

The Novell logo is displayed in red text on a gray background. The word "Novell." is written in a sans-serif font, with a period at the end.

Novell® ZENworks® Patch Management Server

Powered by PatchLink Update

User Guide

© Novell, Inc. 1997 - 2005. ALL RIGHTS RESERVED

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

02_012N-6.2.2a

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

Copyright © 2005 Novell, Inc., All rights reserved. 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: NOVELL, INC. MAKES NO REPRESENTATIONS OR WARRANTIES IN REGARDS TO THE ACCURACY OR COMPLETENESS OF THE INFORMATION PROVIDED IN THIS MANUAL. NOVELL, INC. 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. NOVELL, INC. 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: Novell, ZENworks® Patch Management Server, ZENworks Patch Management Server, and Novell Agent are registered trademarks of Novell®, Inc. All trademarks mentioned in this manual are the property of their respective owners.

Table of Contents

Table of Contents ii

Chapter 1: ZENworks Patch Management Overview 1

Overview	1
Key features	2
System Requirements	4
Hardware Requirements	4
Software Requirements	4
Supported Operating Systems	5

Chapter 2: Getting Started 9

Understanding the ZENworks Patch Management Server Interface	9
Determining Access	12
Windows-based Authentication	12
ZENworks Patch Management Server Access Rights	12
Installing Your Agents	13

Chapter 3: ZENworks Patch Management Home Page 15

ZENworks Patch Management Server Status Page	17
Replication Status	17
Deployment Status	18
Cache Status	18
Comprehensive Graphical Assessments	18
Patch Status for all Computers	18
Patch Status for all Vulnerabilities	19
Status for all computers	19
Baseline Status for all Groups	20
Current Status Information	20
License Expiration	21
Home Page Security	22

Chapter 4: Vulnerabilities**23**

Vulnerability Analysis	23
Vulnerability Impact	28
Statistics	29
Page Functions	30
Action Menu	31
Vulnerability Analysis Security	33
Vulnerability Details	34
Agent Status	35
Page Functions	35
Action Menu	35
Vulnerability Analysis Security	36

Chapter 5: Packages**37**

Packages Page	38
Package Statuses & Types	40
Page Functions	41
Action Menu	41
Distribution Packages Security	42

Chapter 6: Creating and Editing Packages**43**

Package Editor Screen	43
Screen Functions	43
Operating Systems Screen	46
Add Files Page	47
Macros	49
Create Scripts Page	51
Script Types	52
Script Editor	52
License Agreement Page	54
Summary Page	55
Upload Status Page	56
Upload Summary Page	57

Chapter 7: Deployments

59

Overview	59
Package Deployments Page	59
Deployment Types and Status	62
Deployment Summary	64
Page Functions	65
Action Menu	65
Deployment Details Section	67
Page Functions	70
Action Menu	70
Package Information Page	71
Page Functions	72
Action Menu	72

Chapter 8: Patch Deployments

73

Understanding Deployments	73
Understanding the ‘Dirty State’	73
Dirty State “R”	74
Dirty State “C”	74
Rebooting Agents	74
Understanding the ZENworks Patch Management Deployment Logic	74
Chaining Deployments	75
Using Deadlines	76
Using the Deployment Wizard	76
Introduction Page	76
Computer/Groups Selection Page	78
Package Selection Page	80
Associated Vulnerability Analysis Page	82
Licenses Page	83
Deployment Options Page	84
Schedule Configuration Page	86
Package Deployment Order and Behavior Page	91
Package Deployment Behavior Options Page	95
Notification Options Page	99
Deployment Notification Options	99
Reboot Notification Options	100
Deployment Confirmation Page	101
Package Applicability Page	105
Deployment Summary Page	106

Change	107
Page Security	108
Package Deployments Security	108
Distribution Packages Security	108
Package Information Security	109
Deployments Details Security	110
Deployments Results Security	110

Chapter 9: Computers

111

Computer Information Page	111
Computer Information Columns	111
Agent Status	112
Page Functions	112
Action Menu	113
Computers Security	114
Computer Details Section	115
Computer Information	116
Agent Information	116
Group Information	116
Policy Information	116
Page Functions	117
Action Menu	117
Computer Details Security	117
Vulnerabilities by Computer	118
Page Functions	118
Action Menu	119
Computer Vulnerability Security	119
Computer Inventory Summary	120
Action Menu	120
Computer Inventory Security	121
Computer Deployments	122
Action Menu	122
Computer Deployments Security	123

Chapter 10: Inventory**125**

About Inventory	125
How it works	126
Detection Agent	126
Detection Results	128
Access Levels	129
Using the Workspace	130
Viewing Inventory Data	130
Default Views	131
Creating Default Views	131
Inventory Types	131
Operating Systems View	132
Software View	133
Hardware View	134
Services View	135
Inventory Groups	137
Inventory Devices	138
Searching Inventory	139
Search Rules	139
Search Dependencies	140
Exporting Inventory Data	141
Scanning Inventory	142
Printing Inventory Pages	143

Chapter 11: Groups**145**

Defining Effective Grouping Methods	145
Groups Page	146
Group Status	147
Page Functions	148
Action Menu	148
Groups Security	149
Group Information	150
Lock Information	153
Page Functions	153
Action Menu	153
Security	153
Vulnerabilities by Group	154
Page Functions	155
Action Menu	155

Group Vulnerability Security	156
Group Inventory Summary	157
Page Functions	158
Action Menu	159
Group Inventory Security	159
Group Membership	160
Page Functions	161
Action Menu	161
Group Membership Security	162
Group Deployments	163
Page Functions	163
Action Menu	163
Group Deployments Security	164

Chapter 12: Working With Groups

165

Add a Group Wizard	165
Group Property Screen - Info	165
Group Property Screen - Members	167
Group Property Screen -Mandatory Baseline	169
Edit a Group Wizard	171
Advanced Group Management	171

Chapter 13: Mandatory Baselines

175

Groups Mandatory Baseline Tab	176
Column Descriptions	176
Applicable User Access Rights	179
Vulnerability Analysis Results Page	180
Column Descriptions	180
Applicable User Access Rights	181
Applying a Mandatory Baseline	182
Removing Deployments Created By Mandatory Baselines	189

Chapter 14: Reporting**193**

About Reports	193
Access Levels	194
Report Parameters	194
Computers	194
Groups	194
Deployments	195
Packages	195
Vulnerabilities	195
Date Range	195
Report Types	196
Agent Policy Report	196
Computer Duplicate Report	197
Computer Status Report	197
Deployment Detail Report	198
Deployment Summary Report	198
Mandatory Baseline Detail Report	199
Mandatory Baseline Summary Report	200
Package Compliance Detail Report	200
Package Compliance Summary Report	201
Vulnerability Analysis Report	202
Using the Workspace	203
Reporting Page	203
Report Parameters Page	204
Displaying Time and Date	205
Report Page	205
Creating Reports	206
Available and Selected Options	206
Searching and Updating	207
Exporting and Printing Reports	207
Exporting Reports	208
Printing Reports	208
Troubleshooting	209
Active Server Pages (ASP) Error	209
Reports Do Not Reflect Recent Patch Activity	210

Chapter 15: Managing Users and Roles**211**

About User Management	212
Access Levels	213
Users	213
Creating a ZENworks Patch Management Server User	213
Adding Existing Windows Users	214
Roles	214
Predefined System Roles	214
Custom Roles	215
Access Rights	216
Accessible Groups	220
Accessible Computers	220
Working with Users	221
Creating New Users	221
Adding Users	223
Editing User Profiles	226
Removing ZENworks Patch Management Server Users	228
Deleting ZENworks Patch Management Server Users	229
Working with Roles	230
Creating User Roles	231
Editing User Roles	236
Assigning User Roles	237
Disabling User Roles	240
Removing User Roles	240
Exporting User Data	241

Chapter 16: Configuring Default Behavior**243**

About Configuration Options	243
Configuration Options	244
Monitoring the Subscription Service	245
Access Levels	246
Subscription Service Information	246
Subscription Service History Section	247
Action Menu	248
Verifying Subscription Licenses	250
Access Levels	250
License Information	251
Action Menu	251
Creating a Default Account Policy	253

Access Levels	254
Summary Information	254
Concurrent Deployment Limits	255
Deployment Agent Defaults	256
Discovery Agent Defaults	257
Deployment and Reboot Deadline Options	257
Deployment Messages	258
Legacy Agent Configuration	258
ISAPI Settings	259
IAVA Settings	259
Action Menu	260
Customizing and Administering Agent Policy Sets	261
Access Levels	262
Summary Information	262
Resolving Agent Policy Conflicts	264
Adding (Creating) a New Policy	264
Editing a Policy	267
Removing a Policy	270
Exporting Policy Definitions	271
Assigning E-mail Alerts	272
Access Levels	272
E-Mail Notification Settings	273
Alert Thresholds	273
Action Menu	274
Contacting Technical Support	276
Access Levels	276
ZENworks Patch Management Server Information	277
Other Installed Novell Products	277
Component Version Information	278
Subscription Status	278
Novell Contact Information	278
Action Menu	279

Appendix A: Hardening ZENworks Patch Management 281

Install Your Server With SSL	281
Turn Off Non-Critical Services	281
Use Secure Passwords	281
Turn Off Windows Networking	282
Put Your ZENworks Patch Management Server Behind a Firewall	283
Lock Down Unused TCP and UDP Ports	283
Turn Off File and Printer Sharing	287
Apply the Microsoft SQL Patches	288

Appendix B: ZENworks Patch Management Server Reference 289

ZENworks Patch Management Server Security	289
Web Site Authentication	289
Web Site Encryption via SSL	289
User (Security) Roles	289
Error Pages	290
Error Codes	290
Novell Websites	291
Computer Status Icons	291

1 ZENworks Patch Management Overview

Overview

The ZENworks Patch Management Agent scans the host computer and compiles information on operating system, software, hardware, and services on that machine. 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 computer. If applicable, the ZENworks Patch Management Agents perform another scan using the patch fingerprints incorporated into each vulnerability to determine the computer's patch status in relation to that vulnerability. Once patch status is established, the Novell Administrator can deploy the desired vulnerability to each applicable computer on the network.



Note: As recommended with all patches, you should first deploy the patch within your test environment before rolling it out into production.

Patch deployment consists of three simple steps:

1. Use the Vulnerability detail view to see the computers that are not patched
2. Select the computers that should receive the patch
3. Schedule the date and time for the deployment to occur

Once a deployment has been scheduled, the detail view shows you the status of the ZENworks Patch Management Agent - how many computers are downloading the patch, how many completed successfully, and delivery error codes in the event of an unsuccessful deployment.

Once installed, your ZENworks Patch Management Server stays current with the latest patches and fixes by daily communication with the Subscription Service via its secured connection. When a newly released patch matches your stored network profile, you receive proactive e-mail notification and the new vulnerability appears on the ZENworks Patch Management Server interface with the description and business impact as well as the list of computers that require it. At this time you can choose to deploy the patch or disregard it.

Key features

ZENworks® Patch Management v6.2.2 provides you with a new set of features that substantially raise the patch, vulnerability, and compliancy management capabilities for your organization. Included in this release are features that enhance Novell's asset management capabilities, simplify agent management activities, provide new options for remediation deployments, and increase support for large enterprise implementations.

Table 1.1 ZENworks® Patch Management v6.2.2 Key Features

Increased Large Enterprise Support	Subscription Service Customization - Customize subscription notifications to include only the platforms and languages needed
	Optimized Subscription Service Update - Incremental subscription service updates increase reliability and reduce WAN loads
	Agent/Server Communications Optimization - Improved transaction/query efficiency increases performance and scalability
	Communication via Authenticated Proxy - Option to require agent authentication to proxy servers increases deployment security
Enhanced Asset Management	Enhanced Standard Inventory - Additional items for asset inventory (e.g. computer model/serial number, hyper-threaded CPUs, virtualized hardware, last logged user, reboot time, etc.)
	Customizable Inventory - Retrieval and manipulation of custom inventory data created locally by customer scripts, applications, etc.
Advanced Remediation Options	Immediate Agent Execution - ZENworks Patch Management Server can initiate real-time commands to agents for immediate execution
	Deployment Deadlines - Administrative option provides end-users more flexibility while ensuring implementation by a specific date/time
	Improved End-User Deployment Experience - Administrative options to allow end users to cancel non-critical deployments

Table 1.1 ZENworks® Patch Management v6.2.2 Key Features

Simplified Agent Management	Discovery and Agent Installation Wizard - Step-by-step wizard discovers unprotected devices and facilitates agent installation
	Improved Active Directory and eDirectory Discovery - Simplified set up and execution for these and other LDAP directories
	Flexible Agent Management Center (AMC) Installation - Multiple instances of AMC can cover multiple network segments
	Key New Features - Wake-On-LAN for agent installation, auto-population of groups, enhanced agent detection, PC list import
	Improved Agent for Macintosh - Control Panel and PDDM (Novell Desktop Deployment Manager) integration; flexible start-up options for: process ownership, detection-only operation, and reinstallation

System Requirements

Hardware Requirements

For every 1000 devices managed using ZENworks Patch Management Server, we recommend:

- Intel Pentium 1 GHz-processor
- 1024 MB of RAM
- 20 GB of available disk space
- A LAN connection (enabling a browser connection to the Internet)



Note: Deployments over multiple locations or large numbers of nodes may require additional resources. Please check with your Novell representative.

Software Requirements

- Windows Server™ 2000 Service Pack 4 or higher (Standard or Advanced)
- Windows Server 2003 (Standard or Enterprise)
- Windows Server 2003 Service Pack 1
- Windows® XP Service Pack 1 or higher (for evaluation only)
- Microsoft® Internet Explorer 5.01 (or higher)



Notes:

- All operating systems should be the default installation with load additional software loaded prior to installing ZENworks Patch Management
- You must **NOT** have Microsoft SQL Server, Microsoft SQL Server Desktop Engine (MSDE), or Microsoft Access installed on the ZENworks Patch Management Server target system
- Do not install Netscape® 5 (or higher) until after successfully installing ZENworks Patch Management
- Do not install the server software on a Primary Domain Controller (PDC). Installation onto a PDC is not supported in this release of ZENworks Patch Management
- In many cases, when deploying the agent, you must be logged in as a Domain Administrator

Supported Operating Systems

The charts below list the operating systems and machine architectures on which the ZENworks Patch Management Agent v6.2.2 is known to successfully install and operate.

Table 1.2 Supported Operating Systems

Vendor	Operating System	Version
Apple®	Mac OS® X Panther®	10.3.8 & 10.3.8 Server
		10.3.7 & 10.3.7 Server
		10.3.6 & 10.3.6 Server
		10.3.5 & 10.3.5 Server
		10.3.4 & 10.3.4 Server
		10.3.3 & 10.3.3 Server
		10.3.2 & 10.3.2 Server
		10.3.1 & 10.3.1 Server
		10.3 & 10.3 Server
Apple	Mac OS X Jaguar	10.2.8 & 10.2.8 Server
		10.2.7 & 10.2.7 Server
		10.2.6 & 10.2.6 Server
		10.2.5 & 10.2.5 Server
		10.2.4 & 10.2.4 Server
NOTE: The UNIX agent requires Sun’s Java		

Table 1.2 Supported Operating Systems

Vendor	Operating System	Version
Microsoft®	Windows	XP Professional
		XP Home
		Server 2003, Web Edition
		Server 2003, Standard Edition
		Server 2003, Enterprise Edition
		NT Server 4.0, Terminal Server Edition
		NT Server 4.0, Enterprise Edition
		NT Server 4.0
		NT Workstation 4.0
		2000 Advanced Server
		2000 Server
		2000 Professional
		Me
		98 Second Edition
		98
		95 OSR25
		95 OSR2
		95
Novell®	NetWare™	6.5 Service Pack 3
		6.5 Service Pack 2
		6.0 Service Pack 5
		5.1 Service Pack 8
		5.1 Service Pack 7
NOTE: The UNIX agent requires Sun’s Java		

Table 1.2 Supported Operating Systems

Vendor	Operating System	Version
Sun™	Solaris™	10
		9
		8
		7
		2.6
NOTE: The UNIX agent requires Sun's Java		

Table 1.3 Supported Machine Architectures

Vendor	Operating System	Architecture
Apple	Mac OS X	PowerPC™ G3/G4/G5
Microsoft	Windows	x86
Sun	Solaris	SPARC®
		x86

2 Getting Started

Use this guide as a reference to describe the ZENworks Patch Management Server (ZENworks Patch Management Server).

Understanding the ZENworks Patch Management Server Interface

Contained in each section of ZENworks Patch Management Server, as illustrated by this document, are certain page functions and features designed either to aid the user's tasks, or to simply enhance other functions.



Note: If you have not installed your ZENworks Patch Management Server, you should do so now. Refer to the ZENworks Patch Management Server [Installation Guide](#) for further guidance.

The standard page functions and features are broken down as follows:

Help

The ZENworks Patch Management Server is a very comprehensive, web-based interface, designed to provide users with the information they need to properly patch and manage thier network. It assists new users in learning the product, yet all of the core functionality remains available for advanced users. Throughout the ZENworks Patch Management Server, context sensitive help is provided by clicking on the Help text located in the top menu or the help icon found at the top of wizard and property pages.

Navigation Menu

The user interface provides a consistent and easy to use navigation menu, which is always present across the top portion of the screen. This navigation menu quickly takes you to the various major sections of ZENworks Patch Management Server, as well as providing secondary notification of what section you are currently in. This navigation menu will behave differently based on your defined access rights associated with your user role.

[Home](#) | [Vulnerabilities](#) | [Inventory](#) | [Packages](#) | [Computers](#) | [Groups](#) | [Users](#) | [Reports](#) | [Options](#) | [Help](#)

Figure 2.1 Navigation Menu

Action Menu

A variety of context sensitive actions are always located along the bottom of the page. These buttons provide quick access to all the common actions available for each page.

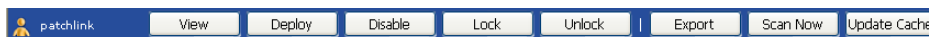


Figure 2.2 Action Menu

Like the navigation menu, the action menu functionality also depends on your user role (and its defined access rights) and the view you are working in (if a filter dropdown selection is applicable).

Display and Hide

The display more information and hide information functions appear regularly throughout ZENworks Patch Management Server. If the display and hide function is present on a certain page, it will be identified each section's Page Functions. The information is refreshed each time it is displayed.



Note: The information expansion functionality is only available for Microsoft Internet Explorer at this time.

Advanced Page Search, Filtering, and View Saving

You can search, filter, and save results views as your default view for the next time you visit the page. This makes the job of finding what you are looking for much easier and less time consuming. The advanced page search, filtering dropdown menus, and saving functions appear in various ZENworks Patch Management Server pages.

 A search and filtering interface. It includes a text input field for 'Search (vulnerability name/CVE no.):', a dropdown menu for 'Status:' with 'Not Patched' selected, a dropdown menu for 'Results for Groups:' with 'All' selected, and a dropdown menu for 'Impact:' with 'Critical Patches (NEW)' selected. Below these are checkboxes for 'Save as Default View:' and an 'Update View' button.

Figure 2.3 Page Search and Filtering

Depending on what page you are viewing determines your ability to search, filter, and save your viewable results. For instance, you may search Inventory for more granular results by entering the computer name text into the Search field and clicking on the Update View button. This will return the computer(s) having the name of the entered text. You may then click the Save as Default View button to save your filtered view as your default view for the next time the page is visited. Page search, filtering dropdown menus, and saving functionality varies depending on what page you are on. To understand the full advanced page search, filtering dropdown menus, and saving functions appearing on the ZENworks Patch Management Server pages, see the respective Page Functions sections of this document where applicable.

Sort

The sort function enables views by Ascending (default) or Descending order by clicking on a sort enabled column heading or the sort icon.

Mouse Overs

Additional information may be displayed by hovering your mouse pointer over an enabled icon or link.

Display (Pagination)

Depending on the amount of items available for display and what page you are viewing, determines the display function. The Display function, if enabled, is located at the bottom above the Action Menu.

- **Next:** To display the next page of computers, click on the next button. If the last computer is displayed, the next button is disabled.
- **Previous:** To display the previous page of computers, click on the previous button. If the first computer is being displayed, the previous button is disabled.
- **Computers per Page:** The computer list initially displays up to 100 computers per page. To change the number of computers to display per page, enter a new number in to the Computers per Page input field. To display all computers enter a zero in the input field.

Auto Refresh

Where present and when selected, the Auto Refresh function automatically refreshes the page every 15 seconds.

Checkboxes

Checkboxes are used to either select a single item or a group of items to initialize them for a certain function or selection. Checkboxes appear throughout the ZENworks Patch Management Server and are not visible in Netscape.

Determining Access

Determining who gets access to ZENworks Patch Management Server, what they can see, and what they can do is completely user-configurable. The goal of ZENworks Patch Management Server Security is not to mandate how you define your security policies, but to allow you the ability to effectively institute your own security policies. Security access is determined by two mechanisms: Windows-based authentication and ZENworks Patch Management Server access rights.

Windows-based Authentication

Authenticating to ZENworks Patch Management Server is handled by the Windows operating system. Any user(s) who are members of a local Windows group, ZENworks Patch Management Server Administrators, will gain all the necessary rights and abilities to log on to the web site. Authorization of what users can and can not do is handled by Access Rights (see below). Upon installation, the PatchLink user (who is created during the installation) is given the Administrator user role, but you may remove this at any time, as long as there exists at least one user who belongs to the Administrator user role.

ZENworks Patch Management Server Access Rights

Once a user has authenticated into ZENworks Patch Management Server, their assigned user role is checked to see what features (sections of ZENworks Patch Management Server) and functionality (actions they can perform in those sections) they have. Each user role is assigned its own set of groups and computers (computers outside of the membership of the assigned groups) on which their access right-based functionality operates.

If a user manages to get past the Windows security (Domain User who is not a member of the local ZENworks Patch Management Server Administrators group for example), they will be unable to view any sections of ZENworks Patch Management Server, see any groups or computers or perform any actions on them. 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 to ZENworks Patch Management Server and assign them a user role.

Installing Your Agents

Both the deployment (also known as Deployment Agent) and Detection Agent are bundled together and installed at the same time. The deployment agent is a service that is constantly running to ensure that when deployments are ready to start, policy changes, etc., the agent will act on them in a timely manner. The behavior of this agent is entirely defined by the agent's policies, whether the agent is using the default agent policies for ZENworks Patch Management Server or the superset of the group's agent policy sets the agent is a member of. The detection agent will run only when the user on the individual computer initiates it, or the deployment agent deploys the Discover Applicable Updates System Task.

Installing agents is a simple function and there are various installers available to install agents on to your computers. They can be found by clicking on the Install button in the Computers section. This will initialize a screen showing the available ZENworks Patch Management Agent Installers.



Note: If you cannot access the Computers section or do not have access for the Install button speak with your ZENworks Patch Management Server Administrator on obtaining access to those sections of the product.

Refer to the [ZENworks Patch Management Agent Installation Guide](#) for further details regarding the installation of agents.

3 ZENworks Patch Management Home Page

ZENworks Patch Management gives you the ability to detect and patch your workstation and servers across your entire network. The Home Page gives you latest information and status about your ZENworks Patch Management Server (ZENworks Patch Management Server). If ZENworks Patch Management Server licenses have expired, the License Expiration page will be displayed instead. From here you can access the Novell Online Documentation, Support Forum, What is Novell Demo, New Users page, Help Files, Known Issues and Resolutions and the ZENworks Patch Management Server Status Page.

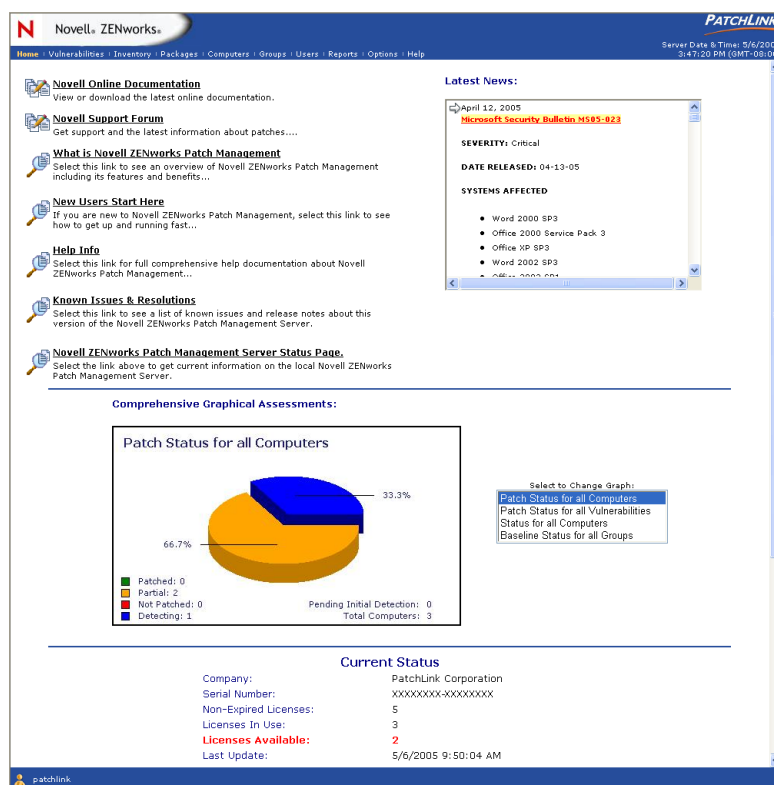


Figure 3.1 ZENworks Patch Management Server Home Page

Novell Online Documentation

The Novell Online Documentation link provides a direct link to all the latest ZENworks Patch Management Server documentation. Follow the various links to provide support, forums, and resources for your ZENworks Patch Management Server.

Novell Support Forum

The Novell Support Forum provides a location where the latest information and technical support about ZENworks Patch Management Server, its processes, functions and features are displayed. You can search through other customer questions and answers to see if their answers can assist you. Additionally you can post your own questions and Novell Customer Service will assist you in a timely manner. Registered users can select to receive notifications when any of the different forum topics receives new activity. Select the Novell Support Forum link to open the Support Forum.

What is ZENworks Patch Management?

What is ZENworks Patch Management provides a detailed overview of the ZENworks Patch Management Server system.

New Users Start Here

New User's Start Here displays a quick start user's guide to understanding the interface, defining access, agent behavior and their installation.

Help Info

Help Info provides comprehensive documentation on ZENworks Patch Management Server.

Known Issues & Resolutions

Known Issues displays a list of Known Issues, Release Notes, and Important Links about ZENworks Patch Management Server.

Latest News

This window displays the latest news, articles, announcements, and press releases direct from Novell.

ZENworks Patch Management Server Status Page

Replication Status

The ZENworks Patch Management Server Status Page shows, at a glance, the Replication Status between the ZENworks Patch Management Server and the Novell Subscription Service. The Type of replication, the Status of the replication, and the Percent Complete are displayed. It also shows the current patch deployment Discovery and Analysis Status; showing whether a patch is being detected, has failed, has not started or was successful.

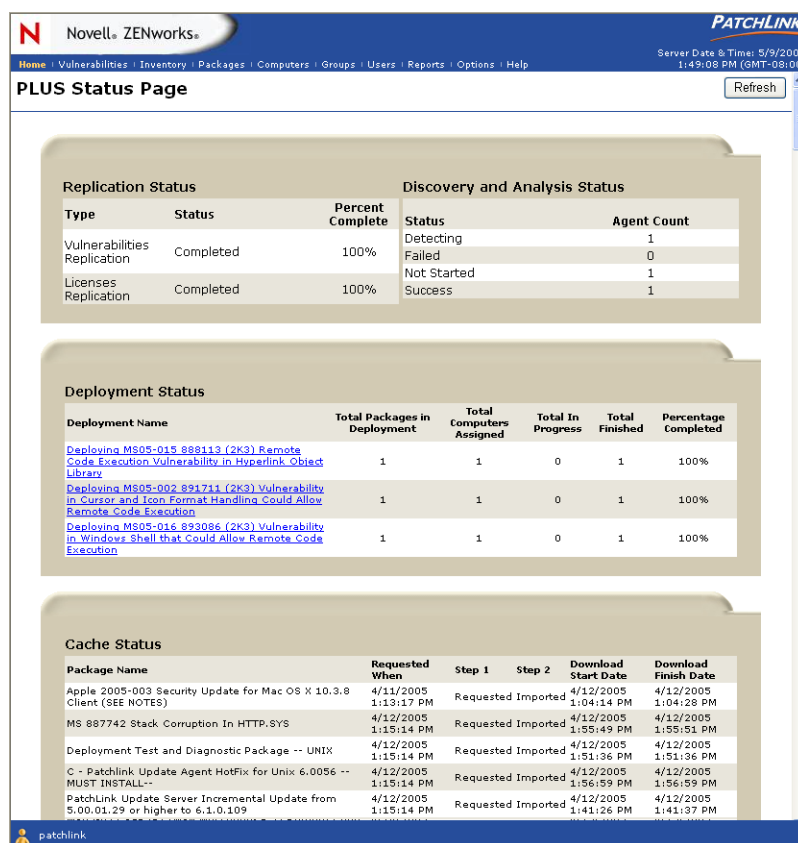


Figure 3.2 ZENworks Patch Management Server Status Page

Deployment Status

The Deployment Status portion of the page shows all deployment statuses so you can quickly check whether a package was deployed. Click on the Deployment Name link to view the computer's details.

Cache Status

The Cache Status is a chronological detail of your packages downloaded into the ZENworks Patch Management Server cache, including: Package Name, Requested When (Date and Time), Steps involved, Download Start Date (Date and Time), and Download Finish Date (Date and Time).

Comprehensive Graphical Assessments

A pie chart graphical display illustrate various statuses of certain patch elements of ZENworks Patch Management Server

There are four different display views with different colors and percentages representing these various statuses. The displays are:

Patch Status for all Computers

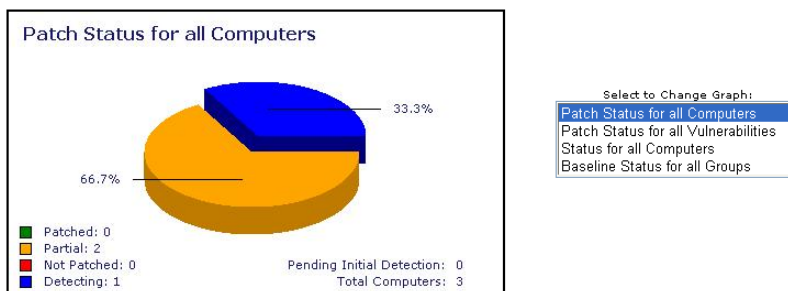


Figure 3.3 Patch Status for all Computers Pie Chart

- Displays the status for all computers which are:
 - Completely Patched
 - Partially Patched
 - Not Patched
 - Performing the analysis detection
 - Pending the initial analysis detection

Patch Status for all Vulnerabilities

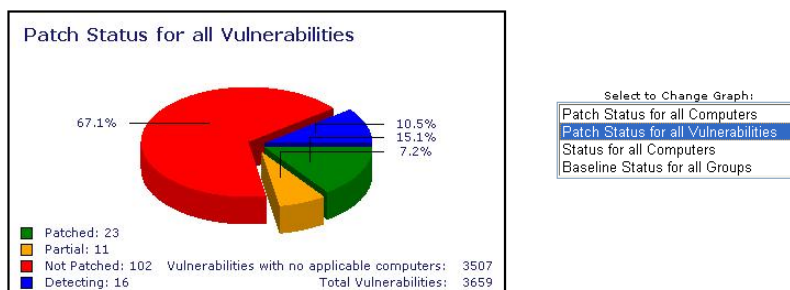


Figure 3.4 Patch Status for all Vulnerabilities Pie Chart

- Displays the status of all vulnerabilities which are:
 - Completely Patched
 - Partially Patched
 - Not Patched
 - Detecting
 - Vulnerabilities which have no applicable computers assigned to

Status for all computers

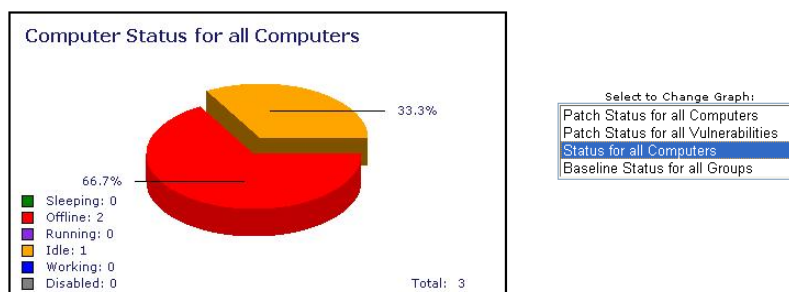


Figure 3.5 Status for all computers Pie Chart

- Sleeping (outside their hours of operation)
- Detect offline or have not communicated with ZENworks Patch Management Server in over two intervals (15 minutes minimum).

- Running: currently performing the analysis detection outside the normal means (rarely occurring when the detection process happens outside of the deployment mechanism).
- Idle: Agent is communicating fine and currently not performing any tasks.
- Working: the Agent is currently working on a task.
- Disabled and unable to perform any tasks.

Baseline Status for all Groups

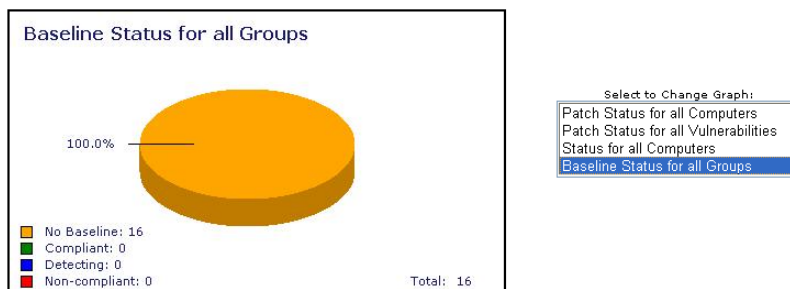


Figure 3.6 Baseline Status for all Groups Pie Chart

- Groups whose members are fully compliant with their baseline.
- Groups whose members are not compliant with their baseline.
- Groups whose members are in the detection and analysis process.
- Groups which have no baseline.

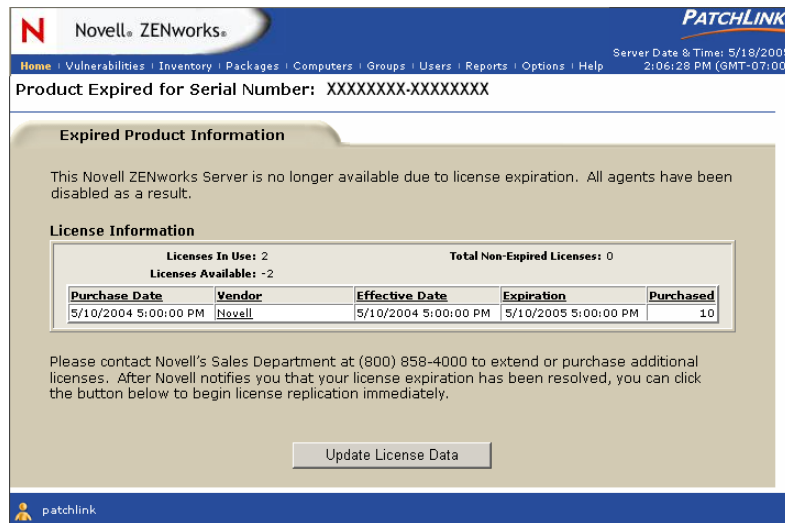
Current Status Information

This provides you with an overall relative condition, position or state of your ZENworks Patch Management Server system.

- **Company:** This is the name of the company that was entered at the time of installation.
- **Serial Number:** This is Your ZENworks Patch Management Server Serial Number.
- **Non-Expired Licenses:** This is the total number of active licenses. Each registered computer requires one license.
- **Licenses in Use:** This is the number of active licenses being used by registered computers.
- **Licenses Available:** This is the number of active and available licenses that can be used to register computers to ZENworks Patch Management Server.
- **Last Update:** This is the Date and Time that ZENworks Patch Management Server last updated itself from the Novell Host Server (PLHOST).

License Expiration

When ZENworks Patch Management Server licenses expire, the agents will no longer be able to perform any of their tasks and the home page display is replaced with this license page. Clicking the **Update License Data** button will initiate the license verification process that connects up to the ZENworks Patch Management Subscription Server and retrieves your updated licenses. This page will automatically refresh to the home page, once your updated licenses have been saved (this usually takes 1 minute)



Novell ZENworks **PATCHLINK**

Home | Vulnerabilities | Inventory | Packages | Computers | Groups | Users | Reports | Options | Help Server Date & Time: 5/18/2005 2:06:28 PM (GMT-07:00)

Product Expired for Serial Number: XXXXXXXX-XXXXXXX

Expired Product Information

This Novell ZENworks Server is no longer available due to license expiration. All agents have been disabled as a result.

License Information

Licenses In Use: 2		Total Non-Expired Licenses: 0		
Licenses Available: -2				
Purchase Date	Vendor	Effective Date	Expiration	Purchased
5/10/2004 5:00:00 PM	Novell	5/10/2004 5:00:00 PM	5/10/2005 5:00:00 PM	10

Please contact Novell's Sales Department at (800) 858-4000 to extend or purchase additional licenses. After Novell notifies you that your license expiration has been resolved, you can click the button below to begin license replication immediately.

[Update License Data](#)

patchlink

Figure 3.7 License Expiration Page



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

Home Page Security

The Home Page section of ZENworks Patch Management Server requires the View Home Page access right. If a user does not have the correct access the access denied error message is displayed.

The status section of the Home Page requires the View ZENworks Patch Management Server Status access right. If a user does not have the correct access, this section is not displayed.

The ability to initiate the License Verification function requires the Manage ZENworks Patch Management Server Licenses access right. If a user does not have the correct access, the button to initiate the verification does not appear.

Contact your Novell Administrator for more information on ZENworks Patch Management Security.

4 Vulnerabilities

The Vulnerabilities page is where the majority of patch management work will be performed. It contains a listing of all patch related vulnerabilities across all the systems registered to the ZENworks Patch Management Server server. It is strongly encouraged that you always manage patches from the Vulnerabilities interface, since it offers the most functionality and granularity.

A Vulnerability consists of the vulnerability description, the signatures and fingerprints required to determine whether the vulnerability is patched or not patched, and the associated package or packages for performing the patch.

Vulnerability Analysis

This section displays the analysis results from the Discover Applicable Updates process on each computer. The analysis gives a simple top-down view of vulnerability patch status. The total number of vulnerabilities is displayed just above the table in the top right corner.

The Vulnerability Analysis can be viewed at the network level, for computer groups, and for individual computers. The various statuses are detailed in this section.

Vulnerabilities PATCHLINK

Home | **Vulnerabilities** | Inventory | Packages | Computers | Groups | Users | Reports | Options | Help

Server Date & Time: 9/9/2005 4:28:45 PM (GMT-08:00)

Vulnerability Analysis Search (vulnerability name/CVE no.): Status: **Not Patched**

Results for Groups: **--- All ---** Impact: **--- All ---**

Save as Default View: ☐

Vulnerabilities		Total: 145									
<input type="checkbox"/>	<input type="checkbox"/>	Vulnerability Name	Impact	1	2	3	4	5	6	7	8
<input type="checkbox"/>	<input type="checkbox"/>	Microsoft .NET Framework 1.1 SP1	Critical - 01	1	1	0	0	2	100%		
<input type="checkbox"/>	<input type="checkbox"/>	MPSB03-08: Update to Flash Player Addressing Local Shared Object Security for IE	Critical - 01	0	1	0	0	1	100%		
<input type="checkbox"/>	<input type="checkbox"/>	MS 826939 Update Rollup 1 for Windows XP	Critical - 01	0	1	0	0	1	100%		
<input type="checkbox"/>	<input type="checkbox"/>	MS 828026 Update for Windows Media Player (7.1, XP, 9) URL Script Command Behavior	Critical - 01	0	2	0	0	2	100%		
<input type="checkbox"/>	<input type="checkbox"/>	MS 831464 IIS 6.0 Compression Corruption Causes Access Violations	Critical - 01	0	1	0	0	1	100%		
<input type="checkbox"/>	<input type="checkbox"/>	MS 842773 Update package that includes Background Intelligent Transfer Service (BITS) version 2.0 and WinHTTP 5.1	Critical - 01	0	1	0	1	2	50%		
<input type="checkbox"/>	<input type="checkbox"/>	MS 870669 Disable the ADODB.Stream object from Internet Explorer (SEE NOTES)	Critical - 01	0	2	0	0	2	100%		
<input type="checkbox"/>	<input type="checkbox"/>	MS01-059 314757 314941 315000 315056 Unchecked Buffer in Universal Plug and Play can Lead to System Compromise	Critical - 01	0	1	0	1	2	50%		
<input type="checkbox"/>	<input type="checkbox"/>	MS02-008 318202 XMLHTTP Control Can Allow Access to Local Files for MSXML 2.6	Critical - 01	0	1	0	0	1	100%		
<input type="checkbox"/>	<input type="checkbox"/>	MS02-008 318203 XMLHTTP Control Can Allow Access to Local Files for MSXML 3.0	Critical - 01	0	1	0	0	1	100%		
<input type="checkbox"/>	<input type="checkbox"/>	MS02-009 - Incorrect VBScript Handling in IE 6.0	Critical - 01	0	1	0	0	1	100%		

patchlink

Figure 4.1 Vulnerability Analysis Page

Clicking the plus sign next to a vulnerability will display the detailed results of the analysis. The same detailed results are displayed when you place a check mark in the box next to the vulnerability and click on the View button.

