
ZENworks 11 SP4

Patch Management Reference

October 2016

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.novell.com/company/legal/>.

Copyright © 2016 Novell, Inc. All Rights Reserved.

Contents

About This Guide	7
1 What's New in ZENworks 11 SP4 Update 2	9
SLES 12 Support	9
SLES 12 Support Instructions	9
Cached Patch Bundle Cleanup	12
Performance Improvements	12
Pre-Computed Responses	13
Enhanced Vulnerability Detection	13
Patch Policy Notification and Cancel Options	13
New Patch Reports	13
2 Patch Management Overview	15
Product Overview	15
Patch Management Process	16
Features of Patch Management	17
Supported ZENworks Server and Agent Environments	18
3 Getting Started with ZENworks 11 SP4 Update 2	27
Downloading Patches	27
Deploying a Patch	27
Setting a Baseline	28
Dashboard	28
Patch Download Status	29
Patch Wizard	29
4 Using Patch Management	31
Viewing Subscription Service Information	31
Configuring HTTP Proxy Detail	33
Configuring Patch Subscription Credentials	35
Adding a Credential	38
Configuring Subscription Service Content Download Details	39
Configuring Email Notification Details	43
Configuring Patch Dashboard and Trending Behavior	45
Configuring the Schedule for Vulnerability Detections	49
Vulnerability Detection Schedule: Date Specific	52
Vulnerability Detection Schedule: Recurring	53
Vulnerability Detection Schedule: Set Vulnerability Detection at Folder Level	58
Configuring Mandatory Baseline Settings	60
Patch Management Licensing	62
5 Using the Patch Management Tab	67
Viewing Patches	67
Dashboard	68

Status	72
Status	72
Cache Status	73
Using the Patches Page	73
Patches	73
Patch Information	84
Searching for a Patch	85
Patch Management	87
Patch Management Reports	88

6 Using the Deploy Remediation Wizard 91

Creating a Deployment Schedule	91
Confirm Devices	92
Confirm Devices: All Non-patched Devices	93
Confirm Devices: Select Applicable Devices	93
Confirm Devices: Select Devices, Folders, and Groups	94
License Agreement	95
Remediation Schedule	95
Remediation Schedule: Now	96
Remediation Schedule: Date Specific	97
Remediation Schedule: Recurring	98
Remediation Schedule: Wake On LAN	103
Deployment Order and Behavior	105
Remediation Options	106
Advanced Remediation Options	107
Pre Install Notification Options	108
Distribution Schedule	110
Distribution Schedule: No Schedule	111
Distribution Schedule: Date Specific	111
Distribution Schedule: Recurring	113
Notification and Reboot Options	118
11.3 New variables	120
Choose Deployment Name	121
Deployment Summary	122

7 Using Mandatory Baselines 123

About Mandatory Baselines	123
Viewing Mandatory Baselines	124
Using the Mandatory Baseline Page	127
Working with Mandatory Baselines	128
Assigning or Managing a Mandatory Baseline	129
Removing a Mandatory Baseline	132
Using Update Cache	134

8 Patch Management for a Device 135

Accessing the Patches Tab for a Device	135
Using the Patches Tab for a Device	138
Patches	138
Patch Name	139
Total Number of Patches Available	139
Patch Impacts	139
Patch Statistics	140
Action Menu Items	140
Searching Patches	141

Patch Information	143
Workstation Device Patches	144
9 Patch Management for a Device Group	147
Using the Patches Tab within a Server Group	147
Using the Patches Tab within a Workstation Group	150
10 License Behavior of ZPM	153
ZCM Only State	153
Trial State	153
Trial Expired State	154
Licensed State	154
License Expired State	154
11 ZENworks Reporting Reports	155
Viewing the Predefined Report	155
12 Best Practice with ZENworks 11 SP4 Update 2 Patch Management	157
Testing Patches	158
Deploying Patches in a Controlled Way	158
Setting a Baseline	159
Monitoring	159
13 Patch Policy	161
Setting up a Patch Policy	161
Publishing Patch Policy	165
Advanced Configuration for Patch Policy	165
Testing a Policy before deploying to Live Environment	171
Scheduling a Patch Policy	171
Patch Policy Assignment Wizard	172
Patch Policy Enforcement	172
Patch Policy Distribution	175
Patch Policy - Best Practice	177
A Patch Management Appendix	179
Patch Management Issues	179
Configuration Issues	186
Error Codes	186
Patch Management System Variables	195

About This Guide

This *ZENworks 11 SP4 Patch Management Reference* includes information to help you successfully install a Novell ZENworks 11 SP4 Patch Management system. The information in this guide is organized as follows:

- ♦ Chapter 1, “What’s New in ZENworks 11 SP4 Update 2,” on page 9
- ♦ Chapter 2, “Patch Management Overview,” on page 15
- ♦ Chapter 3, “Getting Started with ZENworks 11 SP4 Update 2,” on page 27
- ♦ Chapter 4, “Using Patch Management,” on page 31
- ♦ Chapter 5, “Using the Patch Management Tab,” on page 67
- ♦ Chapter 6, “Using the Deploy Remediation Wizard,” on page 91
- ♦ Chapter 7, “Using Mandatory Baselines,” on page 123
- ♦ Chapter 8, “Patch Management for a Device,” on page 135
- ♦ Chapter 9, “Patch Management for a Device Group,” on page 147
- ♦ Chapter 10, “License Behavior of ZPM,” on page 153
- ♦ Chapter 11, “ZENworks Reporting Reports,” on page 155
- ♦ Chapter 12, “Best Practice with ZENworks 11 SP4 Update 2 Patch Management,” on page 157
- ♦ Chapter 13, “Patch Policy,” on page 161
- ♦ Appendix A, “Patch Management Appendix,” on page 179

Audience

This guide is intended for ZENworks administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Additional Documentation

ZENworks 11 SP4 is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. See the [ZENworks 11 SP4 documentation Web site \(http://www.novell.com/documentation/zenworks114\)](http://www.novell.com/documentation/zenworks114).

