User Guide
ZENworks Patch Management 6.4 SP2

N.

Notices

Version Information

ZENworks Patch Management User Guide - ZENworks Patch Management Version 6.4SP2 - Released: September 2009
Document Number: 02_012N_6.4SP2_092651134

Legal Notices

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.

www.novell.com

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

Novell Trademarks

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

Third-Party Materials

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

Table of Contents

Table of Contents

Preface

About This Document

This User Guide is a resource written for all users of Novell ZENworks Patch Management 6.4 SP2. This document defines the concepts and procedures for installing, configuring, implementing, and using Novell ZENworks Patch Management 6.4 SP2.

Tip: Novell documentation is updated on a regular basis. To acquire the latest version of this or any other published document, please refer to the *Novell Documentation Web page* (*http://www.novell.com/documentation/*).

Typographical Conventions

The following conventions are used throughout this documentation to help you identify various information types.

Convention	Usage
bold	Buttons, menu items, window and screen objects.
bold italics	Wizard names, window names, and page names.
italics	New terms, options, and variables.
UPPERCASE	SQL Commands and keyboard keys.
monospace	File names, path names, programs, executables, command syntax, and property names.

Contacting Novell

The following table lists the available technical support options.

Call Novell Support	Web Support
Phone: +1 800.858.4000	*http://www.novell.com/support*

Preface

Chapter

1

ZENworks Patch Management Overview

In this chapter:

- *Product Overview*
- *System Requirements*
- *Agent Supported Operating Systems*
- *Agent Supported Languages*

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

A vulnerability includes information that is used by the agents to identify the requirements for the devices. This identification process uses prerequisite profiles to determine if a patch is applicable to a computer. If the prerequisite profile matches then the agent will use detailed patch identifiers, called fingerprints, to verify the device is fully patched and protected.

Product Overview

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

Patch Management Server and Agent Process

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

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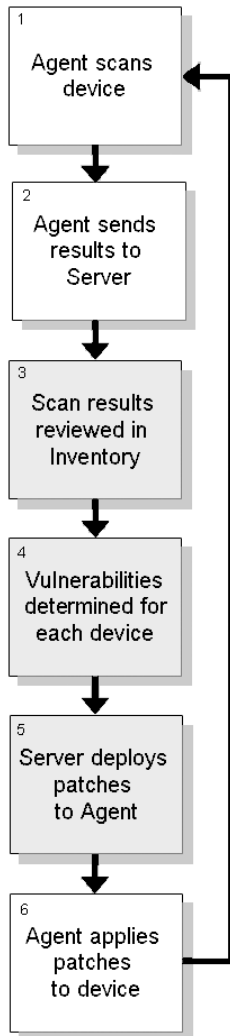
1. The Agent scans the host device and compiles information on operating system, software, hardware, and services on that device via the Discover Applicable Updates (DAU) task.
2. The DAU runs an inventory scan on the agent and sends the results back to Patch Management Server, which compares it with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

System Requirements

Minimum Hardware Requirements

The hardware requirements for ZENworks Patch Management 6.4 SP2 vary depending upon the number of devices you manage. As the device count increases, so do the requirements. The following, minimum hardware requirements, will support up to 250 devices:

- A single 1.4 GHz Pentium or equivalent processor
- 1024 MB RAM
- 36 GB of available disk space
- A single 100 Mbps network connection (with access to the Internet)

For optimal performance please refer to the settings defined under *Recommended Configuration* on page 22.

Supported Operating Systems

ZENworks Patch Management 6.4 SP2 is supported on the following Operating Systems:

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

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

Note: Prior to installing ZENworks Patch Management 6.4 SP2, you must also install the **Update for Windows Server 2003 (KB925336)** available from *Microsoft Knowledge Base Article #925336*.

Other Software Requirements

ZENworks Patch Management 6.4 SP2 requires the following software:

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

Supported Database Servers

ZENworks Patch Management 6.4 SP2 is supported on the following database servers:

- Microsoft SQL Server 2005 Express Edition with SP2 or later.
- Microsoft SQL Server 2005 Standard Edition with SP2 or later.
- Microsoft SQL Server 2005 Enterprise Edition with SP2 or later.

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

Recommended Configuration

Novell recommends the following hardware and software configurations for ZENworks Patch Management 6.4 SP2:

Table 1: ZENworks Patch Management 6.4 SP2 Recommended Configuration

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

Note: Refer to the *Novell Knowledge Base* (*http://www.novell.com/support/*) for additional configuration recommendations.

Agent Supported Operating Systems

The following table lists the supported platforms on which the Patch Management Agent 6.4 SP2 is supported.

Table 2: Agent Supported Operating Systems

Operating System	OS Versions	OS Edition	OS Data Width	Proc. Family	Proc. Data Width	Min. JRE
Apple Mac OS X	10.3 - 10.5.x	All	32/64 bit	x86(Intel)/ PowerPC	32/64 bit	1.4.0
HP-UX	11.00 - 11.31	All	64 bit	PA-RISC	64 bit	1.4.0
IBM AIX	5.1 - 6.1	All	32/64 bit	PowerPC	32/64 bit	1.4.0
Microsoft Windows XP	All	Pro [1]	32/64 bit	x86	32/64 bit	N/A
Microsoft Windows Vista[3]	All	Business Enterprise Ultimate	32/64 bit	x86	32/64 bit	N/A
Microsoft Windows Server 2008[3]	All	Web [2] Standard Enterprise	32/64 bit	x86	32/64 bit	N/A
Novell Netware	6.5	All	32 bit	x86	32 bit	1.3.0
Novell SUSE Linux	9 -10	Enterprise	32/64 bit	x86	32/64 bit	1.4.0
Red Hat Linux	3 - 5	Enterprise AS, ES, WS	32/64 bit	x86	32/64 bit	1.4.0
Sun Solaris	8 - 10	All	32/64 bit	SPARC/ x86	32/64 bit	1.4.0

(1) Home, Media Center, and Tablet PC editions are not supported.

(2) The Datacenter and Core Editions of this OS family are not supported.

(3) Windows Vista and Windows Server 2008 support requires .NET 3.0.

Note: Red Hat Enterprise Linux and Sun Solaris support requires additional configuration steps. Please refer to the *Supporting Red Hat Enterprise and Sun Solaris Agents* on page 251 section of the ZENworks Patch Management 6.4 SP2 User Guide for additional details.

Agent Supported Languages

ZENworks Patch Management Agent 6.4 SP2 is supported on the following languages:

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

Chapter

2

Using ZENworks Patch Management

In this chapter:

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

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

Getting Started with ZENworks Patch Management

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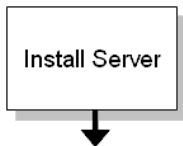
Install Server

Within the install function, initial administration roles and parameters are established. Refer to the Patch Management Server Installation Guide for more information on installing and configuring your initial usage.

Install Agents	After installing the Patch Management Server, the agent can be installed. In order to install the agent, the devices must be able to download it from the Patch Management Server. Refer to the Agent Installation Guide for more information.
Create Groups	Groups are created in preparation for deployment. A group associates similar devices for the purpose of deploying to multiple workstations.
Create Agent Policies	Agent policy sets are associated with a group and applied to the group. An agent policy is a set of constraints that govern the communication interval, logging level, and agent start and stop times.
Deploy Vulnerabilities	The agent deploys to the devices within the network. This process is aided by the Deployment Wizard which provides instructions for defining and distributing deployments to the selected devices in the network.
Create Mandatory Baselines	After the initial vulnerabilities are resolved, a mandatory baseline can be set. This is a user-defined range of required patches for a group of devices. If a device falls out of compliance, applying the mandatory baseline ensures the device is patched back into compliance.
Create Users/Roles	User permissions, credentials and roles can be established for all users of the system.

Accessing ZENworks Patch Management

Logging on to ZENworks Patch Management

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

1. Launch your web browser.

2. Type the Server URL in your web browser's **Location** field.

3. Press **Enter**.

   Step Result: The system displays the *Connect to Update Server* dialog box.
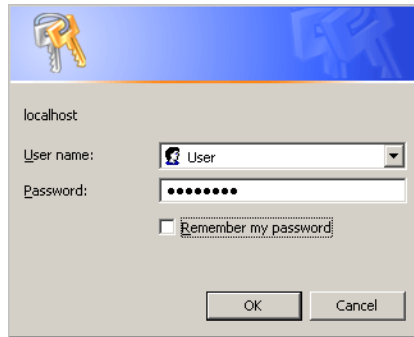
Figure 1: Log on dialog box

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

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

6. Click **OK**.

   Step Result: The *Home* page opens.

Logging Out of Update

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

   Example:

Server Date and Time: 3/8/2006 10:54:37 AM (GMT-08:00)
Log Out

   Figure 2: Log Out Menu Item

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

Example:
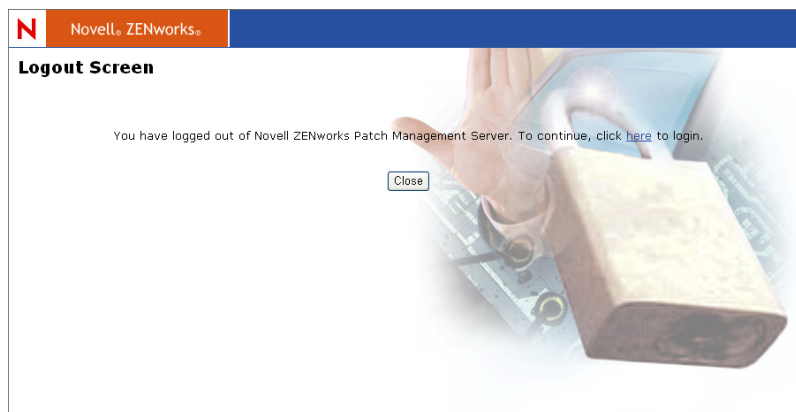
Figure 3: Patch Management Server Logout Screen

Common Functions within Patch Management Server

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

Defining Browser Conventions

Novell ZENworks Patch Management supports the following browser conventions:

Table 3: Browser Conventions

Screen Feature	Function
Entry Fields	Type data in to these fields, which allow the system to retrieve matching criteria or to enter new information.
Drop-Down Menus	Displays a list to select pre-configuration values.
Command Buttons	Perform specific actions when selected.
Check Boxes	A check box is selected or cleared to enable or disable a feature. Lists also include a **Select All** check box that lets you select all the available listed items on that page.
Radio Buttons	Select the button to select an item.

Screen Feature	Function
Display Screens	Show areas that are part of a window or an entire window. The data on display screens can be viewed, but not changed.
Sort	Data presented in tables can be sorted by ascending (default) or descending order within a respective column by clicking on a (enabled) column heading.
Mouseovers	Additional information may be displayed by hovering your mouse pointer over an item.
Auto Refresh	Where present and when selected, the Auto Refresh function automatically refreshes the page every 15 seconds.

Note: The *Groups* page supports the right-click function, however in some areas right-click is not supported.

Using Search

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

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

Figure 4: Search feature for Vulnerabilities example

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

Table 4: Search Settings

Select	To
Save as Default View	Save the active search and filter criteria as the default view for the page. The default view displays each time the page is accessed. You can change this setting at any time.

Select	To
Show results automatically	Automatically retrieves and displays results from the database when the module is selected from the Navigation Menu.

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

Using Filters

You can filter information retrieved from the database and the Global Subscription Server using the filter functionality that appears on the top of most pages. The filter parameters differ within each function in ZENworks Patch Management.

Use the drop down lists to select the parameters you need for your search. To toggle the filter fields, click **Show Filters** or **Hide Filters**.

Note: Your search and filter criteria will remain applicable, even after browsing to a different page, until you perform a new search or log out of Novell ZENworks Patch Management.
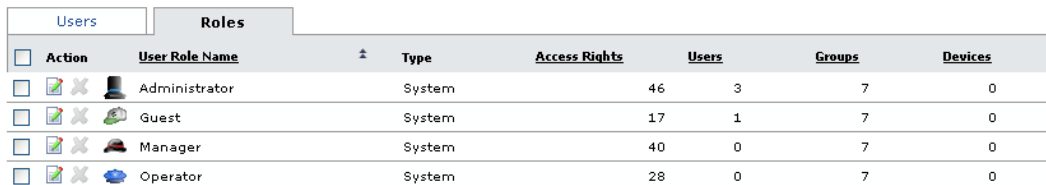
In addition to the filter criteria described above, you can select display options for data from the **Options** drop-down list. The following table describes these options.

Table 5: Data Display Options

Select	To
Save as Default View	Save the active search and filter criteria as the default view for the page. The default view displays each time the page is accessed. You can change this setting at any time.
Show results automatically	Automatically retrieves and displays results from the database when the module is selected from the Navigation menu.
Show/Hide Group By Row	Toggles the visibility of the Group By row. This row appears at the top of data table. To group data according by a column header, click the column header and drag it to the column header to the Group By row.

Using Tabbed Pages

Tabs are labeled groups of options used for similar settings within a page. Select each tab to view the available options.
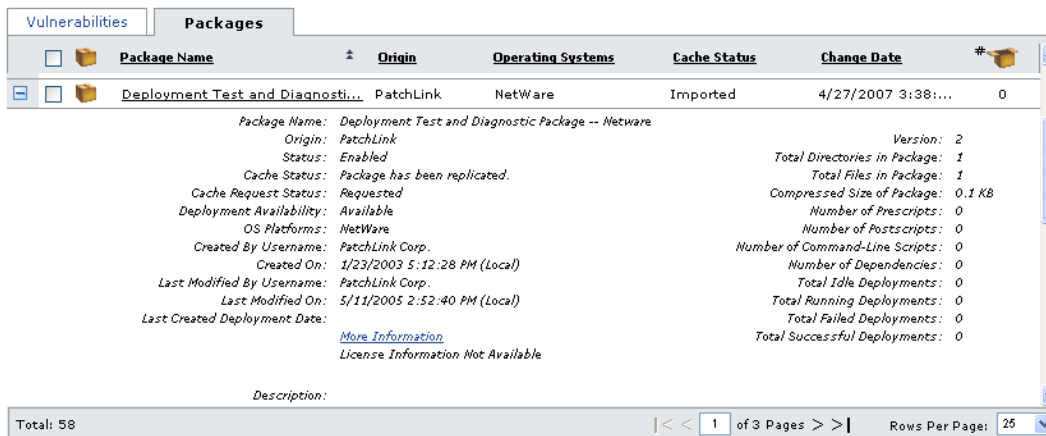
Figure 5: Tabbed Page Example

Expanding and Collapsing Folders and Outlines

Novell ZENworks Patch Management allows you to expand and collapse folders, outlines, and other data sources on the page. The information is refreshed each time it is displayed.

Figure 6: Expanded Row Option

Advancing Through Pages

Each page provides page-through options at the bottom of each tabbed page. The amount of items available for display and the specific page you are viewing determines how the options are presented.
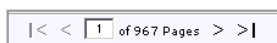
Figure 7: Pagination Feature

Table 6: Pagination Controls

Function	Use To
Next	Advance to the next page of entries or to the last page of entries by clicking the next page (>) or last page (> |) links.
Previous	Return to the previous page of entries or to the first page of entries by clicking the previous page (<) or first page (| <) links.
Displaying Page	Indicate the current page number.
Rows Per Page	Modify the number of entries displayed on a single page by selecting the desired number of records to display.

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

Using the Action Menu

The **Action** menu displays below the filter options and provides access to all actions available for each page. The available commands vary depending where you are in the application and depend on the role assigned to the user.

Figure 8: Action Menu

Using Help

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

Access to context sensitive help is available by clicking **Help** located in the navigation menu.
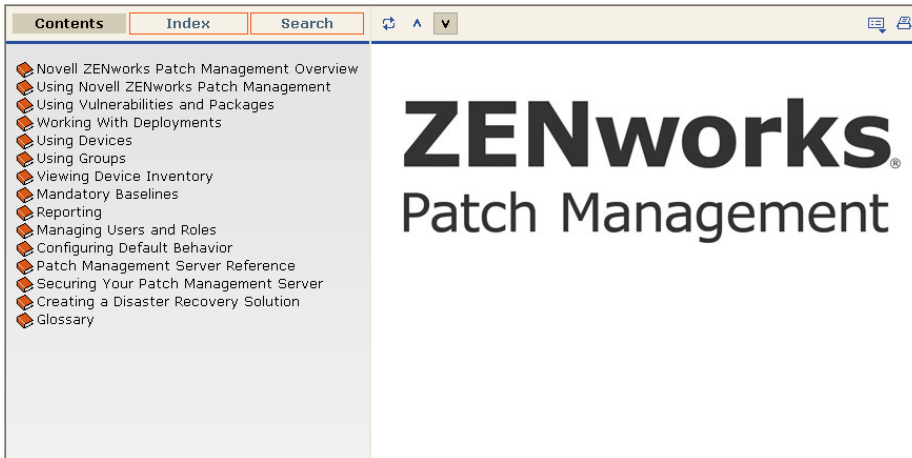
Figure 9: Example Help Screen

Exporting Data

The information presented can be exported into a comma-separated value (*.csv*) file. You may elect to save the file in a different file format after opening it from the download option.

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

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

2. Click **Export**.

3. In the *File Download* dialog box, select from the available options: **Open**, **Save**, **Cancel**.

- **Open** - Creates the file and opens it in your Web browser. From the browser you can save to a variety of file formats including; *.csv*, *.xml*, *.txt*, and numerous spreadsheet applications.
- **Save** - Creates the file and saves it to a local folder. The file is saved to your My Documents folder in comma-separated value (*.csv*) format.
- **Cancel** - Does not create or save the report.

Example:

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

Figure 10: Exported Inventory Data

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

Viewing the Patch Management Server Home Page

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

From the *Home* page, you can access all features of the Patch Management for which you are authorized. The *Home* page provides links to documentation, support resources, status information, patch-related news, and charts.
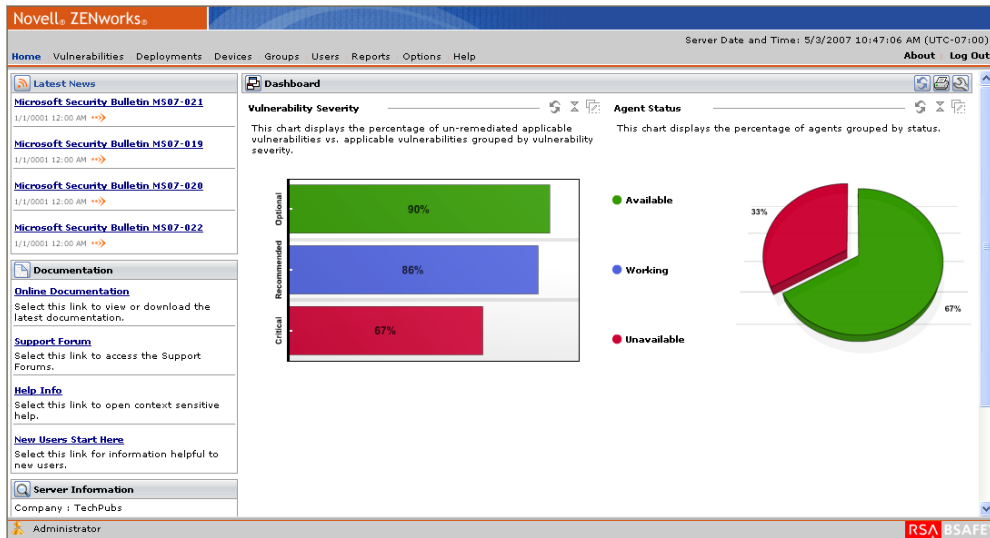
Figure 11: Patch Management Server Home Page

The page is divided into four areas.

- *Using the Navigation Menu* on page 35.
- *Viewing Latest News* on page 37.
- *Viewing the Documentation Links* on page 38.
- *Viewing Server Information* on page 38.

Using the Navigation Menu

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

Figure 12: Navigation Menu

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

Table 7: Patch Management Server Navigational Menu

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

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

Viewing Latest News

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

Figure 13: Latest News Window

Viewing the Documentation Links

The Documentation links provide access to obtaining information about Patch Management Server. The links provide access to help, user documentation, and support regarding your Patch Management Server status.
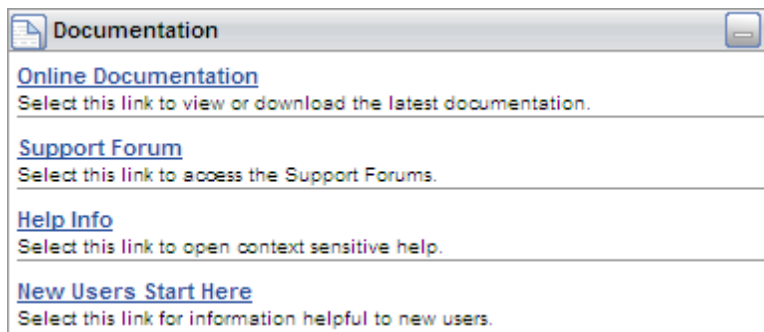
Figure 14: Documentation Links

The following table provides a description of the Documentation links.

Table 8: Documentation Links

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

Viewing Server Information

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

Viewing the Graph Dashboard

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

Dashboard Charts

The following table describes all of the available charts.

Table 9: Dashboard Charts

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

Dashboard Settings and Behavior Icons

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

Table 10: Dashboard Settings and Behavior Icons

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

Adding a Graph to the Dashboard

1. Click the **Dashboard Settings** icon.

> **Step Result:** The *Dashboard Settings* dialog opens.
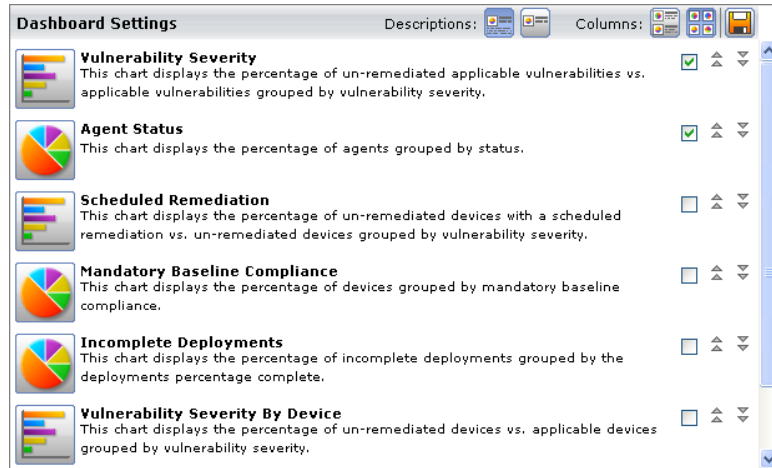
Figure 15: Dashboard Settings Dialog

2. Select check boxes associated with the charts you want to display.

3. Move the graphs up or down according to your priorities.

4. Select the number of columns for display: Select a one or two column width view from **Columns**.

- Click the **View as One Column** icon to display charts in one column.
- Click the **View as Two Columns** icon to display charts in two columns.

5. Display or hide the chart descriptions.

- Click the **Show the Chart Descriptions** icon to display chart descriptions.
- Click the **Hide the Chart Descriptions** icon to hide chart descriptions.

6. Click **Save**.

Result: Your graph setting selections are saved and displayed.

Removing a Graph from the Dashboard

1. Click the **Dashboard Settings** icon.

> **Step Result:** The **Dashboard Settings** drop-down list opens.

2. Deselect the checkbox next to the graph(s) you want to remove.

3. Click **Save Dashboard Settings**.

4. Click **Save**.

   Step Result: The graph(s) is removed from the *Dashboard* window

License Expiration

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

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

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

To proceed, select Update License Data. The license verification process begins and connects to the Global Subscription Server, retrieving updated license information. The page refreshes to the home page once your updated licenses have been saved.
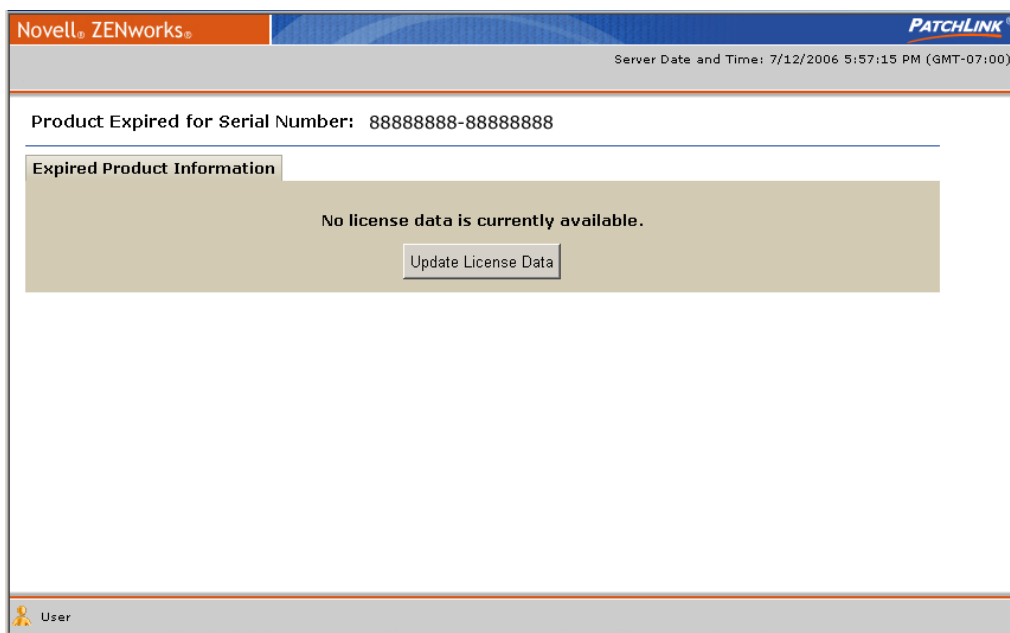
Figure 16: License Expiration Page

Note: If you need to renew licenses or add new licenses, visit *http://www.novell.com/company/ contacts-offices/* to contact your Novell Sales representative.

Chapter

3

Using Vulnerabilities and Packages

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

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

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

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

The Relationship Between Vulnerabilities and Packages

The following graphic illustrates the relationship between vulnerabilities and packages. Typically, a single vulnerability is shared by multiple products on multiple operating system platforms. There may be a series of separate patches to mediate the same vulnerability in different

environments. The separate patches are grouped in packages identified by their respective product or OS. As a result, a series of packages are included for one vulnerability.
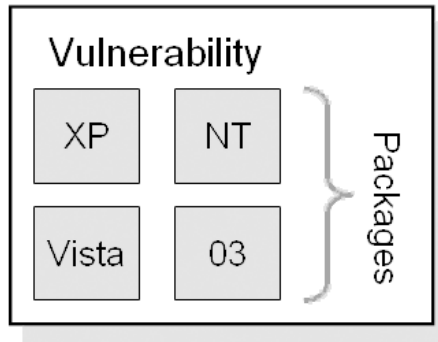
Figure 17: Vulnerability and Package Relationship

About Vulnerabilities

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

The Patch Management Agent installed on each device checks for known vulnerabilities using the Discover Applicable Updates (DAU) task. The DAU runs an inventory scan and sends the results back to Patch Management Server, which compares it with the list of known vulnerabilities. If the device is found to have vulnerabilities, a deployment can be set up to remedy the issues.
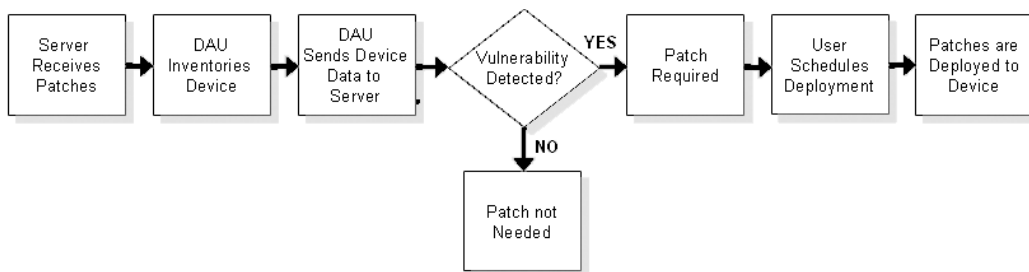
Figure 18: Discover Applicable Updates

Defining Vulnerability Structure

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

As depicted in the following diagram, for each vulnerability you can have more than one signature. For each signature, you can have multiple fingerprints and pre-requisites. However, you can only have one package assigned per signature.
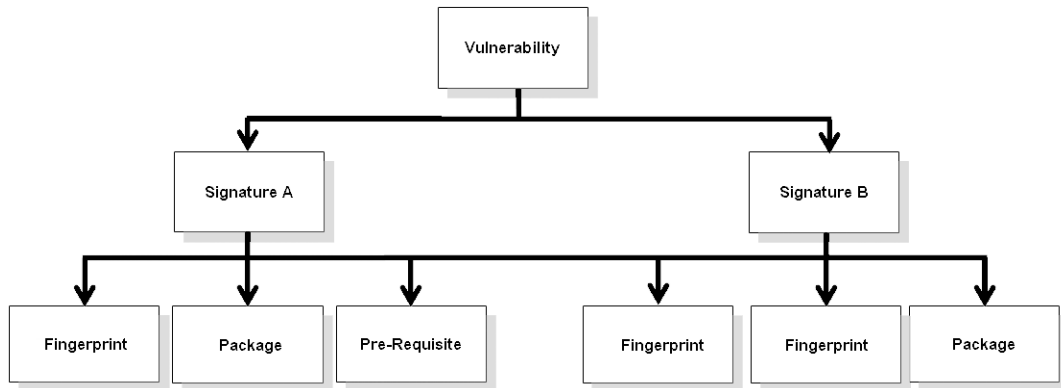
Figure 19: Patch Structure

Vulnerabilities

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

Signatures

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

Fingerprints

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

Pre-requisites

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

Packages

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

The Vulnerabilities Page

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

Figure 20: The Vulnerabilities Page

To Access The Vulnerabilities Page

1. From the toolbar, select **Vulnerabilities**.

2. If needed, select the desired filter criteria.

3. Click **Update View**.

Result: The system displays the existing vulnerabilities in the Vulnerabilities page.

Viewing Vulnerabilities

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

1. In the Vulnerabilities list, select a vulnerability. You can only view the details of one vulnerability at a time.

2. Click the Vulnerability name.

   Step Result: The *Vulnerability Details* page for the selected vulnerability opens.

Figure 21: Vulnerability Details

Viewing Vulnerability Details

Selecting the **Expand** icon next to a vulnerability will display detailed information about the vulnerability. You can view this same detailed information on the **Information** tab located on the *Vulnerability Details* page.

Figure 22: Vulnerability Details

Vulnerability Status and Types

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

Table 11: Vulnerability Status and Descriptions

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

The following table includes descriptions of the Vulnerability status icons.

Table 12: Vulnerability Status Icons and Descriptions

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

Vulnerability Package Cache Status and Type

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

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

Package Status and Descriptions

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

Table 13: Package Status and Description

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

Package Icons and Descriptions

The icons and their status are classified as follows:

Table 14: Package Status Icons and Descriptions

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

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

Vulnerability Name

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

Vulnerability Impacts

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

- **Critical** - Novell or the product manufacturer has determined that this patch is critical and should be installed as soon as possible. Most of the recent security updates fall in to this category. The patches for this category are automatically downloaded and stored on your ZENworks Patch Management Server.
- **Critical - 01** - Novell or the product manufacturer has determined that this patch is critical and should be installed as soon as possible. This patch is older than 30 days and has not been superseded.
- **Critical - 05** - Novell or the product manufacturer has determined that this patch is critical and should be installed as soon as possible. These patches have been superseded.
- **Critical - Intl** - An international patch, where Novell or the product manufacturer has determined that this patch is critical and should be installed as soon as possible. Most of the recent international security updates fall in to this category. After 30 days international patches in this category will be moved to Critical - 01.
- **Detection** - These vulnerabilities contain signatures that are common to multiple vulnerabilities. They contain no associated patches and are only used in the detection process.
- **Informational** - These vulnerabilities detect a condition that Novell or the product manufacturer has determined as informational. If the report has an associated package, you may want to install it at your discretion.
- **Recommended** - Novell or the product manufacturer has determined that this patch, while not critical or security related is useful and should be applied to maintain the health of your computers.

- **Software** - These vulnerabilities are software applications. Typically, this includes software installers. The vulnerabilities will show not patched if the application has not been installed on a machine.
- **Task** - This category contains tasks which administrators may use to run various detection or deployment tasks across their network.
- **Virus Removal** - This category contains packages which administrators may use to run various virus detections across their network. Anti-Virus tools and updates are included in this category.

Vulnerability Statistics

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

Table 15: Column Icon Definitions

Icon	Definition
✓	Total number of devices that are patched.
✗	Total number of devices that are not patched.
⊘	Total number of devices which returned an error.
🕐	Total number of devices that are in the process of detecting. [whether the device is patched or not patched]
🖥	Total number of assigned or impacted devices.
%	Percentage of the devices that have completed the detection = [(Total Patched + Total Not Patched) / Total Assigned devices].

Searching, Filtering, and Saving Views

ZENworks Patch Management offers options that allow you to search for specific items and filter result sets. Searching and filtering can be performed independent of each other or can be combined to provide drill-down capabilities. Search and filter settings can be saved as the default view displayed on subsequent visits to the page. See *Using Search* on page 29 for additional information.

Working with Vulnerabilities

There are several tasks in vulnerabilities designed to assist with management and deployment. These are available from buttons located on the *Vulnerabilities* page. These tasks include:

- *Deploying Vulnerabilities* on page 53.
- *Viewing Vulnerabilities* on page 46.
- *Disabling and Enabling Vulnerabilities* on page 53.
- *Updating the Cache* on page 55.
- *Using the Scan Now Feature* on page 53.

Vulnerability Status Tabs

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

Table 16: Tabs and Descriptions

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

Column Definitions

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

Table 17: Vulnerability Column Definitions

Name	Definition
Device Name	The name of the device.
IP Address	The IP address of the device.
DNS Name	The DNS name for the device or its IP address if it does not have an assigned DNS name.
Operating System	The operating system (abbreviated) running the device.

Name	Definition
OS Service Pack	Additional operating system version information.
Analysis Date	The date the agent on the device last ran the Discover Applicable Updates system task.

Device Status

Also displayed in the *Vulnerability Details* page is the status of the agent installed on the device.

Table 18: Device Status Icons

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

Deploying Vulnerabilities

Deploying a vulnerability to selected devices is a key function of the ZENworks Patch Management Server. Deployments are initiated by selecting **Deploy** and completing the Deployment Wizard. The Deployment Wizard provides step-by-step instructions for defining and distributing vulnerabilities to the protected devices in the network. Refer to *Working With Deployments* on page 81 for additional information.

Disabling and Enabling Vulnerabilities

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

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

Disabling a Vulnerability

1. In the **Vulnerabilities** list, select one or multiple vulnerabilities.

2. In the action menu, click **Disable**.

   Step Result: The vulnerability displays with the **disabled** icon in the status column.

Enabling a Vulnerability

1. In the **Vulnerabilities** list, select a disabled vulnerability.

2. In the action menu, click **Enable**.

   Step Result: The vulnerability displays with the **enabled** icon in the status column.

Using the Scan Now Feature

The Scan Now feature will start a Discover Applicable Updates (DAU) task for the selected devices or device groups. Complete the following steps to use the **Scan Now** Action Menu item.

1. Select one or more devices or device groups (if you do not select a device or device group, the DAU will be scheduled for all devices).

2. Click **Scan Now**.

   Step Result: The *Scan Now* window opens.

Figure 23: Scan Devices

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

   Step Result: The *Scan Now - Success* dialog box appears informing you that the scan has been scheduled and providing a link to view the scheduled deployment.
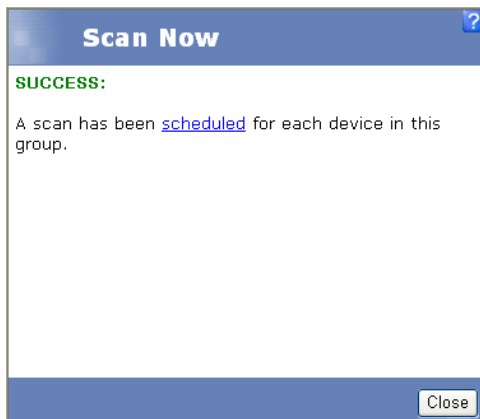
Figure 24: Scan Group Scheduled

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

4. Click **Close**.

   Step Result: The window closes.

Updating the Cache

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

1. On the *Vulnerabilities* page, click **Update View** to display the vulnerabilities that match your filter criteria.

2. Select the vulnerabilities to cache.

3. In the *Action* menu, click **Update Cache**.

   Step Result: The *Warning* dialog box opens informing you that the update request and this action may take an extended period of time.

4. Click **OK**.

About Packages

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

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

1. From the toolbar, select **Vulnerabilities**.

2. in the Vulnerabilities page, select the **Packages** tab.

3. If needed, select filter criteria from the available fields.

4. Select **Update View**.

Step Result: The system displays the existing package list in the *Packages* tab.

Figure 25: Packages Tab

Using the Packages Tab

Click the expand icon to display detailed package information. Select the package name to display the package details.This includes the package deployment information and the package information tabs.
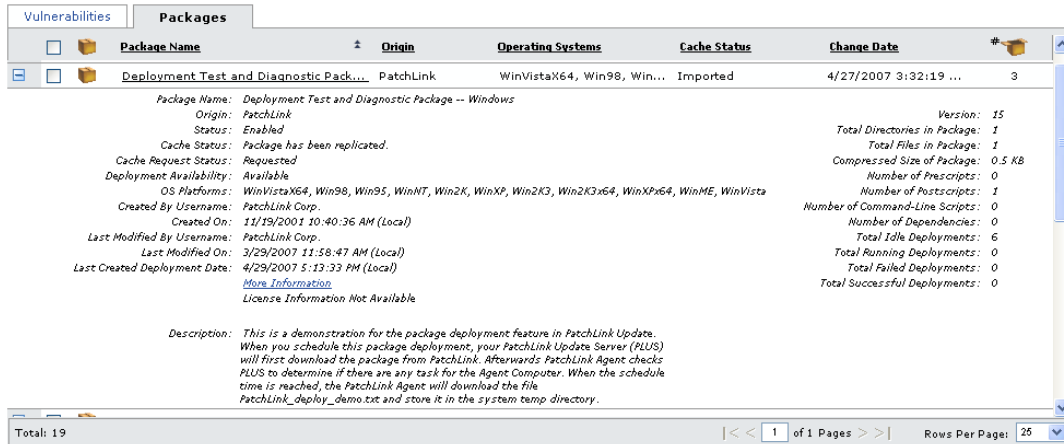
Figure 26: Package Details

The package summary includes the following information:

Table 19: Package Summary Information

Status	Description
Package Name	Title of the package.
Origin	Point of origin of the package. An origin of **Novell** or **System** refers to packages created by Novell.
Status	The current status of the package, stating if the package is enabled and ready to be requested from the Global Subscription Server.
Cache Status	The current cache status of the package. A package is considered cached when it has been downloaded from the Global Subscription Server and actually resides on the local server.
Cache Request Status	Indicates if the package has been requested from the Global Subscription Server.

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

Status	Description
Total Failed Deployments	The number of failed deployments.
Total Successful Deployments	The number of successful deployments.

Package Information Tab

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

Figure 27: Package Details - Package Information Tab

Table 20: Package Information Definitions

Status	Description
Package Information	
Package Name	Title of the package
Status	The current status of the package, stating if the package is enabled and ready to be requested from the Global Subscription Server.
Origin	The origin of the task or which company created the package.
Operating Systems	The operating systems and platforms that the package supports and may be deployed to.
Created By	The user who created the package.

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

Package Statuses and Types

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

Figure 28: Package Status

Package Status and Descriptions

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

Table 21: Package Status and Description

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

Package Icons and Descriptions

The icons and their status are classified as follows:

Table 22: Package Status Icons and Descriptions

New	Current	Tasks	Local	Description
			N/A	The package is not cached.

New	Current	Tasks	Local	Description
			N/A	The package has been scheduled to be cached or is in the process of being cached.
			N/A	An error occurred while trying to cache the package.
				The package is cached and ready for deployment.
				The package is currently deploying (animated icon)
				The package is disabled.

Package Column Definitions

The following table includes descriptions of the package column definitions.

Table 23: Package Column Definitions

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

Searching, Filtering, and Saving Views

ZENworks Patch Management offers options that allow you to search for specific items and filter result sets. Searching and filtering can be performed independent of each other or can be combined to provide drill-down capabilities. Search and filter settings can be saved as the default view displayed on subsequent visits to the page. See *Using Search* on page 29 for additional information.

Working with Packages

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

- *Deploying a Package* on page 63.
- *Creating a Package* on page 64.
- *Editing a Package* on page 64.
- *Deleting a Package* on page 63.
- *Updating the Package Cache* on page 63.

Deploying a Package

Deploying a package is performed similarly to deploying a vulnerability. Deployments are initiated by clicking **Deploy** and completing the Deployment Wizard. The Deployment Wizard provides step-by-step instructions for defining and pushing deployments out to the protected devices in the network. See *Working With Deployments* on page 81 for more information.

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

Deleting a Package

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

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

1. In the *Packages* list, select one or multiple packages.

2. In the action menu, click **Delete**.

   Step Result: The *Warning* dialog box opens, informing you of the expected processing time for the action.

3. Confirm the request to delete the package(s).

   Step Result: The package(s) is deleted from the packages list.

Updating the Package Cache

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

1. In the *Packages* list, select one or multiple packages.

2. In the action menu, click **Update Cache**.

> **Step Result:** The *Warning* dialog box opens, informing you of the expected processing time for the action.

3. Click **OK**.

> **Step Result:** The Package Data is cached.

Editing a Package

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

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

1. In the *Packages* list, select a package.

2. In the action menu, click **Edit**.

> **Step Result:** The package is displayed in the **Edit Packages** dialog box.

3. Make the desired edits and click **OK**.

4. Refer to the *Using the Package Editor* on page 64 for details on changing packages through the Package Editor Wizard.

Creating a Package

Complete the following steps to create a package.

1. In the *Packages* list, click **Create**.

> **Step Result:** The *Welcome to the Package Editor* page opens.

2. Refer to the *Using the Package Editor* on page 64 for details on changing packages through the Package Editor wizard.

Using the Package Editor

Creating distribution packages is performed using the Package Editor wizard.

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

1. In the *Packages* list, click **Create**.

> **Step Result:** The *Welcome to the Package Editor* screen opens.

Welcome to the Package Editor
This wizard will help you create or edit a Package.
With this wizard you will:
Name the Package and provide general information about it.
Associate Operating Systems to the Package.
Define the File list for the Package.
Associate Package Dependencies with this Package.

When clicking next, the Package Editor will be downloaded and installed.
☐ Do not display this page in the future.

[< Back] [Next >] [Cancel]

Figure 29: Package Editor Welcome Screen

2. Click **Next**.

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

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

> **Note:** Deployment options for manual installations of a patch can be included in the **Description** field. See *Including Deployment Options in a Package* on page 73 for more information about using deployment options.

4. Click **Next**.

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

Example:
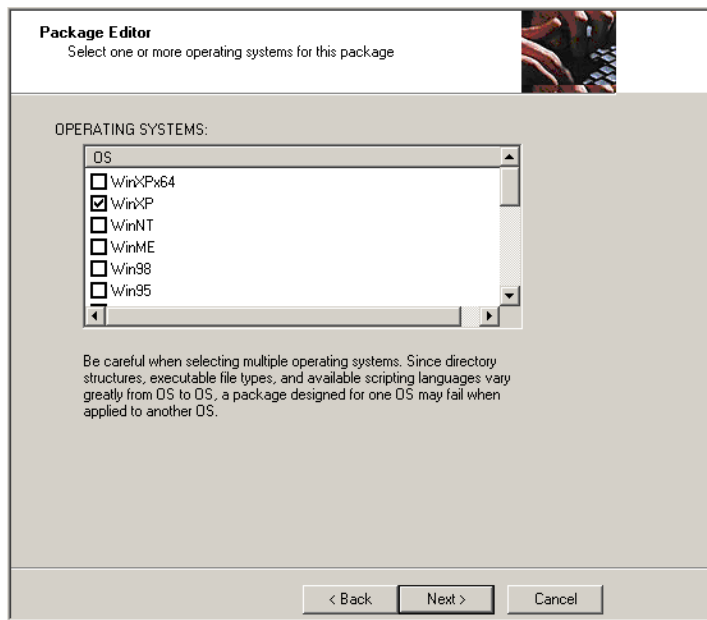
Figure 30: Package Editor - Select Operating System

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

6. Click **Next**.

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

Example:
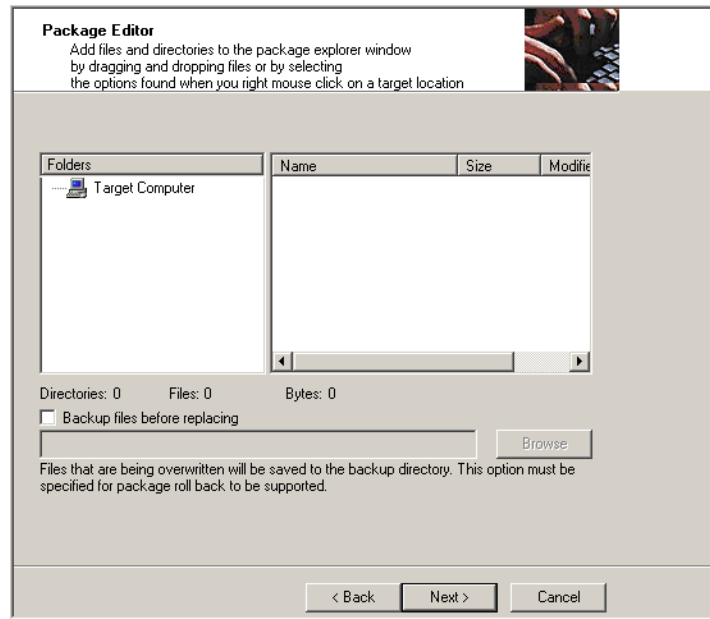
Figure 31: Package Editor - Add Files

Refer to *Adding File and Directories to a Package* on page 75 for additional details regarding adding files to a package.