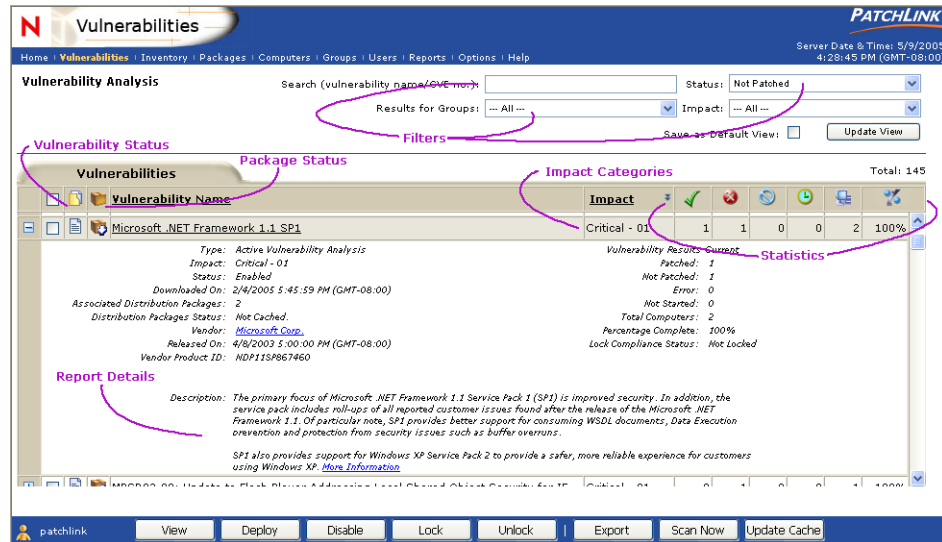


Figure 4.2 Vulnerability Details

Vulnerability Status & Types



Figure 4.3 Vulnerabilities Tab

The status of a vulnerability is indicated by the following icons:

Table 4.1 Vulnerability Status Icons and Descriptions

Beta	New	Current	Status Description
			This is an active vulnerability
			This vulnerability has been locked and is in compliance
			This vulnerability has been locked and is out of compliance
			This vulnerability has been disabled

Additional information about the status of the associated distribution package is displayed upon hovering your mouse pointer over the icon.

- **Beta:** This vulnerability has been released to the BETA community of Novell.
- **New:** This vulnerability has been downloaded from PLHOST and has arrived since you started your ZENworks Patch Management Server session.
- **Current:** This is a current vulnerability that has been downloaded from PLHOST before you started your ZENworks Patch Management Server session.






















Package Cache Status & Types

**Figure 4.4** Vulnerabilities Tab

A vulnerability may have any number of distribution packages associated with it. A distribution package contains the patch to fix the vulnerability. Each distribution package may be cached (downloaded) from the ZENworks Patch Management Host Server (PLHOST) to ZENworks Patch Management Server. They may be cached automatically

if the vulnerability's impact is critical or if a deployment has been created to deploy the package(s). The package cache status icon is a hyperlink. By clicking on the icon, you will initialize a list of the individual packages that are associated with that vulnerability.

Table 4.2 Package Status Icons and Descriptions

New	Current	Tasks	Local	Description
				The package is not cached
				The package has been scheduled to be cached or is in the process of being cached
				An error occurred while trying to cache the package
				The package is cached and ready for deployment
				The package is currently deploying (animated icon)
				The package is disabled

Additional information about the status of the associated distribution package is displayed upon hovering your mouse pointer over the icon.

- **New:** This distribution package has been released and its metadata has been downloaded from PLHOST since you began your ZENworks Patch Management Server session.
- **Current:** This distribution package has been released and its metadata has been downloaded from PLHOST before you began your ZENworks Patch Management Server session.

Vulnerability Impact



Figure 4.5 Vulnerability Impact

The agent list initially sorts by Impact alphanumerically in ascending order. To sort by another field (other than vulnerability or package status) click on the field name. To reverse the alphanumeric sort from ascending to descending, click on field name again.

- **Critical** - Novell or the product manufacturer has determined that this patch is critical and should be installed ASAP. 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 ASAP. While this patch has not been superseded, it is older than 30 days
- **Critical - 05** - Novell or the product manufacturer has determined that this patch is critical and should be installed ASAP. These patches have been superseded and are older than 120 days
- **Critical - Intl** - An international patch, where Novell or the product manufacturer has determined that this patch is critical and should be installed ASAP. 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 reports contain signatures that are common to multiple vulnerabilities. They contain no associated patches are only used in the detection process
- **Informational** - These reports 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. Documentation updates are an example of an item in this category
- **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 reports contain software applications. Typically, this includes software installers. The reports 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 tasks which administrators may use to run various virus detections across their network. Anti-Virus tools and updates are included in this category







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.



Figure 4.6 Vulnerability Statistics

Table 4.3 Column Icon Definitions

Icon	Definition
	Total number of computers or groups that finished the deployment successfully
	Total number of computers or groups that finished the deployment unsuccessfully
	Total number of computers or groups that are assigned the deployment
	Total number of computers or groups that are in the process of executing the deployment
	Total number of computers or groups that finished the deployment
	Percentage of the computers or groups that finished the deployment

You may sort by Ascending (default view) or Descending order by clicking on the corresponding results definition icon.

Page Functions

Display and Hide

Click the plus icon to display additional information and statistics about the represented item. Click the Minus to hide this information from view. The information is refreshed each time it is displayed. This information expansion functionality is only available for Microsoft Internet Explorer at this time.

Advanced Page Search, Filtering, and View Saving

The advanced page search, filtering dropdown menus, and saving functions appear in the Vulnerabilities page header.

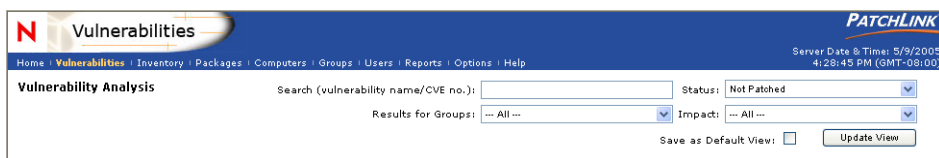


Figure 4.7 Advanced Page Search, Filtering, and View Saving

Search

You may search vulnerabilities for more granular results by entering the vulnerability name (CVE; Common Vulnerabilities and Exposures) text into the Search field and clicking on the Update View button. This will return the vulnerabilities having the name of the entered text. You may then click the Save as Default View button to save your filtered view as your default view for the next time the page is visited.

Results for Groups

Filter by Groups using the dropdown menu and click on the Update View button. This will return the vulnerability having the selected group. You may then click the Save as Default View button to save your filtered view as your default view for the next time the page is visited.

Status

Filter by Vulnerability Status using the dropdown menu and click on the Update View button. This will return the vulnerabilities having the selected status. You may then click the Save as Default View button to save your filtered view as your default view for the next time the page is visited.

Impact

Filter by vulnerability impact using the dropdown menu and click on the Update View button. This is extremely useful when you want to find or display only the vulnerabilities that, for example, are Critical (NEW). This will return the vulnerabilities having the selected impact. You may then click the Save as Default View button to save your filtered view as your default view for the next time the page is visited.

Sort

The sort function enables views by Ascending (default) or Descending order by clicking on a sort enabled column heading or the sort icon.

Mouse Overs

Additional information may be displayed by hovering your mouse pointer over an enabled icon or link.

Checkboxes

Checkboxes are used to either select a single item or a group of items to initialize them for a certain function. Checkboxes appear throughout the ZENworks Patch Management Server and are not visible in Netscape.

Action Menu

- **View** - The vulnerabilities filter controls which vulnerabilities are displayed. There are three options to choose from: Vulnerabilities that have computers applicable to them, Disabled Vulnerabilities or view All Vulnerabilities.
- **Deploy** - This creates a deployment for the selected vulnerability.
- **Disable** - This removes the selected enabled vulnerabilities from being able to be scanned during the Discover Applicable Updates process from all levels of the system (network level down to the individual computer level).
- **Enable** - This re-enables the scanning ability for the selected disabled vulnerabilities during the Discover Applicable Updates process.
- **Lock** - Selecting a vulnerability and clicking on the lock button will save the current vulnerability analysis values. When the analysis is again displayed this data is compared to the current data to determine if the vulnerability is in or out of compliance. If the vulnerability is out of compliance, it is highlighted in red.
- **Unlock** - Selecting a locked vulnerability and clicking on the unlock button will clear out the vulnerability's locked data.
- **Export** - Will export the vulnerability analysis to a comma-separated value (CSV) file. The amount and order of the data is based on what the analysis view is filtered and sorted on.

- **Scan Now** - Initializes a screen that allows you to reschedule the Discover Applicable Updates System Task deployment for immediate execution to all selected computers. To initialize (choose) all computers, click on Scan Now button without selecting any computers. If you choose not to select any computers, the screen will ask you if you wish to confirm the reschedule the Discover Applicable Updates System Task for all of the computers.

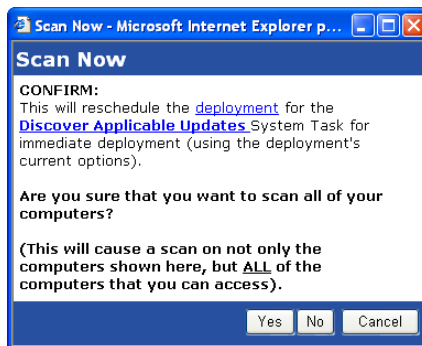


Figure 4.8 Scan Now

- To reschedule the Discover Applicable Updates, select Yes and ZENworks Patch Management Server will reschedule the selected computer(s), initialize a screen stating its success and provide a deployment link to initialize a new screen with the results of the Discover Applicable Updates Deployment. Upon clicking the Close button on the screen, the Computers page will be refreshed. Previously selected deployment options are maintained.
- **Update Cache** - Update Cache initiates the process to cache (or re-cache) the associated distribution packages for the selected vulnerability.

Vulnerability Analysis Security

The Vulnerabilities section of ZENworks Patch Management Server requires the View Vulnerabilities Page access right. If a user does not have the correct access the access denied error message is displayed.

To be able to view the detailed vulnerability analysis requires the View Vulnerability Details access right. If a user does not have the correct access, the hyperlink will not be shown and the View button is disabled.

To be able to change the filter from detected vulnerability to disabled or all requires the Change Vulnerability Filter access right. If a user does not have the correct access, the filter will not have any options to choose from.

To be able to view the associated distribution packages for a given vulnerability requires the View Packages access right. If a user does not have the correct access, the link on the package status image is disabled.

To be able to create a deployment based on the vulnerability analysis requires the Deploy Vulnerabilities access right. If a user does not have the correct access, the Deploy button is disabled.

To be able to enable or disable vulnerabilities from being available by the Discover Applicable Updates process requires the Manage Vulnerabilities access right. If a user does not have the correct access, the Enable and Disable buttons are disabled.

To be able to lock or unlock the selected vulnerabilities requires the Manage UI Vulnerability Locks access right. If a user does not have the correct access, the Lock and Unlock buttons are disabled.

To export all of the vulnerability analyses to a comma-separated value (CSV) file requires the Export Vulnerability Data access right. If a user does not have the correct access, the Export button is disabled.

To restart the Discover Applicable Updates process for all of the computers registered to the ZENworks Patch Management Server requires the Manage System Tasks access right. If a user does not have the correct access, the Scan Now button is disabled.

To cache the associated distribution of the selected vulnerabilities requires the Cache Packages access right. If a user does not have the correct access, the Update Cache button is disabled.

Vulnerability Details

The Status data for each vulnerability is based on your unique configuration of systems. By clicking the vulnerability link, a full list of all computers that require the patch in question will be displayed. From there, the patch can be easily deployed. From the Vulnerabilities page, click on the Vulnerability Name Link to view the computer-level analysis of the vulnerability. The analysis results of the vulnerability are detailed and separated into four tabbed displays. The name of the tab represents status for those computers in the vulnerability analysis.

The screenshot shows the 'Vulnerabilities' page in the PatchLink application. The title bar indicates 'MS05-019 893066 Vulnerabilities in TCP/IP Could Allow Remote Code Execution and Denial of Service'. Below the title, there are four tabs: 'Not Patched', 'Patched', 'Error', and 'Detecting'. The 'Patched' tab is currently selected. A table displays the analysis results for one computer, 'TECHPUBS-PLUS'. The table has five columns: 'Computer Name', 'Other Name', 'Operating System', 'OS Version', and 'Analysis Date'. The 'Analysis Date' for the listed computer is '5/9/2005 3:59:10 PM'. At the bottom of the interface, there are buttons for 'Deploy', 'View Package', and 'Export'.

Computer Name	Other Name	Operating System	OS Version	Analysis Date
TECHPUBS-PLUS	TechPubs-PLUS	Win2K3	Win2K3	5/9/2005 3:59:10 PM

Figure 4.9 Vulnerability Details

Analysis Results

- **Not Patched:** These computers were detected as needing the vulnerability patch.
- **Patched:** These computers were detected as being patched for the vulnerability.
- **Error:** These computers produced an error while determining the patch status for the vulnerability.
- **Detecting:** These computers are either in the process of determining the patch status for the vulnerability or waiting for the detection and analysis process to begin.

Agent Status

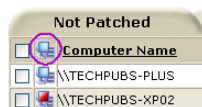


Figure 4.10 Agent Status



Note: Refer to [Appendix B, “ZENworks Patch Management Server Reference”](#) for a complete definition of all available computer status icons.

Agent Information

- **Host Name:** This displays the name of the computer.
- **Other Name:** This displays either the DNS name for the computer or its IP address if it does not have an assigned DNS name.
- **Operating System:** This displays the abbreviated the operating system name
- **OS Version:** This displays additional operating system version information.
- **Last Reported Date:** This is the date the agent last ran the Discover Applicable Updates process.

Page Functions

Action Menu

- **Deploy** - This invokes the Deployment Wizard and allows you to create a deployment for the selected vulnerability. See Section 9; Deploying Packages: Schedule Deployment Wizard for more information.
- **View Package** - This displays the associated distribution packages for the vulnerability.
- **Export** - Will export the vulnerability analysis to a comma-separated value (CSV) file. The amount and order of the data is based on what the analysis view is selected and sorted on.

Vulnerability Analysis Security

The Vulnerability Analysis Details section of ZENworks Patch Management Server requires the View Vulnerability Details access right. If a user does not have the correct access the access denied error message is displayed.

To be able to create a deployment based on the vulnerability analysis requires the Deploy Vulnerabilities access right. If a user does not have the correct access, the Deploy button is disabled.

To be able to view the associated distribution packages for a given vulnerability requires the View Packages access right. If a user does not have the correct access, the View Package button is disabled.

To export the vulnerability analysis to a comma-separated value (CSV) file requires the Export Vulnerability Data access right. If a user does not have the correct access, the Export button is disabled.

5 Packages

Distribution Packages contain all the actual patch software and executable code used for patch deployment. Vulnerabilities may contain several patch packages that will be deployed in a specific order. You can create custom packages from this page that do not require the patented Novell Fingerprinting technology. The ability to create custom packages demonstrates the software distribution capabilities of ZENworks Patch Management Server as well as other tasks that you may require.

Distribution packages will contain whatever you want to deploy on a computer or group. A distribution 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 the packages contain the patches for vulnerabilities, defects or bugs. If you would like to create your own patch, application or script package.

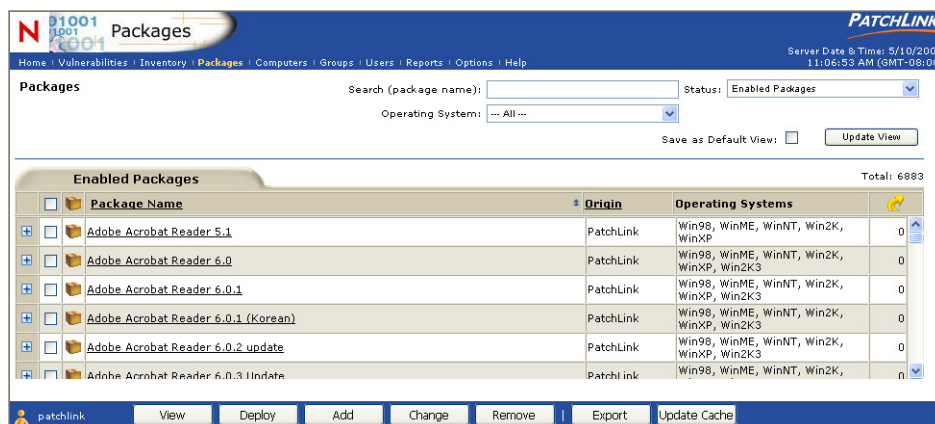


Figure 5.1 Packages View

Packages Page

Package Name

This displays the name of the distribution package. Clicking on the distribution package will display the deployments for that distribution package.

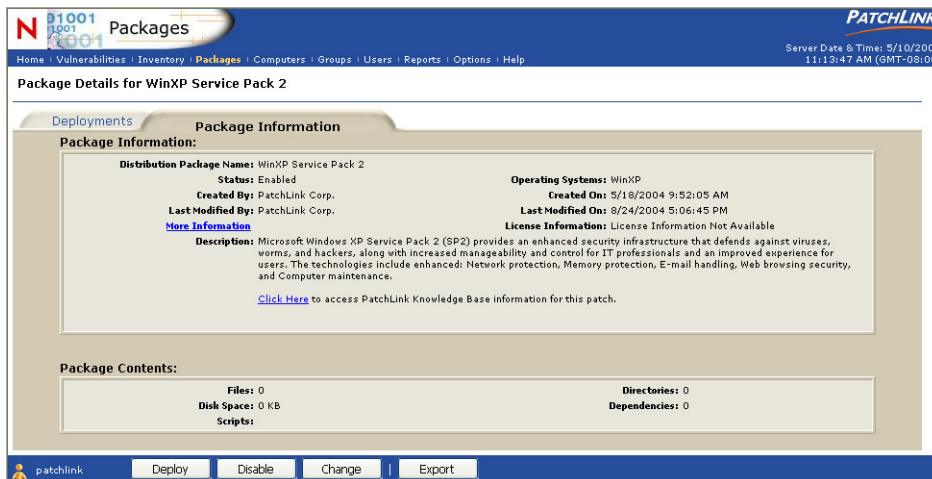


Figure 5.2 Package Information

The package and Deployment details are as follows:

- Distribution Package Name
- Origin
- Status
- Cache Status
- Cache Request Status
- Deployment Availability
- OS Platforms
- The user who created this distribution package
- The date the distribution package was created
- The user who last modified the distribution package
- When the distribution package was last modified
- The date when a deployment was last created for this distribution package Version
- Total number of directories found in the package
- Total number of files found in the package
- Total size of the compressed package size (in KB)

- Total number of prescripts
- Total number of postscripts
- Total number of command-line scripts
- Total number of dependent distribution packages
- Total number of idle deployments
- Total number of running deployments
- Total number of deployments that failed
- Total number of deployments that were fully successful
- Total number of deployments for this distribution package
- Description of the distribution package
- Any additional Notes (if applicable)

Origin

This displays where this distribution package was distributed from.

Operating Systems

This displays operating system platforms that this distribution package can deploy to.

Deployments

The number of deployments previously created for this distribution package.

Package Statuses & Types



Figure 5.3 Package Status

Table 5.1 Package Status Icons and Descriptions

New	Current	Tasks	Local	Description
				The package is not cached
				The package has been scheduled to be cached or is in the process of being cached
				An error occurred while trying to cache the package
				The package is cached and ready for deployment
				The package is currently deploying (animated icon)
				The package is disabled

- **New** - This distribution package has been released and its metadata has been downloaded from PLHOST since you began your ZENworks Patch Management Server session.
- **Current** - This distribution package has been released and its metadata has been downloaded from PLHOST before you began your ZENworks Patch Management Server session.
- **Tasks** - This is a system task distribution package.
- **Local** - This is a locally created distribution package.

Page Functions

Display and Hide

Click the plus icon to display additional information and statistics about the represented item. Click the minus icon to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality is only available for Microsoft Internet Explorer at this time.

Advanced Page Search, Filtering, and View Saving

The advanced page search, filtering dropdown menus, and saving functions appear in the Packages page header.

- **Search** - You may search packages for more granular results by entering the package text into the Search field and clicking on the Update View button. This will return the package(s) having the name of the entered text. You may then click the Save as Default View button to save your filtered view as your default view for the next time the page is visited.
- **Status** - Filter by package status using the dropdown menu and click on the Update View button. You may then click the Save as Default View button to save your filtered view as your default view for the next time the page is visited
- **Operating Systems** - Filter by Operating Systems using the dropdown menu and click on the Update View button. You may then click the Save as Default View button to save your filtered view as your default view for the next time the page is visited

Action Menu

- **View** - This displays additional information about the distribution package. In this view you can also click to view the distribution package's deployments.
- **Deploy** - This creates a deployment for the selected distribution package.
- **Add** - Create a new local distribution package
- **Change** - Change a local distribution package.
- **Remove** - This removes any non-System Task selected distribution packages. ZENworks Patch Management Server will re-download the package metadata (and not the files or scripts) for any deleted Novell provided distribution package (via the ZENworks Patch Management Server's subscription service). ZENworks Patch Management Server will only cache the package if it is critical or being requested by a deployment.
- **Export** - Exports the distribution package list (and their information) to a comma-separated value (CSV) file. The order of the data is based on what the current display is sorted on.
- **Update Cache** - Initiates the process to cache (or re-cache) for the selected distribution packages. If no distribution packages are selected this will re-cache all of the previously cached distribution packages.

Distribution Packages Security

The Distribution Packages section of ZENworks Patch Management Server requires the View Packages access right. If a user does not have the correct access the access denied error message is displayed.

To be able to view the deployments for a distribution package requires the View Deployments access right. If a user does not have the correct access the hyperlink on the Package Name will not be displayed.

To be able to create a deployment for a selected distribution package requires the Deploy packages access right. If a user does not have the correct access the Deploy button is disabled.

To be able to create, change or remove distribution packages requires the Manage Packages access right. If a user does not have the correct access the Add, Change and Remove buttons are disabled.

To export all of the distribution packages and their information to a comma-separated values (CSV) file requires the Export Package Data access right. If a user does not have the correct access the Export button is disabled.

To cache the selected (or re-cache all of the previously cached) distribution packages requires the Cache Packages access right. If a user does not have the correct access, the Update Cache button is disabled.

6 Creating and Editing Packages

The Package Editor steps through the process of creating or editing packages.

Package Editor Screen

From the Packages homepage, click **Add** (or **Edit** if you wish to change a previously created package) on the *Action Menu*. The package editor screen is initialized.

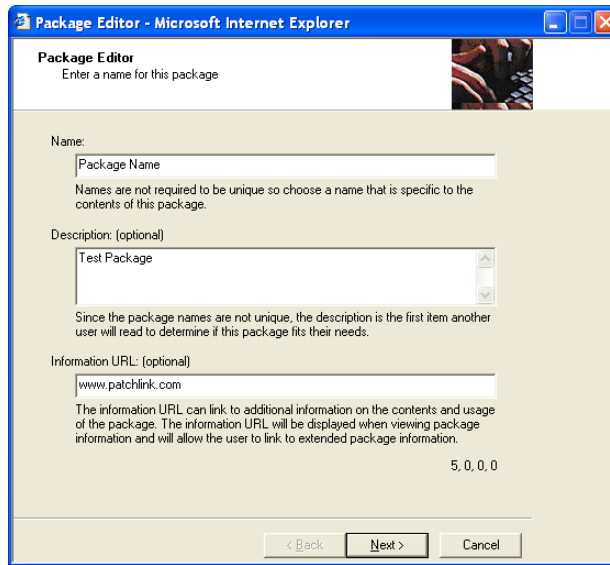


Figure 6.1 Package Editor

Screen Functions

Skip - The Skip the Introduction checkbox will determine if the Introduction page will be displayed each time the wizard is accessed. Click in the checkbox to prevent the Welcome screen from appearing the next time the Package Editor Wizard is initialized.

Back - The Back button is disabled since this is the first page of the wizard. In subsequent screens, the Back button will initialize the previous screen.

Next - The Next button initializes the wizard's next screen.

Cancel - The Cancel button closes the wizard.

Name: - Enter a name or title for your package. The name is required and you will not be able to move to the next page of the wizard until a name has been entered. Make your package names descriptive but short and remember that two or more packages may have the same name. You may change this name at a later time by modifying this package.

Description: - An optional description allows you to specify further information 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.

Deployment Options: - 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 here by including them in with the flags delimiter. To add these, add `(PLFlags: <Your Flags>)` to the description field.

Table 6.1 Package Flag Descriptions and Behavior

Description (flag behavior)	Flag to Display the option	Flag to Select the option
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
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

Table 6.1 Package Flag Descriptions and Behavior

Description (flag behavior)	Flag to Display the option	Flag to Select the option
Suppress Repair	-dsr	-sr
Force the script to reboot when the installation is done	-1d	-1
The installer may reboot	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.

Information URL

The optional 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.

Click on the **Next** button to initialize the wizard's next screen which allows you to select operating systems

Operating Systems Screen

The Operating Systems screen allows you to select which Operating Systems you wish to deploy the package to.

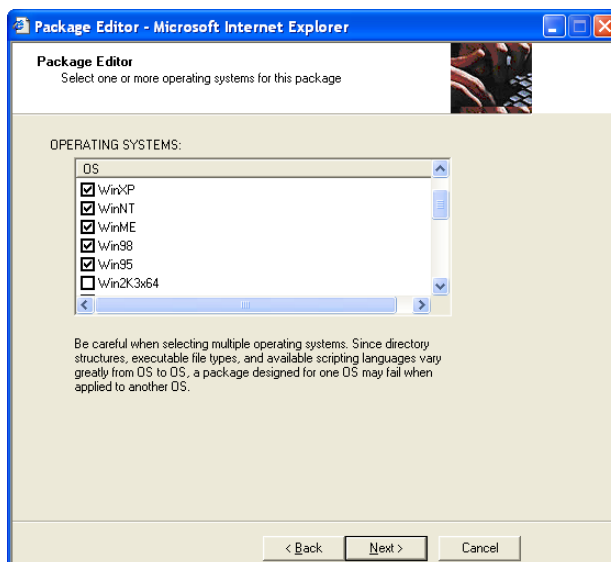


Figure 6.2 Package Editor - Operating Systems

To select an Operating System, click in the checkbox to the left of the Operating System name. You can not click on the **Next** button until you have chosen at least one Operating System.



Note: Be careful when selecting multiple Operating Systems. 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.

Add Files Page

The File Editor screen allows you to add files to the package and describe where the files will be installed when the package is deployed to the computers on your network.

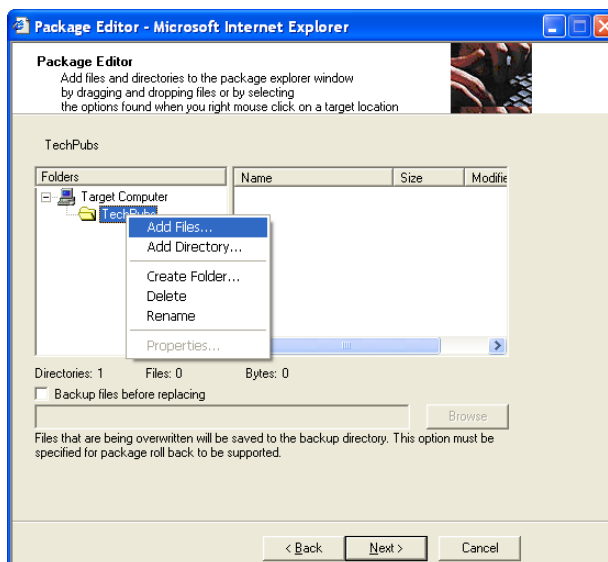


Figure 6.3 Package Editor - Add Files

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.
- 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).

Once the files you want in the package have been added, or while you are adding them, you can create the directory structure for the package. You can right mouse click on most of the items in either window for options on adding, renaming, or deleting items. You can also drag and drop items from one place on the tree to another or from one window to another in much the same way you would in Windows Explorer. 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 % 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.

Macros

The following are a few examples of common macros:

Table 6.2

%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

Not all macros are available on all Operating Systems. Please only choose the macros that are available for the operating systems and configurations you are using. This option only becomes available on the directory level directly under Target Computer.

- **Create Drive** - If your standard computer installation uses drives other than 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.

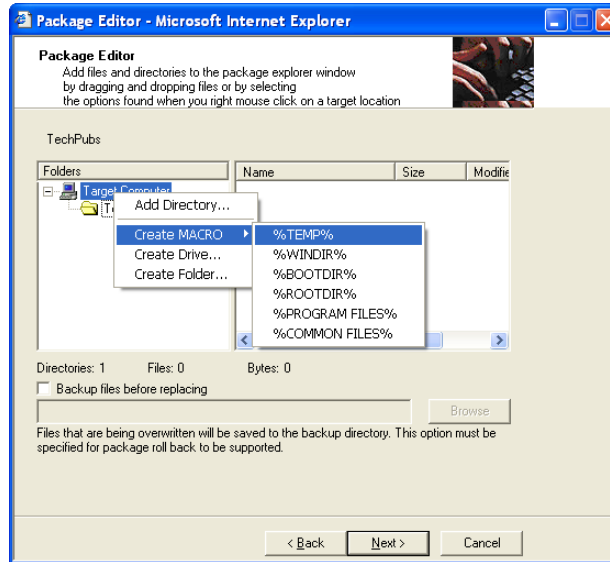


Figure 6.4 Package Editor - Macros



Note: Please 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

Backup Directory

Select “Backup files before replacing” if you wish to 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.

Create Scripts Page

The Create Scripts screen allows you to create scripts that will be run on the computer during the deployment process. A software package can have up to three scripts, one of each type. Scripts are executed in the following sequence:

- Pre-Script
- Files are downloaded and copied to target locations
- Command Line Script
- Post-Script

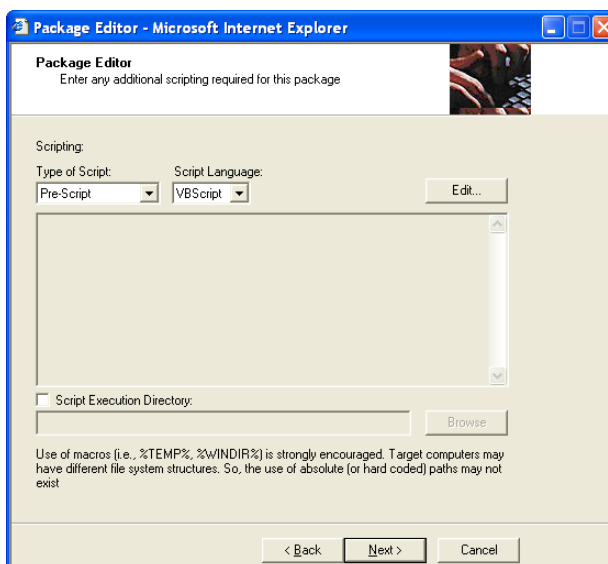


Figure 6.5 Package Editor - Scripts

Script Types

- **Pre-Script** - The Pre-Script can be 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.
- **Command Line** - Command Line Scripts are often used to launch executables. The format is the same as a standard CMD or BAT file.
- **Post-Script** - Post-Script can be used for any clean-up operations, delete files, start services, run a installer, etc. Post-Scripts can take the form of VBScript or JScript.

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 default 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.

Here is a simple VB Script below that will just execute the package once the package gets delivered to the target computer.

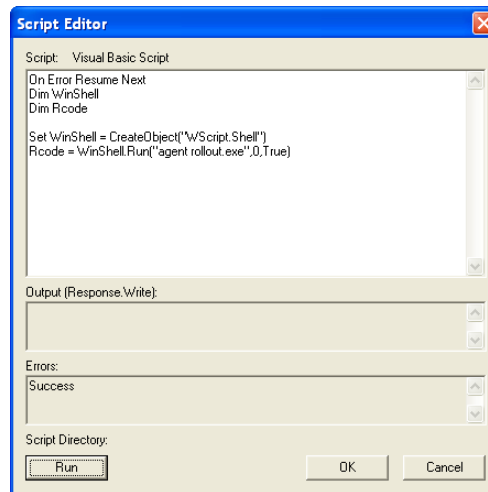


Figure 6.6 Script Editor

Test the script by click the Run button on the bottom left corner. View the Errors field: If the results read “success,” click the OK button to close his window and the Next button to initialize the next window. If you get a failure message, correct your script until a success message is achieved.

Click the Next button to initialize the wizard's next screen, which allows you to select package dependencies.

License Agreement Page

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.

Simply select the License Agreement checkbox and type in the URL destination address of the License Agreement.

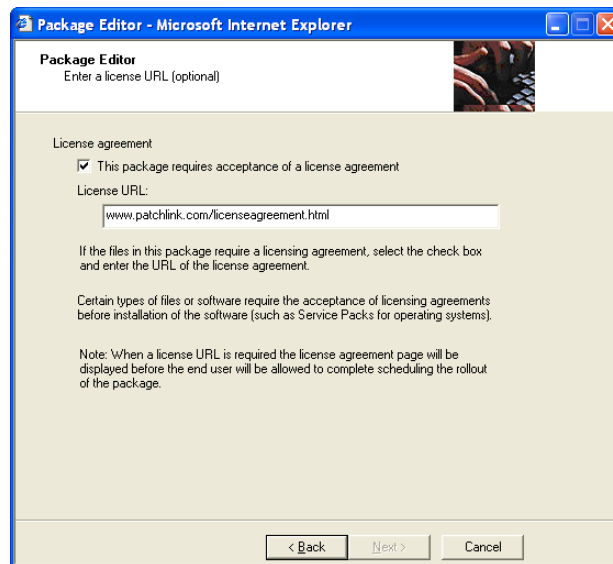


Figure 6.7 Package Editor - License Agreement Page

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.

After entering the License URL (optional), click the Next button to initialize the wizard's next screen, which is a summary of the package.



Note: If you select the License Agreement checkbox, you must type in the URL destination address of the License Agreement to initialize the Next button

Summary Page

The Summary screen displays a simple summary of the package before the package created or the changes are committed.

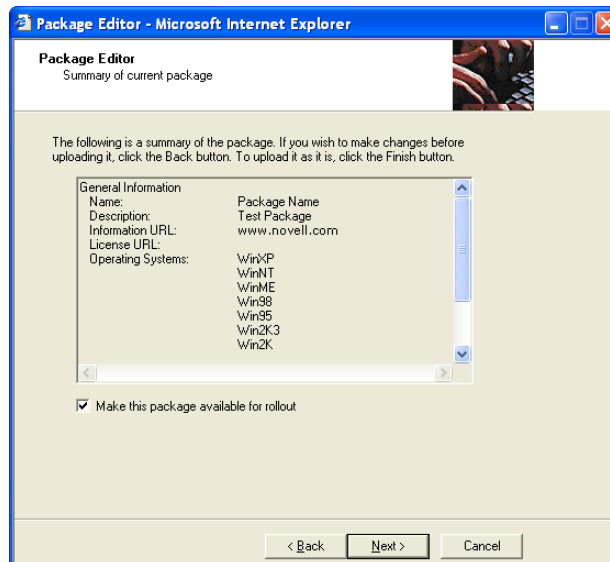


Figure 6.8 Package Editor - Summary

Selecting the Make this package available for rollout checkbox, will enable the package to show up in the list of available packages / available for deployment (once 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 have the package scheduled for deployment at this time.

Click the Next button to initialize the wizard's next screen, which will commit the changes, create the package, and upload the package data.

Upload Status Page

The Upload screen appears verifying that the data is unpacking and uploading.

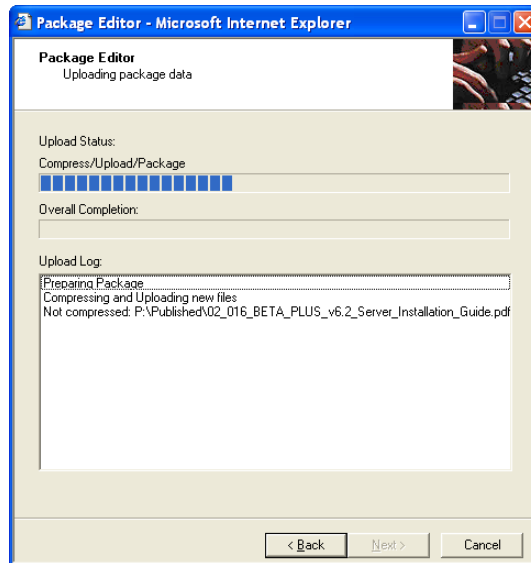


Figure 6.9 Package Editor - Upload Status

Once the Upload is complete, the Next button will initialize. Click the Next button to initialize the Updated Summary screen.

Upload Summary Page

The final screen displays a simple summary on the saving of the package, and whether it was successful or failed. If a failure occurred, the error code and description will be displayed.

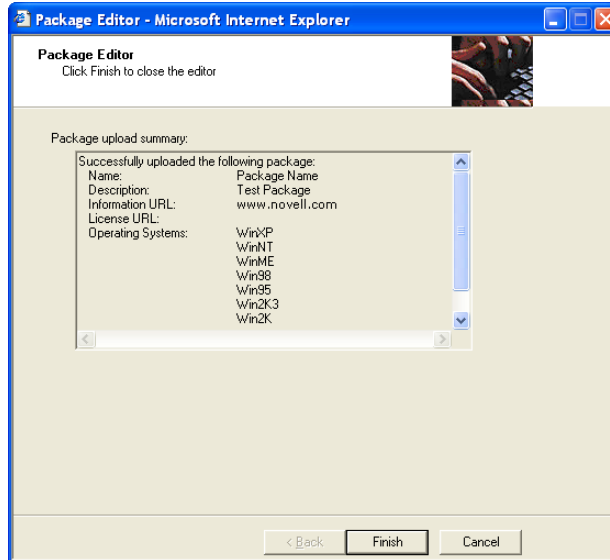


Figure 6.10 Package Editor - Upload Summary

Click the Finish button to close the wizard and complete the operation.

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.

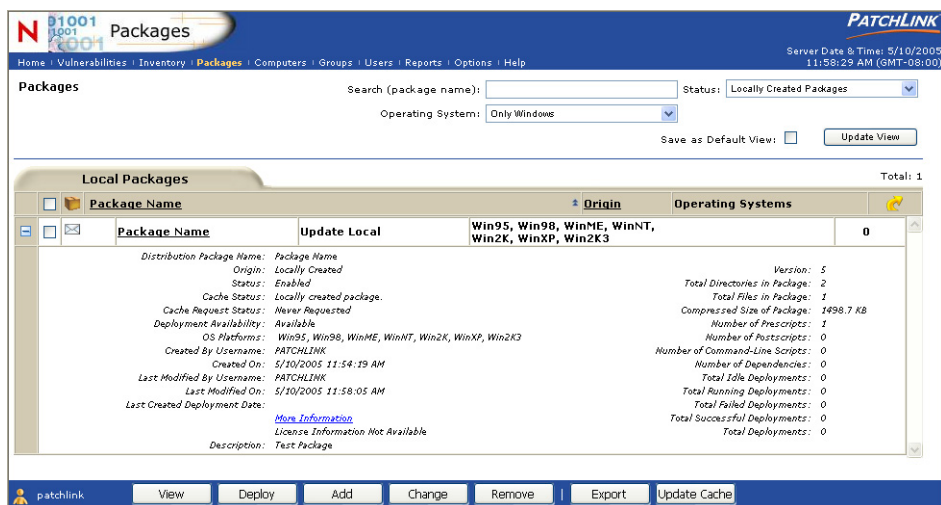


Figure 6.11 Packages Page - Custom Package

7 Deployments

A Deployment, in its simplest form, allows a Patch to be downloaded by a Deployment Agent, so it can install it. In more generic terms, a Deployment is the encompassing instructions around a Distribution Package that describes to the Deployment Agent how to deploy the package. The contents of the Distribution Package contain all the other necessary information (info, files and scripts) required to actually perform whatever needs to be done: install this patch executable, stop this service, validate a system condition, change a database entry, etc.

Overview

Deployments can be created throughout the product, but basically encompass three main areas: Vulnerability-based Deployments, Package-based Deployments and a Group's Mandatory Baseline.

- **Vulnerability-based Deployments** - A Vulnerability contains multiple associated distribution packages and the target package to be deployed depends on the assigned computers. As a computer goes through the Discover Applicable Updates process, it is assigned Vulnerabilities to scan as ZENworks Patch Management Server determines they are applicable to the computer. Based on these results, a Novell User has the ability to determine which computers to deploy the “Patch” (Vulnerability Fix) to. Behind the scenes, ZENworks Patch Management Server goes through and makes sure that the computers get assigned the correct Distribution Package.
- **Package-based Deployments** - A Distribution Package is assigned a single operating system, thus only those computers whose operating system matches 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 Novell User which computers really apply to this patch (or package) or not.
- **Group Mandatory Baseline** - A group contains a feature called its Mandatory Baseline, or the ability to define a baseline of Vulnerabilities or Locally-created Distribution Packages as being the base set of patches and other packages that must be installed for the group's computer members. In terms of Vulnerabilities, a Mandatory Baseline will continually check to verify and validate that the patch is actually installed; if it is not, it will deploy the necessary distribution package to get it to be installed.

Package Deployments Page

Select a specific Package Name link from the Package Name column to view information and deployment details. The package deployments section displays all of the deployments that have been created for the distribution package. The Distribution

Packages section displays all of the packages that the ZENworks Patch Management Server has available to it, various functions to manage them, and the number of Deployments created to deploy a package.

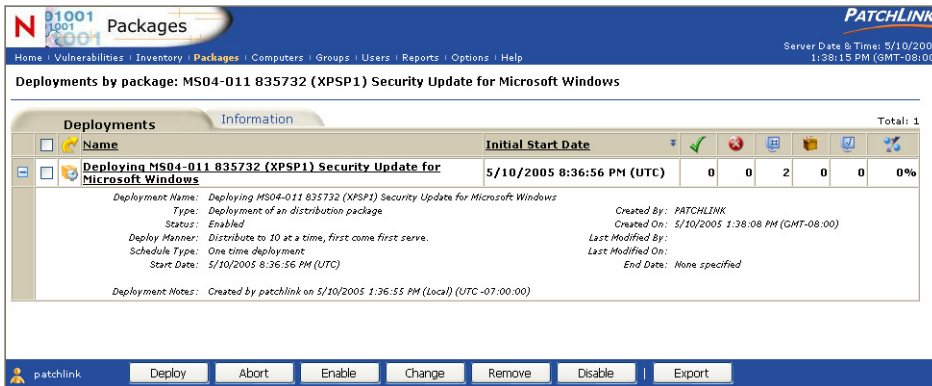


Figure 7.1 Package Deployments page

Clicking the plus icon will display additional information about the deployment. Clicking the minus icon will hide this information from view. The information is refreshed each time it is displayed.































