**. (Labeled **Agent Policy Sets** when selected)



Subscription	Products	Configuration	Policies	E-Mail	Support	Total: 3
			Action	Agent Policy Set Name		
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	First Policy		
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Policy		
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Test Policy		

Figure 11.23 Removing a Policy

3. Select the policy to remove by clicking the checkbox to the left of the policy
4. In the *Action Menu*, click **Delete**
5. In the confirmation dialog box, click **Yes**
The policy is deleted from the system.



Defining Agent Policy Conflict Resolution

When an agent is a member of more than one group such that it receives multiple agent policies, the policies applied to the agent are calculated as follows:

- If all of the groups of which the agent is a member are assigned No policy (the policy named No Policy), the agent will use the options as defined on the *Configuration* page.
- If the agent is a member of a only one group which has been assigned a policy other than No Policy, the agent will use the settings defined within that policy.
- If the agent is a member of multiple groups, some of which have been assigned different (conflicting) policies, the agent will use a combination of settings from each of the groups to which it belongs. This combination of settings is determined as follows:

Table 11.17 Agent Policy Conflict Resolution

Policy Setting	Resolution
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.
Inventory Collection Options	The agent will use an all inclusive set of Inventory Collection options.
Communication Interval	The agent will use the shortest (smallest) Communication Interval.
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)
Agent Listener Port	If any group has an Agent Listener port defined (not zero), the agent listens on the highest defined port value.
Resumable Downloads	If any group is not using Resumable Downloads, the agent will not use Resumable Downloads.
Bandwidth Throttling	The agent will use the smallest Transfer Rate and File Size.
Deployment Notification Defaults	The agent will use the smallest Deployment and Reboot Notification values.
FastPath Servers	The agent will use all of the defined FastPath Servers.
Discover Applicable Updates (DAU) Frequency	The agent will use the shortest (smallest) DAU Frequency.



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.

Click **Options** in the tool bar and then click the **E-Mail** tab.

The screenshot displays the 'E-Mail Notifications' tab within a web application. At the top, there are navigation tabs: Subscription, Products, Configuration, Policies, **E-Mail Notification**, and Support. Below the tabs, the 'E-Mail Notifications' section contains a table with columns for various alert types: New Vulnerabilities, New Agent Registrations, Subscription Failure, Deployment Failure, Low System Disk Space, Low Storage Disk Space, Low Available License Count, Up-Coming License Expiration, and License Expiration. Each column has a checkbox, and the 'Notification Address' column contains the email 'QA.Team@Corp.com'. Below this table, the 'Alert Thresholds' section is visible, showing settings for 'Low System Disk Space', 'Low Storage Disk Space', 'Low Available License Count', and 'Up-Coming License Expiration'. Each threshold has an 'Alert When Below' value and a 'MBCheck Disk Space Every' frequency. At the bottom of the interface, there is a toolbar with buttons: PatchLink, Create, Save, Delete, Export, and Test.

Figure 11.24 E-Mail Notifications Tab

Table 11.18 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" on page 16.
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 11.19 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 11.20 E-Mail Notification Alert Definitions

Alert Thresholds	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

The *Technical Support* page provides a variety of system data pertaining to the ZENworks Patch Management Server environment. This page is an important reference if you should ever need to contact technical support.

Click **Options** in the tool bar and then click the **Support** tab.

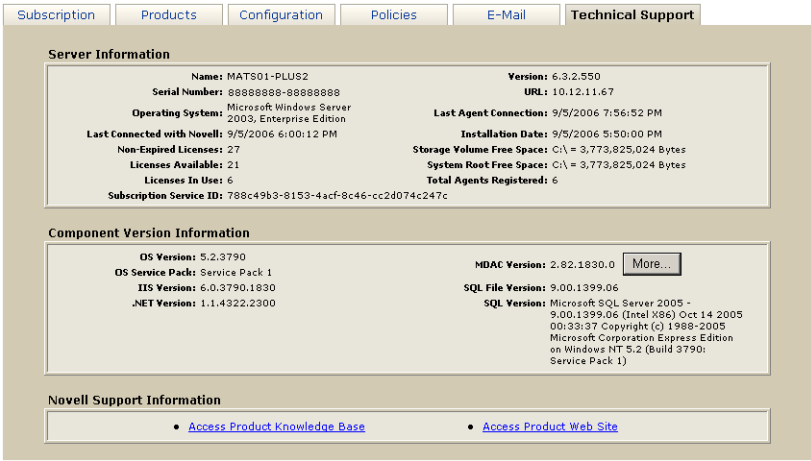


Figure 11.25 Technical Support Tab

Table 11.21 Page Functions

Button	Function
Export	The Export button allows you to export technical support information to a comma separated value (.csv) file. For more information on exporting data, see "Exporting Data" on page 16.



Server Information

Server information appears along the top of the page and provides general notes regarding the ZENworks Patch Management Server. The information is not editable.

Table 11.22 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 provided here is not editable.

Table 11.23 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 11.24 Novell Support Information Link Descriptions

Field Name	Description
Contact Technical Support	Sends an e-mail message to Technical Support.
Access Product Knowledge Base	Accesses the Novell Knowledge Base.
Access Product Web Site	Accesses the Novell Main Web site.
Ask a Question	Sends a support question to Technical Support via e-mail.
Request a Patch	Sends a patch request to Technical Support via e-mail.
Request a Feature	Sends a feature request to Technical Support via e-mail.
Provide Product Feedback	Sends product input to Technical Support via e-mail.



12 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 vulnerabilities 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”
- “Agent Components”
- “User Interaction During a Deployment”
- “User Interaction During a Reboot”

About the ZENworks Patch Management Agent

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.

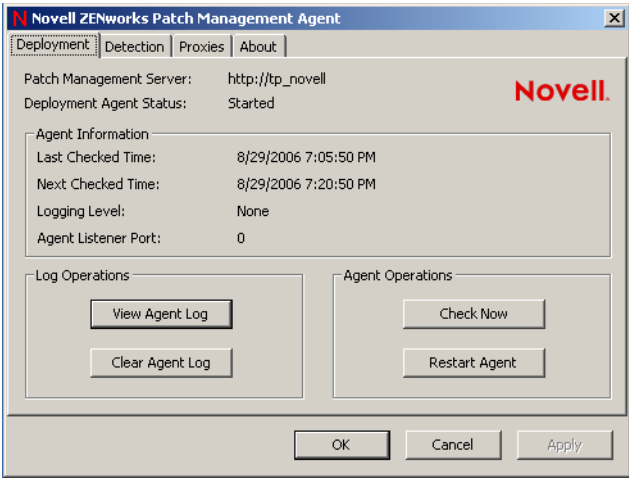


Figure 12.1 Agent initial screen

Server Information and Status

The following table displays the ZENworks Patch Management Server location and the communication status:

Table 12.1 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 12.2 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 12.3 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

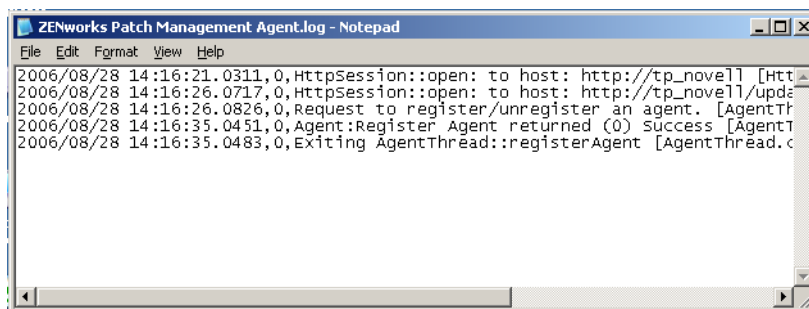


Figure 12.2 View Agent Log



To Clear the Agent Log

- 1. Click **Clear Agent Log**.
The Clear confirmation message dialog box opens.

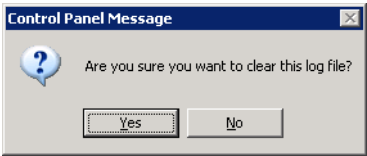


Figure 12.3 Clear Agent Log Message

- 2. Click **Yes**.
The system clears the Agent Log.

Agent Operations

The following table describes the Agent Operations area:

Table 12.4 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.

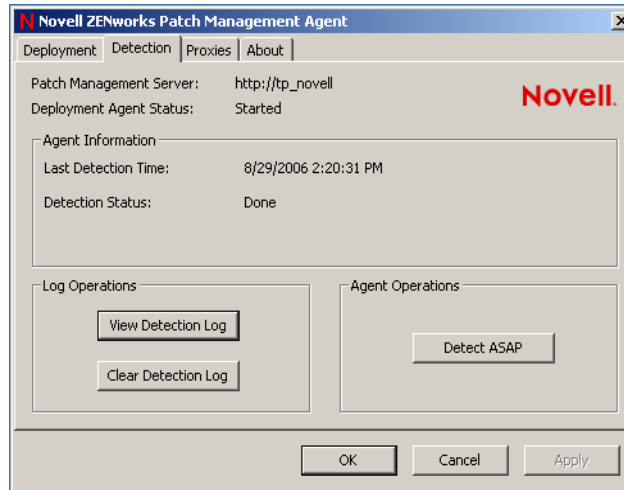


Figure 12.4 Detection Tab

Server Information and Status

The following table displays the ZENworks Patch Management Server location and the communication status:

Table 12.5 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 12.6 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 12.7 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

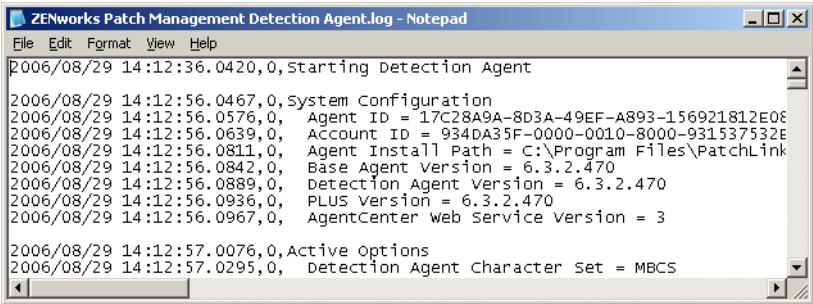


Figure 12.5 View Detection Log



To Clear the Detection Log

1. Click **Clear Detection Log**.
The Clear confirmation message dialog box opens.

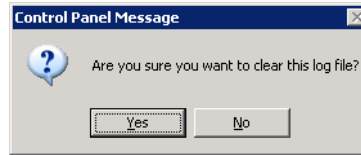


Figure 12.6 Clear Agent Log Message

2. Click **Yes**.
The system clears the Detection Log.

Agent Operations

The following table describes the Agent Operations area:

Table 12.8 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.