8. Click **Next**.

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

Example:
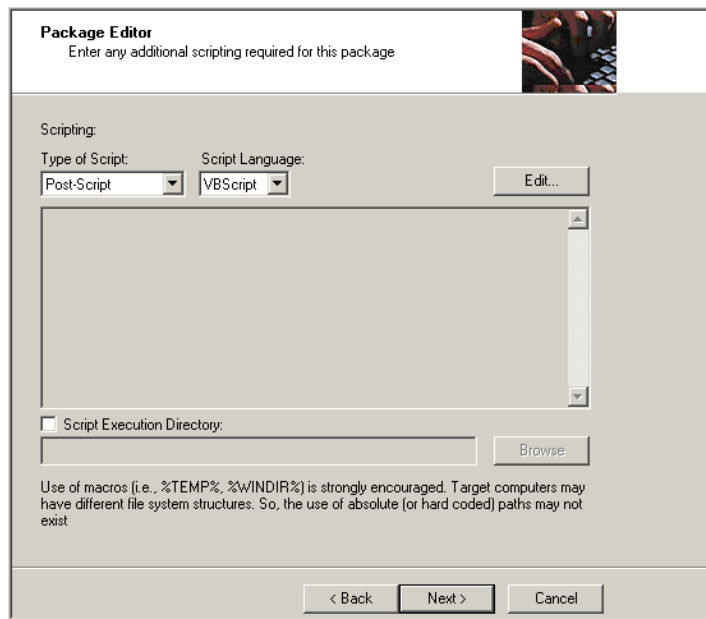
Figure 32: Package Editor - Create Script

Refer to *Creating Scripts for a Package* on page 79 for additional details regarding Package scripts.
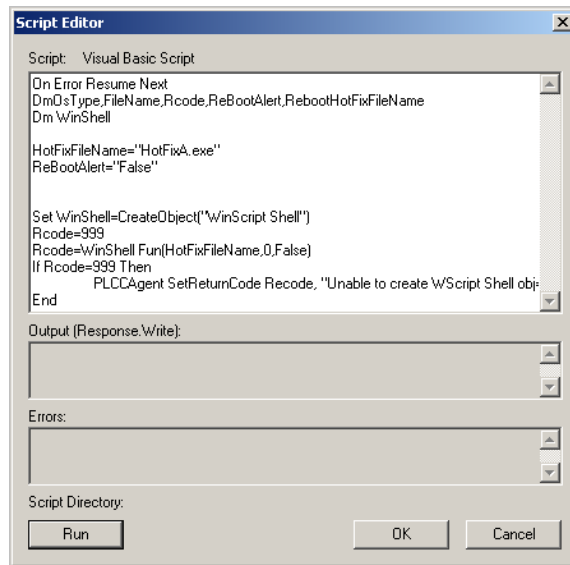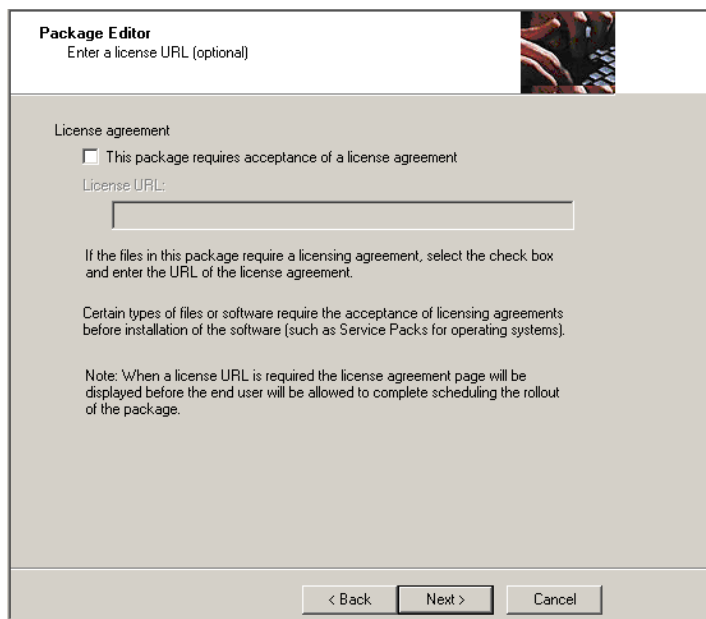
Figure 33: Script Editor

10. Click **Next**.

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

Example:

Figure 34: Package Editor - License URL

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

12. Click **Next**.

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

Example:

Figure 35: Package Editor - Summary

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

14. Click **Next**.

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

> **Step Result:** The *Upload Summary* page opens.
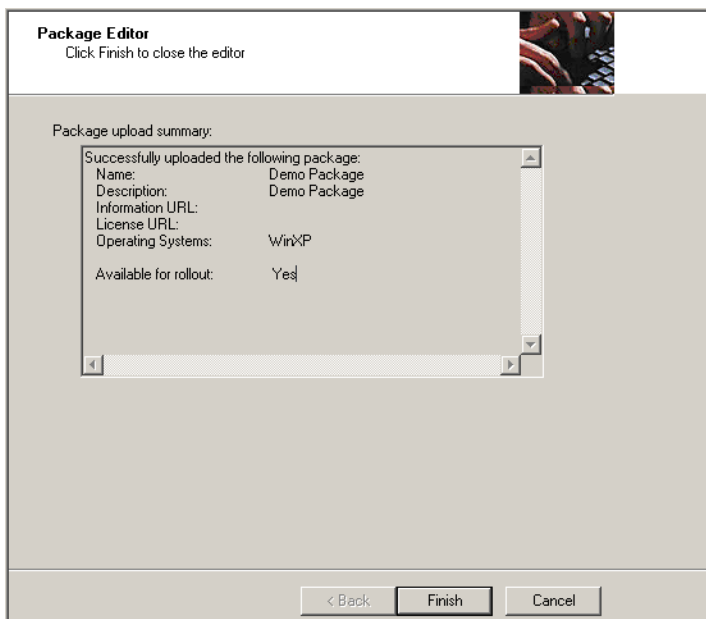
Figure 36: Package Editor - Upload Summary

16. Click **Finish**.

Result: The page refreshes and the *Package* page opens with the custom package. Upon refreshing of the *Packages* page, you can view the package by the name you gave

it, and view the operating systems that you chose to deploy to during the patch building process.

Figure 37: Packages Page - Custom Package

Including Deployment Options in a Package

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

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

A number of additional deployment options are available by including them in with the flags delimiter. To add these, enter *(PLFlags: <Your Flags>)* to the **Description** field. The following table describes the flag behavior and their descriptions.

Table 24: Package Flag Descriptions

Description (flag behavior)	Display Flag	Select Flag
Perform an uninstall; can be used with -m or -q.	-yd	-y
Force other applications to close at shutdown.	-fd	-f
Do not back up files for uninstall.	-nd	-n
Do not restart the computer when the installation is done.	-zd	-z
Use quiet Mode, no user interaction is required.	-qd	-q

Description (flag behavior)	Display Flag	Select Flag
Use unattended Setup mode.	-dmu	-mu
Install in multi-user mode (UNIX, Linux only).	-dsu	-su
Restart service after installation (UNIX, Linux only).	-drestart	-restart
Do not restart service after installation (UNIX, Linux only).	-dnorestart	-norestart
Reconfigure after installation (UNIX, Linux only).	-dreconfig	-reconfig
Do not reconfigure after installation (UNIX, Linux only).	-dnoreconfig	-noreconfig
This package is chainable and will run *Qchain.exe* (Windows) or (UNIX/Linux).	-dc	-c
Suppress the final chained reboot.	-dc	-sc
Repair permissions.	-dr	-r
Deploy only.	-PLD1	-PLD0
No Pop-up	-PLN1	-PLNP
Debug	-PLDG	-PLDEBUG
Suppress Repair	-dsr	-sr
Force the script to reboot when the installation is done.	-1d	-1
Reboot is required.	Not applicable	-2
Reboot may occur.	Not applicable	-3
Reboot is required, and *may* occur.	Not applicable	-4

Adding File and Directories to a Package

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

- *Adding a Directory to a Package* on page 76.
- *Creating a Drive for a Package* on page 77.
- *Adding a New Macro to a Package* on page 75.
- *Creating a Folder for a Package* on page 77.
- *Adding a File to a Package* on page 77.
- *Deleting a File from a Package* on page 78.
- *Renaming a File within a Package* on page 78.
- *File Properties for a Package* on page 79.
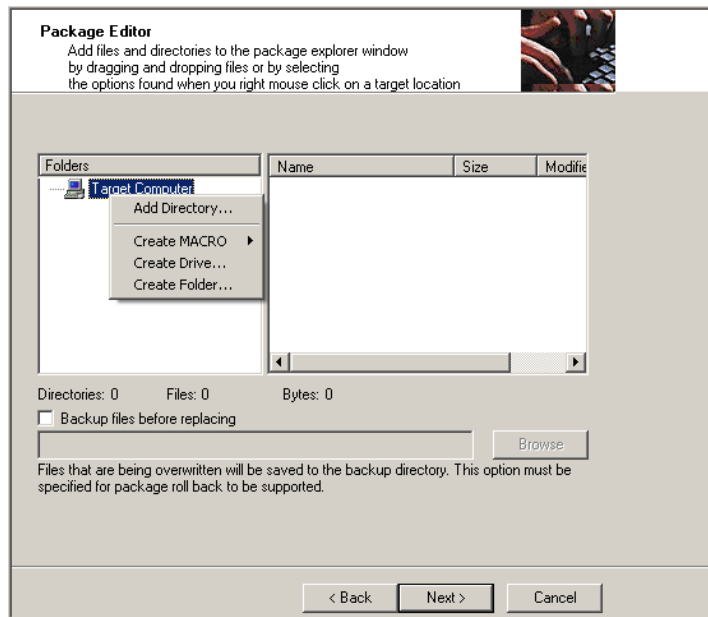
Figure 38: Package Content

Adding a New Macro to a Package

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

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

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

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

1. Right-click inside the *Target Computer* window.

Step Result: The *Add* pop-up window opens.

2. Select **Create Macro** and the macro required for the package.

Step Result: The selected macro displays in the *Target Computer* window.
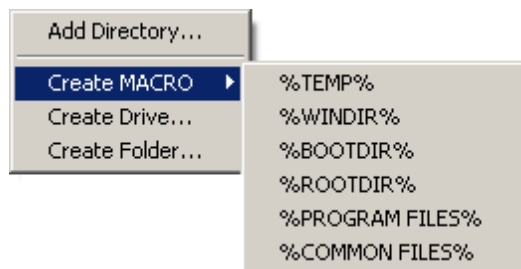
Figure 39: Macro Menu

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

Adding a Directory to a Package

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

1. Right-click the directory, folder, or macro associated with the target computer.

Step Result: The *Add* pop-up window opens.

2. Select **Add Directory**.

Step Result: The *Browse for Folder* window opens.

3. Select the directory to add to the directory, folder, or macro.

4. Click **Open**.

   Step Result: The directory is aded ot the directory, folder, or macro.

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

Creating a Drive for a Package

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

1. Right-click inside the *Target Computer* window.

2. Select **Create Drive** from the pop-up menu.

   Step Result: The *Create Drive* window opens.
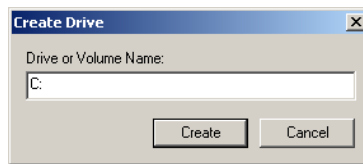
Figure 40: Create Drive

3. In the **Drive** or **Volume Name** field, type the letter you require for the drive name, followed by a colon in *X:* format.

4. Click **OK**.

   Step Result: The drive is added to the *Target Computer* window.

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

Creating a Folder for a Package

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

1. Right-click inside the *Target Computer* window.

2. Select **Create Folder**.

   Step Result: The *Create Folder* window opens.

3. In the **Folder Name** field, type the name of the new folder.

4. Click **OK**.

   Step Result: The folder is added to the *Target Computer* window.

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

Adding a File to a Package

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

1. Right-click the directory, folder, or macro associated with the *Target Computer*.

   Step Result: The *Add* pop-up window opens.

2. Select **Add File**.

   Step Result: The *Open* window opens.

3. Select the file to add to the directory, folder, or macro.

4. Click **Open**.

   Step Result: The file is added to the directory, folder, or macro.

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

Deleting a File from a Package

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

1. Right-click the directory, folder, or macro associated with the *Target Computer* that you want to delete.

   Step Result: The *Add* pop-up window opens.

2. Select **Delete**.

   Step Result: The file is deleted fro the package.

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

Renaming a File within a Package

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

1. In the *Target Computer* directory tree, select the directory where the file is to be renamed

   Step Result: The file is highlighted and the cursor becomes active.

2. Type the new name of the file.

3. Click **OK**.

   Step Result: The folder name is changed and displays in the *Target Computer*.

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

File Properties for a Package

Brings up the properties page for the selected item. Only available when you right click on a file that has previously been added to the Target Computer window.
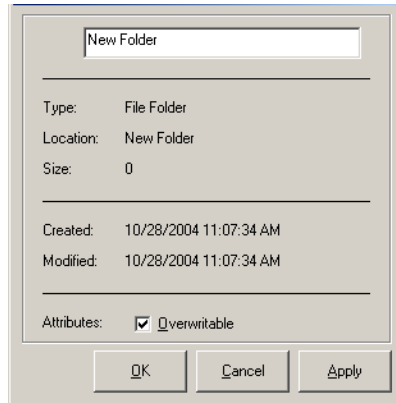
Figure 41: Properties

1. In the *Target Computer* directory tree, select the directory where the file is located.

2. Select the file needed.

3. Right-click the selected file.

4. Select **Properties**.

   Step Result: The *Properties* window opens.

5. In the **Attribute** field, select or deselect the **Overwritable** check box.

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

6. Click **Apply**.

   Step Result: The folder properties are changed.

Creating Scripts for a Package

There are three types of scripts. These scripts can be written in Microsoft Visual Basic Script or Microsoft Jscript. Documentation regarding these languages can be found at the Microsoft scripting web site: *http://msdn2.microsoft.com/en-us/library/ms950396*.

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

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

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

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

1. Select the type of script to execute from the **Type of Script** drop-down list.
2. Select the scripting type from the **Script Language** drop-down list.
3. Click **Edit**.

   Step Result: The *Script Editor* window opens.

4. Type or copy the script to be added in the **Script** field.
5. Click **Run**.

   Step Result: The script is checked and the *Errors* box displays **Success** when the script is validated.

6. Click **OK**.

   Step Result: The *Script Editor* window closes and returns to the *Package Editor* wizard.

7. If needed, select **Script Execution Directory** if a different directory location is required.

   Step Result: The **Script Execution Directory** field becomes active.

8. Type the backup directory path, or click **Browse**.

   Step Result: The location displays in the **Script Execution Directory** field.

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

Chapter

4

Working With Deployments

In this chapter:

- *About Deployments*
- *Using the Deployment Pages*
- *Working With Deployments*
- *Using the Deployment Wizard*

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

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

- *About Deployments* on page 81.
- *Using the Deployment Pages* on page 86.
- *Working With Deployments* on page 90.
- *Using the Deployment Wizard* on page 97.

About Deployments

Several key concepts and status indicators are associated with a deployment. These concepts are used to define deployment behavior.

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

- *Explaining Deployment Distribution Order* on page 95 - the order that the deployment is submitted to target devices.
- *Deployment Types* on page 84 - deployments can be based on vulnerabilities, packages, or a mandatory baseline.
- *Standard and Chained Deployments* on page 85 - deployments are processed as either standard or chained.

Viewing Deployments

You can view Deployments on the following pages:

- Deployments
- Devices
- Vulnerabilities and Packages
- Groups

Viewing All Deployments

1. Select the **Deployments** tab.

> **Step Result:** The *Deployments* page opens.

Figure 42: Deployments Page

2. Select the desired filter criteria.

3. Click **Update View**.

4. Click the expand icon to view the Deployment details.

Viewing Deployments within Devices

1. Select the **Devices** tab.

2. Select your filter options.

3. Click **Update View**.

> **Step Result:** The applicable devices display in the *Devices* page.

4. Select the hyperlink for a device with at least one deployment to view it's details.

> **Step Result:** The *Details by Device* page opens.

5. Select the **Deployments** tab.

> **Step Result:** The *Device Deployments* page opens.

Figure 43: Device Deployments Tab

6. Select the desired deployment, and click the expand icon.

> **Step Result:** The deployment details display.

Figure 44: Device Deployments Tab Expanded

Viewing Deployments within Groups

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

1. In the *Groups* page, select **Deployments** from the **View** drop-down list.

> **Step Result:** The *Deployments* page displays next to the *Group Browser*.

2. Select a group from the directory tree.

> **Step Result:** The selected group is highlighted and displays the assigned deployments.

Figure 45: Group Deployments

Deployment Types

Deployments are created through the *Vulnerabilities*, *Packages*, *Devices*, *Deployments*, or *Groups* pages. On each page, the Deploy command is presented in the Action menu. A different deployment type, Mandatory Baseline, is created by establishing a mandatory baseline for a device group. See *Mandatory Baseline* on page 168 for more information on the mandatory baseline feature.

Vulnerability-based Deployments

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

Package-based Deployments

A package contains all vendor-supplied updates and executable code used to correct or patch security issues for the target devices. The majority of packages are part of specific vulnerabilities, and are deployed to multiple devices within the network. See *About Packages* on page 55 for more information.

Mandatory Baseline Deployments

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

Standard and Chained Deployments

Deployments come in two varieties: Standard Deployments and Chained Deployments. The following sections describe the differences between the two deployment types.

Standard Deployments

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

Chained Deployments

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

Reboot and Chained State

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

Table 25: Reboot and Chained State

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

There are two deployments which will always perform a reboot:

Table 26: Reboot Deployments

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

Standard packages reboot for one of three reasons.

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

Using the Deployment Pages

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

Figure 46: Deployments Page

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

Table 27: Deployments Page Column Descriptions

Column	Description
Name	The name of the main unit containing a group of deployments.
Created Date	The date the initial deployment job was created.
Created by	The user who created the package.
Action	Allows you to Edit or Delete a deployment.
Name	The name of the deployment task. Typically, the name of the Vulnerability or Task deployed.
Scheduled Date	The date the deployment was scheduled to occur.
Deployment Statistics	Refer to *Deployment Statistics* on page 88 for details regarding the Deployment Statistics icons.

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

Figure 47: Device Deployments Page

See *Deployment Status and Type* on page 87 for information on the fields for individual deployments.

Deployment Status and Type

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

Table 28: Deployment Status Options

Status	Description
New	Downloaded from the Global Subscription Server since the last session.

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

Deployment Statistics

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

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

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

The following table defines the status icons:

Table 29: Column Icon Definitions

Icon	Icon Name	Definition
✔	Number of Successful Devices	Total number of devices or groups that finished the deployment successfully.
❌	Number of Failed Devices	Total number of devices or groups that finished the deployment unsuccessfully.
📦#	Number of Devices Assigned to the Deployment	Total number of devices or groups that are assigned the deployment.
📦	Number of In Progress Devices	Total number of devices or groups that are in the process of executing the deployment.
📦✓	Number of Devices That Have Completed the Deployment	Total number of devices or groups that finished the deployment.
%	The Percentage of Completed Devices	Percentage of the devices or groups that finished the deployment. = [Total Finished devices / Total Assigned devices]

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

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

Deployment Details Summary

Expanding (by clicking the expand **>** icon) a deployment will display the deployment details as described in the following table.

Table 30: Deployment Details Summary Fields

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

Working With Deployments

There are several tasks associated with deployments designed to assist you in managing and deploying vulnerabilities. These are available from commands located in the toolbar on the *Deployments* page.

- *Deployments Page* on page 90
- *Viewing Deployment Results* on page 94
- *Explaining Deployment Distribution Order* on page 95
- *Aborting Deployments* on page 95
- *Disabling Deployments* on page 95
- *Enabling Deployments* on page 96
- *Modifying Deployments* on page 96
- *Deleting Deployments* on page 96

Deployments Page

The *Deployments* page illustrates the overall information about all deployment jobs and their associated deployments. This page includes information regarding the assigned devices and groups and the status of the deployment for each.

Figure 48: Deployments Page

The following functions can be performed from the *Deployments* page:

Table 31: Deployment Functions

Menu Item	Function
Enable	Enables the selected disabled deployment.

Menu Item	Function
Disable	Disables the selected enabled deployment.
Abort	Cancels the deployment for any devices which have not already received the deployment package.
Delete	Removes the deployment from your ZENworks Patch Management Server.
Deploy	Re-deploys the selected packages.
Export	The Export button allows you to export subscription data to a comma separated value (*.csv*) file.

Viewing the Deployment Details

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

Figure 49: Deployment Details

The following columns appear on the *Deployment Details* page:

Table 32: Deployment Details Column Definitions

Column	Description
Device Status icon	The status of the device or device group.
Name	Displays the name of the device or device group. The device group name is a link, and clicking the link will display the group membership and individual device results.
Status	The deployments current status.
Last Run Status	The deployments status when last ran. The status is a link, and clicking the link will display the Deployment Results page.

Column	Description
Last Run Start Date	The Date/Time the deployment began.
Last Run Complete Date	The Date/Time the deployment completed.
Next Run Date	The next scheduled start Date/Time for this deployment.

The following page functions are available on the *Deployment Details* page:

Table 33: Deployment Details Page Functions

Button	Function
Enable	Enables the selected disabled deployment assignments. See *Enabling Deployments* on page 96 for additional information.
Disable	Disables the selected enabled deployment assignments. See *Disabling Deployments* on page 95 for additional information.
Export	The Export button allows you to export subscription data to a comma separated value (.CSV) file. See *Exporting Data* on page 33 for additional information.

Viewing Deployment Details by Device

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

The following functions are available on the **Device Deployments** tab:

Table 34: Deployment Tab Functions

Menu Item	Function
Edit	Launches the deployment wizard allowing you to make modifications to the deployment. See *Modifying Deployments* on page 96 for additional information.
Export	The Export button allows you to export subscription data to a comma separated value (.CSV) file. See *Exporting Data* on page 33for additional information.

Viewing Deployment Details by Device Group

Another view of deployments is available through the *Groups* page. This view displays the deployments that the selected group has been assigned. This view is the same as the Deployment Summary view, but displays only deployments for the selected group.
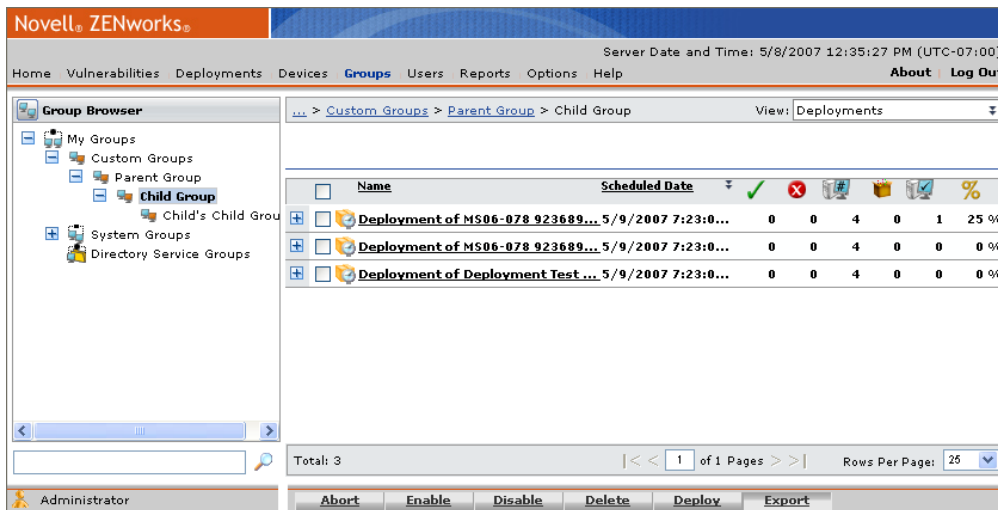
Figure 50: Deployments Page - Groups

The following functions are available on the *Group Deployments* page.

Table 35: Deployment Functions

Menu Item	Function
Enable	Enables the selected disabled deployment.
Disable	Disables the selected enabled deployment.
Abort	Cancels the deployment for any devices which have not already received the deployment package.
Delete	Removes the deployment from your ZENworks Patch Management Server.
Deploy	Re-deploys the selected packages.
Export	The Export button allows you to export subscription data to a comma separated value (*.csv*) file.

Viewing Deployment Results

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

Figure 51: Deployment Results

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

Table 36: Deployment Results Fields

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

Explaining Deployment Distribution Order

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

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

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

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

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

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

Aborting Deployments

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

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

1. Select the deployment you wish to abort.
2. Click **Abort**.

   Step Result: This cancels the selected deployment.

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

Disabling Deployments

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

Note: You cannot disable deployments of System Task Packages.

1. Select the deployment you need to disable.

2. Click **Disable**.

   Step Result: The selected deployment is disabled.

Enabling Deployments

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

1. Select the *disabled* deployment you need to enable.

2. Click **Enable**.

   Step Result: The selected deployment is enabled.

Modifying Deployments

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

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

1. Select the deployment you need to modify.

2. Click **Edit**.

   Step Result: The Deployment Wizard opens, see *Using the Deployment Wizard* on page 97 for additional information.

Deleting Deployments

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

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

1. Select the *disabled* deployment you wish to delete.

2. Click **Delete**.

Explaining Deployment Deadlines

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

Using the Deployment Wizard

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

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

Table 37: Deployment Actions

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

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

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

Introduction Page

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

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

Device / Device Groups Selection Page

The *Available Devices/Groups* page of the *Deployment Wizard* allows for selecting devices and groups to receive a deployment.
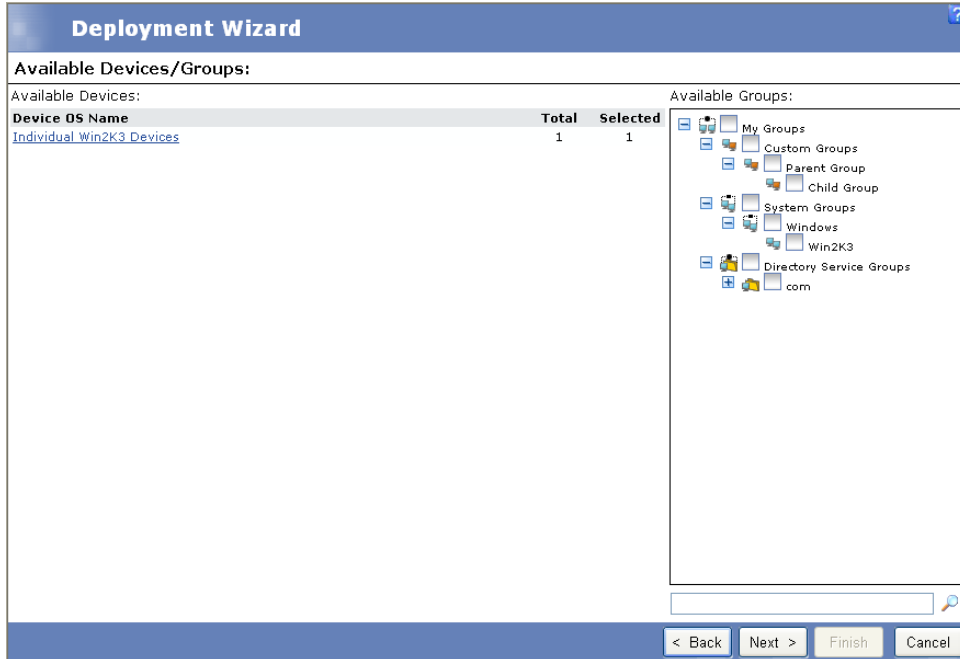
Figure 52: Deployment Wizard - Available Devices/Groups Selection Page

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

To Create a Device Deployment

1. From the **Available Devices** list, select the Device OS Name required.

    Step Result: The list of devices within that operating system display.

2. Select the device from the list.

    Step Result: The device(s) are highlighted.

3. Click **Next**.

Result: The *Package Selection* window opens.

To Create a Group Deployment

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

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

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

2. Click **Next**

Result: The *Package Selection* window opens.

Package Selection Page

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

1. Select the vendor required for the deployment.

   Step Result: The list of associated packages displays in the *Selected Packages* window.
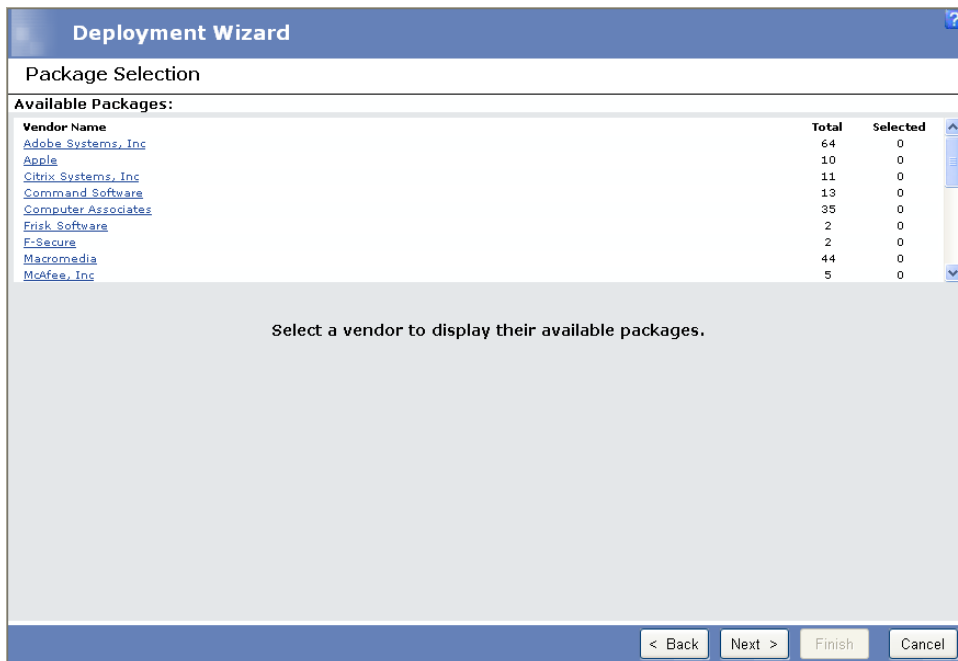
Figure 53: Deployment Wizard - Packages Selection Page

2. Select the packages needed. Click the arrows to page through the available packages, if needed.

   Step Result: The package is selected and highlighted.

   > **Note:** Checking the **Package Name** check box selects all of the packages available in the list.

3. Click the **Package Name** link to open the *Associated Vulnerability Analysis* page.

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

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

Associated Vulnerability Analysis

The *Associated Vulnerability* Analysis page of the Deployment Wizard allows you to view the devices associated with this package and whether their status is **Patched**, **Not-Patched**, or **Not-Applicable** in relation to the selected package.
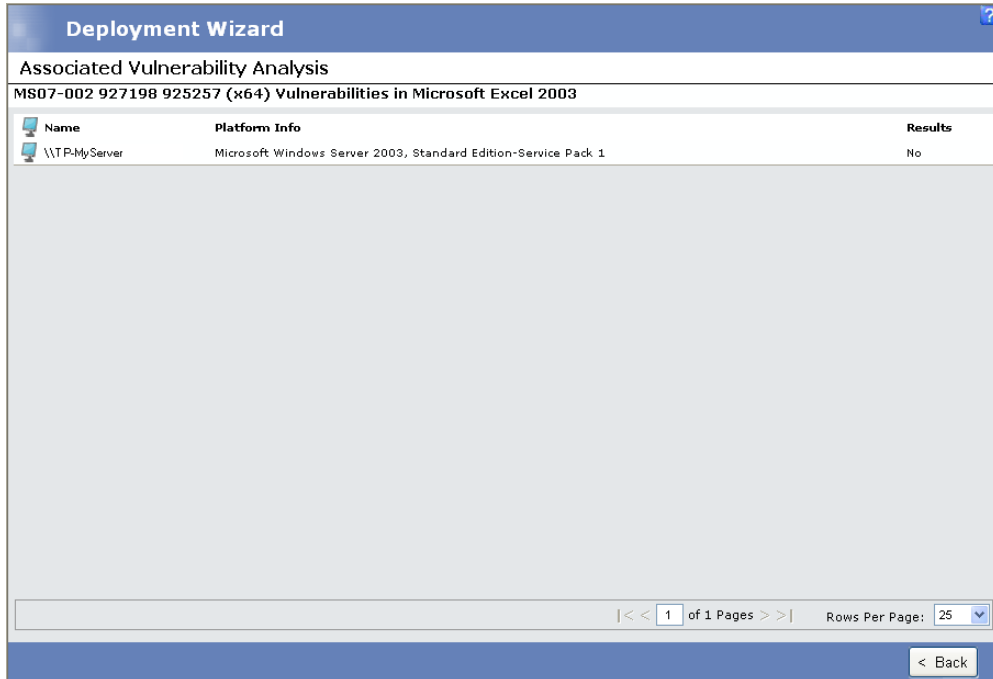
Figure 54: Deployment Wizard - Associated Vulnerability Analysis Page

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

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

Licenses Page

The Licenses page of the Deployment Wizard displays the end user license agreements associated with the vendor packages. Any license agreements displayed on the page must be agreed to prior to continuing the deployment.
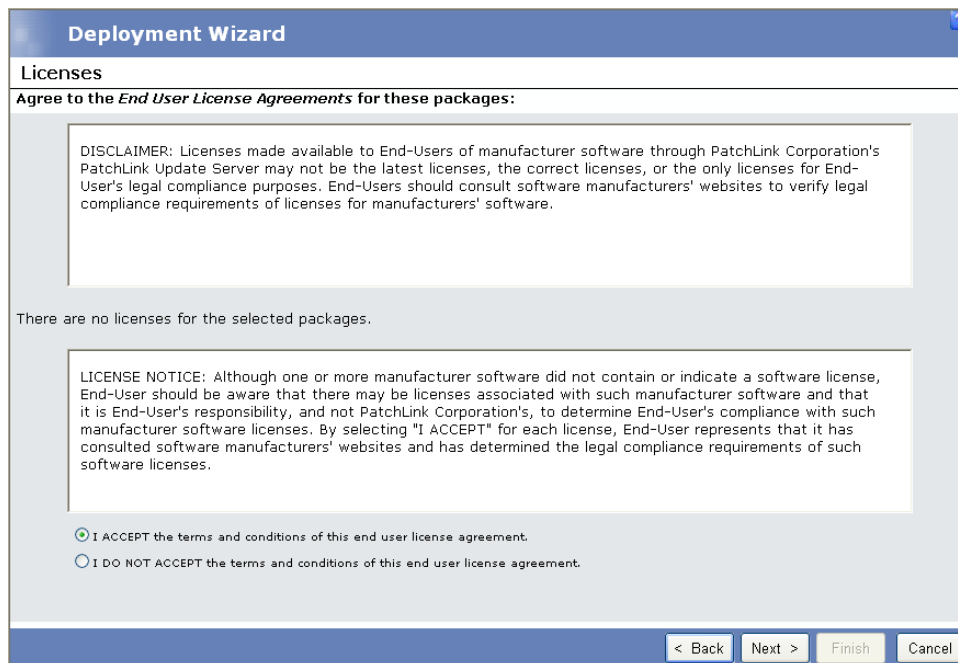
Figure 55: Deployment Wizard - Licenses Page

1. Review the agreement.

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

3. If there are multiple agreements, repeat steps 1 and 2.

   Note: All agreements must be accepted before the deployment wizard can be continued.

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

Deployment Options Page

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

Figure 56: Deployment Wizard - Deployment Options Page

Note: When deploying to an agent at its UTC time, if the agent's time zone is before the server's time zone, the local time of the server will be read, resulting in a possible later deployment to that agent. When using UTC, the time when the agent retrieves the deployment is dependent upon the agent's DAU Communication Interval. If the time zone of the server is before the UTC time, the deployment may be delayed until the server gets to the deployment time.

Table 38: Deployment Options Fields

Field	Description
Job Name	The display name of the deployment job. (Note: This field must not be blank.)
Task Name	The editable display name of the deployment task. The {Package Name} variable will be replaced with the name of the Package included in the task.

Field	Description
Start Time	Displays the Local and UTC times the deployment is scheduled for. Click **Change** to open the *Schedule Configuration* page and modify time options. **Deployment Time Zone** • **Agent Local Time** - Select to deploy based upon the local time of each device. • **Agent UTC Time** - Select to deploy based upon UTC (Coordinated Universal Time). When UTC is used, the deployment will be scheduled for all devices at the same time, regardless of time zone differences.
Manner	• **Concurrent** - Simultaneous distribution to a specified number of devices. New deployments are distributed as agents report back as having completed the previous deployment. If a computer takes longer than four hours to complete the deployment, it is no longer counted against the Concurrent Deployment Limit. • **Consecutive** - Creates and distributes all deployments simultaneously. The global deployment limit will always take precedence over the defined distribution options defined. • **Suspend the deployment of this package, if it fails to deploy to one or more devices** - Suspends all subsequent deployments following any deployment failure. • **Deploy package even if the device has been previously patched** - deploys the package to all selected computers regardless of patch status.
Notes	Allows for notes or comments.

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

Schedule Configuration Page

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

Figure 57: Deployment Wizard - Schedule Configuration Page

To Schedule a One Time Deployment

1. To navigate to the *Deployment Wizard Schedule Configuration* page, from the *Deployment Wizard Deployment Options* page, click the **Change** button located in the Start Time option.

2. Select **One Time**.

   Step Result: The deployment will start on the selected day at the defined time. If a one time deployment is scheduled for a date and time in the past, the agents will start the deployment the next time they contact the ZENworks Patch Management Server.

3. Select **12 hour** or **24 hour** to determine 12 hour format or military 24 hour format.

4. Select the **Hour** needed using the drop-down list.

5. Select the **Minute** between 00 and 59, using the drop-down list.

6. Select **AM** or **PM** using the drop-down list.

7. Click **Next**.

Result: The changes are saved and the *Deployment Options* page opens.

To Schedule a Recurring Deployment

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

Figure 58: Deployment Wizard - Schedule Configuration Page

To Set Up a Daily Recurring Deployment

1. Select **Recurring**.

2. In the **Occurs** field, select **Daily**.

> **Step Result:** The Deployment Wizard displays the **Daily Deployment Options** field.

Figure 59: Daily Option

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

4. Select the frequency of the deployment.

- **Occurs once a day at the scheduled start time** - the deployment starts at the same time as scheduled in the X screen.
- **Occurs every** - the valid options are 1 through 60 if minutes are selected and 1 through 24 if hours are selected.

5. Continue to *Selecting the Deployment Start and End Functions* on page 108.

To Set Up a Weekly Recurring Deployment

1. Select **Recurring**.

2. In the **Occurs** field, select **Weekly**.

> **Step Result:** The Deployment Wizard displays the **Weekly Deployment Options** field.

Figure 60: Weekly Options

3. From the **Every X week(s) on: Mon, Tue, Wed, Thur, Fri, Sat, Sun,** select the deployment to be scheduled every X weeks on the selected days.

4. Continue to *Selecting the Deployment Start and End Functions* on page 108.

To Set Up a Monthly Recurring Deployment

1. Select **Recurring**.

> **Step Result:** The *Recurring Deployment* window opens.

2. In the **Occurs** field, select **Monthly**.

> **Step Result:** The Deployment Wizard displays the **Monthly Deployment Options** fields.

Figure 61: Monthly Options

3. Select the frequency of the deployment:

- **Day X of every X month(s)** - allows the deployment to be scheduled on a specific date every X months. Valid date options are 1 through 31, with the ability to choose 1 through 99 months.
- **The Xth Weekday of every X month(s)** - allows the deployment to be run on a specific day every X months. The valid day options are: 1st, 2nd, 3rd, 4th, or Last, weekday options are: Sunday through Saturday, Day, Week day, or Weekend day and monthly recurrence options are: 1 through 99 months.

Figure 62: Common Deployment Options

4. Continue to

Selecting the Deployment Start and End Functions

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

Table 39: Deployment Start and End Functions

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

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

Package Deployment Order and Behavior Page

The *Package Deployment Order and Behavior* page of the Deployment Wizard, allows you to set the order and behavior for the individual package deployments.
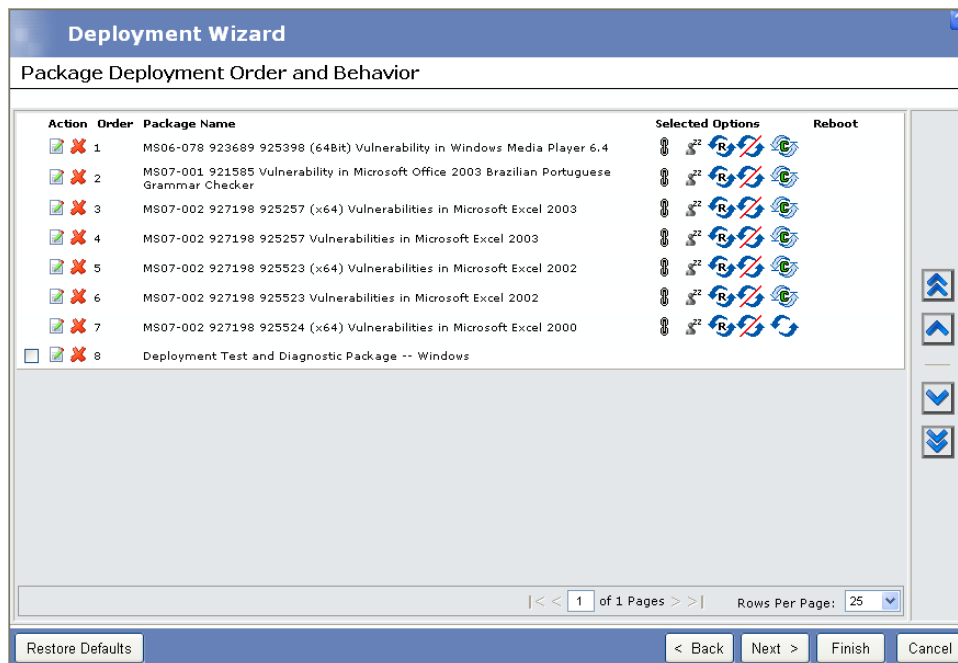
Figure 63: Deployment Wizard - Package Deployment Order and Behavior Page

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

Table 40: Deployment Order Functions

Icon	Action	Use To
	Edit	Open the *Package Deployment Behavior Options* page and change the behavior options for that package.
	Delete	Remove the package from the deployment.
	Selected Options	View the behavior of each package. *Behavior Icon Definitions* on page 111.
	Reboot	View the reboot settings of each package. *Reboot Icon Definitions* on page 113.

Icon	Action	Use To
	Move to top	Move the package to the top of all non-chained deployments (this will place it immediately after the chained deployments).
	Move up one line	Move the package up one.
	Move down one line	Move the package down one.
	Move to bottom	Move the package to the bottom of the listing.
Restore Defaults	Restore defaults	Restore the package order and behavior back to their default settings.

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

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

Behavior Icon Definitions

The following table describes the deployment behavior icons and their descriptions:

Table 41: Behavior Icon Definitions

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

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

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

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

Reboot Icon Definitions

The following table describes the Reboot icons and their descriptions:

Table 42: Reboot Icon Definitions

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

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

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

Package Deployment Behavior Options Page

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

Figure 64: Behavior Options

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

Modifying Behavior Options

To modify the package behavior options.

1. In the *Behavior Options* page, review the pre-selected options.

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

2. Select or deselect the checkbox next to the option to enable or disable the behavior.

3. Click **Next**.

Result: The updated behavior options are saved and the *Notification Options* page opens.

Behavior Icon Definitions

The following table describes the deployment behavior icons and their descriptions:

Table 43: Behavior Icon Definitions

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

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

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

Optional Package Flags

This is an area for any extra package flags unique to a particular deployment. In addition to flags specific to the package being deployed.

Package Flag Descriptions

The following table defines flag behavior and their descriptions:

Table 44: Package Flag Descriptions

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

Package Display Options

Table 45: Package Display Options

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

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

Notification Options Page

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

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

Figure 65: Deployment Wizard - Notification Options Page

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

Table 46: Use Policies - Deployment

Option	When Used
Use Policies	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	There will be no user notification of this deployment, and the deployment will occur automatically. Selection of this option disables all other (except Use Policies) deployment notification options.
Notify users of this deployment	The user will be notified prior to the installation of this deployment.
Message	This field contains the message the user will see when notified about this deployment. The {%Package_Name%} variable will be replaced with the Package Name, allowing you to enter custom text before or after the package name.

Deployment Permissions

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

Table 47: Use Policies - Deployment

Option	Use To
Allow User to Cancel	Define if the recipient can cancel the deployment.
Allow User to Snooze	Define if the recipient can snooze the deployment.
Notification on Top	Define if the Desktop Deployment Manager will display on top of all other applications.
Deadline Offset	Allows you to set a custom deadline offset, or custom deadline date for the deployment. • **From Deployment Start** - Sets the deployment deadline to be X Minutes, Hours, or Days from deployment start date/time. • **Specific Date** - Sets the deployment deadline to a specific date and time.

Reboot Notification Options

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

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

Table 48: Use Policies - Reboot

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

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

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

Deployment Confirmation Page

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

Figure 66: Deployment Confirmation Page

Deployment Confirmation Summary

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

Table 49: Deployment Confirmation Summary Options

Summary Item	Description
Job Name	The name given the deployment job defined in the *Deployment Options* page.
Schedule	The schedule for the deployment defined in the *Deployment Options* page.
Manner	Whether these deployments are Sequential or Parallel, and if Sequential, how many deployments will be distributed at once.

Summary Item	Description
Deployment Notification	Whether or not the users will receive 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 Devices / Groups	If the deployment is a group deployment, the number of groups selected. If the deployment is for individual devices, the total number of devices selected.
Notes	Who created the deployments, and when they were created.

Selected Packages

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

Table 50: Select Packages Column Descriptions

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

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

Associated Vulnerability Analysis Page

The Associated Vulnerability Analysis page of the Deployment Wizard allows you to view the devices targeted for the deployment, and if they are patched for the selected vulnerabilities.
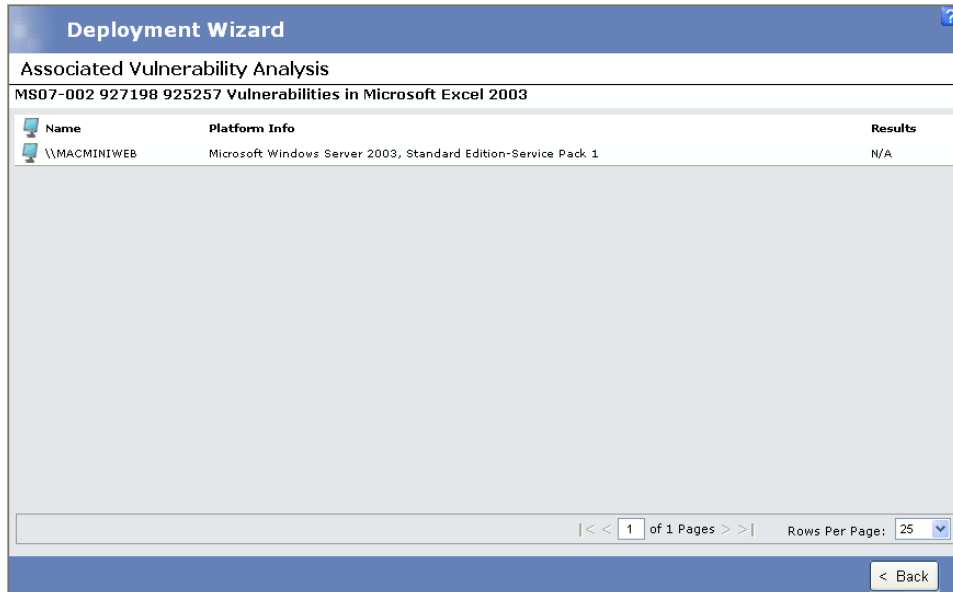
Figure 67: Deployment Wizard - Associated Vulnerability Analysis Page

The following table describes the fields and their descriptions.

Table 51: Associated Vulnerability Analysis Fields

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

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

Deployment Summary Page

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

Figure 68: Deployment Wizard - Deployment Summary Page

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

Table 52: Deployment Summary Items

Summary Item	Description
Job Name	The name given the deployments defined in the *Deployment Options* page.
Schedule	The schedule for the deployments defined in the *Deployment Options* page.
Manner	Sequential or Parallel deployment 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 receive a deployment notification.
Reboot Notification	If the deployments must reboot, whether or not the users will receive a reboot notification.
Total Selected Packages	The total number of packages selected for deployment.

Summary Item	Description
Total Selected Computers / Groups	If the deployment is a group deployment, the number of groups selected. If the deployment is for individual devices, the total number of devices selected.
Notes	When the deployments were created and who created them.

Selected Packages

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

Table 53: Select Packages Column Descriptions

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

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

Chapter
5

Using Devices and Inventory

In this chapter:

- *About Devices*
- *Working with Devices*
- *About Inventory*
- *Using the Inventory Tab*
- *Scanning Inventory*
- *Using Custom Inventory*

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

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

About Devices

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

- Device Name
- IP Address
- Status
- Operating system information (OS Info)
- Version

Figure 69: Devices page

Viewing Devices

1. Select the **Devices** tab.

2. Select your filter options.

3. Click **Update View**.

   Step Result: The *Devices* page displays the devices which match the selected filter options.

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

Using the Devices Page

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

Figure 70: Devices page

The following table describes the fields within the *Devices* page.

Table 54: Devices page columns

Column	Description
Device Name	The name of the device as extracted from system data and inventory. Selecting the device name displays the *Device Details* page. The displayed devices can be determined by the filter criteria defined in the search section.

Column	Description
IP Address	The IP address of the device ascertained during the discovery and initial communication with the agent installed on the device.
Status	The status of the device. Status values include: *Detecting*, *Disabled*, *Idle*, *Offline*, *Sleeping*, *Working*, and *Unknown*.
OS Info	Additional information about the operating system the device is running.
Version	The version number of the agent installed on the device.

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

Table 55: Devices action menu

Menu Item	Description
Install	Select this option to install an agent to a device.
Enable	Select this option to enabled a disabled device.
Disable	Select this option to inactivate an agent on a device.
Delete	Select this option to delete a disabled device.
Deploy	Select this option to deploy to a selected device.
Export	Retrieves all device information and allows for saving to a *.csv* file. See *Exporting Data* on page 33 for additional information.
Scan Now	Prompts the Discover Applicable Updates task to check the device. See *Using the Scan Now Feature* on page 53 for additional information.
Reboot Now	Prompts the selected device to reboot. See *Rebooting Devices* on page 142 for additional information.

Device Status Icons

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

Table 56: Device Status Icons

Active	Pending	Description
	N/A	The agent is currently working on a deployment (animated icon).

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

Using the Details by Device Page

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

Figure 71: Endpoint Details page

Device Information Tab

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

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

Table 57: Action Menu

Menu Item	Description
Export	Retrieves all device information and allows for saving to a .CSV file. See *Exporting Data* on page 33 for additional information.
Scan Now	Prompts the DAU to immediately check the device. See *Using the Scan Now Feature* on page 53 for additional information.
Reboot Now	Prompts the selected device to reboot. See *Rebooting Devices* on page 142 for additional information.

Device Information Section

The Device Information section displays the following device data:

Figure 72: Device Information

Table 58: Device Information Field Descriptions

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

Agent Information Section

The Agent Information section displays the following agent data:

Figure 73: Agent Information

Table 59: Agent Information Field Descriptions

Field	Description
Agent Installation Date	The date the agent registered with Patch Management Server. This is typically the date the agent was installed on the device.
Agent Version	The agent version number.
Agent Status	The status of the agent. Also shown on the *Devices* page.
Last Connected Date	The date the agent last communicated with Patch Management Server.