The deployment information contains:

Table 7.1 Deployment Details

Deployment name	The name of the deployment
Type	Deployment for which type of a package
Status	This can be: <ul style="list-style-type: none">• Enabled• Disabled• Paused
Deploy manner	The manner in which this deployment occurred. It can be: <ul style="list-style-type: none">• Sequential• Parallel• First come first serve• Distribute to # of computers at a time
Schedule type	This can be: <ul style="list-style-type: none">• Recurring• 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 modified this deployment last
Last modified on	The date and time this deployment was last modified
End date	The date and time the deployment was completed

Deployment Types and Status

Table 7.2 Package Deployment Icons and Descriptions

New	Current	Local	System Task	Mandatory Group	Description
					Deployment currently has no assigned computers
					Currently deploying (animated)
					Deployment waiting to start
					Deployment which all of the assigned computers and groups have finished successfully
					Deployment in which at least one computer finished unsuccessfully
					Deployment that is disabled

- **New:** A new deployment is a deployment that has been created since you logged on to your current session.
- **Current:** A deployment that was created before you logged on to your current session.
- **Local:** A deployment is of a locally created distribution package.
- **System Task:** A system task deployment contains a system task distribution package to perform required or Novell provided tasks. These deployments may include automated schedules in which the membership of the deployment may not be modified, though the schedule may.
- **Mandatory Group:** A deployment is created through the mandatory baseline for a group. This deployment is automatically created and managed through the mandatory baseline process.

Name

The name assigned to the deployment.

Initial Start Date

The schedule date the deployment is to begin. For recurring deployments this is the first scheduled date of the deployment.







Statistics



Figure 7.2 Statistics

The right-hand side of the vulnerability entry contains columns which illustrates the current result statistics for deployments by package.






Table 7.3 Column Icon Definitions

Icon	Definition
	Total number of computers or groups that finished the deployment successfully
	Total number of computers or groups that finished the deployment unsuccessfully
	Total number of computers or groups that are assigned the deployment
	Total number of computers or groups that are in the process of executing the deployment
	Total number of computers or groups that finished the deployment
	Percentage of the computers or groups that finished the deployment

Deployment Summary































This view illustrates the overall information about this particular distribution package including its content, deployment status, etc. Deployments of a package are designated by the following types:

Table 7.4 Deployment Types

Icon	Definition
	Deployment of a mandatory baseline item for a group
	Deployment of a distribution package (provided by Novell)
	Deployment of a new distribution package (provided by Novell)
	Deployment of a system task
	Deployment of a locally created distribution package

Each deployment has the following states, depending upon the status results of the deployment (using a distribution package deployment for the deployment type).

Table 7.5 Package Deployment Icons and Descriptions

New	Current	Local	System Task	Mandatory Group	Description
					Deployment currently has no assigned computers
					Currently deploying (animated)
					Deployment waiting to start
					Deployment which all of the assigned computers and groups have finished successfully
					Deployment in which at least one computer finished unsuccessfully
					Deployment that is disabled

Page Functions

Action Menu

Deploy

Deploys the current (selected) package. This will launch the Deployment Wizard. You can quickly schedule a package for deployment or distribution to computers with Client Agents from this wizard.



Note: You will not be allowed to create new deployments of System Task Packages from Novell (only modify their schedule).

Abort

To abort one or more deployments:

1. Select one or more deployments.
2. Click the **Abort** button at the bottom of the page.

This will cancel one or more deployments. The computers that have already received the package will not be affected and any other computers will show that the package deployment was aborted before the deployment could occur.



Note: You will not be allowed to abort deployments of System Task Packages from Novell.

Enable

Click on the Enable button to enable a paused or a disabled deployment. The deployment will then be scheduled to occur according to its schedule type and manner.

Change

This will launch the Deployment Wizard, allowing you to make modifications to any deployment. All deployments can be changed, including deployments of System Task Packages from Novell. Note that 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).

Remove

Removes the selected disabled deployments. To remove one or more deployment entries:

1. Select one or more deployments
2. Click the Remove button.

This will delete the selected package deployments from your ZENworks Patch Management Server. Removing a deployment will have no affect on computers that have already received the deployment.



Note: You will not be allowed to remove deployments of System Task Packages from Novell.

Disable

Disables the deployment. The deployment will be paused and no longer deployed to the assigned computers.

Export

Export the deployment data to a comma-separated value (CSV) file.

Deployment Details Section

The deployment details section displays the assigned computers and groups and the status of the deployment for each. To view the group membership results for the deployment, click on the name of the group, then select that specific deployment package's Name link.

Computers and Groups Scheduled for 5/10/2005 9:46:44 PM (Agent UTC)							Total: 3
<input type="checkbox"/>	 Name	Status	Last Run Status	Last Run Start Date	Last Run Completed Date	Next Run Date	
<input type="checkbox"/>	 \\TECHPUBS-PLUS	Not Started				5/10/2005 9:46:44 PM (UTC)	
<input type="checkbox"/>	 \\TECHPUBS-XP02	Not Started				5/10/2005 9:46:44 PM (UTC)	
<input type="checkbox"/>	 \\TECHPUBSXP03	Not Started				5/10/2005 9:46:44 PM (UTC)	

Figure 7.3 Deployment Details

Computer Status



Figure 7.4 Computer Status



Note: Refer to [Appendix B, “ZENworks Patch Management Server Reference”](#) for a complete definition of all available computer status icons.

Name

This displays the name of the computer or group. The name of the group is also a hyperlink. Clicking the link will display the members of the group and the status of the deployment for each.

Status

This displays the status of the deployment for the computer or group.

Table 7.6

Status	Description
Not Started	<ul style="list-style-type: none"> The computer or group has not started the deployment. The deployment start time has not been reached. The computer has not contacted ZENworks Patch Management Server since the start of the deployment. The deployment or global ZENworks Patch Management Server deployment limit was full the last time the computer contacted ZENworks Patch Management Server. It will try again on its next interval
.In Progress	The computer or the group has started the deployment.
Not Running	The computer or group has finished at least the first occurrence of this recurring deployment, but the next instance of this deployment has not started.
Not Scheduled	Computer members of a group are not assigned the deployment for a group deployment until the computer has contacted ZENworks Patch Management Server once the deployment start time has been reached.

Table 7.6

Status	Description
Obtaining Package	ZENworks Patch Management Server is currently downloading the necessary distribution packages for the deployment. Once they have been cached (and the deployment start time has been reached), the computers will be able to download perform the deployment.
Completed	All computers and groups have finished the deployment.
Disabled	The specific computer or group assignment for this deployment has been disabled.

Last Run Status (link)

This displays the status message from the last time this computer or group performed the deployment. Once the deployment has been performed, the specific results of the deployment for that computer can be displayed by clicking on the status text.

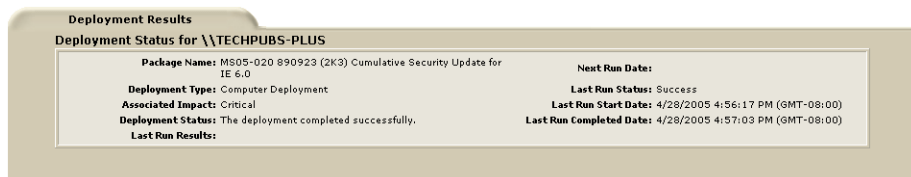


Figure 7.5 Last Run Status

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

Last Run Start Date

This displays the date when the computer or group last started the deployment.

Last Run Completed Date

This displays the date when the computer or group finished the last deployment.

Next Run Date

This displays the date when the computer is to perform the next deployment.

Page Functions

Action Menu

- **Enable** - This enables the selected disabled deployment assignments.
- **Disable** - This disables the selected enabled deployment assignments. Disabled deployment assignments cause the individual deployment for the agent or group to not be performed while not affecting the overall deployment. Recurring mandatory baseline-based deployment assignments will automatically be disabled after the deployment has failed three times.
- **Export** - Exports the deployment status and details to a comma-separated value (CSV) file. The order of the data is based what the view is sorted on.

Package Information Page

Click on the Information tab to display the information about the distribution package. The Information section is broken down into two sections: Package Information and Package Content.

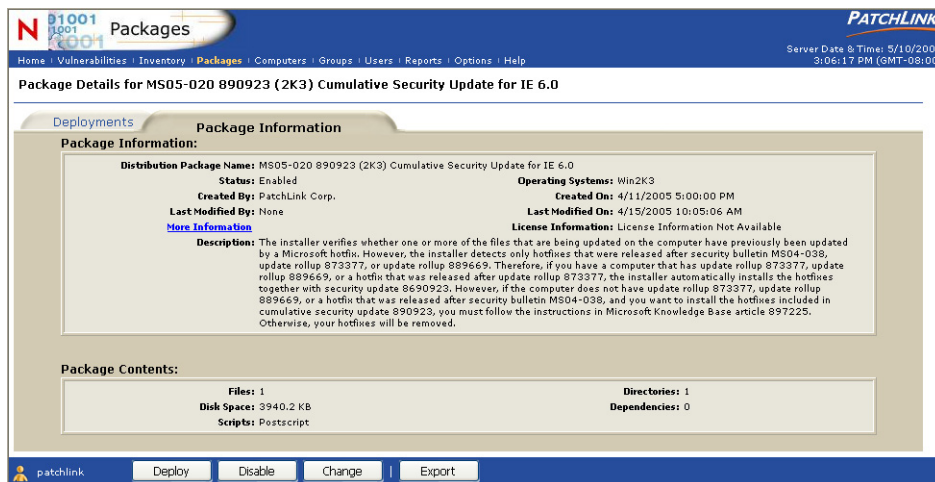


Figure 7.6 Package Information

Package Information

- **Name:** This displays the name of the distribution package.
- **Status:** This displays the status of the distribution package.
- **Operating Systems:** This displays the operating system platforms that this distribution package can deploy to.
- **Created By:** This displays the user who created the distribution package.
- **Created On:** This displays when the distribution package was created.
- **Last Modified By:** This displays the user who last modified the distribution package.
- **Last Modified On:** This displays when the distribution package was last modified on.
- **More Information:** This hyperlink will bring up a browser window with a page that displays more information about the distribution package or the vulnerability.
- **License Information:** If the distribution package requires a license to be agreed to, then this hyperlink will bring up that license page in a browser window. The license will have to be agreed to before (done when creating a deployment for it) a deployment can be created for the package.
- **Description:** This contains additional information about the distribution package or the patch contained inside.

Package Contents

- **Files:** This displays the number of files that are downloaded when the distribution package is deployed.
- **Directories:** This displays the number of directories that are created if they do not exist when the distribution package is deployed.
- **Disk Space:** This displays the compressed size of the distribution package.
- **Dependencies:** This displays the number of other distribution packages, which must be installed prior to this distribution in order to be deployed.
- **Scripts:** This displays the scripts that the distribution package contains.

Page Functions

Action Menu

- **Deploy** - This creates a new deployment of the distribution package.
- **Change** - This allows a Novell User to change the local deployment package.
- **Wait / Disable / Enable** - Wait re-enables the package. Disable the distribution package from being able to be deployed. If the distribution package is already disabled, this button will not be displayed. Enable a distribution package so it can be deployed. If the distribution package is already enabled, this button will not be displayed. This enables the selected disabled deployments so they are now available for computer deployment agents to obtain.
- **Export** - Exports the deployment data to a comma-separated value (CSV) file.

8 Patch Deployments

After successfully installing the ZENworks Patch Management Server, and agents you now need to analyze the agents, identifying vulnerabilities and creating patch deployments.

When initially installing patches, it is suggested that you begin with the service packs and other cumulative patches. This will significantly decrease the number of individual patches that need deployment.

Once the computers are fully brought up-to-date, it will only be necessary to deploy the new patches as they become available.

Understanding Deployments

A *standard deployment* is simply 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.

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.

Understanding the ‘Dirty State’

Dirty state is the term given a ZENworks Patch Management Agent, that has received a deployment which required a reboot, but the computer did not perform the reboot following that deployment. There are two different dirty state types.

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. Either one of the reboot deployments 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 one of the reboot deployments. Either one of the reboot deployments or a manual reboot will clear the dirty state.

Rebooting Agents

There are two deployments which will perform a reboot:

- **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, or the reboot flag was sent to the agent. In the case of the reboot flag being 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.

Understanding the ZENworks Patch Management Deployment Logic

When deploying more than one package to an individual agent or to a group of agents, the deployments can be ordered by scheduling each deployment separately at different times or through the use of **X-Deploy**.

In addition to the scheduled time, deployment order is also influenced by the deployment type and the state of the agent. As long as the agent is not in (and does not enter) a dirty state, deployments will proceed in the following order:

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

Within each deployment type, deployments are ordered by their scheduled time. Although no deployment will occur 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.

Chaining Deployments

On a windows machine deployments are chained through the use of `qchain.exe`, a windows application which will place the newly installed files in the correct order so that when the computer is restarted, only the most recent version of each file is applied. To properly sort the files, `qchain.exe` is run by the client agent after the installation of each package.

Using 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 easy to use, wizard interface to create or edit deployment schedules for multiple recipients and multiple packages. The wizard assists in; the selection of computers to receive the deployments, scheduling a date and time for the deployment, and setting a recurrence (if appropriate). 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 computers and packages required.

Introduction Page

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



Note: Using the Deployment wizard, you can select multiple vulnerabilities, and the wizard will automatically select all of the computers and packages required.

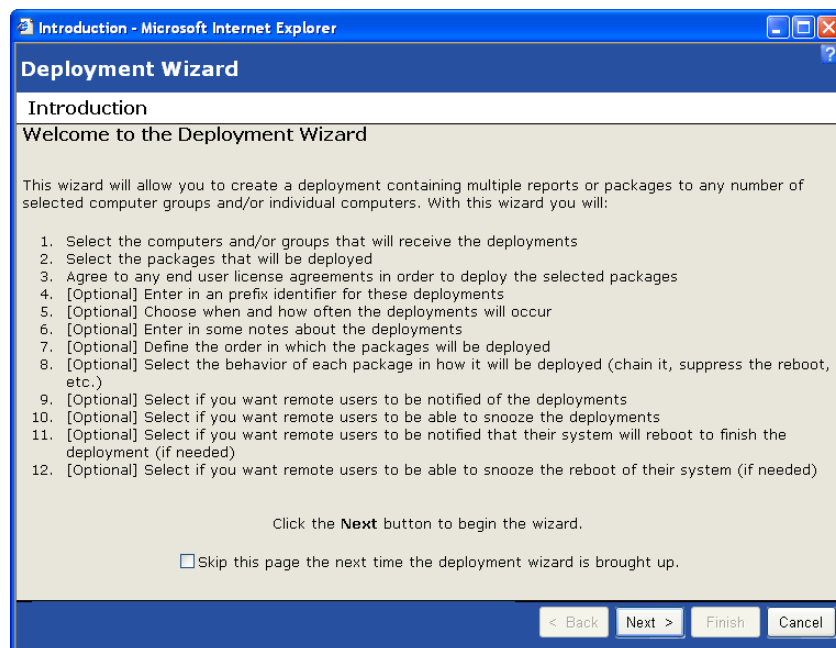


Figure 8.1 Deployment Wizard - Introduction Page

This page can be hidden during future deployments by selecting the **Skip this page the next time the deployment wizard is brought up** checkbox.

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

Click **Cancel** to abort the wizard.

Computer/Groups Selection Page

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

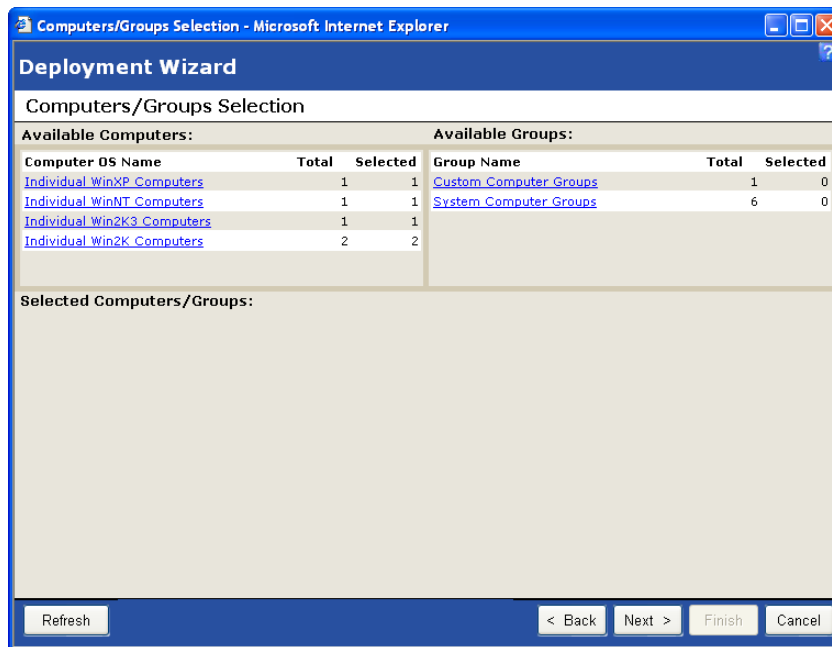


Figure 8.2 Deployment Wizard - Computers/Groups Selection Page

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

- **To select individual computers**
 1. Click the appropriate operating system link
 2. For each computer to be included in the deployment, click its associated checkbox.
- **To select a group of computers**
 1. Click the appropriate group link

- For each group to be included in the deployment, click its associated checkbox.



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

Deployment Wizard

Computers/Groups Selection

Available Computers:			Available Groups:		
Computer OS Name	Total	Selected	Group Name	Total	Selected
Individual WinXP Computers	1	1	Custom Computer Groups	1	0
Individual WinNT Computers	1	1	System Computer Groups	6	0
Individual Win2K3 Computers	1	1			
Individual Win2K Computers	2	2			

Selected Computers/Groups:

<input checked="" type="checkbox"/>	Computer Name	Status	Platform Info	DNS Name	
<input checked="" type="checkbox"/>	\\1550VM05-2KS-01	Idle	Microsoft Windows 2000 Server-Service Pack 4	1550vm05-2ks-01.engineering.patchlink.com	1
<input checked="" type="checkbox"/>	\\DELL1550VM03	Idle	Microsoft Windows 2000 Server-Service Pack 4	dell1550vm03.engineering.patchlink.com	1

1

Display Computers per page

Refresh < Back Next > Finish Cancel

Figure 8.3 Deployment Wizard - Computer/Groups Selection Page

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

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.

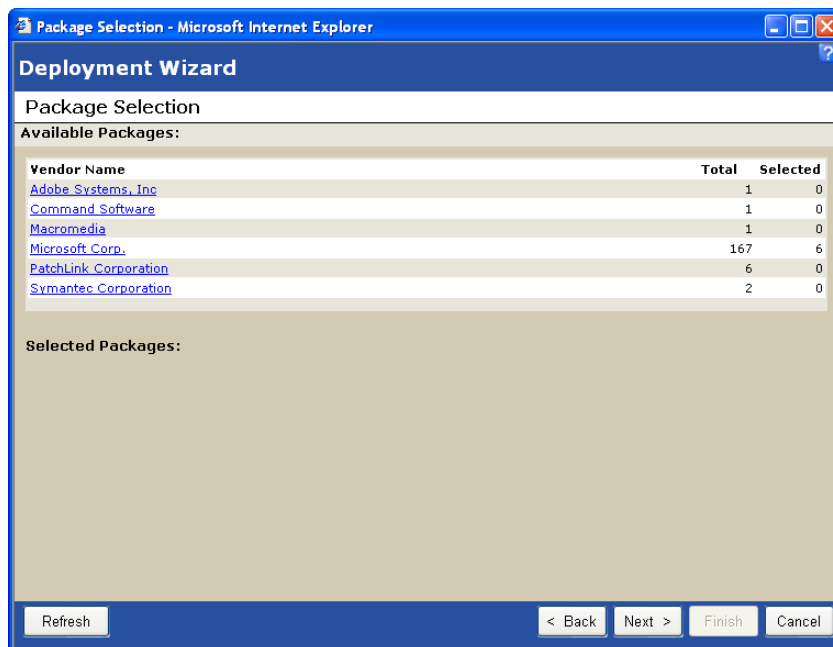


Figure 8.4 Deployment Wizard - Packages Selection Page

When opened this page displays the packages, grouped by manufacturer, that apply to the computers selected on the *Computers/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.

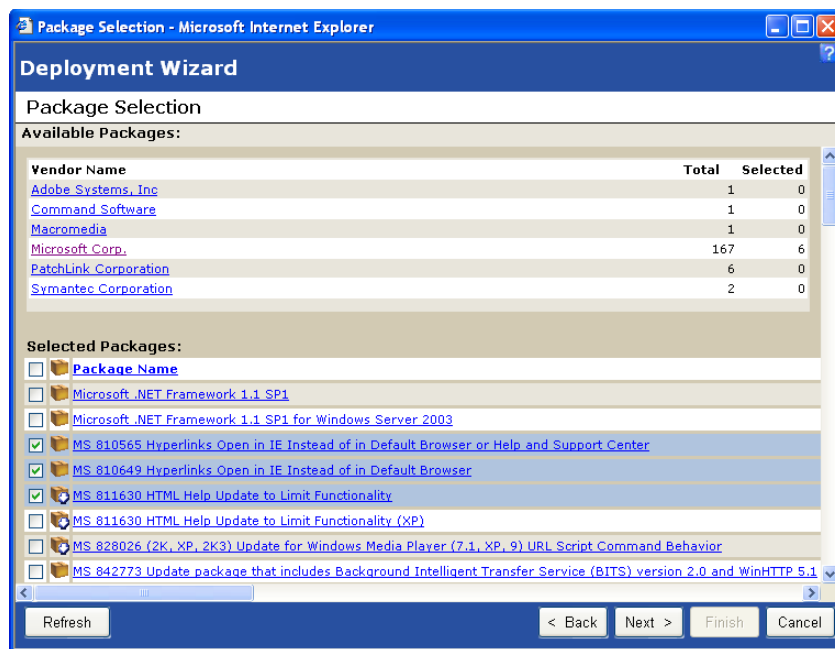


Figure 8.5 Deployment Wizard - Packages Selection Page

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 they are Patched, Not-Patched or Not-Applicable to the selected package.

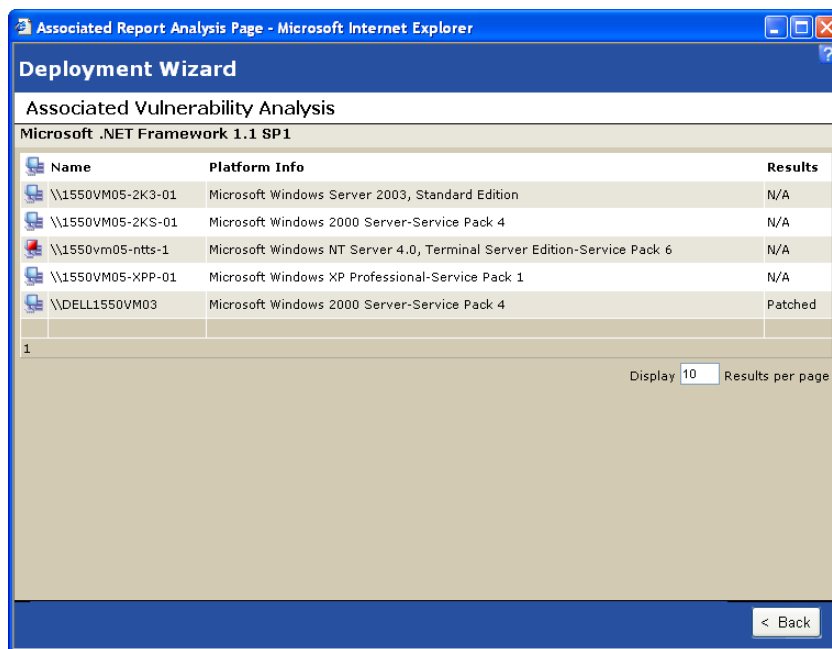


Figure 8.6 Deployment Wizard - Associated Vulnerability Analysis Page

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.

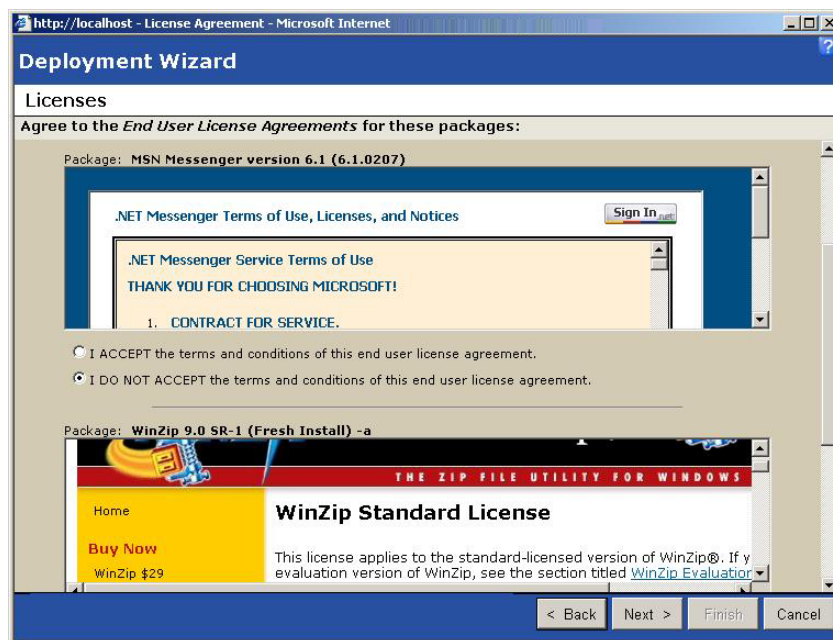


Figure 8.7 Deployment Wizard - Licenses Page

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 this deployment.

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**.

The screenshot shows a web browser window titled "http://localhost - Deployment Options - Microsoft Internet Explorer". The page has a blue header bar with the text "Deployment Wizard" and a question mark icon. Below the header, the page title is "Deployment Options". The main content area is titled "Select the options for this deployment:". It contains several sections: "Deployment Name Prefix:" with a text input field containing "Deploying {Package Name}"; "Start Time:" with "Local Time: 4/13/2005 3:08:51 PM" and "UTC Time: 4/13/2005 10:08:51 PM", and a "Change" button; "One time deployment starting at:" with two radio buttons: "Agent Local Time (Deploy at local time for each individual node)" and "Agent UTC Time (Deploy at UTC time for each individual node)"; "Manner:" with two radio buttons: "Sequential" (selected) and "Parallel", each with a description; "Suspend the deployment of this package, if it fails to deploy to one or more computers." (unchecked); and "Deploy package even if computer has been previously patched." (unchecked); and "Notes:" with a text area containing "Created by patchlink on 4/13/2005 3:08:51 PM (Local) (UTC - 07:00:00)". At the bottom, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Figure 8.8 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.



Note: By removing the {Package Name} variable, you can leave the package name out of the notification.

- **Start Time**

- **Change button** - 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.
- **Local Time** - Local time will vary depending on the time zone of your location (daylight savings time may apply). When the agent communicates with the ZENworks Patch Management Server, the local time of the agent is used when checking to see if there are any deployments available.



Note: Although the agent's local time is selected, a group deployment will never occur prior to the ZENworks Patch Management Server reaching the scheduled time. Therefore, in the case where an agent's time zone is prior to the ZENworks Patch Management Server's time zone, the local time of the ZENworks Patch Management Server not the agents will be used. This is due to the fact that the ZENworks 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.

- **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 dependant upon the local time zone. When UTC is used, the deployment will be scheduled for all agents at the same time.



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 ZENworks Patch Management Server) time and time zone settings are correct.

- **Sequential**
 - **Sequential** - Sequential distribution limits the simultaneous distribution of the deployment to only the specified number of computers at one time. By limiting the number of simultaneous distributions, sequential deployment is an effective way of limiting the bandwidth required for large distributions. 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.



Note: If a computer takes longer than four hours to complete the deployment, it is no longer counted against the limit.

- **Parallel** - Parallel distribution will create and distribute all deployments simultaneously.



Note: The global deployment limit (the **Concurrent Deployment Limit** setting on the *Options* page of the ZENworks Patch Management Server) 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.

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.

Schedule Configuration - Microsoft Internet Explorer

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 8.9 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: < November 2004 >
 End Date: < 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

Save Cancel

Figure 8.10 Deployment Wizard - Schedule Configuration Page

- **Daily Deployment Options**

Occurs:
☒ Daily
☐ Weekly
☐ Monthly

Daily:
 Every 1 day(s)

Figure 8.11

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

The screenshot shows a configuration window for weekly deployments. On the left, under 'Occurs:', there are three radio buttons: 'Daily' (unselected), 'Weekly' (selected), and 'Monthly' (unselected). On the right, under 'Weekly:', there is a section 'Every 1 week(s) on:' with a dropdown menu showing '1'. Below this, there are checkboxes for each day of the week: Mon, Tue, Wed, Thur, Fri, Sat, and Sun. The 'Sun' checkbox is checked, while the others are unchecked.

Figure 8.12

- **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**

The screenshot shows a configuration window for monthly deployments. On the left, under 'Occurs:', there are three radio buttons: 'Daily' (unselected), 'Weekly' (unselected), and 'Monthly' (selected). On the right, under 'Monthly:', there are two options. The first option is 'Day 1 of every 1 month(s)', where 'Day 1' is selected from a dropdown, '1' is in a text field, and '1' is in a dropdown for 'month(s)'. The second option is 'The 1st Sunday of every 1 month(s)', where 'The 1st' is selected from a dropdown, 'Sunday' is in a text field, and '1' is in a dropdown for 'month(s)'.

Figure 8.13 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:

☒ 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: < 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

End 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

☒ No End Date

Figure 8.14 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.

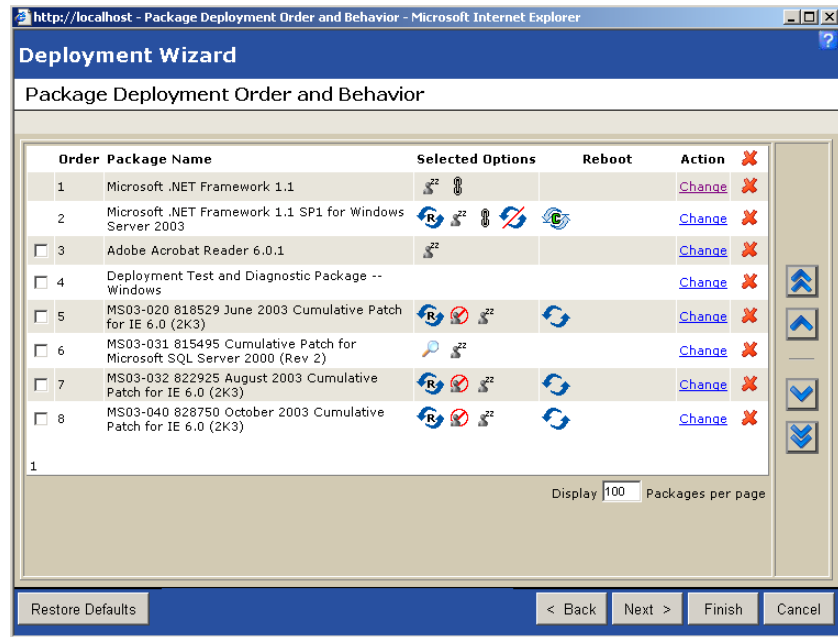


Figure 8.15 Deployment Wizard - Package Deployment Order and Behavior Page

- Selected Options Column** - The **Selected Options** column graphically displays the behavior of each package, (as defined on the *Package Deployment Behavior Options* page) using the behavior icons.



Note: When deploying chained deployments, whenever possible, reboots are suppressed, including the final (chained) deployment. That final deployment will be represented as *May Reboot* because the ZENworks 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.

Table 8.1 Behavior Icon Definitions























	Uninstall - instead of an installation, this option will uninstall the packages.
	Suppress Reboot - prevents the computer from rebooting after installation of the package. This option is not available when the Force Reboot option has been selected.
	List Hot Fixes - returns a listing of the hot fixes installed on the target computers.
	Chainable - sets the package as chainable (package must support chaining).
	Deploy Only - distributes the package without running the package installation script.
	Suppress Repair - suppresses the repair of file name permissions after the reboot.
	Force Shutdown - forces all applications to close during the computer shutdown.
	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.
	Force Reboot - forces the computer to reboot regardless of package requirements. This option is not available when the Suppress Reboot option has been selected.
	Suppress Chain Reboot - suppress the reboot, allowing other chained packages to be sent following this package. It is recommended that you suppress the final reboot for all chained packages, then send a reboot deployment when all packages are finished.
	No Pop-Up - suppresses any pop-up messages during installation.
	Reboot May Occur - sets the package to allow a reboot if the package requires it.
	No Back Up - will not backup files for un-installation purposes.

Table 8.1 Behavior Icon Definitions

	Unattended Setup - uses the packages unattended setup mode.
	Reboot is Required - indicates that this package requires a reboot prior to completing the installation.
	Repair Permissions - following the package installation, file permissions will be repaired.
	Debug - runs the package installation in debug mode (reserved for troubleshooting installations).

- **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 8.2 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
	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

- **Action Column**
 - **Change Link** - Click the **Change** link, to open the *Package Deployment Behavior Options* page and change the behavior options for that package.
- **Delete Column** - Click the *Delete* icon to remove the package from the deployment.

- **Up/Down buttons** - To move a package first select its corresponding checkbox then select a move button as defined below.

Table 8.3 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.

- **Display __ packages per page** - Changing the value in the **Display __ packages per page** field, will modify the maximum number of packages displayed at once on this page.
- **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.



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.

Package Deployment Behavior Options - Microsoft Internet Explorer

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 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.**

☐ Description

Save Cancel

Figure 8.16

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

Table 8.4 Behavior Icon Definitions


















	Uninstall - instead of an installation, this option will uninstall the packages.
	Suppress Reboot - prevents the computer from rebooting after installation of the package. This option is not available when the Force Reboot option has been selected.
	List Hot Fixes - returns a listing of the hot fixes installed on the target computers.
	Chainable - sets the package as chainable (package must support chaining).
	Deploy Only - distributes the package without running the package installation script.
	Suppress Repair - suppresses the repair of file name permissions after the reboot.
	Force Shutdown - forces all applications to close during the computer shutdown.
	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.
	Force Reboot - forces the computer to reboot regardless of package requirements. This option is not available when the Suppress Reboot option has been selected.
	Suppress Chain Reboot - suppress the reboot, allowing other chained packages to be sent following this package. It is recommended that you suppress the final reboot for all chained packages, then send a reboot deployment when all packages are finished.
	No Pop-Up - suppresses any pop-up messages during installation.
	Reboot May Occur - sets the package to allow a reboot if the package requires it.

Table 8.4 Behavior Icon Definitions

	No Back Up - will not backup files for un-installation purposes.
	Unattended Setup - uses the packages unattended setup mode.
	Reboot is Required - indicates that this package requires a reboot prior to completing the installation.
	Repair Permissions - following the package installation, file permissions will be repaired.
	Debug - runs the package installation in debug mode (reserved for troubleshooting installations).

- **Optional Flags** - The **Optional Flags** field 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:

Table 8.5 Package Flag Descriptions and Behavior

Description (flag behavior)	Flag to Display the option	Flag to Select the option
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
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

Table 8.5 Package Flag Descriptions and Behavior

Description (flag behavior)	Flag to Display the option	Flag to Select the option
No Pop-up	-PLN1	-PLNP
Debug	-PLDG	-PLDEBUG
Suppress Repair	-dsr	-sr
Force the script to reboot when the installation is done	-1d	-1
The installer may reboot	Not Applicable	-2
Reboot may occur	Not Applicable	-3
Reboot is required, and MAY occur	Not Applicable	-4

- **Notes** - The **Notes** field displays the expected deployment behavior.
- **Description** - The **Description** field displays the package description

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

Click **Cancel** to abort the changes and return to the *Package Deployment Order and Behavior* page.

Notification Options Page

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

http://localhost - Deployment Notification Options - Microsoft Internet Explorer

Deployment Wizard

Notification Options

Define the Deployment Notification Options

☐ Use Policies
☐ Do not notify users of this deployment
☒ Notify users of this deployment

Message:

The download and installation of the patch: (%Package_Name%) is ready to begin. If you require any additional information, please contact your PatchLink Update administrator.

Deployment Options	Use Agent Policy	Setting
Agent Time		UTC
Allow User to Cancel	<input type="checkbox"/>	No
Allow User to Snooze	<input checked="" type="checkbox"/>	Yes
Notification On Top	<input type="checkbox"/>	No
Deadline Offset	<input type="checkbox"/>	
<input checked="" type="radio"/> From Deployment Start: 5 Mins <input type="radio"/> Specific Date: 4/13/2005 3:13:51 PM		

Define the Reboot Notification Options

☐ Use Policies
☐ Do not notify users of the reboot
☒ Notify users of the reboot

Message:

To complete the installation of the patch: (%Package_Name%), it is now necessary to reboot your computer. If you require any additional information, please contact your PatchLink Update administrator.

Reboot Options	Use Agent Policy	Setting
Allow User to Cancel	<input type="checkbox"/>	Yes
Allow User to Snooze	<input checked="" type="checkbox"/>	Yes
Reboot Delay Offset:	<input type="checkbox"/>	5 Mins

< Back Next > Finish Cancel

Figure 8.17 Deployment Wizard - Notification Options Page

Deployment Notification Options

- **Use Policies** - When selected the defined *Agent Policies* for each agent will be used. Selection of this option disables all other deployment notification options.
- **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

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
 - **Deadline 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.

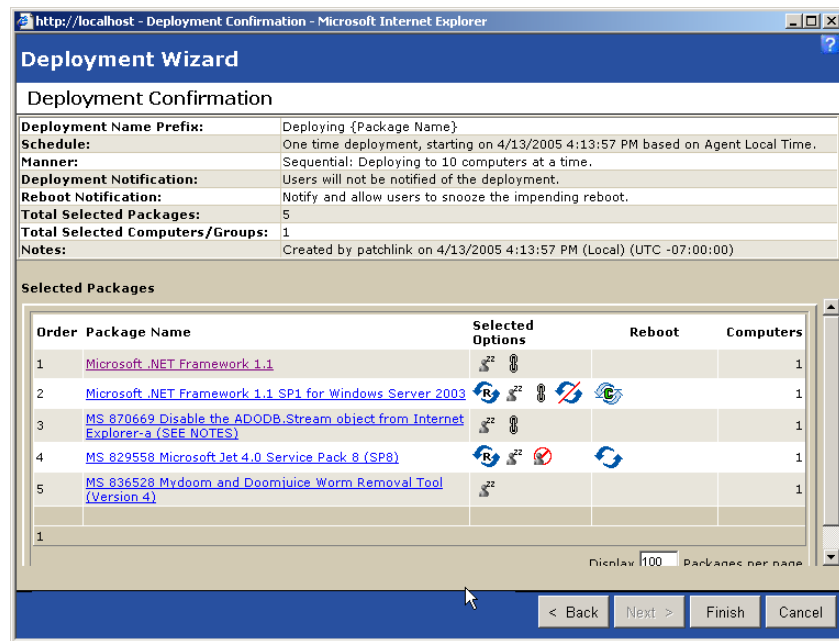


Figure 8.18 Deployment Confirmation Page

- **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** - The **Order** column, displays the order in which the packages will be deployed.
 - **Package Name Column** - The **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** - The **Selected Options** column graphically displays the behavior of each package, (as defined on the *Package Deployment Behavior Options* page) using the behavior icons.

Table 8.6 Behavior Icon Definitions























	Uninstall - instead of an installation, this option will uninstall the packages.
	Suppress Reboot - prevents the computer from rebooting after installation of the package. This option is not available when the Force Reboot option has been selected.
	List Hot Fixes - returns a listing of the hot fixes installed on the target computers.
	Chainable - sets the package as chainable (package must support chaining).

Table 8.6 Behavior Icon Definitions

	Deploy Only - distributes the package without running the package installation script.
	Suppress Repair - suppresses the repair of file name permissions after the reboot.
	Force Shutdown - forces all applications to close during the computer shutdown.
	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.
	Force Reboot - forces the computer to reboot regardless of package requirements. This option is not available when the Suppress Reboot option has been selected.
	Suppress Chain Reboot - suppress the reboot, allowing other chained packages to be sent following this package. It is recommended that you suppress the final reboot for all chained packages, then send a reboot deployment when all packages are finished.
	No Pop-Up - suppresses any pop-up messages during installation.
	Reboot May Occur - sets the package to allow a reboot if the package requires it.
	No Back Up - will not backup files for un-installation purposes.
	Unattended Setup - uses the packages unattended setup mode.
	Reboot is Required - indicates that this package requires a reboot prior to completing the installation.
	Repair Permissions - following the package installation, file permissions will be repaired.
	Debug - runs the package installation in debug mode (reserved for troubleshooting installations).

- **Reboot Column** -The **Reboot** column graphically displays the reboot settings of each package, (as defined on the *Package Deployment Behavior Options* page) using the reboot icons.

Table 8.7 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
	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

- **Computers Column** - The **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.