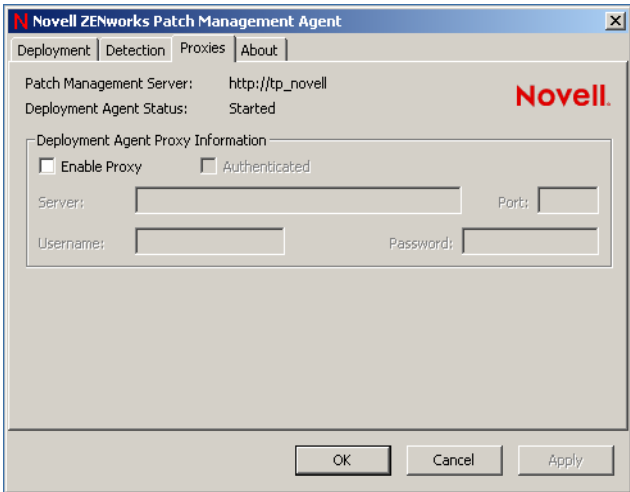


Figure 12.7 Proxies Tab

Server Information and Status

The following table displays the ZENworks Patch Management Server location and the communication status:

Table 12.9 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.

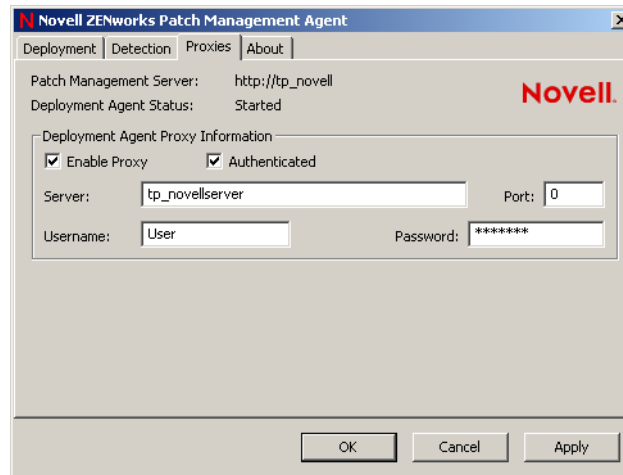


Figure 12.8 Proxy tab with both options activated

5. Type the *Username* in the **Username** field
6. Type the *Password* in the **Password** field
7. Click **OK**
The confirmation dialog box opens.

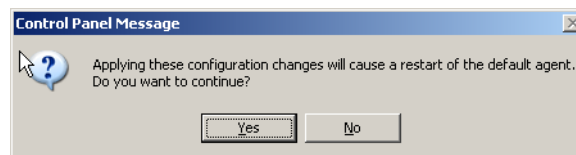


Figure 12.9 Proxy change confirmation



- 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.

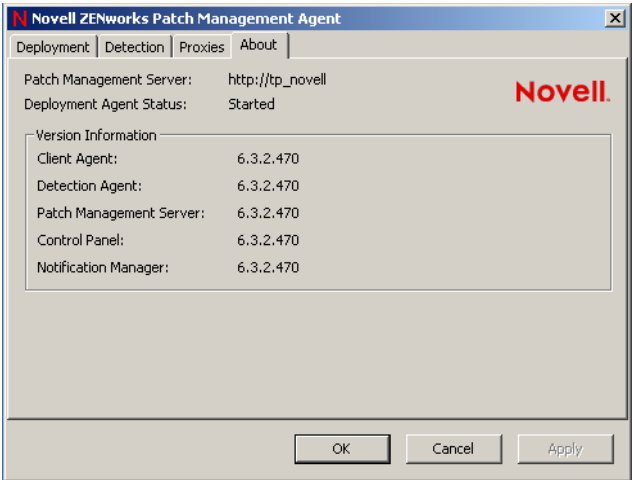


Figure 12.10 Proxies tab

Server Information and Status

The following table displays the ZENworks Patch Management Server location and the communication status:

Table 12.10 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 service</i> on the local device



Version Information

The following table describes the Version Information area for the About tab:

Table 12.11 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 Update 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, the Novell Desktop Deployment Manager will display on the Device screen, if a deployment notification was enabled and a user is logged into the device.

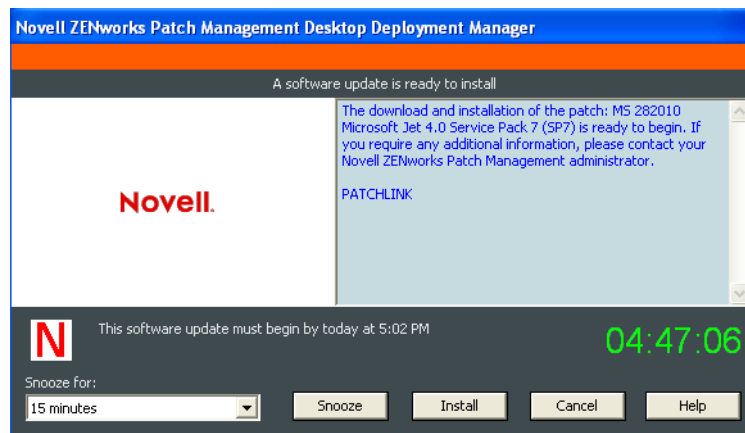


Figure 12.11 Novell Desktop Deployment Manager - Pending Deployment



An icon is also visible in the taskbar.

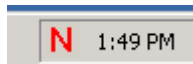


Figure 12.12 Install Icon

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 Update 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 displays on the Device screen.

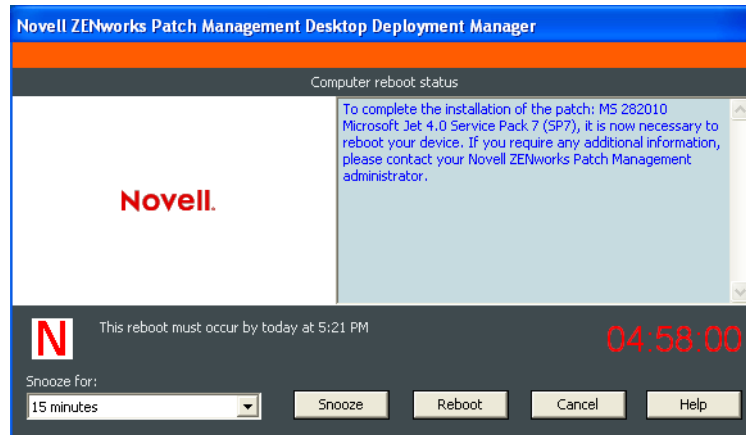


Figure 12.13 Novell Desktop Deployment Manager - Pending Reboot

An icon is also visible in the taskbar.

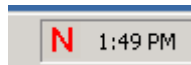


Figure 12.14 Install Icon

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.



A Patch Management Server Reference

In this Appendix

- “Patch Management Server Security”
- “ZENworks Patch Management Server Error Pages”
- “HTTP Status Codes”
- “WinInet Error Codes”
- “Device (ZENworks Patch Management Agent) Status Icons”

Patch Management Server Security

There are multiple layers of security for ZENworks Patch Management:

- “Web Site Authentication”
- “Web Site Encryption via SSL”
- “User (Security) Roles”

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: Due to the enhanced security available when using Internet Explorer 6 SP 1, Novell ZENworks Patch Management default security settings prohibit the use of any other browsers. If you would like to remove the restriction against other browsers, **and disable the enhanced security settings** only available with IE 6 SP1, please refer to [Novell Knowledgebase Article #390 \(http://support.patchlink.com/scripts/rightnow.cfg/php.exe/enduser/std_adp.php?p_faaid=390\)](http://support.patchlink.com/scripts/rightnow.cfg/php.exe/enduser/std_adp.php?p_faaid=390)

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.
- **Unsupported Browser Version** - This page is displayed whenever a user visits the ZENworks Patch Management Server with an unsupported browser.
- **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.



HTTP Status Codes

As a Web based application using Internet Information Services (IIS), ZENworks Patch Management uses HTTP status codes. While many of the status codes are informational only, the following table defines some of the more common errors:

Table A.1 HTTP Status Codes

Code	Description
HTTP 401.1 - Logon failed	Logon attempt was unsuccessful (likely due to invalid user name or password) *
HTTP 403.4 - SSL Required	You must use HTTPS instead of HTTP when access this page
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 **
* ZENworks Patch Management 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 ** ZENworks Patch Management 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	



Note: 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.



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.2 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



Note: Refer to [Microsoft knowledgebase article #193625](#) for additional details regarding the WinInet error codes.

Device (ZENworks Patch Management Agent) Status Icons

The following table describes the Device status icons and their functions.

Table A.3 Device Status Icons

Status	Description
	The agent is idle (this is a valid deployment agent without any current or pending deployments)
	The agent is idle and has pending deployments
	The agent is currently working on a deployment (animated icon)
	An active detection agent that does not correspond with a registered deployment agent



Table A.3 Device Status Icons



















Status	Description
	The agent is offline since it has not contact Patch Management Server in more than two communication intervals (minimum of 15 minutes)
	The agent is offline since it has not contact Patch Management Server in more than two communication intervals (minimum of 15 minutes) and has pending deployments
	The agent is sleeping (it is outside of it's hours of operation)
	The agent is sleeping (it is outside of it's hours of operation) and has pending deployments
	This agent has been disabled
	This agent has been disabled, and has pending deployments
	The agent is offline since it has not contact Patch Management Server in more than two communication intervals (minimum of 15 minutes) and is in a QChain status (the agent can accept chained deployments only until after a reboot)
	The agent is offline since it has not contact Patch Management Server in more than two communication intervals (minimum of 15 minutes), is in a QChain status (the agent can accept chained deployments only until after a reboot), and it has pending deployments
	The agent is offline since it has not contact Patch Management Server in more than two communication intervals (minimum of 15 minutes) and is in a 'Dirty R' status (the agent can accept no more deployments until after it reboots)
	The agent is offline since it has not contact Patch Management Server in more than two communication intervals (minimum of 15 minutes), is in a 'Dirty R' status (the agent can accept no more deployments until after it reboots), and it has pending deployments
	The agent is in a QChain status (the agent can accept chained deployments only until after a reboot)
	The agent is in a QChain status (the agent can accept chained deployments only until after a reboot) and it has pending deployments
	The agent is in a Dirty R status (the agent can accept no more deployments until after it reboots)
	The agent is in a Dirty R status (the agent can accept no more deployments until after it reboots) and it has pending deployments



Table A.3 Device Status Icons

Status	Description
	The agent is in a QChain status (the agent can accept chained deployments only until after a reboot) and is sleeping due to it's hour of operations settings.
	The agent is in a QChain status (the agent can accept chained deployments only until after a reboot) and it has pending deployments and is sleeping due to it's hour of operations settings.
	The agent is in a Dirty R status (the agent can accept no more deployments until after it reboots) and is sleeping due to it's hour of operations settings.
	The agent is in a Dirty R status (the agent can accept no more deployments until after it reboots) and it has pending deployments and is sleeping due to it's hour of operations settings.