Group Information Section

The Group Information section displays the following group data:

Figure 74: Group Information
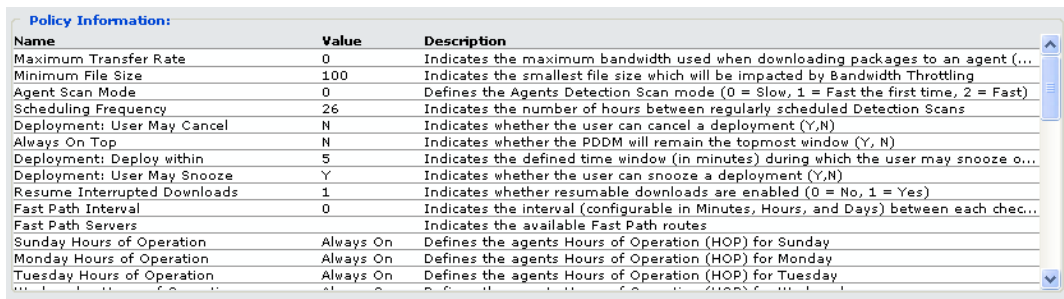
Table 60: Group Information section field descriptions

Field	Description
Group Name	The name of the group(s) that the device is a member. Click the name to go to the *Group Information* page.
Originating Group	The name of the parent group that the device is a member. Click the name to go to the *Group Assessment* page.
Type	The group type. Can be a system created groups (OS), directory service, or custom group.

Field	Description
Deployments Applicable	Indicates if there are applicable deployments available for this device.
Added By	The ZENworks Patch Management user who added the device to the group. System created groups indicate Novell Corp. in this field.
Added On	The date and time that the device was added to the group.

Policy Information Section

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

Figure 75: Policy Information

Table 61: Policy Information Field Descriptions

Field	Description
Name	The name of the policy assigned to the device. Because a device must have all policy values defined, every policy is listed here.
Value	The assigned value of the policy as determined by applying each of the policies defined by the device's group membership, applying conflict resolution when applicable, and filling in any undefined policies from the Global Policy. See *Working With Agent Policy Sets* on page 264 for additional information.
Description	The description of the policy assigned to the device.

Device Vulnerabilities

The **Device Vulnerabilities** tab displays vulnerability information associated with the selected device. The page displays the same information as is presented in the *Vulnerabilities* page.

Figure 76: Device Vulnerabilities

The following table describes the Action menu functions used in the Device Vulnerabilities page:

Table 62: Devices action menu

Menu Item	Description
Enable	Select this option to enabled a disabled device.
Disable	Select this option to inactivate an agent on a device.
Update Cache	Downloads packages and vulnerabilities required by the device.
Deploy	Select this option to deploy to a selected device.
Scan Now	Prompts the Discover Applicable Updates task to immediately check the device. See *Using the Scan Now Feature* on page 53 for additional information.
Reboot Now	Prompts the selected device to reboot. See *Rebooting Devices* on page 142 for additional information.
Export	Retrieves all device information and allows for saving to a *.csv* file. See *Exporting Data* on page 33 for additional information.

Device Inventory

The **Inventory** tab displays the inventory information for the selected device. The page displays the same information as is presented in the *Inventory* page. For details on using this page, see *About Inventory* on page 143.
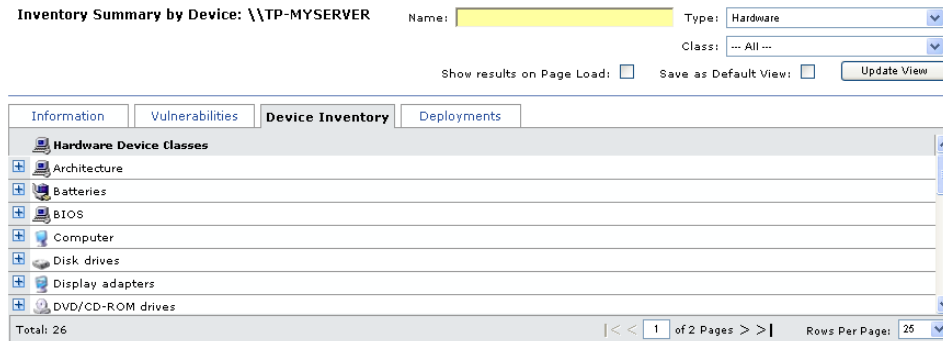
Figure 77: Device Inventory

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

Table 63: Action Menu

Menu Item	Description
Export	Retrieves all device information and allows for saving to a *.csv* file. See *Exporting Data* on page 33 for additional information.
Scan Now	Prompts the DAU to immediately check the device. See *Using the Scan Now Feature* on page 53 for additional information.

Device Deployments

The *Device Deployments* page displays all of the deployments that the device has been associated with or assigned. The page displays the same information as is presented in the Deployments section in the *Vulnerabilities* page.

Figure 78: Device Deployments

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

Table 64: Device Deployments Action Menu

Menu Item	Description
Export	Retrieves all device information and allows for saving to a *.csv* file. *Exporting Data* on page 33

Working with Devices

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

- *Installing an Agent* on page 138.
- *Viewing Device Details* on page 140.
- *Enabling a Device* on page 141.
- *Disabling a Device* on page 140.
- *Deleting a Device* on page 141.
- *Deploying a Vulnerability* on page 141.
- *Exporting Device Information* on page 141.
- *Scanning Devices* on page 142.
- *Rebooting Devices* on page 142.

Installing an Agent

Click **Install** to display the list of agent installers that can be used to register devices to Patch Management Server. When launching the Agent Installers dialog box, the behavior is the same

whether a device is selected or not. Refer to the *ZENworks Patch Management Server 6.4 SP2 Agent Install Guide* for complete instructions regarding the installation of agents.

Figure 79: Agent Installer Page

Viewing Device Details

View details of a specific device by selecting the desired device and clicking the device name. The *Device Details* page is described in *Using the Details by Device Page* on page 132.

Figure 80: Device Details page

Disabling a Device

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

1. In the **Devices** list, select one or multiple devices.

2. In the Action menu, click **Disable**.

> **Step Result:** A *Disable Confirmation* dialog displays.

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

> **Step Result:** The device is displayed in the list of devices identified with the disabled icon in the status column.

Result: After disabling a device, the device can be deleted from Patch Management Server.

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

Deleting a Device

1. In the **Devices** list, select one or multiple disabled devices.

2. In the Action menu, click **Delete**.

> **Step Result:** A *Delete Confirmation* dialog displays.

3. Click **OK** confirming the deletion.

> **Step Result:** The device is deleted from the **Devices** list.

Enabling a Device

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

1. In the **Devices** list, select one or multiple disabled devices.

2. In the **Action** menu, click **Enable**.

> **Step Result:** The device is enabled.

Deploying a Vulnerability

Deploying a vulnerability to selected devices is a key function of the Patch Management Server. Deployments are initiated by clicking **Deploy**. See *Using the Deployment Wizard* on page 97 for additional information.

Note: The **Deploy** command is not exclusive to a selected device and results in the same action whether selected from the *Devices* or *Vulnerabilities* page.

Exporting Device Information

The export utility lets you export device information to a comma-separated value (*.csv*) file format. See *Exporting Data* on page 33 for additional information.

Scanning Devices

The **Scan Now** utility lets you scan a device immediately via the Discover Applicable Updates (DAU) task. See *Using the Scan Now Feature* on page 53 for additional information.

Rebooting Devices

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

1. In the *Devices* page, select one or multiple devices.

2. Click **Reboot Now**.

    Step Result: The *Reboot Device Warning* dialog box opens.
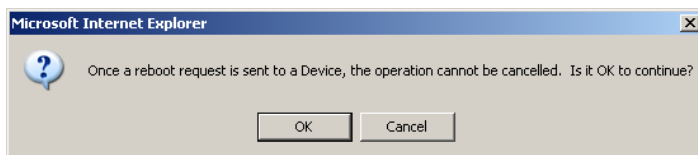
Figure 81: Reboot Device Warning

3. In the *Reboot Device Warning* dialog box, click **OK**.

    Step Result: The *Reboot Now* window opens.

Figure 82: Reboot Now

4. Confirm the reboot, and select **Yes, Reboot the selected device**.

5. Click **Reboot**.

    Step Result: The system schedules the reboot and the *Reboot Success* window opens.
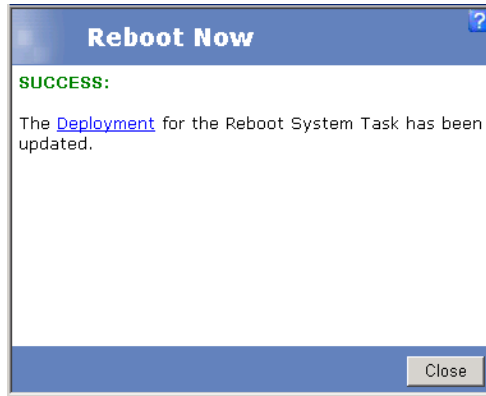
Figure 83: Reboot Device Success Screen

6. Click **Close**.

    Step Result: The window closes.

About Inventory

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

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

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

Viewing Inventory

1. Select **Devices**.

    Step Result: The Devices page displays.

2. Select the **Inventory** tab.
3. Select your filter options.
4. Click **Update View**.

    Step Result: The inventory results display.

5. Click the expand icon to view the details of a particular Inventory class.

Using the Inventory Tab

The *Inventory* Tab displays a list of each inventory type and the associated devices. The devices that have the selected operating systems, hardware, software, and services installed can be viewed by clicking the expand icon.
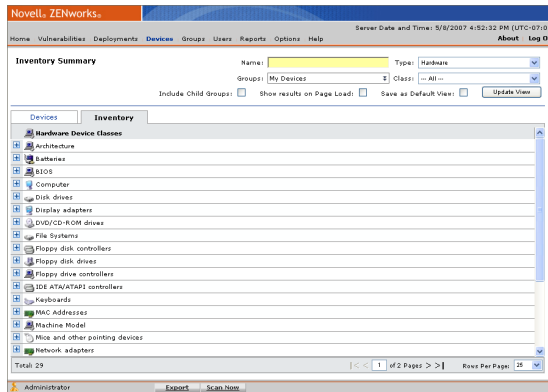
Figure 84: Inventory Tab

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

Table 65: Action Menu

Menu Item	Description
Export	Retrieves all device information and allows for saving to a *.csv* file. See *Exporting Data* on page 33 for additional information.
Scan Now	Prompts the Discover Applicable Updates task (DAU) to immediately check the device. See *Using the Scan Now Feature* on page 53 for additional information.

Inventory Types

The ZENworks Patch Management supports filtering by the following inventory types and views:

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

Inventory Type	Description
Software	Displays the software applications detected on agents. This view displays the name of the software application and the number of instances detected.
	Note: Windows NT reports some software as hardware resulting in displaying within the hardware inventory.
Hardware	Displays the software applications detected on agents. This view displays the name of the software application and the number of instances detected.
	Note: Windows NT reports some software as hardware resulting in displaying within the hardware inventory.
Services	Displays the software applications detected on agents. This view displays the name of the software application and the number of instances detected.

Scanning Inventory

In addition to determining security risks and other vulnerabilities, the Discover Applicable Updates (DAU) task also identifies the device inventory. Each time the DAU runs, the current inventory is compared against the *<Program Files>\Novell \ZENworks Patch Management Agent\localprofile.txt* file. If any changes exist, a differential report is uploaded to the Patch Management Server. The following is an example local profile file (*localprofile.txt*).

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

```
          </devices>
          <software>
             <package>ZENworks Patch Management Agent</package>
          </software>
       </systemprofile>
```

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

Manually Scheduling the DAU Task

The Discover Applicable Updates (DAU) task can be scheduled for immediate execution by selecting the **Scan Now** option. See *Using the Scan Now Feature* on page 53 for additional information.

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

Using Custom Inventory

To use a custom inventory file, you must create the custom inventory file in XML and distribute it to each agent. There is no automated distribution method for custom inventory.

Each agent must have a local file named *CustomInventory.xml* in *<Program Files>\Novell \ZENworks Patch Management Agent* (for Windows Agents) or *patchagent/update* (for Linux/ Unix/Mac Agents).

Guidelines for Microsoft Windows based Operating Systems

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

Literal

> Allows the user to assign an actual text value type into XML.
>
> The string added will be of the form "name = value" where name is the tag name, and value is the literal typed between the open and close tags.
>
> Example XML: (This example will return the string value defined between the open and close tags)

```
<item class="User Defined" name="Example Name" type
="Literal">ZENworks Patch Management 6.4 SP2 Custom Inventory</
item>
```

Returns:

```
"Example Name = ZENworks Patch Management 6.4 SP2 Custom
Inventory"
```

Registry

Allows the user to retrieve the registry key value.

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

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

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

Returns:

```
"Registry Example= <Program Files>\Novell
\ZENworks Patch Management Agent\CustomInventory.xml"
```

Environment

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

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

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

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

Returns:

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

WMI

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

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

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

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

Returns:

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

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

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

Returns:

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

Text_File

Allows the user to retrieve text data from a file.

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

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

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

Returns:

"Line 1 = This is line one"

"Line 2 = This is line two"

XML_File

Allows the user to retrieve text data from a file.

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

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

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

Returns:

"Asset = PLA001"

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

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

Returns:

"Building = Scottsdale-Main"

Where the SampleXML.xml file is as follows:

```
<?xml version="1.0" encoding="utf-8"?>
  <Top><Inventory>
```

```
        <AssetNumber>PLA001</AssetNumber>
        <Location>Scottsdale-Main</Location>
    </Inventory></Top>
```

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

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

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

```
Building = MainLocation = Scottsdale, AZDivision = Corporate
```

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

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

Guidelines for Linux/Unix/Mac based Operating Systems

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

Literal

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

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

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

```
<item class="User Defined" name="Example Name" type
="Literal">ZENworks Patch Management 6.4 SP2 Custom Inventory</
item>
```

Returns:

> "Example Name = ZENworks Patch Management 6.4 SP2
> Custom Inventory"

Dynamic

Allows the user to search using a script.

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

Example XML:

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

Returns:

"ZENworks Patch Management Disk Usage = 18.1 (in kb)"

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

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

Chapter

6

Using Groups

In this chapter:

- *To View Groups*
- *To Search for a Group*
- *Groups and the Directory Tree*
- *Group Information*
- *Group Membership*
- *Device Membership*
- *Mandatory Baseline*
- *Device Group Vulnerabilities*
- *Device Group Inventory*
- *Device Group Deployments*
- *Device Group Policies*
- *Device Group Roles*
- *Device Group Dashboard*
- *Device Group Settings*

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

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

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

To View Groups

The following procedure shows how to display a group.

1. Select **Groups**.

   Step Result: The *Groups* main page displays in the window.
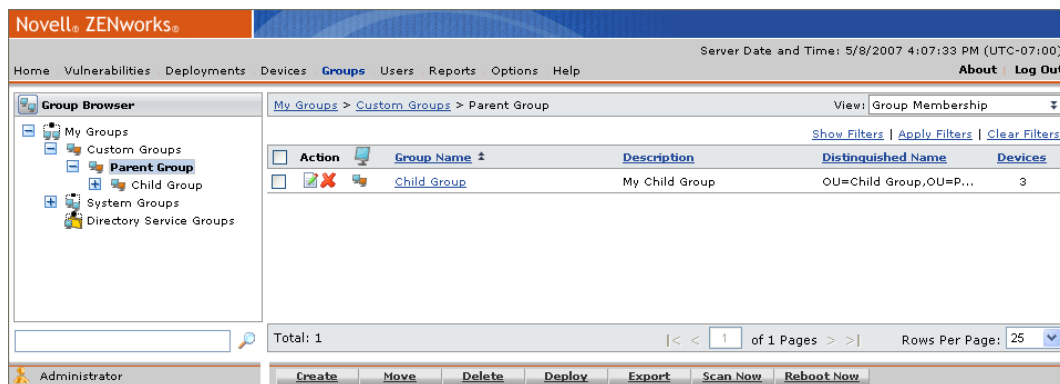
Figure 85: Groups Page

2. Select a group type from the directory tree.

   Step Result: The selected group's information displays in the *Groups* window.

3. Select the function you need from the **View** drop-down list.

Result: The applicable function displays on the *Groups* page.

To Search for a Group

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

1. Select **Groups**.

   Step Result: The *Groups* main page displays in the window.

2. In the **Group Browser** search field, type your search criteria.

   Step Result: The results for your search appear below the **Group Browser** field as you type.

3. Click the desired **Group** link.

Result: Information for the selected group appears on the *Groups* page.

Groups and the Directory Tree

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

Parent and Child Groups

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

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

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

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

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

Defining Groups

Groups can be categorized into the following classifications:

Table 66: Group Definitions

Icon	Group Type	Definition
	Parent System Groups	Devices identified in your network are automatically assigned a group membership based on their operating system, Active Directory membership, IP Address, or Virtualization status/type. Not all operating systems, AD Groups, IP Ranges, and VMs may be shown. This is because Patch Management Server creates system groups based upon those devices present in your network. You cannot modify System Groups or their hierarchies.
	System Groups	

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

Group Information

The *Information* view displays general group-related information concerning the group's membership, hierarchy, policies, roles, mandatory baselines, and other settings.
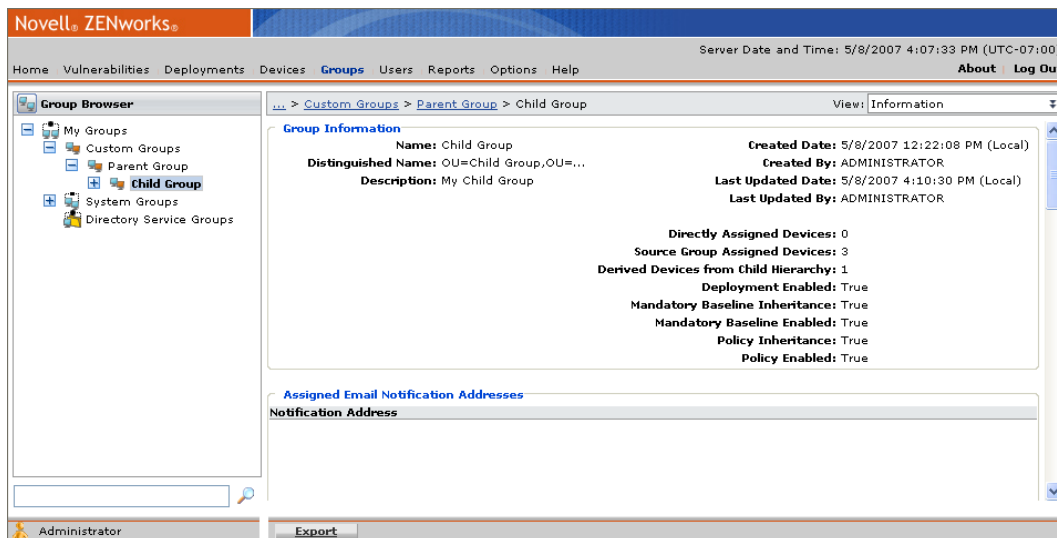
Figure 86: Group Information

The following table describes the button functions in the *Information* view.

Table 67: Group Information Button

Action	Description
Export	Retrieves all page information and allows for saving to a *.csv* file. See *Exporting Data* on page 33 for additional information.

Group Information Settings

Group Information, a section within the *Groups* page **Information** view, lists the following data:

Table 68: Group Information Settings

Field	Description
Name	The name of the group.
Distinguished Name	System-created name based upon the group's parent hierarchy.
Description	Description of the group.
Created Date	The date and time the group was created.
Created By	The user who created the group.
Last Update Date	The date and time the group was last modified.
Last Updated By	The user who last modified the group.
Directly Assigned Devices	Number of devices assigned to the group. Does not include inherited devices.
Source Group Assigned Devices	The number of devices assigned to the source group. See *Assign a Source Group to a Custom Group* on page 190 for more information on Source Groups.
Derived Devices from Child Hierarchy	The number of devices inherited from child groups.
Deployment Enabled	When set to *True*, deployments can be created for the group.
Mandatory Baseline Inheritance	When set to *True*, Mandatory Baseline settings are inherited from the group's parent.
Mandatory Baseline Enabled	When set to *True*, Mandatory Baseline deployments are create based upon the group's Mandatory Baseline configuration.
Policy Inheritance	When set to *True*, policy sets are inherited from the group's parent.
Policy Enabled	When set to *True*, policy sets can be assigned to the group.

Assigned Email Notification Addresses

Assigned Email Notification Addresses, a section within the **Information** view, lists the following data:

Notification Address	The e-mail addresses that will receive group specific notifications.

Assigned Child Groups

Assigned Child Groups, a section in the **Information** view, lists the group's direct children groups.

Table 69: Group Section

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

Assigned Mandatory Baseline Items

The **Assigned Mandatory Baseline Items** list the vulnerabilities defined in the group's mandatory baseline.

Table 70: Assigned Mandatory Baseline Items

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

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

Assigned Policy Sets

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

Table 71: Assigned Policy Sets

Field	Description
Policy Set Name	The name of the policy set.

Field	Description
Assigned	Indicates if the policy set is assigned to or inherited by the group. A value of *True* indicates the policy is assigned directly to the group.

Resultant Policy Information

Resultant Policy Information, a section in the **Information** view, displays the results of the assigned or inherited policy sets and provides the following data:

Table 72: Resultant Policy Information

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

Note: Only those policies that are directly assigned or inherited are displayed in the group's *Resultant Policy Information* section. To see a complete listing of all policies assigned to an agent, refer to the

Assigned Roles

Assigned Roles, a section in the **Information** view, displays all the roles that have access to the group.

Table 73: The Assigned Roles section

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

Group Membership

The *Group Membership* view allows the user to see the group's direct child groups. The number of direct child groups display in the window.
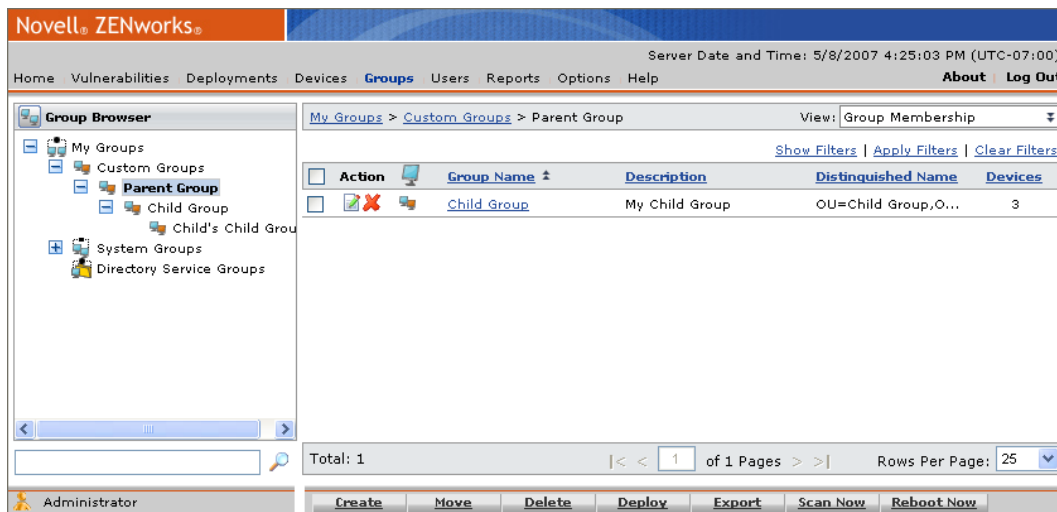
Figure 87: Group Membership

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

Table 74: Group Membership View

Field	Description
Action	Contains **Edit this Group** and **Delete this Group** icons. Use these icons to edit of delete the associated group.
Type (Monitor Icon)	Displays an icon that indicates the group type. For details regarding the different group types, refer to *Defining Groups* on page 155.
Name	The name of the child group.
Description	Description of the group.
Distinguished Name	System-created name based upon the group's parent hierarchy.

Field	Description
Devices	The number of devices assigned to this group.

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

The *Group Membership* view includes the following toolbar functions. Some functions are common throughout the *Groups* page.

Table 75: Group Membership Action Menu

Button	Use to
Create	Create a new group. See *Creating a Group* on page 161 for additional information.
Delete	Remove a group. See *Deleting Groups* on page 163 for additional information.
Move	Assigns a group to a new Parent Group. See *Moving a Group* on page 162 for additional information.
Deploy	Deploy vulnerabilities to a device. See *Using the Deployment Wizard* on page 97 for additional information.
Scan Now	Prompts the Discover Applicable Updates (DAU) task to immediately launch and check a group for vulnerabilities. See *Using the Scan Now Feature* on page 53 for additional information.
Reboot Now	Initiates the Reboot system task to all members of the selected group or groups. See *Rebooting Devices* on page 142 for additional information.
Export	Retrieves all page information and allows for saving to a *.csv* file. See *Exporting Data* on page 33 for additional information.

Creating a Group

Create a group to when you want to manage a number of endpoints with the same agent policy set.

1. In the *Device Groups* page, select **Group Membership** from the drop-down list.

Step Result: The *Group Membership* page displays in the *Groups* window.

2. Click **Create**.

Step Result: A new row appears on the page.

3. In the **Group Name** field, type a name for the group.

4. If desired, type a brief description about the group in the **Description** field.

5. Click the **Save** icon next to the new group.

Result: The group is saved to the list and is added to the directory tree. A *Distinguished Name* is generated for the group.

Moving a Group

Complete the following steps to move a group to a new parent group.

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

1. In the *Device Groups* page, select **Group Membership** from the drop-down list.

Step Result: The *Group Membership* page displays in the *Groups* window.

2. Select a group from the group tree.

3. Click Move.

Step Result: The *Move Groups* window opens.

Figure 88: Move Groups Window

4. Select a new parent group.

5. Click **Next**.

    Step Result: The Move Confirmation window opens.

Figure 89: Move Confirmation

6. Click **Finish**.

Result: The group is moved to the new parent group.

Deleting Groups

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

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

1. In the *Device Groups* page, select **Group Membership** from the drop-down list.

    Step Result: The *Group Membership* page displays in the *Groups* window.

2. Select a group from the directory tree.

3. Delete the desired group or groups using one of the following methods.

Method	Steps
Deleting a Single Group	1. Click the **Delete** icon associated with group you want to delete.
Deleting Multiple Groups	1. Select the check boxes associated with the groups you want to delete. 2. Click the **Delete** button.

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

Result: The selected groups are deleted.

> **Note:** When a group is deleted, all of its associated children are also deleted.

Editing Groups

To change a group name and/or description, edit the group.

1. In the *Device Groups* page, select **Group Membership** from the drop-down list.

   Step Result: The *Group Membership* page displays in the *Groups* window.

2. Select a group from the group tree.

3. Click the **Edit** icon associated with the group you want to edit.

4. Edit the *Name* and *Description* fields as desired.

5. Click the **Save** icon.

Result: The changes are saved to the group.

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

Device Membership

The **Device Membership** view provides an interface for managing the devices assigned to a group.
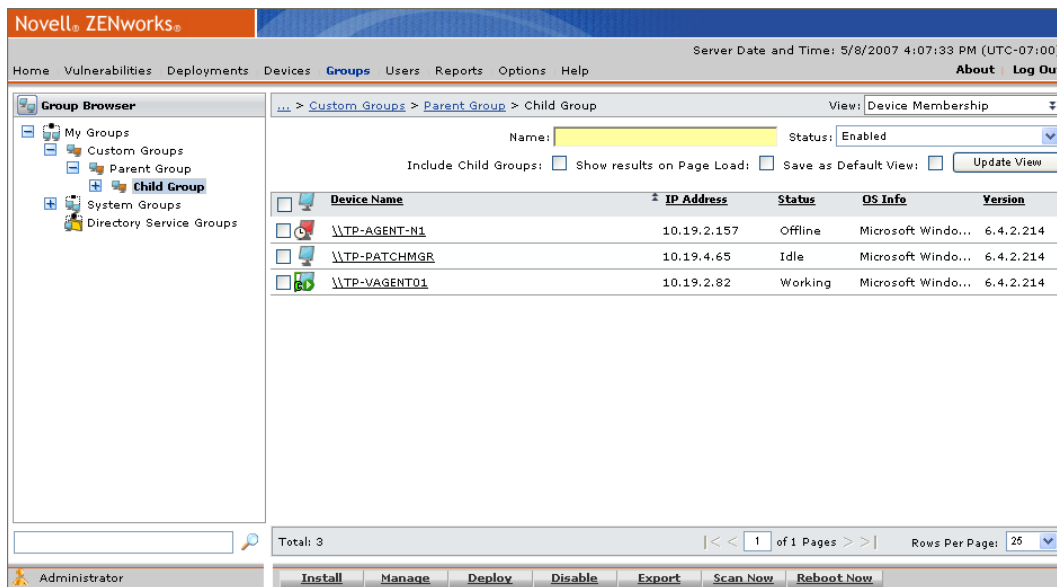
Figure 90: Device Membership

The Device Membership view displays the following device details.

Table 76: Device Membership view

Column	Description
Device Name	The name of the device as extracted from system data and inventory.
IP Address	The IP address of the device.
Status	The status of the device. Status values include: *Detecting*, *Disabled*, *Idle*, *Offline*, *Sleeping*, *Working*, and *Unknown*.
OS Info	Information about the operating system the device is running.
Version	The version number of the agent installed on the device.

The following table describes the functions of the **Device Membership** view toolbar:

Table 77: Device Membership View Toolbar

Button	Use To
Install	Install an agent to a device. For more information, see the *ZENworks Patch Management Server 6.4 SP2 Agent Install Guide*.
Manage	Add or remove devices from a group. For more information, see *Adding or Removing Device Members* on page 166 and *Enabling or Disabling Devices within a Group* on page 168.
Deploy	Deploy vulnerabilities to a device. See *Using the Deployment Wizard* on page 97 for additional information.
Disable	Disables a device within a group. See *Enabling or Disabling Devices within a Group* on page 168 for additional information.
Export	Retrieves all page information and allows for saving to a *.csv* file. See *Exporting Data* on page 33 for additional information.
Scan Now	Prompts the Discover Applicable Updates (DAU) task to immediately launch and check a group for vulnerabilities. See *Using the Scan Now Feature* on page 53 for additional information.
Reboot Now	Initiate the Reboot system task to all members of the selected group or groups. See *Rebooting Devices* on page 142 for additional information.

Adding or Removing Device Members

Add devices to a group for that device to inherit the group's settings.

1. In the *Device Groups* page, select **Device Membership** from the drop-down list.

   Step Result: The *Device Membership* page displays in the *Groups* window.

2. Select a group from the directory tree.

3. Click **Manage**.

Step Result: The *Manage Devices* view opens.
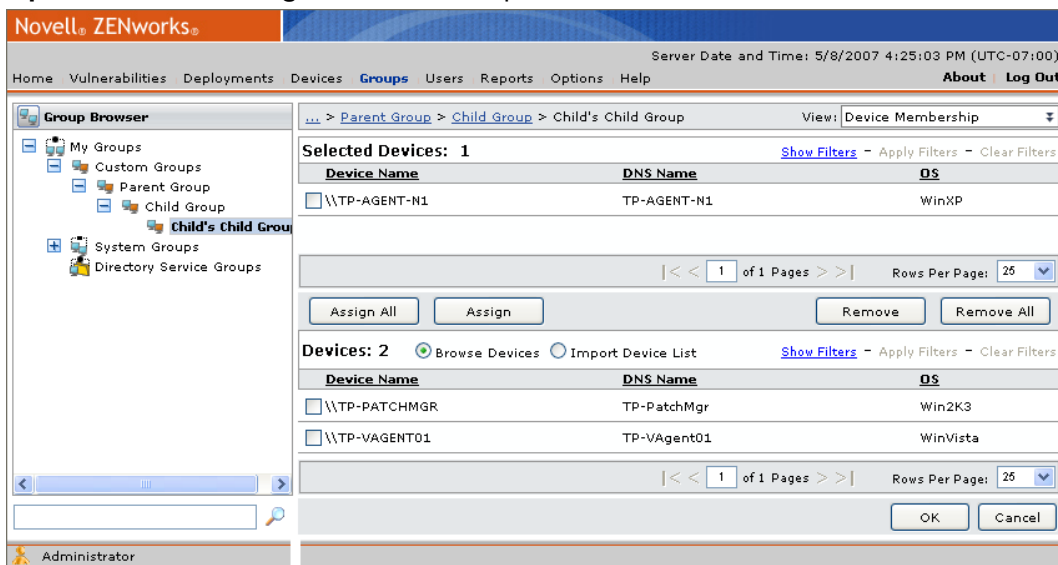
Figure 91: Manage Devices

4. Add or remove devices using one of the following methods.

Task	Methods
To add devices, use one of the following methods:	• Select the check box associated with the device(s) to include in the group from the **Devices** table and click **Assign**. Page to the next screen if needed. • Click **Assign All**.
To remove devices, use one of the following methods:	• Select the check box associated with the device(s) to remove from the group from the **Selected Devices** table and click **Remove**. Page to the next screen if needed. • Click **Remove All**.

5. Click **OK**.

6. Click **Update View** to review the device assignment.

Enabling or Disabling Devices within a Group

1. In the *Device Groups* page, select **Device Membership** from the drop-down list.

   Step Result: The *Device Membership* page displays in the *Groups* window.

2. If necessary, designate search options and click **Update View**.

3. Select the device you want to enable or disable.

4. Enable or disable the device:

   - Click **Disable** to disable an enabled device. Acknowledge the action by clicking **OK**.
   - Click **Enable** to enable a disabled device.

Result: The system disables or enables the device and displays it accordingly.

> **Note:** Disabling a device within a group is not group specific; the device will be disabled everywhere.

Mandatory Baseline

A mandatory baseline is a minimum patch standard set by the administrator that all agents assigned to a group must meet. If a device falls below that minimum patched status, the mandatory baseline will automatically send out the patches necessary to keep the device secure.

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

It is important to consider the following when working with mandatory baselines:

- Mandatory baseline inheritance indicates that a group's devices (both inherited and assigned) are included by the parent group when evaluating it's own baseline items and inheritance.
- If devices receive a mandatory baseline item via inheritance, the mandatory baseline item will also be displayed on the child group's *Mandatory Baseline* view. However, the baseline items will be unavailable, indicating the mandatory baseline originates from a parent group.
- Disabling mandatory baseline deployments only applies to the mandatory baseline items that are directly assigned to the group, and will prevent those directly assigned items from being inherited by the group's child hierarchy.
- Disabling mandatory baseline deployments does not disable the deployments created through mandatory baseline inheritance. Additionally, disabling the baseline deployments will not remove the baseline items from the group's *Mandatory Baseline* view.

When a mandatory baseline is created or modified:

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

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

The **Mandatory Baseline** view provides an interface for managing mandatory baselines within a group:
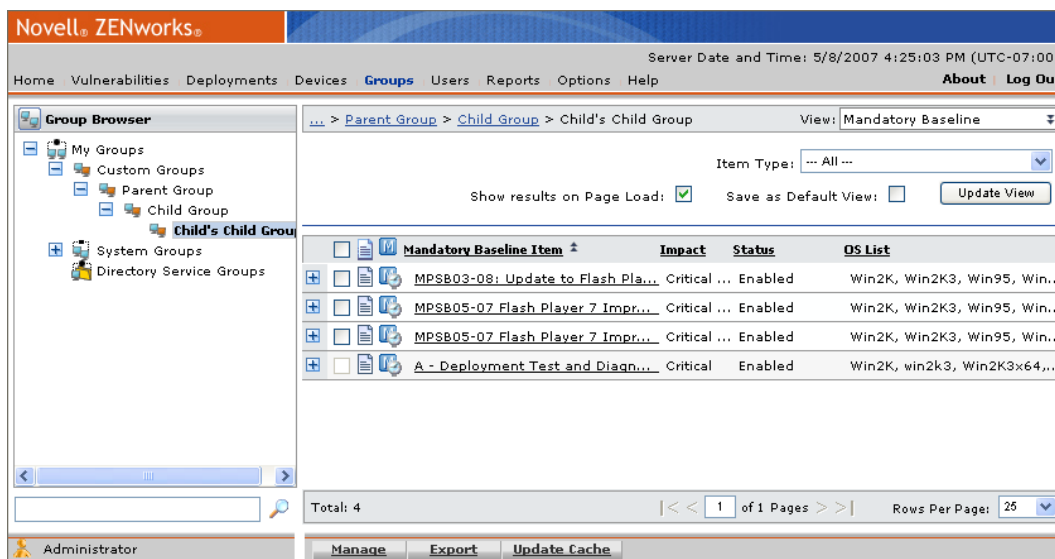
Figure 92: Mandatory Baseline

The following table describes the **Mandatory Baseline** view table:

Table 78: Mandatory Baseline Column Definitions

Column Header	Description
Expand (>)	Expanding allows you to view the devices, their operating systems, and their mandatory baseline compliance.
Vulnerability Status	The status of a mandatory baseline is indicated by an icon. This column displays the status/type of each vulnerability assigned to the baseline. See *Vulnerability Status Icons* on page 171 for additional information.

Column Header	Description
Mandatory Baseline Compliance	Mandatory Baseline compliance is indicated by an icon. This column displays the compliance status of each vulnerability assigned to the baseline. See *Mandatory Baseline Item Compliance Icons* on page 171 for additional information.
	Note: If the mandatory baseline fails to deploy more than twice, ZENworks Patch Management Server will record it as an error in the status column. However, this notification will only show in the **Mandatory Baseline** view.
Mandatory Baseline Item	The name of a mandatory baseline item is presented in the **Mandatory Baseline Item** column. The mandatory baseline item is the same as the vulnerability name.
Impact	The impacts listed here mirror the impacts of the vulnerability.
Status	The status of the *mandatory baseline item*.
OS List	The operating systems listed here mirror the operating systems that apply to the vulnerability (or package).

The following table describes **Mandatory Baseline** view toolbar functions.

Table 79: Mandatory Baseline View Toolbar

Button	Function
Manage	Add or remove vulnerabilities from the mandatory baseline.
Export	Retrieves all page information and allows for saving to a *.csv* file. See *Exporting Data* on page 33 for additional information.
Update Cache	Downloads packages and vulnerabilities required by the device. See *Updating the Cache* on page 55 for additional information.

Viewing a Group Mandatory Baseline

1. In the *Device Groups* page, select **Mandatory Baseline** from the drop-down list.

Step Result: The **Mandatory Baseline** page displays in the **Groups** window.

2. Select a group from the directory tree.

3. If necessary, populate the page.

    a) From the **Item Type** list, select an item type.

    b) Click **Update View**.

Result: The mandatory baselines associated with the group are displayed.

Vulnerability Status Icons

The following table includes descriptions of the Vulnerability status icons:

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

Mandatory Baseline Item Compliance Icons

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

Table 80: Mandatory Baseline Item Compliance Items

Status	Description
🔄	At least one member of this group is either detecting, obtaining the package, waiting on detection, or in a deployment not started state.
➕	At least one member of this group is deploying the package.
M	All of the applicable members of this group are disabled.
✅	All of the members of this group are either not applicable or in compliance for this package (some can also be disabled).
❌	At least one member of this group is out of compliance and has had an error when attempting to deploy. Specific information about the type of error will display in the mouse over text.

Managing Mandatory Baselines

Complete the following steps to manage mandatory baselines within a group.

1. In the *Device Groups* page, select **Mandatory Baseline** from the drop-down list.

   Step Result: The *Mandatory Baseline* page displays in the *Groups* window.

2. From the group tree, select the desired group.

3. Click **Manage**.

> **Step Result:** All known vulnerabilities are retrieved and displayed in the *Groups* window.
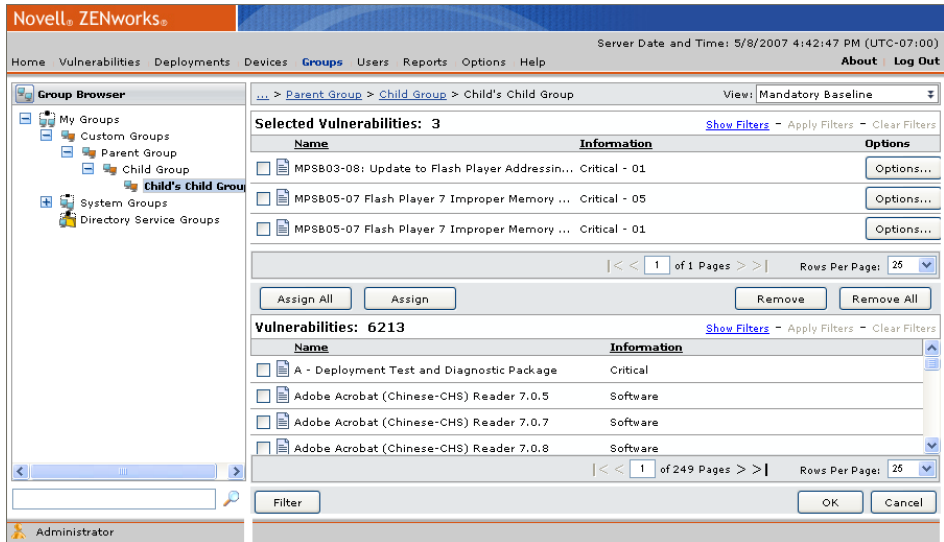
Figure 93: Assign Vulnerabilities

4. Add or remove vulnerabilities to or from the mandatory baseline.

Task	Methods
To add vulnerabilities, use one of the following methods.	• Select the check box associated with the vulnerabilities to include from the **Vulnerabilities** table and click **Assign**. Page to the next screen if needed. • Click **Assign All**.
To remove vulnerabilities, use one of the following methods.	• Select the check box associated with the vulnerabilities to remove from the **Selected Vulnerabilities** table and click **Remove**. Page to the next screen if needed. • Click **Remove All**.

5. Click **OK**.

Result: The selected vulnerabilities are added or removed to or from the mandatory baseline. The **Groups** page reflects your changes.

Using the Filter Functions to Select Vulnerabilities

When managing mandatory baselines, use filter functions to quickly find specific vulnerabilities.

1. From the **Vulnerabilities** or **Selected Vulnerabilities** tables, click **Show Filters**.

2. Type the filter criteria in the **Name** and/or the **Information** fields.

3. Click **Apply Filters**.

4. If desired, click **Clear Filters** to start another search.

Showing Only the Required Vulnerabilities

1. Click **Filter**.

Step Result: The *Needed Detection Vulnerabilities* window opens.

2. Select the check boxes associated with vulnerabilities as needed.

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

3. Click **OK**.

Step Result: The *Needed Detection Vulnerabilities* window closes and the patches display in the **Selected Vulnerabilities** table.

4. From the **Selected Vulnerabilities** table, click the **Options** button associated with the desired vulnerability.

   Step Result: The *Package Deployment Options* window opens.

Figure 94: Package Deployment Options

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

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

6. In **Distribution Options**, select **Concurrent** and the **device amount** or **Consecutive**.

7. If needed, type additional **Deployment Flags**.

8. Select or clear the desired **Deployment Options**.

Table 81: Deployment Options

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

9. Select or clear the desired **Reboot Options**.

Table 82: Reboot Options

Select	To
Do not notify users of this reboot	Reboot the mandatory baseline package without notifying the users of the device.
Notify users of this reboot	Reboot the mandatory baseline package and notify the users of the reboot. When this option is selected the remaining options in Deployment Options become active.
Message	Display a message to notify the users regarding the reboot.
Use Policies	Selecting this option indicates that deployments will use the agent policies to define reboot notification settings.
Allow user to cancel	Permits the recipient of the deployment to cancel the reboot.
Allow user to snooze	Permits the recipient of the deployment to delay the reboot.

Select	To
Notification on top	Displays the Agent Deployment window on top when notifying of a deployment requiring a reboot.
Deploy within	Sets the time frame for the reboot after a deployment. If snooze is enabled, this value is also maximum deployment snooze duration.

10. Click **OK**.

Result: The *Package Deployment Options* page closes.

Removing Deployments Created by Mandatory Baselines

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

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

Removing a Mandatory Baseline Deployment from a Group
The following procedure halts a mandatory baseline deployment.

1. In the *Device Groups* page, select **Mandatory Baseline** from the drop-down list.

   Step Result: The *Mandatory Baseline* page displays in the *Groups* window.

2. Select a group from the directory.
3. Select the mandatory baseline deployment to delete.
4. Click **Delete**.
5. Click **OK** to acknowledge the deletion.

   Note: If the mandatory baseline is still applied, the deployment(s) will be recreated.

Stopping Deployment for Specific Devices
The following procure halts mandatory baseline deployments to specific devices.

1. In the *Device Groups* page, select **Mandatory Baseline** from the drop-down list.

   Step Result: The *Mandatory Baseline* page displays in the *Groups* window.

2. From the directory, select the group to disable.
3. In the *Groups* page, select the group to disable from the directory tree.
4. Select **Deployments** from the drop-down list.
5. Click the desired **Device Name** link.
6. Click **Disable** to disable the deployment for the selected computer.

   Note: If the mandatory baseline is still applied the deployment(s) will be recreated.

Device Group Vulnerabilities

The **Vulnerabilities** view displays the vulnerabilities that have been assigned to the members of the group and the status of each vulnerability for the devices. This view is the same as the **Vulnerability Summary** view but only displays the vulnerabilities applicable to the member devices of the selected group.
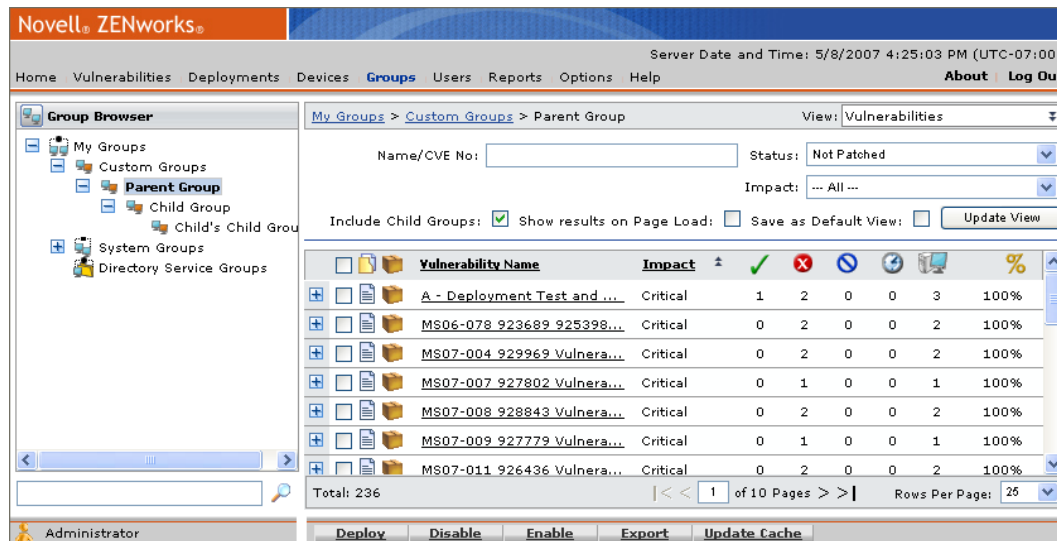
Figure 95: Device Group Vulnerabilities View

The **Vulnerabilities** view displays the following group details.

Table 83: Vulnerabilities View Columns

Column	Description
Vulnerability Status and Type Icons	Indicate vulnerability status and type. See *Vulnerability Status and Types* on page 47 for additional information.
Vulnerability Package Cache Status and Type Icon	Indicate the package cache status and type. See *Vulnerability Package Cache Status and Type* on page 48 for additional information.
Vulnerability Name	The name of the vulnerability. Typically includes the vendor, specific application, and version information.
Impact	Describes the level of requirement for the vulnerability. See *Vulnerability Impacts* on page 49 for additional information.

Column	Description
Vulnerability Statistics Icons	Indicate vulnerability statistics. See *Vulnerability Statistics* on page 50 for additional information.

The following reference describes the **Vulnerabilities** view toolbar functions.

Table 84: Vulnerabilities View Toolbar

Button	Function
Enable	Enables a vulnerability. See *Enabling a Vulnerability* on page 53 for additional information.
Disable	Disables a vulnerability. See *Disabling a Vulnerability* on page 53 for additional information.
Update Cache	Downloads (or re-downloads) the selected packages and vulnerabilities. See *Updating the Cache* on page 55 for additional information.
Deploy	Opens the **Deployment Wizard**.See *Using the Deployment Wizard* on page 97 for additional information.
Export	Retrieves all page information and allows for saving to a *.csv* file. See *Exporting Data* on page 33 for additional information.

Enabling Vulnerabilities within a Group

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

1. In the *Groups* page, select **Vulnerabilities** from the drop-down list.

   Step Result: The *Vulnerabilities* page displays in the *Groups* window.

2. Select a group from the directory tree.

3. If necessary, filter the page.
   a) Enter the desired criteria in the filter field and lists.
   b) Click **Update View**.

4. Select the check box associated with a disabled vulnerability.

   You can select multiple disabled vulnerabilities.

5. Click **Enable**.

Result: The selected vulnerabilities are enabled for the applicable group.