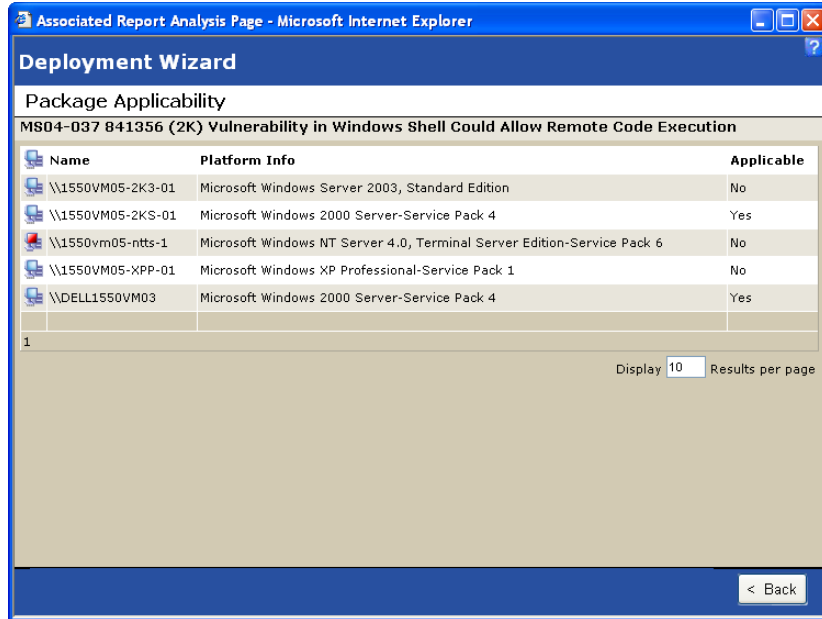


Figure 8.19 Deployment Wizard - Package Applicability Page

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.

http://localhost - Deployment Summary - Microsoft Internet Explorer

Deployment Wizard

Deployment Summary

Deployment Name:	Deploying Adobe Acrobat Reader 6.0.1
Schedule:	One time deployment, starting on 4/13/2005 4:19:57 PM based on Agent UTC Time.
Manner:	Sequential: Deploying to 10 computers at a time.
Deployment Notification:	Users will not be notified of the deployment.
Reboot Notification:	The deployment does not require a reboot.
Total Selected Packages:	1
Total Selected Computers/Groups:	1
Notes:	Created by patchlink on 4/13/2005 4:19:57 PM (Local) (UTC -07:00:00)

Selected Packages (0 of 1 packages have been cached) Auto-Refresh: ☒

Package Name	Status
Adobe Acrobat Reader 6.0.1	Requesting

1

Display 100 Packages per page

Your packages have been requested; once all requested packages have been cached, the deployment will begin as scheduled.

Figure 8.20 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.

Change

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.

Page Security

Package Deployments Security

The package deployments section of ZENworks Patch Management Server requires the View Deployment Status access right. If a user does not have the correct access, the access denied error message is displayed.

To be able to view the information about a distribution package requires the View Packages access right. If a user does not have the correct access, the hyperlink on the Information tab is not enabled.

To be create a deployment for the distribution package requires the Deploy Packages access right. If a user does not have the correct access, the Deploy button is disabled.

To be able to change, disable, enable, abort or remove a deployment(s) requires the Manage Deployments access right. If a user does not have the correct access, the Change, Disable, Enable, Abort and Remove buttons are disabled.

To be able to change the deployment of the Discover Applicable Updates System Task requires the Manage System Tasks access right. If a user does not have the correct access, they will receive a message indicating they do not have access.

To be able to export the distribution package's information to a comma-separated value (CSV) file requires the Export Deployment Data access right. If a user does not have the correct access, the Export button is disabled.

Contact your Novell Administrator for more information on ZENworks Patch Management Security.

Distribution Packages Security

The Distribution Packages section of ZENworks Patch Management Server requires the View Packages access right. If a user does not have the correct access the access denied error message is displayed.

To be able to view the deployments for a distribution package requires the View Deployments access right. If a user does not have the correct access the hyperlink on the Package Name will not be displayed.

To be able to create a deployment for a selected distribution package requires the Deploy packages access right. If a user does not have the correct access the Deploy button is disabled.

To be able to create, change or remove distribution packages requires the Manage Packages access right. If a user does not have the correct access the Add, Change and Remove buttons are disabled.

To export all of the distribution packages and their information to a comma-separated values (CSV) file requires the Export Package Data access right. If a user does not have the correct access the Export button is disabled.

To cache the selected (or re-cache all of the previously cached) distribution packages requires the Cache Packages access right. If a user does not have the correct access, the Update Cache button is disabled.

Package Information Security

The distribution package information section of ZENworks Patch Management Server requires the View Packages access right. If a user does not have the correct access, the access denied error message is displayed.

To be able to view the deployments of the distribution package requires the View Deployments access right. If a user does not have the correct access, the hyperlink on the Deployments tab is not enabled.

To be create a deployment for the distribution package requires the Deploy Packages access right. If a user does not have the correct access, the Deploy button is disabled.

To be able to change a local distribution package requires the Manage Packages access right. If a user does not have the correct access, the Change button is disabled.

To be able to disable or enable a distribution package requires the Manage Packages access right. If a user does not have the correct access, the Enable and Disable buttons are disabled.

To be able to export the distribution package's information to a comma-separated value (CSV) file requires the Export Package Data access right. If a user does not have the correct access, the Export button is disabled.

Contact your Novell Administrator for more information on ZENworks Patch Management Security.

Deployments Details Security

The Deployment Details section of ZENworks Patch Management Server requires the View Deployment Statuses access right. If a user does not have the correct access, the access denied error message is displayed.

To enable and disable a deployment assignment requires the Manage Deployments access right. If a user does not have the correct access, the enable and disable buttons are disabled.

To export the deployment details data requires the Export Deployment Data access right. If a user does not have the correct access, the export button is disabled.

Contact your Novell Administrator for more information on ZENworks Patch Management Security.

Deployments Results Security

The Deployment Results section of ZENworks Patch Management Server requires the View Deployment Statuses access right. If a user does not have the correct access, the access denied error message is displayed.

Contact your Novell Administrator for more information on ZENworks Patch Management Security.

9 Computers

The computers section of ZENworks Patch Management Server displays all computers which have an agent registered against ZENworks Patch Management Server. Clicking on a computer name will allow you to display a computer's specific information.

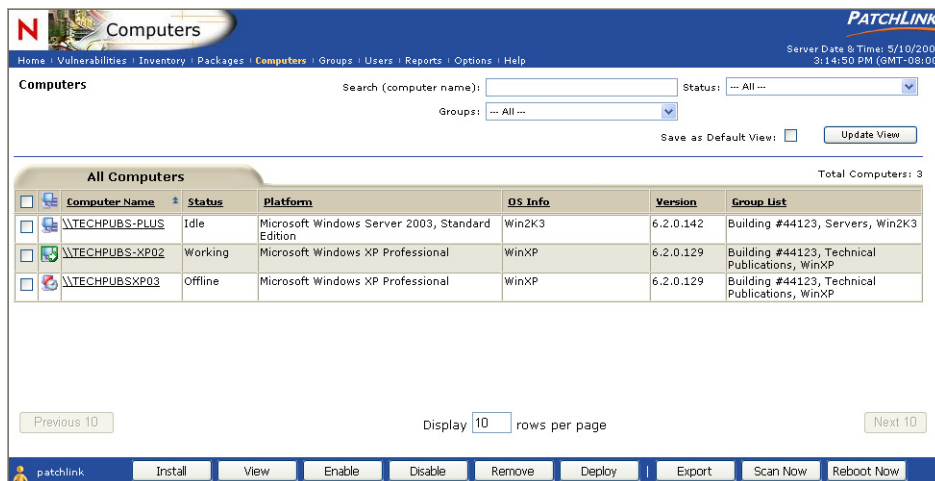


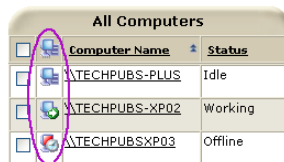
Figure 9.1 All Computers

Computer Information Page

Computer Information Columns

- **Computer Name** - This the name of the computer. Click on the computer name to display specific information about the computer.
- **Status** - This displays the status of the computer.
- **Platform** - This displays the operating system platform the computer is running.
- **OS Info** - This displays additional information about the operating system the computer is running.
- **Version** - This displays the version of the agent running on the computer.
- **Group List** - This displays the list of groups that the computer is a member of.

Agent Status



All Computers		
<input type="checkbox"/>	Computer Name	Status
<input type="checkbox"/>	VTECHPUBS-PLUS	Idle
<input type="checkbox"/>	VTECHPUBS-XP02	Working
<input type="checkbox"/>	VTECHPUBSXP03	Offline

Figure 9.2 Computer Status



Note: Refer to [Appendix B, “ZENworks Patch Management Server Reference”](#) for a complete definition of all available computer status icons.

Additional information may be displayed by hovering your mouse pointer over an enabled icon.

To display additional information about the computer, click on the name of the actual computer. This performs the same function as selecting the computer and clicking on the View button on the Action Menu.

* This usually means that either the deployment agent was removed from ZENworks Patch Management Server or there has been a problem in registering the deployment agent. For more information on this check the agent installation section.

Page Functions

- **Display and Hide** - Click the plus icon to display additional information and statistics about the represented item. Click the minus icon to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality is only available for Microsoft Internet Explorer at this time.
- **Advanced Page Search, Filtering, and View Saving** - The advanced page search, filtering dropdown menus, and saving functions appear in the Computers page header.
- **Search** - You may search computers for more granular results by entering the computer name text into the Search field and clicking on the Update View button. This will return the computer having the name of the entered text. You may then click the Save as Default View button to save your filtered view as your default view for the next time the page is visited.

- **Status** - Filter by status using the dropdown menu and click on the Update View button. This allows the user to search on enabled, sleeping, offline, and disabled systems that exist. You may then click the Save as Default View button to save your filtered view as your default view for the next time the page is visited.
- **Groups** - Filter by group using the dropdown menu and click on the Update View button. This allows the user to search on any user defined or server defined groups that exist. You may then click the Save as Default View button to save your filtered view as your default view for the next time the page is visited.

Action Menu

- **Install** - Click on the Install button to display the list of agent installers that can be used to register computers to ZENworks Patch Management Server. Refer to the [Agent Installation Guide](#) for further details regarding installing agents.
- **View** - To display additional information about the computer, select a computer and click on the View button. This performs the same function as clicking on the name of the computer.
- **Enable** - To enable selected disabled computers, click on the Enable button.
- **Disable** - To disable selected enabled computers, click on the Disable button. Disabled computers do not take up an agent license.
- **Export** - Exports the computer list data to a comma-separated value (CSV) file. The filter and order of the data is based on what the Computer List view is selected and sorted on. This may display only a certain number of computers per page, the export will save all computer data based on your selected filter.
- **Scan Now** - Initializes a screen that allows you to reschedule the Discover Applicable Updates System Task deployment for immediate execution to all selected computers. To initialize (choose) all computers, click the Scan Now button without selecting any computers.

Computers Security

The Computer List section of ZENworks Patch Management Server requires the View Computers access right. If a user does not have the correct access, the access denied error message is displayed.

To be able to be able display the agent installers' page requires the Install Computers access right. If a user does not have the correct access, the Install button is displayed. Once a computer registers against ZENworks Patch Management Server a Novell Administrator must give access to that computer to other user security roles.

To be able to enable, disable, and remove computers requires the Manage Computers access right. If a user does not have the correct access, the Enable, Disable, and Remove buttons are disabled.

To export the computer data to a comma-separated value (CSV) file requires the Export Computer Data access right. If a user does not have the correct access, the Export button is disabled.

To restart the discovery and analysis process for all of the computers registered to the ZENworks Patch Management Server requires the Manage System Tasks access right. If a user does not have the correct access, the Scan Now button is disabled.

Contact your Novell Administrator for more information on ZENworks Patch Management Security.

Computer Details Section

The Computer Details section of ZENworks Patch Management Server displays important information about a specific computer. Click on the **Computer Name** link under the *Computer Name* column. This will bring you to the details page.

- Selecting the Vulnerabilities tab will display the Vulnerability Analysis for the computer.
- Selecting Inventory tab will display the Inventory for the computer.
- Selecting Deployments tab will display the deployments for the computer.

The Vulnerabilities, Inventory, and Deployments tabs serve as a quick link to those related inquiries for a specific computer

Computers PATCHLINK
 Home | Vulnerabilities | Inventory | Packages | **Computers** | Groups | Users | Reports | Options | Help
 Server Date & Time: 5/10/2005 3:58:23 PM (GMT-08:00)

Computer Details for \\TECHPUBS-PLUS

Information Vulnerabilities Inventory Deployments

Computer Information:

Name: \\TECHPUBS-PLUS	Description:
Operating System: Win2K3	OS Version: 5.2
OS Service Pack:	OS Build Number: 3790
DNS Name: TechPubs-PLUS	IP Address: 10.11.1.192

Agent Information:

Agent Installation Date: 5/4/2005 12:43:34 PM (GMT-08:00)	Agent Status: Idle
Agent Version: 6.2.0.142	Last Connected Date: 5/10/2005 3:55:37 PM (GMT-08:00)

Group Information:

Group Name	Type	Status	Added By	Added On
Win2K3	Computer (system created)	Enabled	PatchLink Corp.	4/11/2005 12:40:00 PM (GMT-08:00)
Servers	Computer (user created)	Enabled	PATCHLINK	4/28/2005 5:21:00 PM (GMT-08:00)
Building #44123	Computer (user created)	Enabled	PATCHLINK	5/3/2005 5:24:00 PM (GMT-08:00)

Policy Information:

Communication Interval	Hours of Operation	Logging Level	Ping Port	Discovery Agent Mode
5 Minutes	Always Run	Basic Info	Off	Normal

Interactive Agent Information:

Deployment Notification Options	Reboot Notification Options
Cancelable: Yes	Cancelable: Yes
Snoozable: Yes	Snoozable: Yes
Deadline Date Offset: 15	Deadline Date Offset: 30
Offset Server Time: Yes	

patchlink Export Scan Now Reboot Now

Figure 9.3 Computer Details - Information Tab

If information is not applicable to a specific section, the section will simply not be present on the details page.

Computer Information

- **Name:** This displays the name of the computer
- **Operating System:** This displays the abbreviated operating system platform name of the computer.
- **OS Service Pack:** This displays the service pack level of the computer
- **DNS Name:** This displays the DNS name of the computer.
- **Description:** This displays the description of the computer.
- **OS Version:** This displays the operating system version number of the computer.
- **OS Build Number:** This displays the operating system build number of the computer.
- **IP Address:** This displays the IP Address of the computer.

Agent Information

- **ZENworks Patch Management Server Agent Installation Date:** The date the agent was installed and registered against ZENworks Patch Management Server.
- **ZENworks Patch Management Server Agent Version:** This displays the version of the agent.
- **ZENworks Patch Management Server Agent Status:** This displays the status of the agent.
- **Last Connected Date:** The date the agent last contacted ZENworks Patch Management Server.

Group Information

- **Group Name:** This displays the name of the group the computer is a member of.
- **Type:** This displays the type of the group.
- **Status:** This displays the status of the group.
- **Added By:** This displays the Novell User who added the computer to the group.
- **Added On:** This displays the date the computer was added to the group.

Policy Information

- **Communication Level:** This displays how often the agent communicates with ZENworks Patch Management Server.
- **Hours of Operation:** This displays the hours of operation in which the agent will communicate with ZENworks Patch Management Server.
- **Logging Level:** The logging level determines how much data the agent will log while it performs its tasks.

Page Functions

Vulnerabilities Tab - Selecting this tab will display the Vulnerability Analysis for the computer.

Inventory Tab - Selecting this tab will display the Inventory for the computer.

Deployments Tab - Selecting this tab will display the deployments for the computer.

Action Menu

Export - Exports the computer information to a comma-separated value (CSV) file.

Scan Now - Initializes a screen that allows you to reschedule the Discover Applicable Updates System Task deployment for immediate execution to all selected computers. ZENworks Patch Management Server will reschedule the computer and initialize a screen stating its success and provide a Deployment link to initialize a new window with the results of the Discover Applicable Updates Deployment.

Computer Details Security

The Computer Information section of ZENworks Patch Management Server requires the View Computers access right. If a user does not have the correct access, the access denied error message is displayed.

To export the computer information to a comma-separated value (CSV) file requires the Export Computer Data access right. If a user does not have the correct access, the Export button is disabled.

To restart the discovery and analysis process for all of the computers registered to the ZENworks Patch Management Server requires the Manage System Tasks access right. If a user does not have the correct access, the Scan Now button is disabled.

To be able to view the vulnerability results for the computer requires the View Vulnerabilities access right. If a user does not have the correct access, the Vulnerabilities tab is disabled.

To be able to view the computer inventory section requires the View OS Inventories access right. If a user does not have the correct access, the Inventory tab is disabled.

To be able to view the computer deployments section requires the View Deployment Status access right. If a user does not have the correct access, the Deployments tab is disabled.

Contact your Novell Administrator for more information on ZENworks Patch Management Security.

Vulnerabilities by Computer

A Vulnerability consists of the vulnerability description, the signatures and fingerprints required to determine whether the vulnerability is patched or not patched, and the associated package or packages for performing the patch.

Click on the Vulnerabilities tab in the Computer Details screen.

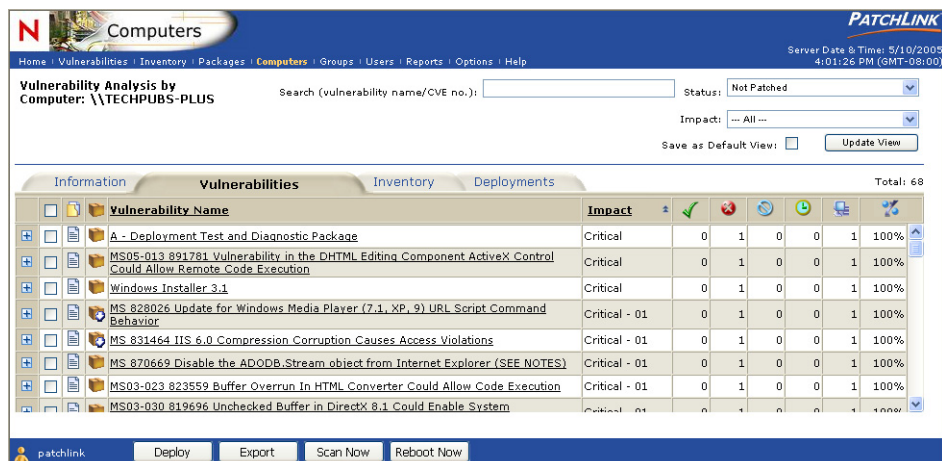


Figure 9.4 Computer Details - Vulnerabilities Tab

Vulnerability Analysis

This section displays the analysis results from the Discover Applicable Updates process on the computer. The analysis gives a simple top-down view of vulnerability patch status. The total number of vulnerabilities is displayed just above the table in the top right corner. The Vulnerabilities, Inventory, and Deployments tabs serve as a quick link to those related inquiries for a specific computer.

Page Functions

Information Tab - Selecting this tab will display additional Computer Information.

Inventory Tab - Selecting this tab will display the Inventory for the computer.

Deployments Tab - Selecting this tab will display the deployments that the computer has been assigned to.

Action Menu

Deploy - This creates a deployment for the selected vulnerability. See Section 9; Deploying Packages: Schedule Deployment Wizard for more information.

Export - Exports the vulnerability analysis to a comma-separated value (CSV) file. The amount and order of the data is based on what the analysis view is filtered and sorted on.

Computer Vulnerability Security

The Computer Vulnerabilities section of ZENworks Patch Management Server requires the View Vulnerabilities Page access right. If a user does not have the correct access the access denied error message is displayed.

To be able to change the filter from detected vulnerabilities to disabled or all requires the Change Vulnerability Filter access right. If a user does not have the correct access, the filter will not have any options to choose from.

To be able to view the associated distribution packages for a given vulnerability requires the View Packages access right. If a user does not have the correct access, the link on the package status image is disabled.

To be able to create a deployment based on the vulnerability analysis requires the Deploy Vulnerabilities access right. If a user does not have the correct access, the Deploy button is disabled.

To export all of the vulnerability analyses to a comma-separated value (CSV) file requires the Export Vulnerability Data access right. If a user does not have the correct access, the Export button is disabled.

To restart the discovery and analysis process for all of the computers registered to the ZENworks Patch Management Server requires the Manage System Tasks access right. If a user does not have the correct access, the Scan Now button is disabled.

To be able to view the computer inventory section requires the View OS Inventories access right. If a user does not have the correct access, the Inventory tab is disabled.

To be able to view the computer deployments section requires the View Deployment Status access right. If a user does not have the correct access, the Deployments tab is disabled.

Contact your Novell Administrator for more information on ZENworks Patch Management Security.

Computer Inventory Summary

The following inventories are gathered while in the discovery and analysis process: Operating Systems, Installed Software, Hardware and their device drivers, and Services. The Filter changes the display between the different inventories. When displaying the Inventory based on a single computer, the Operating Systems inventory is the initial inventory displayed. The Vulnerabilities, Inventory, and Deployments tabs serve as a quick link to those related inquiries for a specific computer.

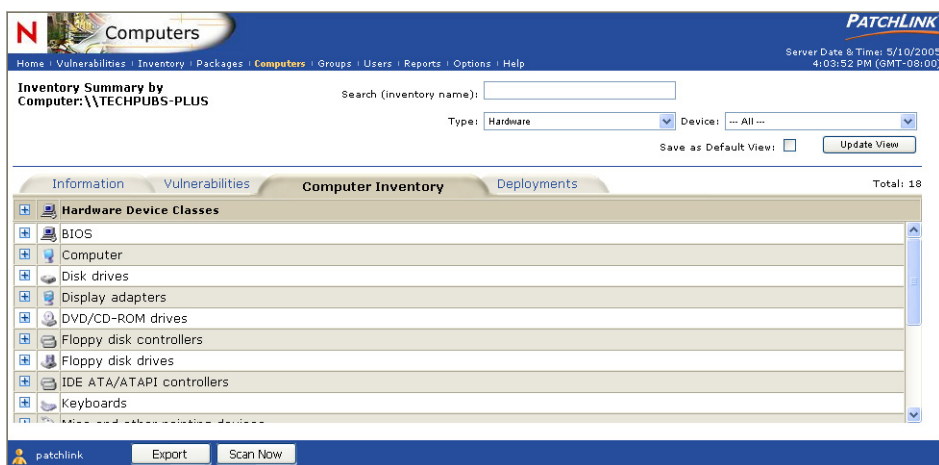


Figure 9.5 Computer Details - Inventory Tab

Action Menu

Export - Exports the inventory data to a comma-separated value (CSV) file. The amount and order of the data is based on what the view is filtered and sorted on.

Scan Now - Initializes a screen that allows you to reschedule the Discover Applicable Updates System Task deployment for immediate execution to all selected computers. ZENworks Patch Management Server will reschedule the computer and initialize a screen stating its success and provide a Deployment link to initialize a new window with the results of the Discover Applicable Updates Deployment.

Computer Inventory Security

The Computer Inventory section of ZENworks Patch Management Server requires the View OS Inventories access right. If a user does not have the correct access, the access denied error message is displayed.

To be able to view the Software inventory requires the View Software Inventories access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the Hardware inventory requires the View Hardware Inventories access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the Services inventory requires the View Services Inventories access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the list of computers on which an inventory belongs to requires the View Computers access right. If a user does not have the correct access, the hyperlink on the inventory item is disabled.

To export the inventory to a comma-separated value (CSV) file requires the Export Inventory Data access right. If a user does not have the correct access, the Export button is disabled.

To be able to view the vulnerability results for the computer requires the View Vulnerabilities access right. If a user does not have the correct access, the Vulnerabilities tab is disabled.

To be able to view the computer deployments section requires the View Deployment Status access right. If a user does not have the correct access, the Deployments tab is disabled.

Computer Deployments

The Computer Deployments section displays all of the deployments that the computer has been assigned to.

Name	Initial Start Date	1	0	1	0	0	0%
System Task: Reboot	Not Scheduled	1	0	1	0	0	0%
System Task: Refresh Inventory Data	5/14/2005 6:00:00 AM (Local)	1	0	1	0	0	0%
System Task: Discover Applicable Updates	5/11/2005 1:11:29 PM (Local)	1	0	1	0	0	0%
Deploying MS05-015 888113 (2K3) Remote Code Execution Vulnerability in Hyperlink Object Library	4/28/2005 4:48:33 PM (UTC)	1	0	1	0	1	100%
Deploying MS05-016 893086 (2K3) Vulnerability in Windows Shell that Could Allow Remote Code Execution	4/28/2005 4:48:33 PM (UTC)	1	0	1	0	1	100%
Deploying MS05-018 890859 (2K3) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege and Denial of Service	4/28/2005 4:48:33 PM (UTC)	1	0	1	0	1	100%

Figure 9.6 Computer Details - Deployments Tab

The Vulnerabilities, Inventory, and Deployments tabs serve as a quick link to those related inquiries for a specific computer.

Action Menu

Export - Exports the deployment data to a comma-separated value (CSV) file. The amount and order of the data is based on what the view is filtered and sorted on.

Computer Deployments Security

The computer deployments section requires the View Deployment Status access right. If a user does not have the correct access, the access denied error message is displayed.

To be able to view the vulnerability results for the computer requires the View Vulnerabilities access right. If a user does not have the correct access, the Vulnerabilities tab is disabled.

To be able to view the computer inventory section requires the View OS Inventories access right. If a user does not have the correct access, the Inventory tab is disabled.

To be able to view the computer deployments section requires the View Deployment Status access right. If a user does not have the correct access, the Deployments tab is disabled.

To be able to export the computer deployment data requires the Export Deployment Data access right. If a user does not have the correct access, the Export button is disabled.

Contact your Novell Administrator for more information on ZENworks Patch Management Security.

10 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.

[“About Inventory” on page 125](#)

[“Using the Workspace” on page 130](#)

[“Viewing Inventory Data” on page 130](#)

[“Searching Inventory” on page 139](#)

[“Exporting Inventory Data” on page 141](#)

[“Scanning Inventory” on page 142](#)

About Inventory

Inventory captures a comprehensive snapshot of your entire systems inventory. You can generate an inventory list for software, hardware, operating systems, and services installed on a system.

Using this feature, you can quickly and easily determine all computers that have a particular component installed. Once identified, you can directly access the *Computer Details* page for the specified computer. The inventory list displays each item belonging to a specific *Inventory Type*. For example, it will display all operating systems detected on the network. For each listed item, click the expand icon (plus icon) to view all computers 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 across the network.

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

- **Computers** - Click a computer name to view the details page for the selected computer. In the *Computer 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.

How it works

Inventory is collected through the installation of ZENworks Patch Management Agent on every client machine (computer) managed and monitored by the ZENworks Patch Management Server. In a typical installation, the ZENworks Patch Management Agent installed on a client machine include client, detection and subscription agents.

As part of the Detection Agent Update system task, ZENworks Patch Management Server obtains data from the software installation database native to the operating system by running the appropriate command. That data is then compiled and generated into a text file (`localprofile.txt`) and uploaded to the ZENworks Patch Management Server.

Table 10.1 Source Files for Inventory

OS	Source	Command
Windows	Registry database	
Unix	rpm database	
Linux	rpm database	<code>rpm -q</code>



Note: If the ZENworks Patch Management Agent (client agent) is installed on separate virtual systems, these systems will behave as distinct physical systems (hosts) with identical hardware. Each virtual system therefore is inventoried and the data submitted to ZENworks Patch Management Server. As such, the virtual system is reported as having identical hardware information.

Detection Agent

The detection agent has the primary role of performing detection scans which allow the ZENworks Patch Management Server to determine security holes and other vulnerabilities present in your computing environment. This network analysis is a key component in determining 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 patch reports. The ZENworks Patch Management Server then instructs the applicable agent to implement corrective action.

Detection Agent Update Task

The Detection Agent Update task (DAU) runs the Detection Agent. This system task is performed daily on an established schedule and also after every successful deployment. The DAU task is managed through the Packages page. Click **Packages**, select *Discover Applicable Updates* in the list of available packages, then use any of the tools available to manage the DAU task.



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

Refresh Inventory Data Task

The Refresh Inventory Data (RID) task is a system task that performs an inventory check over the entire network. The RID task agent scans the local system and generates a list of operating systems, software applications, hardware devices, and services installed on each computer within your network. This information is compiled in a text file and saved on the local computer (the client). The file is named `localprofile` and resides in the installation directory.

The RID task is performed as a one-time deployment (system-wide) when a computer is registered to the ZENworks Patch Management Server. As well, the task is automatically scheduled to run as a recurring deployment (system-wide). The task is scheduled to run weekly on Saturdays. At this time, the RID task erases the `localprofile.txt` file, causing the DAU task to create a new `localprofile.txt` file and upload the inventory report to the ZENworks Patch Management Server.

Table 10.2 Inventory Profile File

File name	<code>localprofile.txt</code>
Directory*	<code>C:\Program Files\Patchlink\Update Agent</code>
*Assume default installation directory was used during client agent installation.	

Example File

The following is an example local profile file (localprofile.txt).

```
<systemprofile>
<computer>
  <BuildNumber>2600</BuildNumber>
  <Caption>Microsoft Windows XP Professional</Caption>
  <CSDVersion>Service Pack 2</CSDVersion>
  <Version>5.1.2600</Version>
  <computername>\\USER</computername>
  <DAversion>6.1.0.109</DAversion>
  <type>information</type>
  <agentid>0FD3FDF5-1654-410C-91A8-9842247E7F50</agentid>
</computer>
<services>
  <caption svcName="Fax" State="Stopped" Startup="Automatic">Fax</caption>
</services>
<devices>
  <caption class="Monitors">Plug and Play Monitor</caption>
</devices>
<software>
  <package>PatchLink Update Agent</package>
</software>
</systemprofile>
```

Detection Results

If the ZENworks Patch Management Agent are 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 do this, click **Computers** and then select the computer in question. On the *Computers Details* page, click the **Computer Deployments** tab.

If both system tasks are scheduled for deployment, the problem is likely due to issues specific to the Agent computer. You can open the `debug.log` file in `C:\Program Files\Patchlink\Update Agent\` and look for error codes or messages indicating why the Agent cannot upload its discovery results to the local ZENworks Patch Management Server.

Access Levels

Access to the inventory feature is limited to user roles that have the following access rights assigned; View Operating System Inventories, View Hardware Inventories, View Service Inventories, or View Software Inventories. To export inventory to a comma-separated value (CSV) file requires the Export Inventory Data access right.

By default, all roles have access rights to each of the inventory features. Exporting is available to all roles except guest.



Note: Users must have the *View Computers* access right assigned in order to view inventory information for a particular computer. This is a default access right in the Administrator, Manager, Operator, and Guest role templates.

The following access rights are associated with inventory:

- View Operating System Inventories - allows you to run and view inventory reports for the operating system inventory type only. This is a default access right in the Administrator, Manager, Operator, and Guest role templates.
- View Software Inventories - allows you to run and view inventory reports under for the software inventory type only. This is a default access right in the Administrator, Manager, Operator, and Guest role templates.
- View Hardware Inventories - allows you to run and view inventory reports for the hardware inventory type only. This is a default access right in the Administrator, Manager, Operator, and Guest role templates.
- View Service Inventories - allows you to run and view inventory reports for the services inventory type only. This is a default access right in the Administrator, Manager, Operator, and Guest role templates.
- Export Inventory Data- can export inventory data to a CSV file. This access right enables the Export feature in the *Inventory* page. This is a default access right in the Administrator, Manager, and Operator role templates.



Note: If a user is not assigned any of these access rights, the Inventory option in the toolbar is turned off (disabled) and the application returns an *access denied* error message if an attempt to access the *Inventory* page is made by entering the URL directly. If the user is not assigned rights to a particular inventory type, that type cannot be selected in the *Type:* list box.

Using the Workspace

The *Inventory* page is available by clicking **Inventory** on the main toolbar.



Figure 10.1 Inventory Toolbar

The *Inventory* page displays a listing of each *Inventory Type* and the computers that have the selected type (operating system, software application, hardware device, or service) installed. For each listed type, click the expand icon (plus icon) to view all computers installed with or running the selected component. Clicking the expand icon displays the list of computers meet the selected inventory criteria. Clicking the collapse icon hides this list from view.

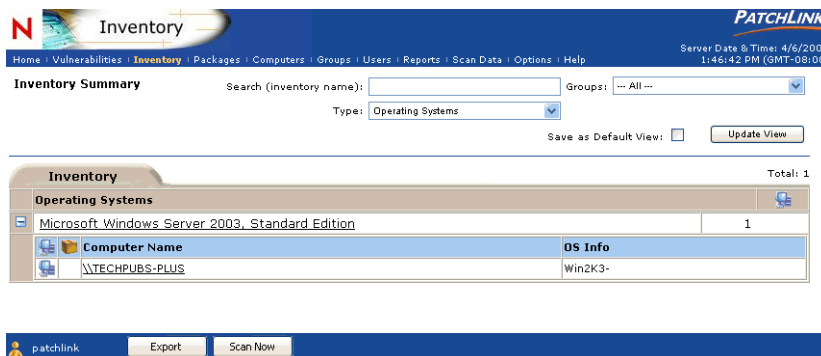


Figure 10.2 Inventory Summary

Viewing Inventory Data

Inventory is presented based on a series of customizable filters, including a search filter. The entry point for inventory is the inventory type, defined as operating system, software, hardware, and services. Each inventory report must have an inventory type assigned before an inventory list can be generated. The operating system type is the default inventory type.

Default Views

Default views allow you to save a particular inventory profile as the default profile to display each time the *Inventory* page is opened. A profile is defined as the entire set of criteria established for a particular inventory view; and can include any combination of type, groups, devices, and search criteria defined for the view.

The view criteria, or profile, you define is then displayed each time you open the *Inventory* page. You can change default views at any time.

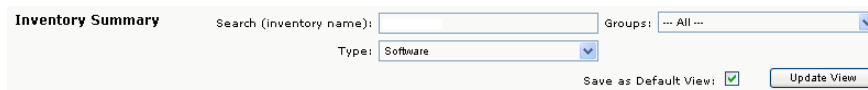
The screenshot shows a web interface titled "Inventory Summary". It features a search bar labeled "Search (inventory name):" with an adjacent text input field. To the right is a "Groups:" dropdown menu currently set to "... All ...". Below the search bar is a "Type:" dropdown menu set to "Software". At the bottom right, there is a checkbox labeled "Save as Default View:" which is checked, and an "Update View" button.

Figure 10.3 Inventory Search and Filter

Creating Default Views

To Create a Default View

1. On the *Inventory* page, define an inventory data set using any combination of type, groups, device, and search criteria.
2. Click **Save as Default View**.
3. Click **Update View**.
4. The inventory list defined by the selected criteria displays on the *Inventory* page.

Inventory Types

You can filter the inventory list that is presented by selecting an Inventory Type from the *Type* list box and clicking **Update View**.

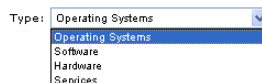
The screenshot shows a "Type:" dropdown menu. The menu is open, displaying a list of options: "Operating Systems", "Software", "Hardware", and "Services". "Operating Systems" is currently selected and highlighted in blue.

Figure 10.4 Inventory Type

ZENworks Patch Management Server supports filtering by the following types and related sub-filters:

- Operating Systems - Groups
- Software - Groups
- Hardware - Groups, Devices
- Services - Groups, Devices



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 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 the operating system inventory for a single computer.

Click the expand icon for an operating system to display the list of computers on which the OS is installed. Click the computer name to go to the computer details page. Click the OS name to go to a detailed description of the computers with the selected OS installed.

Inventory Summary

Search (inventory name): Groups: Type: Save as Default View: ☐

Inventory		Total: 1
Operating Systems		
<input type="checkbox"/>	Microsoft Windows Server 2003, Standard Edition	1
<input type="checkbox"/>	Computer Name	OS Info
<input type="checkbox"/>	\\TECHPUBS-PLUS	Win2K3-

Figure 10.5 Inventory Operating System View

To View Operating System Inventory

1. On the *Inventory* page, define an inventory data set and click **Update View**.
2. With the selected inventory displayed, click **Export**.
3. In the File Download dialog box, select from the available options (Open, Save, Cancel).

- a. 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.
- b. Save - creates the file and saves it to a local folder. By default the file is saved to your My Documents folder in Microsoft Office Excel CSV format.
- c. Cancel - does not create or save the report.

Software View

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

Click the expand icon for a software application to display the list of computers on which the software is installed. Click the computer name to go to the computer details page. Click the software name to go to a detailed description of the computers with the selected software installed.

Inventory Summary Search (inventory name): Groups: Type: Save as Default View: ☐

Inventory		Total: 16
Software Programs		
MICROSOFT XML 4.0 SP 2 - [VERSION 4.0]	1	
PATCHLINK AGENT MANAGEMENT CENTER - [VERSION 6.2.0]	1	
<div>Computer Name</div> <div>\\TECHPUBS-PLUS</div>	<div>OS Info</div> <div>Win2K3-</div>	
PATCHLINK DEVELOPERS KIT - [VERSION 1.4.0]	1	
PATCHLINK SCANNER INTEGRATIONPOINT - [VERSION 6.2.0]	1	
PATCHLINK SIP - [VERSION 2.0]	1	
PATCHLINK SYSTEM INFORMATION - [VERSION 1.0.0]	1	

Figure 10.6 Inventory Software View

To View Software Inventory

1. On the *Inventory* page, define an inventory data set and click **Update View**.
2. With the selected inventory displayed, click **Export**.
3. In the File Download dialog box, select from the available options (Open, Save, Cancel).

- a. 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.
- b. Save - creates the file and saves it to a local folder. By default the file is saved to your My Documents folder in Microsoft Office Excel CSV format.
- c. Cancel - does not create or save the report.

Hardware View

Displays the hardware devices found on the network. 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 on the network.

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

Inventory Summary

Search (inventory name): Groups:

Type: Device:

Save as Default View: ☐

Inventory Total: 18

Hardware Device Classes		
	BIOS	
	Computer	
	Device	Instances
	ADVANCED CONFIGURATION AND POWER INTERFACE (ACPI) PC	1
	Disk drives	
	Display adapters	
	DVD/CD-ROM drives	

Figure 10.7 Inventory Hardware View



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

Click the expand icon for an device class to display a list of all devices within that class. Click the expand icon for a device to display the list of computers on which the device is installed or configured. Click the computer name to go to the computer details page. Click the device name to go to a detailed description of the computers enabled with the selected device.

To View Hardware Inventory

1. On the *Inventory* page, define an inventory data set and click **Update View**.
2. With the selected inventory displayed, click **Export**.
3. In the File Download dialog box, select from the available options (Open, Save, Cancel).
 - a. 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.
 - b. Save - creates the file and saves it to a local folder. By default the file is saved to your My Documents folder in Microsoft Office Excel CSV format.
 - c. Cancel - does not create or save the report.

Services View

Displays the services detected on the network. The list includes all services detected, both those that are running and services that are not. Each service also includes the number of instances that the service was detected on the network.

Click the expand icon for a service to display a list of all computers on which the service is installed (running or not) or configured. Click the computer name to go to the computer details page. Click the service name to go to a detailed description of the computers enabled with the selected service.

Inventory Summary

Search (inventory name): Groups:

Type:

Save as Default View: ☐

Inventory Total: 98

Service Name		
ALERTER		1
	Computer Name	OS Info
	\\TECHPUBS-PLUS	Win2K3-
APPLICATION LAYER GATEWAY SERVICE		1
APPLICATION MANAGEMENT		1
ASP.NET STATE SERVICE		1
AUTOMATIC UPDATES		1

Figure 10.8 Inventory Services View

To View Services Inventory

1. On the *Inventory* page, define an inventory data set and click **Update View**.
2. With the selected inventory displayed, click **Export**.
3. In the File Download dialog box, select from the available options (Open, Save, Cancel).
 - a. 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.
 - b. Save - creates the file and saves it to a local folder. By default the file is saved to your My Documents folder in Microsoft Office Excel CSV format.
 - c. Cancel - does not create or save the report.

Inventory Groups

The inventory summary can be filtered according your ZENworks Patch Management Server groups. As part of setting up the ZENworks Patch Management Server, may have elected to create groups to streamline the management of deployments to computers residing on your network. See Chapter # “Groups” pointer for information on creating and adding groups.



Tip: A group is a collection of computers organized for the purpose of making deployments to a set of computers (a group) with similar needs.

You can filter inventory to list results according to group by selecting from the list of available groups in the *Groups* list box and clicking **Update View**. This option is best used to more narrowly define the results that are generated when filtering by an inventory type. The groups filter is a sub-set of the filter selected in the inventory type filter.



Note: In filtering by group, a type filter must also be selected. There is no option to filter by groups independent of type.

Inventory that meets the group and type filters (and search filter if entered) is returned in the inventory list. To save the filter and establish it as a filter, select the **Save as Default View** option. Each time you open the *Inventory* page, the defined filter is enabled and the appropriate results are presented.

In this example, the ZENworks Patch Management Server environment has been configured to include a number of groups based on various operating system platform categories.

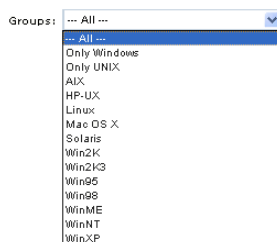


Figure 10.9 Groups

Inventory Devices

The inventory summary can be filtered according to the installed devices on the network. This is only available when the inventory type **hardware** is selected.

You can filter inventory to list results according to group by selecting from the list of available groups in the *Groups* list box and clicking **Update View**. This option is best used to more narrowly define the results that are generated when filtering by an inventory type. The groups filter is used as a sub-set to the filter selected in the inventory type filter.



Note: In filtering by device, the default type must be hardware. There is no option to filter by devices independent of the hardware type.

Inventory that meets the device filters (and any other selected filters, including search) is returned in the inventory list. To save the filter and establish it as a filter, select the **Save as Default View** option. Each time you open the *Inventory* page, the defined filter is enabled and the appropriate results are presented.

In this example, the ZENworks Patch Management Server environment has been configured to include a number of groups based on various operating system platform categories.



Figure 10.10 Devices

Searching Inventory

The search feature lets you create an ad-hoc inventory report based on a very specific criteria and is used to expedite the selection of data or to assist in generating inventory on a very narrow, or specific, range of items. In essence, allowing you to search inventory for more granular results by entering search criteria into the *Search (inventory name)* field and click **Update View**.

Search (inventory name):

Figure 10.11 Search Field

Search Rules

The search feature provides standard searching on a word matching basis (exact and partial matching). 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*.

For example, conducting a search using the search terms *Adobe* within the *Type:* *Software* option will produce a result set that includes all software inventory from Adobe Systems (*Adobe Acrobat*, *Adobe Reader*). The same effort using the search term *A* produces a result set that includes all software inventory from Adobe Systems (*Adobe Acrobat*, *Adobe Reader*) as well as any other software application that contains an *A* in the program name (*Adobe Acrobat*, *PatchLink*, *Microsoft ASP.NET*).