1 What's New in ZENworks 11 SP4 Update 2

The following sections describe the new features and enhancement in Novell ZENworks 11 SP4 Update 2:

- ♦ “SLES 12 Support” on page 9
- ♦ “Cached Patch Bundle Cleanup” on page 12
- ♦ “Performance Improvements” on page 12
- ♦ “Patch Policy Notification and Cancel Options” on page 13
- ♦ “New Patch Reports” on page 13

SLES 12 Support

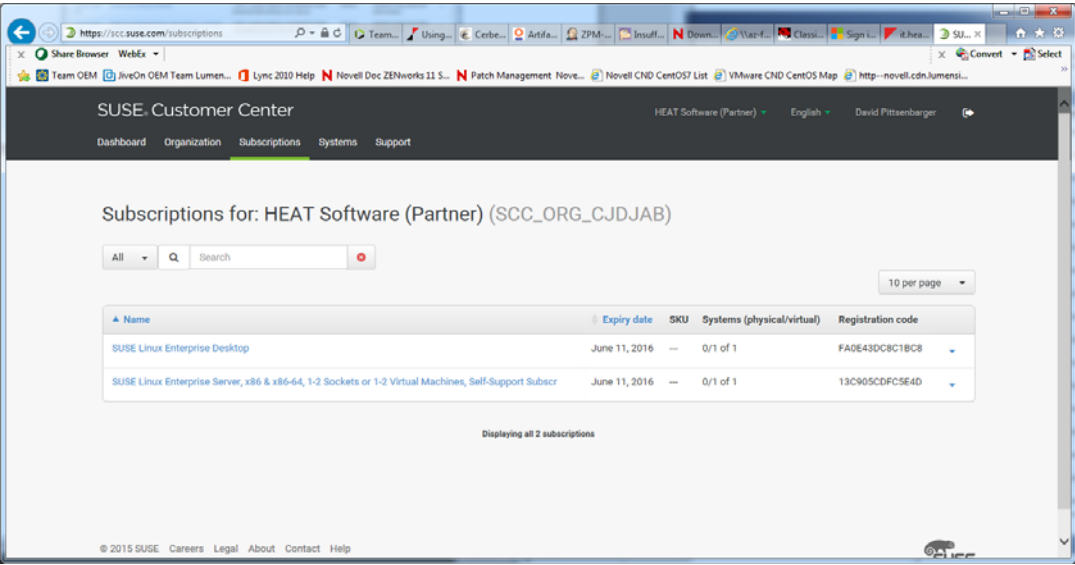
This release adds patch support for SUSE Linux Enterprise Server 12.

To patch these endpoints, register your endpoints using YaST, register them with SUSE Customer Center (<https://scc.suse.com/login>), and then add your Customer Center credentials to the **Subscription Service Settings**.

SLES 12 Support Instructions

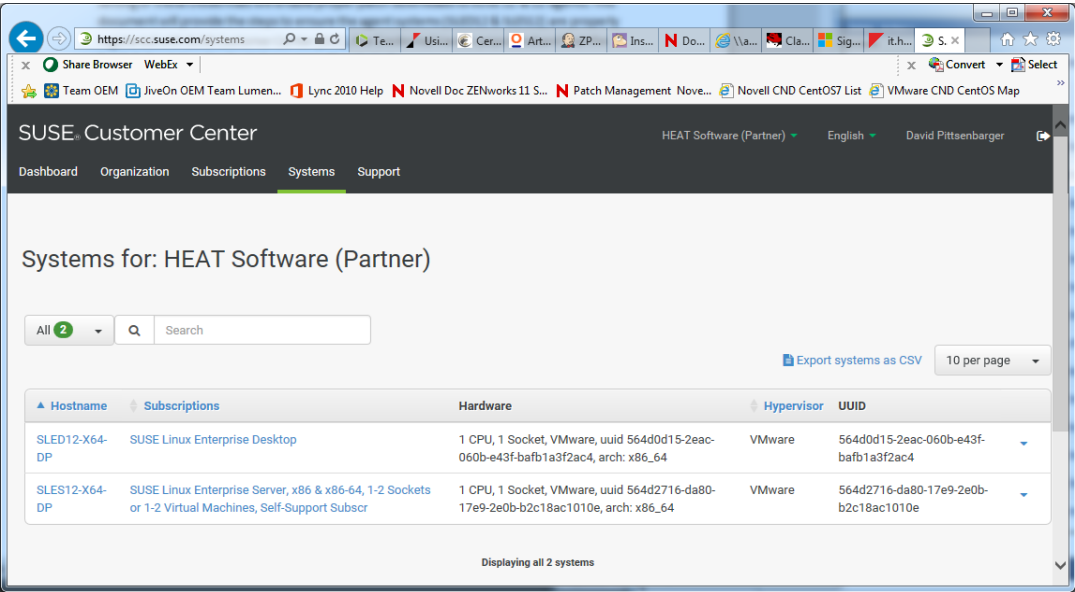
1. Confirm that SLES12 agent systems are registered with SUSE Customer Center (SCC) Configuration via the following steps:
 - a. On each system, launch YaST by selecting **Applications System Tools YaST**.
 - b. Next select **SUSE Customer Center Configuration** under **Support** settings.
 - c. If the system is currently registered with SCC, a “The system is already registered” message is displayed. Otherwise, enter the email address and Registration Code, which can be found by logging into (<https://scc.suse.com/login>) and selecting the **Subscriptions** (or **Systems**) menu option.

Figure 1-1 Registration Code



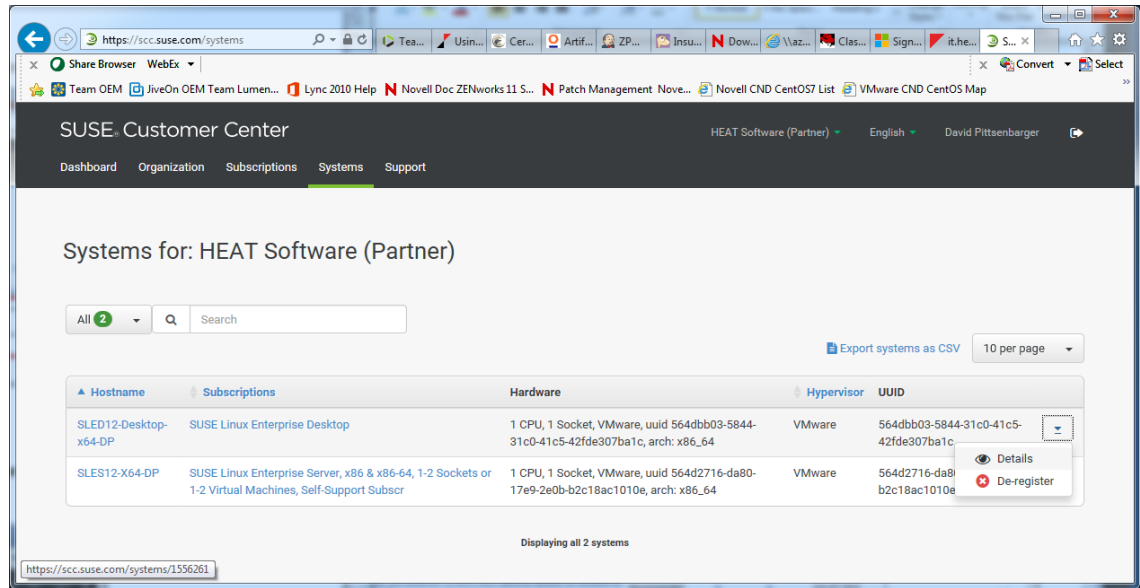
d. Now confirm the agent system is listed under the **Systems** menu.