Disabling Vulnerabilities within a Group

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

1. In the *Groups* page, select **Vulnerabilities** from the drop-down list.

   Step Result: The *Vulnerabilities* page displays in the *Groups* window.

2. Select a group from the directory tree.

3. If necessary, filter the page.

   a) Enter the desired criteria in the filter field and lists.

   b) Click **Update View**.

4. Select the check box associated with a vulnerability you want to disable.

   You can select multiple vulnerabilities.

5. Click **Disable**.

Result: The selected vulnerabilities are disabled for the applicable group.

Device Group Inventory

This view displays the software, hardware, operating systems and services that were detected on the devices in the group. This view is the same as the **Inventory Summary** view, but only displays the inventory of the selected group.
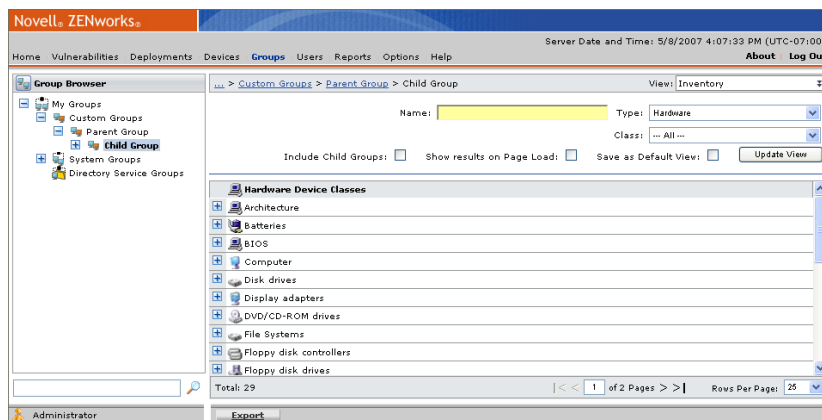
Figure 96: Device Group Inventory View

The following table describes the **Inventory** view toolbar functions

Table 85: Group Inventory Toolbar

Button	Function
Export	Retrieves all page information and allows for saving to a *.csv* file. See *Exporting Data* on page 33 for additional information.

Device Group Deployments

This **Deployments** view displays the deployments that the selected group has been assigned. This view is the same as the **Deployment Summary** view, but displays only deployments for the selected group. See *Using the Deployment Pages* on page 86 for additional information.
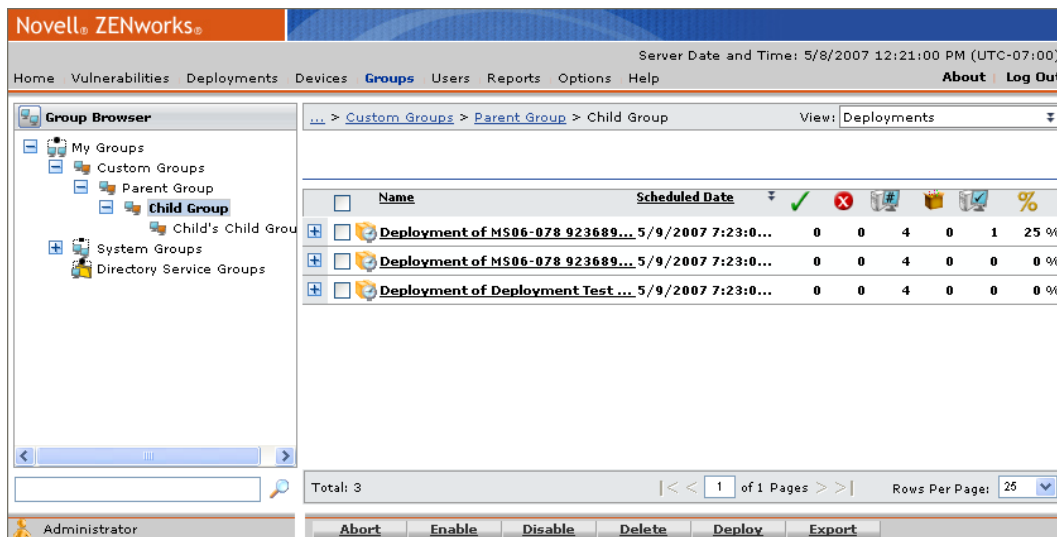
Figure 97: Device Group Deployments

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

The following table describes the *Deployments* view toolbar functions.

Table 86: The Deployments View Toolbar

Button	Function
Abort	Cancels the deployment for any devices which have not already received the deployment package. See *Aborting Deployments* on page 95 for additional information.
Enable	Enables the selected disabled deployment. See *Enabling Deployments* on page 96 for additional information.
Disable	Disables the selected enabled deployment. See *Disabling Deployments* on page 95 for additional information.

Button	Function
Delete	Removes the deployment from ZENworks Patch Management Server. See *Deleting Deployments* on page 96 for additional information.
Deploy	Re-deploys the selected packages. See *Using the Deployment Wizard* on page 97 for additional information.
Export	Export subscription data to a comma separated value *.csv* file. See *Deleting Deployments* on page 96 for additional information.

Deploying to a Group

Deploying to a group of selected devices is a key function of ZENworks Patch Management Server. Deployments are initiated by clicking **Deploy** and completing the *Deployment Wizard*. The *Deployment Wizard* provides step-by-step instructions for defining and pushing deployments out to the protected devices in the network. See *Using the Deployment Wizard* on page 97 for additional information.

Device Group Policies

The **Policies** view displays the policy sets that the selected group has been assigned. For more information on policy sets and policy conflict resolution, see *Working With Agent Policy Sets* on page 264.
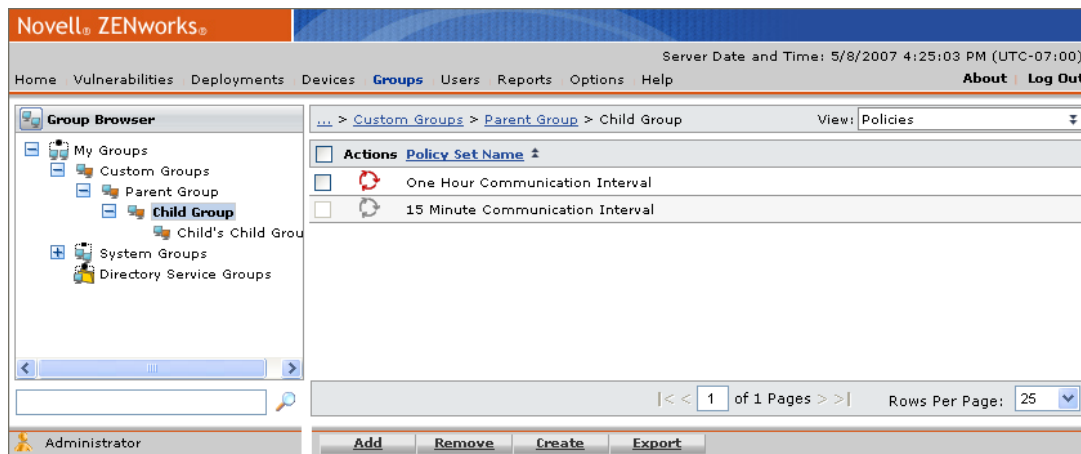
Figure 98: Device Group Policies View

Adding a Policy to a Group

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

1. In the *Groups* page, select **Policies** from the drop-down list.

   Step Result: The *Policies* page displays in the *Groups* window.

2. Select a group from the directory tree.

3. Click **Add**.

4. Select a policy from the **Policy Set Name** list.

5. Click the **Save** icon.

Result: The policy set is saved and associated with the group.

Removing a Policy from a Group

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

Note: You cannot remove inherited policy sets; instead, must change the group's policy inheritance setting. For more information regarding the modification of group inheritance, see *Editing Group Settings* on page 189.

1. In the *Groups* page, select **Policies** from the drop-down list.

   Step Result: The *Policies* page displays in the *Groups* window.

2. Select a group from the directory tree.

   Step Result: The selected group is highlighted and displays any associated policies.

3. Select and remove one or more policies.

   - To remove one policy, click the **Remove** icon associated with the policy.
   - To remove multiple policies, select the check boxes associated with the policies you want to delete and then click the **Remove** button.

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

Result: The policy set is no longer associated with the group.

Device Group Roles

This **Roles** view displays the roles that have been assigned to the selected group.
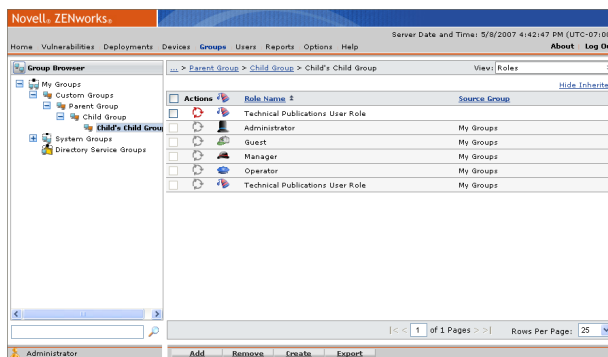
Figure 99: Device Group Roles View

The following reference describes the **Roles** view table.

Table 87: Roles View Columns

Column	Description
Role Name	The name of the user role.
Source Group	The name of the group assigned to the user role.

The following table describes the functions available in the **Roles** view.

Table 88: The Roles View Toolbar

Action	Use To
Add	Adds an already established role to the group.
Remove	Removes a role from the group.
Create	Creates a new role. See *Creating User Roles* on page 233 for additional information.
Export	Retrieves all page information and allows for saving to a *.csv* file. See *Exporting Data* on page 33 for additional information.

Adding a Role to a Group

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

1. In the *Groups* page, select **Roles** from the drop-down list.

   Step Result: The *Roles* page displays in the *Groups* window.

2. Select a group from the directory tree.

3. Click **Add**.

   Step Result: The **Select a Role** drop-down list displays in the *Groups* window.
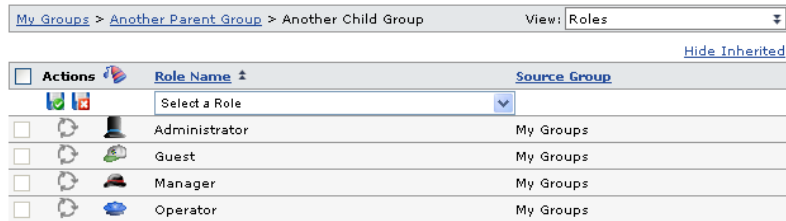
Figure 100: Add a Role

4. Select a role from the *Name* list.

5. Click the **Save** icon.

Result: The role is saved and associated with the group.

Removing a Role from a Group

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

1. In the *Groups* page, select **Roles** from the drop-down list.

   Step Result: The *Roles* page displays in the *Groups* window.
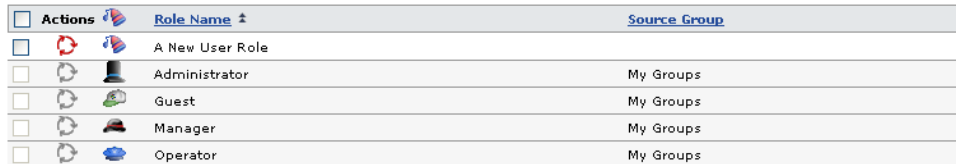
Figure 101: Roles Page

2. Select a group from the directory tree.

3. Select the check box associated with the role you want to remove.

4. Click **Remove**.

5. Acknowledge the removal by clicking **OK**.

Result: The role is removed and no longer associated with the group.

Device Group Dashboard

The **Group Dashboard** view consists of a series of charts providing a current view of the selected group. These charts are generated based on the latest data available and include only those devices that are members of the current group, its child hierarchy, and their applicable vulnerabilities and packages.
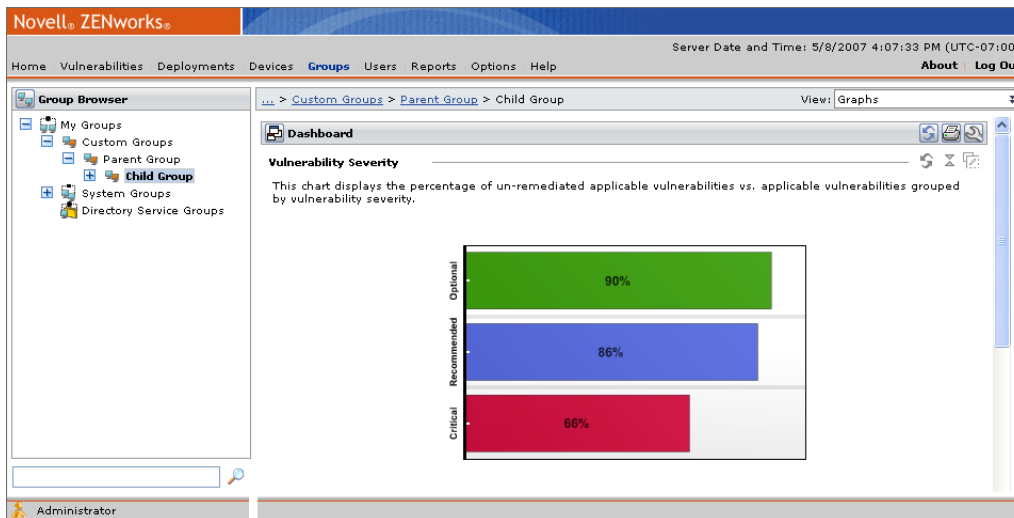
Figure 102: Device Group Dashboard View

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

Dashboard Charts

The following table describes all of the available charts.

Table 89: Dashboard Charts

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

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

Dashboard Settings and Behavior Icons

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

Table 90: Dashboard Settings and Behavior Icons

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

Icon	Function
⩔	Move the selected chart down one level.
⟳	Refresh the selected chart.
⩤	Minimize the chart.
⬚	Hide the chart from view.

Adding a Graph to the Dashboard

1. Click the **Dashboard Settings** icon.

   Step Result: The *Dashboard Settings* dialog opens.
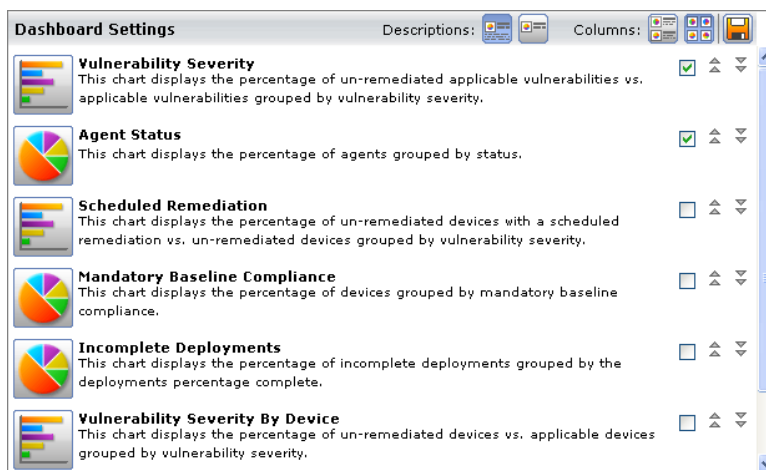
Figure 103: Dashboard Settings Dialog

2. Select check boxes associated with the charts you want to display.

3. Move the graphs up or down according to your priorities.

4. Select the number of columns for display: Select a one or two column width view from **Columns**.

   - Click the **View as One Column** icon to display charts in one column.
   - Click the **View as Two Columns** icon to display charts in two columns.

5. Display or hide the chart descriptions.

   - Click the **Show the Chart Descriptions** icon to display chart descriptions.
   - Click the **Hide the Chart Descriptions** icon to hide chart descriptions.

6. Click **Save**.

Result: Your graph setting selections are saved and displayed.

Removing a Graph from the Dashboard

1. Click the **Dashboard Settings** icon.

Step Result: The **Dashboard Settings** drop-down list opens.

2. Deselect the checkbox next to the graph(s) you want to remove.

3. Click **Save Dashboard Settings**.

4. Click **Save**.

Step Result: The graph(s) is removed from the *Dashboard* window

Device Group Settings

The **Settings** view displays the default group settings.
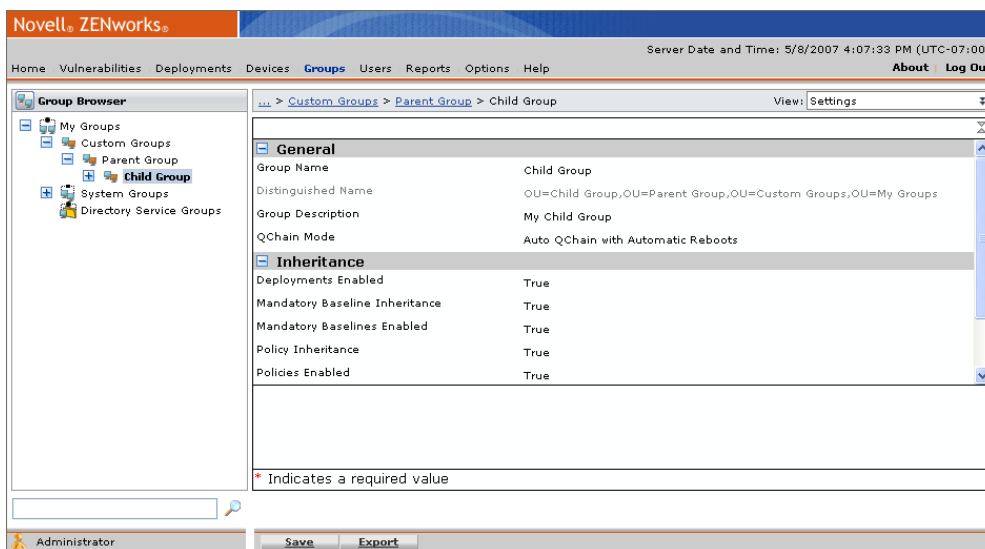
Figure 104: The Settings View

The following table describes **Settings** view toolbar functions.

Table 91: Settings View Toolbar

Button	Function
Save	Saves the settings defined in the page.

Button	Function
Export	Retrieves all page information and allows for saving to a *.csv* file. See *Exporting Data* on page 33 for additional information.

Editing Group Settings

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

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

Field	Description
Group Name	The group name.
	Note: **My Groups**, **System Groups**, and **Directory Service Groups** group names cannot be edited.
Distinguished Name	A system-defined group name that represents the group's parent hierarchy.
	Note: The **Distinguished Name** cannot be edited.
Group Description	The group description.
Chain Mode (list)	Defines chain behavior during mandatory baseline deployments. Select from the following options: • **Standard -- Set Individually** • **Auto QChain with Manual Reboots** • **Auto QChain with Automatic Reboots**
Deployments Enabled (list)	Defines whether deployments may be created for the group. A *True* value will allow users to create deployments for the group.

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

2. In the **Mandatory Baseline** area, edit the following lists as necessary.

List	Description
Mandatory Baseline Inheritance	Defines whether the group inherits the policies assigned to the group's parent hierarchy. A *True* value will set the

List	Description
	group to inherit it's parent hierarchy's mandatory baseline settings.
Mandatory Baseline Enabled	Defines whether mandatory baselines may be assigned to the group. A *True* value will allow users to create mandatory baseline deployments for the group.

3. In the **Policy** area, edit the following lists as necessary.

List	Use To
Policy Inheritance	Defines whether the group inherits the policies assigned to the group's parent hierarchy. A *True* value will set the group to inherit it's parent hierarchy's policy settings.
Policies Enabled	Defines whether policies may be assigned to the group. A *True* value will allow users to assign policies directly to the group.

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

Field	Use To
Email Address	User-defined e-mail addresses to which notifications are sent regarding events impacting the group.
Source Groups (button)	User-defined group or groups whose agents are dynamically assigned to the group. See *Assign a Source Group to a Custom Group* on page 190 for additional information.

5. Click **Save**.

Result: The new settings are saved and applied to the group.

Assign a Source Group to a Custom Group

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

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

1. In the *Groups* page, select **Settings** from the drop-down list.

Step Result: The *Settings* page displays in the *Groups* window.

2. Select a custom group from the directory tree.

3. Click **Modify**.

    Step Result: The *Edit Source Groups* window opens.
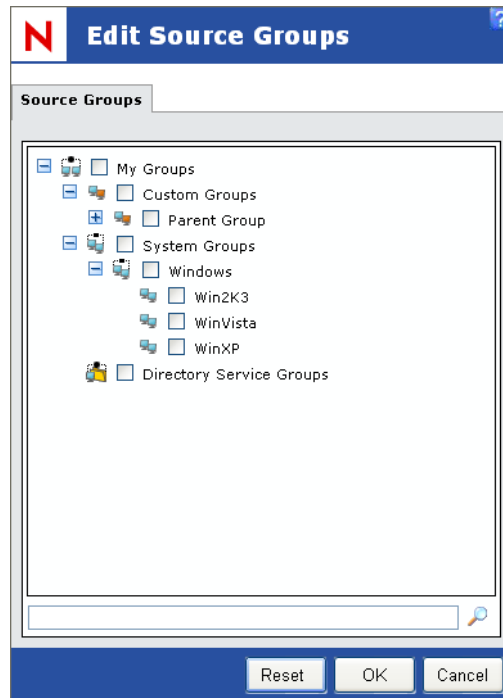
Figure 105: Edit Source Groups

4. Expand the **Source Group** tree or use the search field to locate the group you require as a source.

5. Select the groups you require as a source.

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

6. Click **OK**.

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

Chapter

7

Reporting

In this chapter:

- *About Reports*
- *Working with Reports*
- *Available Reports*

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

About Reports

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

Available Reports Page

The main page from which you select which report to display from a list of available reports. You can click the expand button icon [+] to view a description of each report.
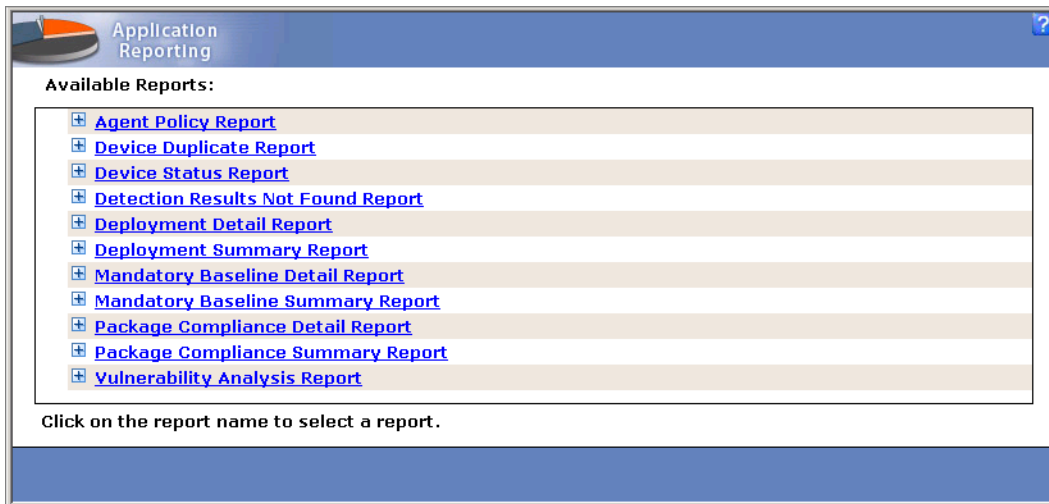
Figure 106: Available Reports

Report Parameters Page

From the Available Reports List, selecting **Device Status Report** displays the *Application Reporting Device Status Report Parameters* page. The report definition page where you define the data to include in the report.
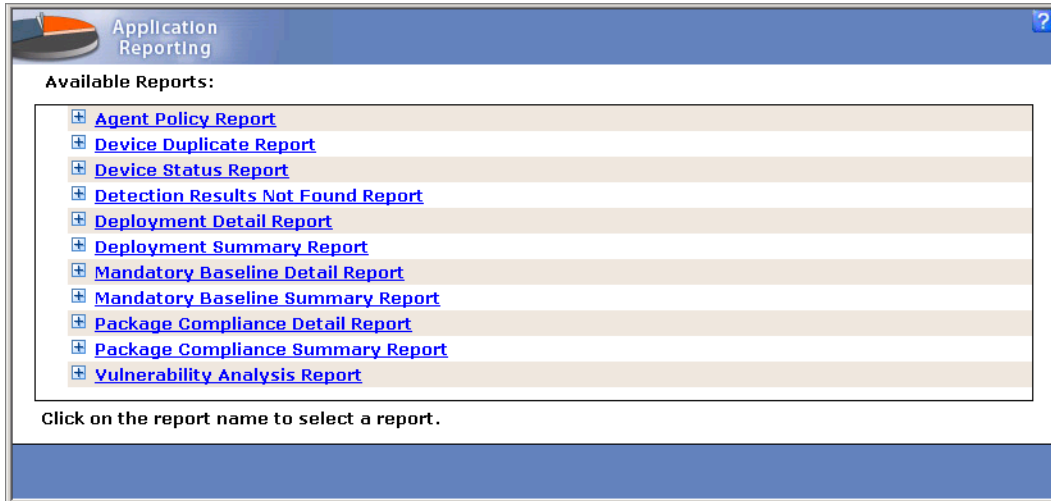
Figure 107: Report Parameters Page

Report Parameters List

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

Table 92: Report Parameters

Select	To
Devices	Choose from a list of all available devices that you have permission to view. All available devices are shown in the Available Devices list. Click a single device or use the CTRL and SHIFT keys to select multiple devices.
	Note: All access is limited to users with access to all Devices or with the Enable Administrative Reports access rights.

Select	To
Groups	Choose from a list of all available groups within Patch Management Server that you have permission to view. All groups are shown in the Available Groups list and all of the devices belonging to the selected group and it's child groups are included in the report. Click a single group or use the CTRL and SHIFT keys to select multiple groups. **Note:** All access is limited to users with access to all Groups or with the Enable Administrative Reports access rights.
Deployments	Choose a deployment from a list of all available deployment names. All available deployments are shown in the Available Deployments list. Click a single deployment or use the CTRL and SHIFT keys to select multiple deployments.
Packages	Choose from a list of all available packages. All available packages are shown in the Available Packages list. Click a package name or use the CTRL and SHIFT keys to select multiple packages.
Vulnerabilities	Choose from a list of all available vulnerabilities identified by Patch Management Server. All vulnerabilities are shown in the Available Vulnerabilities list. Click a vulnerability name or use the CTRL and SHIFT keys to select multiple vulnerabilities.
Date Range	Choose from a list of all deployments that occur within the selected dates. You can also display the time in 12 or 24 hour format and as Patch Management Server local time or UTC time.

Report Results Page

Make your selections and click **Generate**. This page presents the results of the report once it is generated.

Figure 108: Report Page

Viewing Reports

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

1. In the Main Menu, select **Reports**.

   Step Result: The *Available Reports* page opens in a new browser window.
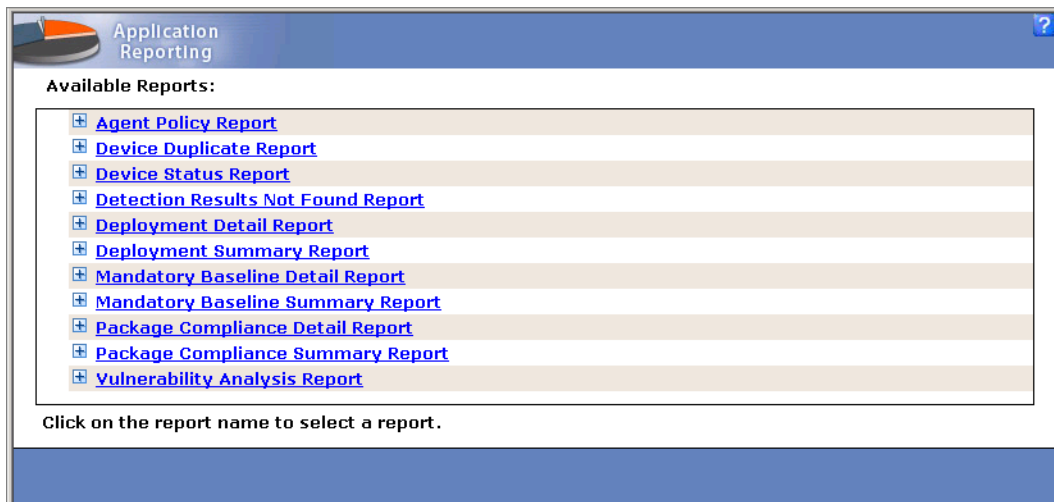
Figure 109: Available Reports

2. Select the report to generate in the *Available Reports* page.

   Step Result: The corresponding *Report Parameters* page opens.
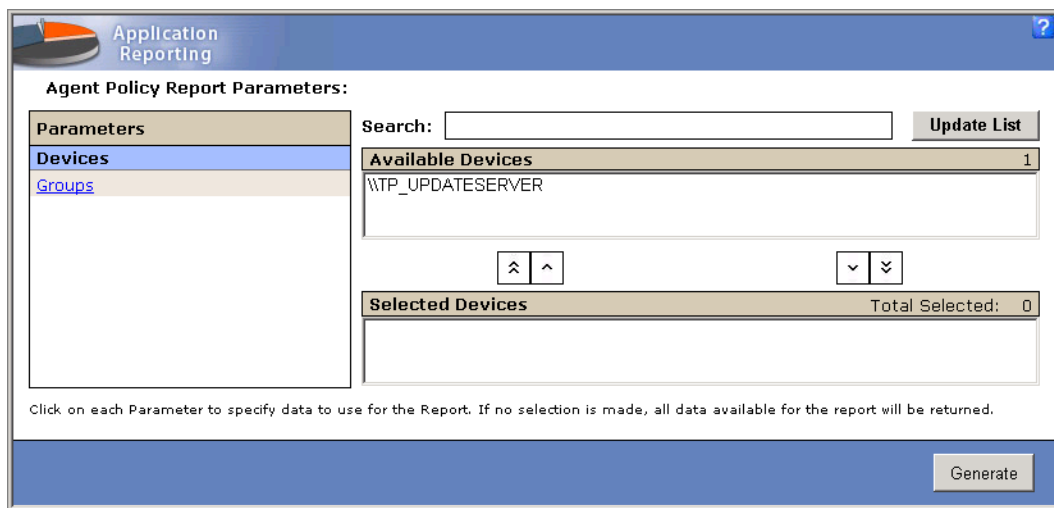
Figure 110: Report Parameters

3. In the *Report Parameters* page, define the report contents and organization by selecting parameters.

   a) In the **Parameters** box, select the parameter to use in defining the report contents from the list of available parameters. This is the left-side pane of the page.

   b) In the **Available Devices** (or **Available Options**) box, select from the list of available parameters to include (Devices, Groups, Vulnerabilities) by selecting with your cursor. Select multiple items using the CTRL or SHIFT keys.

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

4. With the desired items selected, click the **Include** arrow.

5. To include all available items, click the **Include All** arrow.

6. Verify the contents of the **Selected Options** box.

7. Remove items by clicking the **Remove** arrow.

8. Or, to include all available items, click the **Remove All** arrow.

9. Click **Generate** to create the report.

10. The *Report Results* page opens with the retrieved information.

Working with Reports

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

- *Searching within Reports* on page 199.
- *Displaying Time and Date in Reports* on page 200.
- *Exporting Reports* on page 200.
- *Viewing Printable Data in Reports* on page 200.

Searching within Reports

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

- Search does not support the use of Boolean search commands (AND, OR, NOT, nesting (), etc.).
- Search terms are not case sensitive. All letters are treated as lower case. For example, the search term *WIN* is treated the same as *win* and will generate the same results.
- To show all results, remove any content from the **Search** text box (leave blank).
- To search, enter the search term in the **Search** text box and click **Update List**. To return to the pre-search results, click from the list of available options in the **Parameters** list box.

Displaying Time and Date in Reports

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

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

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

Exporting Reports

Once the report is created, you have the option of switching to a printable view for printing, or exporting the report into another file format.

Reports are presented in standard HTML (*.html*) and can be exported into several file formats for your convenience.

- Comma Separated Values (*.csv*)
- Microsoft Excel Worksheet (*.xls*)
- XML Document (*.xml*)

The Export command and drop-down list is presented at the bottom of the page.

Note: All data results will export, not just selected results. However, some of the data may not import into a readable format.

Viewing Printable Data in Reports

When viewing reports, a printable version of the generated report can be previewed for printing.

1. Generate a report.

Step Result: The completed report page displays in the window.

2. Select **Printer Friendly**.

Step Result: The Report's results page refreshes with the data in print preview mode.

3. Select **Send to Printer**.

Step Result: The file is sent to your installed printer.

> **Note:** If you have not established printer connectivity, click **Yes** when the *Print* dialog box appears and use the *Add Printer Wizard* to select and connect your printer.

Available Reports

ZENworks Patch Management provides several predefined reports designed to provide a comprehensive view of the application environment in respect to patch management activities. In many cases there is a detail and summary report for each specific function.

The following reports are available:

- *Agent Policy Report* on page 201
- *Mandatory Baseline Summary Report* on page 208
- *Deployment Detail Report* on page 202
- *Operating System Inventory Detail Report* on page 209
- *Deployment Error Report* on page 202
- *Operating System Inventory Summary Report* on page 209
- *Deployment In-Progress Report* on page 203
- *Package Compliance Detail Report* on page 209
- *Deployment Summary Report* on page 204
- *Package Compliance Summary Report* on page 210
- *Detection Results Not Found Report* on page 205
- *Services Inventory Detail Report* on page 211
- *Device Duplicate Report* on page 205
- *Services Inventory Summary Report* on page 211
- *Device Status Report* on page 206
- *Software Inventory Detail Report* on page 211
- *Hardware Inventory Detail Report* on page 206
- *Software Inventory Summary Report* on page 212
- *Hardware Inventory Summary Report* on page 207
- *Vulnerability Analysis Report* on page 212
- *Mandatory Baseline Detail Report* on page 207

Agent Policy Report

The *Agent Policy Report* shows the policies that are the resolution of all policies assigned to the device. In the report, each policy value is listed in the **Policy Name** column. When using groups as a parameter, it is only a method to select multiple devices, the group policies are not part of the actual results.

Available Parameters: Device, Group

Table 93: Agent Policy Report Column Definitions

Column	Definition
Device Name	The name of the device.
Policy Name	The name of the agent policy.

Column	Definition
Current Value	The policy setting.
Policy Desc	The agent policy's description.

Deployment Detail Report

The *Deployment Detail Report* provides information about a selected list of deployments. In the report, each deployment name is listed in the **Deployment Name** column. The report provides information as to the status of the particular deployment activity.

Available Parameters: Deployments, Vulnerabilities, Date Range

Table 94: Deployment Detail Report Column Definitions

Column	Definition
Deployment Name	The name of the deployment.
Package Name	The name of the package.
Device Name	The name of the device.
Deployment Status	The deployment status or stage.
Deployment Date	The date the deployment was sent.
Install Date	The date the agent was installed on the device.
Vulnerability Status	The vulnerabilities patch status.
Date Last Verified	The date of the last Discover Applicable Updates (DAU) scan.

Note: If a selected vulnerability does not have an associated deployment, it will not appear in the report.

Deployment Error Report

The *Deployment Error Report* provides information about deployments which have returned an error.

Available Parameters: Deployments, Packages, Devices, Date Range

Table 95: Deployment Error Report Column Definitions

Column	Definition
Deployment Status	The deployment status or stage.
Status Code	Reference code for support identification. When contacting support, this code is used to help identify the deployment issue.

Column	Definition
Error Message	The actual error text returned by the deployment.
Install Date	The date the agent was installed on the device.
Package Name	The name of the package.
Deployment Name	The name of the deployment.
Device Name	The name of the device.

Deployment In-Progress Report

The *Deployment In-Progress Report* provides information about deployments that have not completed. Reports can be generated for each deployment, package, or device. The report provides the status of the deployment.

Available Parameters: Deployments, Packages, Devices, Groups

Table 96: Deployment In-Progress Report Column Definitions

Column	Definition
Deployment Name	The name of the deployment.
Package Name	The name of the package.
Total Deployed	The total number of the devices that were assigned the deployment.
Already Patched	The number (or percentage) of devices that are already patched.
Not Applicable	The number (or percentage) of devices where the deployment does not apply.
Not Successful	The number of devices patched successfully.
Total In-Progress	The total number of devices currently receiving the deployment.
Not Started	The number of devices yet to receive the deployments.
Caching Package	Indicates whether the deployment is still caching the package. 1 = Caching, 0 = Complete
Total Failed	The total number of deployments that have failed.
Total Disabled	The total number of devices that are disabled and cannot receive the deployment.

Column	Definition
Percent Success	The percentage of devices that have successfully received the deployment.
Percent Failure	The percentage of devices on which the deployment has failed.

Deployment Summary Report

The *Deployment Summary Report* provides information about a selected list of deployments.The report provides a summary of the particular deployment activity.

Available Parameters: Deployments, Vulnerabilities, Date Range

Table 97: Deployment Summary Report Column Definitions

Column	Definition
Deployment Name	The name of the deployment.
Package Name	The name of the package.
Total Deployed	The total number of the devices that were assigned the deployment.
Already Patched	The number (or percentage) of devices that are already patched.
Not Applicable	The number (or percentage) of devices where the deployment does not apply.
Total Successful	The total number of devices successfully patched.
Total In-Progress	The total number of devices currently receiving the deployment.
Not Started	The number of devices yet to receive the deployments.
Caching Package	Indicates whether the deployment is still caching the package. 1 = Caching, 0 = Complete
Total Failed	The total number of deployments that have failed.
Total Disabled	The total number of devices that are disabled and cannot receive the deployment.
Total Patched	The total number of devices that have been patched by this deployment.
Percent Success	The percentage of devices that have successfully received the deployment.

Column	Definition
Percent Failure	The percentage of devices on which the deployment has failed.

Note: If a selected vulnerability does not have an associated deployment, it will not appear in the report.

Detection Results Not Found Report

The *Detection Results Not Found Report* returns a list of devices that have not completed a Discover Applicable Updates (DAU) task with the server. The report lists each agent name, the installation date of the agent, and information required to identify and locate the device.

Available Parameters: Device, Group

Table 98: Detection Results Not Found Report Column Definitions

Column	Description
Agent Name	The name of the agent.
OS Abbr Name	The abbreviated operating system name.
Agent Version	The version of the agent.
Last Contact Date	The last date the Patch Management Server had contact with the agent.
Installation Date	The date the agent was installed on the device.
IP Address	The internet protocol address.
DNS Name	The name used by the Domain Name System (DNS) to identify the device.
OS Info	A description of the operating system.

Device Duplicate Report

The *Device Duplicate Report* returns a list of duplicate devices registered with Update Server. Duplicate devices are usually the result of applying the Agent Uniqueness feature that permits an agent installed on ghost images to register multiple times with ZENworks Patch Management Server.

Available Parameters: Date Range

Table 99: Device Duplicate Report Column Definitions

Column	Definition
Device Name	The name of the device.
Status	The current status of the device.

Column	Definition
Install Date	The date the agent was installed on the device.

Device Status Report

The *Device Status Report* returns the current status of the selected devices (or devices in the selected groups). In the report, each device is listed in the **Device Name** column. The report then provides information about the particular device.

Available Parameters: Device, Group

Table 100: Device Status Report Column Definitions

Column	Definition
Device Name	The name of the device.
DNS Name	The name used by the Domain Name System (DNS) to identify the device.
IP Address	The internet protocol address.
OS Name	The operating system name.
OS Build No.	The operating system's build number.
OS Service Pack	The latest service pack applied to the operating system (if applicable).
Agent Version	The version of the agent.
Last Contact Date	The last date the Patch Management Server had contact with the agent.
Patchable Status	The reboot/chained status of the agent.
Group List	A listing of the groups, by Distinguished Name, to which the device belongs.

Hardware Inventory Detail Report

The *Hardware Inventory Detail Report* provides information about hardware associated with a device and device status.

Available Parameters: Devices, Groups

Table 101: Hardware Inventory Detail Report Column Definitions

Column	Definition
Hardware Device Class	The type of hardware.
Hardware Device Name	The name of the hardware device.

Column	Definition
Device Name	The name of the device.
Device OS Info	A description of the operating system.

Hardware Inventory Summary Report

The *Hardware Inventory Summary Report* provides a summary of reported hardware and the devices associated with them.

Available Parameters: Devices, Groups

Table 102: Hardware Inventory Summary Report Column Definitions

Column	Definition
Hardware Device Class	The type of hardware.
Hardware Device Name	The name of the hardware device.
Instances	The number of times this device occurs. (Within the parameters of the report.)

Mandatory Baseline Detail Report

The *Mandatory Baseline Detail Report* provides information about the mandatory baseline status associated with a device.

Available Parameters: Devices, Groups

Table 103: Mandatory Baseline Detail Report Column Definitions

Column	Definition
Device Name	The name of the device.
Assigned By Group	The distinguished name of the group that assigned the mandatory baseline.
Package Name	The name of the package.
Mandatory Baseline Enabled	Indicates whether the *Assigned By* group has mandatory baselines enabled.
Package Enabled	Indicates whether the package is enabled. If the package is disabled, it cannot be deployed to a device.
Mandatory Status	Identifies whether the device is applicable, patched, or needs patching by the mandatory baseline.
Deployment Status	The deployment status or stage.

Column	Definition
Package Release Date	The date the package was released.
Date Deployed	The date the package was deployed.
Date Installed	The date the package was installed on the device.
Date Last Verified	The date of the last Discover Applicable Updates (DAU) scan.
Assigned	Indicates whether the mandatory baseline has been assigned to the device. 1 = Assigned, 0 = Not Assigned

Mandatory Baseline Summary Report

The **_Mandatory Baseline Summary Report_** returns a summary list of patch and deployment information for all mandatory baseline packages and vulnerabilities associated with the selected list of devices.

Available Parameters: Devices, Groups

Table 104: Mandatory Baseline Summary Report Column Definitions

Column	Definition
Mandatory Baseline Item Name	Name of the mandatory baseline vulnerability.
Total Devices	The total number of devices.
Total Patched	The total number of devices that have been patched by this deployment.
Total Not Applicable	The total number of devices for which the deployment does not apply.
Total In-Progress	The total number of devices currently receiving the deployment.
Total Disabled	The total number of devices that are disabled and cannot receive the deployment.
Total Error Conditions	The total number of devices on which the deployment has failed.
Percent Patched	The percentage of applicable devices that are patched.

Operating System Inventory Detail Report

The *Operating System Inventory Detail Report* provides information about the operating system associated with a device and the device status.

Available Parameters: Devices, Groups

Table 105: Operating System Inventory Detail Report Column Definitions

Column	Definition
Operating System	The operating system name and description.
Device Name	The name of the device.

Operating System Inventory Summary Report

The *Operating System Inventory Summary Report* provides a summary about the operating system associated with a device and the device status.

Available Parameters: Devices, Groups

Table 106: Operating System Inventory Detail Report Column Definitions

Column	Definition
Operating System	The operating system name and description.
Instances	The number of times this operating system occurs. (Within the parameters of the report.)

Package Compliance Detail Report

The *Package Compliance Detail Report* provides information about patch and deployment status for a specific package or device. The report lists each package associated with the selected device(s) or group(s). In the report, each package is listed in the **Package Name** column. The report then provides details for the vulnerability status for each package; and the associated device, status, and deployment details.

Available Parameters: Devices, Groups, Packages

Table 107: Package Compliance Detail Report Column Definitions

Column	Definition
Package Name	The name of the package.
Device Name	The name of the device.
Vulnerability Status	The vulnerabilities patch status.
Last DAU Run	The date of the last Discover Applicable Updates (DAU) scan.

Column	Definition
Last DAU Status	The status of the last Discover Applicable Updates (DAU) scan.
Date Last Verified	The date of the last Discover Applicable Updates (DAU) scan.
Deployment Name	The name of the deployment.
Deployment Status	The deployment status or stage.
Package Release Date	The date the package was released.
Date Deployed	The date the package was deployed.
Date Installed	The date the package was installed on the device.
Date Scheduled	The date the package was scheduled for deployment to the device.

Note: If a selected package does not have an associated deployment, it will not appear in the report.

Package Compliance Summary Report

The *Package Compliance Summary Report* returns a summary list of patch and deployment information by package name for all applicable devices.

Available Parameters: Devices, Groups, Packages

Column	Definition
Package Name	The name of the package.
Total Devices	The total number of devices.
Applicable Devices	The total number of applicable devices.
Devices Detecting	The number of devices currently running a Discover Applicable Updates (DAU) task.
Devices Patched	The number of devices that are already patched.
Not Patched/Not Scheduled	The number of devices that are not patched, and do not have a deployment scheduled.
Not Patched/Scheduled	The number of devices that are not patched, and do have a deployment scheduled.
Deployments Completed	The number of deployments that have completed successfully.

Column	Definition
Deployments Failed	The number of failed deployments.
Deployments In Progress	The number of devices currently receiving the deployment.

Note: If a selected package does not have an associated deployment, it will not appear in the report.

Services Inventory Detail Report

The **Services Inventory Detail Report** provides information about the service associated with a device and the device status.

Available Parameters: Devices, Groups

Table 108: Services Inventory Detail Report Column Definitions

Column	Definition
Service Name	The name of the service.
Device Name	The name of the device.
Service Startup State	The state the service should enter upon device boot.
Service Current State	The current state of the device.

Services Inventory Summary Report

The **Services Inventory Summary Report** provides summary information about the service associated with a device and the device status.

Available Parameters: Devices, Groups

Table 109: Services Inventory Summary Report Column Definitions

Column	Definition
Service Name	The name of the service.
Instances	The number of times this service occurs. (Within the parameters of the report.)

Software Inventory Detail Report

The **Software Inventory Detail Report** provides information about the software associated with a device and the device status.

Available Parameters: Devices, Groups

Table 110: Software Inventory Detail Report Column Definitions

Column	Definition
Software Program	The name of the software installed on the device.
Device Name	The name of the device.

Software Inventory Summary Report

The *Software Inventory Summary Report* provides information about the software associated with a device and the device status.

Available Parameters: Devices, Groups

Table 111: Software Inventory Summary Report Column Definition

Column	Definition
Software Program	The name of the software installed on the device.
Instances	The number of times this software program occurs. (Within the parameters of the report.)

Vulnerability Analysis Report

The *Vulnerability Analysis Report* provides a summary of the remediation status for the selected vulnerabilities. The report lists each vulnerability affecting the selected device or group. The report also can be generated for a single vulnerability or group of vulnerabilities. In the report, each vulnerability is listed in the **Vulnerability Name** column. The report then provides patch status details for each vulnerability and if a deployment is required.

Available Parameters: Devices, Groups, Vulnerabilities

Table 112: Vulnerability Analysis Report Column Definitions

Column	Definition
Vulnerability Name	The name of the vulnerability.
Vulnerability Release Date	The date the vulnerability was released.
Total Devices	The total number of devices.
Applicable Devices	The total number of applicable devices.
Devices Detecting	The number of devices currently running a Discover Applicable Updates (DAU) task.

Column	Definition
Devices Patched	The number of devices that are already patched.
Not Patched	The number of devices not patched.
Percent Patched	The percentage of applicable devices that are patched.

Note: If a selected vulnerability does not have an associated deployment, it will not appear in the report.

Chapter

8

Managing Users and Roles

In this chapter:

- *About User Management*
- *Defining User Access*
- *Defining Users*
- *Defining Roles*
- *Working with Users*
- *Working with User Roles*

This section provides information on managing users of ZENworks Patch Management. The user management features allow you to create users and define their permissions and access rights.

About User Management

The *User Management* page allows the system administrator to define which users can access Patch Management Server and the role each user has within the system. Roles define the permissions and access rights for each user.

Figure 111: User Management View

Viewing Users

1. From the Main menu, select the **Users** tab.

   Step Result: The users display in the *Users* window.

2. If desired, type a user name or select a role on which to filter.

3. Click **Update View**.

   Step Result: The Users table is populated based upon your filter criteria.

Defining User Access

ZENworks Patch Management allows for establishing security policies in accordance with your company needs. Security access is determined by a combination of two mechanisms: Windows-based authentication and ZENworks Patch Management access rights.

Windows-based Authentication

Patch Management Server authentication is controlled by the Windows operating system. Users who have access to the Patch Management Server are members of the local Windows group *PLUS Admins.*

Update Access Rights

Once a user has logged into Patch Management Server, their assigned user role is authenticated by the system. If a user does not have access to a given section, an access denied error message will display.

In the Users Section, the **Roles** tab is where these roles are defined, while the **Users** tab is where you can add or remove users and assign them a user role.

Defining Users

Users can be defined as individuals (John Smith) or conceptual users (Quality Assurance Manager). The user profile includes access credentials and the role assigned to the user. While a user only can be assigned one role, there can be many users assigned to a certain role.

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

- **Creating New Users**

  When a user is created, the user is added to both Patch Management Server and Windows.

  Note: If the user is given permission to manage other users within Patch Management Server, they will be added to the Windows *Administrators* group.

- **Adding Existing Windows Users**

  An existing Windows user can be added and granted access to Patch Management Server. Using this method, existing users are searched and can be added to Patch Management Server.

  Note: If the user is given permission to manage other users within Patch Management Server, they will be added to the Windows *Administrators* group.