Inventory Summary

Search (inventory name): Groups:

Type:

Save as Default View: ☐


Inventory		Total: 2
Software Programs		
<input type="checkbox"/>	ADOBE DOWNLOAD MANAGER 2.0 (REMOVE ONLY) - [VERSION 2.0]	1
<input type="checkbox"/>	ADOBE READER 7.0 - [VERSION 7.0.0]	1

Figure 10.12 Software Programs

Search Dependencies

The search feature is used as a sub-set with the filters selected in the inventory type and groups filter options. For example, conducting a search on *Microsoft* will return unique results based on the inventory type that is also selected. Using the filter, *Type: Software*, produces a result set that includes all software inventory from Microsoft (*Microsoft ASP.NET*, *Microsoft SQL Server*), while using the filter, *Type: Operating System*, produces a result set that includes the operating system inventory (*Microsoft Windows Server*, *Microsoft XP*).

To Search Inventory Data

1. On the *Inventory* page, define an inventory type or use the default type.
2. In the Search text box, enter the search term(s) that describe the inventory you want to return.
3. Click **Update View**.

Exporting Inventory Data

Inventory is presented in ZENworks Patch Management Server can be exported into a comma-separated value (CSV) file supporting the Microsoft Excel Worksheet file type. You may elect to save the file in a different file format *after* opening it from the download option.

Click Export at the bottom of the page to save inventory information into a CSV file.

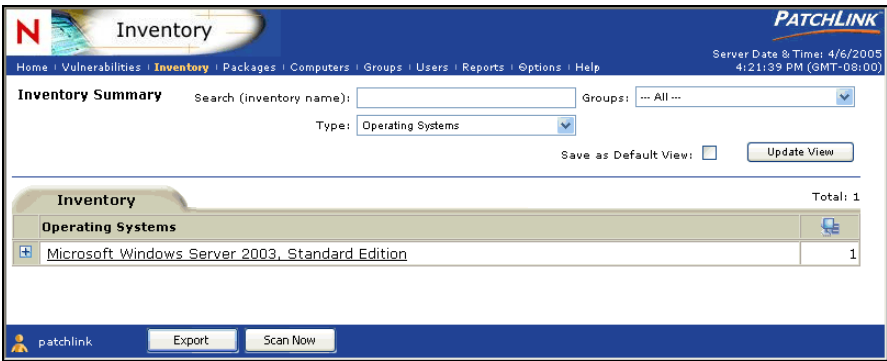


Figure 10.13 Operating Systems

The file naming convention incorporates the inventory type and group name. For example;

Table 10.3

Type	Group	File name
Operating System	All	OSAllInventoryExport.csv

To Export Inventory Data

- On the *Inventory* page, define an inventory data set and click **Update View**.
- With the selected inventory displayed, click **Export**.
- In the File Download dialog box, select from the available options (Open, Save, Cancel).

- a. 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.
- b. Save - creates the file and saves it to a local folder. By default the file is saved to your My Documents folder in Microsoft Office Excel CSV format.
- c. Cancel - does not create or save the report.

Scanning Inventory

Within inventory, you can elect to initiate a scan of the environment to capture up-to-the-minute inventory data. The **Scan Now** option initializes a process that allows you to reschedule the deployment of the Discover Applicable Updates (DAU) system task for immediate execution to all selected computers.

To initialize (choose) all computers, click the Scan Now button without selecting any computers. If you choose not to select any computers, the screen will ask you if you wish to confirm the reschedule the Discover Applicable Updates System Task for all of the computers.

Click **Scan Now** at the bottom of the page to initiate the deployment of the DAU agent.

To Scan the Network for Inventory

1. On the *Inventory* page,
2. Click **Scan Now**. The DAU deployment pertains to all computers, therefore the inventory definitions you may have on the screen are immaterial.
3. In the Scan Now dialog box, click **Yes**.
 - Click deployment to open the *Deployments by system package* page.
 - Click Discover Applicable Updates to open the *System Package Details* page.



Note: Understand that scheduling a DAU deployment entails traffic to all computers on the network.

See Running /Editing RID

See Running / Editing DAU

Printing Inventory Pages

Inventory was not designed to generate well-formatted print version of the *Inventory* page directly from the PLUS Web application (that is, in a Web browser). While you certainly can use the print command in your Web browser, please note the following:

- The page is not resized to fit the print output page size.
- Categories are not expanded by default.
- Data contained within a scrolling area is not printed. that is, the print output comprises only a representation of the contents of the page online.
- Attempting to print an inventory page using the Web browser (File | Print) can result in an error in cases where the inventory data comprises more than one printed page. In these cases, only the first page of a multi-page inventory report will successfully print.

A solution for printing that not only solves this issue, but also permits you greater control over the layout of the printed report, is to use the Export feature to bring the inventory data into an Excel (CSV) file and then use the print features within Excel.



Tip: For best printing results, export the data to a CSV file and open it as a worksheet. Then you can edit and modify the data in the worksheet and print it from your spreadsheet application (Microsoft Excel). Excel offers many options to help you present worksheet data. For example, use the Auto Filter feature to create views and manipulate the display of inventory data.

To Print Inventory

1. Update the *Inventory* page to view the desired inventory data
2. In the Web browser, click **File**, then click **Print...** (In the File menu, click **Print...**).



Note: Use the Print Preview and page Setup settings in your Web browser to better adapt the *Inventory* page for printing.

11 Groups

A group is a collection of computers for the purpose of making deployments to multiple computers at once. The purpose is based upon user specification to provide an easier way to manage the entire group rather than managing each computer one at a time.

Defining Effective Grouping Methods

Effective Grouping is a vital step in managing your ZENworks Patch Management implementation. In addition to the system created groups, it is recommended that you create some or all of the following group types, dependent upon your organizational needs:

- **Criticality Groups** - Machines grouped by criticality such as mission critical, production, and development. These are perhaps your most critical groups. These groups contain the computers which **MUST** never, under any circumstances, be inaccessible during business hours. Assign these groups **Agent Policy Sets** that limit the hours of operation, thus preventing any deployments or reboots during business hours.
- **Functional Groups** - Machines grouped by functions such as web servers, SQL servers, file servers, and print servers
- **Geographical Groups** - These are groups that are created based on geographical limitations. They are generally unique physical locations such as remote offices, different campuses, countries, and other geographical criteria
- **Operational Groups** - These groups are synonymous with the users that administer them
- **Reporting Groups** - These read-only groups are created for management and auditing reports



Note: The system created groups are created based on agent reporting and should **NOT** be disabled. These will be the catch-all groups that prevent machines from being omitted from any deployments

Groups Page

Clicking on the group name will display the group information and properties page. This is the same thing as selecting the group and clicking on the Properties button.

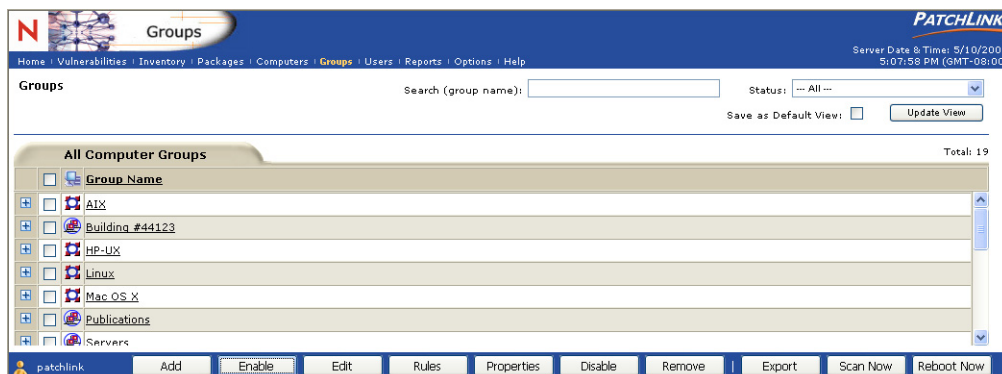


Figure 11.1 All Groups

With a group you can:

- Deploy a distribution package (from an associated Vulnerability or local distribution package) to all computers of the group. When deploying from the Vulnerabilities section, the only computers which will receive the distribution package are the ones that are applicable to the vulnerability.
- Define a set of policies which determine the behavior of the agents installed on those computers.
- Define a baseline of Vulnerabilities or local distribution packages which are declared as mandatory. This ensures that these baseline items must be installed or detected as patched; else the deployments for those items will be auto-generated for immediate execution.
- View the results of the Vulnerability Analysis for the entire membership of the group.
- View the results of the detected Inventory for the entire membership of the group.
- Reschedule the Discovery and Analysis process (Discover Applicable Updates System Task) to verify the Inventory and Vulnerabilities data is current.

Group Status

This displays the various groups that have been pre-generated by ZENworks Patch Management Server or user-defined by the local administrator. Each group entry displays the name of the group, the group status and type of the group.

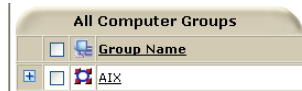






Figure 11.2 Group Status

Table 11.1 Group Status Icons

Icon	Description
	Enabled System group (a system group is created for each recognized operating system)
	Disabled System group (a system group is created for each recognized operating system)
	Enabled User group (user groups are manually created)
	Disabled User group (user groups are manually created)

Page Functions

- **Display and Hide** - Click the plus icon to display additional information and statistics about the represented item. Click the minus icon to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality is only available for Microsoft Internet Explorer at this time.
- **Advanced Page Search, Filtering, and View Saving** - The advanced page search, filtering dropdown menus, and saving functions appear in the Groups page header.
- **Search** - You may search Groups for more granular results by entering the group name text into the Search field and clicking on the Update View button. This will return the Group(s) having the name of the entered text. You may then click the Save as Default View button to save your filtered view as your default view for the next time the page is visited.
- **Status** - Filter by Status using the dropdown menu and click on the Update View button. This will return the Group(s) having the selected status. You may then click the Save as Default View button to save your filtered view as your default view for the next time the page is visited.

Action Menu

- **Add** - Clicking this button will bring up the Group Property page allowing new groups to be created. See Section 12; Add a Group Wizard for more information.
- **Edit** - By clicking on the button, a edit group wizard comes up in which u can enter all the information about the already existing group. See Section 12; Add a Group Wizard for more information.
- **Rules** - Clicking the Rules button allows the Novell User the ability to create and populate a group based on a few minimal parameters. Group Name, Group Description, and a comma-delimited list of computer names (Windows computers must be prefixed with \\) may be entered.
- **Properties** - Selecting a group and clicking on this button will display the group information and properties page.
- **Disable** - This disables all group-based functionality for the group members.
- **Enable** - This enabled all of the group-based functionality for the group members.
- **Remove** - This will delete all selected disabled groups.
- **Export** - Exports the group data to a comma-separated value (CSV) file. The amount and order of the data is based on what the Group List view is filtered and sorted on.
- **Scan Now** - Initializes a screen that allows you to reschedule the Discover Applicable Updates System Task deployment for immediate execution to all selected groups.

Groups Security

The Groups section of ZENworks Patch Management Server requires the View Groups access right. If a user does not have the correct access, the access denied error message is displayed.

To be able to create, edit, enable, disable, and remove groups requires the Manage Groups access right. If a user does not have the correct access, the Add, Edit, Rules, Enable, Disable and Remove buttons are disabled.

To export all of the group data to a comma-separated value (CSV) file requires the Export Group Data access right. If a user does not have the correct access, the Export button is disabled.

To reschedule the discovery and analysis process (Discover Applicable Updates System Task) for all members of the selected groups requires the Manage System Tasks access right. If a user does not have the correct access, the Scan Now button is disabled.

Contact your Novell Administrator for more information on ZENworks Patch Management Security.

Group Information

The group information and properties section of ZENworks Patch Management Server displays group related information, properties, and assessment graphs for viewing various statuses concerning the group's membership. Click on the actual group name link. The information tab of the Computer Information page (default) appears. (Win XP, All vendors, All Impacts, By Agent is used as an example)

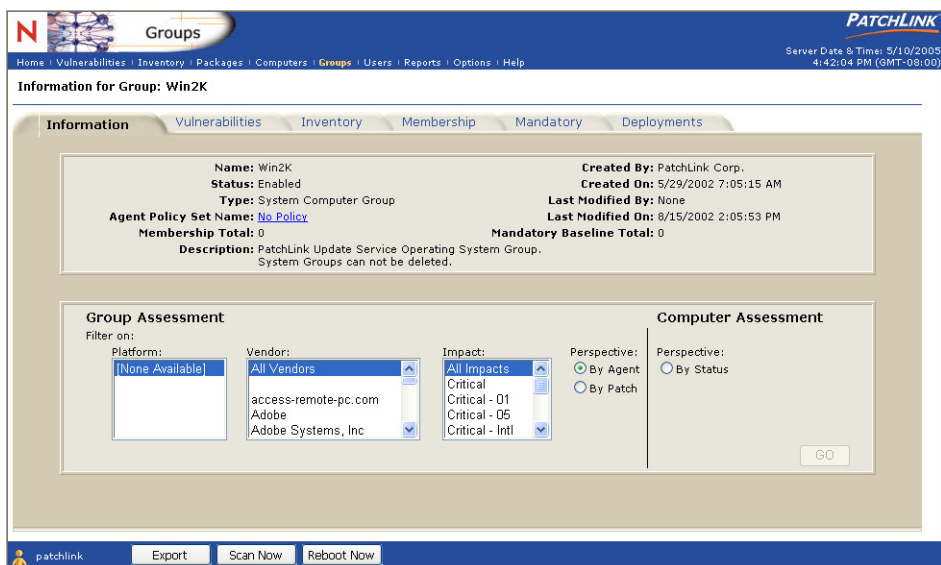


Figure 11.3 Group Information Tab

Information

- **Name:** This displays the name of the group.
- **Status:** This displays the current status of the group.
- **Type:** This displays the type of the group with respect to how it was created.
- **Agent Policy Set Name:** This displays the assigned Agent Policy Set name and link to view the agent policy set information.
- **Membership Total:** This displays the total number of computers which are a member of the group.
- **Created By:** This displays the user who created the group.
- **Created On:** This displays when the group was created.
- **Last Modified By:** This displays the user who last modified the group.
- **Last Modified On:** This displays when the group was last modified.
- **Mandatory Baseline Total:** This displays the total number of patches which create the baseline for the group.
- **Description:** This displays the group's description.

Group Assessment

There are three basic graphs that can display status information about the group's membership. Selecting any one of the three options and clicking the Go button will initialize a graphical representation pie chart screen illustrating the assessment.

Group Patch Status by Agent

This displays the how many agents are in each of the following patch statuses:

- **Fully Patched:** the computer requires no additional patches at this time.
- **Partially Patched:** the computer is not fully patched, but has some patches installed.
- **Not Patched:** The computer contains 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.

Additionally there are three filters that can define down to obtain more precise status information. The filters are:

- Platform
- Vendor
- Vulnerability Impact

Group Patch Status by Patch

This displays the how many applicable patches are in each of the following patch statuses:

- **Fully Patched:** the computer requires no additional patches at this time.
- **Partially Patched:** the computer is not fully patched, but has some patches are installed.
- **Not Patched:** The computer contains is not patched at all.
- **Detecting:** In process of running the Discovery and Analysis Process
- **Non-applicable:** The number of computers which have no Vulnerabilities applicable to them.

Additionally there are three filters that can define down to obtain more precise status information. The filters are:

- Platform
- Vendor
- Vulnerability Impact

Agent Status

This displays the number of computers in each of the various agent states. The various states are:

- **Sleeping:** these computers are outside their defined hours of operation.
- **Offline:** these computers haven't contacted ZENworks Patch Management Server in over two communication intervals (15 minutes minimum for intervals smaller than 10 minutes).
- **Running:** these computers are currently running the Discovery and Analysis process and they do not correspond to a registered Deployment agent.
- **Idle:** these computers are active yet not performing any deployments.
- **Working:** these computers are working on some deployments.
- **Disabled:** these computers are disabled and will be given no work to do.

Lock Information

If a Novell User has locked a group's vulnerabilities, software, hardware or services, then information about the lock is displayed here.

Lock Type

This displays what type of group lock was done. The four various types are:

- Group Vulnerability Locks
- Group Inventory Software Locks
- Group Inventory Hardware Locks
- Group Services Hardware Locks

Total Locked

This displays the total number of items which were locked.

- **Last Locked By:** This displays who locked the group.
- **Last Locked On:** This displays when the group was locked.
- **Lock Notes:** This displays any notes that were added when the group was locked.

Page Functions

Action Menu

- **Export** - Exports the group information to a comma-separated value (CSV) file.
- **Scan Now** - Initializes a screen that allows you to reschedule the deployment of the Discover Applicable Updates System Task for immediate execution to all enabled group members. Previously selected deployment options are maintained.

Security

The Group Information and Properties section requires the View Groups access right. If a user does not have the correct access, the access denied error message is displayed.

To export all of the group information data to the comma-separated value (CSV) file requires the Export Group Data access right. If a user does not have the correct access, the Export button is disabled.

To restart the discovery and analysis process for all of the computers registered to the ZENworks Patch Management Server requires the Manage System Tasks access right. If a user does not have the correct access, the Scan Now button is disabled.

The Vulnerabilities tab requires the View Vulnerabilities access right. If a user does not have the correct access, the Vulnerabilities tab is disabled.

The Inventory tab requires the View Software Inventory access right. If a user does not have the correct access, the Inventory tab is disabled.

The Membership tab requires the View Computers access right. If a user does not have the correct access, the Membership tab is disabled.

The Deployments tab requires the View Deployment Status access right. If a user does not have the correct access, the Deployments tab is disabled.

Contact your Novell Administrator for more information on ZENworks Patch Management Security.

Vulnerabilities by Group

A Vulnerability consists of the vulnerability description, the signatures and fingerprints required to determine whether the vulnerability is patched or not patched, and the associated package or packages for performing the patch.

The screenshot shows the 'Groups' section of the ZENworks Patch Management Security interface. The 'Vulnerability Analysis by Group: Win2K3' is selected. The search filter is empty, and the status is set to 'Not Patched'. The impact is set to 'Critical Patches (NEW)'. The table shows three vulnerabilities, all with a 'Critical' impact and a status of '100%'. The vulnerabilities are:

Vulnerability Name	Impact	0	1	0	0	1	100%
A - Deployment Test and Diagnostic Package	Critical	0	1	0	0	1	100%
MS05-013 891781 Vulnerability in the DHTML Editing Component ActiveX Control Could Allow Remote Code Execution	Critical	0	1	0	0	1	100%
Windows Installer 3.1	Critical	0	1	0	0	1	100%

The interface also includes a 'patchlink' logo, a 'View' button, and a row of action buttons: Deploy, Lock, Unlock, Disable, Export, Update Cache, Scan Now, Reboot Now, and Enable.

Figure 11.4 Group Vulnerability Tab

Vulnerability Analysis

This section displays the analysis results from the Discover Applicable Updates process on each computer. The analysis gives a simple top-down view of vulnerability patch status. The various statuses are detailed below.

Page Functions

- **Display and Hide** - Click the plus icon to display additional information and statistics about the represented item. Click the minus icon to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality is only available for Microsoft Internet Explorer at this time.
- **Advanced Page Search, Filtering, and View Saving** - The advanced page search, filtering dropdown menus, and saving functions appear in the Groups Vulnerability Analysis page header.
- **Search** - You may search vulnerabilities for more granular results by entering the vulnerability name (CVE; Common Vulnerabilities and Exposures) text into the Search field and clicking on the Update View button. This will return the vulnerabilities having the name of the entered text. You may then click the Save as Default View button to save your filtered view as your default view for the next time the page is visited.
- **Status** - Filter by Vulnerability Status using the dropdown menu and click on the Update View button. This will return the vulnerabilities having the selected status. You may then click the Save as Default View button to save your filtered view as your default view for the next time the page is visited.
- **Impact** - Filter by Vulnerability impact levels using the dropdown menu and click on the Update View button. This is extremely useful when you want to find or display only the Vulnerabilities that, for example, are Critical (NEW). This will return the vulnerabilities having the selected impact. You may then click the Save as Default View button to save your filtered view as your default view for the next time the page is visited.

Action Menu

- **View** - To display additional information about the vulnerability for this group computer, select a vulnerability and click on the View button. This performs the same function as clicking on the name of the vulnerability.
- **Deploy** - Deploys the selected vulnerabilities associated update packages. See Section 9; Deploying Packages: Schedule Deployment Wizard for more information.
- **Lock** - Locks vulnerabilities for this group and its computer members.
- **Unlock** - Unlocks vulnerabilities for this group and its computer members
- **Enable** - To enable selected disabled computers, click on the Enable button.
- **Disable** - To disable selected enabled computers, click on the Disable button. Disabled computers do not take up an agent license.
- **Export** - Exports the vulnerability analysis to a comma-separated value (CSV) file. The amount and order of the data is based on what the analysis view is filtered and sorted on.
- **Update Cache** - Deploys all of the Discover Applicable Updates System Task to all computers (or selected computers).
- **Scan Now** - Initializes a screen that allows you to reschedule the Discover Applicable Updates System Task deployment for immediate execution to all selected groups.

Group Vulnerability Security

The Vulnerabilities section of ZENworks Patch Management Server requires the View Vulnerabilities Page access right. If a user does not have the correct access the access denied error message is displayed.

To be able to view the detailed vulnerability analysis requires the View Vulnerability Details access right. If a user does not have the correct access, the hyperlink will not be shown and the View button is disabled.

To be able to change the filter from detected vulnerabilities to disabled or all requires the Change Vulnerability Filter access right. If a user does not have the correct access, the filter will not have any options to choose from.

To be able to view the associated distribution packages for a given vulnerability requires the View Packages access right. If a user does not have the correct access, the link on the package status image is disabled.

To be able to create a deployment based on the vulnerability analysis requires the Deploy Vulnerabilities access right. If a user does not have the correct access, the Deploy button is disabled.

To be able to enable or disable vulnerabilities from being available by the discovery and analysis process requires the Manage Vulnerabilities access right. If a user does not have the correct access, the Enable and Disable buttons are disabled.

To be able to lock or unlock the results of the selected vulnerability analysis for the group's membership requires the Manage Group Vulnerability Locks access right. If a user does not have the correct access, the Lock and Unlock buttons are disabled.

To export all of the vulnerability analyses to a comma-separated value (CSV) file requires the Export Vulnerability Data access right. If a user does not have the correct access, the Export button is disabled.

To restart the discovery and analysis process for all of the computers registered to the ZENworks Patch Management Server requires the Manage System Tasks access right. If a user does not have the correct access, the Scan Now button is disabled.

To cache the associated distribution of the selected vulnerabilities requires the Cache Packages access right. If a user does not have the correct access, the Update Cache button is disabled.

The Inventory tab requires the View Software Inventory access right. If a user does not have the correct access, the Inventory tab is disabled.

The Membership tab requires the View Computers access right. If a user does not have the correct access, the Membership tab is disabled.

The Deployments tab requires the View Deployment Status access right. If a user does not have the correct access, the Deployments tab is disabled.

Contact your Novell Administrator for more information on ZENworks Patch Management Security.

Group Inventory Summary

This view will display the software, hardware, operating systems and services that were detected on the computers in the group. When displaying the Inventory based on a single computer, the Software inventory is the initial inventory displayed. This view is the same as the Inventory Summary view with the following differences:

- Only displays the inventory based upon the member computers of the selected group.
- The Scan Now button will only reschedule the Discover Applicable Updates System Task for the selected group's membership.

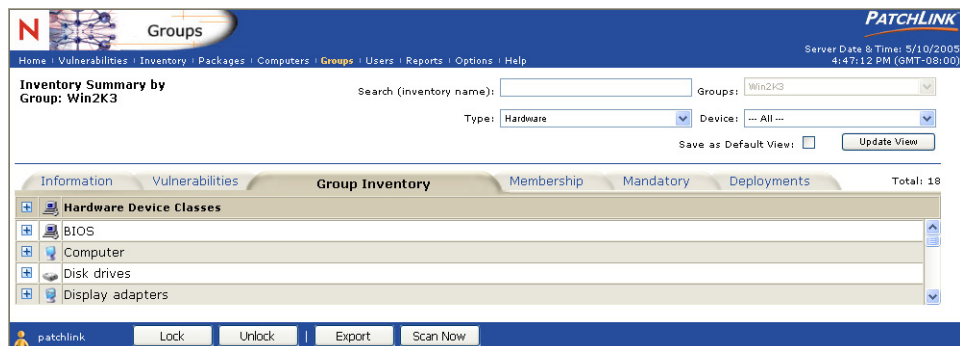


Figure 11.5 Group Inventory Tab

Software Programs

This displays the name of the software application.

Lock Status

If the software is locked for the group this image indicates if the software application is in compliance or not.

Number of Instances

The number of times this software application was detected.

Page Functions

- **Display and Hide** - Click the plus icon to display additional information and statistics about the represented item. Click the minus icon to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality is only available for Microsoft Internet Explorer at this time.
- **Advanced Page Search, Filtering, and View Saving** - The advanced page search, filtering dropdown menus, and saving functions appear in the Group Inventory page header.
- **Search** - You may search inventory for more granular results by entering the inventory name text into the Search field and clicking on the Update View button. This will return the inventory having the name of the entered text. You may then click the Save as Default View button to save your filtered view as your default view for the next time the page is visited.
- **Type** - Filter by Type using the pull down menu and click on the Update View button. This allows you to search for Operating Systems, Software, Hardware and Services.
- **Operating Systems View** - Displays the full operating system platform names and the number of instances, or times this operating system was detected.
- **Software View** - Displays the installed software applications and the number of instances, or times this **software application was detected.**
- **Software Programs** - This displays the name of the software application. Click the for a software application to display the list of computers for that application. Click on the to close this list.
- **Number of Instances** - The number of times this software application was detected.
- **Groups** - Filter by Group using the pull down menu and click on the Update View button. This allows the user to search on any user defined or server defined groups that exist.
- **Operating Systems** - Displays the selected or filtered operating system.
- **Number of Instances** - This displays the number of times this operating system platform has been detected. For displaying the Operating System Inventory for a single computer, this is always one.
- **Hardware View** - Displays the client Hardware devices.
- **Hardware Device Class** - Hardware is separated into device classes such as disk drives, processors, network adapters, etc. Click the to display the list of devices for each class, or click on the to display them all (for a long list of devices this may take a few moments to generate).
- **Device** - A device is a specific piece of hardware, such as a "Microsoft USB IntelliMouse Optical". Click the for a device to display the list of computers for that device. Click the to close this list.
- **Number of Instances** - An Instance is a specifically detected device or installed driver. A computer may contain multiple instances of a installed device or driver. For example, a computer may contain a video graphics adapter that contains multiple video sources and destinations in which each source or destination is discovered as multiple instances of the same device or driver.
- **Services View** - Displays the detected services that may or may not be running.

- **Service Name** - This displays the name of the service.
- **Number of Instances** - The number of times this service was detected.

Action Menu

- **Lock** - Clicking on the lock button will lock the selected inventory for all computers members of the group. When the inventory changes for one of the computer members the inventory item is highlighted as being out of compliance and an e-mail notification is sent to the group notification list of the occurrence.
- **Unlock** - Clicking on the unlock button will clear the lock.
- **Export** - Clicking on the Information tab will display the Group Information and Properties page.
- **Scan Now** - Initializes a screen that allows you to reschedule the Discover Applicable Updates System Task deployment for immediate execution to the selected groups.

Group Inventory Security

The Group Inventory section of ZENworks Patch Management Server requires the View Software Inventory access right. If a user does not have the correct access, the filter will not have this option available and the inventory display will default to the inventory the user has access to view or the access denied error message is displayed.

To be able to view the Operating Systems Inventory requires the View Inventory OS access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the Hardware Inventory requires the View Hardware Inventory access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the Services Inventory requires the View Services Inventory access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the list of computers on which an inventory belongs to requires the View Computers access right. If a user does not have the correct access both the hyperlink and the more information images are disabled.

To export the inventory to a comma-separated value (CSV) file requires the Export Inventory Data access right. If a user does not have the correct access, the Export button is disabled.

The Vulnerabilities tab requires the View Vulnerabilities access right. If a user does not have the correct access, the Vulnerabilities tab is disabled.

The Membership tab requires the View Computers access right. If a user does not have the correct access, the Membership tab is disabled.

The Deployments tab requires the View Deployment Status access right. If a user does not have the correct access, the Deployments tab is disabled.

Contact your Novell Administrator for more information on ZENworks Patch Management Security.

Group Membership

The Group Membership section of ZENworks Patch Management Server displays all computers which are members of the group. Clicking on a computer name will allow you to display a computer's specific information.



Figure 11.6 Group Membership Tab



Note: This view is almost identical to the computers section of ZENworks Patch Management Server.

- **Computer Name** - This displays the name of the computer. Click on the computer name to display specific information about the computer.
- **Status** - This displays the status of the computer.
- **Platform** - This displays the operating system platform the computer is running.
- **OS Info** - This displays additional information about the operating system the computer is running.
- **Version** - This displays the version of the agent running on the computer.

- **Group List** - This displays the list of groups that the computer is a member of.



Note: Refer to [Appendix B, “ZENworks Patch Management Server Reference”](#) for a complete listing and definition of all available computer status icons

Page Functions

- **Advanced Page Search, Filtering, and View Saving** - The advanced page search, filtering dropdown menus, and saving functions appear in the Computers page header.
- **Search** - You may search computers for more granular results by entering the computer name text into the Search field and clicking on the Update View button. This will return the computer having the name of the entered text. You may then click the Save as Default View button to save your filtered view as your default view for the next time the page is visited.
- **Status** - Filter by status using the dropdown menu and click on the Update View button. This allows the user to search on enabled, sleeping, offline, and disabled systems that exist.
- **Groups** - Filter by group using the dropdown menu and click on the Update View button. This allows the user to search on any user defined or server defined groups that exist.

Action Menu

- **Install** - Click on the Install button to display the list of agent installers that can be used to register computers to ZENworks Patch Management Server. The agent installer screen contains links to all of the agent installations and additional information on Operating Systems, Requirements, and Installation Notes.
- **Manage** - Manages the group's computer membership. Initializes the Group Property page.
- **View** - To display additional information about the computer, select a computer and click on the View button. This performs the same function as clicking on the name of the computer.
- **Enable** - To enable selected disabled computers, click on the Enable button.
- **Deploy** - To deploy a package to specified computers within the computer membership, simply click the Deploy button, select the package, the computers, and the deployment options.
- **Disable** - To disable selected enabled computers, click on the Disable button. Disabled computers do not take up an agent license.
- **Export** - Exports the group membership information to a comma-separated value (CSV) file.
- **Scan Now** - Initializes a screen that allows you to reschedule the Discover Applicable Updates System Task deployment for immediate execution to the selected group.

Group Membership Security

The Group Membership section of ZENworks Patch Management Server requires the View Group Membership access right. If a user does not have the correct access, the filter will not have this option available and the inventory display will default to the inventory the user has access to view or the access denied error message is displayed.

To be able to view the Enabled Group Membership requires the View Enabled Group Membership access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the Disabled Group Membership requires the View Disabled Group Membership access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the All Group Membership requires the View All Group Membership access right. If a user does not have the correct access, the filter will not have this option available.

To be able to utilize the Scan Now capability requires the Scan Now access right.

To be able to install, manage, view, deploy or disable group memberships requires the Manage Group Membership access right. If a user does not have the correct access, the Install, Manage, View, Deploy and Disable buttons are disabled.

To export the inventory to a comma-separated value (CSV) file requires the Export Group Membership Data access right. If a user does not have the correct access, the Export button is disabled.

Contact your Novell Administrator for more information on ZENworks Patch Management Security.

Group Deployments

This view displays the deployments that the selected group has been assigned to.

</

Figure 11.7 Group Deployments Tab



Note: This view does not display the individual deployments each member has been assigned to, only the deployments that the group, as an entity, have been assigned to.

This view is the same as the Deployment Summary view, but displays all deployments that the selected group has been assigned to.

Page Functions

Action Menu

- **Abort** - Allows the user to abort the deployment for the group.
- **Enable** - Allows the user to enable the selected disabled deployments.
- **Change** - Allows the user to change the selected deployment.
- **Remove** - Allows the user to change the selected disabled deployment(s).
- **Disable** - Allows the user to disable the selected deployments.
- **Export** - Exports the group deployment(s) information to a comma-separated value (CSV) file.

Group Deployments Security

To be able to change, disable, enable, abort or remove a deployment(s) requires the Manage Deployments access right. If a user does not have the correct access, the Change, Disable, Enable, Abort and Remove buttons are disabled.

To export the inventory to a comma-separated value (CSV) file requires the Export Group Membership Data access right. If a user does not have the correct access, the Export button is disabled.

Contact your Novell Administrator for more information on ZENworks Patch Management Security

12 Working With Groups

Add a Group Wizard

ZENworks Patch Management Server has the ability to add groups. From the Groups homepage, click on the Add button on the Action Menu.

Group Property Screen - Info

The Group Information Screen section of ZENworks Patch Management Server allows the Novell User the ability to create a group, System-defined groups cannot be changed. The Group Information tab of the property page contains the base information and it is this tab in which a group's information is loaded and saved.

Add a Group

Group Information Members Mandatory

Enter the Group Information:

* Name:

Description:

Agent Policy Set: No Policy

☐ itdirector@novell.com

☐ patch_admin@novell.com

E-Mail:

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

* indicates a required field.

Reset OK Cancel

Figure 12.1 Add a Group

- **Group Name** - The name of the group to be created. This field is required for groups to be created.
- **Description** - Notes or information describing the group.
- **Agent Policy Set** - The desired Agent Policy Set to use for the computers who are members of the group. When a computer's policies are calculated, ZENworks Patch Management Server determines the superset of all Agent Policy Sets for the groups the computer is a member of. Thus, if one policy set says the agent has a 60 minute interval and another says the computer has a 30 minute interval, the resulting policy set is 30 minutes. Set the Agent Policy Set to the Empty Policy if this group is to have to effect on the policy calculations.
- **E-Mail** - Select any users who have been added to the E-Mail Notification list on ZENworks Patch Management Server The selected users will be sent group-based notifications.
- **Number of Computer Members** - The total number of computers that are in the selected group.
- **Number of Computers assigned to the Mandatory Baseline** - The total number of computers who are currently assigned to the group.

Screen Functions

- **Reset** - Resets the page back to its initial state.
- **OK** - Initiates the process to save the group. If an error occurs during the save process the window will display the error. If no errors occur then the window will be closed.
- **Cancel** - Cancels the add process and closes the group property page window.

Group Property Screen - Members

The Computer Members Group Property Page section of ZENworks Patch Management Server allows the Novell User the ability to create a group. System-defined groups cannot be changed. The Computer Members tab of the property page contains a list of all computers which have been assigned as members of the group and the list of computers which are not a member of the group.

Select Member Computers

Information **Computer Members** Mandatory

Selected Computers:

Operating System	Computer Name	DNS Name	Total
Win2K3	\\TECHPUBS-PLUS	TechPubs-PLUS	1

Assign All Assign Remove Remove All

Computers:

Operating System	Computer Name	DNS Name	Total
WinXP	\\TECHPUBS-XP02	TechPubs-XP02	2
WinXP	\\TECHPUBSXP03	TechPubsXP03	



Reset OK Cancel

Figure 12.2 Select Group Members

Selected Computers

- **Operating System** - The operating system platform name. Click the to display the list of computers for that operating system. Click to close the list.
- **Computer Name** - The name of the computer.
- **DNS Name** - The DNS name assigned to the computer
- **Total Selected per OS** - The total number of computers that have been selected for the operating system platform.

Available Computers

- **Operating System** - The operating system platform name. Click the  to display the list of computers for that operating system. Click  to close the list.
- **Computer Name** - The name of the computer.
- **DNS Name** - The DNS name assigned to the computer
- **Total Selected per OS** - The total number of computers that have not been selected for the operating system platform.

Screen Functions

- **Assign All** - Assigns all available computers to the group.
- **Assign** - Assigns all available computers to the group.
- **Remove** - Removes the selected computers from the group.
- **Remove All** - Removes all selected computers from the group.
- **Reset** - Resets the page back to its initial state.
- **OK** - Initiates the process to save the group (or the group's changes). If an error occurs during the save process the window will display the error. If no errors occur then the window will be closed.
- **Cancel** - Cancels the add process and closes the group property page window.

Group Property Screen -Mandatory Baseline

The Group Property Page section of ZENworks Patch Management Server allows the Novell User the ability to create a group, system-defined groups cannot be changed. The Mandatory Baseline tab of the property page contains the lists of selected and available Vulnerabilities and Locally-created Distribution Packages for the group's baseline.

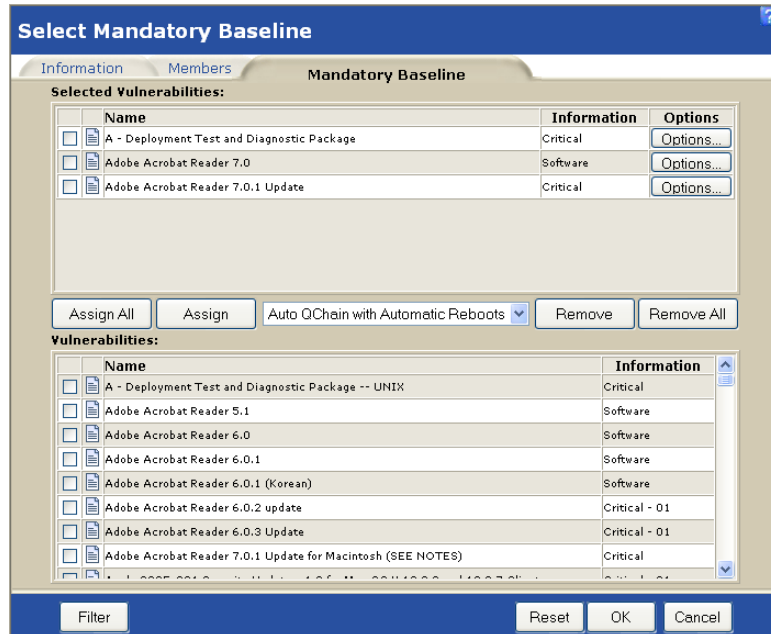


Figure 12.3 Select Mandatory Baseline

Selected Baseline Items

- **Baseline Item Name** - The name of the vulnerability or package.
- **Baseline Item Type** - This is either a Vulnerability or a Distribution Package.
- **Information** - This contains information about the operating systems for the package or the impact for a vulnerability.
- **Options** - Click the Options button to display a screen with the deployment options and information about the item.

- **Sequential** (default) indicates that only N (defaulted to 25) number of computers may perform this deployment at any given moment. The other computers will get the deployment, but it is on a first come first serve basis.
- **Parallel**, or all computers may receive the deployment as they connect up to ZENworks Patch Management Server to get their tasks.

Available Computers

- **Baseline Item Name** - The name of the vulnerability or package.
- **Baseline Item Type** - This is either a Vulnerability or a Distribution Package.
- **Information** - This contains information about the operating systems for the package or the impact for a vulnerability.

Screen Functions

- **Assign All** - Assigns all available computers to the group.
- **Assign** - Assigns all available computers to the group.
- **Remove** - Removes the selected computers from the group.
- **Remove All** - Removes all selected computers from the group.
- **Reset** - Resets the page back to its initial state.
- **OK** - Initiates the process to save the group (or the group's changes). If an error occurs during the save process the window will display the error. If no errors occur then the window will be closed.
- **Cancel** - Cancels the add process and closes the group property page window.
- **Options** - Displays a window with the deployment options for the item.
- **Edit** - Selecting a group and clicking on this button will bring up the Group Property screen with this group's information allowing the group to be changed.

Upon clicking the OK button of the Manual Group Creation status screen, the Groups Homepage is automatically refreshed showing the newly created computer group.

Edit a Group Wizard

ZENworks Patch Management Server has the ability to edit groups. To Edit a group, you must first create one. From the Groups homepage, select the group that you wish to edit and click on the **Edit** button on the *Action Menu*. The *Edit a Group* wizard has the same features and functionality as the *Create a Group* wizard.

Advanced Group Management

ZENworks Patch Management Server has the ability to add computers to new (or existing) groups based upon the membership of other groups or through the use of a comma-delimited list of computers.

To Create a New Group

1. Click the **Rules** button on the *Action Menu*
2. Select the **Create a New Group** option
3. Define a **Group Name** and **Description**
4. Select to either
 - a. **Import computer list from existing group** (by selecting the group name in the drop-down box) or
 - b. Type a comma separated list of computer names

Groups

Advanced Group Management

☒ Create New Group ☐ Edit Existing Custom Group

* **Group Name:** Advanced Group

Description:

Import computer list from existing group: Select a Group

\\TECHPUBS-XP02,\\TECHPUBS-XP03

Comma-delimited list of Computers to add to the group:

*NOTE: Windows computer names must start with two backslashes.
Example: \\MyWorkstation*

* Required Field

Reset OK Cancel

Figure 12.4 Advanced Group Management - Create Group

5. Click **OK**, saving the group

To Edit an Existing Custom Group

1. Click the **Rules** button on the *Action Menu*
2. Select the **Edit Existing Custom Group** option
3. Select the **Group Name** of the group to edit
4. Select to either
 - a. **Import computer list from existing group** (by selecting the group name in the drop-down box) or
 - b. Type a comma separated list of computer names

The screenshot shows the 'Groups' application window with the 'Advanced Group Management' tab selected. The 'Edit Existing Custom Group' radio button is chosen. The 'Group Name' field is set to 'Publications'. The 'Description' field is empty. The 'Import computer list from existing group' dropdown is set to 'Select a Group'. Below this, a text area contains the comma-delimited list of computers: '\\TECHPUBS-XP02,\\TECHPUBS-XP03'. To the left of this text area, there is a note: 'Comma-delimited list of Computers to add to the group: NOTE: Windows computer names must start with two backslashes. Example: \\MyWorkstation'. At the bottom left, a legend indicates '* Required Field'. At the bottom right, there are 'Reset', 'OK', and 'Cancel' buttons.