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 Windows Networking”
- “Put ZENworks Patch Management Behind a Firewall”
- “Turn Off Non-Critical Services”
- “Lock Down Unused TCP and UDP Ports”
- “Turn Off File and Printer Sharing”
- “Apply All Microsoft Security Patches”

Install Your Server With SSL

Purchase a valid certificate from Verisign or Entrust for your IIS web server, and use it with ZENworks Patch Management. This process involves installing your certificate (.CER) file before rebooting after the main phase of the installation. Refer to the *ZENworks® Patch Management 6.3 Server Installation Guide* for additional details regarding installing with SSL.

Use Secure Passwords

Worm attacks frequently try to log in with weak and commonly used passwords. For a secure passwords, the Department of Defense standard of 12 characters with alpha, numeric, punctuation and mixed case characters all included in your password is recommended.



Turn Off Windows Networking

An intruder can easily exploit a Windows networking share, and therefore if the networking share is not required for other purposes; it should be turned off.

To Turn Off Windows Networking:

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

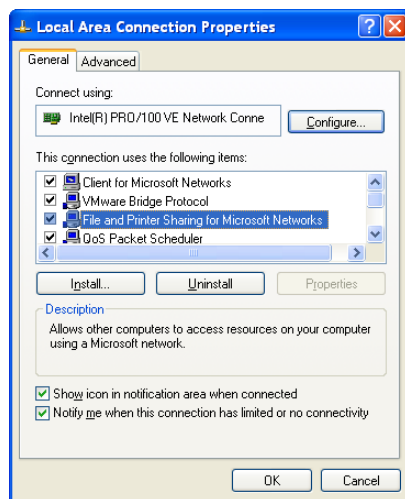


Figure B.1 Turn Off Windows Networking

4. Select **File and Printer Sharing for Microsoft Networks**
5. Click **Uninstall**



Note: Do not uninstall **Client for Microsoft Networks** because it is required by both Microsoft SQL Server and Internet Information Server.

Put ZENworks Patch Management Behind a Firewall

Since the ZENworks Patch Management Server pulls its patch updates from the subscription servers, there is no need to allow access from the Internet to the Patch Management Server server. However, you must allow access to the Subscription Server specified during installation from your ZENworks Patch Management Server.

Turn Off Non-Critical Services

Microsoft Windows allows most features to be active. There are a number of services you may wish to turn 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 done 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. Select **Local Area Connection**
3. On the *Local Area Connections Status* General tab click **Properties**

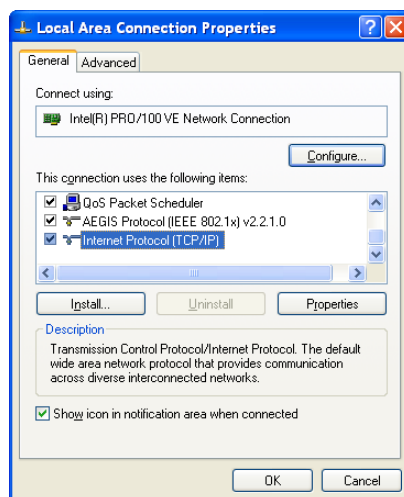


Figure B.2 Local Area Connection Properties

4. Select the *Internet Protocol (TCP/IP)* protocol and click the **Properties** button

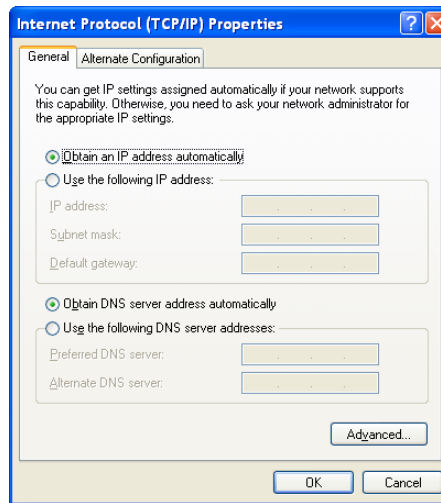


Figure B.3 General tab

5. In the *Internet Protocol (TCP/IP) Properties* General tab click **Advanced...**
6. Select the **Options** tab

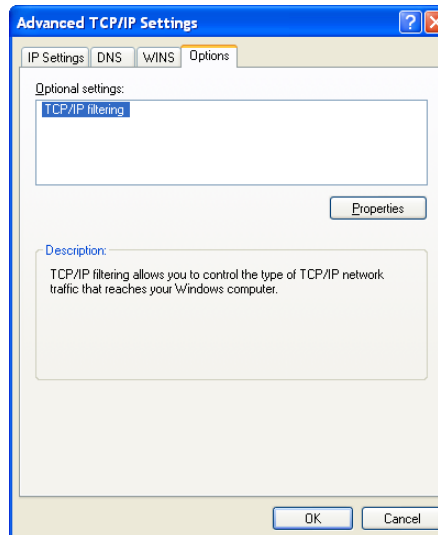


Figure B.4 Advanced TCP/IP Settings



7. Select *TCP/IP filtering* and click **Properties**
8. Select **Enable TCP/IP Filtering (All adapters)**
9. Select the **Permit Only TCP Ports** option

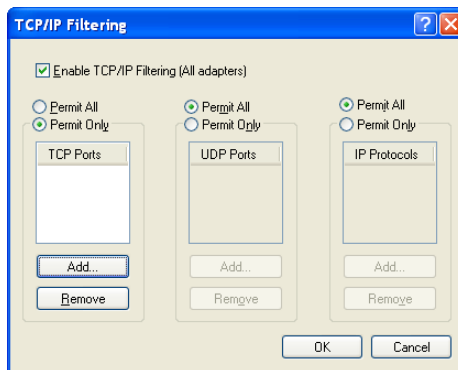


Figure B.5 TCP/IP Filtering

10. Add TCP ports 443 and 80 to the listing of permitted ports
 - a. Click **Add...**
 - b. Enter *443* in the **TCP Port** field
 - c. Click **OK**
 - d. Repeat steps a through c for port 80
 - No other ports are required, though you may want to allow DNS, TS, or VNC
11. Select the **Permit Only UDP Ports** option
 - Since no UDP ports are required, leave this section blank



Warning: If you lock out everything except ports 80 and 443 it will be necessary to add entries to `www.novell.com` and the Subscription Service you specified during installation in your `HOSTS` file (in the `%WINDIR%\system32\drivers\etc` directory) so that your Patch Management Server can download your patch subscriptions.

Warning: You will also need to add your proxy server (Name and IP) to your `HOSTS` file (in the `%WINDIR%\system32\drivers\etc` directory) if you access that server by name

Turn Off File and Printer Sharing

Since your ZENworks Patch Management Server should not be used as a file or print server, File and Printer Sharing for Microsoft Networks should be disabled.

To Turn Off File and Printer Sharing

1. From within the *Windows Control Panel*, double-click the **Network Connections** icon
2. Open (by double-clicking) the *Local Area Connection*
3. Click **Properties** and select the *File and Printer Sharing for Microsoft Networks* protocol

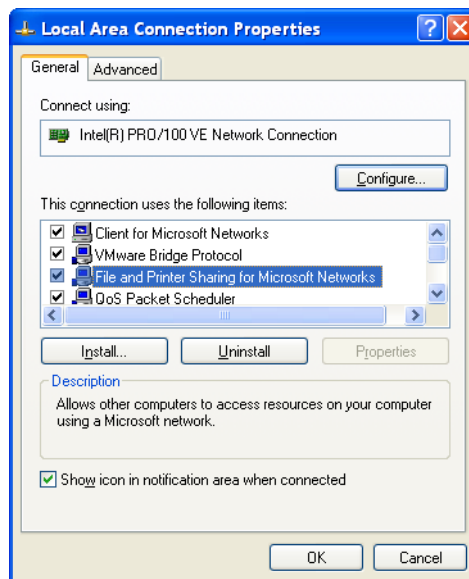


Figure B.6 Local Area Connection Properties

4. Click **Uninstall** to remove the protocol



Warning: Do **NOT** uninstall *Client for Microsoft Networks*; it is required by *SQL Server* and *Internet Information Server*.



Apply All Microsoft Security Patches

Apply all applicable Microsoft Security Patches to ensure that your system remains protected against all know security threats. Be sure to apply the most recent patches for your version of IIS, SQL Server, and Windows Server 2003.



C 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*.