Figure 1-2 Systems Menu



2. Copy the system credentials by selecting the **Details** drop-down option:

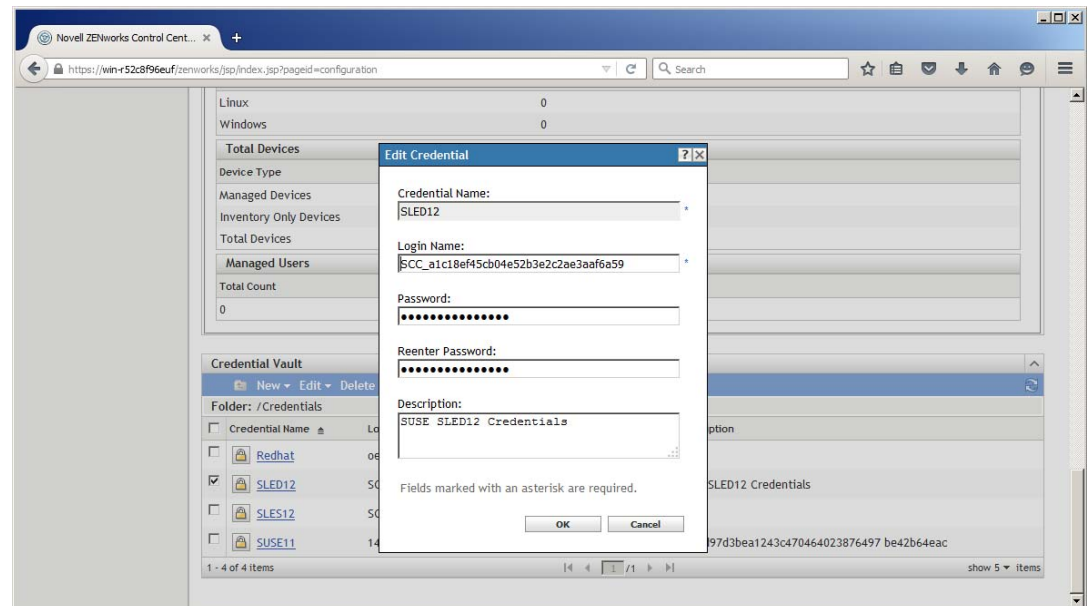
Figure 1-3 Detail Drop Down



NOTE: The SCC credentials will also be stored on the agent systems in the following folder: /etc/zypp/credentials.d/

- Navigate to **Credential Vault** on **Configuration** page and **Add** or **Edit** SLES 12 credentials using the copied systems credentials from SUSE Customer Center.

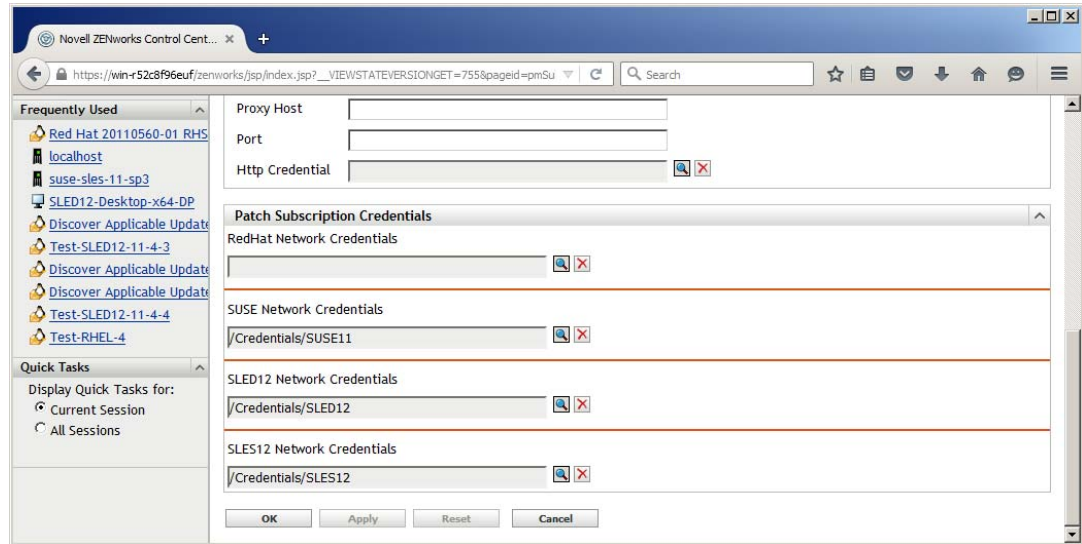
Figure 1-4 Edit Credentials



- If necessary, perform similar credential creation or modification for SLES from 11 using corresponding subscription credentials obtained through SUSE (prior to SCC – SUSE 12).

3. Navigate to **Subscription Service Settings** page via **Configuration Subscription Service Settings**.
 - a. Select each of the corresponding credentials defined in the **Credential Vault** under the **Patch Subscription Credentials** section. Example:

Figure 1-5 Patch Credentials



- b. Select **Apply** or **OK** button to commit the credentials per each distribution.

The patch subscription credentials are now set. Patch subscriptions and deployments can now be performed per all three agents.

Cached Patch Bundle Cleanup

ZENworks Patch Management now features an option that automatically deletes old patches for previous deployments. Use this feature to prevent cached patches from consuming excessive disk space on your server.

Performance Improvements

Performance improvements include pre-computed responses to speed up server performance and enhanced vulnerability detection to speed up client performance.

Pre-Computed Responses

When the number of patches within a given Patch Policy increases to a sizeable amount, the load on the ZENworks Server is high as it needs to cater to on-demand Patch Policy computation requests from every managed device. This in turn results in an increased response time between the ZENworks server and the managed device.

To address these issues, Patch Policies are now pre-computed, which eliminates the need for on-demand computation requests. These pre-computed responses are compressed and saved in the database. This reduces the size of the data transferred from the ZENworks server to the managed device, thereby improving the capability of the ZENworks server to apply patches on the managed device.

In order to benefit from this feature, this update has to be applied to the managed devices as well.

Enhanced Vulnerability Detection

Patch detections now complete more quickly due to some behind-the-scene improvements that increase the speed of patch detections.

Patch Policy Notification and Cancel Options

When configuring a patch policy deployment, you can now configure the deployment to notify users that a new patch policy is being applied to their workstation. Additionally, you can configure the patch policy to allow users to cancel application of the policy.

New Patch Reports

Five new reports are available for Patch Management in ZENworks 11 SP4 Update 2.

- ♦ **DAU Status:** Includes a pie chart that shows how many days since the Discover Applicable Updates (DAU) task was run on agents in the management zone (those greater than 7 days and those from 1-3 days).
- ♦ **Device Status:** Provides a date-time stamp by device name for the following status indicators: Last Contact Date, Last Full Refresh, Last Inventory Scan, and Last DAU.
- ♦ **Overall Patch Percentage:** Lists the total number of devices, Patched and Not Patched, with their respective percentages. The percentages are also reflected in a pie chart.
- ♦ **Patch Percentage by Folder:** Shows the number of devices patched and not patched in each folder with a percentage of those not patched.
- ♦ **Not-Patched Patches by Device:** Provides a table for each device in the management zone that shows patches that are not patched, to include patch names, release dates, impacts, and vendors.

NOTE: After updating or installing ZENworks 11.4.2, you will need to configure the ZENworks Reporting Appliance to have access to the new reports. See [Reconfiguring ZENworks Reporting](#) in the [ZENworks Reporting Appliance 5.6.1 Deployment and Administration Reference](#).