Groups

Advanced Group Management

☐ Create New Group ☒ Edit Existing Custom Group

* Group Name: Publications

Description:

Import computer list from existing group: Select a Group

\\TECHPUBS-XP02,\\TECHPUBS-XP03

Comma-delimited list of Computers to add to the group:

NOTE: Windows computer names must start with two backslashes.
Example: \\MyWorkstation

* Required Field

Reset OK Cancel

Figure 12.5 Advanced Group Management - Edit group

5. Click **OK**, saving the changes

13 Mandatory Baselines

A baseline is a set of configurations for a system that will automatically keep the system in the most secure state; meaning that all of your critical vendor released patches will be automatically applied to the system if, for whatever reason, it were to come out of 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, it is not appropriate and **strongly discouraged**, to apply mandatory baselines to your groups of mission critical servers, or desktops where unscheduled reboots would disrupt your daily operations.

When a mandatory baseline is created or modified:

- a. The ZENworks Patch Management Server will automatically schedule a DAU (Discover Applicable Update) task for all machines in that group
- b. Following the DAU task, the ZENworks Patch Management Server will determine which systems are applicable and out of compliance (based upon the baseline criteria)
- c. Then the necessary packages, as defined in the baseline, will be deployed as soon as possible for each machine



Note: When adding a server to a mandatory baseline, keep in mind that unless your *Hours of Operation* prevents patch deployment during business hours, the server may reboot during business hours. Additionally, 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.



Tip: You can research each patch before adding it to your mandatory baseline by opening the reports screen, locating the patch, and expanding the description of the patch, displaying any special notes concerning this patch.

Groups Mandatory Baseline Tab

To view the mandatory baseline for a particular group, select the **Mandatory** tab of the *Group Details* view.

Mandatory Baseline Item			* Impact	OS List
A - Deployment Test and Diagnostic Package	Critical	Win2K,Win2K3,Win95,Win98,WinMe,WinNT,WinXP		
Adobe Acrobat Reader 6.0.1	Software	Win2K,Win2K3,Win98,WinMe,WinNT,WinXP		
Adobe Acrobat Reader 6.0.3 Update	Critical - 01	Win2K,Win2K3,Win98,WinMe,WinNT,WinXP		
CA QOS0562 Alert Message Does Not Display Military Time	Critical - 01	Win2K,Win2K3,WinNT,WinXP		
CA QOS0563 Cannot Continue Scan Zip File With Password	Critical - 01	Win2K,Win2K3,WinNT,WinXP		
Exchange Server 2003 Service Pack 1	Critical - 01	Win2K,Win2K3		

Figure 13.1 Mandatory Baseline Tab

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

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

Column Descriptions

Status Columns

There are two status columns for each mandatory baseline. The first column displays the status/type of each assigned vulnerability

Table 13.1 Vulnerability Status Icons and Descriptions

Beta	New	Current	Status Description
			This is an active vulnerability
			This vulnerability has been locked and is in compliance
			This vulnerability has been locked and is out of compliance
			This vulnerability has been disabled

The second column displays the groups patch status as it relates to the mandatory baseline:

Table 13.2 Group Patch Status

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. (None of the members have errors).
	At least one member of this group is Deploying this patch. (None of the members have errors, nor are they Detecting).
	All of the members of this group are Disabled for this patch.
	All of the members of this group are either Not Applicable or In Compliance for this patch. (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.

Mandatory Baseline Item Column

Displays the name of the vulnerability (or package)

Impact Column

Displays the impact of the vulnerability (does not apply to packages)

OS List Column

Lists the operating systems which apply to this vulnerability (or package)

Manage Button

Opens the *Edit Group Wizard* to the **Mandatory Baseline** tab to allow the management of the groups baseline. Refer to [“Applying a Mandatory Baseline”](#) on page 182 for details on creating the baseline.

View Button

Opens the *Vulnerability Analysis* page for the selected vulnerability filtering to display only computers in the group. Refer to [“Vulnerability Analysis Results Page”](#) on page 180 for further details regarding the *Vulnerability Analysis* page.

Deploy Button

Deploys the selected package to the group

Export Button

Exports the group’s mandatory baseline information to a comma-separated value (CSV) file

Scan Now Button

Reschedules the *Discover Applicable Updates System Task* to deploy immediately

Update Cache Button

Requests, from the ZENworks Patch Management Subscription Server, the packages associated with the defined vulnerabilities



Note: Selecting a particular Vulnerability or package will open the [“Vulnerability Analysis Results Page”](#).

Applicable User Access Rights

The following Access Rights apply:

Table 13.3 Required Access Rights

Access Right	Applicable Functionality
View Groups	Required to access the <i>Groups</i> section
Export Group Data	Required to export the baseline information. Without this access the Export button will be disabled
Manage Groups	Required to add or remove vulnerabilities (or packages) from the baseline
Cache Packages	Required to enable the Update Cache button and functionality
Manage System Tasks	Required to enable the Scan Now button and functionality
Deploy Packages / Deploy Vulnerabilities	Required to enable the Deploy button and functionality

Vulnerability Analysis Results Page

The Vulnerability Analysis Results page displays the computers applicable to the selected Vulnerability. The computers are filtered by the status of **Patched**, **Not Patched**, **Error**, or **Detecting** and displayed in a tabular format.

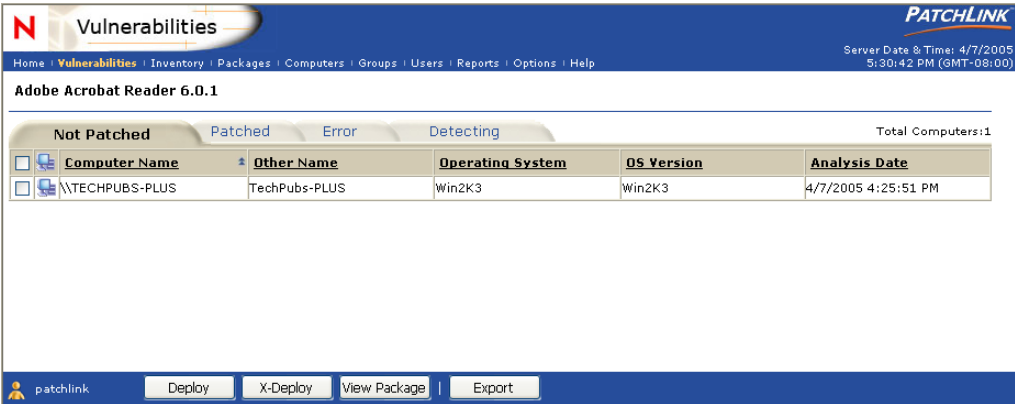


Figure 13.2 Vulnerability Analysis Results

Column Descriptions

Status Column

The status column displays the status of the applicable computer



Note: Refer to [Appendix B, “ZENworks Patch Management Server Reference”](#) for a complete listing and definition of all available computer status icons.

Computer Name

The reported computer name

Other Name

Displays the computers DNS name. If the computer does NOT have a DNS name the IP address will be displayed

Operating System

The operating system name

OS Version

Displays the operating system version data

Analysis Date

The date/time of this agent's last DAU (Discover Applicable Updates) task

Applicable User Access Rights

The following Access Rights apply:

Table 13.4 Required Access Rights

Access Right	Applicable Functionality
View Groups	Required to access the <i>Groups</i> section
Export Group Data	Required to export the baseline information. Without this access the Export button will be disabled
Manage Groups	Required to add or remove vulnerabilities (or packages) from the baseline
Cache Packages	Required to enable the Update Cache button and functionality
Manage System Tasks	Required to enable the Scan Now button and functionality
Deploy Packages / Deploy Vulnerabilities	Required to enable the Deploy button and functionality

Applying 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 computer can be a member of multiple groups, each of which could have a different mandatory baseline. To create and apply a mandatory baseline to an existing group:

1. Within your ZENworks Patch Management Server, select the **Groups** page
2. Select the name of your group
3. Select the **Mandatory** tab

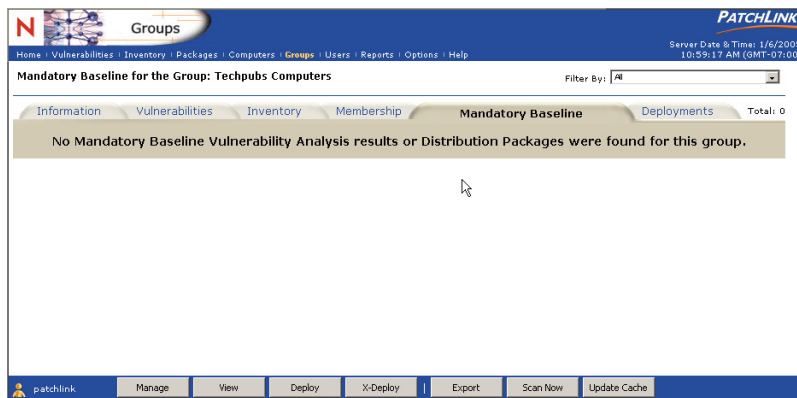


Figure 13.3 Mandatory Baseline Tab

4. Click **Manage** to open the *Select Mandatory Baseline* window

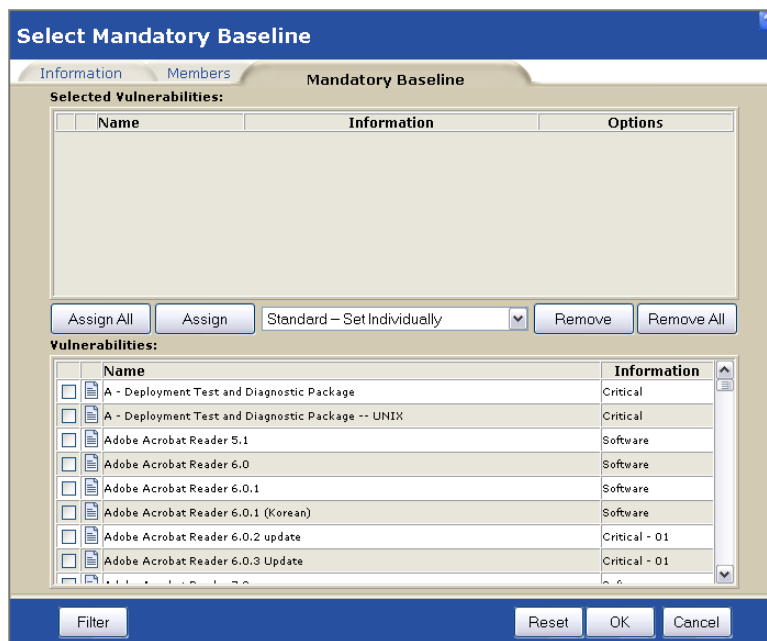


Figure 13.4 Select Mandatory Baseline

5. Select the desired vulnerabilities, using the checkboxes to the left of the vulnerability name, from the **Vulnerabilities:** section



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

6. Click **Assign** to add them to the **Selected Reports** section
 - If you would like to populate the mandatory baseline with only those patches which are applicable and not installed on one or more machines in the group:

- a. Click the **Filter** button opening a new window

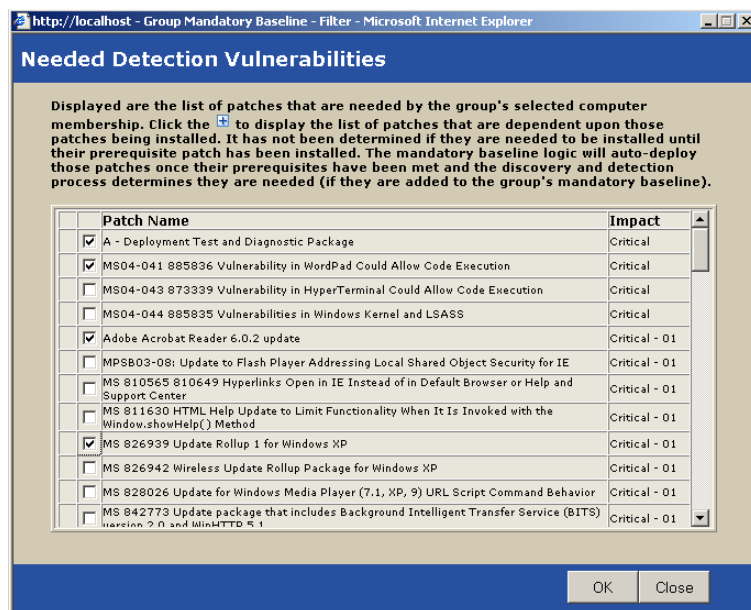


Figure 13.5 Needed Vulnerabilities



Note: If all the machines in the selected group have been fully patched, this list will be very small if not empty.

- b. Select the desired vulnerabilities, using the checkbox to the left of the vulnerability name, from this list

- c. Click **OK** to apply the selection and closing the *Needed Vulnerabilities* window

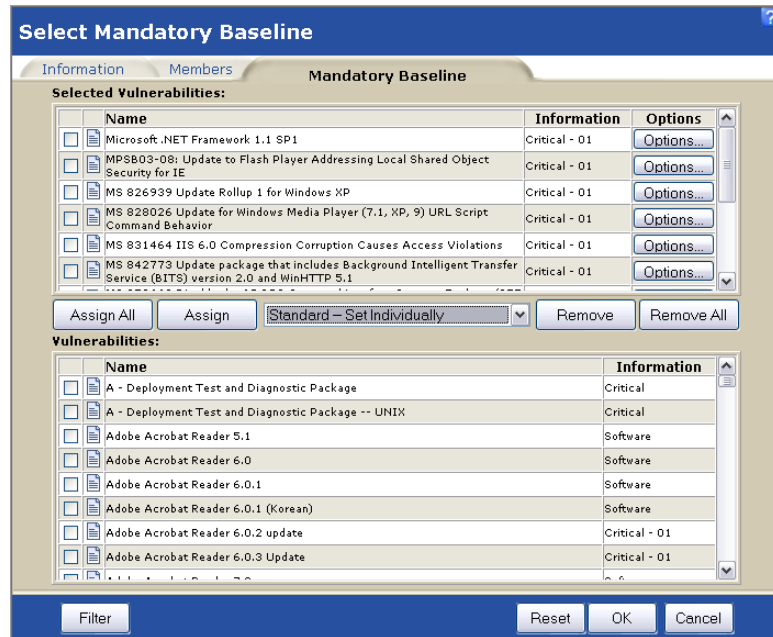


Figure 13.6 Mandatory Baseline - Selected Vulnerabilities

7. Select one of the following deployment options:

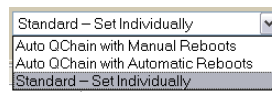


Figure 13.7 QChain Options

- **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 using one of the following methods:
 - Schedule the **Task - Reboot System** package
 - Select the Agent and click the **Reboot Now** button

- Perform a reboot outside of the PatchLink System



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 **w/o reboot** option. You should also ensure there are no patches in the baseline that require a login after patch installation.

- **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.

To Set The Vulnerability Options

- Click **Options...**, opening the *Package Deployment Options* page

Figure 13.8 Mandatory Baseline Distribution Options

- Select the desired Operating System from the **Deployment Options For:** drop-down

- c. Set the desired **Distribution Options** and **Deployment Flags**

Deployment Options

☐ Use Agent Policies
☒ Custom Behavior

☒ Do not notify users of this deployment.
☐ Notify users of this deployment.

Message: Microsoft .NET Framework 1.1 SP1

☒ Use server UTC time.

Option	Use Agent Policy	Local
Deploy within	<input type="checkbox"/>	5 Minutes
Allow user to snooze	<input type="checkbox"/>	Yes
Allow user to cancel	<input type="checkbox"/>	No

Figure 13.9 Mandatory Baseline Deployment Options

- d. Set the desired **Deployment Options**

Reboot Options

☐ Use Agent Policies
☒ Custom Behavior

☐ Do not notify users of this reboot.
☒ Notify users of this reboot.

Message: Microsoft .NET Framework 1.1 SP1 requires a reboot to complete

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

Reset OK Close

Figure 13.10 Mandatory Baseline Reboot Options

- e. Set the desired **Reboot Options**

- 188

Removing Deployments Created By Mandatory Baselines

If you wish to stop a patch that has been initiated by a mandatory baseline, after opening the **Deployments** tab for each package associated with the mandatory baseline:



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

1. Within your ZENworks Patch Management Server, select the **Groups** page
2. Select the name of your group
3. Select the **Group Deployments** tab

Name	Initial Start Date	Progress
Deployment of Adobe Acrobat Reader 6.0.2 update	1/6/2005 6:27:31 PM (UTC)	0%
Deployment of MS04-041, 885936 (2K3) Vulnerability in WordPad Could Allow Code Execution	1/6/2005 6:27:06 PM (UTC)	0%
Deployment of Deployment Test and Diagnostic Package -- Windows	1/6/2005 6:25:00 PM (UTC)	0%
Deployment of MS04-040, 889293 Cumulative Security Update for IE 6.0 SP1-a (Win95, Win98, WinME)	1/4/2005 5:50:00 PM (Local)	0%
Deployment of MS04-040, 889293 (NT) Cumulative Security Update for IE 6.0 SP1-a (WinNT)	1/4/2005 5:50:00 PM (Local)	0%
Deployment of MS04-040, 889293 Cumulative Security Update for IE 6.0 SP1-a (Win2K, WinXP)	1/4/2005 5:50:00 PM (Local)	100%

Figure 13.11

If you wish to stop all scheduled deployments associated with the package:

4. Select the checkbox associated with the deployment(s) you wish to stop
5. Click **Remove**

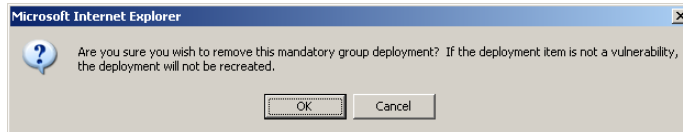


Figure 13.12

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

If you wish to stop the deployment for only specific computers:

- Click the appropriate **Name** link, opening the **Deployment Details** page

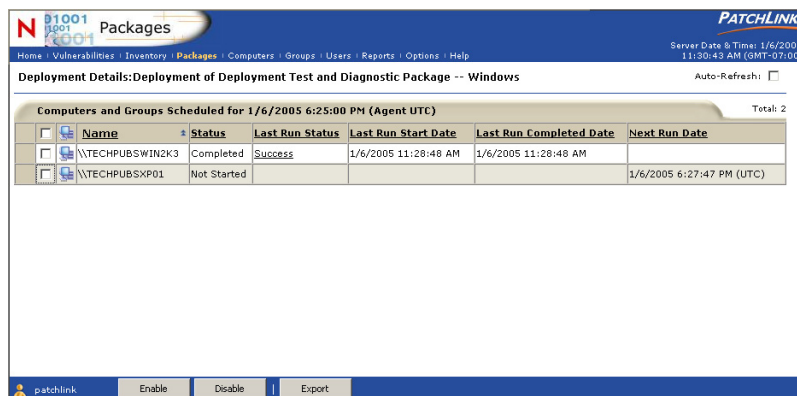


Figure 13.13

- Select the computer(s) for which you wish to stop the deployment

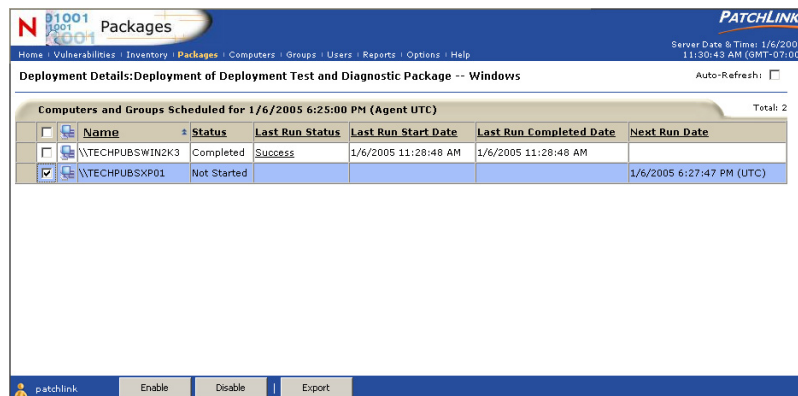


Figure 13.14

- Click **Disable** to disable the deployment for the selected computer

14 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.

[“About Reports”](#) on page 193

[“Using the Workspace”](#) on page 203

[“Creating Reports”](#) on page 206

[“Troubleshooting”](#) on page 209

About Reports

Reports cover a broad range of key indicators and can be customized to cover a general category (computers, 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.

Reports are presented within the ASP.NET Web site with each report type associated with a particular ID. The following are the report related Web pages in the application:

- **Available Reports Page** - select from the available reports.
- **Report Parameters Page** - the ID number represents the ID assigned to the report type. This page is where you define the report content.
- **Reports Page** - the ID number represents the ID assigned to the report type. This page is where the report output is presented.

Access Levels

Access to reports is limited to user roles that have the following access rights assigned; Manage User-Based Reports, Manage Administrative Reports.

- **Manage User-Based Reports** - can run reports only for those computers and groups specifically assigned to the user in the user roles section. This is a default access right in the Administrator, Manager, and Operator role templates.
- **Manage Administrative Reports** - can run reports for all computers and groups on the network, regardless of user role or computer/group assignments. This is a default access right in the Administrator role template.



Note: If a user is not assigned one of these access rights, the Reports option in the toolbar is turned off (disabled) and the application returns an *access denied* error message if an attempt to access the *Reports* page is made by entering the URL directly.

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 computer, package or other means, including date.

The following parameters are available across all reports. Note that not all parameters are available for each report.

Computers

Select **Computers** to choose from a list of all available computers registered by the ZENworks Patch Management Agent. All available computers are shown in the *Available Data* list. Click a single computer or use the CTRL and SHIFT keys to select multiple computers.

Groups

Select **Groups** to choose from a list of all available groups created in ZENworks Patch Management Server. All groups are shown in the *Available Data* list and any computers belonging to the selected group are included in the report. Click a single group or use the CTRL and SHIFT 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 *Available Data* list. Click a single deployment or use the CTRL and SHIFT keys to select multiple deployments.

Packages

Allows the user to select from a list of all available packages.

Select **Packages** to choose from a list of all available packages. All available packages are shown in the *Available Data* list. Click a package name or use the CTRL and SHIFT keys to select multiple packages.

Vulnerabilities

Select **Vulnerabilities** to choose from a list of all available vulnerabilities identified by ZENworks Patch Management Server. All vulnerabilities are shown in the *Available Data* list. Click a vulnerability name or use the CTRL and SHIFT 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 PLUS local time or UTC time.

Report Types

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
- Computer Duplicate Report
- Computer Status Report
- Deployment Detail Report
- Deployment Summary Report
- Mandatory Baseline Detail Report
- Mandatory Baseline Summary Report
- Package Compliance Detail Report
- Package Compliance Summary Report
- Vulnerability Analysis Report

Agent Policy Report

Available Parameters: Computer, Group

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

In the report, each policy value is listed in the *Policy Name* column. A single computer 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:

- Computer Name
- Policy Name
- Current Value
- Policy Description

Computer Duplicate Report

Available Parameters: Date Range

The Computer Duplicate Report returns a list of computers 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 ZENworks 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

Computer Status Report

Available Parameters: Computer, Group

The Computer Status Report returns the current state of remediation for a specified computer, list of computers, computers in a group, or computers in a list of groups.

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

- Computer Name
- DNS Name - Domain Name Server name
- IP Address - Internet Protocol address
- Operating System Name
- OS Build No.
- Service Pack
- Agent Version
- Last Contact Date
- Patchable Status - refers to the reboot status of the agent.
 - Clean - the agent is ready to receive a patch.
 - Dirty - the agent requires a reboot before receiving the next patch.
 - Q-Chain - the agent is waiting for a Q-chain deployment.
- Group List - A delimited list of groups the agent belongs to.

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 computer 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
- Computer Name
- Deployment Status
- Deployment Date
- Install Date
- Vulnerability Status
- Date Last Verified

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

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 computer 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

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

Mandatory Baseline Detail Report

Available Parameters: Computers, Groups

The Mandatory Baseline Detail Report provides information about a selected list of computers and the status of the mandatory baseline package and deployment status associated with each computer.

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

- Computer 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: Computers, 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 computer 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: Computers, Groups, Packages

The Package Compliance Detail Report provides information about patch and deployment status for a specific package and computer. The report identifies the compliance status for the any of the specified packages, or for any package deployed to a specified computer or group.

The report lists each package associated with one of the selected computer(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 computer.

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 computer, status, and deployment details. The values included in the report are defined as follows:

- Package Name
- Computer Name
- Vulnerability Status
- Data Last Verified
- Deployment Name
- Deployment Status
- Package Release Date

- Date Deployed
- Date Installed
- Date Scheduled

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

Package Compliance Summary Report

Available Parameters: Computers, 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 computer. The report lists each package that impacts one of the selected computer(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 computers 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 Computers - Count of computers applicable to the selected report criteria.
- Applicable Computers - Count of computers applicable to the vulnerability.
- Computers Detecting - Count of computers applicable to the vulnerability.
- Computers Patched - Count of computers applicable to the vulnerability.
- Not Patched/Not Scheduled- Count of computers applicable to the vulnerability.
- Not Patched/Scheduled- Count of computers applicable to the vulnerability.
- Deployments Completed -
- Deployments Failed -
- Deployments In-Progress - Count of computers applicable to the vulnerability.

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

Vulnerability Analysis Report

Available Parameters: Computers, 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 computer(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 computers 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 Computers - Count of computers applicable to the selected report criteria.
- Applicable Computers - Count of computers applicable to the vulnerability.
- Computers Detecting - Count of computers applicable to the vulnerability.
- Computers Patched - Count of computers applicable to the vulnerability.
- Not Patched - Count of computers applicable to the vulnerability.
- Pct Patched - Count of computers applicable to the vulnerability.

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

Using the Workspace

The Reports link in the main menu launches the *Reporting* page, which contains a list of all available reports.



Figure 14.1

Reporting Page

Click on the expand/collapse box next to each report to see a general description of the data each report handles. Click on the report name to define and create the report. For a detailed description of each report type, see “[Report Types](#)” on page 196.

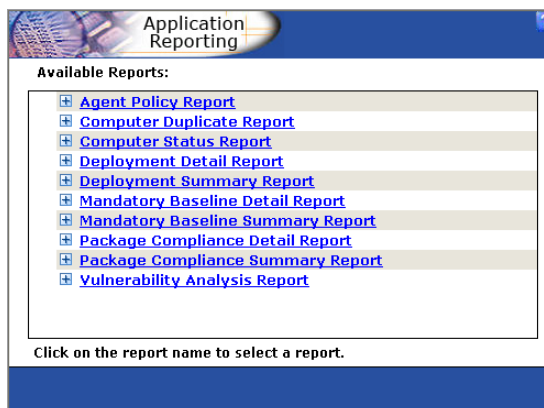


Figure 14.2 Reporting Page

Report Parameters Page

Once you determine the report type you want to create, you then define how you want to organize and present the data in the report. This is done in the *Report Parameters* page. Once you have defined the report, create the report by clicking **Generate**.

Defining report parameters allows you more quickly and easily define the specific information you want included in the report. For a detailed explanation of report parameters, see [“Report Parameters”](#) on page 194.

In this example, the report is presenting information based on Groups. Using the Search feature, the target groups could be more narrowly defined.

The screenshot shows the 'Application Reporting' interface for 'Package Compliance Summary Report Parameters'. On the left, a 'Parameters' sidebar lists 'Packages', 'Computers', and 'Groups' (which is selected). The main area features a 'Search:' input field with an 'Update List' button. Below this is a list of 'Available Groups' with a 'Total Available: 16' count. The list includes: AIX, Building #44123, HP-UX, Linux, Mac OS X, Publications, and Servers. Navigation arrows are present below the list. At the bottom of the main area is a 'Selected Groups' section with a 'Total Selected: 0' count and an empty list. A footer note states: '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.' A 'Generate' button is located at the bottom right.

Parameters
Packages
Computers
Groups

Search:

Available Groups	Total Available: 16
AIX	
Building #44123	
HP-UX	
Linux	
Mac OS X	
Publications	
Servers	

Selected Groups Total Selected: 0

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 14.3 Report Parameters Page

Displaying Time and Date

For reports that generate date range data, you have two options for display date/time information;

- Use the ZENworks Patch Management Server date (this is the time and date established by the ZENworks Patch Management Server (usually local time).
- Use Coordinated Universal Time (UTC)



Note: Coordinated Universal Time or UTC, also referred to as Universal Time, Zulu time or Greenwich Mean Time (GMT).

Report Page

Each report is presented in a tabular format with the first column representing the subject, or focus, of the report. Reports can be sorted by the data in any column by clicking the column header. Doing this, the sort order for the column switches between ascending and descending order.

Application Reporting

Package Compliance Summary Report Report created: 5/6/2005 11:43:28 AM

Package Name	Total Computers	Applicable Computers	Computers Detecting	Computers Patched	Not Patched / Not Scheduled	Not Patched / Scheduled	Deployments Completed	Deployments Failed	Deployments In-Progress
MS05-002 891711 (2K3) Vulnerability in Cursor and Icon Format Handling Could Allow Remote Code Execution	3	1	0	1	0	0	4	0	0
MS05-015 888113 (2K3) Remote Code Execution Vulnerability in Hyperlink Object Library	3	1	0	1	0	0	4	0	0
MS05-016 893086 (2K3) Vulnerability in Windows Shell that Could Allow Remote Code Execution	3	1	0	1	0	0	4	0	0
MS05-018 890859 (2K3) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege and Denial of Service	3	1	0	1	0	0	4	0	0
MS05-019 893066 (2K3) Vulnerabilities in TCP/IP Could Allow Remote Code Execution and Denial of Service	3	1	0	1	0	0	4	0	0

Display 100 Results per page

Export Comma Separated Values (CSV) View Printable Close

Figure 14.4 Report Page

Creating Reports

To create a report, click **Report** in the ZENworks Patch Management Server main menu. The Reports link in the main menu opens the *Available Reports* page, where you can select the type of report you want to create. Select a report type by clicking on the Report name. This opens the *Report Parameters* page where you will define and generate your report.

To Create a Report

1. Click Report in the main menu.
2. Select the report to generate in the *Available Reports* page.
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 (Computers, 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.

Available and Selected Options

Report parameters are defined by selecting an option in the parameters list then narrowing the report data using the *Available Options* box in the *Report Parameters* page. Here, you select the parameter to use in presenting information. Then you can further define the report by selecting components to either include or exclude from the report in the *Available Options* box. Another way to select the precise components to include in the report is to use the *Search* feature to identity specific components.

Use the Arrow buttons to add and remove selected or all items to the *Selected Options* box. To move items into the *Selected Options* box from the *Available Options* box, highlight the items and click the **Include** button. Move all items from the *Available Options* box to the *Selected Options* box by clicking the **Include All** button.

Items can be removed from the *Selected Options* box by selecting the items to remove and clicking the **Remove button**. You can use the **Remove button** to remove one or more selected items and the **Remove All** button to remove the entire list.

You may choose not to define any parameters; in this case, all applicable data for the report type is included in the report.

Searching and Updating

The Search feature is used to expedite the selection of data or to assist in reporting on a very narrow, or specific, range of items (parameters). The search feature provides standard searching on a word matching basis (exact and partial matching). 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*.

This means that conducting a search on *Win* will produce a result set that includes *Win*, *Windows*, *WinXP*, *Windy*, et al).

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 computers, 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.

Exporting and Printing 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.

Exporting Reports

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.

To Export a Report

1. On the *Reports* page, select an available export format from the **Export** drop-down list box.
2. Click **Export**.
3. In the File Download dialog box, select from the available options (Open, Save, Cancel).
 - c. Open - creates the file and opens it in the appropriate application.
 - d. Save - creates the file and saves it to a local folder.
 - e. Cancel - does not create or save the report.

The report is created with a file name matching the report type and file extension (for example, Vulnerability Analysis Report.xml).

Printing Reports

An HTML version of the report can be quickly printed using the View Printable option. The View Printable command and drop-down list is presented at the bottom of the page.

To Print a Report

1. On the *Reports* page, click **View Printable**.
2. In your Web browser, click **Print...** (In the File menu, click **Print...**).



Note: Use the Print Preview and page Setup settings in your Web browser to better adapt the report for printing. Also, modifying the size of your browser window will alter the format of the printed report.

Troubleshooting

This section is designed to assist in using the reporting feature in the ZENworks Patch Management Server system.

Table 1:

Problem	Description
ASP error	The maximum amount of time permitted by the web browser for a script to execute was exceeded.
Reports not current	After deploying a patch, the Deployment Details page indicates the deployment was successful and the Computers page shows the target computer is Online but the Vulnerability Reports page indicates Not Patched.

Active Server Pages (ASP) Error

The maximum amount of time for a script to execute was exceeded. You can change this limit by specifying a new value for the property `Server.ScriptTimeout` or by changing the value in the IIS administration tools. This occurs when the default setting of 90 seconds set by the IIS Metabase for loading an ASP script is exceeded.

Some reports, and particularly those monitoring large networks, comprise a considerable amount of data and will exceed this load time limit. You can increase the default load time (the ASP script time out value) to permit loading.

To Adjust the Default Time-Out Value

1. Open the IIS Manager.
2. Select the PLUS Web site and right-click. In the tasks menu, click **Properties**.
3. In the PLUS Properties dialog box, click the **Home Directory** tab. Click **Configuration**.
4. In the Application Configuration dialog box, click the **Options** tab.
5. In the ASP script time-out value field, increase the value to 1800 seconds.
6. Click **OK**.
7. In the PLUS Properties dialog box, click **OK**.
8. At a command prompt, type *iisreset* to restart IIS.

Reports Do Not Reflect Recent Patch Activity

The report can provide an inaccurate reading of the patch status in the following cases:

- While a patch was successfully installed, the machine has not been rebooted (applies to patches requiring a reboot).
- The Discover Applicable Updates (DAU) System Task has not run following the patch. This means the Agent has not sent an updated status to the ZENworks Patch Management Server.
- A vulnerability scan has not been performed on the target computer since the last update.

15 Managing Users and Roles

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

[“About User Management” on page 212](#)

[“Working with Users” on page 221](#)

[“Creating New Users”](#)

[“Adding Users”](#)

[“Editing User Profiles”](#)

[“Removing ZENworks Patch Management Server Users”](#)

[“Deleting ZENworks Patch Management Server Users”](#)

[“Working with Roles” on page 230](#)

[“Creating User Roles” on page 231](#)

[“Editing User Roles”](#)

[“Assigning User Roles”](#)

[“Disabling User Roles”](#)

[“Removing User Roles”](#)

[“Exporting User Data” on page 241](#)

About User Management

The *User Management* page is available by clicking **Users** on the main toolbar.



Figure 15.1 Main Toolbar > Users

The *User Management* page allows the system administrator the ability to manage who has access to the ZENworks Patch Management Server (the users) and the role that each user plays within the system. Roles define the access rights that each user carries on the system as well as the groups and computers that the user has control over.

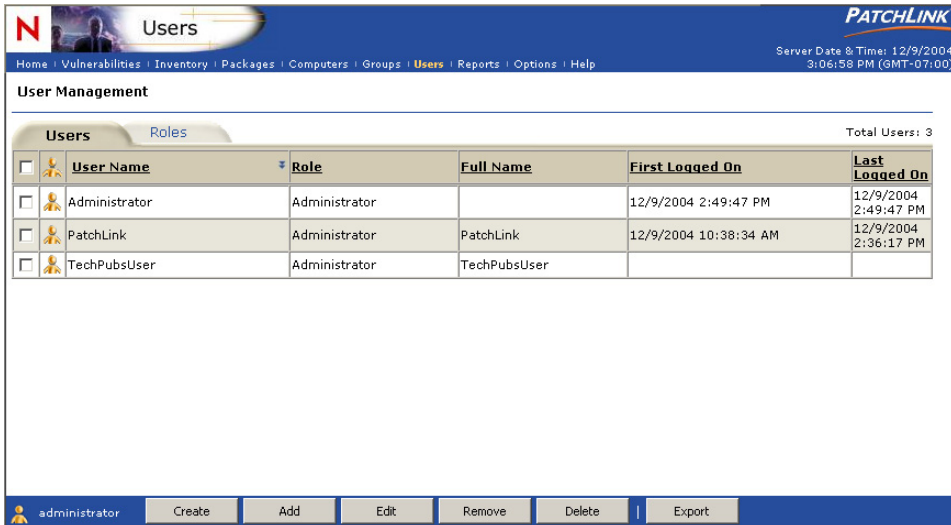


Figure 15.2 User Management View

Access Levels

Access to user management options is limited to user roles that have the following access rights assigned; View Users, Export User Data, and Manage Users. Commands are disabled in the interface depending on the access right assigned to the user. See [Chapter 15, “Managing Users and Roles”](#) for more information about user roles and access rights.

- **View Users** — Can access and view the Users and Roles tabs in the *Users* page. This is a default access right in the Administrator, Manager, Operator, and Guest role templates.
- **Export User Data** — Can export subscription data to a comma-separated value (CSV) file. This is a default access right in the Administrator and Manager role templates.
- **Manage Users** — Can access, view, create, add, edit, remove, and delete user and role definitions. This is a default access right in the Administrator role template only.

Users

Users are defined as individual computers users (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 a ZENworks Patch Management Server User

Creating a user allows you to create a new local machine user and provide them with access to PLUS. The end result is that the new user is added as a Windows user, added to the PLUS database, and added to the ZENworks Patch Management Server Access Group. Using this method, ZENworks Patch Management Server not only adds the user to the ZENworks Patch Management Server system but also updates (through a Windows API) 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 Server. Using this method, ZENworks Patch Management Server generates a list of Windows users and allow you to select a user from that list to be added to the ZENworks Patch Management Server 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.

Roles

The ZENworks Patch Management Server system permits two types of roles: system and custom. System roles are default 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 groups and computers by default. Custom roles allow you to define any combination of access rights and selected machines or groups of machines for a particular user.



Note: See “[Access Rights](#)” on page 216 for detailed description of the available access rights for each role.

Roles are defined by a combination of three attributes; access rights, groups and computers. Access rights define the application pages and functionality available to the user. Computers and groups define the specific machines or group of machines that the user is permitted to act upon. As such, computer and group rights are secondary to access rights. This means that the user is allowed to apply their assigned access rights to the computers and groups assigned to a role.

Predefined System Roles

The predefined system roles are provided to assist you in defining the roles that newly created users should inherit. The ZENworks 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: All groups and computers are added to these user roles when they are created or registered.

There are four system roles: Administrator, Manager, Operator and Guest.

Administrator

Any user who is assigned this role is considered a PatchLink Super-User and is permitted full access to all areas and functionality of the product. Users of this role are the only users who can delegate newly installed computers to other user roles. The administrator role includes all 55 available access rights. Administrators can view *all* computers/groups and perform any function within the ZENworks Patch Management Server (ZENworks Patch Management Server) environment. There must be at least one user assigned the administrator user role.

Manager

Users assigned this role can manage every section of the ZENworks Patch Management Server system with the exception of *Advanced Configuration Options* and *User Management* options. The role includes 50 of the 55 available access rights. Managers can view *only* defined computers/groups.

Operator

This user role is permitted to perform all routine operations (deploy, detect, export). The role is granted 33 of the 55 available access rights. Operators can view only defined computers/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 grants 22 of the 55 available access rights, allowing view-only access for defined computers/groups.

Custom Roles

Custom roles are created by the ZENworks Patch Management Server administrator. Custom roles are created based on one of the predefined roles. In this sense, custom roles use a predefined role as a template for a custom role.

Unlike system roles which cannot be disabled, you can disable a custom role at any time. Disabled custom roles removes the role from the system and effectively removes the role from the database. Any users assigned this role are maintained and their role is changed to the system role that served as the template for the disabled custom role when it was created.

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 ZENworks Patch Management Server environment, access rights pertaining to the installed module are added by the system to the access rights list.

The following table identifies the entire set of predefined access rights, describes the functionality of each, and illustrates the predefined system role assigned to each access right.

Table 15.1 User Role Access Rights

Access Right Name	Description	Administrator	Manager	Operator	Guest
Cache Packages	Permits caching (or re-cache) of distribution packages from the subscription agent (PLHOST).	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	

Table 15.1 User Role Access Rights

Access Right Name	Description	Administrator	Manager	Operator	Guest
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	
Manage Groups	Conduct group administration tasks.	X	X		
View Home Page	Access the <i>Home</i> page.	X	X	X	X
View PLUS Status	Display the current PLUS 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		

Table 15.1 User Role Access Rights

Access Right Name	Description	Administrator	Manager	Operator	Guest
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
Export Agent Policies Sets Data	Save agent policy data to CSV file format.	X	X		
View Options: Defaults	Access <i>Options > PLUS 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 Options > Subscription Information 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 Reboot Now 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	

Table 15.1 User Role Access Rights

Access Right Name	Description	Administrator	Manager	Operator	Guest
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	
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 PLUS 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			

Accessible Groups

Accessible groups are those groups of computers that you associate 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 ZENworks Patch Management Server system is available to users if they have the appropriate role-based access rights.



Note: The accessible computers 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 access rights to manage deployments can be limited to managing deployments only for a select group(s).

The accessible groups option is available in the Add/Edit Role Wizard.

- **Selected Groups** — Lists the groups of computers assigned to the role.
- **Groups** — Lists the available groups of computers that can be assigned to the role.

Accessible Computers

Accessible computers are those individual computers that you associate with a particular role. This option works in the same manner as the *accessible groups* option works by allowing you to achieve a level of granularity in the assignment of roles to system users.

The accessible computers option allows you to limit the control that a user is permitted to specified computers. For example, a user assigned access rights to manage computers can be limited to managing only a single computer using this option.



Note: The accessible computers option is disabled when working with a predefined system role.

The accessible computers option is available in the Add/Edit Role Wizard.

- **Selected Computers** — Lists the computers assigned to the role.

- **Computers** — Lists the available computers that can be assigned to the role.

Working with Users

This section describes the user-based tasks available from the *User Management* page.