To Change Your Database Recovery Model

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 database folder until you see your **PLUS** database
3. Right-click to select the **PLUS** database



- 4. Select **Properties** to open the *Database Properties* window

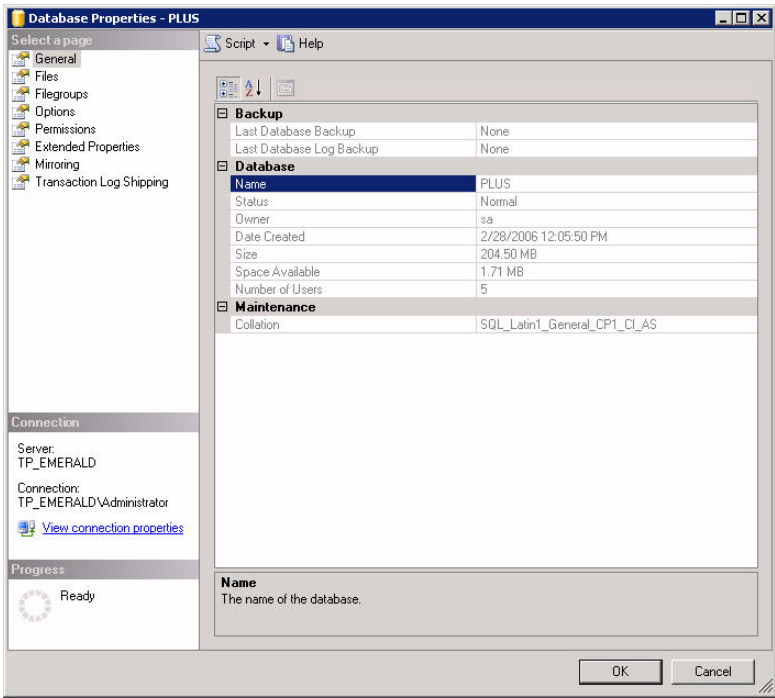


Figure C.1 Database Properties

- 5. Select *Options* within the **Select a page** field



6. In the **Recovery model:** field select **Full**

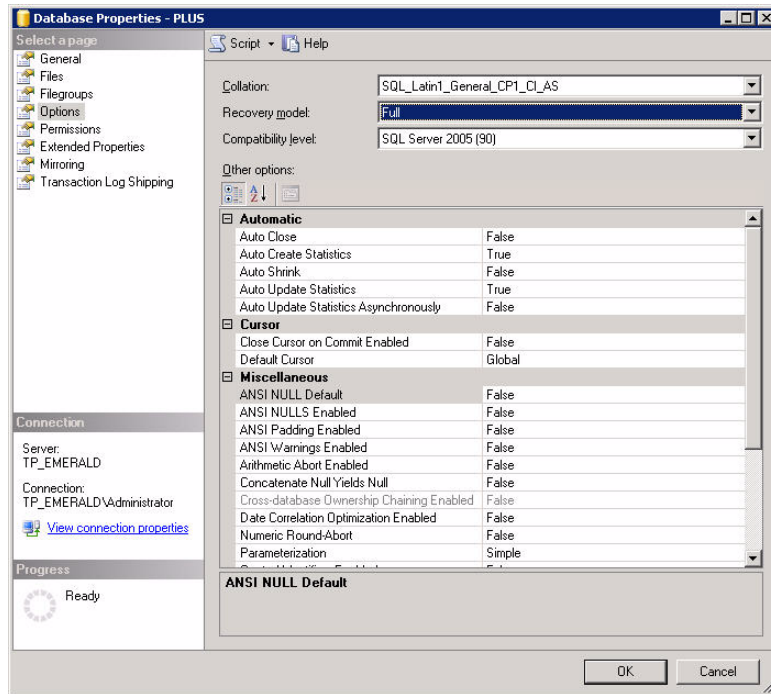


Figure C.2 Database Properties - *Options* page

7. Click **OK** to save the changes
8. Repeat steps 3 through 7 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**” on page 315 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 backup 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](#)” on page 297 for additional details.

To Create 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. Connect to your 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** to open the *Database Maintenance Plan Wizard*