Note: The Microsoft IIS Web server software does not support the entering of user names or passwords in languages (Korean, Kanji, etc.) that require Unicode characters. Since the Patch Management Server software uses a Microsoft IIS Web server, ZENworks Patch Management user names and passwords cannot be created in unicode and authentication does not support some native languages.

Defining Roles

The Patch Management Server includes both system and custom roles. System roles are roles native to every installation and cannot be edited or disabled. They allow control over all device groups and devices. Custom roles are created by the administrator and allow for combining access rights and selected devices or groups for a particular user.

Note: See *Defining Access Rights* on page 218 for detailed descriptions of the access rights assigned each role.

Roles are defined by a combination of three attributes; access rights, groups and devices.
- Access rights define the application pages and functionality available to the user.
- Groups and Devices define the specific machines or group of machines the user has permission to access.

Defining the Predefined System Roles

Predefined system roles are provided to assist you in defining the roles that newly created users inherit. The ZENworks Patch Management administrator can assign these roles to the user, or may use a predefined role as a model in defining a custom role.

Note: System roles provide access to all groups and devices. A user assigned a system role has access to all devices and groups.

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

Role	Description
Administrator	Any user assigned this role is permitted full access to all areas and functionality of the product. Users assigned this role are the only users who can delegate newly installed devices to other user roles. The administrator role includes all available access rights. Administrators can view all devices/groups and perform any function within the 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 Patch Management Server system with the exception of Advanced Configuration and User Management options.
Operator	This user role is permitted to perform all routine operations (deploy, detect, export). Operators can only perform typical daily functions.
Guest	This role provides access to the system but restricts the user from performing any patch management tasks. The role allows view-only access.

Defining Custom Roles

Custom roles are created by the ZENworks Patch Management administrator. Custom roles can be based on any pre-existing role and then can be altered to fit a particular need. Creating a custom role involves selecting a predefined role as a model, or template. Unlike system roles which cannot be disabled, you can disable a custom role at any time.

Defining Access Rights

Every page, feature, function, and individual action within the application is constrained to a series of access rights. The functionality and pages (views) available to the user are based on the access rights associated with the role user has been assigned. The four predefined system 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 environment, access rights pertaining to the installed module may be added by the system to the access rights list.

The following table identifies the default set of access rights, describes the functionality of each, and illustrates the system role assigned to each access right.

Table 113: User Role Access Rights

Access Right Name	Description	Admin	Mgr	Oper	Guest
Enable Update Cache Button	Ability to cache (download) packages from the Global Subscription Service.	X	X		
View Devices	Access the Devices section.	X	X	X	X
Export Device Data	Enable the export of device data.	X	X	X	
Install Agents	Access to the **Agent Installers** page.	X	X		
Manage Devices	Ability to enable, disable, and delete devices.	X	X		
View Deployments	Access to the Deployments section.	X	X	X	X
Manage Deployments	Ability to enable, disable, abort, change, and delete deployments.	X	X	X	
Export Deployment Data	Enable the export of deployment data.	X	X	X	
View Device Groups	Access the Device Groups section.	X	X	X	X
Export Device Group Data	Enable the export of Device Group data.	X	X	X	
Manage Device Groups	Ability to add, edit, disable, enable, and delete device group.	X	X		
View Home Page	Access to the **Home** page.	X	X	X	X
View Current Status	Display the server status (on the **Home** page).	X	X	X	X
View Inventory	Access the Inventory data.	X	X	X	X
Export Inventory Data	Enable the export of Inventory data.	X	X	X	
Manage Product Licenses	Manage the product licenses.	X			
View Support Options	Access the **Options** > **Support** tab.	X	X	X	X
Export Support Data	Enable the export of support data.	X	X		

Access Right Name	Description	Admin	Mgr	Oper	Guest
View Agent Policies	Access to the **Options** > **Policies** tab.	X	X	X	X
Export Agent Policy Data	Enable the export of agent policy data.	X	X		
View Default Configuration	Access the **Options** > **Configuration** tab.	X	X	X	X
Export Configuration Data	Enable the export of configuration data.	X	X		
View E-mail Notifications	Access the **Options** > **E-Mail Notifications** tab.	X	X	X	X
Export E-mail Notification Data	Enable the export of e-mail notification data.	X	X		
View Product Licenses	Access the **Options** > **Products** tab.	X	X	X	X
Export Product License Data	Enable the export of product license data.	X	X		
Manage Options	Manage subscription, product licenses, configuration, agent policies, e-mail notifications, and support options.	X			
View Subscription Information	Access the **Options** > **Subscription** tab.	X	X	X	X
Export Subscription Data	Enable the export of subscription data.	X	X		
View Packages	Access the Packages section.	X	X	X	X
Create Deployments	Ability to create deployments.	X	X	X	
Export Package Data	Enable the export of package data.	X	X	X	
Manage Packages	Ability to add, change, disable, enable, and delete packages.	X	X		
Enable Reboot Now Button	Ability to reboot devices using the **Reboot Now** button.	X			
View Vulnerabilities	Access the Vulnerability section.	X	X	X	X
View Vulnerability Details	Access the vulnerability details.	X	X	X	X

Access Right Name	Description	Admin	Mgr	Oper	Guest
Export Vulnerability Data	Enable the export of vulnerability data.	X	X	X	
Manage Vulnerabilities	Ability to disable and enable vulnerabilities.	X	X		
Enable Administrative Reports	Ability to run reports that return data for all devices and device groups regardless of user role, device, or group assignments.	X			
Export Reports	Ability to export application reports.	X	X	X	
Enable User Reports	Ability to run reports returning data for only the devices and device groups to which the user has access.	X	X	X	X
Enable Scan Now Button	Ability to deploy the Discover Applicable Updates (DAU) Task using the **Scan Now** button.	X	X	X	
View Users	Access to the **Users** tabs.	X	X	X	X
Change Password	Ability to change the password for a user.	X			
Export User Data	Enable the export of user data.	X	X		
Manage Users	Ability to create, add, edit, remove, delete, enable, and disable users or user roles.	X			

Defining Accessible Device Groups

Accessible device groups are groups of devices associated with a particular role. This option is used to achieve a level of granularity in the assignment of roles to system users.

As mentioned, roles are defined primarily by the access rights associated to the role. In the case of the default system roles, the entire network monitored by the Patch Management Server is available to users if they have the appropriate role-based access rights.

Note: The accessible groups option is disabled when working with a predefined system role.

The accessible groups option allows you to restrict a user to specified groups. For example, a user assigned the access rights to manage deployments can be limited to managing deployments for select groups.

The accessible groups option is available in the *Add/Edit Role Wizard*.
* **Selected Groups** - Lists the groups of devices assigned to the role.
* **Groups** - Lists the available groups of devices that can be assigned to the role.

Defining Accessible Devices

Accessible devices are individual devices associated with a particular role. This option works in the same manner as the accessible groups option by allowing you to achieve a level of granularity in the assignment of roles to system users.

The accessible devices option allows you to limit a user's permissions to specified devices. For example, a user assigned access rights to manage devices can be limited to managing only a single device using this option.

Note: The accessible devices option is disabled when working with a predefined system role.

The accessible devices option is available in the *Add/Edit Role Wizard*.
* **Selected Devices** - Lists the devices assigned to the role.
* **Devices** - Lists the available devices that can be assigned to the role.

Working with Users

This section describes the user-based tasks available from the User Management page. The available user-based tasks are:

Creating New Users

When creating users, you have two options: create a new local user, or add an existing local or domain user.

Note: User names may be between 1-20 characters in length and cannot include any of the following characters: ' \ " @ ^ % & { } ( ) [ ] ; < > ! # : ? ' / * = |

Passwords are case sensitive and must meet password the rules defined by local and/or domain password policies. Note that although a *Password Strength Indicator* is provided to display the strength or weakness of your password, the actual password policy is defined by Windows.

The **Full Name**, **Office Phone**, **Cell Phone**, **Pager**, **E-mail**, and **Description** fields are not validated and apply no formatting rules other than maximum length of 25 characters.

1. In the *User Management* page, click **Create**.

    Step Result: The *Create User Wizard* opens.

Figure 112: Create User Wizard - Create or Add User Page

2. Select the **Creating a new local user** option.

3. Click **Next**.

    Step Result: The *Create User* page opens.

Figure 113: Create User Wizard - Create a New User

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

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

5. Select a **Role** (Administrator, Manager, Operator, or Guest) for the user from the pull-down window list.

6. Click **Next**.

Step Result: The *Confirm User* page opens.

Figure 114: Create User Wizard - Creation Confirmation Page

7. Confirm the user information and click **Close**.

> **Step Result:** The *Creation Summary* page opens.
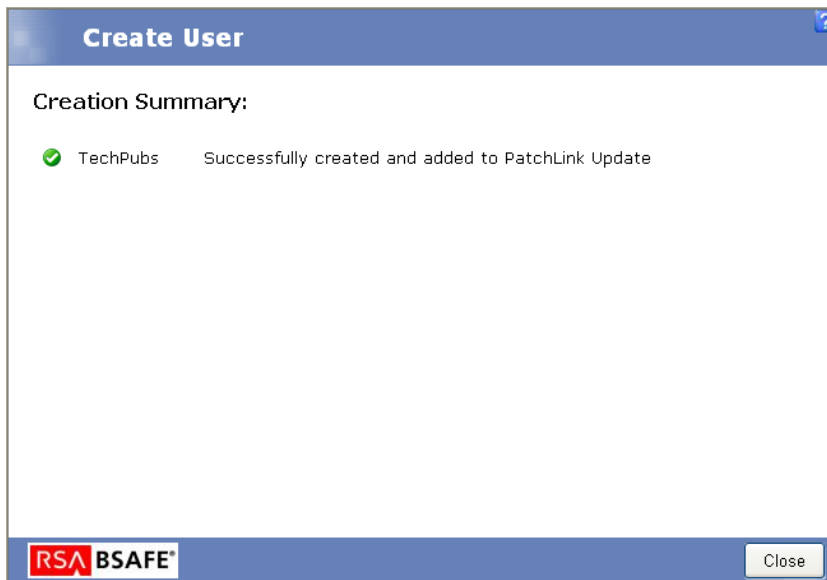
Figure 115: Create User Wizard - Creation Summary Page

8. Click **Close** to exit the wizard.

Result: The new user is created, added to Windows, and granted the appropriate access to the Patch Management Server.

Adding Existing Users

Adding a user imports an existing Windows user into the ZENworks Patch Management database and access group, and can import a user from an existing domain by logging into that domain as a domain user.
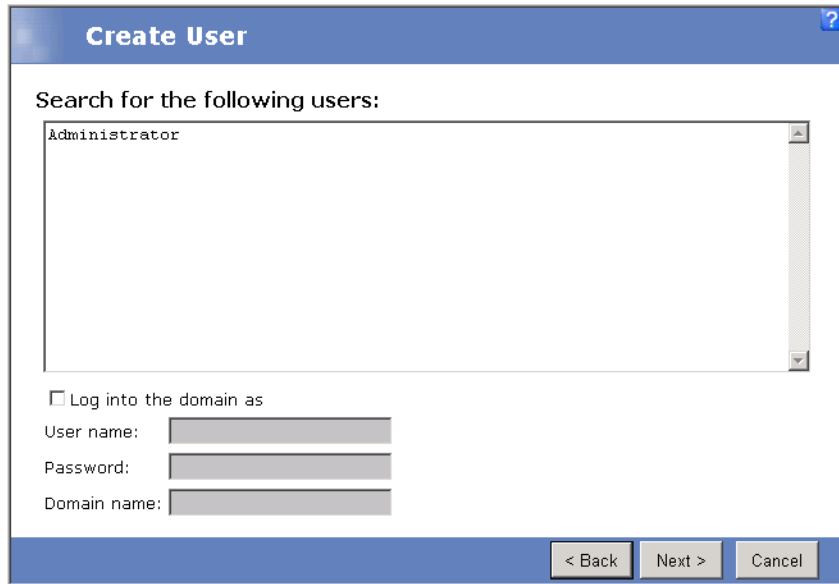
1. In the *User Management* page, click **Create**.

> **Step Result:** The *Create User Wizard* opens.

2. Select the **Adding existing local or domain users** option.

3. Click **Next**.

> **Step Result:** The **Search for the following users** page opens.

Figure 116: Create User Wizard - Search for Users

4. In the **Search for the following users** field type a user name, or the beginning characters of one or more user names. Use semicolons to separate user names. To search for users within a specific domain, prefix the user name with the domain (DOMAINNAME\UserName).

If searching using the domain, select **Log into the domain as**. Enter the **User name**, **Password**, and **Domain** name.

Note: There must be a secure connection between the domain and the Patch Management servers domain, or the users will be unable to access the Patch Management Server.

5. Click **Next**.

    Step Result: The *Users Found* page opens.

Figure 117: Create User Wizard - Users Found

6. Select a **User Role** for each of the users found.

    Step Result: The **No Action** value indicates that the user will not be added to the Patch Management Server, or if the user already exists as an Patch Management user, no changes are made to the user.

7. Confirm the user information and click **Finish**.

    Step Result: The *Summary* page opens.

8. Verify the summary data and click **Close**.

    Step Result: The *Create User Wizard* closes.

Editing User Profiles

Editing user profile information allows you to change the role assigned to a user as well as update the user's contact information. If you have the Change Password access right, you can edit other user's passwords using the procedure defined under *Changing a User's Password* on page 230.

1. From the **Users** grid located under **Action**, click the **Edit user details** icon associated with the user profile.

    Step Result: The *Edit User Wizard* opens.

Figure 118: Edit User Wizard - User Information page

2. Make the necessary modifications as defined in *Creating New Users* on page 222.

3. Click **Finish** to exit the wizard when complete.

Removing Users

Removing a user from ZENworks Patch Management disables their access to the Patch Management Server without deleting the user's Windows account. Once removed, the user is deleted from the Patch Management Server database and is removed from the user list in the *User Management* page.

Note: You cannot remove or delete a user that has been assigned the *Administrator* role, or a custom role that has been given the *Manage Users* access right. You must first edit the user, change the user's role, then remove or delete the user.

1. Click **Users** to open the *Users* page.

2. On the *Users* page, select the checkbox for the users to remove.

3. Click **Remove**.

    Step Result: A *Remove User* warning displays.

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

> **Step Result:** The user is removed.

Deleting Users

Deleting a user from ZENworks Patch Management disables their access to the Patch Management Server and deletes the Windows account for that particular user.

Note: Deleting a user not only removes the users access to ZENworks Patch Management, but also deletes the user from the device and/or Active Directory.

1. Click **Users** to open the *Users* page.

2. On the *Users* page, select the checkbox for the users delete.

3. Click **Delete**.

> **Step Result:** A *Delete User warning* displays.

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

> **Step Result:** A *Delete User confirmation* displays.

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

> **Step Result:** The user is deleted.

Changing a User's Password

Changing a User's Password in ZENworks Patch Management also changes the user's Windows password on the (physical) Patch Management Server.

Note: Passwords are case sensitive and must meet password the rules defined by local and/ or domain password policies. Note that although a *Password Strength Indicator* is provided to display the strength or weakness of your password, the actual password policy is defined by Windows.

1. Click **Users** to open the *Users* page.

2. Select the user requiring the password change.

3. Click **Change Password**.

Step Result: The *Change Password Wizard* opens.

Figure 119: Change Password Wizard - Weak Password

4. Type the new password in the **New Password** field.

Step Result: The **Password Strength indicator** displays the effectiveness of the password you select and displays the **Weak** indicator when the first character is typed in the **New Password** field.

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

The **Password Strength Meter** monitors factors such as the password length, complexity, variety of characters, and resemblance to common words. Strong passwords usually contain more than eight characters, and combine capital and lower case letters, numbers and

symbols. Also, they do not resemble common words or names including words with numbers in place of letters.
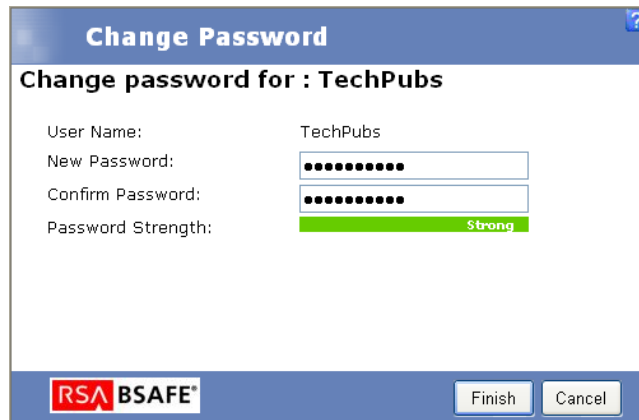
Figure 120: Change Password Wizard - Strong Password

6. Click **Finish**.

Step Result: The password is changed.

Working with User Roles

The Patch Management Server includes both system and custom roles. System roles are roles native to every installation and cannot be edited or disabled. They allow control over all device

groups and devices. Custom roles are created by the administrator and allow for combining access rights and selected devices or groups for a particular user.

Figure 121: User Role View

This section describes the role-based tasks available from the *User Management* page.

- *Creating User Roles* on page 233.
- *Editing User Roles* on page 235.
- *Assigning a User Role to an Existing User* on page 236.
- *Disabling User Roles* on page 237.
- *Enabling User Roles* on page 238.
- *Deleting User Roles* on page 238.

Note: When sorting user roles, regardless of the requested sort column or order, the system defined user roles (Administrator, Manager, Operator, and Guest) will remain as the first four items.
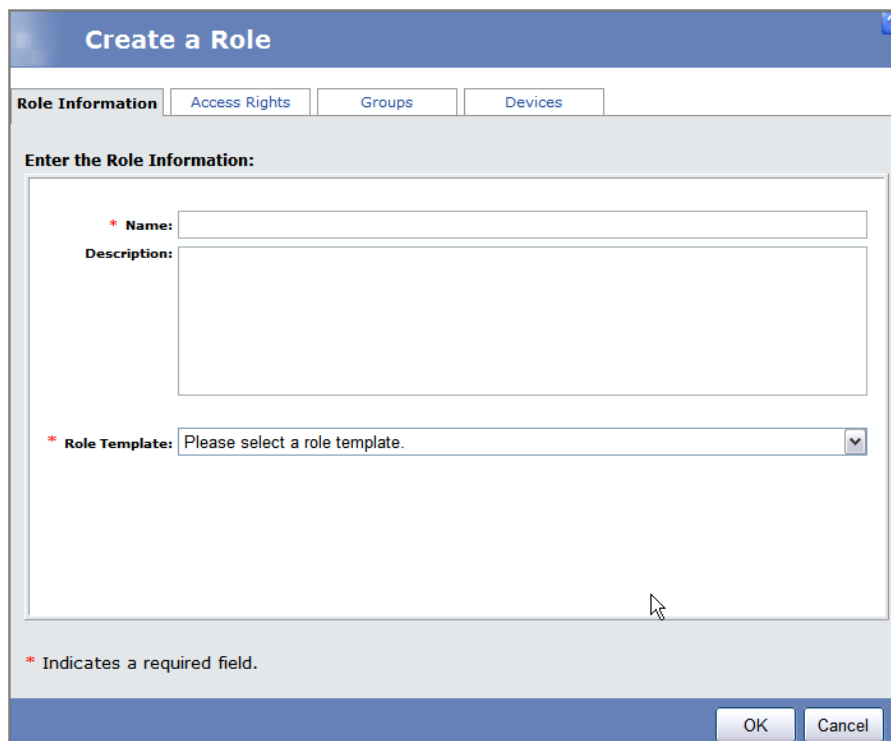
Creating User Roles

Creating custom-defined roles is an effective means to delegate patch management responsibilities to stakeholders throughout the organization. Once you define the template, you can then modify access rights and modify group and device access levels.

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

2. Click **Create**.

> **Step Result:** The *Create a Role wizard* opens.

Figure 122: User Role Wizard - Role Information tab

3. On the **Role Information** tab:

   a) Type a name for the role in the **Name** field.
   b) Type a description for the role in the **Description** field.
   c) Select a role template in the **Role Template** drop-down list.

   Any existing role can be used as a template and as such, will determine what access rights the new user role will start with. You can add or remove access rights regardless of which role was selected as the template.

4. Select the **Access Rights** tab.

   a) To define which rights the users assigned this role will have, select the checkbox to the left of each of the desired access rights.
   b) Click **Assign** to move the selected access rights to the **Selected Access Rights** table or click **Assign All** to move all of the access rights to the **Selected Access Rights** table.

     c) To remove access rights, select the checkbox to the left of each of the desired access rights.

     d) Click **Remove** to remove the selected access rights from the **Selected Access Rights** table or click **Remove All** to remove all of the access rights from the **Selected Access Rights** table.

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

     a) To assign group access, select the checkbox to the left of each of the desired groups.

     b) Click **Assign** to move the selected groups to the **Selected Groups** table or click **Assign All** to move all of the groups to the **Selected Groups** table.

     c) To remove group access, select the checkbox to the left of each of the desired groups.

     d) Click **Remove** to remove the selected groups from the **Selected Groups** table or click **Remove All** to remove all of the groups from the Selected Groups table.

     Granting access to a Device Group gives permission to all devices within that group, regardless of the options selected within the **Devices** tab.

6. Select the **Devices** tab, to define which devices the users assigned this role will be able to access.

     a) To assign device access, select the checkbox to the left of each of the desired devices.

     b) Click **Assign** to move the selected devices to the **Selected Devices** table or click Assign All to move all of the devices to the Selected Devices table.

     c) To remove device access, select the checkbox to the left of each of the desired devices.

     d) Click **Remove** to remove the selected devices from the **Selected Devices** table or click **Remove All** to remove all of the devices from the **Selected Devices** table.

7. Click **OK**.

     Step Result: The wizard saves your changes and closes.

Editing User Roles

The editing feature is available only to custom-defined roles (system-defined roles cannot be edited) and is performed within the *Edit a Role Wizard*.

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

2. Click the **Edit** icon to the left of the role you wish to edit.

     Step Result: The *Edit a Role wizard* opens.

3. On the **Role Information** tab, Edit the **Name** or **Description** as desired.

4. Select the **Access Rights** tab.

     a) To define which rights the users assigned this role will have, select the checkbox to the left of each of the desired access rights.

     b) Click **Assign** to move the selected access rights to the **Selected Access Rights** table or click **Assign All** to move all of the access rights to the **Selected Access Rights** table.

c) To remove access rights, select the checkbox to the left of each of the desired access rights.

d) Click **Remove** to remove the selected access rights from the **Selected Access Rights** table or click **Remove All** to remove all of the access rights from the **Selected Access Rights** table.

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

a) To assign group access, select the checkbox to the left of each of the desired groups.

b) Click **Assign** to move the selected groups to the **Selected Groups** table or click **Assign All** to move all of the groups to the **Selected Groups** table.

c) To remove group access, select the checkbox to the left of each of the desired groups.

d) Click **Remove** to remove the selected groups from the **Selected Groups** table or click **Remove All** to remove all of the groups from the Selected Groups table.

Granting access to a Device Group gives permission to all devices within that group, regardless of the options selected within the **Devices** tab.

6. Select the **Devices** tab, to define which devices the users assigned this role will be able to access.

a) To assign device access, select the checkbox to the left of each of the desired devices.

b) Click **Assign** to move the selected devices to the **Selected Devices** table or click Assign All to move all of the devices to the Selected Devices table.

c) To remove device access, select the checkbox to the left of each of the desired devices.

d) Click **Remove** to remove the selected devices from the **Selected Devices** table or click **Remove All** to remove all of the devices from the **Selected Devices** table.

7. Click **OK**.

Step Result: The wizard saves your changes and closes.

Assigning a User Role to an Existing User

User roles are assigned to users when you create or add a user.

Note: At any given time, ZENworks Patch Management must have at least one user assigned the Administrator role.

1. In the **Users** tab, select the user profile that will be assigned the user role.

2. Click **Edit User Details**.

    Step Result: The *Edit User Wizard* opens.

Figure 123: Edit User Wizard - User Information Page

3. Edit the user as defined in *Editing User Profiles* on page 228, changing the role as desired.

4. Click **Finish** to save your selections.

5. Click **Close** to exit the *Edit User Wizard*.

Disabling User Roles

You can disable any non-system role, allowing you to continue maintaining the role within ZENworks Patch Management but restricting its assignment to any users.

You cannot disable the system defined User Roles (*Administrator*, *Manager*, *Operator*, and *Guest*).

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

2. Ensure the page filter (**Status**) is *not* set to Disabled.

3. Click **Update View** to populate the tab.

4. Select the role or roles to disable.

5. Click **Disable**.

Result: The role is disabled.

> **Note:** If you disable a role that is assigned to a user, the user will be able to log on to the Patch Management Server, but will be unable to view any pages.

Enabling User Roles

You can enable, edit, and delete disabled roles. Disabled user roles appear with a gray background in the list of user roles on the *User Management* page.

1. From the Users view, select the **Roles** tab.
2. Ensure the page filter (**Status**) is set to All or Disabled.
3. Click **Update View** to populate the tab.
4. Select the disabled role or roles to enable.
5. Click **Enable**.

Result: The roles are re-enabled.

Deleting User Roles

Removing a role deletes the role and its data from the Patch Management Server database. In order to remove a role, it must first be disabled. You cannot delete a system role.

1. From the *Users* view, select the **Roles** tab.
2. Ensure the **Status** filter is set to All or Disabled.
3. Click **Update View** to populate the tab.
4. Select the role or roles to delete.

   Note: You cannot delete Enabled User Roles or the system defined User Roles (*Administrator*, *Manager*, *Operator*, and *Guest*).

5. Click **Delete**.

Result: The disabled User Role is deleted.

Caution: If you delete a role that is assigned to a user, the user will be able to log on to the Patch Management Server, but will be unable to view any pages.

Chapter

9

Configuring Default Behavior

In this chapter:

- *About the Options Page*
- *Viewing Subscription Service Information*
- *Supporting Red Hat Enterprise and Sun Solaris Agents*
- *Verifying Subscription Licenses*
- *Default Configuration*
- *Working With Agent Policy Sets*
- *Using E-Mail Notification*
- *Technical Support Information*

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

About the Options Page

The *Options* page is available by clicking **Options** on the main toolbar. The page comprises six management and configuration views as individual tabs.

Viewing Configuration Options

Configuration options are viewable from the *Options* page.

1. From the Main menu, select **Options**.

    Step Result: The *Options* page displays with the *Subscription Service* tab as the default view.

Figure 124: Configuration Options

2. Select a tab to view the desired Patch Management Server details.

Viewing Subscription Service Information

The *Subscription Service* page allows you to modify the Subscription Communication interval, initiate a standard or full replication, configure the subscription service, and view Subscription Service history and status information.

Figure 125: Subscription Service Tab

Patch Management Agents gather a list of software, hardware, services and patches installed on each agent within the network. With this detailed information, the Patch Management Server generates a complete analysis of your network to identify the patches, hot fixes, service packs and updates of importance to your network.

The Patch Management Server connects to the Global Subscription Server (GSS) once daily to download a series of vulnerability definitions and packages.

Table 114: Subscription Service Tab Page Functions

Button	Function
Save	Saves changes made to the subscription communication interval.
Update Now	Initiates replication of the Patch Management Server with the Global Subscription Server. This option retrieves the changes made since your last replication.

Button	Function
Reset	Resets the replication status and initiates a complete replication with the Global Subscription Server.
	Note: Once you click **Reset**, a confirmation window opens stating the replication status has been reset and you can choose whether to initiate the replication process by clicking **OK**, or wait until a later time, by clicking **Cancel**.
Configure	Opens the *Subscription Service Configuration* page.
Export	The **Export** button allows you to export subscription data to a comma separated value (*.csv*) file. See *Exporting Data* on page 33 for additional information.

Subscription Service Information

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

Table 115: Subscription Service Information

Information	Description
Last Subscription Poll	Date and time of the last successful contact with Patch Management Server.
Subscription Replication Status	Current replication status. Replication ensures that the Patch Management Server remains current with the latest vulnerability, package, and license information.
Account ID	Passed to the Global Subscription Server and validates the request. The account ID is created by the Patch Management Server when it registers with the Global Subscription Server.
Subscription Communication Interval	Time frame for connecting to the Global Subscription Server and retrieving updates.
	Note: If you modify the **Subscription Communication Interval** you must save the changes by clicking **Save** on the Action Menu.
Subscription Host	URL and port of the Global Subscription Server.

Subscription Service History

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

Field	Description
Type	Defines the type of task, the available types include: • **Licenses** - Verifies the validity of your Patch Management Server license. • **Vulnerabilities** - Downloads the current vulnerabilities according to the subscription type defined for the account. • **Packages** - Downloads the current packages based upon the vulnerabilities selected for deployment.
Status	The status of the task. While the task is active, the process begins with a status of *Initializing Replication*, followed by downloads. When the task is finished, the status is *Completed*.
Start Date	The date and time the task started.
Stop Date	The date and time the task completed.
Duration	Indicates the duration of the task. This is shown in seconds or minutes.
Successful	Confirms communication settings between your Patch Management Server and the Global Subscription Server.

Subscription Service Configuration

The *Subscription Service Configuration* page allows you to perform the following actions:

- View your current status.
- Define your proxy.
- Define communication settings.
- Set the user interface language.
- Enable or disable enhanced content.

Figure 126: Subscription Service Configuration

The following table describes the available functions in the *Subscription Service Configuration* window.

Table 116: Subscription Service Configuration Functions

Button	Function
Restart	Stops and restarts the Global Subscription Server. This button is located on the Service tab.
Save	Saves any changes to the database, then closes the *Subscription Service Configuration* window.

Button	Function
Cancel	Closes the *Subscription Service Configuration* window without saving changes.
Apply	Saves changes to the database, without closing the *Subscription Service Configuration* window.

Accessing the Configuration Page

The *Subscription Service Configuration* page allows you to view and define your Patch Management Server communication settings.

1. Select the **Options** tab.

    Step Result: The *Configuration Options* window opens with the Subscription Service tab displaying as the default.

2. Click **Configure**.

    Step Result: The *Subscription Service Configuration* window opens.

Figure 127: Subscription Service Configuration Page

Subscription Service Status

The following table describes the fields within the **Status** area of the *Subscription Service Configuration* window's *Service* tab.

Field	Description
Service Status	The current status of the local Subscription Service's communication with the Global Subscription Server.
Last Checked	The last date and time the local Subscription Service contacted the Global Subscription Server.
Next Check	The next scheduled date and time for the local Subscription Service to contact the Global Subscription Server.

Subscription Service Proxy Configuration

The following table describes the fields within the **Proxy** area of the *Subscription Service Configuration* window's *Service* tab.

Table 117: Subscription Service Proxy Field Descriptions

Field	Description
Address	Uses the defined proxy address when connecting to the Global Subscription Server.
Port	Uses the defined proxy port when connecting to the Global Subscription Server.
Authenticated	When using an authenticated proxy, you must provide a valid user name.
User Name	When using an authenticated proxy, you must provide a valid user name.
Password **Confirm Password**	The password associated with the defined proxy user.

Subscription Service Communication Settings

The following table describes the fields within the **Communication** area of the *Subscription Service Configuration* window's *Service* tab.

Table 118: Subscription Service Communication Field Descriptions

Field	Description
Logging Level	The level of detail recorded to the Subscription Service Log. Options include: *Debug*, *Info*, *Warn*, *Error*, and *Fatal*.

Field	Description
Use SSL	Enable SSL for use when communicating with the Global Subscription Server.
Enable Bandwidth Throttling	Enables the Kilobytes per second field, allowing you to set the maximum bandwidth used when communicating with the Global Subscription Server.
__ Kbytes per second	The maximum Kbytes per second used when communicating with the Global Subscription Server.
Retry Limit	The number of times the Patch Management Server attempts to establish a connection with the Global Subscription Server.
Retry Wait	The number of seconds between retries.
Connect Timeout	The number of seconds before a connection will be considered unsuccessful (when the connection time-outs, it will be retried based upon the **Retry Limit** and **Retry Wait** values).
Command Timeout	The seconds of inactivity before a command will be considered unsuccessful.

Setting the Vulnerability and Package Languages

The *Subscription Service Configuration* window's *Languages* tab displays the various vulnerability and package languages available.

1. Select the **Options** tab.

> **Step Result:** The *Configuration Options* window opens with the *Subscription Service* tab displaying as the default.

2. Click **Configure**.

> **Step Result:** The *Subscription Service Configuration* window opens.

3. Select the *Languages* tab.

> **Step Result:** The *Subscription Service Configuration* window's *Language* tab displays.
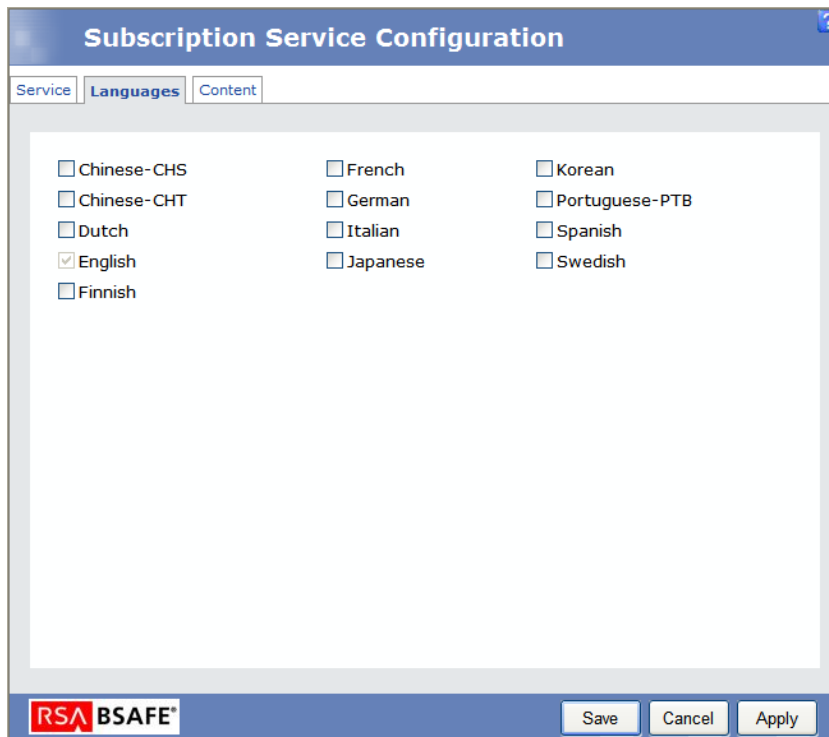
Figure 128: Subscription Service Configuration Language Tab

4. Select the check box corresponding to the language that you want to display.

5. Click **Apply**.

6. Click **Save**.

Configuring Enhanced Content

The *Subscription Service Configuration* window allows you to enable, disable, and export enhanced content. Enhanced content streamlines the manner in which applicable updates are detected by applying vendor tools to detect available and applicable updates.

Enabling Enhanced Content

Enabling Enhanced Content streamlines the manner in which applicable updates are detected by ZENworks Patch Management.

1. Select the **Options** tab.

    Step Result: The *Configuration Options* window opens with the *Subscription Service* tab displaying as the default.

2. Click **Configure**.

    Step Result: The *Subscription Service Configuration* window opens.

3. Select the **Content** tab.

    Step Result: The *Subscription Service Configuration* window's *Content* tab displays.
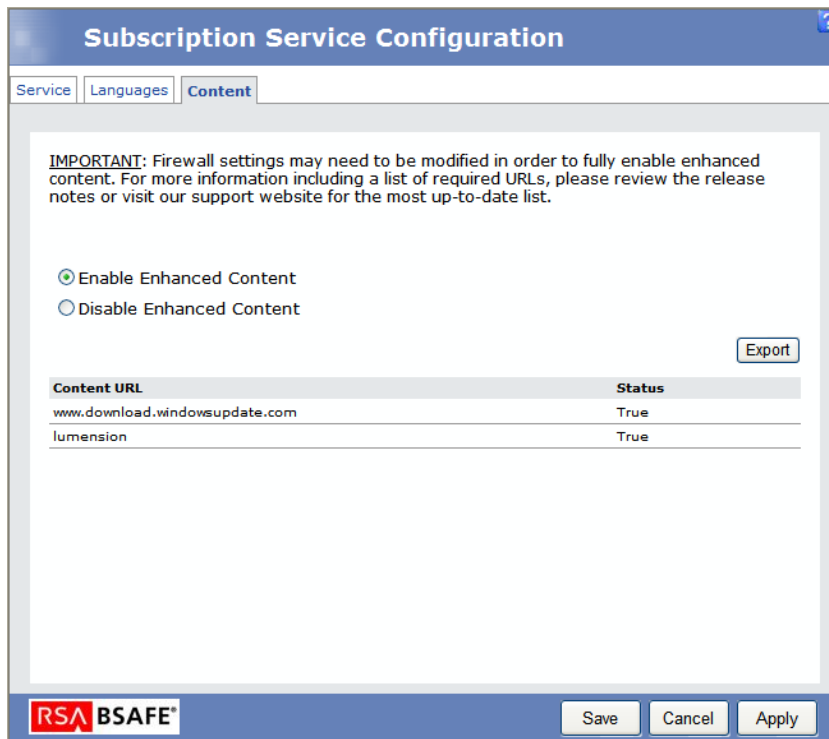
Figure 129: Subscription Service Configuration Content Tab

4. Select the **Enable Enhanced Content** option.

5. Click **Apply**.

6. Click **Save**.

After Completing This Task:

To support Red Hat Enterprise Linux, you must also allow outbound access through ports 80 and 443 to *http://rhn.redhat.com*.

To support Sun Solaris, you must also allow outbound access through ports 80 and 443 to *https://identity.sun.com/amserver/UI/Login*, *http://sunsolve.sun.com/*, *http://sunsolve.sun.com/show.do?target=home*, and *http://sunsolve.sun.com/pdownload.do*.

Disabling Enhanced Content

The following procedure will walk you through disabling the Enhanced Content functionality of ZENworks Patch Management.

1. Select the **Options** tab.

> **Step Result:** The *Configuration Options* window opens with the *Subscription Service* tab displaying as the default.

2. Click **Configure**.

> **Step Result:** The *Subscription Service Configuration* window opens.

3. Select the **Content** tab.

> **Step Result:** The *Subscription Service Configuration* window's *Content* tab displays.

4. Select the **Disable Enhanced Content** option.

5. Click **Apply**.

6. Click **Save**.

Exporting Enhanced Content Data

Enhanced Content data can be exported to a *.csv* file using the following procedure.

1. Select the **Options** tab.

> **Step Result:** The *Configuration Options* window opens with the *Subscription Service* tab displaying as the default.

2. Click **Configure**.

> **Step Result:** The *Subscription Service Configuration* window opens.

3. Select the **Content** tab.

> **Step Result:** The *Subscription Service Configuration* window's *Content* tab displays.

4. Click **Export**.

> **Step Result:** A File Download dialog opens.

5. Click **Open** to open the *.csv* file containing the export data.

6. Click **Save** to save the *.csv* file containing the export data.

7. Click **Cancel** to return to the *Content* tab, canceling the file export.

Supporting Red Hat Enterprise and Sun Solaris Agents

Red Hat and Sun Microsystems require users to subscribe to the *Red Hat Network* and the *Sun Microsystems SunSolve Support Site* prior to downloading patches for Red Hat Enterprise Linux or Sun Solaris. Therefore, prior to patching your Red Hat or Sun Solaris systems, using ZENworks Patch Management, you must configure your Patch Management Server to use your Red Hat Network and SunSolve subscription credentials when downloading and patching your Red Hat Enterprise and Sun Solaris Agents.

Attention: To patch your Red Hat Enterprise Agents, you must have Management Entitlement's. If you do not have Management Entitlements for your Red Hat Enterprise systems, please visit *https://rhn.redhat.com*.

To configure Patch Management Server to use your Red Hat Network and SunSolve subscription credentials you must perform the following tasks:

1. Obtain valid subscriptions, and login credentials, to the Red Hat Network and/or the Sun Microsystems SunSolve Support Site.
2. Enable Enhanced Content within your Patch Management Server. For details refer to *Enabling Enhanced Content* on page 248.
3. Configure the Content Credentials Manager. For details refer to *Content Credentials Manager* on page 252.

Enabling Enhanced Content

Enabling Enhanced Content streamlines the manner in which applicable updates are detected by ZENworks Patch Management.

1. Select the **Options** tab.

> **Step Result:** The *Configuration Options* window opens with the *Subscription Service* tab displaying as the default.

2. Click **Configure**.

> **Step Result:** The *Subscription Service Configuration* window opens.

3. Select the **Content** tab.

> **Step Result:** The *Subscription Service Configuration* window's *Content* tab displays.
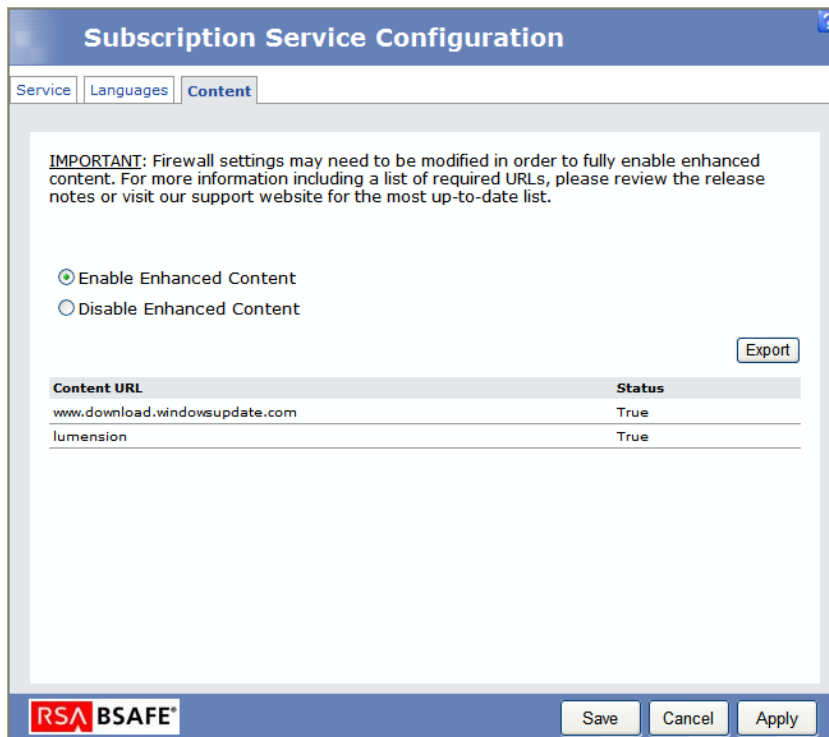
Figure 130: Subscription Service Configuration Content Tab

4. Select the **Enable Enhanced Content** option.

5. Click **Apply**.

6. Click **Save**.

After Completing This Task:

To support Red Hat Enterprise Linux, you must also allow outbound access through ports 80 and 443 to *http://rhn.redhat.com*.

To support Sun Solaris, you must also allow outbound access through ports 80 and 443 to *https://identity.sun.com/amserver/UI/Login*, *http://sunsolve.sun.com/*, *http://sunsolve.sun.com/show.do?target=home*, and *http://sunsolve.sun.com/pdownload.do*.

Content Credentials Manager

The Content Credentials Manager is downloaded to the Patch Management Server during the first replication after installing ZENworks Patch Management 6.4 SP2. The Content Credentials

Manager allows you to register your Patch Management Server to receive entitled content. This registration process only needs to be completed once for each entitled content type.

Red Hat Enterprise Linux Content Support

Novell offers patch and remediation support for the following versions of Red Hat Enterprise Linux:

- Red Hat Enterprise Linux 3 (AS, ES, or WS, x86 or x86_64)
- Red Hat Enterprise Linux 4 (AS, ES, or WS, x86 or x86_64)
- Red Hat Enterprise Linux 5 (Server or Client, x86 or x86_64)

Configure Red Hat Network Credentials

Prerequisites:
To patch your Red Hat Enterprise Agents, you must have Management Entitlement's. If you do not have Management Entitlements for your Red Hat Enterprise systems, please visit *https://rhn.redhat.com*.

---

1. Select the **Options** tab.

   Step Result: The *Configuration Options* window opens with the *Subscription Service* tab displaying as the default.

2. Click **Update Now**.

   Step Result: Replication between your Patch Management Server and the Global Subscription Server begins.

3. When the replication is complete, Open a command prompt to *<Program Files>\Novell \ZENworks Patch Management Server\Replication Services*.

4. Run the following from the command prompt (entering your Red Hat Network Information as appropriate).

   Example:

   ```
   CredentialsManager /source:redhat /u:<RedHatUserName>
   /p:<RedHatPassword> /hostname:<MyServerName>
   /release:<RedHatRelease> /arch:<RedHatArchitecture>
   ```

   - For <RedHatRelease>, use one of the following releases: 3AS, 3ES, 3WS, 4AS, 4ES, 4WS, 5Server, or 5Client.
   - For <RedHatArchitecture>, use one of the following architectures: i386 or x86_64

   Step Result: A warning indicating that registering your server with the Credentials Management tool may result in a loss of patch deployment history and will increase replication time is displayed.

5. Acknowledge the warning by typing Y to confirm the registration.

> **Note:** Steps 4 and 5 must be repeated for each Red Hat subscription that ZENworks Patch Management will remediate. For example, if you wish to remediate RHEL 4 AS, RHEL 4 ES, and RHEL 5 Server, you must perform these steps three times.

6. Validate the systemid for the ServerName used.
   a) Navigate to *http://rhn.redhat.com*.
   b) Log in using the same Username/Password combination used in step 4.
   c) Search for Systems matching the ServerName entered in step 4.
   d) Validate that the server matches the expected subscription.

7. You can now remediate your Red Hat Enterprise Linux machines through the standard ZENworks Patch Management user interface.

Sun Solaris Content Support

Novell offers patch and remediation support for the following versions of Sun Solaris:

- Sun Solaris 8 SPARC
- Sun Solaris 9 SPARC
- Sun Solaris 10 SPARC
- Sun Solaris 10 x86
- Sun Solaris 10 x86_64

Configure SunSolve Credentials

1. Select the **Options** tab.

> **Step Result:** The *Configuration Options* window opens with the *Subscription Service* tab displaying as the default.

2. Click **Update Now**.

> **Step Result:** Replication between your Patch Management Server and the Global Subscription Server begins.

3. When the replication is complete, Open a command prompt to *<Program Files>\Novell \ZENworks Patch Management Server\Replication Services*.

4. Run the following from the command prompt (entering your Sun Solaris Network Information as appropriate).

> **Example:**
> ```
> CredentialsManager /source:solaris /username:<SolarisUserName>
> /password:<SolarisPassword> /vendor:sun
> ```

5. You can now remediate your Sun Solaris machines through the standard ZENworks Patch Management user interface.

Verifying Subscription Licenses

The *Products* page allows you to view, validate and export license information. The page provides a summary of all product, third-party software, and plug-in component licenses that are part of your patch management activities. This information is updated as part of the daily replication with the Global Subscription Server.

Figure 131: Products Tab

Table 119: Products Tab Page Functions

Button	Function
Validate	Initiates a license replication that searches for any changes to your license data.
Export	Exports license data to a comma separated value (*.CSV*) file. See *Exporting Data* on page 33 for additional information.

Product Information

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

Table 120: License Availability

License	Description
License In Use	The total number of licenses in use by registered agents.
License Available	The total number of licenses available for use.
Total Non-Expired Licenses	The total number of licenses active and available for use. This number represents a sum of available licenses.

License summary information is presented according to license group. A license group is defined as a block of licenses purchased at a time. For example, you may have 3 license groups

comprising 500 total licenses with a group of 300 licenses purchased initially, and two additional groups of 100 licenses each added during subsequent quarters.

The license group information includes the following information.

Table 121: License Group Information

Field	Description
Description	The license name or description.
Purchase Date	The date the license group was purchased.
Vendor	The source of the license. Click the vendor name to open a Web browser to the vendor's home page.
Effective Date	The date the license(s) went into effect. This is the first day that the licenses were valid, not necessarily the installation date.
Expiration	The date the license(s) expires.
Purchased	The number of licenses in this group.

Default Configuration

The Patch Management Server **Configuration** page lets you establish, modify and export the Deployment Defaults, Agent Defaults (Default Agent Policy), ISAPI Communication, and User Interface settings.

Figure 132: Configuration Tab

Table 122: Configuration Tab Page Functions

Button	Function
Save	Saves any changes made on this page. **Caution:** If you make any changes, you must click **Save** to save those changes. If you do not click **Save**, the system will return to the last saved settings when you navigate away from the *Configuration* page.
Export	Allows you to export the configuration information to a comma separated value (*.csv*) file. See *Exporting Data* on page 33 for additional information.

Configuring Deployment Defaults

The Deployment Defaults area establishes the global deployment limitations.