2 Patch Management Overview

Novell ZENworks 11 SP4 Patch Management is a part of the ZENworks 11 SP4 product line that provides a fully integrated version of leading patch and patch management solutions for medium and large enterprise networks. Patch Management enables customers to easily translate their organizational security patch policies into automated and continuous protection against more than 90% of vulnerabilities that threaten today's enterprise networks. By providing the most accurate and timely vulnerability assessment and patch management available, Patch Management ensures that policy measurement and security audits are a true representation of network security status.

- ♦ [“Product Overview” on page 15](#)
- ♦ [“Patch Management Process” on page 16](#)
- ♦ [“Features of Patch Management” on page 17](#)
- ♦ [“Supported ZENworks Server and Agent Environments” on page 18](#)

Product Overview

Patch Management is a fully integrated feature of the ZENworks 11 SP4 suite that provides the same agent-based patch, vulnerability patch, and compliance management solution that was used in prior stand-alone versions such as ZENworks Patch Management 6.4.

Patch Management provides rapid patch remediation, allowing you to proactively manage threats by automating the collection, analysis, and delivery of patches throughout your heterogeneous enterprise to secure end points.

The ZENworks Server has a Web-based management user interface known as ZENworks Control Center. Its Patch Management feature allows you to monitor and maintain patch compliance throughout the entire enterprise. The ZENworks 11 SP4 Primary Server can deploy a ZENworks Adaptive Agent on every client system in the target network, ensuring that all systems are protected with the latest security patches, software updates, and service packs.

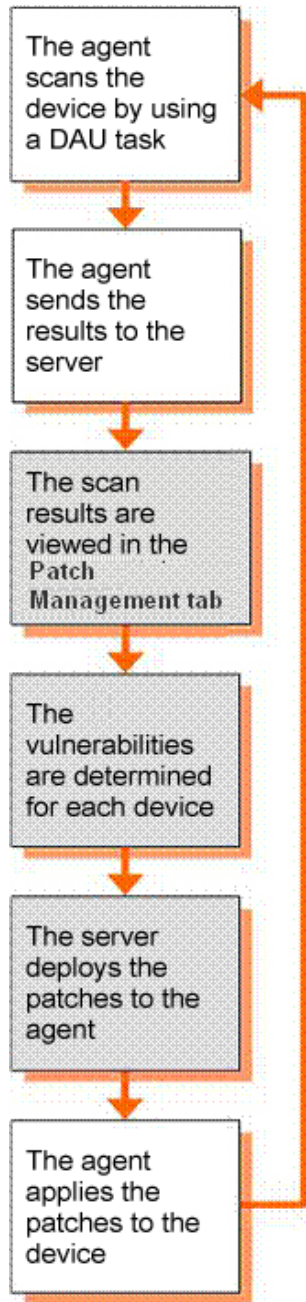
The Patch Management feature stays current with the latest patches and fixes by regular communication with the ZENworks Patch Subscription Network through a secure connection. After the initial 60-day free trial period, the Patch Management feature requires a paid subscription to continue its daily download of the latest patch and vulnerability information.

When a new patch is released into the ZENworks Patch Subscription Network, it is downloaded automatically to the ZENworks Server and an e-mail is sent to the administrator. When the administrator logs in to the ZENworks Control Center, the list of devices and the new patches that require deployment can easily be viewed along with the description and business impact. At this time, the administrator can choose to deploy the patch to a device or disregard the patch.

Patch Management Process

The following process map demonstrates how patch information is communicated between the ZENworks Server and the ZENworks Adaptive Agent:

Figure 2-1 Process Map



The patch detection cycle begins each day at the ZENworks Server where a Vulnerability Detection task is scheduled for all ZENworks managed devices (servers and workstations).

For all patches in the Vulnerability Detection task, the ZENworks Adaptive Agent performs patch detection by using the patch fingerprints incorporated into each individual patch, which determines the status (Patched, Not Patched, or Not Applicable) of that patch.

The results of the patch detection scan are sent to the ZENworks Server and can be viewed anytime in the Patches section under the **Patch Management** tab or in the **Devices** tab, even if a workstation is disconnected from your network.

After completion of the patch detection cycle, the ZENworks administrator can deploy the desired patches to each applicable device on the network.

Features of Patch Management

Patch Management has the world's largest repository of automated patches, including patches for all major operating systems and various third-party applications. Patch Management features an agent-based architecture, patch package pre-testing, highly scalable software, and easy-to-use features that allow customers to patch 13 times faster than the industry average.

Its patented Digital Fingerprinting Technology provides a highly accurate process for patch and vulnerability assessment, remediation and monitoring—leaving no systems open to attack. Remediation is fast and accurate with wizard-based patch deployments, support for phased rollouts, rapid verification of patch installations, and more. Patch Management continuously monitors end points to ensure that they achieve patch compliance quickly and then stay patched over time.

With Patch Management, you can be sure that your systems are effectively patched and compliant for successful IT and regulatory audits. Patch Management creates a Patch Fingerprint Profile that includes all missing patches for that machine, ensuring the continued compliance of each end point. Each end point is then continually monitored to make sure it stays patched. Administrators can also establish a mandatory baseline to automatically remediate end points that do not meet defined patch levels, which is a key aspect of regulatory compliance. In addition, because many organizations need to demonstrate patch compliance, Patch Management provides standard reports that document changes and demonstrate progress toward internal and external audit and compliance requirements.

The following table describes the important features of Patch Management:

Table 2-1 Patch Management Features

Feature	Description
Patented multi-platform patch management	Enables security of all operating systems and applications within heterogeneous networks, including Windows (32-bit and 64-bit) and Linux distributions. US Pat #6999660.
World's largest automated patch repository	Provides the largest repository of tested patches to support all major operating systems and applications used in the enterprise.
Extensive pre-testing	Reduces the amount of development and testing required prior to patch deployment.
Agent-based architecture	Protects laptop and mobile devices that are often disconnected from the network, and reduces network bandwidth usage.
Automatic notifications	Distributes e-mail alerts directly to administrators for proactive security and administrative management.
Patch fingerprint accuracy	Ensures the highest level of accuracy in the detection of security patches.

Feature	Description
Multi-patch deployments	Delivers multiple patches to multiple computers in one distribution to increase IT productivity.
Flexible application reporting	Audits and reports on the status of the organization's security.
Policy-based administration	Ensures that all systems meet a mandatory baseline policy, which is a key aspect of regulatory compliance.