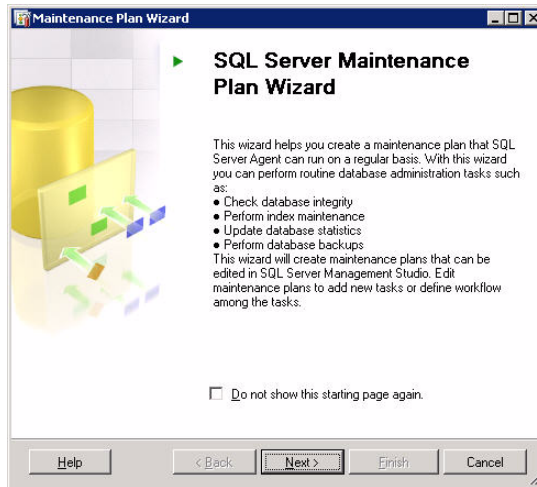


Figure C.3 Maintenance Plan Wizard

6. Click **Next**

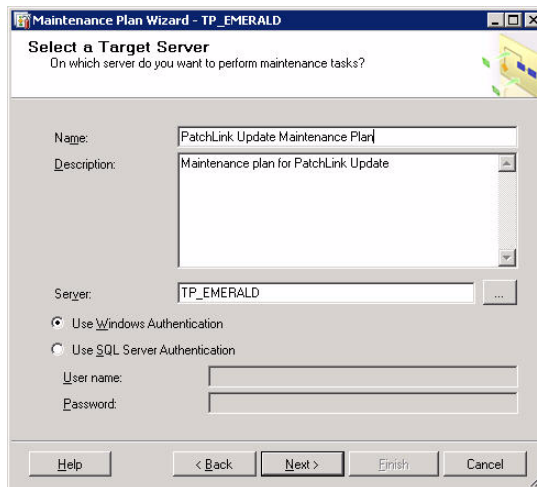


Figure C.4 Maintenance Plan Wizard - Select Target Server

7. Define the Maintenance Plan **Name**, **Description** [optional], target **Server**, and **Authentication** method



8. Click Next

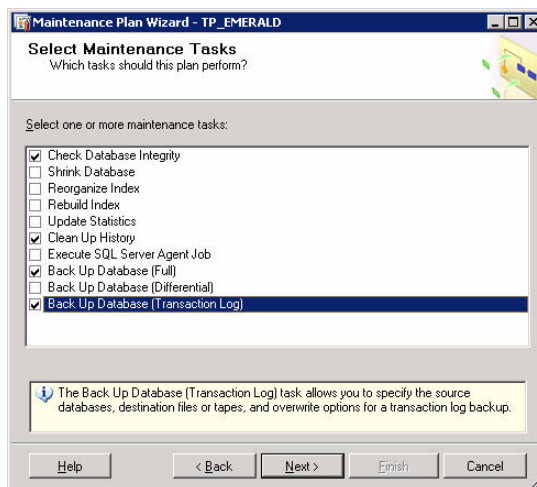


Figure C.5 Maintenance Plan Wizard - Select Maintenance Tasks

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

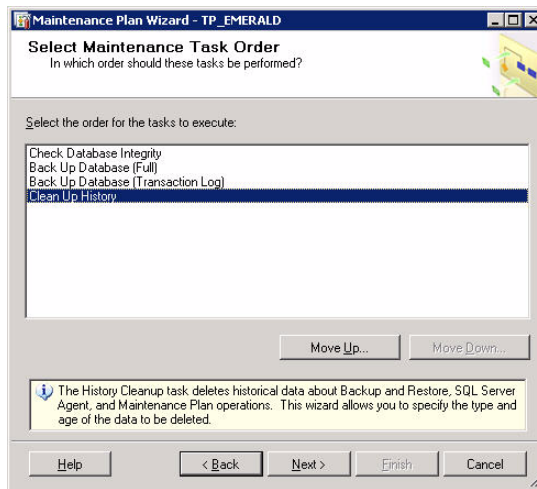


Figure C.6 Maintenance Plan Wizard - Select Maintenance Task Order

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

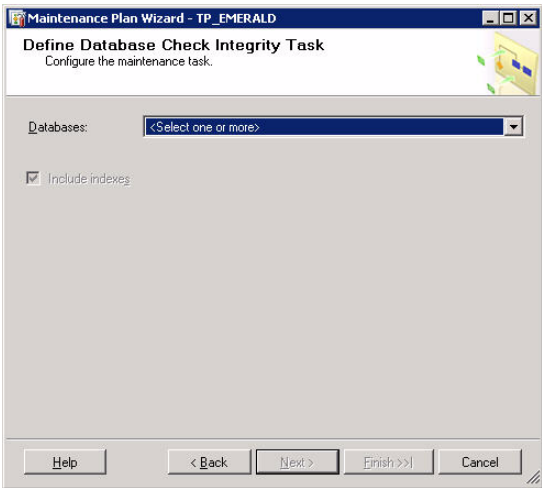


Figure C.7 Maintenance Plan Wizard - Define DB Check Integrity Task

13. Click the **Databases:** drop-down

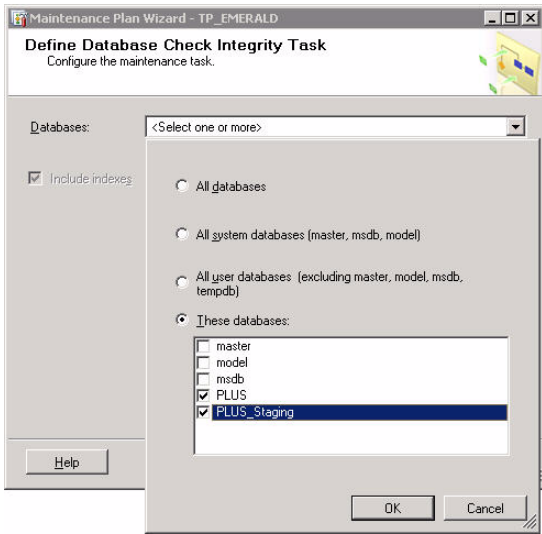


Figure C.8 Maintenance Plan Wizard - Select Databases

a. Select the **These databases:** option



- b. Select the **PLUS** and **PLUS_Staging** databases
- c. Click **OK**

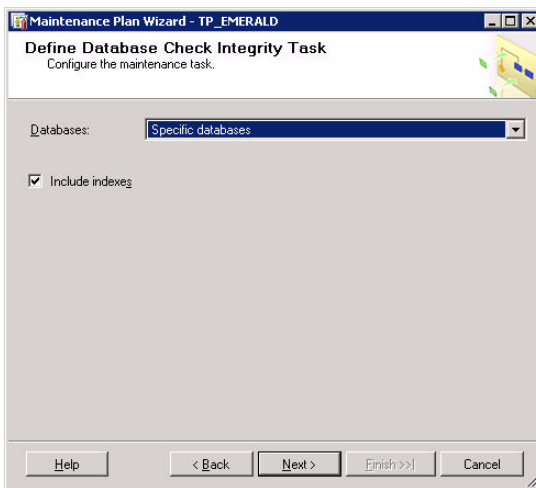


Figure C.9 Maintenance Plan Wizard - Specific Databases

- 14. Ensure that the **Include indexes** option is selected



15. Click **Next**
The *Define Back Up Database (Full) Task* page will display

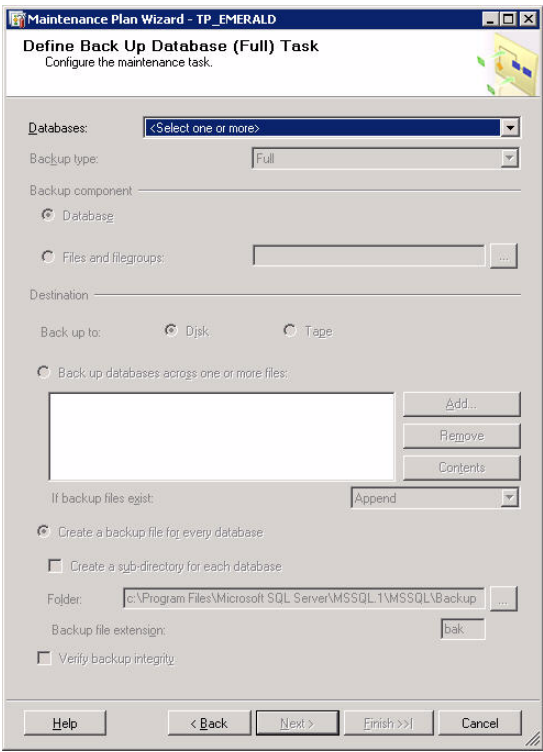


Figure C.10 Maintenance Plan Wizard - Define Back Up DB (Full) Task



16. Click the **Databases:** drop-down

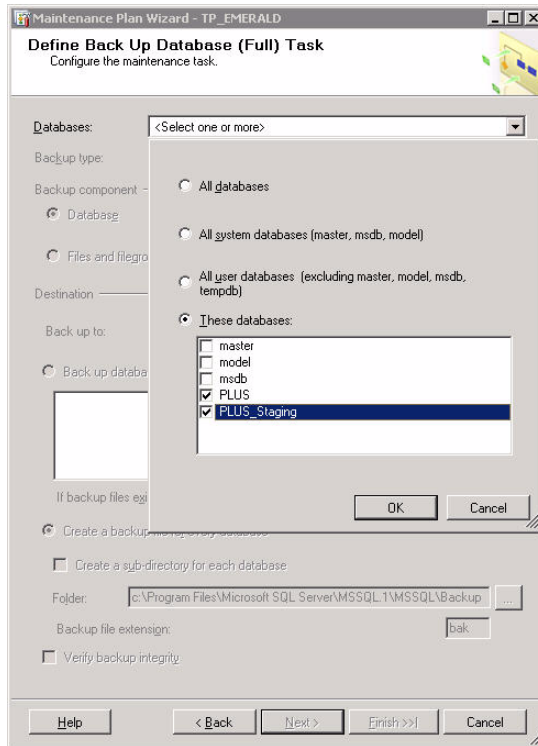


Figure C.11 Maintenance Plan Wizard - Select Databases

- Select the **These databases:** option
- Select the **PLUS** and **PLUS_Staging** databases



- c. Click **OK**

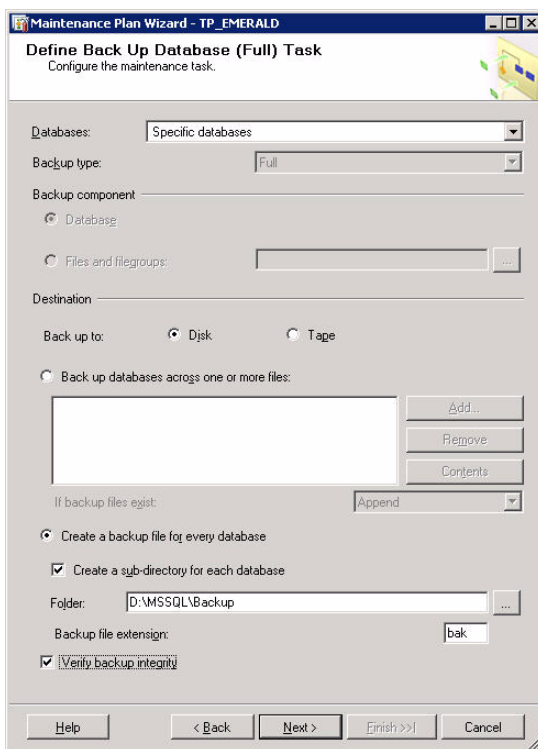


Figure C.12 Maintenance Plan Wizard - Specific Databases

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 will display

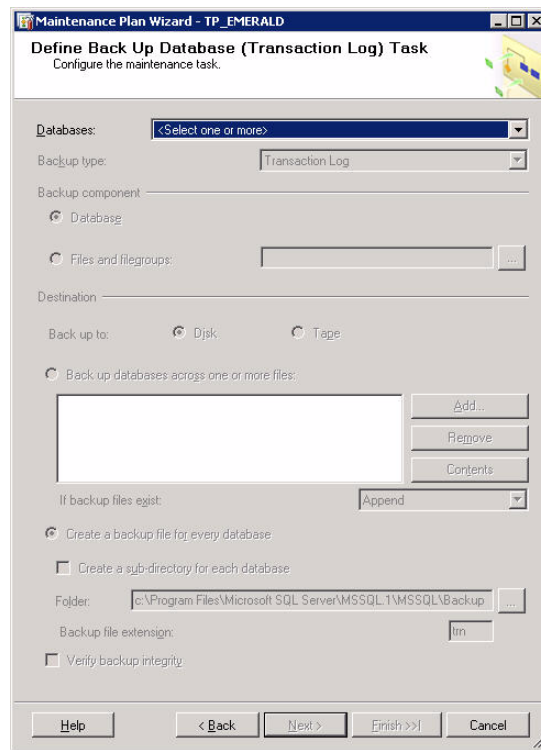


Figure C.13 Maintenance Plan Wizard - Define Back Up DB (Transaction Log) Task

19. Click the Databases: drop-down

- a. Select the **These databases:** option
- b. Select the **PLUS** and **PLUS_Staging** databases



- c. Click **OK**

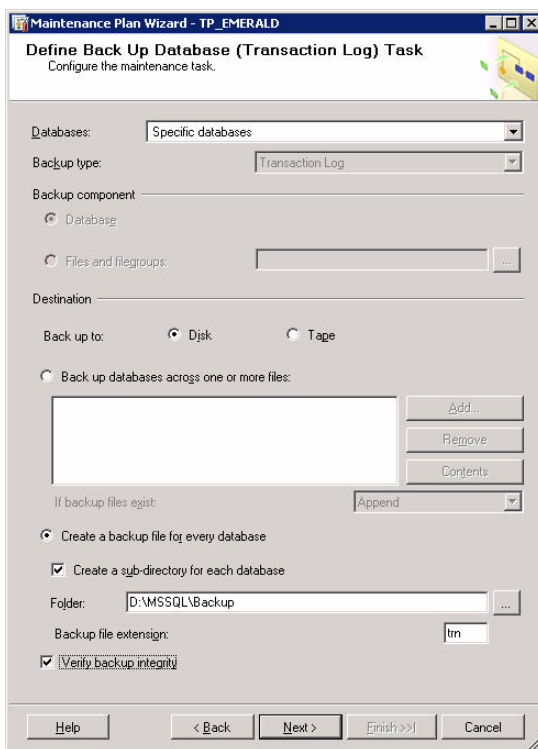


Figure C.14 Maintenance Plan Wizard - Specific Databases

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 will display

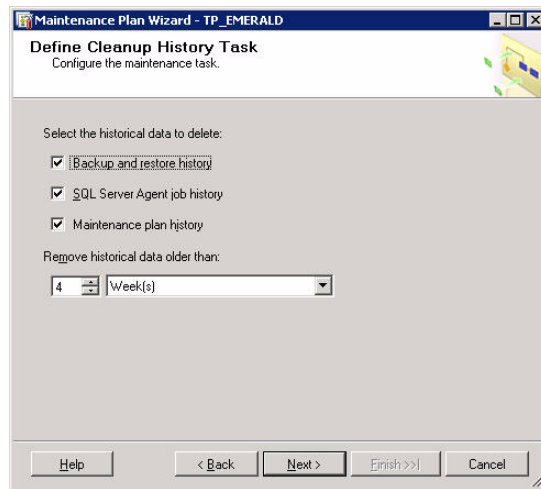


Figure C.15 Maintenance Plan Wizard - Define Cleanup History Task

- 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 display

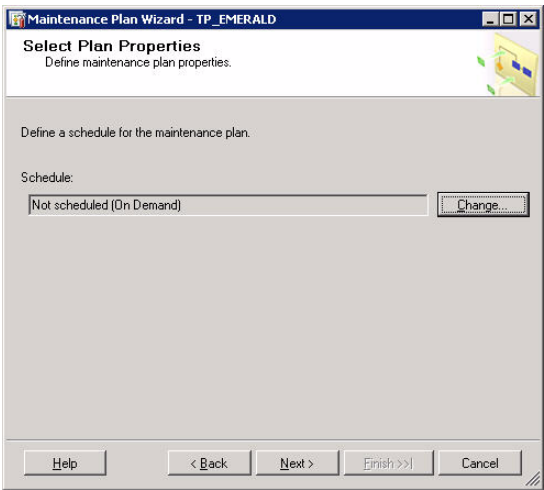


Figure C.16 Maintenance Plan Wizard - Select Plan Properties



27. [Optional] Click **Change...** to define the Maintenance plan schedule

New Job Schedule

Name:

Schedule type: ☒ Enabled

One-time occurrence

Date: Time:

Frequency

Occurs:

Recur every: week(s) on

☐ Monday ☐ Wednesday ☐ Friday ☐ Saturday ☒ Sunday

☐ Tuesday ☐ Thursday

Daily frequency

☒ Occurs once at:

☐ Occurs every: hour(s)

Starting at:

Ending at:

Duration

Start date: ☐ End date:

☒ No end date

Summary

Description:

Figure C.17 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**



- 28. Click **Next**
The Select Report Options page will display

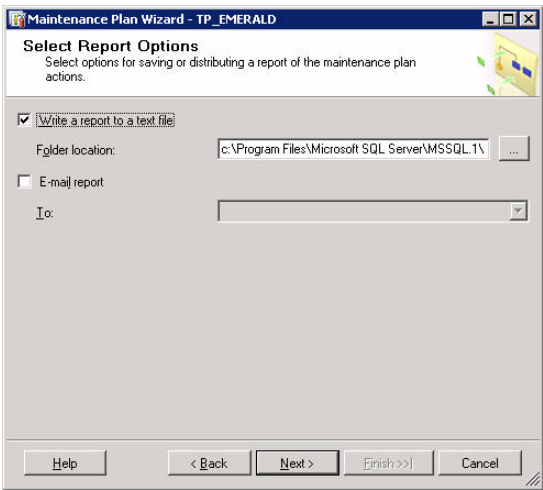


Figure C.18 Maintenance Plan Wizard - Select Report Options

- 29. Set your desired reporting options
- 30. Click **Next**
The *Complete the Wizard* page will display
- 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.