Figure 133: Configuration Tab - Deployment Defaults

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

Table 123: Deployment Defaults

Deployment Setting	Description
Concurrent	
Maximum number of Deployments that can run simultaneously (Deployment Limit)	The maximum amount of agents that can receive simultaneous deployments.
Maximum number of Discover Applicable Update System tasks that can be run simultaneously (DAU)	The maximum number of agents that can receive the DAU System Task at the same time.
Maximum number of Reboot tasks that can be run simultaneously	The maximum number of agents that can receive a simultaneous deployment requiring a reboot.
Maximum number of Simultaneous mandatory baseline deployments	The maximum number of agents that can receive simultaneous mandator baseline deployments.
Consecutive	

Deployment Setting	Description
Maximum number of times a deployment will be consecutively attempted	The number of failed deployment attempts permitted before Update Server disables the deployment. However, this does not apply to mandatory baseline deployments.

Configuring Agent Defaults

Agent defaults allows for establishing default behavior for the deployment agent.

Figure 134: Configuration Tab - Agent Defaults

Communication

Agent communication settings are defined in the *Communication* section of the *Configuration* page. The following table describes the fields within this section.

Table 124: Agent Communication Settings

Field	Description
Agents should be shown Offline when inactive for	Configures a time interval (defined in minutes, hours or days) that must elapse before an agent is considered to be offline. Agents are noted as being offline when they have not communicated with Patch Management Server for the defined period of time. If an agent is disabled or uninstalled it does not appear as offline. When disabled, an agent is considered offline after failing to connect to the Patch Management Server after two of its communication intervals.

Field	Description
Agent Uniqueness Based On	Defines the Agent Uniqueness method used to identify agents. Options are: • **Instance** - Validates using instanced validation. Instanced validation, when determining agent uniqueness, uses logic which does not rely upon the device name. • **Device Name** - Validates based on the device name.

Notification Defaults

Applies to deployments where a notification is required. The behavior defined in this section may be overridden within a Agent Policy or on a per-deployment basis using the Deployment Wizard.

Table 125: Agent Notification Defaults

Field	Description
User Notification window should always be on top	Selection of this option will force all notification windows to display on top of other windows.
Manual Installation	Edit and display a message advising the user that the package still requires installation. (Maximum of 256 characters.)
Default Deployment Message	Edit and display the default message advising the user that a deployment is about to begin. (Maximum of 256 characters.)
May Reboot	Edit and display a message advising the user that the computer may be rebooted. (Maximum of 256 characters.)
Default Reboot Message	Edit and display the default message advising the user that the computer requires a reboot. (Maximum of 256 characters.)
Legacy Agents have a Notification Timeout	Time allotment for the notification window to display for pre-6.3 agents.
Legacy Agents have a Snooze Duration	Maximum time allotment the agent can be set to snooze for pre-6.3 agents.

Discover Applicable Updates

Applies to events which can initiate a Discover Applicable Updates (DAU) task.

Table 126: Agent Discover Applicable Updates Defaults

Field	Description
Should be run after Subscription Replication	Select this option if you want the Discover Applicable Updates (DAU) task to run after your local subscription server communicates with the Global Subscription Server.
Should be run after Agent detects inventory change	Select this option if you want the DAU task to run when the agent detects changes to Inventory.

Absentee Agent Management

The Absentee Agent option allows for removing an agent that has failed to communicate with the server.

Table 127: Absentee Agent Settings

Field	Description
Delete Absentee Agent after	Removes uncommunicative agents after the set time frame. Runs, daily at 12:30 AM. If set to zero, this function is disabled.

Configuring User Interface Defaults

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

Figure 135: Configuration Tab - User Interface Defaults

Table 128: User Interface Defaults

Field	Description
Display _ Rows Per Page	Allows you to set the default number of rows [25, 50, 100, 200, 500, or 1000] displayed within Patch Management Server. The setting applies to users who have not set their own parameters.
Password Expiration Notification should be displayed in _ days	Allows you to define when users will start receiving warnings regarding when their password will expire.

Field	Description
Cache Timeout	Allows you to define the maximum amount of time in minutes before the data grid will refresh (updated from the database).
How should Deployment Wizard Start Times be displayed?	• **Agent Local Time** - Sets the deployment wizard to default to the agent local time. • **Agent UTC Time** - Sets the deployment wizard to default to UTC time.
Activate Automatic IP Collection Grouping	Automatically groups agents by IP Group.

Note: Patch Management Server default security settings prohibit the use of any browser other than Internet Explorer 6 SP1 and above.

Customizing Row Values

The *Customize Row Values* page allows you to define the amount of rows you want to display when using Patch Management Server.

1. On the *Configuration* page, click **Modify**.

>   **Step Result:** The *Customize Row Values* window opens.
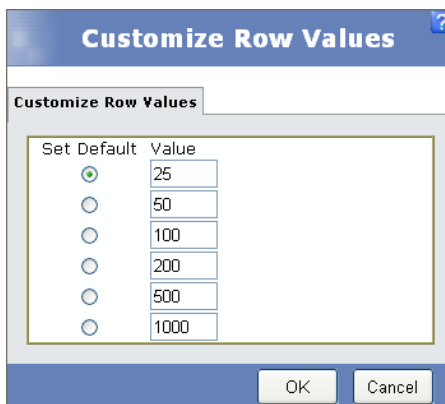
Figure 136: Customize Row Values

2. If needed, type a new row value in the **Value** field.

3. Set the default value by selecting the desired **Set Default** radio button.

4. Click **OK**.

Result: The custom row values and default setting is saved, and the *Customize Row Values* window closes.

Configuring ISAPI Communication Settings

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

Figure 137: Configuration Tab - ISAPI Communication Settings

Concurrent Agent Limit

Defines the maximum number of threads used by ZENworks Patch Management.

Table 129: Concurrent Agent Limit

Field	Description
SQL Default (64 threads)	Select to enable the recommended thread count for a SQL Server implementation.
Custom Setting	Select to define a custom (between 5 and 256) thread count.

Connection Timeout

The time (in seconds) before an ISAPI thread expires (times out).

Table 130: Connection Timeout

Field	Description
Default	Select to set the Connection timeout to the default value of 30 seconds.
Custom Setting	Select to define a custom (between 5 and 300 seconds) timeout setting.

Command Timeout

The time (in seconds) before an ISAPI command expires (times out).

Table 131: Command Timeout

Field	Description
Default	Select to set the Command timeout to the default value of 30 seconds.

Field	Description
Custom Setting	Select to define a custom (between 5 and 900 seconds) timeout setting.

Working With Agent Policy Sets

Agent Policies are the key element in defining agent behavior. Agent Policies consist of the rules for communicating with the Patch Management Server and define settings such as communication interval, deployment notification options, reboot notification options, logging levels, discovery mode, and hours of operation.

Agent policies are assigned to agents by assigning Agent Policy Sets to Device Groups. The policy values are then assigned to the agents based upon their group membership. When agents or groups are assigned conflicting policies, the conflict resolution rules found under *Defining Agent Policy Conflict Resolution* on page 278 are applied. Any agent that does not have all of the policies defined by it's various group memberships will have any missing policy values defined by the Global System Policy.

The Agent Policies Sets page allows you to define the behavior of the Update Agent. Click **Options** in the tool bar and then click the **Policies** tab.
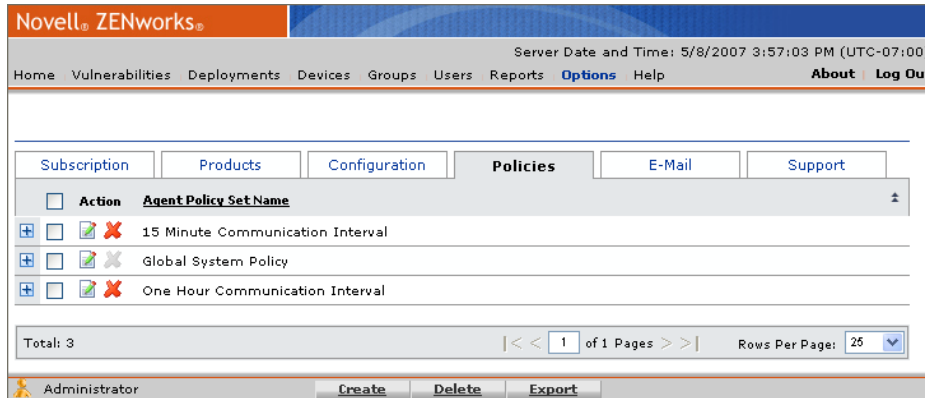
Figure 138: Agent Policy Set Tab

The following functions are available when using Policy Sets.

Table 132: Policy Sets Page Functions

Button	Function
Create	Creates a new Agent Policy Set.
Delete	Deletes an existing Agent Policy Set.

Button	Function
Export	Exports policy data to a comma separated value (*.csv*) file. See *Exporting Data* on page 33 for additional information.

Table 133: Policy Sets Column Functions

Icon	Name	Function
	Edit	Edits the associated Agent Policy Set.
	Delete	Deletes the associated Agent Policy Set.

Viewing Agent Policy Summary Information

Expanding an Agent Policy set listing displays information regarding each policy as illustrated in the following figure.
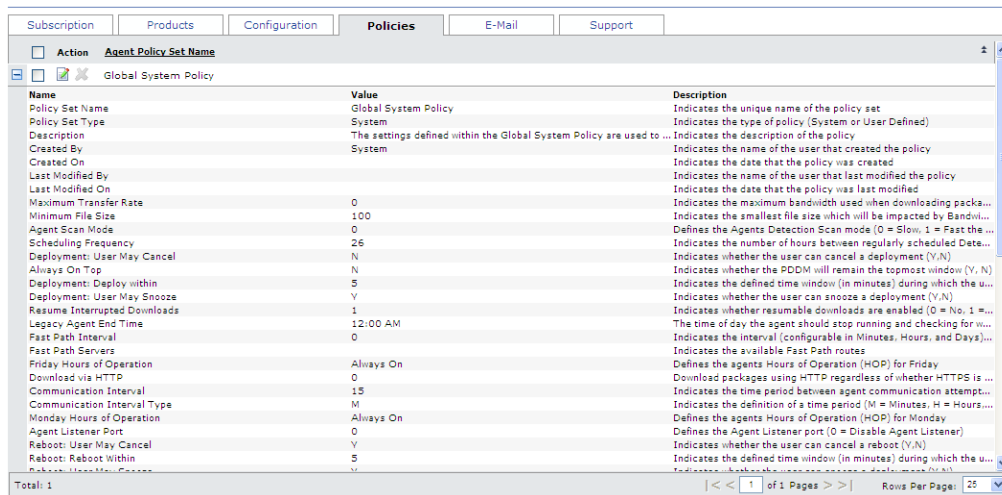
Figure 139: Agent Policies

Creating a Policy Set

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

1. Open the Agent Policy Sets page (**Options** > **Policies**).

2. Click Create.

Step Result: The Create a Policy Set window opens.

Figure 140: Create a Policy Set

3. In the *Policy Set Information* tab, click within the fields to activate the options.

The following table lists and describes the available agent policies.

Table 134: Agent Policy Set Descriptions

Name	Description
Policy Set Details	
Policy Set Name	The name designated to the policy. Limited to 256 characters.

Name	Description
Policy Set Description	The description attributed to the policy.
Communication	
Logging Level	The agent logging level. Levels include: • **None** - Only errors are logged and recorded. • **Basic Information** - Captures all errors and basic system and usage information. • **Detailed** - Captures all errors and the major system actions. • **Debug** - Captures all errors and system actions.
Agent Scan Mode	The mode in which the Discover Applicable Updates task runs. Levels include: • **Fast Scan** - Always run in Fast mode, performs the discovery faster but uses more resources. • **Initial Only** - Performs the first discovery scan in Fast mode and subsequent scans in Normal mode. • **Normal** - Always run in normal mode, performs the scan using the least amount of resources.
Communication Interval	The interval (in minutes, hours or days) between each communication between the agent and server.
Agent Listener Port	When contacted on this port, the agent will respond with the current version and initiate communication with server. A value of 0 (zero) turns the agent listener off.
Inventory Collection Options	Launches the *Select Inventory Collection* page, allowing the selection of which inventory values to record during collection.
Resume Interrupted Downloads	When enabled, the agent will resume interrupted downloads at the point of interruption.
Hours of Operation	Launches the *Edit Agent Policy Set* page. Hours of Operation is based on Agent local time and allows for further definition of the Agent start and end times. This page may contain a Legacy Agent Hours of Operation if the appropriate box was checked in the *Configuration Defaults Communications* Section.

Name	Description
Download via HTTP	Download packages using HTTP regardless of whether HTTPS is used for agent to server communication.
Legacy Agent Start Time	Relates to Hours of Operation settings. Identifies when the agent can begin communication.
Legacy Agent End Time	Relates to Hours of Operation settings. Identifies when the agent must suspend communication.
Deployment Notification Defaults	
User May Cancel	User can cancel the deployment.
User May Snooze	User can snooze the deployment.
Deploy within	Snooze or cancel the deployment time window, in minutes. When the defined Offset has elapsed, the deployment will automatically occur.
Always on Top	Selection of this option keeps this window on top of all other windows until the recipient acknowledges the notification by selecting a valid option (Snooze, Cancel, Deploy, or Reboot).
Reboot Notification Defaults	
User May Cancel	User can cancel the reboot.
User May Snooze	User can snooze the reboot.
Reboot Within	Snooze or cancel the reboot time window, in minutes. When the defined Offset has elapsed, the reboot will automatically occur.
Discover Applicable Updates (DAU)	
Scheduling Frequency	Defines how often the agent must perform a Discover Applicable Updates (DAU). The value here indicates the maximum amount of time between scans.
FastPath Servers	
FastPath Interval	The time interval between agent and server communication. The interval can be defined in minutes, hours, or days.
Servers	Provides a listing of the Fastpath servers the agents can use when communicating with server.
Bandwidth Throttling	

Name	Description
Maximum Transfer Rate	Defines the maximum amount of bandwidth used when downloading packages to an Agent. A setting of zero (0) will disable Bandwidth Throttling.
Minimum File Size	The smallest file size which will be impacted by Bandwidth Throttling.

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

Editing a Policy Set

The *Edit a Policy Set* wizard allows you to modify an agent policy and the policies behavior.

1. Select the **Agent Policy Set** you wish to edit.

2. Select the **Edit** icon to the left of the policy.

   Step Result: The *Edit a Policy Set* window opens.

Figure 141: Edit a Policy Set

3. Edit the policy set as desired.

   Refer to *Creating a Policy Set* on page 265 for details regarding the available policy options.

4. Click **Save** to save your changes.

Deleting a Policy Set

You can delete a policy at any time. Deleting a policy will delete the policy from the database and any groups associated to the policy are automatically associated to the default policy.

1. Click **Options**.

2. In the Options page, click **Policies**.

Step Result: The *Policies* tab is displayed.
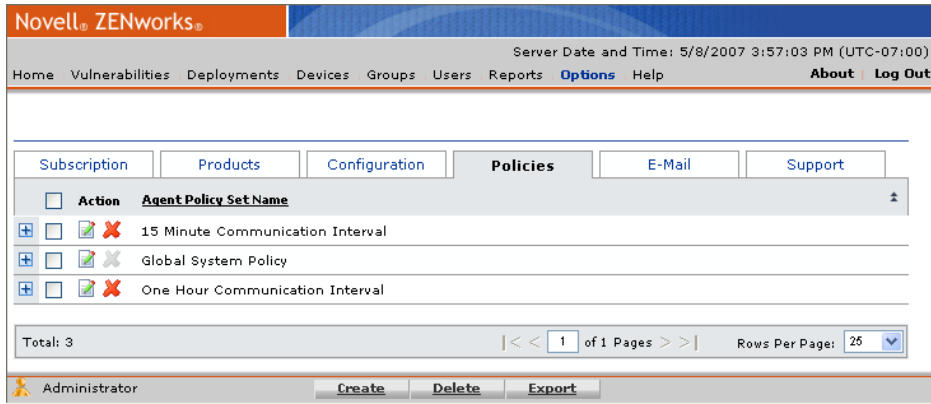
Figure 142: Agent Policy Sets

3. Select the policy to remove by selecting the checkbox to the left of the policy.

4. Click **Delete**.

Step Result: A *Delete Confirmation* dialog opens.

5. Click **Yes** to acknowledge the deletion.

Result: The policy is deleted from the system.

Defining Inventory Collection Options

The Select Inventory Collection page allows you to chose the inventory items collected by the Discover Applicable Updates (DAU) task.
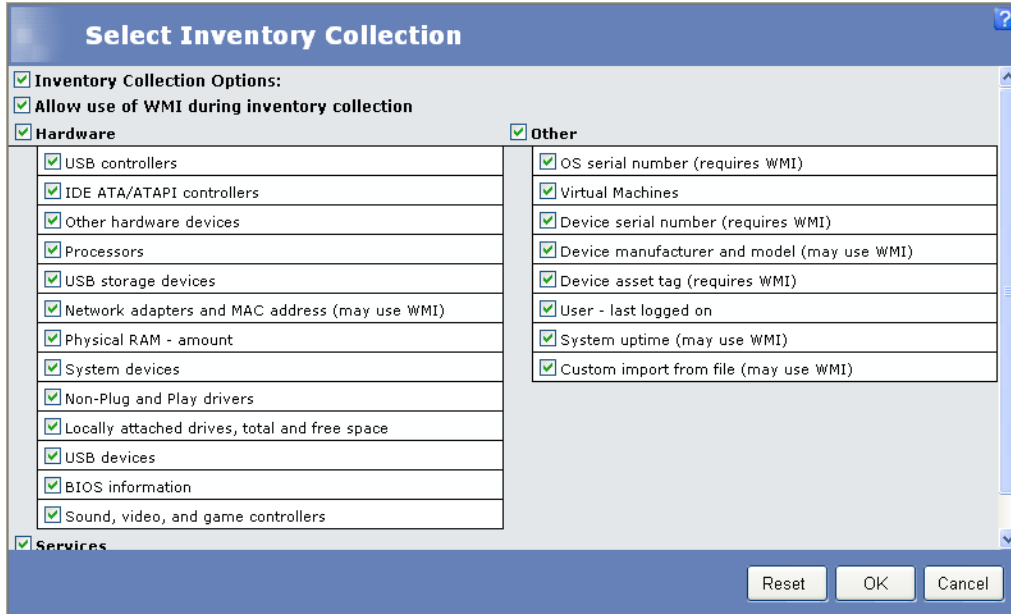
Figure 143: Inventory Collection Options

Button	Function
Reset	Resets the window, returning to the previous settings.
OK	Closes the window (saving changes).
Cancel	Cancels all changes and closes the window.

Setting Inventory Collection Options

The following procedure will walk you through setting the inventory collection options.

1. Open *Create/Edit Policy* Set.

   Step Result: The *Create/Edit a Policy Set* window opens.

2. Scroll to the Inventory Collection area, and click **Define**.

   Step Result: The *Select Inventory Collection* window opens.

3. Select and define the inventory options.

Table 135: Inventory Collection Options

Inventory Option	Description
Inventory Collection Options	Deselecting this option will deselect all inventory collection options.
Allow use of WMI during inventory collection	Required if WMI data will be gathered. Deselecting this option will deselect all inventory options which require WMI.
Hardware	Deselecting this option will deselect all Hardware inventory options.
USB Controllers	Scan for data regarding USB Device inventory (from *...\Enum \USB*).
IDE ATA/ATAPI Controllers	Scan for data regarding IDE ATA/ATAPI controllers.
Other Hardware Devices	Scan for system device data.
Processors	Scan for processor data.
USB Storage Devices	Scan for data regarding USB device inventory (from *...\Enum \USBSTOR*).
Network Adapters and MAC Addresses (may use WMI)	Scan for data regarding network adapters.
Physical RAM - amount	Scan the devices physical RAM.
System Devices	Scan the Windows Registry for additional hardware information.
Non-Plug and Play drivers	Scan for data regarding non-Plug and Play drivers.
Locally attached drives, total and free space	Scan for data regarding disk drives.
USB Devices	Scan for data regarding USB devices.
BIOS Information	Scan for BIOS data.
Sound, Video, and Game Controllers	Scan for data regarding sound, video, and game controllers.

Inventory Option	Description
OS Serial Number (requires WMI)	Scan for the Operating System serial number.
Virtual Machines	Scan to determine if device is a virtual machine.
Device Serial Number (requires WMI)	Scan for the device serial number.
Device Manufacturer and Model (may use WMI)	Scan for the device manufacturer and model.
Device Asset Tag (requires WMI)	Scan for the device's asset tag.
User - Last Logged On	Scan for last logged in user and time.
System Uptime (may use WMI)	Scan for and return the time since last reboot (system uptime).
Custom import from file (may use WMI)	Scan for a file containing custom inventory data. See *Using Custom Inventory* on page 146 for additional information.
Services	Scans for a listing of Windows services (not applicable for Windows 9x or ME).
Software	Scans for a listing of installed software.

4. Click **OK**.

Result: The *Inventory Collection Options* window closes, saving your changes.

> **Caution:** Changes made to the *Inventory Collection Options* will not be saved until you have selected **Save** on the originating page.

Defining Agent Hours of Operation

Agent communication can be enabled or disabled to restrict agent communication with the Patch Management Server to a specific time range only.

Note: Hours of Operation is based on the Agent's local time.
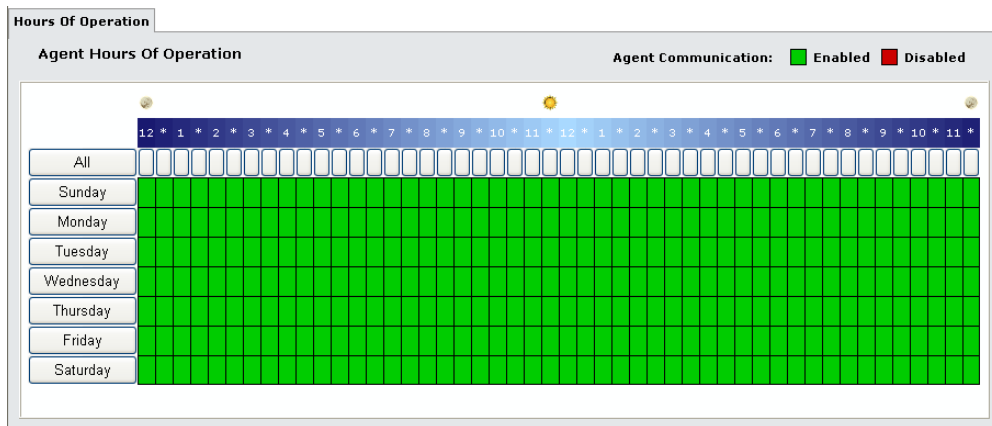
Figure 144: Agent Hours of Operation

Table 136: Hours of Operations Page Functions

Button	Function
Reset	Resets the previous Hours of Operations settings, leaving the page open for edit.
OK	Closes the window, saving your changes.
Cancel	Cancels all changes and closes the window.

Setting An Hours of Operation Policy

1. Open *Create/Edit Policy* Set.

   Step Result: The *Create/Edit a Policy Set* window opens.

2. Scroll to the Hours of Operation area, and click **Define**.

   Step Result: The *Hours of Operation* window opens.

3. Click the Day and Hour combinations during which you want to restrict agent communication.
   - **All** toggles all agent communication.
   - The *day unit* toggles the entire day.
   - The *time unit* toggles 30 minute increments across all days.

4. Click **OK**.

Result: The *Hours of Operations* window closes, saving your changes.

> ⚠️ **Caution:** Changes made to the *Hours of Operations* will not be saved until you have selected **Save** on the originating page.

Defining FastPath Servers

The Fastpath functionality will allow for the redirection of an agent from the Patch Management Server to a Fastpath Server (or any caching proxy server) based upon the fastest route.

Table 137: FastPath Server Fields

Field	Description
Communication Interval	The time interval between each check by fastpath to determine the fastest communication path back to the Update Server. A setting of zero (0) will disable the use of Fastpath Servers.
Servers	A listing of the available Fastpath servers.

Adding and Editing FastPath Servers

1. Open *Create/Edit Policy* Set.

   Step Result: The *Create/Edit a Policy Set* window opens.

2. Scroll to the FastPath Servers area, and click **Modify**.

   Step Result: The *Edit FastPath Servers* window opens.

Figure 145: Edit FastPath Servers Window

3. Click the **Add** link (or **Edit** icon).

> **Step Result:** The *Add FastPath Server* dialog opens.

Figure 146: Add FastPath Server Dialog

4. Provide the following data about your FastPath server.

- **Url** - The Url should be added in the *http://servername* format.
- **Port** - The port on which your FastPath server operates.
- **Authenticated** - Select this option if the FastPath server requires authentication. Enables the User Name and Password fields.
- **User Name** - If your FastPath server requires authentication, provide a valid user name.
- **Password** / **Confirm Password** - Enter the password associated with the defined user name.

5. Click **OK**.

> **Step Result:** The FastPath server data is saved and the *Add FastPath Server* dialog closes.

6. Click **Save**.

> **Step Result:** The *Edit FastPath Server* window closes.

Defining Agent Policy Conflict Resolution

When a group is assigned conflicting policies, those policies must be validated, and any conflicting policies resolved. The policies are resolved in the following order:

1. **Group Policies** - The conflicting policy sets assigned to a group are resolved prior to attempting to resolve the agent policies. The following rules apply:
   a. Any directly assigned policies, with conflicting values, are resolved as defined in the *Agent Policy Conflict Resolution Rules* on page 278.
   b. If a group has inherit policies turned on, it will receive the resultant (after conflict resolution) policies assigned to it's parent. Any policy values that are not directly assigned to the group, but are inherited from the group's parent, are assigned to the group.

   Note: If inherit policies is turned off, only directly assigned policies are considered and this step is skipped.

2. **Agent Policies** - After resolving the group policies, the conflicting policies assigned to an agent (via it's group membership) are resolved. The following rules apply:
   a. The resultant policies of all groups to which the agent is a member are resolved as defined in the *Agent Policy Conflict Resolution Rules* on page 278.
   b. Any policy values that have not been defined via the agent's group membership are populated based upon the policy settings defined in the Global Policy Set.

   Note: The policy settings defined in the Global Policy Set are only used to fill the empty agent policy values. Therefore, conflict resolution rules do not apply to the Global Policy Set.

Agent Policy Conflict Resolution Rules

Table 138: Agent Policy Conflict Resolution

Policy Setting	Resolution
Logging Level	The agent will use the most verbose Logging Level. (Debug > Detailed > Basic Information > None)
Agent Scan Mode	The agent will use the fastest Agent Scan Mode. (Fast Scan > Initial Scan > Normal Scan)
Communication Interval	The agent will use the shortest Communication Interval.
Agent Listener Port	If any group has an Agent Listener port defined (not zero), the agent listens on the highest defined port value.
Inventory Collection Options	The agent will use an all inclusive set of Inventory Collection options.

Policy Setting	Resolution
Resumable Downloads	If any group is not using Resumable Downloads, the agent will not use Resumable Downloads.
Hours of Operation	If any group is not using Hours of Operation, the agent will not use Hours of Operation. However, if all groups are using Hours of Operation, the agent will use an all inclusive setting. The on value takes precedence during this operation.
User May Cancel Deployment	The agent will use True.
User May Snooze Deployment	The agent will use True.
Deployment Within n Minutes	The agent will use the smallest Deploy Within value.
Always on Top	The agent will use True.
User May Cancel Reboot	The agent will use True.
User May Snooze Reboot	The agent will use True.
Reboot Within n Minutes	The agent will use the smallest Reboot Within value.
Discover Applicable Updates (DAU) Scheduling Frequency	The agent will use the longest possible DAU frequency.
FastPath Interval	The agent will use the shortest FastPath interval.
FastPath Servers	The agent will use all of the defined FastPath servers.
Maximum Transfer Rate	The agent will use the smallest transfer rate.
Minimum File Size	The agent will use the smallest file size.

Using E-Mail Notification

The *E-Mail Notification* page lets you configure system alerts to help in monitoring your Patch Management Server. You can enter any number of e-mail addresses and then assign the

particular alert types that you want each recipient to receive. This page also allows you to define the trigger levels for individual alerts.

Figure 147: E-Mail Notification Tab

The following table describes the functions available on the **E-Mail Notification** tab.

Table 139: E-Mail Notification Page Functionality

Button	Function
Create	Creates a new e-mail notification.
Save	Saves the changes made to e-mail notification.
	Note: Be sure to click **Save** after making any changes. If you do not click **Save**, the system will revert to the last saved settings when you navigate away from the E-Mail page.
Delete	Deletes the selected e-mail address from the notification list. Once deleted, the entry cannot be restored.
Export	Exports a list of e-mail notification addresses and settings to comma separated value (*.csv*) file format. See *Exporting Data* on page 33 for additional information.
Test	Sends a test e-mail message to the selected e-mail address(es).

Defining E-Mail Notification

The following options can be defined for each e-mail address included in the notification address column. Notification trigger levels (default values) for disk space, checking intervals, and license data are defined in the Alert Thresholds section.

Table 140: E-Mail Notification Column Descriptions

Column Name	Description
New Vulnerabilities	Alerts when a new vulnerability becomes available for deployment.
New Agent Registrations	Alerts when an agent registers with the 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 Patch Management Server, falls below the defined minimums.
Low Storage Disk Space	Alerts when the available storage space, on the Patch Management Server, falls below the defined minimums.
Low Available License Count	Alerts when the number of licenses available to the Patch Management Server falls defined minimums.
Up-Coming License Expiration	Alerts when licenses will expire within the defined time frame.
License Expiration	Alerts when a license expires.
Notification Address	The e-mail address that receives notifications. Must be a validly formatted e-mail address (name@domain.tld); the system does not, however, validate the actual address.
Outgoing Mail Server (SMTP)	The mail host used by your Patch Management Server for sending e-mail messages.

Defining E-Mail Alert Thresholds

Alert thresholds allow you to define the limits that trigger various alerts (notifications). Trigger limits are available for system disk space, storage disk space and license information.

Table 141: E-Mail Notification Alert Threshold Definitions

Alert Threshold	Definition
Low System Disk Space	Alert is generated if the system disk space on the Update Server drops below the defined level. The level is measured in Megabytes (MB) and must be a whole number between 1 and 9,999 MB (9.765 GB).

Alert Threshold	Definition
Low Storage Disk Space	Alert is generated if the storage drive disk space on the Update Server drops below the defined level. The level is measured in Megabytes (MB) and must be a whole number between 1 and 9,999 MB (9.765 GB).
Check Disk Space Every __ Interval	Represents the schedule that the thresholds are checked. This is defined in units of minutes, hours or days. The interval must be defined as a whole number between 1 and 99.
Low Available License Count	Alert is generated if the number of available licenses drops below the defined level. The level is measured in units of available licenses, and must be a whole number between 1 and 999.
Up-Coming License Expiration	Alert is generated if licenses will expire within the defined days. The level is measured in units of days to expiration, and must be defined as a whole number between 1 and 99.

Sending a Test E-Mail

1. On the *Options* page, click **E-Mail**.

2. In the **Current E-Mail Notifications** section, select the e-mail address(es) to receive the test message.

3. Click **Test**.

Result: A confirmation message informs you that the test message was sent.

Technical Support Information

Clicking on the **Support** tab causes the *Technical Support* page to be displayed. The *Technical Support* page is a view-only page that provides a variety of system data pertaining to the Patch Management Server environment. It also provides links to contacting support.

Figure 148: Technical Support Tab

The following table describes the Action Menu functions of the *Technical Support* page.

Button	Function
OS Packs	Regenerates and synchronize the relevant information for each of the Operating Systems supported by your Patch Management Server.
Export	Exports a list of support information and settings to comma separated value (*.CSV*) file format. See *Exporting Data* on page 33 for additional information.

Server Information

This section provides general notes regarding the Patch Management Server. The information is not editable.

Table 142: Server Information Field Descriptions

Field	Description
Name	The name of the computer on which Patch Management Server is installed.
Serial Number	The serial number used by this server.
Operating System	The operating system installed and running on the Patch Management Server machine.
Last Connected with Novell ZENworks	The date and time the system last made a connection with the Global Subscription Server.
Non-Expired Licenses	Total number of active licenses.
Licenses Available	Number of licenses that can be used to register devices with this Patch Management Server.
Licenses in Use	Number of licenses being used by agents.
Subscription Service ID	The ID assigned to the Patch Management Server upon its registration with the Global Subscription Server.
Version	The version number of the Patch Management Server installed.
URL	The URL assigned to this Patch Management Server.
Last Agent Connection	The date and time an Agent last made a connection to the Patch Management Server.
Installation Date	The date Patch Management Server was installed.
Storage Volume Free Space	The amount of free disk space on your storage volume.
System Root Free Space	The amount of free disk space on your system volume.
Total Agents Registered	The total number of agents registered with this Patch Management Server.
Replication Service Version	The version of the local Global Subscription Server.

Component Version Information

This section identifies the basic component software and services running on the Patch Management Server. The information is not editable.

Table 143: Component Version Information Field Description

Field	Description
OS Version	Additional operating system information (typically the version number).
OS Service Pack	Service pack information, if available, regarding your operating system.
IIS Version	The version of Internet Information Server (IIS) running on the system.
.NET Version	The .NET Framework versions installed on the server.
MDAC Version	The Microsoft Data Access Components (MDAC) version. Click **More...** to view a detailed list of MDAC product and file versions.
SQL File Version	The SQL Server version installed on the server.
SQL Version	Detailed SQL Server version information.

Support Information

This section provides links to the Novell Support team.

Table 144: Support Information Link Descriptions

Link	Description
Contact Technical Support	Sends an e-mail to the Novell technical support team.
Access Product Knowledge Base	Accesses the Novell Knowledge Base.
Access Product Web Site	Accesses the Novell Web site.
Ask a Question	Sends a support question to the Novell technical support team via e-mail.
Request a Patch	Sends a patch request to the Novell technical support team via e-mail.
Request a Feature	Sends a feature request to the Novell technical support team via e-mail.
Provide Product Feedback	Sends product input to the Novell technical support team via e-mail.

Chapter

10

Using the Agent

In this chapter:

- *About the Agent for Pre Windows Vista*
- *About the Agent for Windows Vista*
- *About the Agent for Mac*
- *About the Agent for Linux/ Unix*

When installed on a device, the Agent scans that device for vulnerabilities and communicates the results of the scan to your Patch Management Server. The results returned to Patch Management can be viewed at any time, even if the workstation is disconnected from your network. The scan results are used, by ZENworks Patch Management, to determine a vulnerability's applicability for each device. If a vulnerability is applicable, ZENworks Patch Management will display the device as *Not Patched.*

After installing the Patch Management Agent, there is generally, no additional user interaction required at the device.

About the Agent for Pre Windows Vista

The agent is responsible for retrieving device data, uploading the device data to Patch Management Server, and deploying vulnerabilities to the device.

Viewing the Pre Windows Vista Agent

1. Go to **Start** > **Settings** > **Control Panel**.

2. Select **ZENworks Patch Management**.

Result: The *Novell Agent Control Panel* opens with the Deployment tab selected by default.

> **Note:** When opening the ZENworks Patch Management Agent, the *Control Panel* must be displayed in the Windows Classic View. Viewing the *Control Panel* in Category View will not display the Agent.

Deployment Tab

The Deployment tab is comprised of four functional areas.
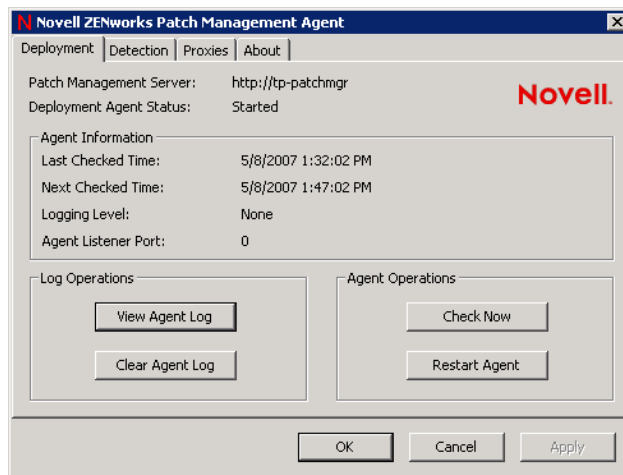
Figure 149: Agent Initial Window

Server Information and Status

The following table displays the Patch Management Server location and the communication status:

Table 145: Server Information - Deployment Tab

Field	Description
Patch Management Server	The URL of the ZENworks Patch Management Server the agent is registered against.
Deployment Agent Status	Indicates the current status (started, stopped, working, waiting, or restarting) of the *ZENworks Patch Management service* on the local device.

Agent Information

The following table describes the information in the Agent Information area of the Deployment tab:

Table 146: Agent Information

Field	Description
Last Checked Time	When the agent last communicated with the Patch Management Server.

Field	Description
Next Checked Time	Next scheduled time when the agent will contact the ZENworks Patch Management Server.
Logging Level	The agent's current logging level.
Agent Listener Port	The port on which the agent will listen for communication. 0 = Disabled.

Log Operations

The following table describes the log operations:

Table 147: Log Operations

Use	To
View Agent Log	View the Agent's activity log.
Clear Agent Log	Clear the contents of the agent log.

Viewing the Agent Log
Perform the following procedure to view the agent log.

Click **View Agent Log**.

Result: The Agent Log (*ZENworks Patch Management Agent.log*) opens.
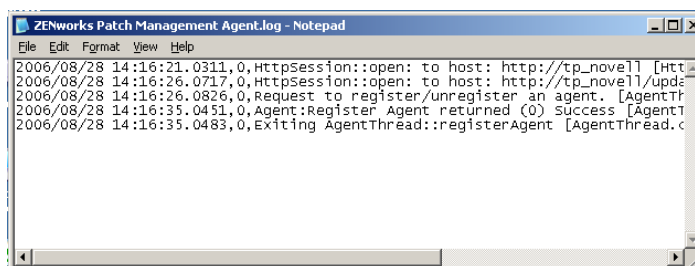
Figure 150: Agent Log

Clearing the Agent Log
Perform the following procedure to clear the agent log.

1. Click **Clear Agent Log**.

   Step Result: The clear confirmation message dialog box opens.
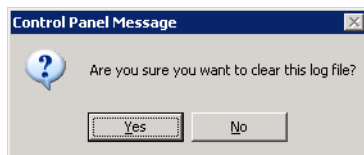
Figure 151: Clear Agent Log Message

2. Click **Yes**.

Result: The system clears the Agent Log.

Agent Operations

The following table describes the Agent Operations area:

Table 148: Agent Operations on the Deployment tab

Use	To
Check Now	Cause the Agent to contact the Patch Management Server.
Restart Agent	Restarts the ZENworks Patch Management service.

Initiating Communication Between the Agent and Server
Complete the following procedure to initiate communication between the Patch Management
Agent and the Patch Management Server.

   Click **Check Now**.

Result: The agent initiates communication with the Patch Management Server and checks
             for any pending tasks or deployments and the **Last Checked Time** is updated to
             reflect the current time.

Restarting the Agent
Complete the following procedure to restart the Agent.

1. Click **Restart Agent**.

2. The Agent restarts.

Result: The **Deployment Agent Status** field confirms that the Agent is restarting by
             displaying **Restarting**, and then **Started** when complete.

Detection Tab

The Detection tab is comprised of four functional areas.
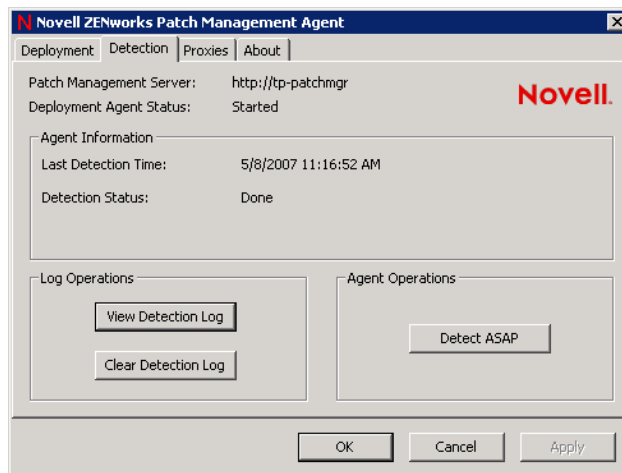
Figure 152: Detection Tab

Server Information and Status

The following table displays the Patch Management Server location and the communication status:

Table 149: Server Information - Detection Tab

Field	Description
Patch Management Server	The URL of the ZENworks Patch Management Server the agent is registered against.
Deployment Agent Status	Indicates the current status (started, stopped, working, waiting, or restarting) of the *ZENworks Patch Management service* on the local device.

Agent Information

The following table describes the information in the Agent Information area of the **Deployment** tab:

Table 150: Agent Information - Detection Tab

Field	Description
Last Detection Time	The last time the Discover Applicable Updates (DAU) task ran.
Detection Status	The status of the DAU task.

Log Operations

The following table describes the Log Operations area:

Table 151: Log Operations - Detection Tab

Use	To
View Agent Log	View the Detection log.
Clear Agent Log	Clear the Detection log.

Viewing the Detection Log
Complete the following procedure to view the Detection Log.

   Click **View Detection Log**.

Result: The Detection Log opens.
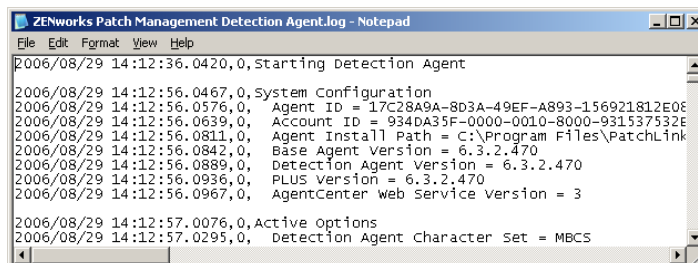
Figure 153: View Detection Log

Clearing the Detection Log
Complete the following procedure to clear the Detection Log.

1. Click **Clear Detection Log**.

   Step Result: The Clear confirmation message dialog box opens.
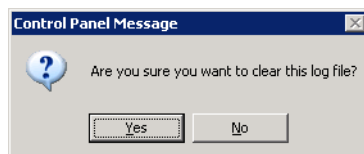
Figure 154: Clear Agent Log Message

2. Click **Yes**.

Result: The system clears the Detection Log.

Agent Operations

The following table describes the Agent Operations area:

Table 152: Agent Operations

Use	To
Detect ASAP	Causes the agent to start a Discoverable Applicable Updates task as soon as possible.

Prompting the Agent to Detect Vulnerabilities Immediately
Complete the following procedure to prompt the Agent to detect vulnerabilities immediately.

Click **Detect ASAP**.

Result: The Agent starts the Discover Applicable Updates task. The **Last Detection Time** field reflects the current time.

Proxies Tab

The **Proxies** tab allows you to configure proxy settings for communication with the Patch Management Server.
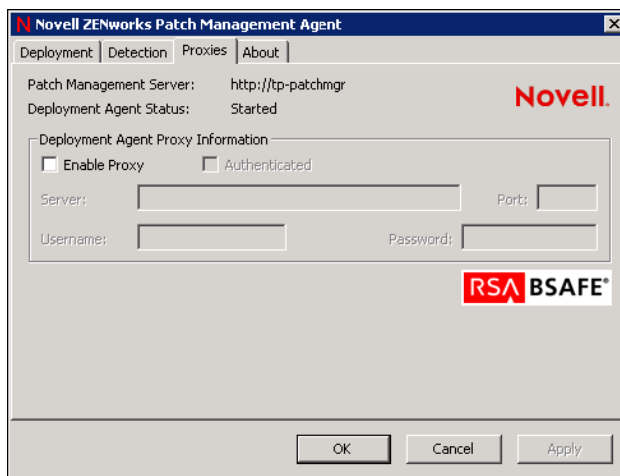
Figure 155: Proxies Tab

Server Information and Status

The following table displays the Patch Management Server location and the communication status.

Table 153: Server Information - Proxies Tab

Field	Description
Patch Management Server	The URL of the ZENworks Patch Management Server the agent is registered against.

Field	Description
Deployment Agent Status	Indicates the current status (started, stopped, working, waiting, or restarting) of the *ZENworks Patch Management service* on the local device.

Configuring Proxy Settings

Complete the following procedure to configure proxy settings.

1. Select **Enable Proxy**.

   Step Result: The **Server** and **Port** fields become active.

2. Type the server's URL address in the **Server** field.

3. Type the port in the **Port** field.

4. If you are using an Authenticated proxy, select **Authenticated**.

   Step Result: The **Username** and **Password** fields become active.
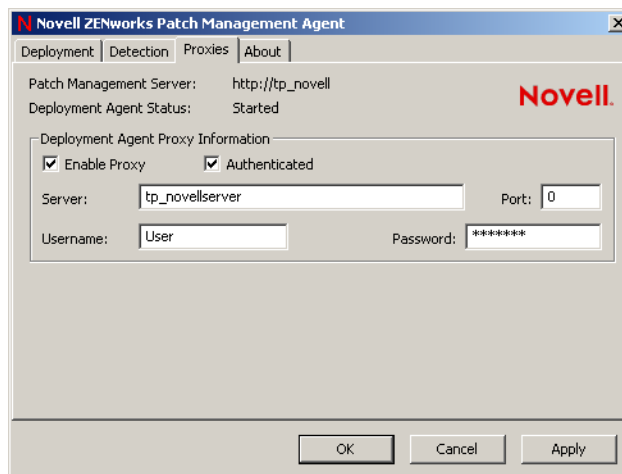
Figure 156: Proxy Tab

5. Type the username in the **Username** field.

6. Type the password in the **Password** field.

7. Click **OK**.

   Step Result: The confirmation dialog box opens.
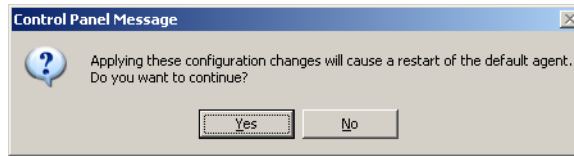
Figure 157: Proxy Change Confirmation

8. Click **Yes**.

Result: The proxy information is saved.

About Tab

The About Tab displays information regarding the Agent and its associated ZENworks Patch Management Server.
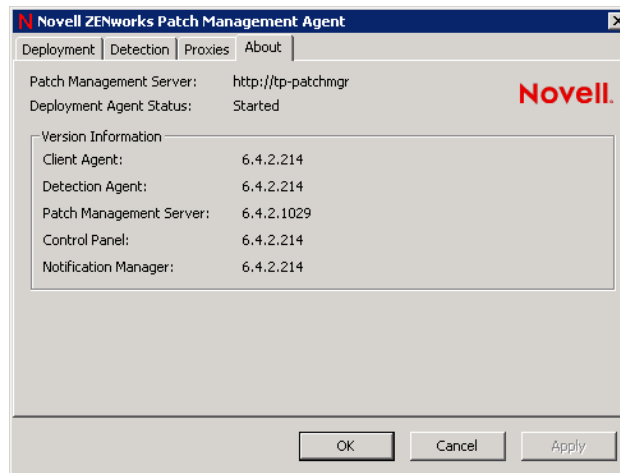
Figure 158: About Tab

Server Information and Status

The following table displays the Patch Management Server location and the communication status:

Table 154: Server Information - About Tab

Field	Description
Patch Management Server	The URL of the ZENworks Patch Management Server the agent is registered against.

Field	Description
Deployment Agent Status	Indicates the current status (started, stopped, working, waiting, or restarting) of the *ZENworks Patch Management service* on the local device.

Version Information

The following table describes the Version Information are for the **About** tab:

Table 155: Version Information

Field	Description
Client Agent	Version number of the Patch Management Agent.
Detection Agent	Version number of the Detection Agent.
Patch Management Server	Version number of the ZENworks Patch Management Server.
Control Panel	Version number of the Control Panel.
Notification Manager	Version number of the Notification Manager.

User Interaction During a Deployment

After you create a deployment within the Patch Management Server, the agent can retrieve the deployment from the server. When the agent receives a deployment, if a deployment notification was enabled and a user is logged into the device, the Novell ZENworks Desktop Deployment Manager displays on the Device screen.

Figure 159: Novell ZENworks Desktop Deployment Manager - Pending Deployment

An icon is also visible in the taskbar.

Figure 160: Novell ZENworks Desktop Deployment Manager Icon

Beginning the Deployment
Complete the following procedure to begin a deployment.

1. Verify the deployment details.

2. Click **Install**.

Result: The Agent starts the deployment.

Delaying a Deployment
Complete the following procedure to delay a deployment.

1. Select a time frame from the **Snooze for** drop-down list.

2. Click **Snooze**.

Result: The deployment is delayed for the selected duration.

Canceling a Deployment
Complete the following procedure to cancel a deployment.

1. Click **Cancel** (if Cancel is not available, your Administrator has disabled your ability to do so).

   Step Result: A confirmation dialog box displays, confirming your choice.

2. Click **Yes**.

Result: The deployment is cancelled.

> **Note:** If the deployment is part of a mandatory baseline, the Patch Management
> Server will redeploy the patch until it is installed on the device.

User Interaction During a Reboot

If the agent must reboot the device, a user is logged into the device, and reboot notification was enabled, the Novell ZENworks Desktop Deployment Manager will displays on the Device screen.

Figure 161: Novell ZENworks Desktop Deployment Manager - Pending Reboot

An icon is also visible in the taskbar.