[“Creating New Users”](#) on page 221

[“Adding Users”](#) on page 223

[“Editing User Profiles”](#) on page 226

[“Removing ZENworks Patch Management Server Users”](#) on page 228

[“Deleting ZENworks Patch Management Server Users”](#) on page 229

Creating New Users

Creating a user adds the user to 1) the local machine and, 2) the PLUS database and access group. The end result is that the new user is added to Windows and PLUS. See [“Users”](#) on page 213 for more information.

To create a new ZENworks Patch Management user:

1. In the ZENworks Patch Management Server main menu, click **Users**.
2. In the *User Management* page, click **Create**.

Figure 15.3 Create a User Wizard

3. In the Create a User dialog box, click **Next**.

- Select the **skip** option to hide this page in the future.
4. In the *User Information* page, enter the user credentials, contact information and assign a role to the new user.

http://localhost - Create a User - Microsoft Internet Explorer

Create a User

User Information:

User Name: TechPubsOperator

Password:

Confirm Password:

Password Reminder: Password Reminder

Full Name: TechPubs Operator

Office phone: 800.858.4000

Cell phone:

Pager:

Email: techpubs@novell.com

Description: Operator Login for TechPubs

Role: Operator

< Back Next > Cancel

Figure 15.4



Note: User Name, Password, Confirm Password and Role are required fields. Contact information is not validated and there are no formatting rules other than max. characters (25).

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.

5. Click **Next**. A new user summary is shown.
6. Confirm the user information and click **Finish**.
7. Verify the status information and click **Close**.

Adding Users

Adding a user adds a user to the PLUS database and access group from a list of existing Windows users. See “Users” on page 213 for more information.

To add a new ZENworks Patch Management user:

1. In the ZENworks Patch Management Server main menu, click **Users**.
2. In the *User Management* page, click **Add**.

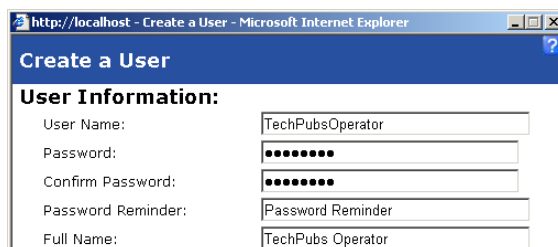
The image shows a screenshot of a web browser window titled "http://localhost - Create a User - Microsoft Internet Explorer". The page has a blue header with the text "Create a User". Below the header, there is a section titled "User Information:" followed by five input fields. The first field is "User Name:" with the text "TechPubsOperator" entered. The second field is "Password:" with a masked password of seven dots. The third field is "Confirm Password:" also with a masked password of seven dots. The fourth field is "Password Reminder:" with the text "Password Reminder" entered. The fifth field is "Full Name:" with the text "TechPubs Operator" entered.

Figure 15.5 Create a User Wizard

3. In the Add a User dialog box, click **Next**.

- Select the **skip** option to hide this page in the future.
4. In the *Add a User* page, select a user from the list of available users. You may select multiple users from this list (press **CTRL** and select).

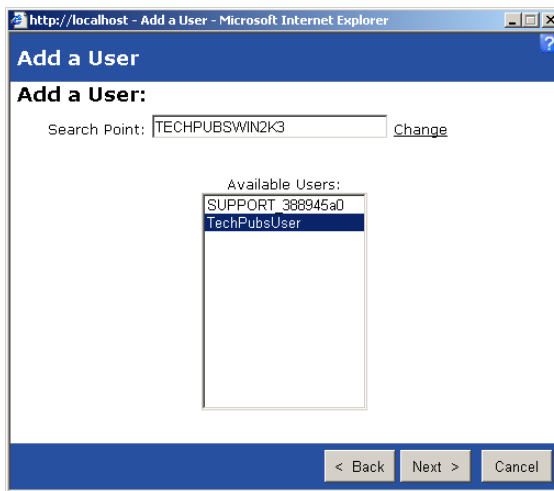


Figure 15.6



Note: The default location to search for available users is the current computer. If you wish to select a domain or other computer for user accounts, type the name of that computer in the **Search Point:** field, and click **Change**.

5. Click **Next**.
6. In the *Select a Role* page, assign each user with a particular role. You may select from the predefined system roles or any custom roles you may have added.

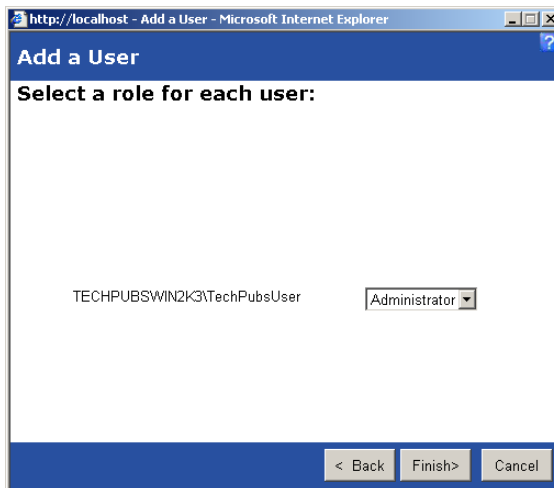


Figure 15.7

7. Click **Finish**, confirm the status information, and then click **Close**.

8. The new user is added to the list of users in the *User Management* page.

<input type="checkbox"/>	User Name	Role	Full Name	First Logged On	Last Logged On
<input type="checkbox"/>	Administrator	Administrator		12/9/2004 2:49:47 PM	12/9/2004 2:49:47 PM
<input type="checkbox"/>	PatchLink	Administrator	PatchLink	12/9/2004 10:38:34 AM	12/9/2004 2:36:17 PM
<input type="checkbox"/>	TechPubsUser	Administrator	TechPubsUser		

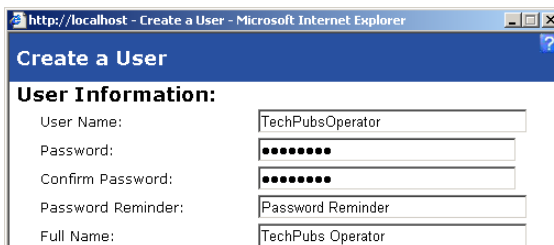
Figure 15.8

Editing User Profiles

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

To Edit user Profile Information

1. In the ZENworks Patch Management Server main menu, click **Users**.
2. In the *User Management* page, select the checkbox for the user profile to edit and click **Edit**.



The screenshot shows a web browser window titled "http://localhost - Create a User - Microsoft Internet Explorer". The page has a blue header with the text "Create a User". Below the header, the section "User Information:" is displayed. It contains five input fields with labels to their left: "User Name:" (containing "TechPubsOperator"), "Password:" (containing seven dots), "Confirm Password:" (containing seven dots), "Password Reminder:" (containing "Password Reminder"), and "Full Name:" (containing "TechPubs Operator").

Figure 15.9 Create a User Wizard

3. In the Edit a User dialog box, click **Next**.

- Select the **skip** option to hide this page in the future.
4. In the **Edit User** dialog box, make the desired modifications and click **Next**.

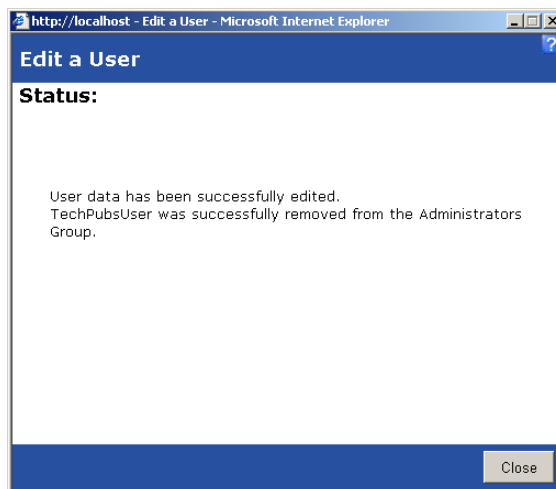


Figure 15.10

5. In the *Summary* page, click **Finish**. Click **Back** to return to editing.
6. Click **Close** to exit the *Status* page.

Removing ZENworks Patch Management Server Users

Removing a user from ZENworks Patch Management Server disables access to the ZENworks Patch Management Server without deleting the user's Windows account. Once removed, the user is deleted from the ZENworks Patch Management Server database and access 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 user's role, then remove or delete the user.

To Remove a User

1. In the ZENworks Patch Management Server main menu, click **Users**.
2. In the *User Management* page, select the checkbox for the user profile to remove and click **Remove**.
 - You may select multiple users for removal.
3. In the *Warning* dialog box, click **OK**.

Deleting ZENworks Patch Management Server Users

Deleting a user from ZENworks Patch Management Server disables access to the ZENworks Patch Management Server and removes the Windows account for that particular user. This not only prevents access to the ZENworks Patch Management Server but also removes rights to the Windows machine.

To Delete a User

1. In the ZENworks Patch Management Server main menu, click **Users**.
2. In the *User Management* page, select the checkbox for the user profile to remove and click **Delete**.
 - You may select multiple users for removal.
3. In the *Warning* dialog box, click **OK**.



Warning: Deleting a user effectively prevents not only access to ZENworks Patch Management Server, but also **deletes** the user from the *Users Tree* for that computer or Active Directory.

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

Working with Roles

This section describes the role-based tasks available from the *User Management* page.

[“Creating User Roles” on page 231](#)

[“Adding Users” on page 223](#)

[“Editing User Profiles” on page 226](#)

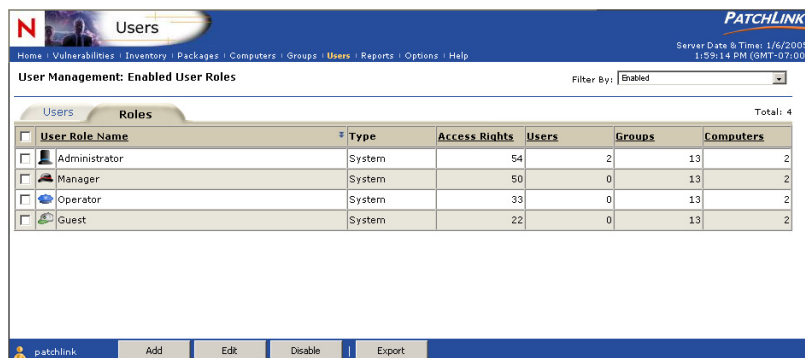
[“Removing ZENworks Patch Management Server Users” on page 228](#)

[“Deleting ZENworks Patch Management Server Users” on page 229](#)

Creating User Roles

To create a User Role:

1. Within your ZENworks Patch Management Server, select the **Users** page
2. Select the **Roles** tab



Users

Home | Vulnerabilities | Inventory | Packages | Computers | Groups | **Users** | Reports | Options | Help

Server Date & Time: 1/6/2005 1:59:14 PM (GMT-07:00)

User Management: Enabled User Roles Filter By: Enabled

Users Roles Total: 4

<input type="checkbox"/>	User Role Name	Type	Access Rights	Users	Groups	Computers
<input type="checkbox"/>	Administrator	System	54	2	13	2
<input type="checkbox"/>	Manager	System	50	0	13	2
<input type="checkbox"/>	Operator	System	33	0	13	2
<input type="checkbox"/>	Guest	System	22	0	13	2

patchlink Add Edit Disable Export

Figure 15.11

3. Click **Add**

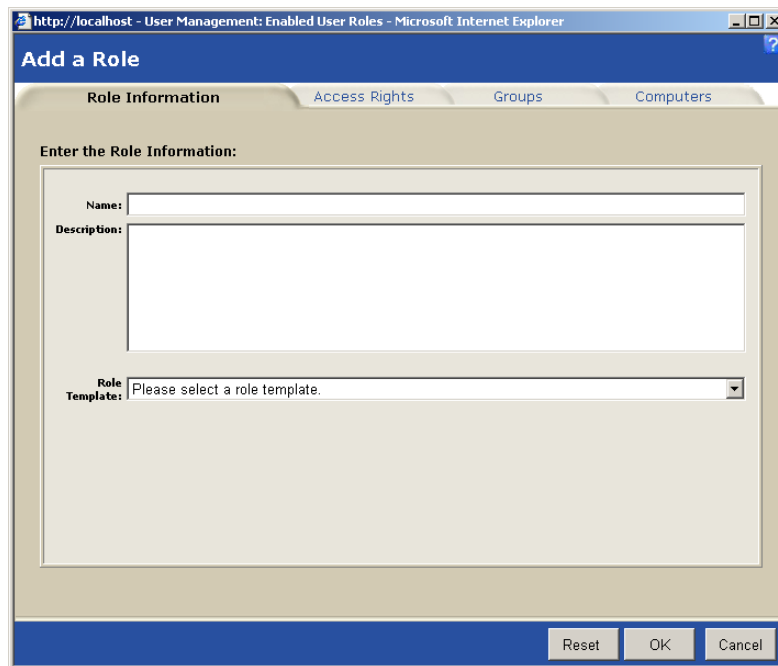


Figure 15.12



Note: If you are editing an existing role: Select the desired role, using the checkbox to the left of the **User Role Name**, and click **Edit**

4. 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)



Note: The **Role Template:** selected, will determine what access rights your role will start with. You can add or remove any access right regardless of which role was selected as the template.

5. Select the **Access Rights** tab, to define which rights the users assigned this role will have

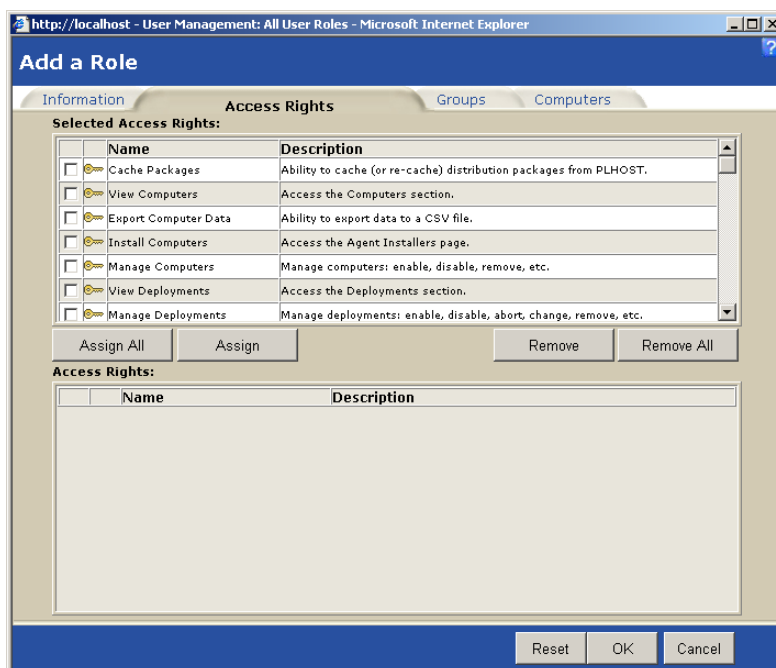


Figure 15.13

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

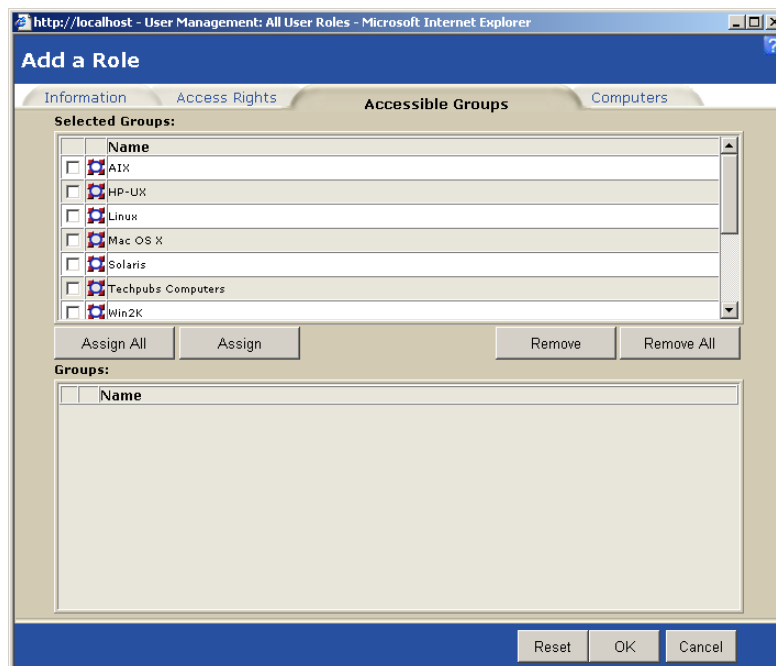


Figure 15.14

- Assign group access by selecting the checkbox to the left of each group and clicking the **Assign** button to move them into the **Selected Groups:** table (the **Assign All** button 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 the **Remove** button to move them to the **Groups:** table (the **Remove All** button will move all groups from the **Selected Groups** table to the **Groups** table)
7. Select the **Computers** tab, to define which computers the users assigned this role will be able to access

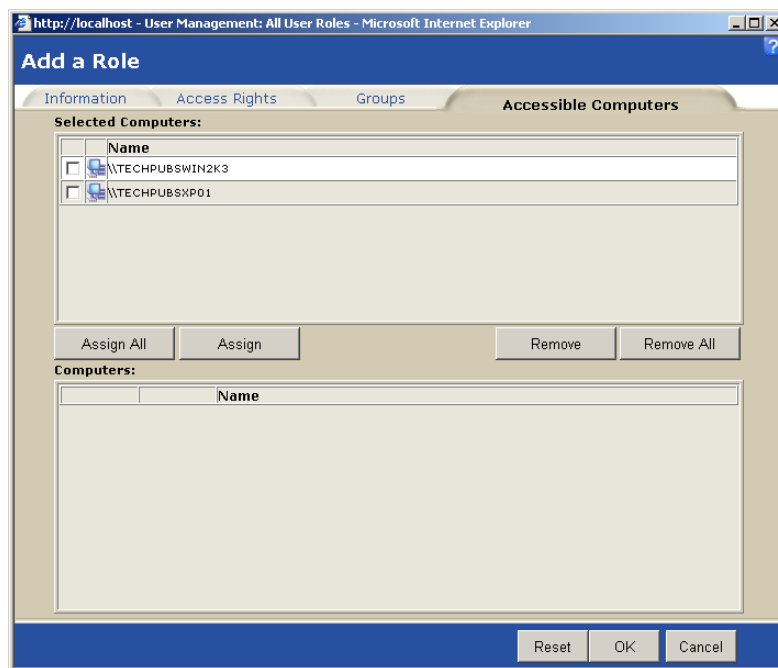


Figure 15.15

- Assign specific computer access by selecting the checkbox to the left of each computer and clicking the **Assign** button to move them into the **Selected Computers:** table (the **Assign All** button will move all computers from the **Computers:** table to the **Selected Computers:** table)
 - Remove specific computer access by selecting the checkbox to the left of each computer and clicking the **Remove** button to move them to the **Computers:** table (the **Remove All** button will move all groups from the **Selected Computers** table to the **Computers** table)
8. Click **OK** to save your changes

Editing User Roles

To edit a User Role:

1. Within your ZENworks Patch Management Server, select the **Users** page
2. Select the **Roles** tab

Users

Home / Vulnerabilities / Inventory / Packages / Computers / Groups / **Users** / Reports / Options / Help

Server Date & Time: 1/6/2005 1:59:14 PM (GMT-07:00)

User Management: Enabled User Roles

Filter By: Enabled

Users Roles

Total: 4

User Role Name	Type	Access Rights	Users	Groups	Computers
<input type="checkbox"/> Administrator	System	54	2	13	2
<input type="checkbox"/> Manager	System	50	0	13	2
<input type="checkbox"/> Operator	System	33	0	13	2
<input type="checkbox"/> Guest	System	22	0	13	2

patchlink Add Edit Disable Export

Figure 15.16

3. Select the checkbox to the left of the role you wish to edit
4. Click **Edit**
5. Follow the instructions detailed under [“Creating User Roles”](#) on page 231

Assigning User Roles

To assign a user role to a user:

1. Within your ZENworks Patch Management Server, select the **Users** page
2. Select, if necessary, the **Users** tab

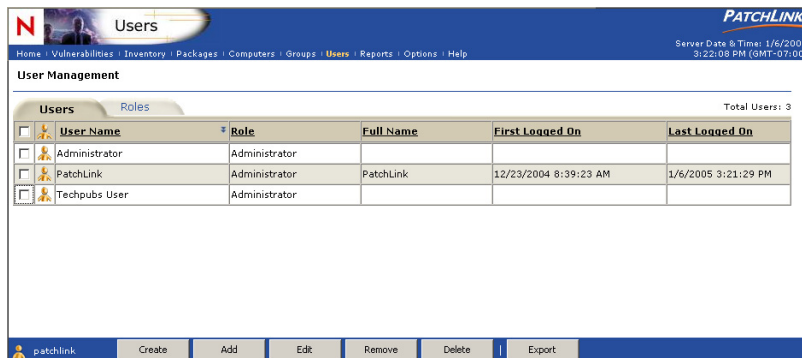


Figure 15.17

3. Select the user, by selecting the checkbox to the left of the **User Name**, which will be assigned the role

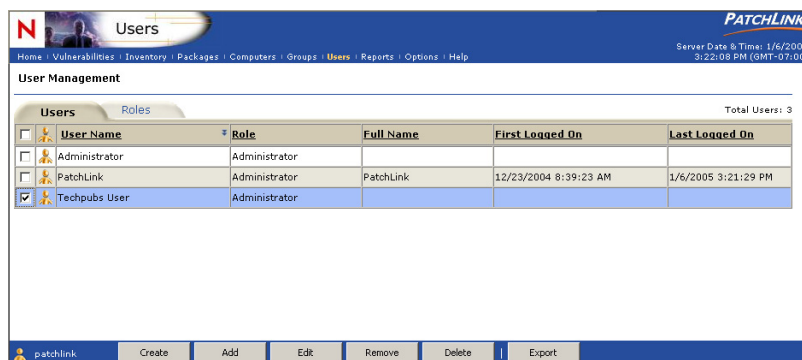


Figure 15.18

4. Click **Edit**

5. Click **Next** (if necessary to proceed to *Edit User* page)
6. Select the appropriate role from the **Role:** drop-down list

http://localhost - Edit a User - Microsoft Internet Explorer

Edit a User

Edit User Techpubs User:

Password Reminder:

Full Name:

Office phone:

Cell phone:

Pager:

Email:

Description:

Role:

< Back Next > Cancel

Figure 15.19

7. Click **Next** to proceed to the *Summary* page

http://localhost - Edit a User - Microsoft Internet Explorer

Edit a User

Summary:

User Name: Techpubs User

Full Name: Technical Publications U

Office Phone: 800.858.4000

Cell Phone: 800.858.4000

Pager:

Email: techpubs@novell.com

Password Reminder:

Description: TechPubs User Account

Role: Techpubs User Role

Will edit this PLUS user

< Back Finish> Cancel

Figure 15.20

8. Click **Finish** to apply the changes

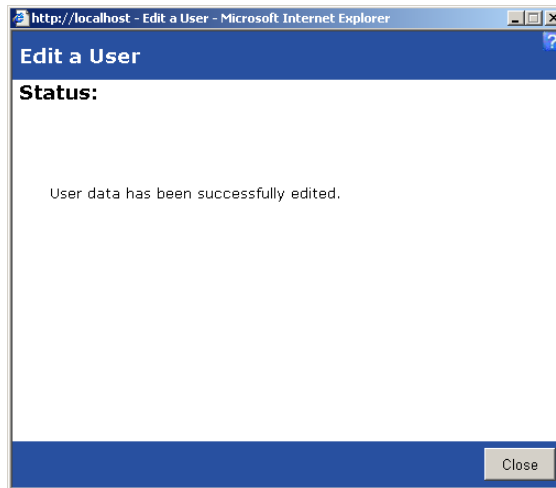


Figure 15.21

9. Click **Close** to close the wizard

Disabling User Roles

To disable a user role:

1. Select the checkbox to the left of the role you wish to disable
2. Click **Disable**



Note: You cannot disable system roles, and if you disable a custom role which is currently in use by a user, that user will still be able to log in to ZENworks Patch Management, but will have no permissions, and thus unable to view any pages.

Removing User Roles

To remove a user role:

1. Select the checkbox to the left of the role you wish to remove
2. Click **Remove**



Note: You cannot remove system roles, and if you remove a custom role which is currently assigned to a user, that user will still be able to log in to ZENworks Patch Management, but will have no permissions, and thus unable to view any pages.

Exporting User Data

The export data functionality, permits you to export a comprehensive .CSV file, which contains the **User's Name, Role, Full Name, First logged date in and last logged in date.**

To export and then view the exported .CSV file:

1. Click **Export**, which will open the *File Download* screen

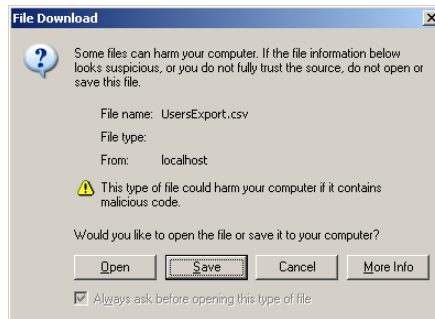


Figure 15.22 File Download

2. Click **Save** and save the file
3. You can now open the file with *Microsoft Excel*

	A	B	C	D	E
1	User Name	Role	Full Name	First Logged In (GMT-07:00)	Last Logged In (GMT-07:00)
2	Administrator	Administrator		12/9/2004 7:49	12/10/2004 8:28
3	PatchLink	Administrator	PatchLink	12/9/2004 3:38	12/9/2004 7:36
4	TechPubsUser	Administrator	TechPubsUser		

Figure 15.23 Export to Microsoft Excel

16 Configuring Default Behavior

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

[“About Configuration Options” on page 243](#)

[“Monitoring the Subscription Service” on page 245](#)

[“Verifying Subscription Licenses” on page 250](#)

[“Creating a Default Account Policy” on page 253](#)

[“Customizing and Administering Agent Policy Sets” on page 261](#)

[“Assigning E-mail Alerts” on page 272](#)

[“Contacting Technical Support” on page 276](#)

About Configuration Options

The *Advanced Configuration Options* page is available by clicking **Options** on the main toolbar.



Figure 16.1 Main Toolbar > Options

Configuration Options

The page comprises six management and configuration views as individual tabs. The available *Configuration Views* include the following:

Table 16.1 Configuration Options Views

Tab Title	Full Title	Description
Subscription	Subscription Service Information	Provides status and a record of activity for the subscription agent.
Licenses	Subscription Licenses	View ZENworks Patch Management Server and Plug-In licenses and current usage.
Defaults	ZENworks Patch Management Server Default Account Policies and Information	Manage default configuration settings for ZENworks Patch Management Server Agents registered to the ZENworks Patch Management Server.
Policies	Agent Policy Sets	Create custom agent policy sets to configure the default agent behavior for deployments.
E-Mail	E-Mail Notification Alerts	Create, define and manage system alerts.
Support	Support Information	Offers product registration option, technical support contact information, and detailed system and component information.

Monitoring the Subscription Service

The *Subscription Information* page allows you to manually run an update, configure a proxy server, and view update history and status information. Click **Options** in the tool bar and then click the **Subscription** tab.

Subscription Service | Licenses | Defaults | Policies | E-Mail | Support

Subscription Service Information

Last Subscription Poll: 4/15/2005 1:00:06 PM

Subscription Agent Status: Sleeping

Account ID: 466C4ECF-B42D-4722-BF8A-CB312DD7E1E9

Subscription Communication Interval: 1 Day at 07:30 (24-hour)

Subscription Host URL: https://update.patchlink.com/update/

Proxy Host:

Subscription Service History

Type	Status	Start Date	Stop Date	Duration	Successful
Licenses	Completed	4/15/2005 1:00:06 PM	4/15/2005 1:00:31 PM	25 (secs)	True
Packages	Completed	4/15/2005 7:58:25 AM	4/15/2005 7:58:36 AM	11 (secs)	True
Vulnerabilities	Completed	4/15/2005 7:30:13 AM	4/15/2005 7:57:17 AM	27.07 (mins)	True
Packages	Completed	4/15/2005 12:00:04 AM	4/15/2005 12:00:04 AM	0 (secs)	True
Packages	Completed	4/14/2005 2:50:05 PM	4/14/2005 2:50:45 PM	41 (secs)	True
Packages	Completed	4/14/2005 2:41:15 PM	4/14/2005 2:47:37 PM	6.37 (mins)	True
Packages	Completed	4/14/2005 1:40:00 PM	4/14/2005 1:40:04 PM	20 (secs)	True

Figure 16.2 Subscription Service View

ZENworks Patch Management Agents gather a list of software, hardware, services and patches installed on each computer within your network. With this detailed information, the ZENworks Patch Management Server generates a complete analysis of your network profile to identify the patches, hot fixes, service packs and updates of importance to your network.

The Subscription Service communicates with the ZENworks Patch Management Host Server (PLHOST) to download a series of patch reports that ensure the ZENworks Patch Management environment remains current. The PLHOST Server (also referred to as the Subscription Server) is the central repository where vulnerability reports and their associated patches are stored for retrieval by the ZENworks Patch Management Server. The ZENworks Patch Management Server attempts a connection to the PLHOST once daily to update system and patch information.

Access Levels

Access to subscription services configuration options is limited to user roles that have the following access rights assigned; View Options: Subscription, Export Subscription Data, and Manage Options.

- **View Options: Subscription** — Can access and view the Subscription Services tab in the *Options* page. This is a default access right in the Administrator, Manager, Operator, and Guest role templates.
- **Export Subscription Data** — Can export subscription data to a comma-separated value (CSV) file. This is a default access right in the Administrator and Manager role templates.
- **Manage Options** — Can access, view and update subscription service rules. This is a default access right in the Administrator role template only.

Subscription Service Information

The Subscription Service Information section provides a summary of the configuration settings and status of the subscription service. You can find additional management tools for the subscription agent in the Novell Agent Control Panel. Go to the Windows control panel to access the Novell Agent Control Panel.

You can modify the communication interval and enter a proxy host. If you make a change to either the communication interval or proxy host settings, you must click **Save** or any changes will be lost and not saved.

- **Last Subscription Poll** — Displays the date and time of the last successful update. An update is defined as contact by the subscription agent to the subscription host (URL) and the Novell retrieval of updates to ZENworks Patch Management.
- **Subscription Agent Status** — The current status of the subscription agent. This is not the same as the status of individual updates as reported in the history section but rather the status of the agent residing in the system. The following status conditions are reported: Sleeping and Running.
 - **Sleeping** — The agent is inactive (not running).
 - **Running** — The agent is active. Either as a result of the scheduled communication interval or a recent manual update request.
- **Account ID** — The Account ID is a key passed to the subscription host and used to validate the update request. The account key is created by the ZENworks Patch Management Server when it registers with the ZENworks Patch Management Host Web site. (The ZENworks Patch Management Host is also referred to as the Subscription Host in the product and documentation).

- **Subscription Communication Interval** — This is the interval at which the ZENworks Patch Management Server attempts a connection to the ZENworks Patch Management Host Web site and retrieves updates. The update is performed daily at the time indicated in the drop-down list box. You can select the time you want the connection to be initiated daily from the list of available times (half-hour increments).



Note: Unless you click **Update Now** on the *Action Menu*, the ZENworks Patch Management Server attempts a connection to the ZENworks Patch Management Host once daily.

- **Subscription Host URL** — the URL (or Web address) of the host site. This value is established by the ZENworks Patch Management Server and is not an editable field.
- **Proxy Host** — a proxy server acts as an intermediary between the ZENworks Patch Management Server, ZENworks Patch Management Host Server (PLHOST) and client machines to provide greater security in communication required by the subscription agent.



Note: If you modify the **Subscription Communication Interval** or **Proxy Host** fields, you must save the changes. Click **Save** on the *Action Menu*.

Subscription Service History Section

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

You can find additional management tools for the subscription agent in the Novell Agent Control Panel. Go to the Windows control panel to access the Novell Agent Control Panel.

- **Type** — Defines the type of task, the available types include:
 - **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 an agent task. While the task is active, the process begins with a status of *Initializing Replication*, followed by the downloads comprising the update. When the task is finished, the status reads *Completed*.
 - Initializing Replication
 - Downloading Platform Data
 - Downloading Package Data
 - Downloading Package Descriptions
 - Downloading Package OS Information

- Downloading Vulnerability Data
- Downloading Vulnerability Codes
- Downloading Vulnerability Information
- Downloading Vulnerability Descriptions
- Committing Vulnerability Data
- Downloading Vulnerability Packages
- Completed
- **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; *19 (secs)*, *1.22 (mins)*.
- **Successful** — *True* indicates the communication was a success and the update complete. *False* indicates the update was not successfully completed.

Action Menu

The action menu offers three commands: Save, Update Now, and Export.



Figure 16.3 Subscription Service Action Menu

- **Save** — Saves changes made to the ZENworks Patch Management communication interval or Proxy Host.
- **Update Now** — Initiates a complete replication of the ZENworks Patch Management Server, including an update of the Subscription Service. This options lets you manually update by running the subscription at a time of your choosing. Using this option overrides the time interval for that day only.

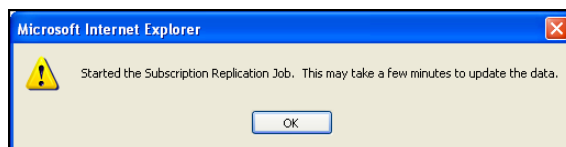


Figure 16.4 Subscription Service Update



Note: Replication ensures that ZENworks Patch Management Server remains current with the latest vulnerability, distribution package, and subscription license information.

- **Export** — The Export button allows you to export all subscription data to a comma separated value (.CSV) file. The file `SubscriptionExport.csv` is generated and the *File Download* dialog box allows you to define where the file should be saved.

To Export Subscription Data

1. On the *Options* page, click **Subscription**.
2. In the *Action Menu*, click **Export**.
3. In the File Download dialog box, select from the available options (Open, Save, Cancel).
 - a. **Open** — Creates the file and opens it in your Web browser. From the Web browser you can save to a variety of file formats including; CSV, XML, text, and numerous spreadsheet applications.
 - b. **Save** — Creates the file and saves it to a local folder. By default the file is saved to your My Documents folder in Microsoft Office Excel CSV format.
 - c. **Cancel** — Does not create or save the report.

Verifying Subscription Licenses

The *Subscription Licenses* page allows you to view, verify and export ZENworks Patch Management Server license information. As well, the option provides a summary of all product licenses associated to third-party software and plug-in components that are required and installed as part of your patch management activities. This information is captured as part of the daily ZENworks Patch Management Agent task (Discovery Agent Update task). Click **Options** in the tool bar and then click the **Licenses** tab.



Figure 16.5 Subscription License View

Access Levels

Access to subscription license configuration options is limited to user roles that have the following access rights assigned; View Options: Licenses, Export License Data, and Manage Options: Licenses.

- **View Options: Licenses** — Can access and view the Subscription Licenses tab in the *Options* page. This is a default access right in the Administrator, Manager, Operator, and Guest role templates.
- **Export License Data** — Can export license data to a comma separated value (CSV) file. This is a default access right in the Administrator and Manager role templates.
- **Manage Options: Licenses** — Can access, view, verify, and export license information. This is a default access right in the Administrator role template only.

License Information

The Subscription Licenses Information section provides a summary the license availability and usage for the ZENworks Patch Management system. You can verify (update) and export license information from within this section.

- **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 licenses currently being used and licenses available.

License summary information is presented according to license group. A license group is defined as the total block of licenses purchased at a time. For example, you may have 3 license groups comprising 500 total licenses with an initial group of 300 licenses purchased on March 1, and two additional groups of 100 licenses each added each subsequent quarter.

License groups information includes:

- **Purchase Date** — The date the license 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 total number of licenses authorized for the ZENworks Patch Management system and belonging to the group.

Action Menu

The action menu offers two commands: Verify and Export.

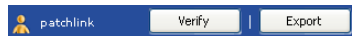


Figure 16.6 Subscription Licenses Action Menu

- **Verify** — Initiates a replication job that searches for license information and any changes to the license summary. This allows you to update license information manually at any time.



Note: License information is updated daily as part of the ZENworks Patch Management Agent tasks.

- **Export** — The Export button allows you to export all license data to a comma separated value (.CSV) file. The file `LicenseExport.csv` is generated and the *File Download* dialog box allows you to define where the file should be saved.

To Export License Data

1. On the *Options* page, click **Licenses**.
2. In the *Action Menu*, click **Export**.
3. In the File Download dialog box, select from the available options (Open, Save, Cancel).
 - a. **Open** — Creates the file and opens it in your Web browser. From the Web browser you can save to a variety of file formats including; CSV, XML, text, and numerous spreadsheet applications.
 - b. **Save** — Creates the file and saves it to a local folder. By default the file is saved to your My Documents folder in Microsoft Office Excel CSV format.
 - c. **Cancel** — Does not create or save the report.

Creating a Default Account Policy

The *ZENworks Patch Management Server Default Account Policy* page lets you establish, modify and export the agent policy set used as a default policy. The default policy is used in the absence of a customized agent policy set. Click **Options** in the tool bar and then click the **Defaults** tab.

The screenshot displays the 'PLUS Defaults' tab in the 'Novell ZENworks Patch Management Server (PLUS) Default Account Policies and Information' window. The interface is organized into several sections with various input fields, dropdown menus, and checkboxes.

- Subscription** and **Licenses** tabs are visible at the top.
- PLUS Defaults** is the active tab, showing the title 'Novell ZENworks Patch Management Server (PLUS) Default Account Policies and Information'.
- Agent Registration:** 'Total Agents Registered: 2', 'Default Agent Total: 0', 'Deployment Agent Total: 2'.
- Consecutive Deployment Failure Limit:** Set to 2.
- Use Agent Offline Threshold:** Checked, set to 3 hours.
- Deployment Agent Default Logging Level:** Set to 'None'.
- Hours of Operation:** 'Enable' button is active, 'Disable' is disabled.
- Ping Port:** Set to 0 (0 turns off the agent listener).
- Discovery Agent Mode:** Set to 'Normal'.
- Agent Uniqueness Validations:** Set to 'Standard'.
- Deployment Deadline Options:** 'Cancelable: No', 'Snoozeable: Yes', 'Deadline Offset: 5 mins', 'Offset Server Time: Yes'.
- Deployment Messages:** 'Manual Installation (download only deployment flag enabled)' is selected, showing a message box.
- Legacy Agent Configuration:** 'Notification timeout: 2 min(s)', 'Snooze duration: 60 min(s)'.
- ISAPI Concurrent Agent Limit:** Radio buttons for 'MSDE Default (5 threads)', 'SQL Default (64 threads)', and 'Custom Setting (5 threads)'.
- PLUS Machine Name:** 'TECHPLUS-PLUS'.
- PLUS URL:** 'techplus-plus'.
- Connection Mode:** 'http://'.
- Concurrent Deployment Limit (CDL):** Set to 10.
- CDLs for System Tasks:** 'Reboot: 5', 'RID: 5', 'DAU: 5'.
- Deployment Agent Default Communication Interval:** Set to 5 minutes.
- Agent Start Times:** Set to 12:00 AM.
- Agent Stop Times:** Set to 12:00 AM.
- Popup Each Notification as the Topmost Window:** Set to 'No'.
- Reboot Deadline Options:** 'Cancelable: Yes', 'Snoozeable: Yes', 'Reboot Offset: 5 mins'.
- May Reboot (-3 deployment flag enabled):** A message box is shown.
- ISAPI Connection Timeout:** Set to 30 sec(s), 'Use Default' checked.
- ISAPI Command Timeout:** Set to 60 sec(s), 'Use Default' checked.

Figure 16.7 Default Account Policies View

An Agent Policy Set is the key element in defining deployment behavior within the system. These policy sets are associated to groups that you create to manage your package and vulnerability deployments.

All system generated groups and the initial value for custom groups are defaulted to the *No Policy* agent set and the values defined in the default account policy are applied.

When you create a custom policy set, the values defined by the default account policy are replaced with those assigned to the custom policy. Note that the following values are NOT overridden by a custom policy and always stand as valid.

- *Concurrent Deployment Limit* settings and *CDLs for System Tasks* settings.
- *Consecutive Deployment Failure Limit* settings and *Offline Threshold* options.

Access Levels

Access to ZENworks Patch Management Server account configuration options is limited to user roles that have the following access rights assigned; View Options: Defaults, Export Default Data, and Manage Options.

- **View Options: Defaults** — Can access and view the ZENworks Patch Management Server Defaults tab in the *Options* page. This is a default access right in the Administrator, Manager, Operator, and Guest role templates.
- **Export Default Data** — Can export default account data to a comma separated value (CSV) file. This is a default access right in the Administrator and Manager role templates.
- **Manage Options** — Can access, view and update (save) default account settings. This is a default access right in the Administrator role template only.

Summary 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.

- **Total Agents Registered** — The total number of agents registered to the ZENworks Patch Management Server.
- **ZENworks Patch Management Server Machine Name** — The name of the machine on which the ZENworks Patch Management Server is installed.
- **Detection Agent Total** — The total number of detection agents registered to the ZENworks Patch Management Server.
- **ZENworks Patch Management Server URL** — The URL of the ZENworks Patch Management Server.
- **Deployment Agent Total** — The total number of deployment agents registered to the ZENworks Patch Management Server.
- **Connection Mode** — The connection mode used by the ZENworks Patch Management Server. For example, *http://* for standard mode or *https://* for secure mode.

Concurrent Deployment Limits

Concurrent deployment limits (CDL) let you establish deployment limitations.

- **Consecutive Deployment 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: Go to *E-Mail Notification* to establish recipients for deployment failure notifications.

- **Concurrent Deployment Limit (CDL)** — The maximum number of agents that can receive active deployments at the same time. The purpose of this limit is to throttle the number of deployments given to agents across the entire ZENworks Patch Management Server (ZENworks Patch Management Server).



Note: If an agent takes longer than four hours to report a successful deployment, it will no longer be counted against the **Concurrent Deployment Limit**.

- **Use Agent Offline Threshold** — Select to **configure a time interval that must expire before an agent is considered to be offline**. Agents are noted as being offline when they have not communicated with ZENworks Patch Management Server for a specified period of time (threshold). If an agent is disabled or uninstalled it does not appear as offline. The interval can be defined in minutes, hours, or days.