To Create a Database Backup

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 your **PLUS** database

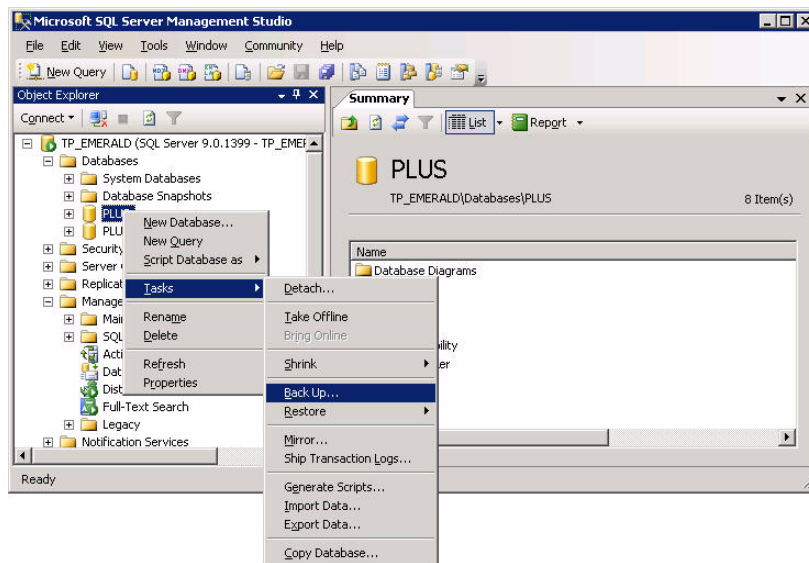


Figure C.19 SQL Server Management Studio - Database Context Menu



- 4. Select **Tasks > Back Up...**
The *Back Up Database - PLUS* window opens

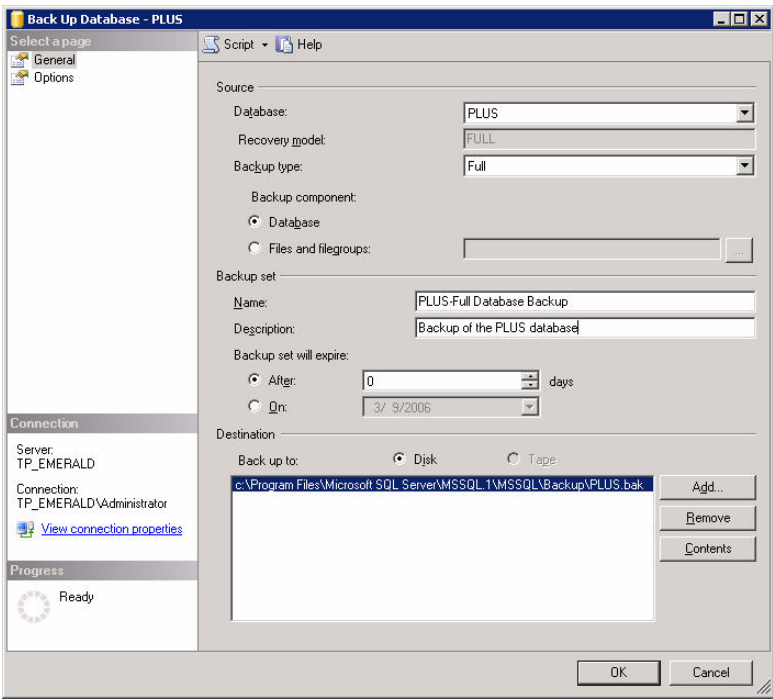


Figure C.20 *Back Up Database - PLUS - General page*

- 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** [optional], and when the **Backup set will expire** [optional]



7. Define your Back up *Destination* settings
 - a. Select either the **Disk** or **Tape** option and 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.

8. Select *Options* within the **Select a page** field
The *Options* page displays

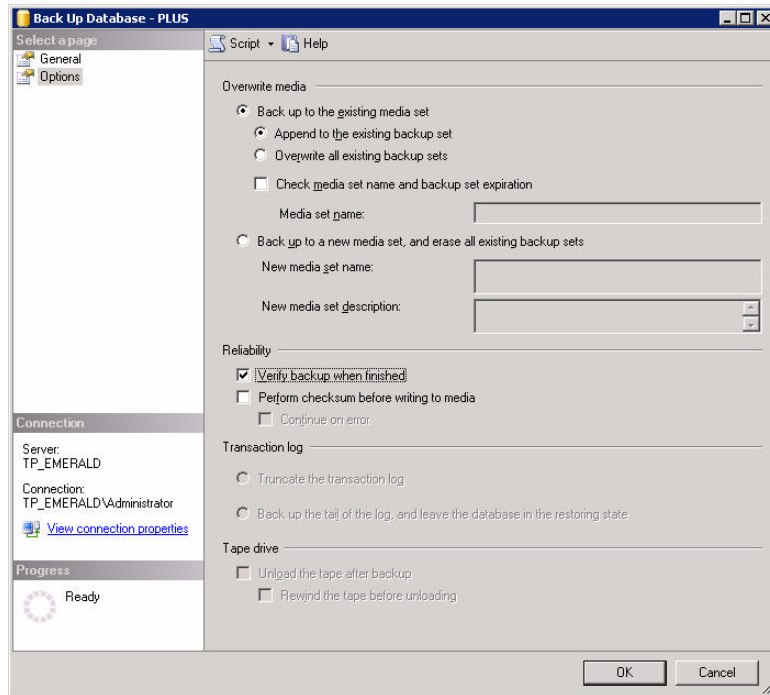


Figure C.21 *Back Up Database - PLUS - Options page*

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.