Figure 162: Novell ZENworks Desktop Deployment Manager Icon

Rebooting Immediately
Complete the following procedure to reboot immediately.

1. Verify the details of the reboot.

2. Click **Reboot**.

Result: The Agent reboots the device.

Delaying a Reboot
Complete the following procedure to delay a reboot.

1. Select a time frame from the **Snooze for** drop-down list.

2. Click **Snooze**.

Result: The reboot is delayed for the selected duration.

Canceling the Reboot

Complete the following procedure to cancel reboot.

1. Click **Cancel** (if Cancel is not available, your Administrator has disabled your ability to cancel reboots).

   Step Result: A confirmation dialog box displays, confirming your choice.

2. Click **Yes**.

Result: The reboot is cancelled.

About the Agent for Windows Vista

The following section describes the Agent for Microsoft Windows Vista and its components.

Viewing the Agent

1. Go to **Start** > **Settings** > **Control Panel**.

   Step Result: The Control Panel opens.

2. Select **Security**.

   Step Result: The Security Panel opens.

3. Select **Patch Management Agent**.

Result: The Agent Control Panel opens.
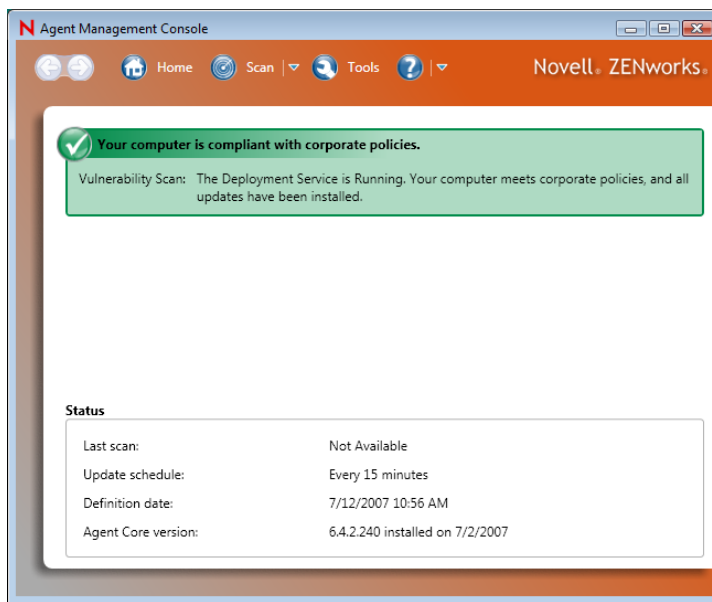
Figure 163: Agent Control Panel

Home Page

The Home page is comprised of the following functional areas.
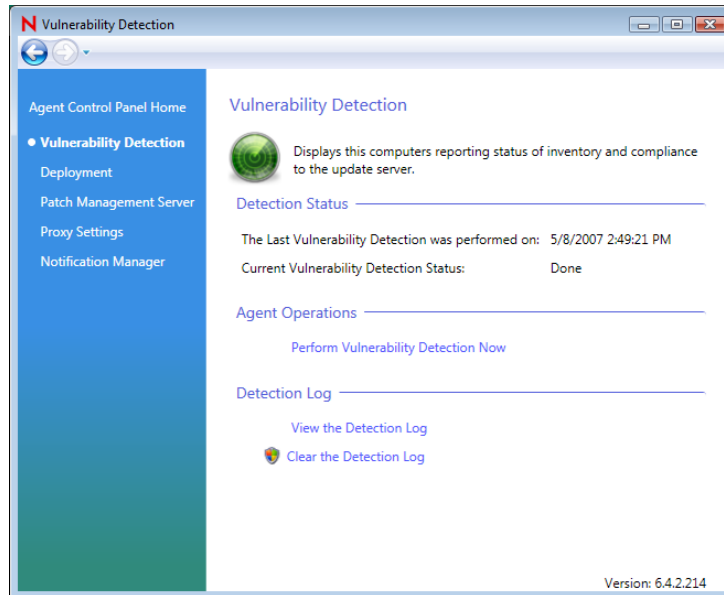
Figure 164: Vulnerability Detection Page

Compliance - Displays whether your computer is compliant with corporate policies. The available values are as follow:

Table 156: Computer Compliance Status

Status	Description	Displays
Compliant	Green (Service is running and the Patch Management Agent is idle).	✓ **Your computer is compliant with corporate policies.** Vulnerability Scan: Deployment Service is Running Your computer meets corporate policies, and all updates installed on your computer.
Unable to Determine Compliance	Red (Service is not running).	✗ **Agent is unable to determine your computer's compliance with corporate policies.** Critical Deployment Service is Stopped the agent is ofline.
Not Compliant	Yellow (Service is running and the Patch Management Agent is busy).	! **Your computer not is compliant with corporate policies.** Vulnerability Scan: Deployment Service is Running your computer requires a reboot to finish installing updates.
Unable to Contact Server	Blue (Service is running and the Patch Management Agent is offline or unknown).	? **Your computer has not been able to contact the management server.** Critical Deployment Service is Running the agent is in an unknown state.

Active Scan Statistics - Only displays after clicking the **Scan** button. The Active Scan Statistics section will start a scan if one is not already active, and displays the Scan Type, Start Time, Duration, and Status.

Note: The scan Start Time and Duration values are only populated if you started the Scan. If the scan was running prior to you clicking the Scan button, the exact start time duration are unknown.

Status - Provides general Agent status values. Including the Last Scan, the Update Schedule (as defined by the Communication Interval), the scan Definition Date, and the Agent Version.

Tools and Settings

The *Tools and Settings* page is comprised of links to the following:

- *Proxy Settings* on page 303 - The Proxy Settings link opens the *Proxy Settings* page, allowing you to view or modify the agent's current proxy configuration.
- *Logging* on page 304 - The Logging link opens the *Log Files* page, allowing you to view or clear the Agent log files.
- *Notification Manager* on page 305 - The Notification Manager link opens the *Notification Manager* page, allowing you to define the Notification Manager behavior.
- *Management Server* on page 306 - The Management Server link opens the *Server Settings* page.

Proxy Settings

The *Proxy Settings* page allows you to override the server provided proxy settings for communication with the Patch Management Server.
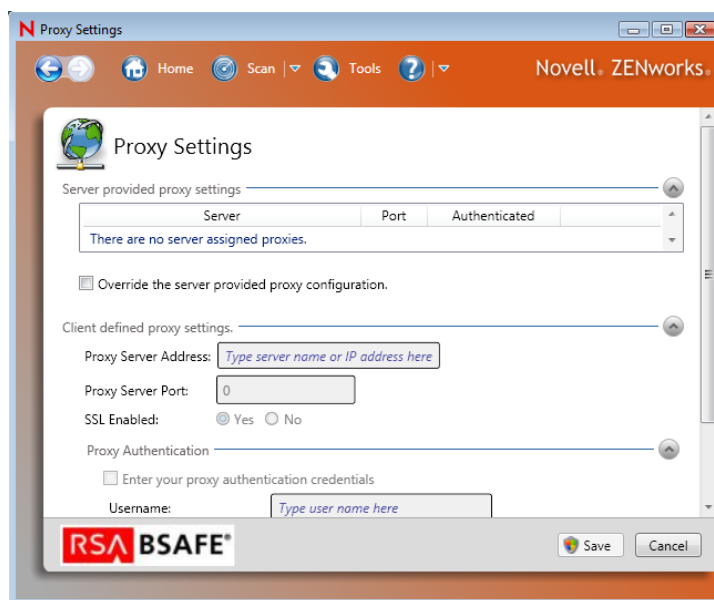
Figure 165: Proxy Settings

Configuring the Proxy Settings
Complete the following procedure to configure proxy settings.

1. Select **Override the Server Provided Proxy Settings**.

   Step Result: The **Proxy Server Address**, **Proxy Server Port** and **SSL Enabled** fields become active.

2. Type the proxy server's address in the **Proxy Server Address** field.

3. Type the port in the **Proxy Server Port** field.

4. If your proxy uses https, select the **SSL Enabled** field.

5. If you are using an Authenticated proxy:
   a) Select **Enter proxy authentication credentials**.

   Step Result: The **Username**, **Password**, and **Retype Password** fields become active.

   b) Type the username in the **Username** field.
   c) Type the password in the **Password** and **Retype Password** fields.

6. Click **Save**.

Result: The proxy information is saved.

Logging

The Log Files page, provides buttons to view and clear the Agent log files.
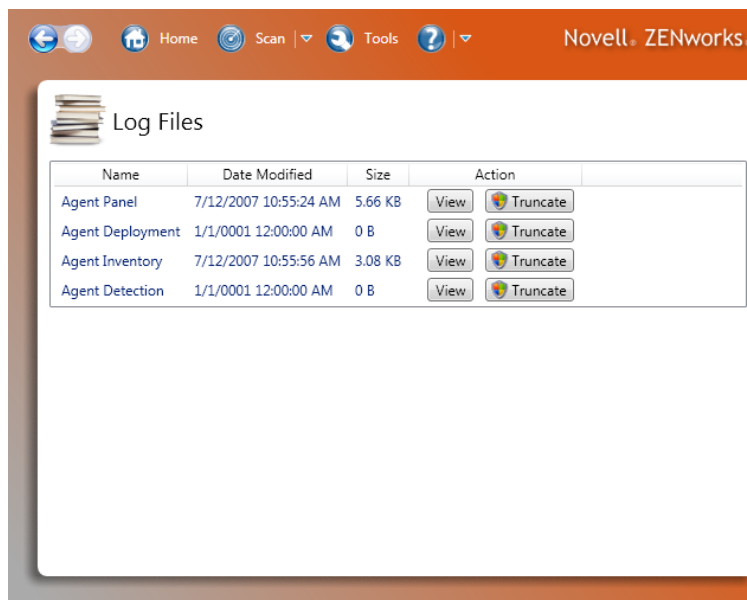
Figure 166: Log Files Page

Viewing a Log File
Complete the following procedure to view a log file.

1. If desired, click the **Name**, **Date Modified**, or **Size** column heading to sort the log files.

2. Click the **View** button to open the *Log Detail* page.

Clearing a Log File
Complete the following procedure to clear the log file.

1. If desired, click the **Name**, **Date Modified**, or **Size** column heading to sort the log files.

2. Click the **Truncate** button to clear the log.

Log Detail Page

The *Log Detail* page displays the Name, Size, last Updated date, and log contents. From the Log Detail page, you can search the log contents, change to a single page, or facing pages view, and refresh.

Notification Manager

The *Notification Manager* page is comprised of the Notification Settings area, which provides the following information.
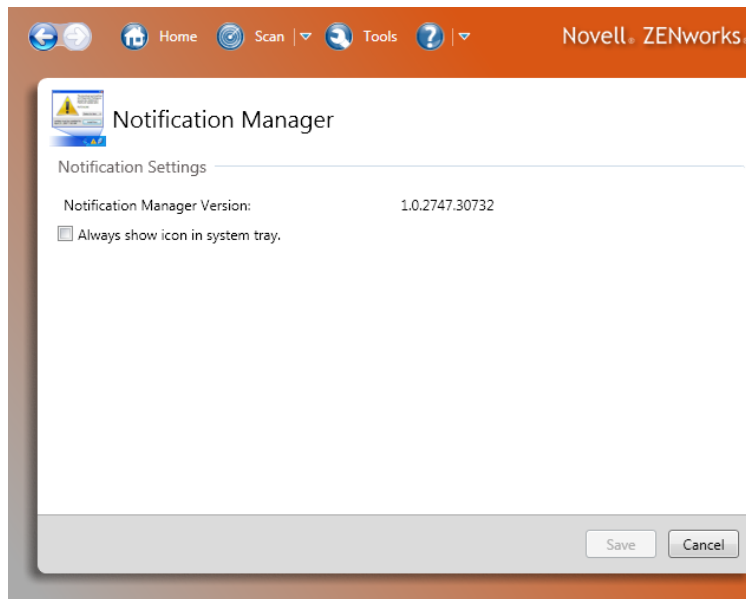
Figure 167: Vista Agent Notification Manager Page

Table 157: Notification Manager Page - Field Descriptions

Field	Description
Notification Manager Version	Displays the version of the Notification Manager.
	For use by Technical Support.
Always Show Icon in System Tray	When selected will force the Notification Manager icon to display in the Windows System Tray area.

Management Server

The *Server Settings* page is comprised of the Patch Management Server Settings area which provides the following information.
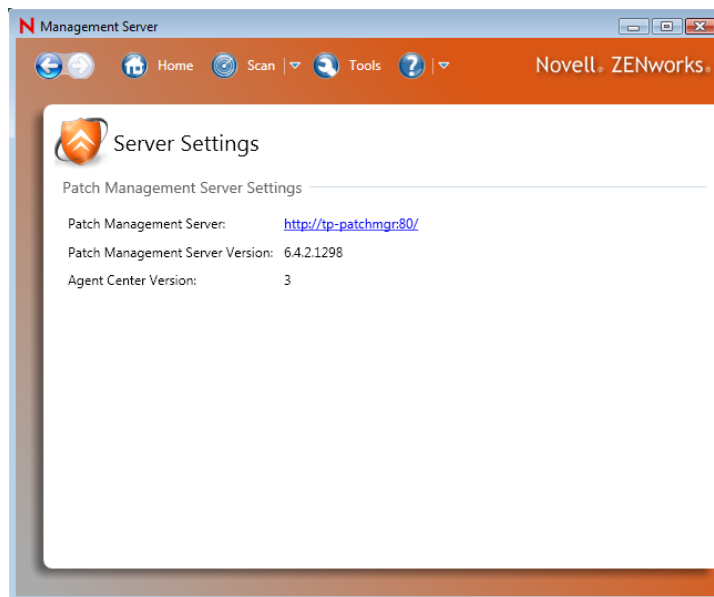
Figure 168: Vista Agent Server Settings Page

Table 158: Server Settings Page - Field Descriptions

Field	Description
Patch Management Server Version	Provides the version of the Patch Management Server that this agent is registered against.
Open Patch Management Server	A link that, when clicked, will open the Patch Management Server in a web browser.
Agent Center Version	Provides the associated Agent Center version. For use by Technical Support.

User Interaction During a Deployment

After you create a deployment within the Patch Management Server, the agent can retrieve the deployment from the server. When the agent receives a deployment, if a deployment notification

was enabled and a user is logged into the device, the Novell ZENworks Desktop Deployment Manager displays on the Device screen.
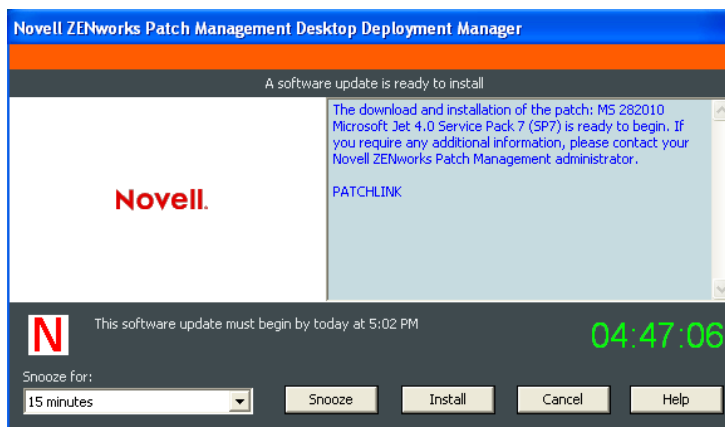

Figure 169: Novell ZENworks Desktop Deployment Manager - Pending Deployment

Beginning the Deployment
Complete the following procedure to begin a deployment.

1. Verify the deployment details.

2. Click **Install Now**.

Result: The Agent starts the deployment.

Delaying a Deployment
Complete the following procedure to delay a deployment.

1. Verify the deployment details.

2. Select a time frame from the **Remind me in** drop-down list.

Result: The deployment is delayed for the selected duration.

Canceling a Deployment
Complete the following procedure to cancel a deployment.

1. Click **Cancel** (if Cancel is not available, your Administrator has disabled your ability to do so).

   Step Result: A confirmation dialog box displays, confirming your choice.

2. Click **Yes**.

Result: The deployment is cancelled.

> **Note:** If the deployment is part of a mandatory baseline, the Patch Management Server will redeploy the patch until it is installed on the device.

User Interaction During a Reboot

If the agent must reboot the device, a user is logged into the device, and reboot notification was enabled, the Novell ZENworks Desktop Deployment Manager displays on the Device screen.
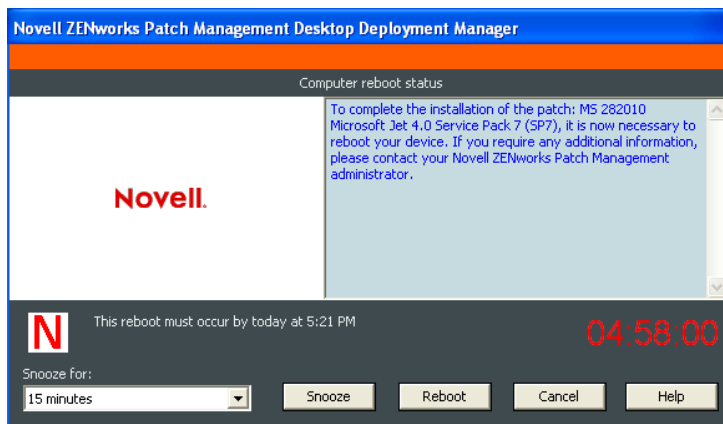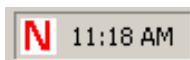

Figure 170: Novell ZENworks Desktop Deployment Manager - Pending Reboot

Rebooting Immediately
Complete the following procedure to reboot immediately.

1. Verify the reboot details.

2. Click **Restart Now**.

Result: The Agent reboots the device.

Delaying a Reboot
Complete the following procedure to delay a reboot.

1. Verify the reboot details.

2. Select a time frame from the **Remind me in** drop-down list.

Result: The reboot is delayed for the selected duration.

Canceling the Reboot
Complete the following procedure to cancel reboot.

1. Click **Cancel** (if Cancel is not available, your Administrator has disabled your ability to cancel reboots).

   Step Result: A confirmation dialog box displays, confirming your choice.

2. Click **Yes**.

Result: The reboot is cancelled.

About the Agent for Mac

The Patch Management Agent for Mac is a graphical user interface application for Apple OS X. The agent is responsible for uploading device data to the TBD and retrieving vulnerabilities.

Viewing the Agent

Complete the following procedure to view the Agent.

1. Click **System Preferences**.

2. Click **Patch Management Agent Control Panel**.

Result: The *Novell Agent Control Panel* opens. The **Deployment** tab is the default.

Deployment Tab

The **Deployment** tab is comprised of three functional areas.
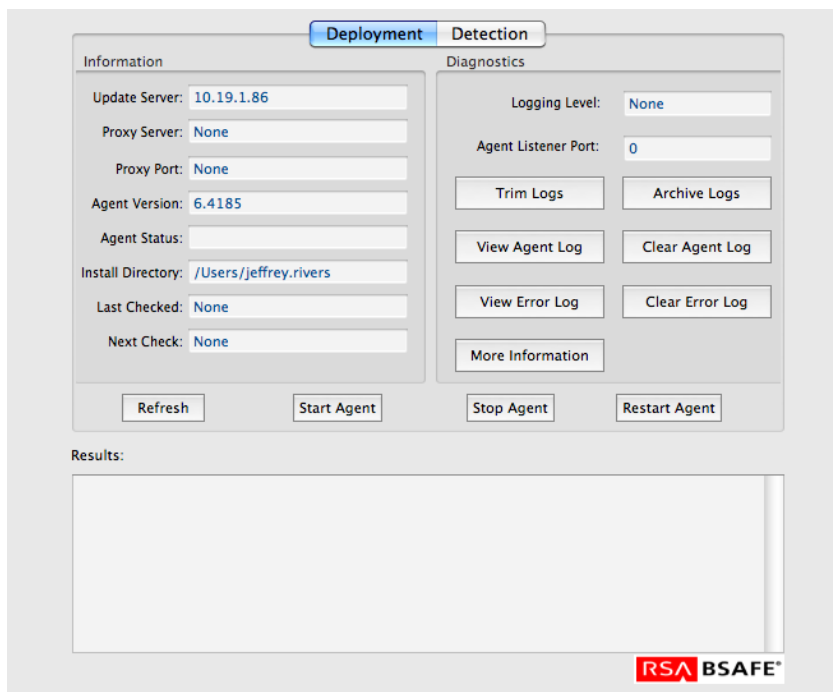
Figure 171: Agent Deployment Tab

Server Information

The following table displays server information:

Table 159: Server Information Displayed in the Mac Agent

Field	Description
Patch Management Server	The URL of the ZENworks Patch Management Server the agent is registered against.
Proxy Server	The URL of the proxy server, if a proxy server is configured.
Proxy Port	The port used by the proxy server, if a proxy server is configured.
Agent Version	The version number of the Patch Management Agent.
Agent Status	Indicates the current status (started, stopped, working, waiting, or restarting) of the Patch Management Agent service on the local device.
Install Directory	The directory in which the Patch Management Agent is installed.
Last Checked	The time at which the agent last communicated with the ZENworks Patch Management Server.
Next Checked	The next scheduled time when the agent will contact the ZENworks Patch Management Server.

Diagnostics Information

The following table displays the Patch Management Agent diagnostics information and log operations:

Table 160: Diagnostics Information

Field	Description
Logging Level	The logging level performed by the Patch Management Agent. Valid values for this field are: None, Basic Info, Detailed, and Debug.
Agent Listener Port	The port that the Patch Management Agent uses to connect to the ZENworks Patch Management Server.
Trim Logs	Reduces the size of the error, agent, and detect log files. Oldest entries are deleted and the file is truncated at 100,000 lines.
Archive Logs	Archives log files. The location of the archive appears in the **Results** field.
View Agent Log	Opens a text file containing the agent activity log.

Field	Description
Clear Agent Log	Clears the agent activity log.
View Error Log	Opens a text file containing the agent error log.
Clear Error Log	Clears the agent error log.
More Information	Displays agent configuration information, usage information, and excerpts of the agent activity and error logs in the **Results** field.

Results

The **Results** field shows the results of the Patch Management Agent activities performed on the **Deployment** tab.

Detection Tab

The **Detection** tab allows you to perform detection operations and view the detection log. The **Detection** tab is comprised of two areas:
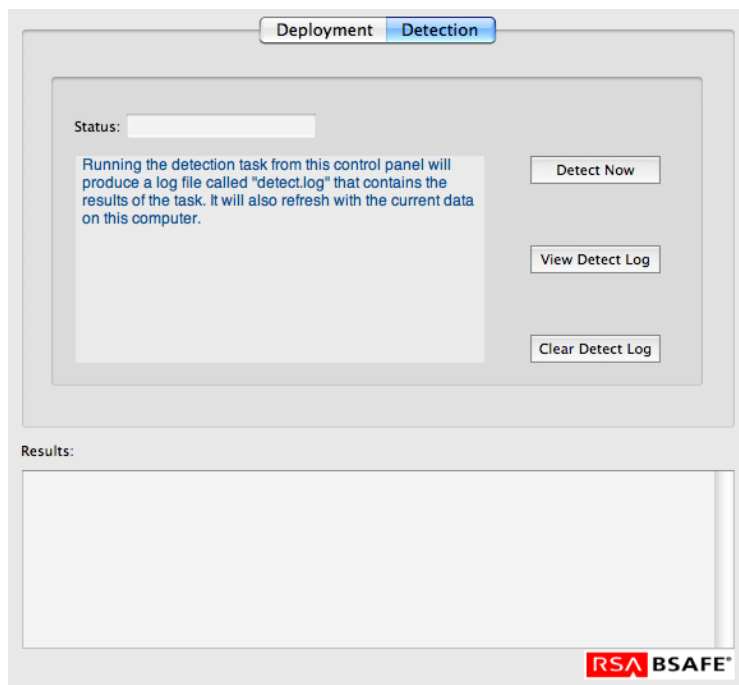
Figure 172: Agent Detection Tab

Agent Detection Operations

The following table displays the Patch Management Agent detection and log operations:

Table 161: Diagnostics Information

Field	Description
Status	The status of the Discover Application Updates (DAU) task. A summary of the status appears below this field.
Detect Now	Performs the DAU operation.
View Detect Log	Opens a text file containing the DAU activity log.
Clear Detect Log	Clears the DAU activity log.

Results

The **Results** field shows the results of the Patch Management Agent activities performed on the **Detection** tab.

Refreshing the Agent Information

Refreshing the Patch Management Agent information updates the information that appears on the Patch Management Agent's **Deployment** tab.

1. Click **System Preferences**.

2. Click **Patch Management Agent Control Panel**.

    Step Result: The *Novell Agent Control Panel* opens.

3. Click **Refresh**.

Starting the Agent

Starting the Patch Management Agent activates the agent and initiates a connection attempt between the Patch Management Agent and the configured ZENworks Patch Management Server.

1. Click **System Preferences**.

2. Click **Patch Management Agent Control Panel**.

    Step Result: The *Novell Agent Control Panel* opens. The **Deployment** tab is the default.

3. Click **Start Agent**.

Stopping the Agent

Stopping the Patch Management Agent deactivates the agent and terminates any connection between the Patch Management Agent and ZENworks Patch Management Server. The Agent will automatically restart after a reboot.

1. Click **System Preferences**.

2. Click **Patch Management Agent Control Panel**.

   Step Result: The *Novell Agent Control Panel* opens. The **Deployment** tab is the default.

3. Click **Stop Agent**.

Restarting the Agent

Restarting the Patch Management Agent stops and then restarts the Patch Management Agent, then initiates a connection attempt between the Patch Management Agent and ZENworks Patch Management Server.

1. Click **System Preferences**.

2. Click **Patch Management Agent Control Panel**.

   Step Result: The *Novell Agent Control Panel* opens. The **Deployment** tab is the default.

3. Click **Restart Agent**.

User Interaction During a Deployment

After you create a deployment within ZENworks Patch Management Server, the agent can retrieve the deployment from the server. When the agent receives a deployment, if a deployment notification was enabled and a user is logged into the device, the Novell ZENworks Desktop Deployment Manager displays on the *Device* screen.
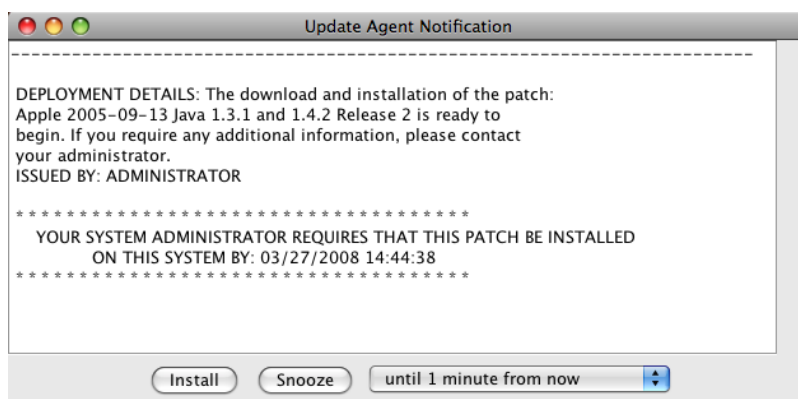
Figure 173: Novell ZENworks Desktop Manager - Pending Deployment

Beginning the Deployment

Complete the following procedure to begin a deployment.

1. Verify the deployment details.

2. Click **Install**.

Result: The Agent starts the deployment.

Delaying a Deployment
Complete the following procedure to delay a deployment.

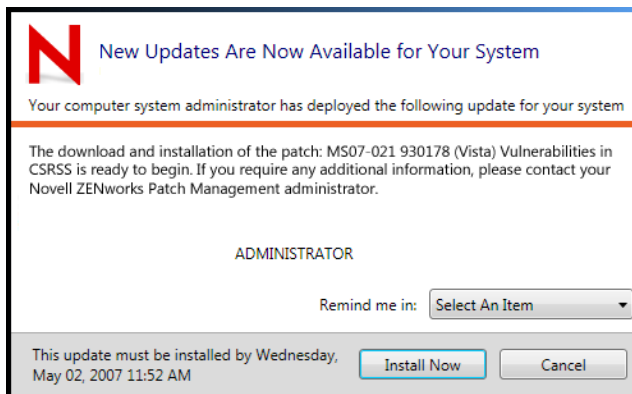1. Select a time frame from the drop-down list.

2. Click **Snooze**.

Result: The deployment is delayed for the selected duration.

Canceling a Deployment
Complete the following procedure to cancel a deployment.

1. Click **Cancel** (if **Cancel** is not available, your Administrator has disabled your ability to cancel deployments).

   Step Result: A confirmation dialog box displays, confirming your choice.

2. Click **Yes**.

Result: The deployment is cancelled.

> **Note:** If the deployment is part of a mandatory baseline, the Patch Management Server will redeploy the patch until it is installed on the device.

User Interaction During a Reboot

If the agent must reboot the device, a user is logged into the device, and reboot notification was enabled, the Novell ZENworks Desktop Deployment Manager will displays on the *Device* screen.
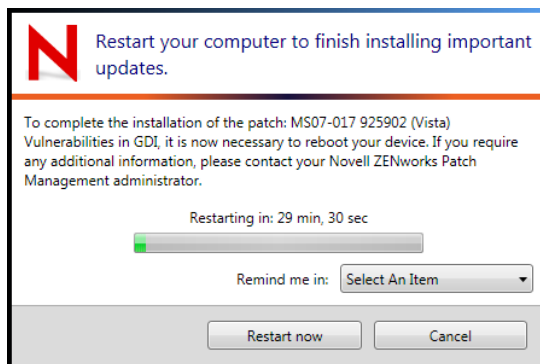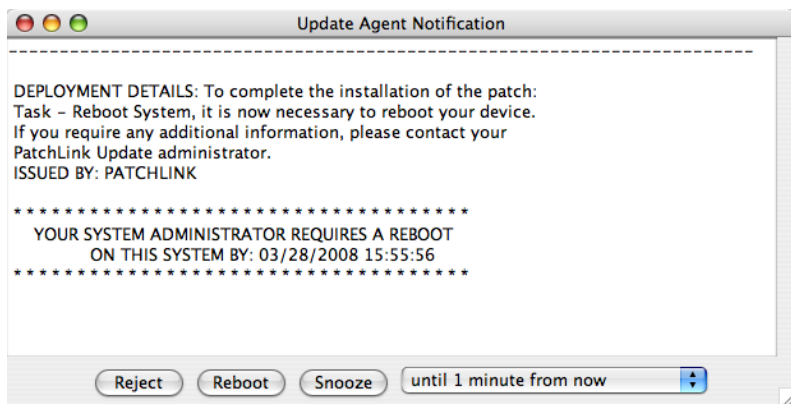

Figure 174: Novell ZENworks Desktop Deployment Manager - Pending Reboot

Rebooting Immediately
Complete the following procedure to reboot immediately.

1. Verify the reboot details.

2. Click **Reboot**.

Result: The Agent reboots the device.

Delaying a Reboot
Complete the following procedure to delay a reboot.

1. Select a time frame from the drop-down list.

2. Click **Snooze**.

Result: The reboot is delayed for the selected duration.

Canceling the Reboot
Complete the following procedure to cancel a reboot.

1. Click **Reject** (if **Reject** is not available, your Administrator has disabled your ability to cancel a reboot).

   Step Result: A confirmation dialog box displays, confirming your choice.

2. Click **Yes**.

Result: The reboot is cancelled.

About the Agent for Linux/Unix

The Linux/Unix Agent is a command line based application that does not have a user interface. While you are in the root directory, inside the Patch Service program, type:

user\local\patchagent\readme

Refer to the following commands to complete tasks within these agents:

Table 162: Linux/Unix Agent Commands

Command	Description
info	General information about the Agent.
status	Status of the Agent process.
daustatus	Status of the Discover Applicable Updates task.
detect	Starts the detection task.
stop	Stop the Agent process.
restart	Stop and start the Agent process.
patchdirectory	Sets the directory where patches will be temporarily downloaded.

Command	Description
setmacro	Specifies the macro definitions that should be used by the agent.
archivelogs	Archives the Agent logs so that they can be sent to Novell.
proxysetup	Set up your proxy server.
clearAgentLog	Clears the Patch Management Agent error log file.
clearErrLog	Clears the Patch Management Agent detection log file.
help	Displays the patch server script usage information.

Appendix

A

Patch Management Server Reference

In this appendix:

- *Server Security*
- *Server Error Pages*
- *WinInet Error Codes*
- *HTTP Status Codes*
- *Device Status Icons*

This section contains reference information pertaining to your Patch Management Server.

Server Security

There are multiple layers of security for ZENworks Patch Management. These layers include:

Web Site Authentication	Internet Information Services (IIS) controls authentication in to the ZENworks Patch Management web site, which means the operating system itself is validating users and their passwords.
Web Site Encryption via SSL	SSL provides an encrypted wrapper around all web communication to and from the product. Therefore installing ZENworks Patch Management with SSL will provide another level of protection.
User (Security) Roles	Every feature, page and action throughout ZENworks Patch Management has been assigned to a series of Access Rights. These access rights combine together to form a user role. Roles also contain a list of devices and device groups. Regardless of how a user is authenticated, the access and permissions are defined solely by the ZENworks Patch Management Administrator.

Note: ZENworks Patch Management default security settings prohibit the use of any browser other than Internet Explorer 6 SP1 and above. If you need to remove this restriction, and disable the enhanced security settings available with IE 6 SP1, refer to Novell Knowledge base.

Server Error Pages

The ZENworks Patch Management Server provides several distinct error pages. these pages are:

- **Access Denied** - This page is displayed whenever a users fails to provide valid credentials when accessing the Patch Management Server or they attempt to access an area to which they do not have access.
- **Internal Server Error** - This page is displayed whenever an unspecified internal error occurs. In most cases, closing the browser window and restarting your task will resolve the issue.
- **Refresh User Data** - This page is displayed whenever the current session expires, such as when there has been an extended period of inactivity.
- **Requested Page Not Found** - This page is displayed whenever a user attempts to navigate to an address that does not exist on the server. Links are provided to common sections of the server to assist the user in returning to their desired location.
- **System Component Version Conflict** - This page is displayed whenever a system component version is detected. To ensure optimal behavior the system components of ZENworks Patch Management are checked every time a user logs in. If a conflict is detected, this page identifies the component(s) that caused the conflict.

Note: ZENworks Patch Management will also send a notification e-mail to the ZENworks Patch Management Administrator when a conflict occurs.

- **Cache Expired** - This page is displayed whenever the user session expires. Usually the result of an extended period of inactivity.
- **Unsupported Browser Version** - This page is displayed whenever a user attempts to open the Patch Management Server with an unsupported browser.

WinInet Error Codes

ZENworks Patch Management uses Microsoft's WinInet API for communication between the Agents and Server. When this communication fails, the error codes returned are WinInet error codes. The following table defines the most common error codes.

Note: Refer to *Microsoft Knowledgebase article #193625* for additional WinInet error code descriptions.

Table 163: WinInet Error Code Descriptions

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.

HTTP Status Codes

As a Web based application using Internet Information Services (IIS), ZENworks Patch Management users HTTP status codes. While many of the status codes are informational only, the following table defines a few of the common error codes.

Table 164: HTTP Status Codes

Code	Description
HTTP 401.1 - Login failed	Logon attempt was unsuccessful (likely due to invalid user name or password).
	Note: ZENworks Patch Management will display a custom error page (as defined under *Server Error Pages* on page 318 instead of the default *HTTP 401.1 - Logon failed* error page.
HTTP 403.4 - SSL required	You must use HTTPS instead of HTTP when access this page.
HTTP 403.9 - Too many users	The number of connected users exceeds the defined connection limit.
HTTP 404 - Not found	The requested file cannot be found.
	Note: ZENworks Patch Management will display a custom error page (as defined under *Server Error Pages* on page 318 instead of the default *HTTP 404 - Not Found* error page.

Device Status Icons

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

Table 165: Device Status Icons

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

Appendix

B

Securing Your Patch Management Server

In this appendix:

- *Secure Your Server With SSL*
- *Use Secure Passwords*
- *Turn Off File and Printer Sharing*
- *Put Your Server Behind a Firewall*
- *Turn Off Non-Critical Services*
- *Lock Down Unused TCP and UDP Ports*
- *Apply All Security Patches*

This appendix identifies the various options available when securing your Patch Management Server.

Secure Your Server With SSL

Secure Sockets Layer (SSL) is a protocol used to secure data transmitted over the internet. SSL support is included in browsers, web servers, and operating systems so that any type of client and server can use authenticated and encrypted communications over private as well as public networks. ZENworks Patch Management always uses SSL when downloading vulnerability data and packages from the Global Subscription Server. Additionally, SSL can be used when transmitting data between the Patch Management Server and Patch Management Agents by enabling SSL during the installation of ZENworks Patch Management. This process involves obtaining a SSL certificate (.CER), and installing the certificate during the installation. Refer to *ZENworks Patch Management Server 6.4 SP2 Server Install Guide* for details regarding installing with SSL enabled.

Use Secure Passwords

Worm attacks frequently try to log in with weak and commonly used passwords. For secure passwords, the Department of Defense standard of 12 characters with alpha, numeric, punctuation and mixed case characters all included in a password is recommended.

Turn Off File and Printer Sharing

The ZENworks Patch Management Server should not be used as a file or print server. Additionally, an intruder can exploit a Windows networking share. Therefore, File and Printer Sharing for Microsoft Networks should be disabled.

Turning Off File and Printer Sharing

1. From within the *Windows Control Panel*, select the **Network Connections** icon.

2. Open the *Local Area Connection*.

3. Click **Properties**.

   Step Result: The *Local Area Connection Properties* window opens.
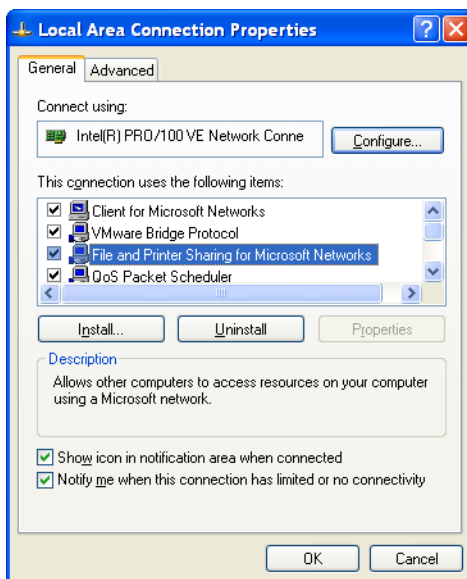
Figure 175: Local Area Connection Properties

4. Select **File and Printer Sharing for Microsoft Networks**.

> ⚠ **Caution:** Do not uninstall **Client for Microsoft Networks** because it is required by both *Microsoft SQL Server* and *Internet Information Server*.

5. Click **Uninstall**.

6. Click **OK**.

Result: File and Printer Sharing for Microsoft Networks is no longer enabled.

Put Your Server Behind a Firewall

Since the ZENworks Patch Management Server receives its patch updates from the Global Subscription Server (GSS), there is no need to allow access from the Internet into the Patch Management Server. However, access to the GSS must be specified in your Firewall configuration.

Turn Off Non-Critical Services

The default installation of Microsoft Windows has most features and services active. Therefore, there are a number of services that can be turned off (e.g.: RPC, Remote Registry, etc.) to reduce the risk of outside attacks. Although Novell does not encourage this type of lock down, it can be an effective method to reduce the risk of hacker attacks. The following services are required to run ZENworks Patch Management:

- World Wide Web Publishing Service
- IIS Admin Service
- MSSQLSERVER
- ZENworks Patch Management

Lock Down Unused TCP and UDP Ports

Preventing network traffic on various unused and vulnerable TCP and UDP ports should be completed through the use of a firewall. However, if a firewall is not available or additional machine level locking is desired, TCP and UDP ports can be locked down as a function of the network connection.

Locking Unused Ports

1. From within the *Windows Control Panel*, select the **Network Connections** icon.

2. Open the **Local Area Connection**.

3. On the *Local Area Connection Status General* tab, click **Properties**.

Step Result: The *Local Area Connection Properties* window opens.
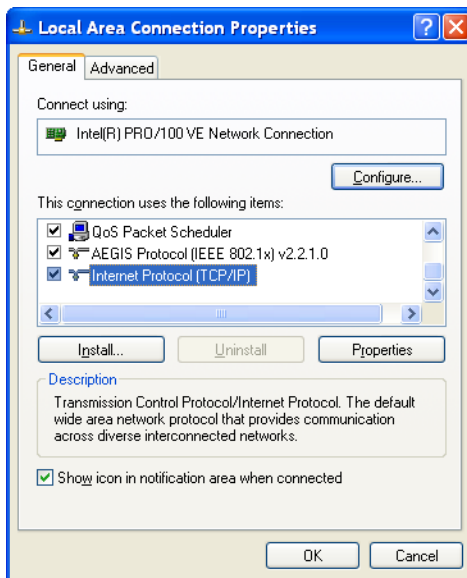
Figure 176: Local Area Connection Properties

4. Select the **Internet Protocol (TCP/IP)** protocol.

5. Click **Properties**.

    Step Result: The *Internet Protocol (TCP/IP) Properties* window opens.
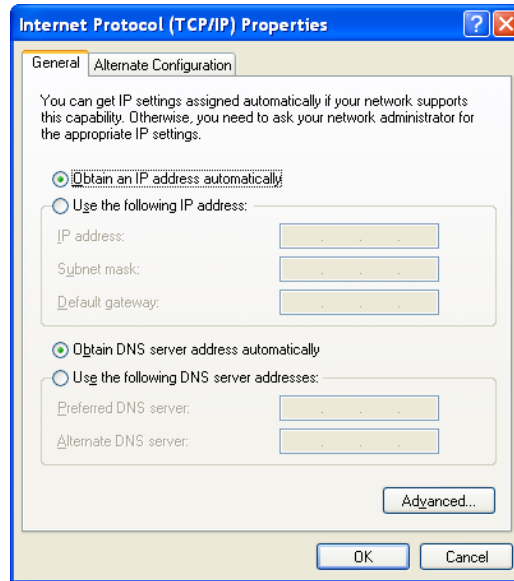
Figure 177: Internet Protocol (TCP/IP) Properties

6. In the *General* tab, click **Advanced...**

    Step Result: The *Advanced TCP/IP Settings* window opens.

7. Select the *Options* tab.

8. Select **TCP/IP Filtering**.

9. Click **Properties**.

> **Step Result:** The *TCP/IP Filtering* window opens.
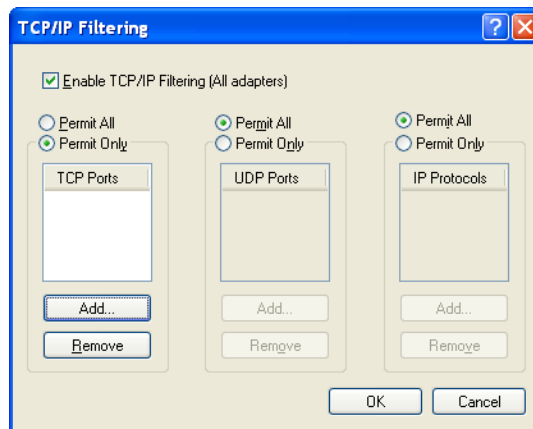
Figure 178: TCP/IP Filtering

10. Enable the **Enable TCP/IP Filtering (All Adapters)** option.

11. Select the **Permit Only TCP Ports** option.

12. Add TCP ports *443* and *80* to the listing of permitted ports.

    a) Click **Add...**

> **Step Result:** The *Add Filter* window opens.

    b) Type *443* in the **TCP Port** field.

    c) Click **OK**.

> **Step Result:** The *Add Filter* window closes.

    d) Repeat steps a, b, and c to add port *80*.

> **Note:** No other ports are required, although you may want to enable additional ports to allow DNS, TS, or VNC.

13. Select the **Permit Only UDP Ports** option, leaving the UPP Ports window blank since no UDP ports are required.

14. Close the open windows.

After Completing This Task:

With all ports locked (except for ports 80 and 443), it will be necessary to add entries to your Proxy or HOSTS file for the necessary Novell websites and the Global Subscription Server.

Apply All Security Patches

Apply all applicable Microsoft Security Patches to ensure that the server remains protected against all known security threats. Be sure to apply the most recent patches for IIS, SQL Server, and Windows Server 2003.

Appendix

C

Working With the Content Update Tool

In this appendix:

- *Content Update Tool System Requirements*
- *Installing the Content Update Tool*
- *Using the Content Update Tool*

With the advent of subscription support, some software manufacturers require a subscription to download software patches and updates. Due to this subscription model some vulnerabilities retrieved from the Global Subscription Server cannot include the vendor's patch. It is the Content Update Tool that will allow you to associate these vulnerabilities with the patches you download from the vendor. By associating these patches with the vulnerability details retrieved from the Global Subscription Server, you can continue to use the power and convenience of ZENworks Patch Management when maintaining your network.

Content Update Tool System Requirements

Supported Operating Systems

The Content Update Tool is supported on the following operating systems:

- Microsoft Windows Server™ 2003 Standard Edition with SP1 or higher.
- Windows Server 2003 Enterprise Edition with SP1 or higher.

Hardware Requirements

The computer on which the Content Update Tool is run, must meet the following minimum hardware requirements:

- 512 MB of RAM.
- 50 MB of free Disk Space.
- 1 GHz Processor.

Note: The actual RAM and Disk Space requirement will vary depending upon the size of the imported patches.

Other Requirements

In order to use the Content Update Tool, the following requirements must also be met:

- ZENworks Patch Management Server version 6.4 SP2.
- An active network connection to your Patch Management Server.
- Microsoft Windows Installer 2.0.
- Local / Domain Administrator or equivalent access.
- Administrator (Admin) rights to ZENworks Patch Management.
- An active Internet connection.

Installing the Content Update Tool

The Content Update Tool is available as a download from the *Agent Installers* page of your ZENworks Patch Management Server.

Downloading the Content Update Tool

Prior to installing the Content Update Tool, you must download the tool from your ZENworks Patch Management Server *Agent Installers* page.

1. Log on to the target computer as the local *administrator* (or a member of the *LOCAL_ADMINS* group).

2. Launch your web browser.

3. Type your Update Server URL in your web browser's **Address** field and press **Enter**.

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

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

6. Click **OK**.

   Step Result: The ZENworks Patch Management Server *Home* page opens.

7. Select **Devices**.

8. Click **Install**.

> **Step Result:** The *Agent Installers* page opens.
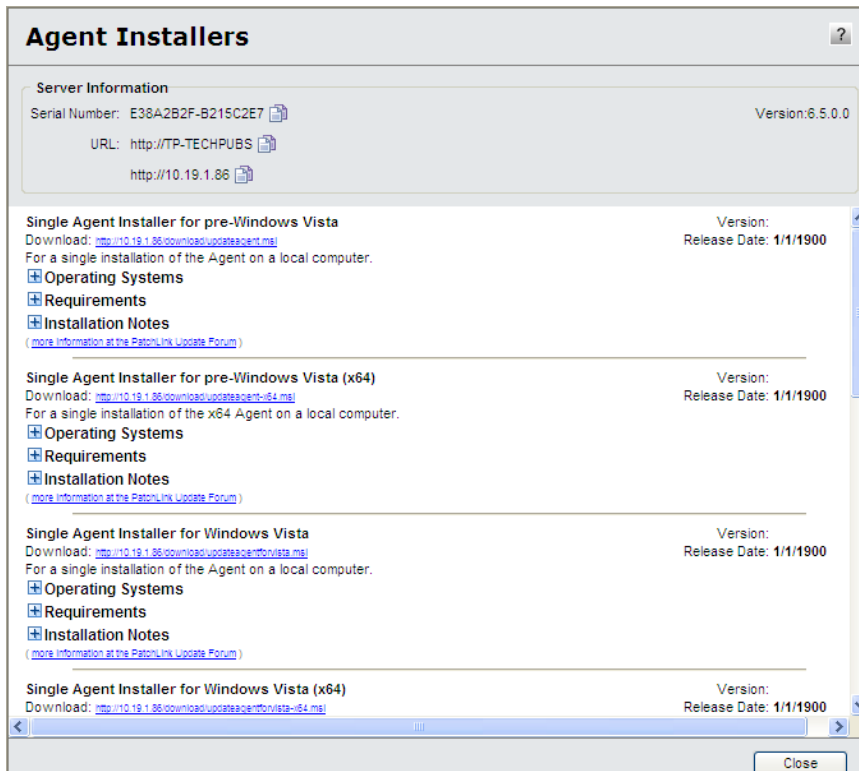
Figure 179: Agent Installers Page

9. From the *Agent Installers* window, select the **Content Update Tool** download link.

> **Step Result:** The *File Download* dialog box opens.

10. In the *File Download* dialog box, click **Save**.

> **Step Result:** The *Save As* window opens.

11. Specify the location to save the *ContentUpdateTool.msi* file, and click **Save**.

Result: The *ContentUpdateTool.msi* file is saved to the specified location.

Installing the Content Update Tool

Having downloaded the installer, you can now install the Content Update Tool.