Note: When **Agent Offline Threshold** is NOT used, an agent is considered offline after failing to connect to ZENworks Patch Management Server after two of its communication intervals. For example: the agent has a communication interval of one (1) hour, if **Agent Offline Threshold** is NOT used, and the agent has not contacted ZENworks Patch Management Server for two (2) hours, it is reported as being offline.

- **CDL for System Tasks** — The number of times that a selected system task deployment is distributed **at one time**.
 - **Reboot** — The maximum number of **Reboot** deployments permitted to be distributed.
 - **RID** — The maximum number of **Refresh Inventory Data** deployments permitted to be distributed.
 - **DAU** — The maximum number of **Discover Applicable Updates** deployments that can be distributed.

Deployment Agent Defaults

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

- **Deployment Agent Default Logging Level** — Displays the default logging level employed by the agent. Levels include; None, Basic Information, Detailed, or Debug.
 - **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.



Note: Based upon your operating system the log files can be found in the following locations:

- **Windows (any version):** C:\Program Files\PatchLink\Update Agent\ZENworks Patch Management Agent.log
- **NetWare:** /export/home/PatchLink/update/log/updateagent.log
- **Linux:** /user/local/PatchLink/update/log/updateagent.log
- **Solaris:** PUPDATE.LOG

- **Deployment Agent Default Communication Interval** — The time interval at which the agent is labeled as being Offline if there is no attempt at communications between the ZENworks Patch Management Server and Deployment Agent. If an agent has not communicated in over two interval periods, the agent is displayed as *Offline*. The interval can be defined in minutes, hours, or days.
- **Hours of Operation** — Enable to restrict agent communication to the ZENworks Patch Management Server during a specific time range only, as indicated by the **Agent Start Time** and **Agent Stop Time**. **If disabled, the agent starts communicating with the ZENworks Patch Management Server when assigned this policy and continues until the policy or the agent is removed.**
- **Ping Port (Agent Listener)** — Define the port on which the agents listen. When pinged on the defined port, the agent responds by sending current version and contacts the ZENworks Patch Management Server to determine current tasks.

Discovery Agent Defaults

Discovery agent defaults let you establish default behavior for the discovery agent.

- **Discovery Agent Mode** — The mode in which the discovery agent runs.
 - **Fast Scan** — Always run in **Fast** mode. This performs the discovery faster, but uses more resources.
 - **Initial Only** — Performs the first discovery scan in **Fast Scan** mode, subsequent scans are performed in **Normal** mode.
 - **Normal** — Always run in **Normal** mode. Performs the scan using less resources, causing minimal impact on the target computer.
- **Popup Each Notification as the Topmost Window** — Choose **Yes** to force all notification windows to display on top (unable to be moved behind other windows).
- **Agent Uniqueness Validation** — Defines the Agent Uniqueness method used to identify agents.
 - **New** — Validates using instanced validation. Instanced validation, when determining agent uniqueness, uses logic which does not rely upon the computer name.
 - **Standard** — Validates based on computer name.

Deployment and Reboot Deadline Options

Deployment deadline options apply to deployment notification rules. The default behavior defined in this section may be overridden on a per-deployment basis using the *DeploymentWizard*.

- **Cancelable** — **Yes** permits the recipient of the notification to cancel the deployment.
- **Snoozable** — **Yes** permits the recipient of the notification to delay the deployment.
- **Deadline Offset** — The time window permitted to the client user to initiate an action. If the window defined by the offset time expires without user action, the deployment will automatically occur.
- **Offset Server Time** — **Yes** starts the deployment clock according to universal time (UTC), **No** starts the deployment based on local time.



Note: The **Offset Server Time** option applies to both the **Deployment Deadline Options** and the **Reboot Deadline Options**.

Reboot deadline options apply to notifications sent to inform the user that a system reboot is required. The default behavior defined in this section may be overridden on a per-deployment basis using the *DeploymentWizard*.

- **Cancelable** — **Yes** permits the recipient of the notification to cancel the system reboot operation.

- **Snoozable** — **Yes** permits the recipient of the notification to delay the system reboot operation.
- **Reboot Offset** — The time window permitted to the client user to initiate an action. If the window defined by the offset time expires without user action, the reboot will automatically occur.

Deployment Messages

Deployment messages are presented to the user when a deployment is pending or a system reboot operation required or recommended.

- **Manual Installation (*download only* deployment flag enabled)** — Packages deployed with the *download only* flag enabled display this message advising the user that the package must still be installed.
- **May Reboot (-3 deployment flag enabled)** — Packages deployed with the *may reboot* (-3) flag enabled display this message advising the user that the computer MAY be rebooted.

Legacy Agent Configuration

Legacy agent configuration rules apply to legacy (pre v6.2.2) ZENworks Patch Management Agents.

- **Notification time-out** — If the deployment 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.

ISAPI Settings

ZENworks Patch Management Server supports the Internet Server API for the Internet Information Server (IIS) Web server.

- **ISAPI Concurrent Agent Limit** — The maximum number of threads used by ZENworks Patch Management, the options are:
 - **MSDE Default** (5 threads) — Select to enable MSDE threads.
 - **SQL Default** (64 threads) — Select to enable SQL threads.
 - **Custom Setting** — User defined thread level.
- **ISAPI Connection Time-out** — Time (seconds) before an ISAPI thread expires (times out).
 - **Default** — Select to set the ISAPI Connection time-out to a default value of 30 seconds.
- **ISAPI Command Time-out** — Time (seconds) before an ISAPI command expires (times out).
 - **Use Default** — Select to set the ISAPI Command time-out to a default value of 30 seconds.

IAVA Settings

ZENworks Patch Management Server supports integration of data based on Information Assurance Vulnerability Alert (IAVA) standards for monitoring and tracking the resolution of network vulnerabilities.

- **IAVA Number Selection** — Choose the emergency response team standard to employ, including: Department of Defense and service branch teams (DoD Cert, ACERT, AFCERT and NAVCIRT).
 - **Blank** — Leave option blank to not include IAVA reference.
- **Run the IAVA Info Again** — Select to generate the IAVA reference information.

Action Menu

The action menu offers two commands: Save and Export.

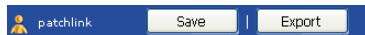


Figure 16.8 PLUS Defaults Action Menu

- **Save** — Saves any changes made on this page.



Note: If you have made ANY changes, you must click **Save**. If you do not click **Save**, the system will refresh to the last saved settings when you navigate off of the **PLUS Defaults** page.

- **Export** — The Export button allows you to export ZENworks Patch Management Server default information to a comma separated value (.CSV) file. The file `ComputerAgentExport.csv` is generated and the *File Download* dialog box allows you to define where the file should be saved.

To Export ZENworks Patch Management Server Default Data

1. On the *Options* page, click **Defaults**.
2. In the *Action Menu*, click **Export**.
3. In the File Download dialog box, select from the available options (Open, Save, Cancel).
 - a. **Open** — Creates the file and opens it in your Web browser. From the Web browser you can save to a variety of file formats including; CSV, XML, text, and numerous spreadsheet applications.
 - b. **Save** — Creates the file and saves it to a local folder. By default the file is saved to your My Documents folder in Microsoft Office Excel CSV format.
 - c. **Cancel** — Does not create or save the report.

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.

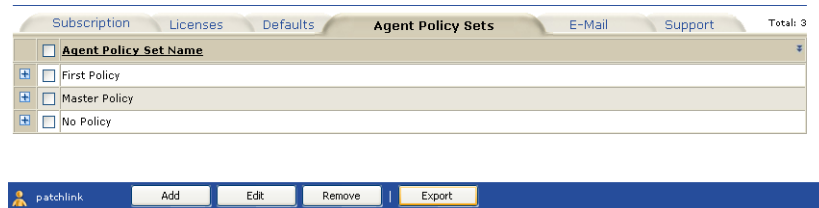


Figure 16.9 Agent Policy Set View



Note: If an group selected to receive the deployment has not been assigned a policy, the settings defined on the ZENworks Patch Management Server Defaults page are applied.

Creating an agent policy set is a simply process guided by the *Add a Policy Wizard*. All custom policies can be edited at any time and exported into a comma separated value (CSV) file format. The default policy is defined in the *Defaults* page.

An agent policy set is the key element in defining deployment behavior within the system. 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, package and vulnerability deployments inherent the behavior rules defined by an agent policy for the target group of the deployment.

When you create an agent policy set, the values defined by the default account policy are replaced with those assigned by you to the custom policy with a couple important exceptions. These exceptions are NOT overridden by a custom policy and always stand as valid.

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

Access Levels

Access to policy configuration options is limited to user roles that have the following access rights assigned; View Options: Policies, Export Policy Data, and Manage Options: Policies.

- **View Options: Policy** — Can access and view the E-mail Notifications tab in the *Options* page. This is a default access right in the Administrator, Manager, Operator, and Guest role templates.
- **Export Policy Data** — Can export data into CSV file format. This is a default access right in the Administrator and Manager role templates.
- **Manage Options: Policy** — Can access, view, modify, and delete e-mail notification rules. This is a default access right in the Administrator role template only.

Summary Information

The Agent Policy Set section lists all policy sets defined in the environment. Expanding an Agent Policy listing displays additional information regarding each policy. The information presented on this page is not editable. Add, edit, remove, and export commands are available in the action menu.

All available Agent Policy Sets are listed with the following information:

Table 16.2 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 255 characters.
Policy Type	There are two types of policies: System and User. Policy type indicates whether the policy was created by a user or by the system and is determined by ZENworks Patch Management Server.
Trace Level	The system logging level assigned to the policy. This is determined by the user when the policy is created and can be edited at any time. Trace levels include: None, Info, Detailed, and Debug. None — Only errors are logged and recorded. Info — Captures all errors, system and usage information. Detailed — Captures all errors and the major system actions. Debug — Captures all errors and system actions.
Operational Start Time Enabled	The time that agent communication with the ZENworks Patch Management Server begins. This is defined by the user in the <i>Hours of Operation</i> field. This feature must be enabled by the user.

Table 16.2 Agent Policy Set Definitions

Value	Description
Operational Stop Time Enabled	The time that agent communication with the ZENworks Patch Management Server ends. This is defined by the user in the <i>Hours of Operation</i> field. This feature must be enabled by the user.
Operational Start Time Disabled	Disabled operational times are labeled as Always . If noted as Always, the agent starts communicating with the ZENworks Patch Management Server as soon as the policy is assigned and continues until the policy or the agent is removed.
Created On	The date and time the policy was first created by a user.
Created By	The user who created the policy. The user name is generated from the ZENworks Patch Management Server user credentials used to sign in to the system.
Last Modified On	The date and time the policy was last modified by a user. Note that in editing a policy, you must click Save to register any changes to the policy.
Last Modified By	The user who issued the modification. The user name is generated from the ZENworks Patch Management Server user credentials used to sign in to the system.
Communication Interval	The interval — as measured by time in number of minutes, hours or days — of contact between the client agent and ZENworks Patch Management Server.
Description	The description attributed to the policy. Policy descriptions are defined by the user when the policy is created and can be edited at any time.
Discovery Agent Mode	The mode in which the discovery agent runs. This is defined by the user. The available options include: Fast Scan — Performs the discovery faster, but uses more resources. Initial Only — Performs the first discovery scan in Fast Scan mode, subsequent scans are performed in Normal mode. Normal — Performs the scan using less resources, causing minimal impact on the target computer.
Ping Port (Agent Listener)	Defines the port on which agents listen. This is established in the Default Agent Policy. When pinged, the agent responds with current version and contacts the ZENworks Patch Management Server for tasking. A value of 0 effectively turns the agent listener off.
Deployment Notification Options	The rules pertaining to how client workstations accept deployments. These options permit the client workstation user to avoid being interrupted by a particular deployment. Options are defined by user at policy creation and can be modified.

Table 16.2 Agent Policy Set Definitions

Value	Description
Reboot Notification Options	The rules pertaining to how client workstations accept reboot requests. These options permit the client workstation user to avoid being interrupted by a system reboot. Options are defined by user at policy creation and can be modified.
Offset Times	Deadline date offset times refer to the time window permitted to the client user initiate an action. If the window defined by the offset time expires without user action, the deployment and reboot will automatically occur.

Resolving Agent Policy Conflicts

When an agent is a member of a group such that it receives two (or more) 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 **ZENworks Patch Management Server Defaults** page.
- If the agent is a member of a 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, each (or some) of which have been assigned different policies, the agent will use a combination of settings from each of the groups to which it belongs. This combination of settings is calculated as follows:
 - It will use the shortest *Communication Interval*.
 - It will use the most verbose *Logging Level* (Debug > Detailed > Basic Information > None).
 - If all groups are using *Hours of Operation*, the agent will use an all inclusive *Hours of Operation*.
 - If one or more of the groups are **NOT** using *Hours of Operation*, the agent will **NOT** use *Hours of Operation*.
 - It will use the fastest *Discovery Agent Mode* (Fast Scan > Initial Scan > Normal Scan).
 - It will use the smallest *Deployment* and *Reboot Notification* values.
 - If one or more of the groups have an **Agent Listener** port defined (not zero), the agent listens on the highest defined port value.

Adding (Creating) a New Policy

The Add a Policy Wizard allows you to create and add a policy to the ZENworks Patch Management Server. To add a new policy, on the *Agent Policy Sets* page, click **Add**.

To Add (Create) an Agent Policy

1. In ZENworks Patch Management Server, click **Options**.
2. In the *Options* page, click **Policies**. (Labeled **Agent Policy Sets** when selected.)
3. In the *Action Menu*, click **Add**.
 - Steps 4-12 are nonsequential policy rules defined in the **Add a Policy** dialog box.

Figure 16.10 Add a Policy Wizard

4. In the **Name** box, enter a descriptive name for the policy. This field is required and can contain up to 255 characters.
5. In the **Description** box, enter comments about the policy. This optional field provides an opportunity to document the purpose and implementation notes for the new policy.
6. In the **Communication Interval** box, enter a number representing the time increment to serve as the interval between client and server communications. Next, select a unit of time that defines the interval. For example; 5 minutes, 5 hours, 5

days. The default is 5 and the maximum permitted value (for any unit) is 9999. Entering 0 has the effect of creating an interval of the lowest permitted time (1 minute) .

7. In the **Trace Level** box, assign a log level. Available options include; None, Info, Detailed, and Debug. See [Table 16.2, “Agent Policy Set Definitions”](#) on page 262 for definitions of these levels.
8. In the **Hours of Operation options**, click **Enable to limit the times that deployments may be deployed to client machines. If Disabled**, the agent starts communicating with the ZENworks Patch Management Server as soon as the policy is assigned and continues until the policy or the agent is removed.
 - d. Select a time to permit deployments to begin in the **Agent Start** spin box.
 - e. Select a time to cease deployments in the **Agent Stop** spin box.



Note: Permitting this option risks the timely deployment of packages and can be particularly troublesome in the case of urgent deployments as the client will not communicate with the server outside of established operation hours. A better approach is to allow continuous agent operation and carefully schedule deployments to not interfere with critical times (such as during the middle of the work day).

9. In the **Agent Listener** box, enter a port number to process ping attempts to the agent. Enter the number only and ensure the entry is correct as it is not validated by the system. Leave blank or assign a value of 0 (zero) to effectively disable the agent listener. See [Table 16.2, “Agent Policy Set Definitions”](#) on page 262 for details.
10. In the **Discovery Mode** box, select the mode for the discovery agent to run. The default is **Normal**. See [Table 16.2, “Agent Policy Set Definitions”](#) on page 262 for definitions of these levels.
11. In the **Deployment Deadline Options**, choose whether or not to permit the client operator to cancel or snooze (delay) the installation of a deployment. If

cancelled, the package is not deployed to the client unless the administrator deploys it again.

12. In the **Reboot Deadline Options**, choose whether or not to permit the client operator to cancel or snooze (delay) a system reboot request required as part of a deployment.



Note: Deadline and reboot date offset times refer to the time window permitted to the client user initiate an action. If the window defined by the offset time expires without user action, the deployment and reboot will automatically occur.

13. Click **Save** to create the agent policy as defined. Click **Reset** to clear the Wizard (or return to the last saved version of the policy). Click **Cancel** to close the Wizard without saving the policy.

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, click **Options**.
2. In the *Options* page, click **Policies**. (Labeled **Agent Policy Sets** when selected)
3. Select the policy to edit by clicking the check box to the left of the policy.

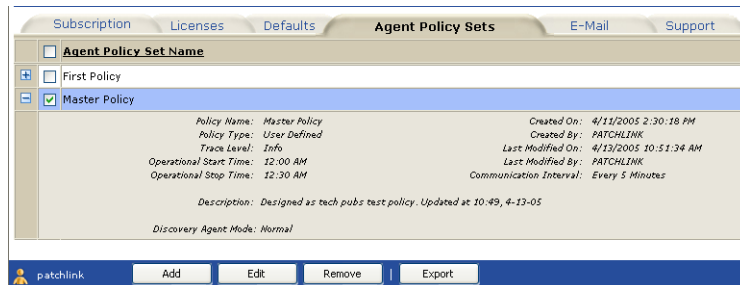


Figure 16.11 Editing Policies

4. In the *Action Menu*, click **Edit**.

5. In the *Edit a Policy* dialog box, edit the policy and click **Save**.

Figure 16.12 Edit a Policy Wizard

The new policy settings take effect immediately.



Note: Refer to “[To Add \(Create\) an Agent Policy](#)” on page 265, and [Table 16.2, “Agent Policy Set Definitions](#)” on page 262 for definitions about the available options.

Removing a Policy

You can remove a policy at any time. Removing a policy effectively deletes the policy from the database and any groups associated to the policy are automatically associated to the default policy.

To Remove a Policy

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

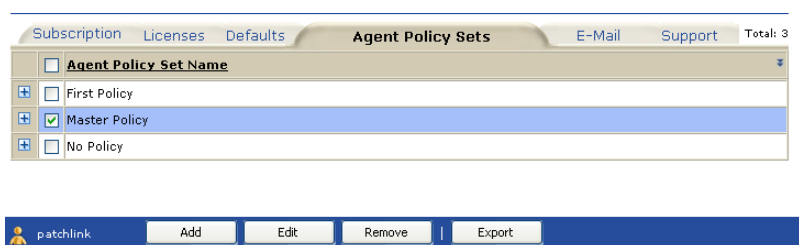


Figure 16.13 Removing a Policy

3. Select the policy to remove by clicking the checkbox to the left of the policy.
4. In the *Action Menu*, click **Remove**.
5. In the *Edit a Policy* confirmation dialog box, click **Yes**.



Note: Refer to “[To Add \(Create\) an Agent Policy](#)” on page 265, and [Table 16.2, “Agent Policy Set Definitions”](#) on page 262 for definitions about the available options.

Exporting Policy Definitions

You can export agent policy set information ZENworks Patch Management Server to the comma separated value (.CSV) file format. The file `PolicyExport.csv` is generated and the *File Download* dialog box allows you to define where the file should be saved.

To Export an Agent policy SetZENworks Patch Management Server

1. On the *Options* page, click **Policies**.
2. Select the policy to export by clicking the check box adjacent to the policy.
3. In the *Action Menu*, click **Export**.
4. In the File Download dialog box, select from the available options (Open, Save, Cancel).
 - a. **Open** — Creates the file and opens it in your Web browser. From the Web browser you can save to a variety of file formats including; CSV, XML, text, and numerous spreadsheet applications.
 - b. **Save** — Creates the file and saves it to a local folder. By default the file is saved to your My Documents folder in Microsoft Office Excel CSV format.
 - c. **Cancel** — Does not create or save the report.

Assigning E-mail Alerts

The *E-Mail Notification* page lets you configure system alerts to help in monitoring the ZENworks Patch Management Server environment. You can enter any number of e-mail addresses and then assign the particular alert types that you want each recipient to receive. As well, this page allows you to define the trigger levels for individual alerts. Click **Options** in the tool bar and then click the **E-Mail** tab.

	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	License Expiration	Notification Address
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	itdirector@novell.com
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	patch_admin@novell.com

Alert Thresholds SMTP Relay: mail.myhost.com

Low System Disk Space: Alert When Below 1024 MB Check Disk Space Every 1 Hours

Low Storage Disk Space: Alert When Below 1024 MB Check Disk Space Every 1 Days

Low Available License Count: Alert When Below 5 Licenses

Up-Coming License Expiration: Alert When Days Remaining Are Below 10

patchlink Add Save Remove Export Test

Figure 16.14 E-Mail Notifications View

Access Levels

Access to e-mail notification configuration options is limited to user roles that have the following access rights assigned; View Options: E-Mail, Export E-Mail Notification Data, and Manage Options.

- **View Options: E-Mail** — Can access and view the E-mail Notifications tab in the *Options* page. This is a default access right in the Administrator, Manager, Operator, and Guest role templates.
- **Export E-Mail Notification Data** — Can export data into CSV file. This is a default access right in the Administrator and Manager role templates.
- **Manage Options** — Can access, view, modify, and delete e-mail notification rules. This is a default access right in the Administrator role template only.

E-Mail Notification Settings

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.

- **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 machine falls below the trigger established in the *Alert Thresholds* section.
- **Low Storage Disk Space** — Alerts when the available storage space on the ZENworks Patch Management Server machine falls below the trigger established in the *Alert Thresholds* section.
- **Low Available License Count** — Alerts when the number of licenses available to the ZENworks Patch Management Server falls below the trigger established in the *Alert Thresholds* section.
- **Up-Coming License Expiration** — Alerts when the number of licenses nearing expiration falls below the trigger established in the *Alert Thresholds* section.
- **License Expiration** — Alerts when a license expires.
- **Notification Address** — The e-mail address that serves as recipient of notifications. This must be a validly formatted e-mail address (*name@domain.tld*); the system does not, however, validate the actual address.
- **SMTP Relay** — The mail host used by your ZENworks Patch Management Server for sending e-mail messages.

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.

- **Low System Disk Space** — Alert is generated if the system disk space on the ZENworks Patch Management Server machine drops below the trigger level. The level is measured in Megabytes (MB) and must be numeral with a minimum of 1 and maximum of 9999 (9999 MB or 9.76465 GB).
- **Low Storage Disk Space** — Alert is generated if the storage drive disk space on the ZENworks Patch Management Server machine drops below the trigger level. The level is measured in Megabytes (MB) and must be numeral with a minimum of 1 and maximum of 9999.

- **Checking Interval** — The checking interval (*Check Disk Space Every...*) represents the schedule that the thresholds are checked. This is measured in units of minutes, hours or days. You can select any whole number between 1 and 99 (do not use decimal fractions such as 1.5).
- **Low Available License Count** — Alert is generated if the number of licenses available in the ZENworks Patch Management Server environment drops below the defined trigger level. The level is measured in units of available licenses. You can select any whole number (1, not 1.5) between 1 and 999.
- **Up-Coming License Expiration** — Alert is generated if the number of licenses nearing or at expiration in the ZENworks Patch Management Server environment drops below the defined trigger level. The level is measured in units of days to expiration. You can select any whole number (1, not 1.5) between 1 and 99.

Action Menu

The action menu offers five commands: Add, Save, Remove, Export, and Test.

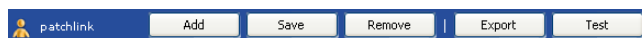


Figure 16.15 E-Mail Notification Action Menu

- **Add** — Creates a new E-Mail Notification address.
- **Save** — Saves any changes made to the notification settings.



Note: Be sure to click **Save** after making any changes. If you do not click **Save**, the system will refresh to the last saved settings when you navigate off of the *E-Mail* page or select another command from the *Action Menu*.

- **Remove** — Deletes the selected e-mail address from the notification list. Once removed, the data is destroyed and not recoverable.
- **Export** — Exports a list of e-mail notification addresses and settings to comma separated value (.CSV) file format. The file `NotificationExport.csv` is generated and the *File Download* dialog box allows you to define where the file should be saved.
- **Test** — Sends a test e-mail message to the selected e-mail addresses assigned to receive notifications.

To Export ZENworks Patch Management Server Default Data

1. On the *Options* page, click **E-Mail**.
2. In the *Action Menu*, click **Export**.
3. In the File Download dialog box, select from the available options (Open, Save, Cancel).
 - a. **Open** — Creates the file and opens it in your Web browser. From the Web browser you can save to a variety of file formats including; CSV, XML, text, and numerous spreadsheet applications.
 - b. **Save** — Creates the file and saves it to a local folder. By default the file is saved to your My Documents folder in Microsoft Office Excel CSV format.
 - c. **Cancel** — Does not create or save the report.

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 to submit a test message. You may select one, multiple, or all notification e-mail addresses.
3. In the *Action Menu*, click **Test**.
4. A confirmation message informs you that the test message was sent.

Contacting Technical Support

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.

The screenshot displays the 'Technical Support' tab in the Novell ZENworks Patch Management Server interface. The main content area is divided into several sections:

- Novell ZENworks Patch Management Server Information:**
 - Version: 6.2.2.178
 - Computer Name: BPPF2K3S
 - Last Connected with Novell: 7/20/2005 12:00:12 AM
 - System Root Free Space: C:\ = 3,267,559,424 Bytes
 - Installation Date: 7/19/2005 4:26:00 PM
 - Operating System: Server
 - Last Agent Connection: 7/20/2005 9:53:02 AM
 - Storage Volume Free Space: C:\ = 3,267,559,424 Bytes
- Other Installed Novell Products:**
 - Product Name: Scanner Integration Common Components
 - Product Version: 2.0.0.101
- Component Version Information:**
 - OS Version: 5.2.3790
 - IIS Version: 6.0.3790.0
 - .NET Versions: v1.0.3705, v1.1.4322
 - SQL Server Agent: Status: Running, Start State: Auto Start, File Name: sqlagent.EXE, Product Version: 8.00.760
 - OS Service Pack: (button)
 - MDAC Version: 2.80.1022.0
 - SQL File Version: 8.00.760
 - SQL Version: Microsoft SQL Server 2000 - 8.00.760 (Intel X86) Dec 17 2002 14:22:05 Copyright (c) 1988-2003 Microsoft Corporation Desktop Engine on Windows NT 5.2 (Build 3790;)
- Subscription Status:**
 - Agent Registration Status: (button)
 - Agent Registration Code: 0
 - Agent Communication Frequency: 86400 Seconds
 - Agent ID: 63A31F61-6E86-4BF7-877A-38F5A3E340F5
- Novell Contact Information:**
 - Mailing Address: Novell, Inc., 1800 South Novell Place, Provo, UT 84606
 - Phone Number: 1-800-858-4000
 - Fax Number: (button)

The bottom toolbar includes a 'patchlink' icon and buttons for 'Support', 'Novell Web', 'Re-Register', and 'Export'.

Figure 16.16 Technical Support View

Access Levels

Access to policy configuration options is limited to user roles that have the following access rights assigned; View Options: Support, Export Support Data, and Manage Options: Policies.

- **View Options: Policy** — can access and view the Technical Support tab in the *Options* page. This is a default access right in the Administrator, Manager, Operator, and Guest role templates.
- **Export Support Data** — can export data into CSV file format. This is a default access right in the Administrator and Manager role templates.

- **Manage Options: Policy** — can access and view support information, reregister components, and access e-mail and Web support links. This is a default access right in the Administrator role template only.

ZENworks Patch Management 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.

- **ZENworks Patch Management Server Version** — The version number of the ZENworks Patch Management Server installed.
- **Installation Date** — The installation date of the current ZENworks Patch Management Server license. This is detected by the first communication that occurred as part of the installation process; it is not the license purchase or effective date.
- **Computer Name** — The name of the computer on which ZENworks Patch Management Server is installed.
- **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 ZENworks Patch Management Host (PLHOST).
- **Last Agent Connection** — The date and time an Agent last made a connection to the ZENworks Patch Management Server.
- **System Root Free Space** — The amount of free disk space on your system volume.
- **Storage Volume Free Space** — The amount of free disk space on your storage volume.

Other Installed Novell Products

This section identifies additional products from Novell installed in the computing environment. The information is not editable.

- **Product Name** — The name of the complimentary product.
- **Product Version** — The version number of the product.

Component Version Information

This section identifies the basic component software and services running on the ZENworks Patch Management Server. The information is not editable. Click **More** to view a detailed list of MDAC product and file versions. Click **Start / Stop** to control the SQL Server Agent.

- **OS Version** — Additional operating system information (typically the version number).
- **OS Service Pack Information** - Service pack information, if available, of your operating system.
- **IIS Version** - The Internet Information Server version running on the system.
- **MDAC Version** - The current MDAC version number. Click **More** for MDAC version details.
- **.NET Version** - The .NET Framework version(s) installed on the server.
- **SQL File Version** - The SQL Server version installed on the server.
- **SQL Server Agent** - Displays SQL Agent status, start state, SQL Agent file name, and product version number.
- **SQL Version** - Detailed SQL Server version information.

Subscription Status

This section reports on the status of the ZENworks Patch Management Server subscription agent.

- **Agent Registration Status** — The last reported registration status between the agent and the ZENworks Patch Management Host (PLHOST).
- **Agent Registration Code** — This is a code returned by the subscription agent.
- **Agent Communication Frequency** — The number of seconds that must elapse before the subscription agent automatically contacts the ZENworks Patch Management Host (PLHOST).
- **Agent ID** — This is assigned to the agent upon its registration with the ZENworks Patch Management Host (PLHOST).

Novell Contact Information

Contact information for technical support at Novell, Inc.. Write, call, or fax to these numbers. Through the *Action Menu*, you can access help over the Web or by e-mail.

Action Menu

The action menu offers four commands: E-Mail, Novell Web, Re-Register, and Export.



Figure 16.17 Technical Support Action Menu

- **E-Mail** — Get e-mail support. Clicking **E-Mail** opens a short Wizard program that helps us to contact the right person to answer your questions or handle your request.
- **Novell Web** — Click to open the Novell, Inc. technical support Web site. Opens a new browser instance.
- **Reregister** — Click to register the subscription agent with the ZENworks Patch Management Host Web site (also referred to as the PL Host, Subscription Host). This option is available only if the subscription agent has not previously registered with the Host Web site.
- **Export** — The Export button allows you to export technical support information to a comma separated value (.CSV) file. The file `SupportInfoExport.csv` is generated and the *File Download* dialog box allows you to define where the file should be saved.

To Export ZENworks Patch Management Server Default Data

1. On the *Options* page, click **Support**.
2. In the *Action Menu*, click **Export**.
3. In the File Download dialog box, select from the available options (Open, Save, Cancel).
 - a. **Open** — Creates the file and opens it in your Web browser. From the Web browser you can save to a variety of file formats including; CSV, XML, text, and numerous spreadsheet applications.
 - b. **Save** — Creates the file and saves it to a local folder. By default the file is saved to your My Documents folder in Microsoft Office Excel CSV format.
 - c. **Cancel** — Does not create or save the report.

A Hardening ZENworks Patch Management

There are a few steps that can be taken to harden a ZENworks Patch Management Server that is to be put on the public Internet. You can opt to implement some or all of these suggestions, and these are of course just guidelines:

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 .CER certificate file before rebooting after the main phase of the installation. The advantage is that with an SSL certificate installed all agent communication and all administration is now fully encrypted - and so there is no way to spoof or snoop communications on the wire. Refer to the *ZENworks® Patch Management v6.2.2 Server Installation Guide* for additional details.

Turn Off Non-Critical Services

Microsoft Windows ships with most features turned on. There are a number of services you may wish to turn off (e.g.: RPC, Remote Registry, etc.) to reduce the risk of hacker 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
- SQLSERVERAGENT
- ZENworks Patch Management

Use Secure Passwords

Worm attacks frequently try to log in with weak and commonly used passwords (letmein, no password, etc.) therefore you should not use them. For a secure password we recommend using the Department of Defense standard of 12 characters with alpha, numeric, punctuation and mixed case characters all included in your password.

Turn Off Windows Networking

To turn off Windows Networking:

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 **File and Printer Sharing for Microsoft Networks**

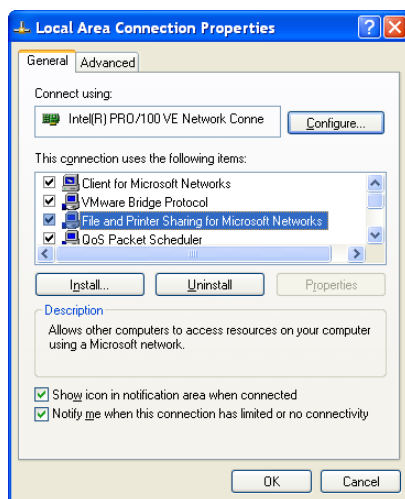


Figure A.1 Turn Off Windows Networking

4. Click **Uninstall**



Note: Do not uninstall **Client for Microsoft Networks** because it is required by both Microsoft SQL Server and Internet Information Server.

Put Your ZENworks Patch Management Server Behind a Firewall

Since the ZENworks Patch Management Server software pulls its patch updates from the subscription servers, there is no need to allow access from the Internet to the ZENworks Patch Management Server. Be sure to allow access to <http://www.novell.com>, <https://update.patchlink.com>, and <https://storage12.patchlink.com> through your firewall.

Lock Down Unused TCP and UDP Ports

1. From within the *Windows Control Panel* double-click the **Network Connections** icon
2. Open (by double-clicking) the *Local Area Connection*
3. On the *Local Area Connections Status* General tab click **Properties**

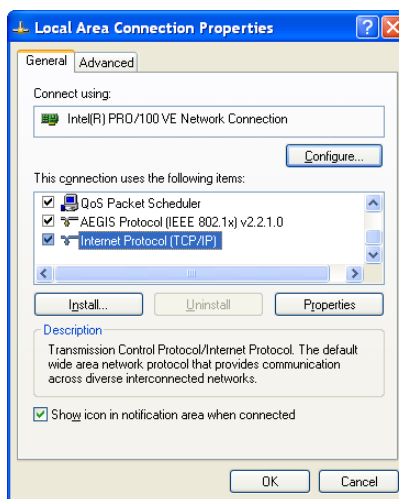


Figure A.2 Local Area Connection Properties

4. Select the *Internet Protocol (TCP/IP)* protocol and click the **Properties** button

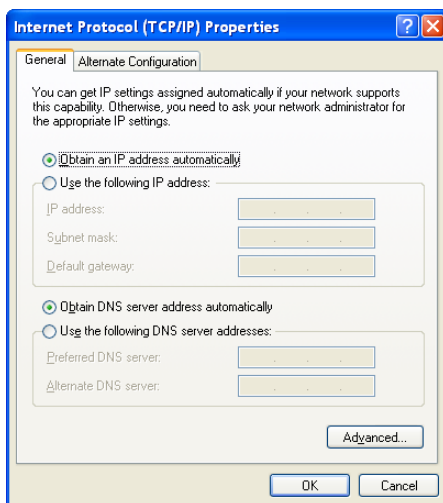


Figure A.3 General tab

5. On the *Internet Protocol (TCP/IP) Properties* General tab click **Advanced...**
6. Select the **Options** tab

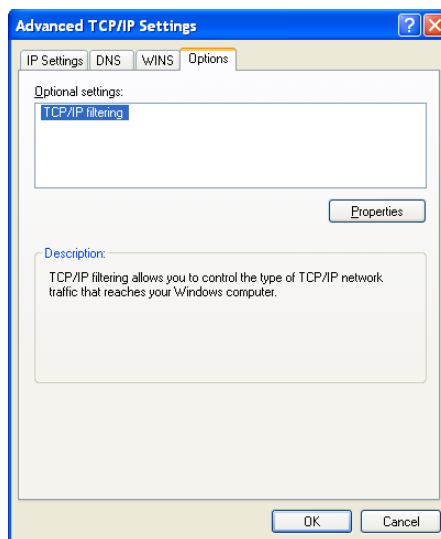


Figure A.4 Advanced TCP/IP Settings

7. Select *TCP/IP filtering* and click **Properties**
8. Check the **Enable TCP/IP Filtering (All adapters)** checkbox
9. Select the **Permit Only TCP Ports** option

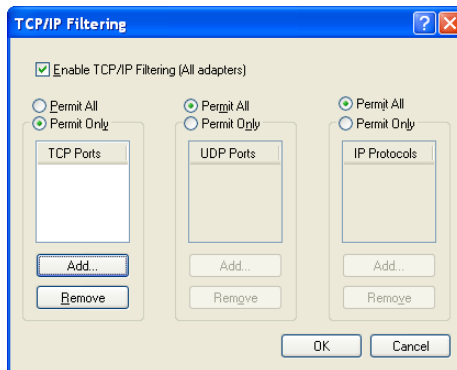


Figure A.5 TCP/IP Filtering

10. Add TCP ports 443 and 80 to the listing of permitted ports

- a. Click **Add...**
- b. Enter *443* in the **TCP Port** field

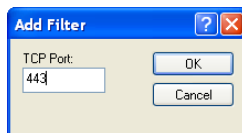


Figure A.6 Add Filter

- 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



Note: If you lock out everything except ports 80 and 443 it will be necessary to add entries to <http://www.novell.com>, <https://storage12.patchlink.com>, and <https://novell.patchlink.com> in your `HOSTS` file (in the `%WINDIR%\system32\drivers\etc` directory) so that your ZENworks Patch Management Server can download your patch subscriptions.



Warning: If you use a proxy server and access that server by name (not IP address) you must add the proxy server name and address to your `HOSTS` file (in the `%WINDIR%\system32\drivers\etc` directory).

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

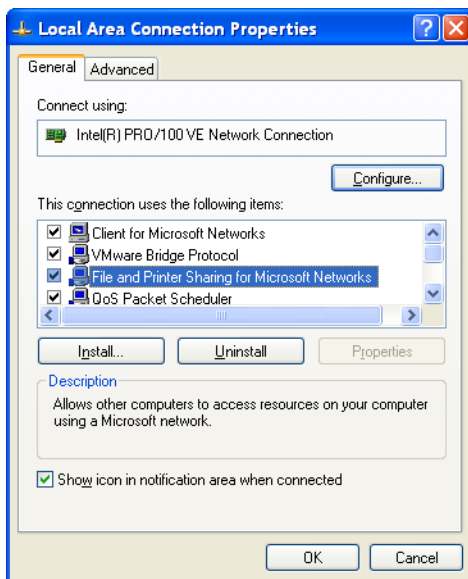


Figure A.7 Local Area Connection Properties

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 the Microsoft SQL Patches

Apply these patches so you don't get the SLAMMER worm on your server, apply the most recent applicable patches for IIS, SQL, and the Operating System.

B ZENworks Patch Management Server Reference

ZENworks Patch Management Server Security

There are multiple layers to security for ZENworks Patch Management:

- Web Site Authentication
- Web Site Encryption via SLL
- User (Security) Roles

Web Site Authentication

Internet Information Services (IIS) controls authentication in to the ZENworks Patch Management Server web site, which means the operating system itself is validating users and their passwords when they log in to the site. Control of who has access and who does not, at this level, is controlled by a local user group.

Web Site Encryption via SSL

SSL provides an encrypted wrapper around all web communication to and from the product. Since all communication is over the web, this means by installing ZENworks Patch Management Server in to SSL mode and then adding an SSL certificate to the ZENworks Patch Management Server web site will provide a wall around customer's data, away from prying eyes.

User (Security) Roles

Every feature, page and action throughout ZENworks Patch Management Server has been assigned to a series of Access Rights. Combining these access rights together form a user role. Roles also contain a list of groups and computers (which do not belong to the list of groups). Put this all together and ZENworks Patch Management Server now contains a mechanism in which regardless of how you authenticated in to the ZENworks Patch Management Server web application, what you can do is defined solely by your Novell Administrator. If a user does not have a User Role, or it is disabled, and their access immediately is denied to everything.

Error Pages

The ZENworks Patch Management Server provides four distinct error pages. These pages are:

- **Insufficient Browser Capabilities** - This page is displayed whenever a user visits the ZENworks Patch Management Server with a browser incapable of properly processing the site. The minimum browser requirements are provided on this page, along with links to download the latest versions of popular browsers.
- **Requested Page Not Found** - This page is displayed whenever a user attempts to navigate to a 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 the site.
- **Login Failure** - This page is displayed whenever a user fails to provide valid credentials for access to the ZENworks Patch Management Server.
- **System Component Version Conflict** - This page is display whenever a system component version conflict is detected. 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 is displayed providing the component(s) that failed to meet the required version. The ZENworks Patch Management Server also attempts to notify the system administrator via e-mail of the conflict.

Error Codes

ZENworks Patch Management uses Microsoft's WinInet API for communication between the Agents and Server. When this communication fails the error code returned are WinInet error codes. Refer to [Microsoft knowledgebase article #193625](#) for a definition of each error code. The following table defines the most commonly seen error codes:

Table B.1 ZENworks Patch Management Agent Error Codes

PL Agent Error Description	WinInet Error Code	Description
Head failed: Head request failed. Error is 12002. . Host=1116 HTTP Error=0	12002	The internet connection timed out
Head failed: Head request failed. Error is 12031. . Host=1109 HTTP Error=0	12031	The connection with the server has been reset
Head failed: Head request failed. Error is 12007. . Host=1109 HTTP Error=0	12007	The server name could not be resolved

Novell Websites

To ensure trouble-free operation of your ZENworks Patch Management Server, you should confirm that your ZENworks Patch Management Server can access the following sites:

Table B.2 Novell Web sites

URL	IP Address *	Port *
http://www.patchlink.com	206.124.169.050	443
https://novell.patchlink.com	204.138.167.005	443
https://storage12.patchlink.com	216.205.112.066	443
All access to the secured sites https://novell.patchlink.com or https://storage12.patchlink.com , is controlled via your ZENworks Patch Management Server. Therefor you are only validating your ability to connect to these sites not your ability to view data.		
* The IP Addresses and Ports shown were accurate at the time of publishing and are subject to change.		

Computer Status Icons

Table B.3 Computer 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 B.3 Computer Status Icons


















Status	Description
	The agent is offline since it has not contact ZENworks Patch Management Server in more than two communication intervals (minimum of 15 minutes)
	The agent is offline since it has not contact ZENworks 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 ZENworks 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 ZENworks 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 ZENworks 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 ZENworks 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)

Table B.3 Computer Status Icons

Status	Description
	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 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.