To Restore 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

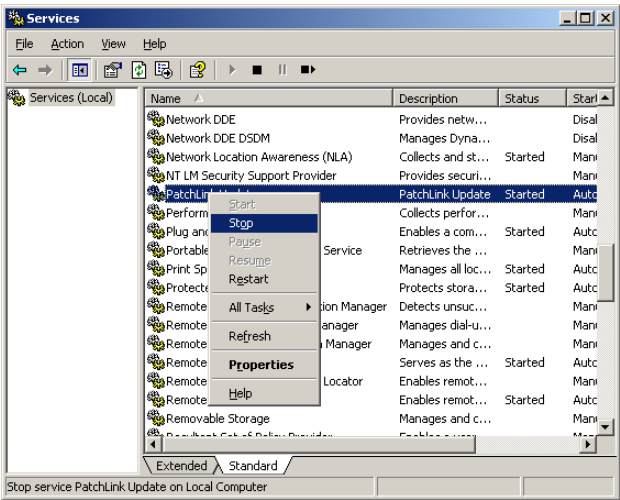


Figure C.22 Services Management Console

- 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

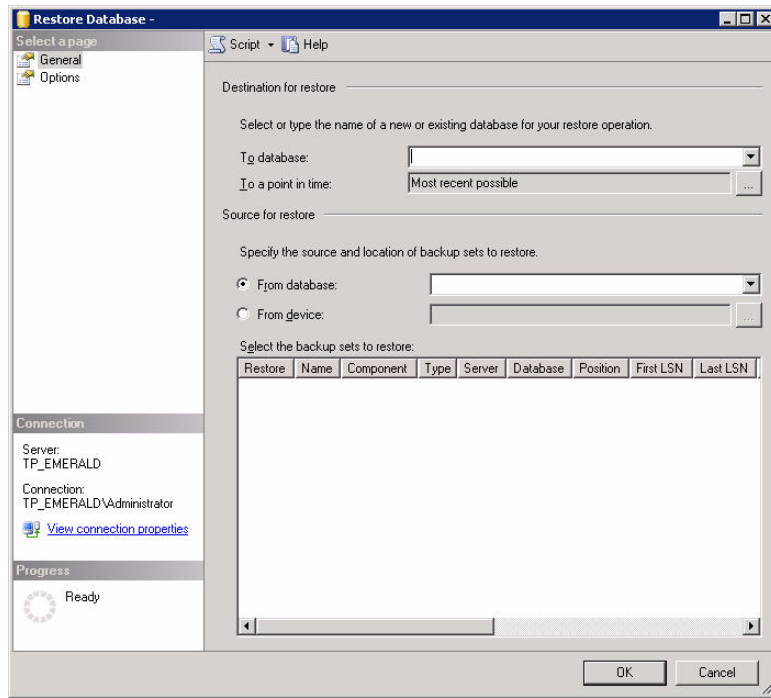


Figure C.23 Restore Database

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

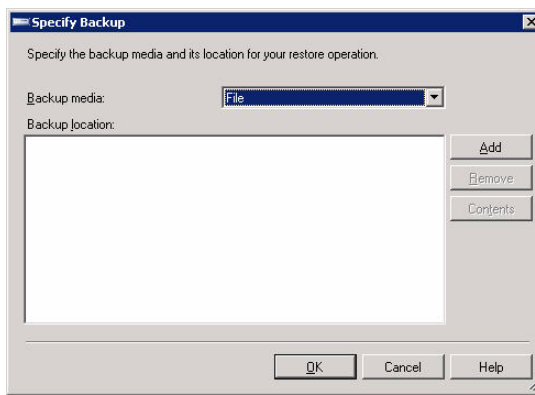


Figure C.24 Specify Backup

11. Click Add

The *Locate Backup File* window opens

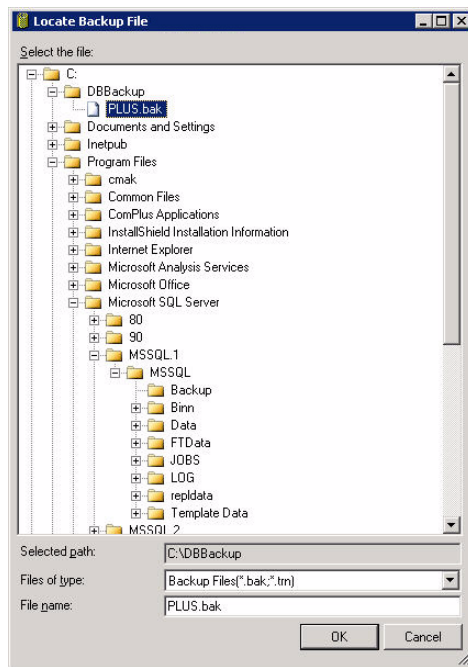


Figure C.25 Locate Backup File

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

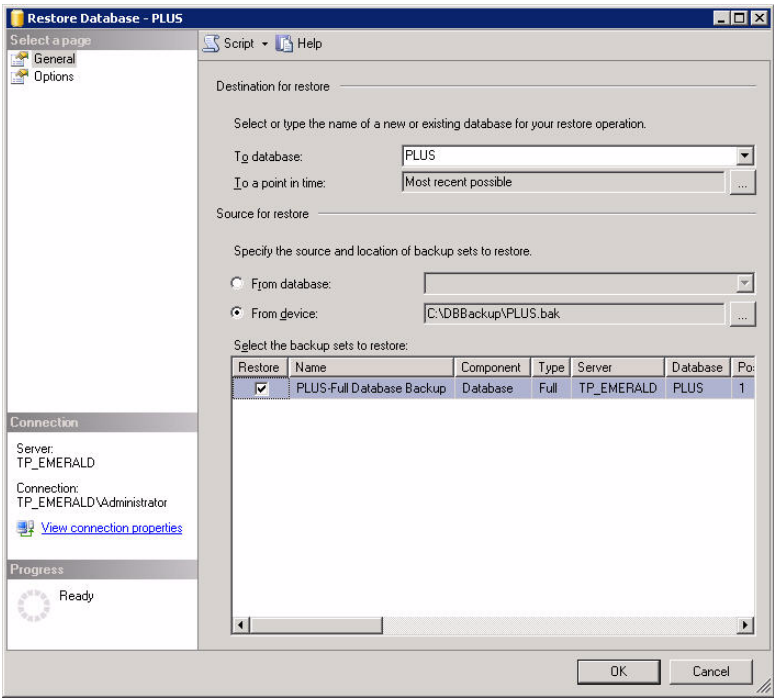


Figure C.26 Restore Database - PLUS - General page



16. Select *Options* within the **Select a page** field
The *Options* page will display

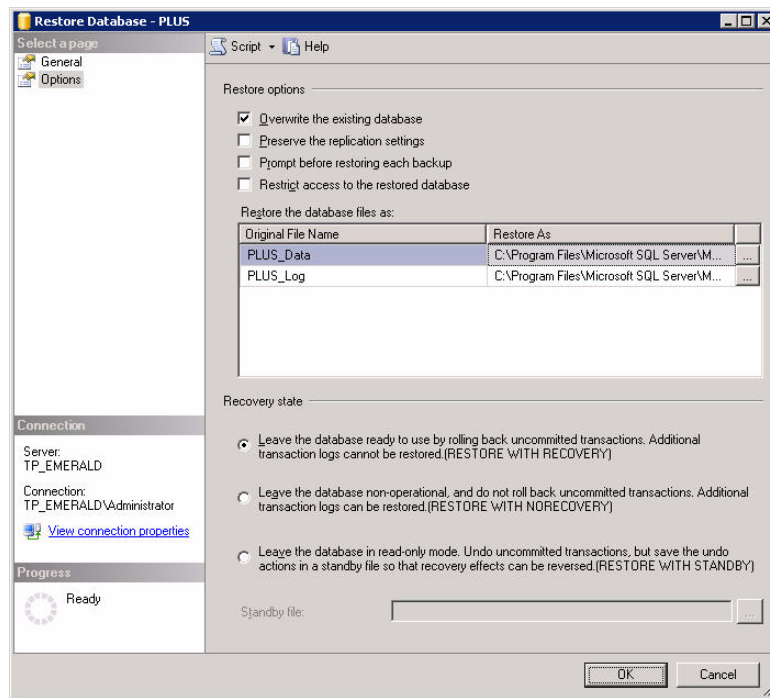


Figure C.27 Restore Database - PLUS - Options page

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





D Using the Distribution Point

The Distribution Point, based upon the Apache HTTP Server 2.2.3 open source product, provides you with a quick and easy way to add remote package caching to your 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 6.3.

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

Installing the Distribution Point

- 1. Log on to the target computer as the local **administrator** (or a member of the **LOCAL_ADMIN**s group)
- 2. Log in to Patch Management Server
- 3. Open the *Devices* page

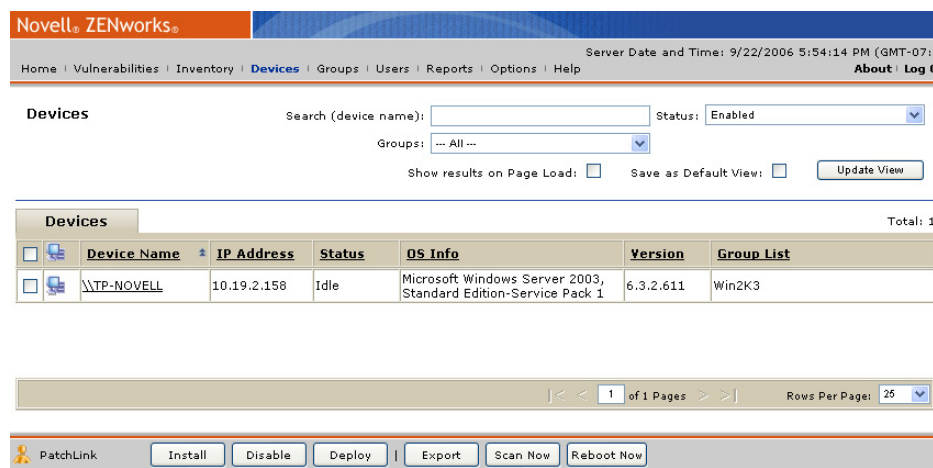


Figure D.1 Devices Page



4. Click **Install**

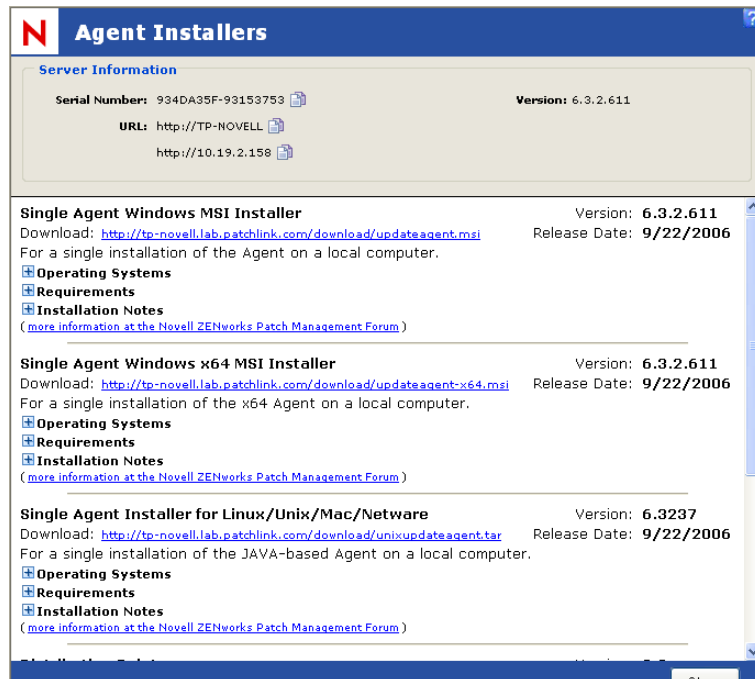


Figure D.2 Agent Installers



Tip: You can copy your **Serial Number**, **Server URL**, and IP from the *Server Information* section by clicking the associated copy icon.

5. Select the **Distribution Point** download link (<http://<YourServerName>/download/PLDISTPT.exe>)



- 6. Click **Open** to start the *Distribution Point Installation Wizard*
The *Welcome* page will display

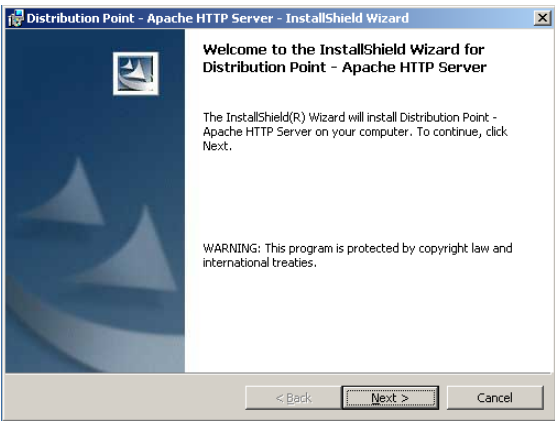


Figure D.3 Welcome page

- 7. Click **Next**
The *License Agreement* page will display

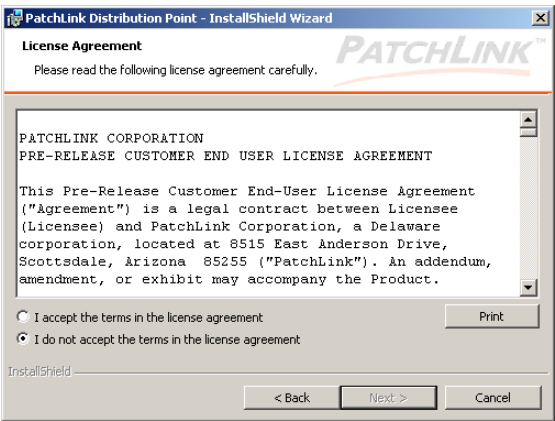


Figure D.4 License Agreement page

- 8. If you agree to the license, select the **I accept the terms in the license agreement** option and click **Next**



The *Destination Folder* page will display

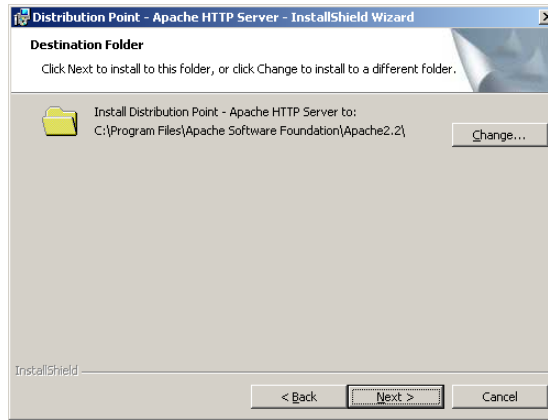


Figure D.5 Destination Folder page

If you need to install the Distribution Point in a location other than the default (C:\Program Files\Apache Software Foundation\Apache2.2\), click the **Change...** button to define the new install path

9. Click **Next**

The *Cache Folder* page will display

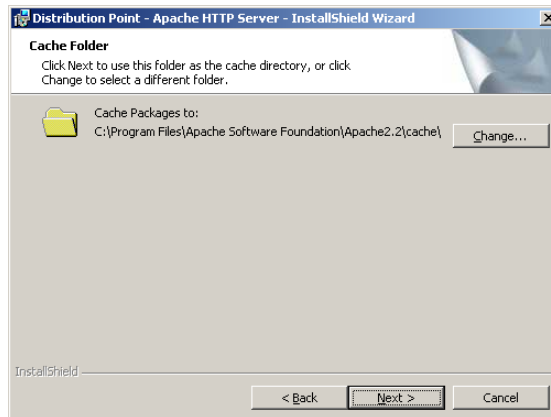


Figure D.6 Cache Folder page

If you need to change the Cache Folder to a location other than the default (C:\Program