1. From the downloaded location, select the *ContentUpdateTool.msi* file to extract the **Content Update Tool Installation Wizard**.

   Step Result: The **Content Update Tool Tool Welcome** page opens.

2. Click **Next**.

   Step Result: The **License Agreement** page opens.

3. If you agree with the license agreement select the **I Agree** option.

4. Click **Next**.

   Step Result: The **Select Installation Folder** page opens.
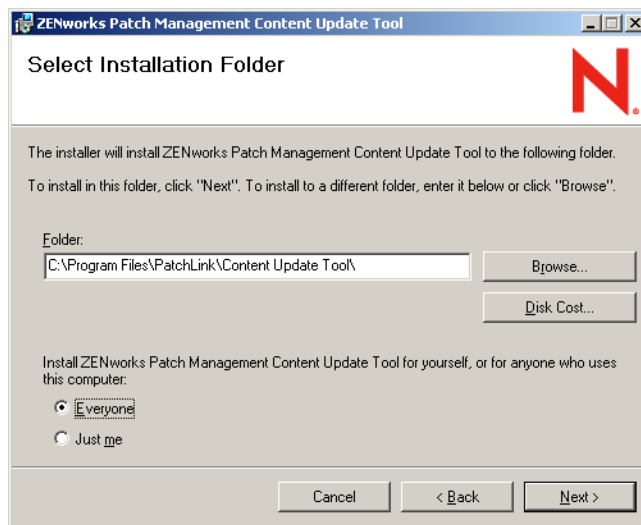
Figure 180: Content Update Tool - Select Installation Folder Page

5. If a different installation folder is required:

   a) Click **Browse...**

   b) Select a new folder and click **Save**.

   Step Result: The **Select Folder** window closes, returning to the **Select Installation Folder** page with the new path displayed.

6. If you want all users of this computer to have access to the Content Update Tool select **Everyone**.

7. Click Next.

   Step Result: The **Confirm Installation** page opens.

8. Click **Next** to install.

9. Click **Close** to exit the wizard.

Using the Content Update Tool

The Content Update Tool is a wizard-based utility that will guide you through the process of associating your ZENworks Patch Management vulnerability definitions with vendor supplied patches.

The Configuration Page

The Configuration page contains the configuration settings required to communicate with your ZENworks Patch Management Server and the Global Subscription Server. You must provide the configuration details, for the Patch Management Server Tab, Proxy Server Tab, and Options Tab before you can continue.

The following table defines the **Update Server** tab configuration options.

Table 166: Content Update Tool - Server Tab Configuration Options

Field	Description
Server Name	The name of your Patch Management Server.
Serial Number	The Patch Management Server serial number.

The following table defines the **Proxy Server** tab configuration options.

Table 167: Content Update Tool - Proxy Server Tab Configuration Options

Field	Description
Use Proxy	Select if a proxy is required during the communication between the Content Update Tool and your Patch Management Server. Selecting this option will enable the **Proxy Server** and **Port** fields.
Proxy URL	The proxy server's name. Do not include the *http://* or *https://* prefix.
Port	The proxy server's port.

Field	Description
Authenticated Proxy	Select if the defined proxy requires a user name and password.
	Selecting this option will enable the **Username** and **Password** fields.
Username	The user name used when connecting via the defined proxy.
Password	The password associated with the defined user name.

The following table defines the *Options* tab configuration options.

Table 168: Content Update Tool - Options Tab Configuration Options

Field	Description
Use SSL	Select to use SSL during communication with your Patch Management Server.
	Should only be enabled if your Patch Management Server is using SSL.
Log Errors	Select to enable error logging.
Product Information	Displays the Content Update Tool version and copyright information.

Note: The first time you use the Content Update Tool you must define the configuration options. The configuration details are then saved to the *C:\Program Files\Novell\Content Update Tool \ContentUpdate.xml* file and will be pre-populated the next time you load the Content Update Tool.

Using the Content Update Tool

1. Select **Start** > **Programs** > **Novell ZENworks** > **ZENworks Content Update Tool 6.4 SP-2** to start the Content Update Tool.

   Step Result: The *Welcome* page opens.

2. Click **Next**.

   Step Result: The *Configuration* page opens.
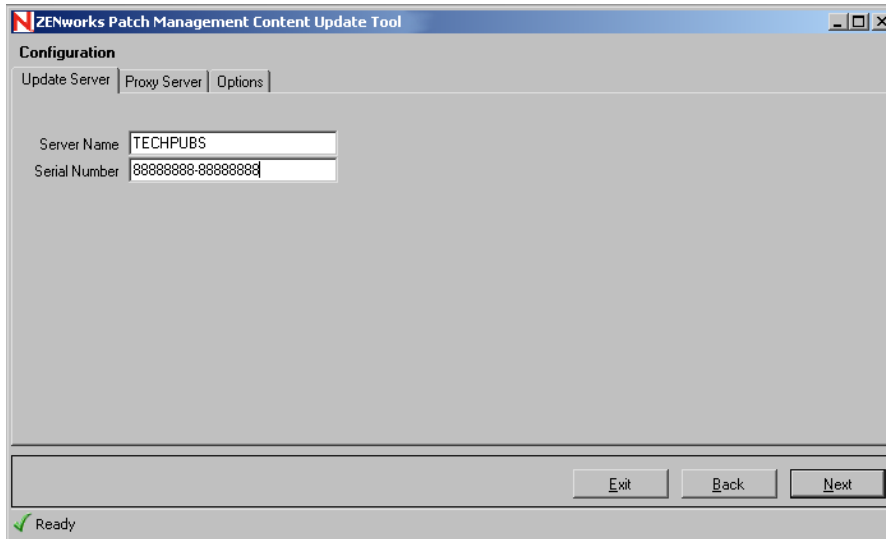
Figure 181: Content Update Tool - Configuration Page

3. Select the *Server* tab and set the configuration options.

   Table 169: Content Update Tool - Server Tab Configuration Options

Field	Description
Server Name	The name of your Patch Management Server.
Serial Number	The Patch Management Server serial number.

4. Select the *Proxy Server* tab and set the configuration options.

   Table 170: Content Update Tool - Proxy Server Tab Configuration Options

Field	Description
Use Proxy	Select if a proxy is required during the communication between the Content Update Tool and your Patch Management Server. Selecting this option will enable the **Proxy Server** and **Port** fields.

Field	Description
Proxy URL	The proxy server's name. Do not include the *http://* or *https://* prefix.
Port	The proxy server's port.
Authenticated Proxy	Select if the defined proxy requires a user name and password. Selecting this option will enable the **Username** and **Password** fields.
Username	The user name used when connecting via the defined proxy.
Password	The password associated with the defined user name.

5. Select the *Options* tab and set the configuration options.

Table 171: Content Update Tool - Options Tab Configuration Options

Field	Description
Use SSL	Select to use SSL during communication with your Patch Management Server. Should only be enabled if your Patch Management Server is using SSL.
Log Errors	Select to enable error logging.
Product Information	Displays the Content Update Tool version and copyright information.

6. Click **Next**.

Step Result: The *Vulnerability Selection* page opens.

7. Select a vendor, or type a search string, in the **Search** field.

8. Select a vulnerability impact in the Impacts field.

9. To limit the results to only those vulnerabilities that are applicable to devices managed by your Patch Management Server, select the **Only show applicable content** option.

10. To limit the results to only those vulnerabilities that have not already been cached, select the **Only show vulnerabilities not cached** option.

11. Click **Search**.

> **Step Result:** The vulnerabilities grid will display the results of your search.
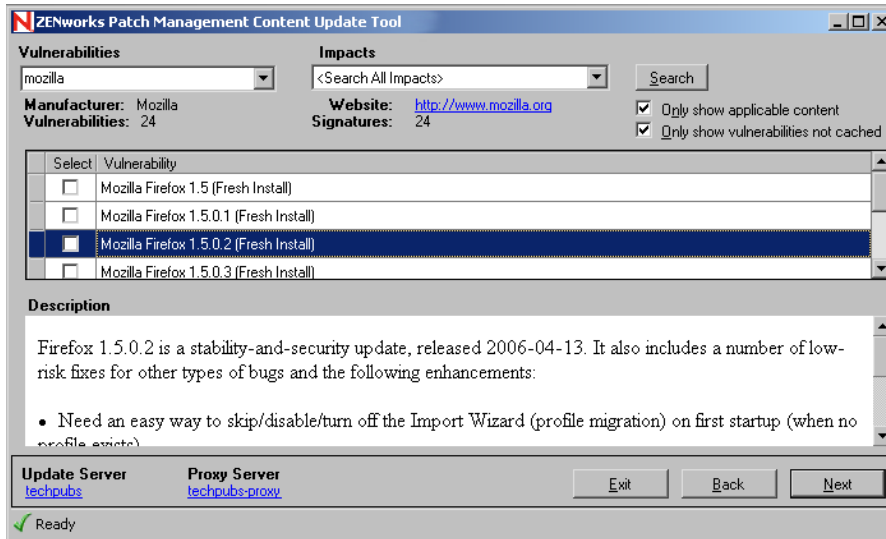
Figure 182: Content Update Tool - Vulnerability Selection Page

12. Select the desired vulnerabilities by selecting (or de-selecting) the checkboxes in the **Selected** column.

When selecting vulnerabilities, the following reference fields are available:

- **Manufacturer** - The manufacturer of the currently selected vulnerability.
- **Website** - The manufacturer's website.
- **Vulnerabilities** - The total number vulnerabilities from the selected manufacturer.
- **Signatures** - The total number of signatures from the selected manufacturer.
- **Description** - A description of the currently selected vulnerability.

13. Click **Next**.

> **Step Result:** The vulnerability metadata will be downloaded from the Global Subscription Server and the *Package Selection* page will open when the download is complete.
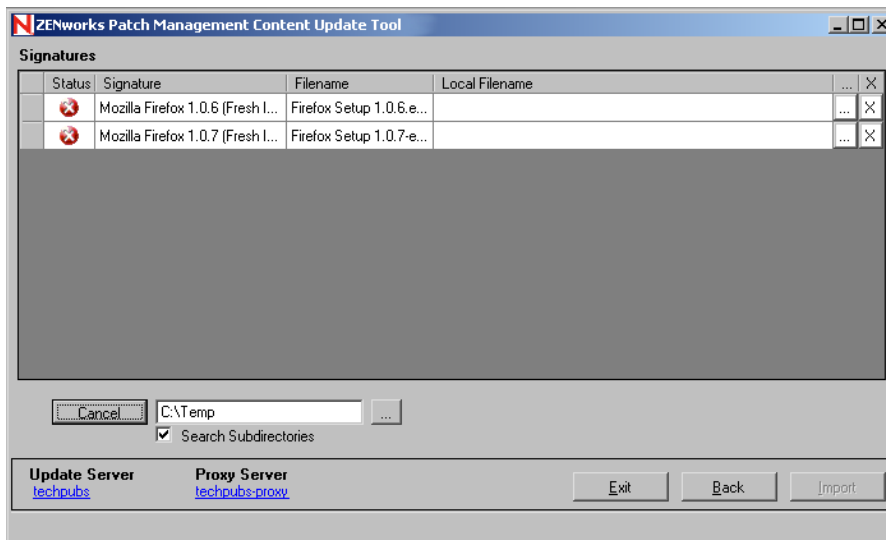
Figure 183: Content Update Tool - Package Selection Page

14. To perform an automatic selection of the package components:

   a) Type, or browse to (using the ellipsis button), the target search directory.

   b) If desired, select the **Search Subdirectories** option to include any sub-folders in the search.

   c) Click **Search**.

> **Step Result:** Files that are an exact match to the vulnerabilities metadata (including filename, file size, checksum, etc.) will be automatically selected.
>
> > **Note:** When you perform an automatic selection the Content Update Tool will attempt to associate the selected vulnerabilities with files found in the defined search directory. If the automatic selection is unable to find all of the necessary packages, you must either repeat the search using a different directory, or manually select the package components.

The following status icons are displayed in the **Status** column.

Table 172: Package Status Icons

Icon	Status Definition
✓	The green check indicates that the package component file has been found and is consistent with the vulnerability definition.
⚠	The yellow caution indicates that the package component file has been found but it is not consistent with the vulnerability metadata.
✗	The red X indicates the package component file has not been found.

15. To manually select the package components:

Note: Solaris patches downloaded from Sun must be renamed to a *.zip* file extension prior to selection and import.

a) Within the results grid, select the ellipsis button associated with the signature.
b) Browse to and select the desired file.

Note: The name of the file you select must match the filename defined in the vulnerability metadata (as displayed in the **Filename** column).

c) Click **Open** to select the file and return to the *Package Selection* page.

The following status icons are displayed in the **Status** column.

Table 173: Package Status Icons

Icon	Status Definition
✓	The green check indicates that the package component file has been found and is consistent with the vulnerability definition.
⚠	The yellow caution indicates that the package component file has been found but it is not consistent with the vulnerability metadata.
✗	The red X indicates the package component file has not been found.

16. Click **Import** to begin the package import.

> ⚠️ **Caution:** Although the Content Update Tool will allow you to force an import when the package is not an exact match to the vulnerability definition, this practice is discouraged. Possible reasons for the package not matching include file corruption and tampering. Additionally, if you choose to perform the import although the package is not an exact match to the vulnerability definition, the text *User Modified* will be added as a prefix to the vulnerability name and a listing of what properties failed to match will be added to the beginning of the vulnerability description.

Step Result: The package components are uploaded to your Patch Management Server and the *Summary Report* page will open when complete.
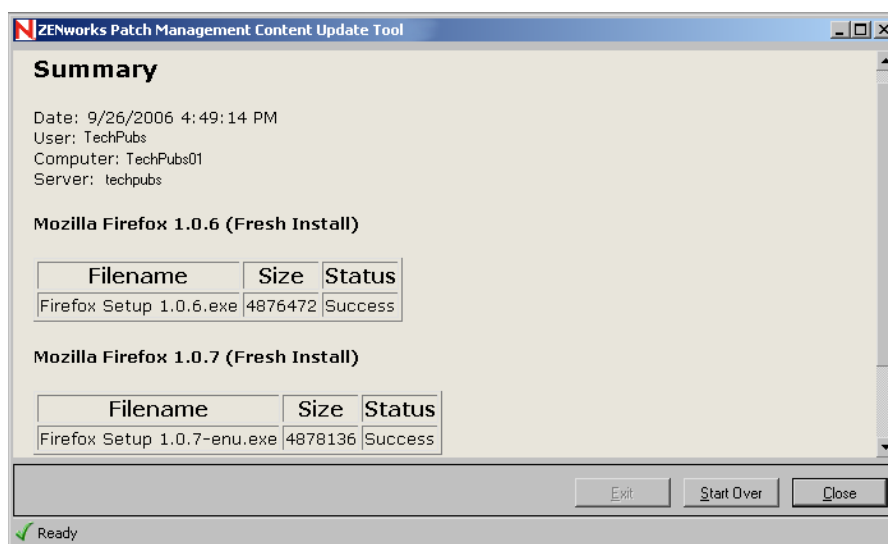
Figure 184: Content Update Tool - Summary Report Page

17. Click **Close** to exit the wizard.

Appendix

D

Creating a Disaster Recovery Solution

In this appendix:

- *Preparing Your Database*
- *Creating a Manual Solution*
- *Creating an Automated Solution*

Note: This appendix applies to Microsoft SQL Server 2005 and requires the Microsoft SQL Server Management Studio. The Management Studio is available by upgrading to SQL Server 2005 Standard or Enterprise or as a download from the *Microsoft Download Center*.

Preparing Your Database

The installation of ZENworks Patch Management sets your database to a recovery model of Simple. To use *Transaction Logs*, and thus increase the quality of your disaster recovery solution, you should change the recovery model to Full.

Changing the Database Recovery Model

1. Open the *Microsoft SQL Server Management Studio* (**Start** > **Programs** > **Microsoft SQL Server 2005** > **SQL Server Management Studio**).

2. Log into your database server.

3. Expand your server group, server, and database folder until you see the *PLUS* database.

4. Right-click on the *PLUS* database.

5. Select **Properties**.

Step Result: The *Database Properties* window opens.
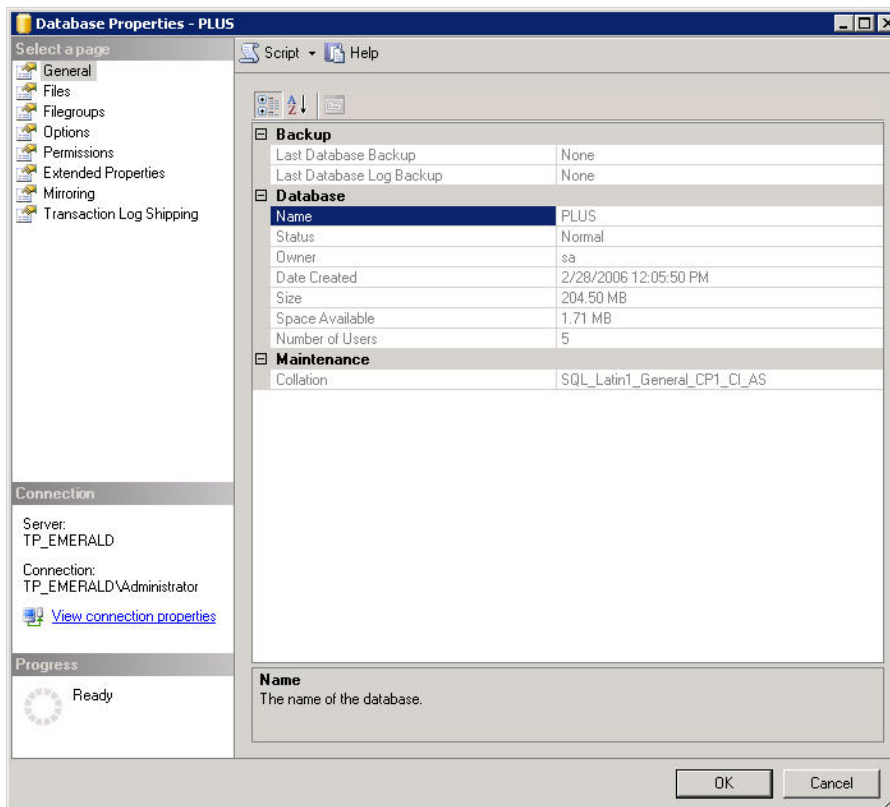
Figure 185: Database Properties

6. Select Options within the **Select a page** field.

Step Result: The *Options* page opens.

7. In the **Recovery model** field, select Full.

8. Click **OK**.

Step Result: The changes are saved and the *Database Properties* window closes.

9. Repeat for the *PLUS_Staging* database (and the *PLAMS* and *PLUS_Reports* databases if they exist).

After Completing This Task:

You must create a backup, of each database, before any Transaction logs will be created. Refer to *Creating a Database Backup* on page 343 to create a one-time backup of your database.

Creating a Manual Solution

While a Maintenance Plan will allow you to automate the backup of your databases and transaction logs, you can also create and restore individual backups using the SQL Server Management Studio.

Creating a Database Backup

The most important part of an effective disaster recovery technique is having a current and valid backup.

1. Open the *Microsoft SQL Server Management Studio* (**Start** > **Programs** > **Microsoft SQL Server 2005** > **SQL Server Management Studio**).

2. Log into your database server.

3. Expand your server group, server, and database folder until you see the *PLUS* database.

4. Right-click on the *PLUS* database.

5. Select **Tasks** > **Backup...**

>   **Step Result:** The *Back Up Database* window opens.
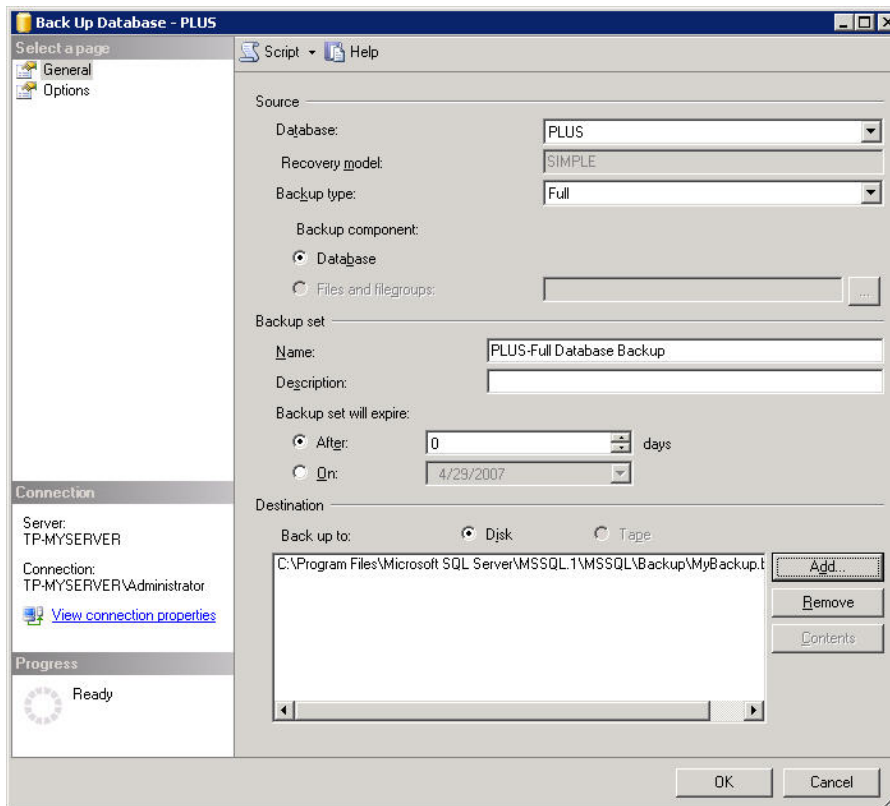
Figure 186: Back Up Database

6. Ensure that the Source values are set as follows:

- **Database**: *PLUS*
- **Recovery model**: Full

>   **Note:** If the **Recovery model** is not set to Full, refer to *Changing the Database Recovery Model* on page 341.

- **Backup Type**: Full
- **Backup Component**: Database

7. Define the backup set **Name**, **Description**, and when the **Backup set will expire**.

8. Define your backup **Destination** settings.

   a) Select either the **Disk** or **Tape** option.

b) Define the destination **Folder**.

> **Note:** For performance reasons, it is recommended that you create your database backup in a directory that is not on the same physical drive as your database.

9. Select Options within the **Select a page** field.

Step Result: The *Options* page displays.
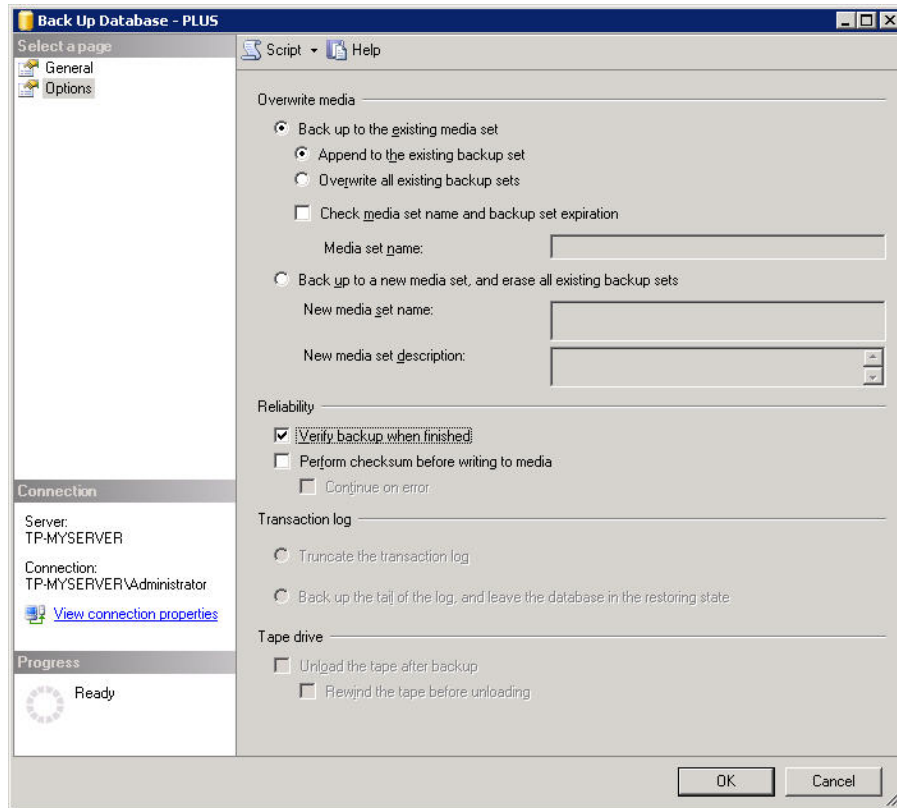
Figure 187: Back Up Database - Options

10. Select whether to **Backup up to the existing media set** or **Back up to a new media set, and erase all existing backup sets** as is appropriate for your organization.

11. Select the **Verify backup when finished** option to ensure a valid backup.

12. Click **OK**.

13. Repeat for the *PLUS_Staging* database (and the *PLAMS* and *PLUS_Reports* databases if they exist).

Restoring a Database Backup

Another important part of an effective Disaster Recovery Solution is having a process defined in which to restore your database backup.

1. Open the *Services Management Console* (**Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services**).

2. Select and right-click the **ZENworks Patch Management Update** service.

3. Select **Stop**, to stop the **ZENworks Patch Management Update** service.

4. Select and right-click the **World Wide Web Publishing** Service.

5. Select **Stop**, to stop the **World Wide Web Publishing** Service.

6. Open the *Microsoft SQL Server Management Studio* (**Start** > **Programs** > **Microsoft SQL Server 2005** > **SQL Server Management Studio**).

7. Log into your database server.

8. Expand your server group, server, and database folder until you see the *PLUS* database.

9. Right-click on the **Databases** folder.

10. Select **Restore Database...**

> **Step Result:** The *Restore Database* window opens.
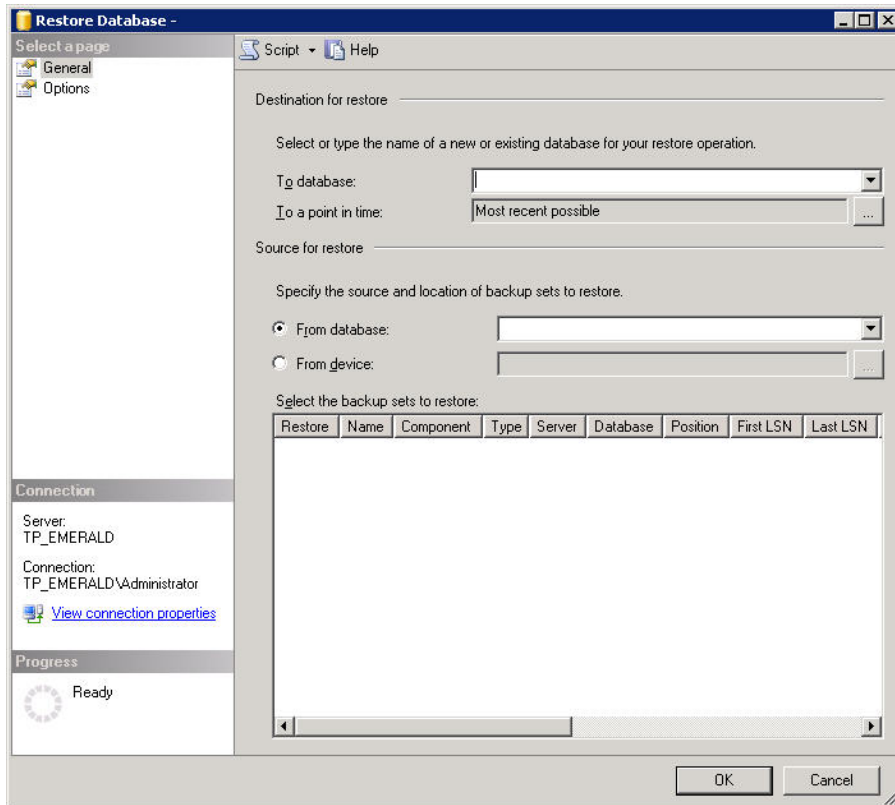
Figure 188: Restore Database

11. In the **To database** field, type or select the database you need.

> **Note:** Specifying a new name for the database automatically defines the database files restored from the database backup.

12. Select **From device** and click the ellipses button.

> **Step Result:** The *Specify Backup* window opens.

13. Click **Add**.

> **Step Result:** The *Locate Backup File* window opens.

14. Locate and select your backup (*.bak*) file.

15. Click **OK**.

16. Click **OK** to return to the *Restore Database* window.

17. Select your backup within the **Select the backup sets to restore** field.

18. Select Options within the **Select a page** field.

    Step Result: The *Options* page will display.
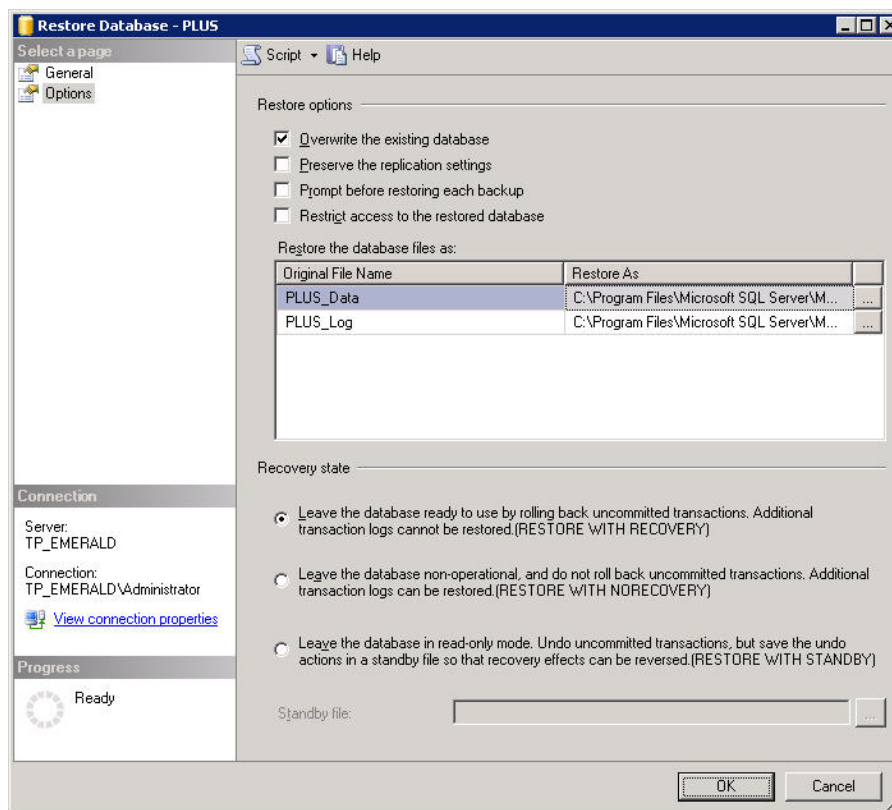
Figure 189: Restore Database - Options

19. Ensure the **Overwrite the existing database** option is selected.

20. Verify, and correct if necessary, the directory path within the **Restore the database files as** field.

21. Ensure the **Leave the database ready to use...** option is selected.

22. Click **OK** to begin the database restoration.

23. Repeat for the *PLUS_Staging* database.

24. Restart the **ZENworks Patch Management Update** and **World Wide Web Publishing Service** services.

Creating an Automated Solution

A Maintenance Plan allows you to create an automated backup and schedule the backup to occur as frequently as your organizational needs dictate. Maintenance Plans allow you to define your back up options as well as which databases and transaction logs to include.

Note: If you have not already done so, you should change your Database Recovery Model to FULL before continuing. Refer to *Changing the Database Recovery Model* on page 341 for additional details.

Creating a Maintenance Plan

The following procedure will walk you through the process of creating an automated Database Maintenance Plan for your *PLUS* and *PLUS_Staging* databases.

Prerequisites:

Prior to creating a Maintenance Plan you must upgrade your database server to ***Microsoft SQL Server 2005 Standard*** or ***Microsoft SQL Server 2005 Enterprise***, install SSIS (***SQL Server Integration Services***), and set the ***SQL Server Agent*** startup type to Automatic.

1. Open the ***Microsoft SQL Server Management Studio*** (**Start** > **Programs** > **Microsoft SQL Server 2005** > **SQL Server Management Studio**).

2. Log into your database server.

3. Expand your server group, server, and database folder until you see the *Maintenance Plans* folder.

4. Right-click on the *Maintenance Plans* folder.

5. Select **Maintenance Plan Wizard**.

Step Result: The **SQL Server Maintenance Plan Wizard** opens.
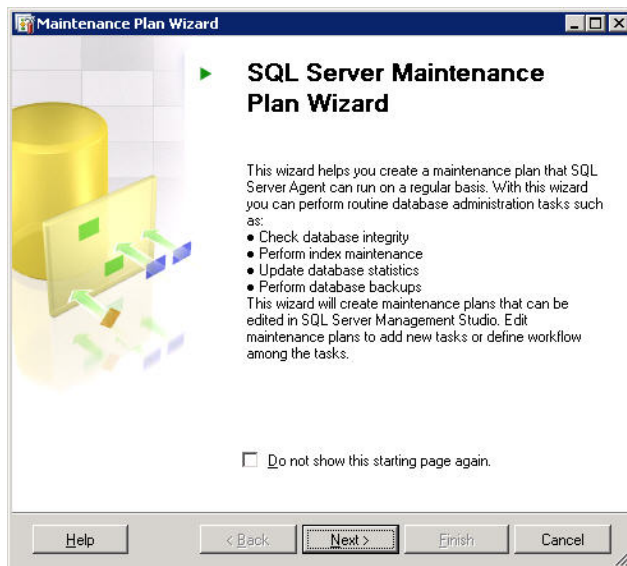
Figure 190: SQL Server Maintenance Plan Wizard

6. Click **Next**.

Step Result: The *Select a Target Server* page opens.

7. Define the maintenance plan **Name**, **Description** [optional], target **Server**, and **Authentication** method.

8. Click **Next**.

Step Result: The *Select Maintenance Tasks* page opens.

9. Select the following maintenance tasks:

- **Check Database Integrity**
- **Clean Up History** [optional]
- **Back Up Database (Full)**
- **Back Up Database (Transaction Log)**

10. Click **Next**.

Step Result: The *Select Maintenance Task Order* page opens.

11. Set the tasks to execute in the following order:

- **Check Database Integrity**
- **Back Up Database (Full)**
- **Back Up Database (Transaction Log)**
- **Clean Up History** [optional]

12. Click **Next**.

Step Result: The *Define Database Check Integrity Task* page opens.

13. Click the **Database** drop-down.

   a) Select the **These databases** option.

   b) Select the *PLUS* and *PLUS_Staging* databases.

   c) Click **OK**.

14. Ensure that the **Include indexes** option is selected.

15. Click **Next**.

     Step Result: The *Define Back Up Database (Full) Task* page opens.
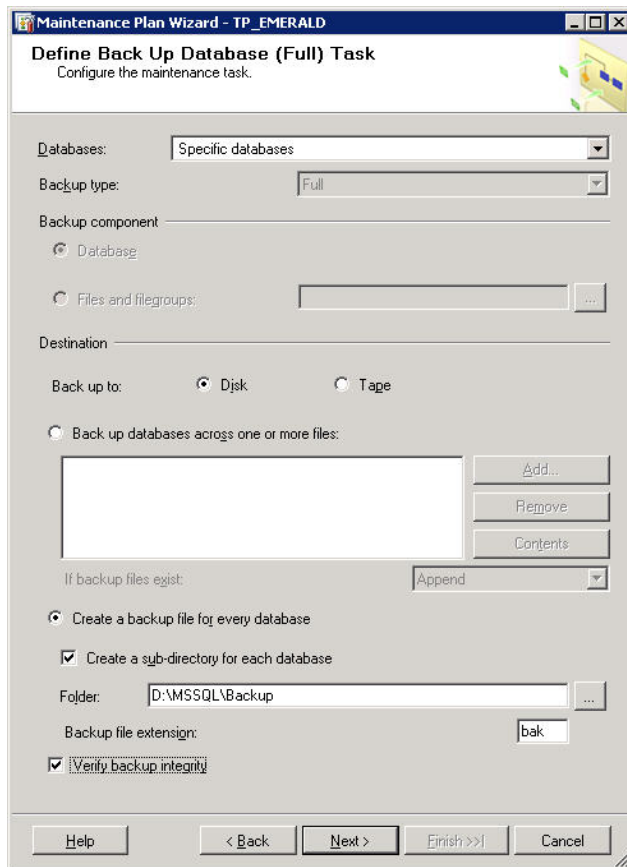
Figure 191: Define Back Up Database (Full) Task

16. Click the **Database** drop-down.

    a) Select the **These databases** option.

    b) Select the *PLUS* and *PLUS_Staging* databases.

    c) Click **OK**.

17. Define your Back up **Destination** settings.

    a) Select either the **Disk** or **Tape** option.

    b) Select to **Create a backup file** for every database.

    c) Select to **Create a sub-directory** for each database.

d) Define your destination **Folder**.

> **Note:** For performance reasons, it is recommended that you create your database backup in a directory that is not on the same physical drive as your database.

e) Ensure the **Backup file extension** is set as *bak*.
f) Select **Verify backup integrity**.

18. Click **Next**.

Step Result: The ***Define Back Up Database (Transaction Log) Task*** page opens.

19. Click the **Database** drop-down.
a) Select the **These databases** option.
b) Select the *PLUS* and *PLUS_Staging* databases.
c) Click **OK**.

20. Define your Back up **Destination** settings.
a) Select either the **Disk** or **Tape** option.
b) Select to **Create a backup file** for every database.
c) Select to **Create a sub-directory** for each database.
d) Define your destination **Folder**.

> **Note:** For performance reasons, it is recommended that you create your database backup in a directory that is not on the same physical drive as your database.

e) Ensure the **Backup file extension** is set as *trn*.
f) Select **Verify backup integrity**.

21. Click **Next**.

> **Step Result:** If the **Clean Up History** option was selected, the *Define Cleanup History Task* page opens. Otherwise the *Select Plan Properties* page will open.
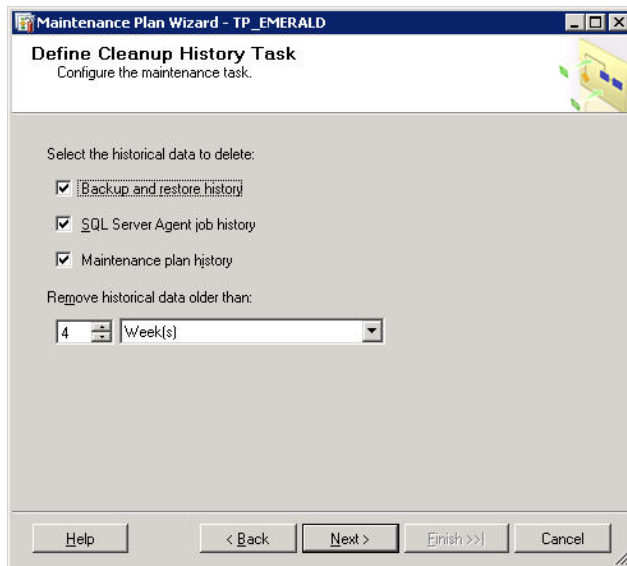
Figure 192: Define Cleanup History Task

22. If the **Clean Up History** option was selected, define the *Cleanup History Task* options.

a) Ensure that **Backup and restore history** is selected.
b) Ensure that **SQL Server Agent job history** is selected.
c) Ensure that **Maintenance plan history** is selected.
d) Define the **Remove historical data older than** setting as appropriate for your organization.
e) Click **Next**.

> **Step Result:** The *Select Plan Properties* page will open.

23. If desired, click **Change...** to open the *New Job Schedule* page and define the maintenance plan schedule.

Figure 193: New Job Schedule

a) Enter a **Name** for the schedule.
b) Select a **Schedule** type.
c) Ensure that **Enabled** is selected.
d) Define the **Occurrence** frequency (**Daily**, **Weekly**, or **Monthly**) and options.
e) Define the **Daily frequency**.
f) Define the **Duration**.
g) Click **OK**.

Step Result: The changes are saved and the *New Job Schedule* page closes.

24. Click **Next**.

Step Result: The *Select Report Options* page opens.

25. Set your desired reporting options.

26. Click **Next**.

    Step Result: The *Complete the Wizard* page opens.

27. Click **Finish** to complete the wizard.

After Completing This Task:

You must now establish a backup procedure which will archive all of your backup files and the contents of the Patch Management Server *Storage* directory on a regular basis. This can be done through the use of any file backup utility.

Appendix
E

Working With the Distribution Point

In this appendix:

- *Distribution Point System Requirements*
- *Installing the Distribution Point*
- *Configuring the Distribution Point*

The Distribution Point, based upon the Apache HTTP Server 2.2.3 open source product, provides remote package caching to a network. Through the use of the Distribution Point, agent communication can be redirected from the primary Patch Management Server to a local web-cache server. This appendix defines the procedures for installing, configuring, and managing the Distribution Point.

Distribution Point System Requirements

Supported Operating Systems

The Distribution Point is supported on the following operating systems:

- Microsoft® Windows Server™ 2003, Standard Edition
- Windows Server 2003, Enterprise Edition
- Windows Server 2003 R2, Standard Edition
- Windows Server 2003 R2, Enterprise Edition

Note: For additional operating system support details refer to *http://httpd.apache.org*.

Hardware Requirements

The computer on which the Distribution Point is installed, must meet the following minimum hardware requirements:

- 256 MB RAM.
- 5 GB of free disk space.
- A LAN connection.

Note: For additional requirements details refer to *http://httpd.apache.org*.

Installing the Distribution Point

The Distribution Point is available as a download from the **Agent Installers** page of your ZENworks Patch Management Server.

Downloading the Distribution Point

Prior to installing the Distribution Point, you must download the tool from your ZENworks Patch Management Server **Agent Installers** page.

1. Log on to the target computer as the local *administrator* (or a member of the *LOCAL_ADMINS* group).

2. Launch your web browser.

3. Type your Patch Management Server URL in your web browser's **Address** field and press **Enter**.

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

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

6. Click **OK**.

   Step Result: The ZENworks Patch Management Server **Home** page opens.

7. Select **Devices**.

8. Click **Install**.

   Step Result: The *Agent Installers* page opens.
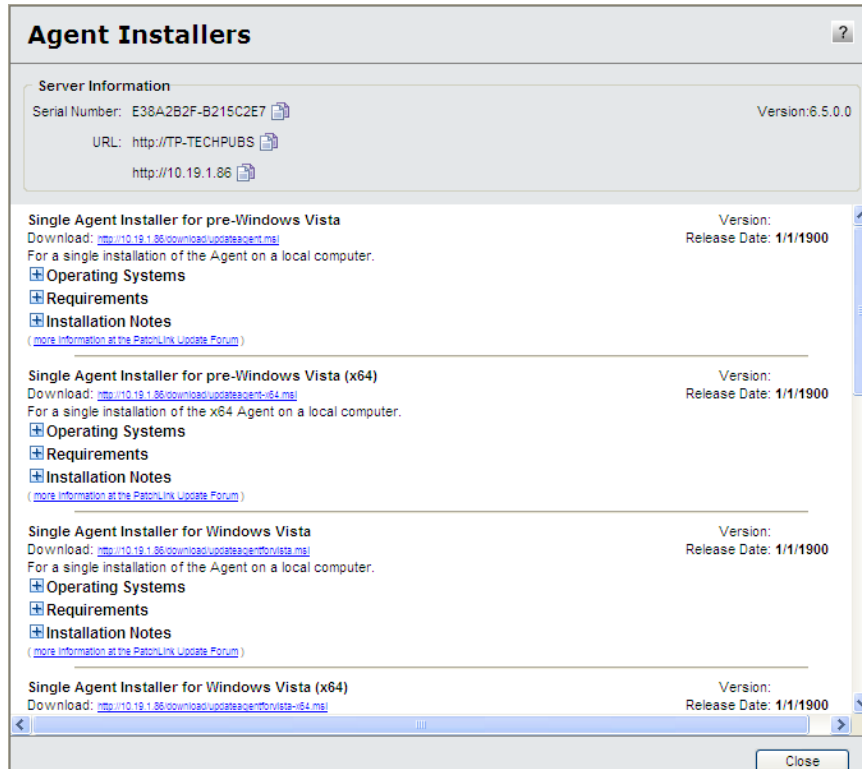
Figure 194: Agent Installers Page

9. From the *Agent Installers* window, select the **Distribution Point** download link.

   Step Result: The *File Download* dialog box opens.

10. In the *File Download* dialog box, click **Save**.

   Step Result: The *Save As* window opens.

11. Specify the location to save the *DistributionPoint.msi* file, and click **Save**.

   Result: The *DistributionPoint.msi* file is saved to the specified location.

Installing the Distribution Point

Having downloaded the installer, you can now install the Distribution Point.

1. Select the *distributionpoint.msi* file to start the Distribution Point Installation Wizard.

   Step Result: The *Welcome* page opens.

2. Click **Next**.

   Step Result: The *License Agreement* page opens.

3. If you agree to the license terms, select the **I accept the terms in the license agreement** option.

4. Click **Next**.

   Step Result: The *Destination Folder* page opens.

5. If a different installation path is required:
   a) Click **Change**.

      Step Result: The *Save As* window opens.

   b) Browse to and select a new path.
   c) Click **Save**.

      Step Result: The *Save As* window closes, returning to the *Destination Folder* window with the new path selected.

6. Click **Next**.

   Step Result: The *Cache Folder* page opens.

7. If a different cache location is required:
   a) Click **Change**.

      Step Result: The *Save As* window opens.

   b) Browse to and select a new path.
   c) Click **Save**.

      Step Result: The *Save As* window closes, returning to the *Cache Folder* window with the new path selected.

8. Click **Next**.

   Step Result: The *ZENworks Patch Management Server Information* page opens.

9. Type the **Patch Management Server URL** and **Serial Number** in their respective fields.

10. Click **Next**.

    Step Result: The Server Information page opens.

11. Enter the following information.

Field	Description
Network Domain	The DNS domain in which your Distribution Point is registered (MyDomain.com).

Field	Description
Server Name	The full DNS name of the server on which you are installing the Distribution Point (ServerName.MyDomain.com).
Administrator's Email Address	The Distribution Point Administrator's (or Webmaster's) e-mail address.
Port	The port on which the Distribution Point will monitor incoming traffic. (Default = 80)

12. Click **Next**.

    Step Result: The *Ready to Install* page opens.

13. Click **Install** to begin the installation.

14. Click **Finish** to exit the wizard.

Configuring the Distribution Point

During the installation of the Distribution Point, the custom installer configures the files in the *conf* subdirectory, based upon your environment and responses. It is recommended that you do not alter these settings. Doing so may disable your Distribution Point and could require re-installation.

Caution: Reinstallation of the Distribution Point will not overwrite any of the configuration files in the *conf* subdirectory. The new file is appended with a *.default* extension. The configuration file must be manually updated by referencing and copying the settings in the *.default* file into your *.conf* file.

Table 174: Configurable Distribution Point Directives

Directive Name	Usage	Default Value
ThreadsPerChild value	The Maximum number of connections the Distribution Point can handle at one time.	100
MaxRequestsPerChild value	The number of requests a child process will serve before exiting. A value of 0 indicates the process will never exit.	0

Directive Name	Usage	Default Value
ServerRoot path	The Distribution Point installation path. Defined during installation	*<Program Files> / Apache Software Foundation /Apache2.2/*
Listen value	The ports on which the Distribution Point monitors incoming traffic. Defined during installation	80
ServerAdmin value	The Distribution Point Administrator's e-mail address. Defined during installation	
ServerName value	The Distribution Point's Hostname (includes port if the Distribution Point was not installed on port 80). Defined during installation	
DocumentRoot path	The directory that forms the main document tree which is visible from the web. Uses the install path defined during installation	*<Program Files> / Apache Software Foundation /Apache2.2/ htdocs*
ErrorLog path	The location defining the Distribution Point Error Logs.	logs/errro.log
LogLevel value	The indicator that controls error logging.	Warn
ProxyRequests value	The indicator that defines whether forward (standard) proxy requests are enabled.	On
CacheRoot path	The directory root where cache files are stored. Defined during installation	*<Program Files> / Apache Software Foundation /Apache2.2/ cache*

Directive Name	Usage	Default Value
CacheMaxFileSize value	The maximum file size (in bytes) that will be cached.	100000000000
CacheMinFileSize value	The minimum file size (in bytes) that will be cached.	1
CacheEnable type URL	The storage type and URLs to cache.	disk /disk[1] http://patchlink-1
CacheDirLevels value	The number of subdirectory levels in the cache.	3
CacheDirLength value	The number of characters in the subdirectory names.	1
CacheDisable URL	The function that disables caching of the specified URLs.	*http://security. update.server /update-list/*

Tip: If additional details are required regarding the Distribution Point (Apache HTTP Server Version 2.2.3), refer to the *Directive Quick Reference* and other *online documentation* published by the Apache Software Foundation.