Supported ZENworks Server and Agent Environments

Patch Management supports the following environments in which you can install the ZENworks Primary Server and Satellite Server software:

Table 2-2 *Supported Primary Server Environments*

Platform	Version
SUSE Linux Enterprise Server (SLES)	SLES 11 SP3 x86
	SLES 11 SP3 x86_64
	SLES 11 SP3 for VMware x86_64
	SLES 12 x86
	SLES 12 x86_64
	SLES 12 for VMware x86_64
Microsoft Windows Server	Windows Server 2008 SP2 Enterprise x86_64
	Windows Server 2008 SP2 Standard x86_64
	Windows Server 2008 R2 Standard x86_64
	Windows Server 2008 R2 Enterprise x86_64
	Windows Server 2008 R2 SP1 Standard x86_64
	Windows Server 2008 R2 SP1 Enterprise x86_64
	Windows Server 2008 R2 Datacenter x86_64
	Windows Server 2012 Foundation x86_64
	Windows Server 2012 Essential x86_64
	Windows Server 2012 Standard x86_64
	Windows Server 2012 Datacenter x86_64
	Windows Server 2012 R2 Foundation x86_64
	Windows Server 2012 R2 Essential x86_64
	Windows Server 2012 R2 Standard x86_64

Platform	Version
Red Hat Enterprise Linux (RHEL)	Windows Server 2012 R2 Datacenter x86_64
	Windows Server 2012 R2 Update 2 x86_64
	RHEL 5.8 x86_64
	RHEL 5.9 x86_64
	RHEL 5.10 x86_64
	RHEL 5.11 x86_64
	RHEL 6.1 x86_64
	RHEL 6.2 x86_64
	RHEL 6.3 x86_64
	RHEL 6.4 x86_64
	RHEL 6.5 x86_64
	RHEL 6.6 x86_64

Table 2-3 Supported ZENworks Satellite Server Environments

Platform	Version
Microsoft Windows Server	Windows Server 2008 SP2 Standard x86
	Windows Server 2008 SP2 Standard x86_64
	Windows Server 2008 SP2 Enterprise x86
	Windows Server 2008 SP Enterprise x86_64
	Windows Server 2008 R2 Standard x86
	Windows Server 2008 R2 Standard x86_64
	Windows Server 2008 R2 Enterprise x86_64
	Windows Server 2008 R2 SP1 Standard x86_64
	Windows Server 2008 R2 SP1 Enterprise x86_64
	Windows Server 2012 Foundation x86_64
	Windows Server 2012 Essential x86_64
	Windows Server 2012 Standard x86_64
	Windows Server 2012 Datacenter x86_64
	Windows Server 2012 R2 x86_64
	Windows Server 2012 R2 Update 2 x86_64
Microsoft Windows	Windows XP Professional SP3 x86
	Windows XP Tablet PC Edition SP3 x86
	Windows 7 x86 Enterprise

Platform	Version
	Windows 7 x86_64 Enterprise
	Windows 7 x86 Professional
	Windows 7 x86_64 Professional
	Windows 7 x86 Ultimate
	Windows 7 x86_64 Ultimate
	Windows 7 SP1 x86 Enterprise
	Windows 7 SP1 x86_64 Enterprise
	Windows 7 SP1 x86 Professional
	Windows 7 SP1 x86_64 Professional
	Windows 7 SP1 x86 Ultimate
	Windows 7 SP1 x86_64 Ultimate
	Windows 8 x86 Enterprise
	Windows 8 x86_64 Enterprise
	Windows 8 x86 Professional
	Windows 8 x86_64 Professional
	Windows Embedded POSReady 2009 (XP)
	Windows Embedded POSReady 7
	Windows 8.1 x86 Enterprise
	Windows 8.1 x86_64 Enterprise
	Windows 8.1 x86 Professional
	Windows 8.1 x86_64 Professional
	Windows 8.1 Update 2 x86 Enterprise
	Windows 8.1 Update 2 x86_64 Enterprise
	Windows 8.1 Update 2 x86 Professional
	Windows 8.1 Update 2 x86_64 Professional
	Windows 10 x86 Professional
	Windows 10 x86_64 Professional
	Windows 10 x86 Enterprise
	Windows 10 x86_64 Enterprise
	Windows 10 x86 Education
	Windows 10 x86_64 Education
	Windows 10 x86 Long Term Servicing Branch
	Windows 10 x86_64 Long Term Servicing Branch

Platform	Version
Macintosh OSX	10.7 x86
	10.7 x86_64
	10.8 x86
	10.8 x86_64
	10.9 x86
	10.9 x86_64
	10.10 x86
	10.10 x86_64
SUSE Linux Enterprise Desktop (SLED)	SLED 11 SP1 x86
	SLED 11 SP1 x86_64
	SLED 11 SP2 x86
	SLED 11 SP2 x86_64
	SLED 11 SP3 x86
	SLED 11 SP3 x86_64
SUSE Linux Enterprise Server (SLES)	SLES 10 SP3 x86
	SLES 10 SP3 x86_64
	SLES 10 SP4 x86
	SLES 10 SP4 x86_64
	SLES 11 SP1 x86
	SLES 11 SP1 x86_64
	SLES 11 SP2 x86
	SLES 11 SP2 x86_64
	SLES 11 SP2 x86 for VMware
	SLES 11 SP2 x86_64 for VMware
	SLES 11 SP3 x86
	SLES 11 SP3 x86_64 for VMware
	SLES 11 SP3 x86_64 for VMware
	SLES 12 x86
	SLES 12 x86_64
	SLES 12 x86_64 for VMware
Red Hat Enterprise Linux (RHEL)	RHEL 5.3 x86
	RHEL 5.3 x86_64
	RHEL 5.4 x86

Platform	Version
	RHEL 5.4 x86_64
	RHEL 5.5 x86
	RHEL 5.5 x86_64
	RHEL 5.6 x86
	RHEL 5.6 x86_64
	RHEL 5.7 x86
	RHEL 5.7 x86_64
	RHEL 5.8 x86
	RHEL 5.8 x86_64
	RHEL 5.9 x86
	RHEL 5.9 x86_64
	RHEL 5.10 x86
	RHEL 5.10 x86_64
	RHEL 5.11 x86
	RHEL 5.11 x86_64
	RHEL 6.0 x86
	RHEL 6.0 x86_64
	RHEL 6.1 x86
	RHEL 6.1 x86_64
	RHEL 6.2 x86
	RHEL 6.2 x86_64
	RHEL 6.3 x86
	RHEL 6.3 x86_64
	RHEL 6.4 x86
	RHEL 6.4 x86_64
	RHEL 6.5 x86
	RHEL 6.5 x86_64
	RHEL 6.6 x86
	RHEL 6.6 x86_64
Open Enterprise Server (OES)	OES 11 x86_64
	OES 11 SP1 x86_64
Scientific Linux (SL)	SL 6.5 x86_64
	SL 6.6 x86_64

The following environments support installation of the ZENworks agent:

Table 2-4 *Supported Agent Environments*

Platform	Version
Microsoft Windows Server	Windows Server 2008 SP2 Standard x86
	Windows Server 2008 SP2 Standard x86_64
	Windows Server 2008 SP2 Enterprise x86
	Windows Server 2008 SP Enterprise x86_64
	Windows Server 2008 R2 Standard x86
	Windows Server 2008 R2 Standard x86_64
	Windows Server 2008 R2 Enterprise x86_64
	Windows Server 2008 R2 SP1 Standard x86_64
	Windows Server 2008 R2 SP1 Enterprise x86_64
	Windows Server 2012 Foundation x86_64
	Windows Server 2012 Essential x86_64
	Windows Server 2012 Standard x86_64
	Windows Server 2012 Datacenter x86_64
	Windows Server 2012 R2 x86_64
	Windows Server 2012 R2 Update 2 x86_64
Microsoft Windows	Windows XP Professional SP3 x86
	Windows XP Tablet PC Edition SP3 x86
	Embedded XP SP3 x86
	Windows 7 x86 Enterprise
	Windows 7 x86_64 Enterprise
	Windows 7 x86 Professional
	Windows 7 x86_64 Professional
	Windows 7 x86 Ultimate
	Windows 7 x86_64 Ultimate
	Windows 7 SP1 x86 Enterprise
	Windows 7 SP1 x86_64 Enterprise
	Windows 7 SP1 x86 Professional
	Windows 7 SP1 x86_64 Professional
	Windows 7 SP1 x86 Ultimate
	Windows 7 SP1 x86_64 Ultimate
	Windows 8 x86 Enterprise

Platform	Version
	Windows 8 x86_64 Enterprise
	Windows 8 x86 Professional
	Windows 8 x86_64 Professional
	Windows Embedded POSReady 2009 (XP)
	Windows Embedded POSReady 7
	Windows 8.1 x86 Enterprise
	Windows 8.1 x86_64 Enterprise
	Windows 8.1 x86 Professional
	Windows 8.1 x86_64 Professional
	Windows 8.1 Update 2 x86 Enterprise
	Windows 8.1 Update 2 x86_64 Enterprise
	Windows 8.1 Update 2 x86 Professional
	Windows 8.1 Update 2 x86_64 Professional
	Windows 10 x86 Professional
	Windows 10 x86_64 Professional
	Windows 10 x86 Enterprise
	Windows 10 x86_64 Enterprise
	Windows 10 x86 Education
	Windows 10 x86_64 Education
	Windows 10 x86 Long Term Servicing Branch
	Windows 10 x86_64 Long Term Servicing Branch
Macintosh OSX	10.7 x86
	10.7 x86_64
	10.8 x86
	10.8 x86_64
	10.9 x86
	10.9 x86_64
	10.10 x86
	10.10 x86_64
SUSE Linux Enterprise Desktop (SLED)	SLED 11 SP1 x86
	SLED 11 SP1 x86_64
	SLED 11 SP2 x86
	SLED 11 SP2 x86_64

Platform	Version
SUSE Linux Enterprise Server (SLES)	SLED 11 SP3 x86
	SLED 11 SP3 x86_64
	SLES 10 SP3 x86
	SLES 10 SP3 x86_64
	SLES 10 SP4 x86
	SLES 10 SP4 x86_64
	SLES 11 SP1 x86
	SLES 11 SP1 x86_64
	SLES 11 SP2 x86
	SLES 11 SP2 x86_64
	SLES 11 SP2 x86 for VMware
	SLES 11 SP2 x86_64 for VMware
	SLES 11 SP3 x86
	SLES 11 SP3 x86_64 for VMware
	SLES 11 SP3 x86_64 for VMware
	SLES 12 x86
	SLES 12 x86_64
	SLES 12 x86_64 for VMware
Red Hat Enterprise Linux (RHEL)	RHEL 5.3 x86
	RHEL 5.3 x86_64
	RHEL 5.4 x86
	RHEL 5.4 x86_64
	RHEL 5.5 x86
	RHEL 5.5 x86_64
	RHEL 5.6 x86
	RHEL 5.6 x86_64
	RHEL 5.7 x86
	RHEL 5.7 x86_64
	RHEL 5.8 x86
	RHEL 5.8 x86_64
	RHEL 5.9 x86
	RHEL 5.9 x86_64
	RHEL 5.10 x86

Platform	Version
	RHEL 5.10 x86_64
	RHEL 5.11 x86
	RHEL 5.11 x86_64
	RHEL 6.0 x86
	RHEL 6.0 x86_64
	RHEL 6.1 x86
	RHEL 6.1 x86_64
	RHEL 6.2 x86
	RHEL 6.2 x86_64
	RHEL 6.3 x86
	RHEL 6.3 x86_64
	RHEL 6.4 x86
	RHEL 6.4 x86_64
	RHEL 6.5 x86
	RHEL 6.5 x86_64
	RHEL 6.6 x86
	RHEL 6.6 x86_64
Open Enterprise Server (OES)	OES 11 x86_64
	OES 11 SP1 x86_64
Scientific Linux (SL)	SL 6.5 x86_64
	SL 6.6 x86_64

For more details about supported platforms, see [ZENworks 11 SP4 System Requirements](#).

3 Getting Started with ZENworks 11 SP4 Update 2

Patch Management is a fully integrated feature of Novell ZENworks 11 SP4 Update 2 that provides the same agent-based patch, vulnerability patch, and compliance management solution that was used in prior versions.

The ZENworks Server schedules a Vulnerability Detection task for all ZENworks managed devices (servers and workstations) and compiles information on the operating system, hardware, and software.

The results of the scan are sent to the ZENworks Server and can be viewed anytime in the Patches section under the **Patch Management** tab or in the **Devices** tab even if a workstation is disconnected from your network.

Based on the above information, it is determined whether the patches are applicable for each device. If applicable, the ZENworks Adaptive Agent performs another scan by using the patch fingerprints incorporated into each patch to determine the device's patch status (Patched or Not Patched) in relation to that patch. The results of the scan are posted under the **Patch Management** tab of the ZENworks Control Center, for review by an administrator.

After patch status is established, the ZENworks administrator can deploy the desired patch to each applicable device on the network.

The following features are included in Patch Management:

- ♦ [“Downloading Patches” on page 27](#)
- ♦ [“Deploying a Patch” on page 27](#)
- ♦ [“Setting a Baseline” on page 28](#)
- ♦ [“Dashboard” on page 28](#)
- ♦ [“Patch Download Status” on page 29](#)
- ♦ [“Patch Wizard” on page 29](#)

Downloading Patches

Before you start downloading a patch, configure the downloading options in the **Configuration** tab. For more information, see [“Configuring Subscription Service Content Download Details” on page 39](#).

Deploying a Patch

To deploy a patch, you can use the Deploy Remediation Wizard. For more information, see [Chapter 6, “Using the Deploy Remediation Wizard,” on page 91](#).