Files\Apache Software Foundation\Apache2.2\cache\), click the **Change...** button to define the new location

10. Click **Next**

The *Update Server* Information page will display

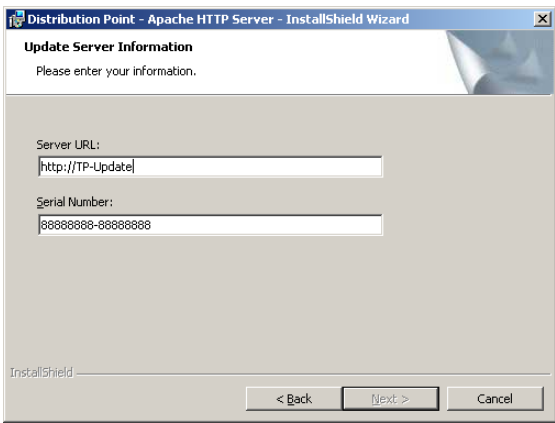


Figure D.7 Update Server Information page

- Type your **ZENworks Patch Management Server URL** and **Serial Number** in their respective fields

11. Click **Next**

The *Server Information* page displays

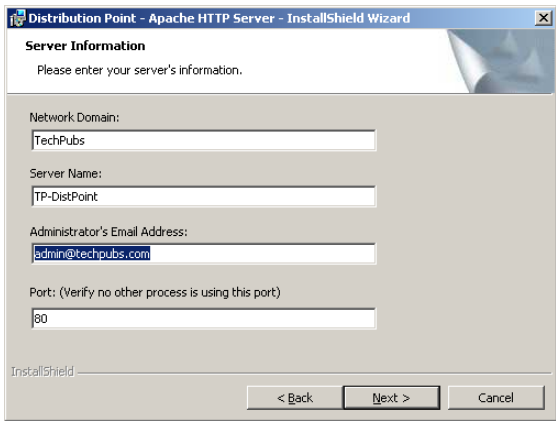


Figure D.8 Server Information page



12. Verify and modify if necessary the following fields:

- **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



Note: The default **Port** is **80**

13. Click **Next**

The *Ready to Install* page will display

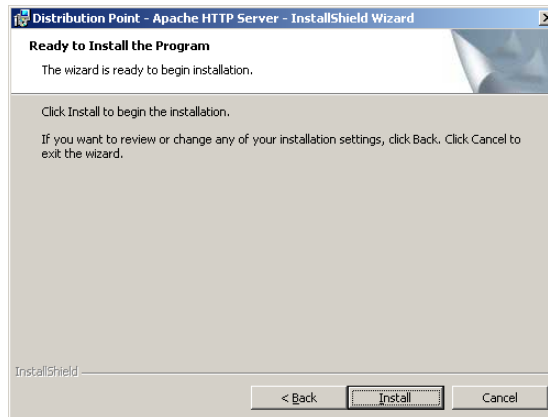


Figure D.9 Registration page



14. Click **Install** to begin the installation

Following the Installation, the *InstallShield Wizard Completed* page will display

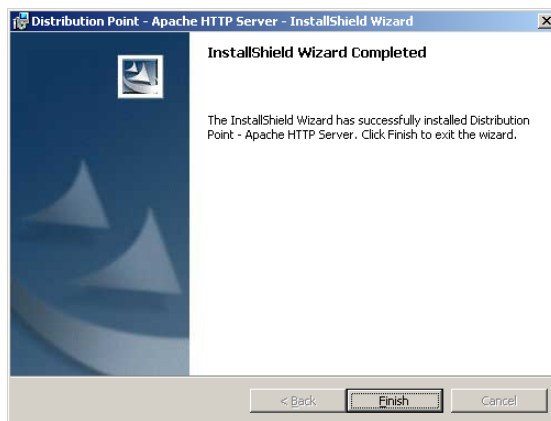


Figure D.10 InstallShield Wizard Completed

15. Click **Finish** to exit the wizard



Note: The service installed by this wizard is called *Distribution Point - Apache HTTP Server*

Configuring the Distribution Point

During the installation of the Distribution Point 6.3, the custom Novell installer will configure the files in the `conf` subdirectory to reflect 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. Rather the new file will be appended with a `.default` extension. Therefore, you must manually update your configuration file by referencing and copying the settings in the `.default` file into your `.conf` file.

Table D.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 (0 = Never exit)
ServerRoot <i>path</i>	The Distribution Point installation path Defined during installation	C:\Program Files\Apache Software Foundation\Apache2.2\
Listen <i>value</i>	Ports on which the Distribution Point monitor incoming traffic Defined during installation	80
ServerAdmin <i>value</i>	The Distribution Point Administrator's e-mail address Defined during installation	
ServerName <i>value</i>	The Distribution Point's Hostname (includes port if Distribution Point was not installed on port 80) Defined during installation	
DocumentRoot <i>path</i>	The directory that forms the main document tree which is visible from the web Uses the install path defined during installation	C:\Program Files\Apache Software Foundation\Apache2.2\htdocs
ErrorLog <i>path</i>	Defines the location of the Distribution Point Error Logs	logs/error.log †
† Due to Apache using Unix-style names internally, you must use forward slashes (/) instead of backslashes (\) when identifying filenames within a directive. Example: C:/logs/error.log not C:\logs\error.log		



Table D.1 Configurable Distribution Point Directives

Directive Name	Usage	Default Value
LogLevel <i>value</i>	Controls the level of error logging	Warn
ProxyRequests <i>value</i>	Indicates whether forward (standard) proxy requests are enabled	On
CacheRoot <i>path</i>	The directory root where cache files are stored Defined during installation	C:\Program Files\Apache Software Foundation\Apache2.2\cache
CacheMaxFileSize <i>value</i>	The maximum file size (in bytes) that will be cached	100000000000
CacheMinFileSize <i>value</i>	The minimum file size (in bytes) that will be cached	1
CacheEnable <i>type URL</i>	Enables caching of the specified URLs using the defined storage type	disk /disk http://patchlink-1
CacheDirLevels <i>value</i>	Then 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>	Disables caching of the specified URLs	http://security.update.server/update-list/
† Due to Apache using Unix-style names internally, you must use forward slashes (/) instead of backslashes (\) when identifying filenames within a directive. Example: C:/logs/error.log not C:\logs\error.log		



Tip: If you require additional details regarding the Distribution Point (Apache HTTP Server Version 2.2.3), please 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.



E 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

An agent's communication with the ZENworks Patch Management Server, and it's behavior is defined by its policies, which are stored in the computer's registry. The policy options 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.



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.



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-compliancy 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 system. A signature typically contains multiple fingerprints. If there is more than one unique configuration, there will be multiple signatures.

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.



F Index

A

AAA Architecture	335
Access Control List.....	335
accounting.....	335
Active Directory.....	335
ActiveX	
definition of	335
template library.....	335
Address Resolution Protocol	335
agent.....	336
agent policies.....	335
ASP	336
authentication	336
vs. authorization.....	336
Authenticode.....	336
authorization.....	336
vs. authentication	336
automatic caching system.....	336

B

baseline	336
behavior.....	336
browser.....	337

C

CDL	337
chained deployment.....	337
Client.....	337
code signing	337
COM	337
communication Interval.....	337
compliance	337

Component Object Model	337
Concurrent Deployment Limit	337
context.....	338
control panel applet	338
credential	338
cross-platform.....	338
CVE	338

D

DAU.....	30, 338
DCOM	338
deadline	338
Decryption	339
Decryption Key.....	338
deployment.....	339
standard.....	348
deployment flag.....	339
deployment script	339
Deployment Wizard.....	84
DHCP	339
dirty state.....	339
dirty state 'R'	339
dirty state 'C'	339
Discover Applicable Updates... 30, 338	
distribution package	
see package	
Distribution Point	
installing.....	326
DLL.....	339
DNS.....	340
domain.....	340



E

encryption 340

encryption key 340

endpoint..... 340

F

fingerprint 340

firewall..... 340

FQDN 341

FTP 341

G

Global Subscription Server 341

group..... 341

GUID 341

H

host name 341

hours of operation 341

HTML 342

HTTP..... 342

HTTPS..... 342

hyperlink 342

I

IANA 342

IIS.....4, 342

install

 Distribution Point..... 326

IP 342

IP address 342

J

JAVA 343

JRE 343

L

LDAP..... 343

library 343

license information..... 235

localhost..... 343

localprofile.txt 343

M

MAC address 343

macro 343

mandatory baseline..... 344

mandatory baselines

 applying 179

 removing deployments created by.

 184

Microsoft Internet Explorer..... 4

Microsoft Internet Information Services

 4

Microsoft Windows Server 2003 3

MSDE..... 344

MSI installer..... 344

N

NDS..... 344

NetWare 344

Novell Directory Services 344

Novell ZENworks Patch Management

 Server..... 344



O

OSD	344
OVAL	345

P

package	345
package deployment flag 63, 105, 339	
package script	345
Patch Developers Kit	345
Patch Management	
administrator	345
user	345
patch management	345
policies	346
policy server	346
port number	346
posture	346
pre-requisite	346
Products page	235
proxy server	346

Q

Q-chain	346
quarantine	346
quiet mode	346

R

RARP	347
Refresh Inventory Data	347
registry	347
remediation	347
replication	347
report	347
RID	347

role	347
rules	347

S

Secure File Transfer Protocol	347
server	348
signature	348
SQL	348
SQL Server	348
SSL	348
SSL Certificate	348

T

TCP/IP	348
--------------	-----

U

UDP	349
URL	349
user name	349
user roles	
assigning	225
creating	222
disabling	226
editing	224
enabling	227
removing	228
users	
adding	207, 215
changing password	219
creating	207
deleting	218
editing	217
removing	217
UTC	349



V

VeriSign certificate..... 349

Vulnerabilities 29

vulnerability 349

vulnerability report 349

W

web server..... 350

Windows-based authentication 206

WWW..... 350

X

XML 350

Z

ZENworks Patch Management Agent...
350

ZENworks Patch Management Server..
350





Novell, Inc.

1800 South Novell Place
Provo, UT 84606

www.novell.com
phone: 800.858.4000