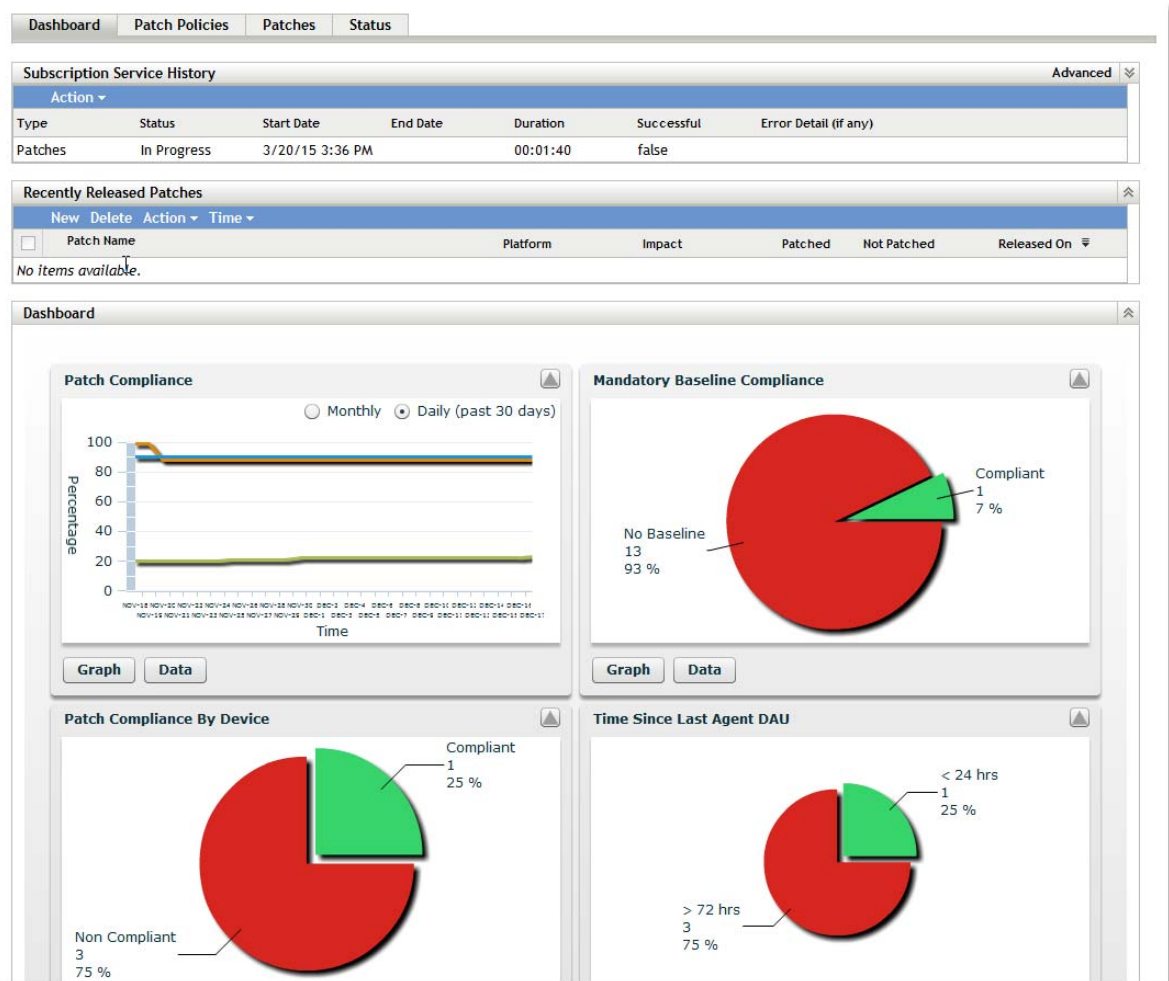
Setting a Baseline

To set a baseline, you must ensure that a group of devices is protected and that all the devices in the group are patched consistently. For more information, see [Chapter 7, “Using Mandatory Baselines,” on page 123](#).

Dashboard

The Dashboard tab contains graphs that allow users a direct overview of the devices in the network. For more information, see [“Dashboard” on page 68](#).

Figure 3-1 Dashboard Page



Patch Download Status

The Status page consists of the system and cache statuses, which show the overall patch information. For more information, see [“Status” on page 72](#).

Figure 3-2 Status Page

Dashboard	Patch Policies	Patches	Status
Status			
Name		Status	
Signature Download			
Last Signature Download Time			
Bundle Download		Complete	
Last Patch Download		Mar/30/2015 15:12:16	
Number of Failed Download(s)		0	
Number of Patches Queued for Caching		6	
Number of Active Patches		852	
Number of New Patches(less than 30 days)		166	
Latest Patch Released On		Mar/25/2015 00:00:00	
Cache Status			
Action ▾			
Name	Status ▲	Error Detail (if any)	
MS15-027 Security Update for Windows Server 2008 R2 x64 (KB3002657)	Caching	Downloading file (1 of 2) ... 0%	
MS15-020 Security Update for Windows Server 2008 R2 x64 (KB3039066)	Queued		
MS15-021 Security Update for Windows Server 2008 R2 x64 (KB3032323)	Queued		
MS15-028 Security Update for Windows Server 2008 R2 x64 (KB3030377)	Queued		
MS15-029 Security Update for Windows Server 2008 R2 x64 (KB3035126)	Queued		
MS15-031 Security Update for Windows Server 2008 R2 x64 (KB3046049)	Queued		
◀ ▶ 1 - 6 of 6 show 10 ▾ items			

Patch Wizard

The Patch Wizard allows you to create custom patches and add them to the Patch Management System. For more information, see [“Patch Creation” on page 79](#).

4 Using Patch Management

Novell ZENworks 11 SP4 Patch Management provides current information about your subscription status and allows you to activate and configure your subscription.

The following sections further introduce you to the capabilities of Patch Management:

- ♦ [“Viewing Subscription Service Information” on page 31](#)
- ♦ [“Configuring HTTP Proxy Detail” on page 33](#)
- ♦ [“Configuring Patch Subscription Credentials” on page 35](#)
- ♦ [“Configuring Subscription Service Content Download Details” on page 39](#)
- ♦ [“Configuring Email Notification Details” on page 43](#)
- ♦ [“Configuring Patch Dashboard and Trending Behavior” on page 45](#)
- ♦ [“Configuring the Schedule for Vulnerability Detections” on page 49](#)
- ♦ [“Vulnerability Detection Schedule: Set Vulnerability Detection at Folder Level” on page 58](#)
- ♦ [“Configuring Mandatory Baseline Settings” on page 60](#)
- ♦ [“Patch Management Licensing” on page 62](#)

Viewing Subscription Service Information

- 1 Click the **Configuration** tab in the left panel.

The Configuration page appears as shown in the following figure:

- 2 Click **Patch Management**.
- 3 Click the **Subscription Service Settings** link.

The Subscription Service Settings page appears, as shown in the following figure:

The Subscription Service Settings page displays includes: information about your the status of the subscription service. It also includes controls for configuring Patch Management for use through a proxy server and all the information about your subscription, including the status. You can also update your subscription settings on this page.

- ♦ Information about the status of the subscription service, as well as controls for starting it, resetting it, or changing the interval that it checks for subscription updates.
- ♦ An area for configuring Patch Management for use with a proxy server.
- ♦ An area for entering credentials used to download Linux patch content subscriptions.

The following table describes each status item featured in Subscription Service Settings:

SubscriptionN Service Setting	Definition
Start the Subscription Service	<p>Enables you to select a server from multiple servers in your management zone. You select a server from the drop-down list and click the Start button to start the subscription service.</p> <ul style="list-style-type: none"> ♦ After the subscription service starts running, the Start button reads Service Running. ♦ If there are multiple ZENworks Servers in your management zone, you can select any one of them to be the Patch Management Server. <p>The Patch Management Server selected will download new patches and updates daily, so it should have good connectivity to the Internet.</p> <p>NOTE: Selecting the Patch Management Server can be done only once per zone in this release.</p>
Last Subscription Poll	The date and time of the last successful update.

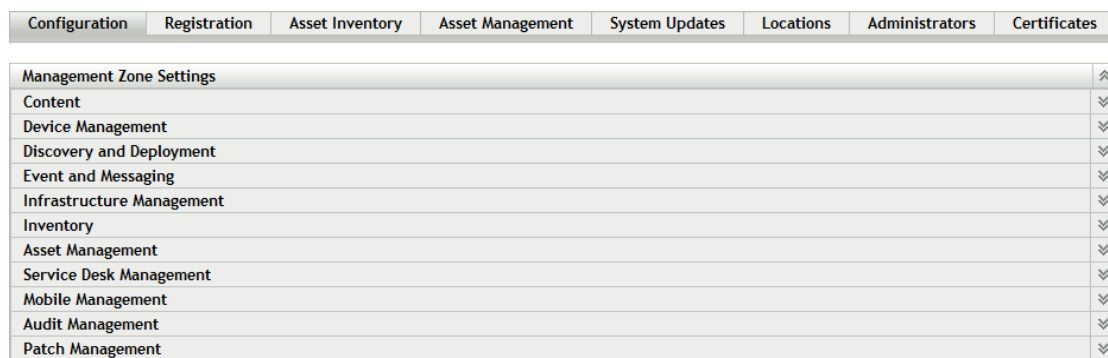
Subscription Service Setting	Definition
Subscription Replication Status	The latest status of the process of patch subscription replication.
Subscription Host	The DNS name of the Patch Management licensing server (http://novell.patchlink.com) .
Subscription Communication Interval (Every Day at)	The time at which the ZENworks Server will communicate with the ZENworks Patch Subscription Network to retrieve new patches and updates.
Reset ZENworks Patch Management Settings	Enables you to set all Patch Management settings, including deployments, back to the default state.
Reset Subscription Service	Restarts the subscription service.

The following table describes the action of each button on the page:

Button	Action
OK	Enables you to go back to the Configuration page.
Apply	Enables you to save the changes made to the Subscription Communication Interval.
Reset	Enables you to reset the replication status and initiate a complete replication with the ZENworks Patch Subscription Network.
Update Now	Initiates replication of the ZENworks Server with the ZENworks Patch Subscription Network and forces an immediate download of the patch subscription.
Cancel	Enables you to cancel the last action performed.

Configuring HTTP Proxy Detail

- 1 Click the **Configuration** tab in the left panel to display the Configuration page:



- 2 Click **Patch Management** to display the seven links (Subscription Service Settings, Subscription Service Content Download, Email Notification, Dashboard and Trending, Vulnerability Detection Schedule, Patch Policy Settings, Mandatory Baseline Settings):

Configuration	Registration	Asset Inventory	Asset Management	System Updates	Locations	Administrators	Certificates
Management Zone Settings							
Content							
Device Management							
Discovery and Deployment							
Event and Messaging							
Infrastructure Management							
Inventory							
Asset Management							
Service Desk Management							
Mobile Management							
Audit Management							
Patch Management							
Category		Description					
Subscription Service Settings		ZPM server with any HTTP proxy and 3rd party subscription settings					
Subscription Service Content Download		Patch subscription content download settings					
Email Notification		Email notifications to be delivered when new patches are discovered					
Dashboard and Trending		Configure patch dashboard and trending behavior					
Vulnerability Detection Schedule		Update vulnerability data and detection schedule					
Patch Policy Settings		Distribution and execution of patch policies					
Mandatory Baseline Settings		Set global values for how mandatory baseline installs will behave					

- 3 Click the **Subscription Service Settings** link. The Subscription Service Settings page appears:

[Configuration](#) > Subscription Service Settings

Subscription Service Settings

ZPM server with any HTTP proxy and 3rd party subscription settings

Subscription Service Settings

Start the Subscription Service

/Devices/Servers/az-tp-win2008r2

Service Running

Last Subscription Poll

3/31/15 12:00 AM

Subscription Replication Status

Complete

Subscription Host

novell.patchlink.com

Subscription Communication Interval(Every Day at)

00:00

Update Now

Reset ZENworks Patch Management Settings

Reset Subscription Service

HTTP Proxy Server Details

Proxy Host

Port

Http Credential

Patch Subscription Credentials

RedHat Network Credentials

SUSE Network Credentials

OK

Apply

Reset

Cancel

The Subscription Service Settings page enables you to configure an HTTP proxy for access to Internet patch subscriptions. The HTTP proxy server allows Patch Management to download the subscription service over the Internet.

The following table describes each HTTP Proxy Server Details field on the Subscription Service Settings page:

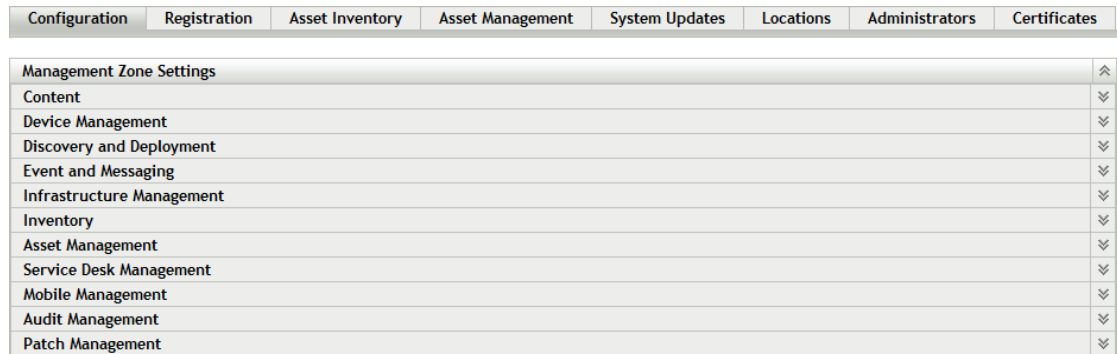
HTTP Proxy Server Detail	Definition
Proxy Host	The name or IP address of the proxy server.
Port	The port number that the proxy uses to route communication.
Http Credential	Credentials used to authenticate with the proxy, if required.

The following table describes the action of each button on the page:

Button	Action
OK	Enables you to go back to the Configuration page.
Apply	Enables you to save the data entered in the text fields.
Reset	Enables you to reset the data entered in the text fields.
Cancel	Enables you to cancel the last action performed.

Configuring Patch Subscription Credentials

- 1 Click the **Configuration** tab in the left panel to display the Configuration page:



- 2 Click **Patch Management** to display the seven links (Subscription Service Settings, Subscription Service Content Download, Email Notification, Dashboard and Trending, Vulnerability Detection Schedule, Patch Policy Settings, Mandatory Baseline Settings):

Configuration	Registration	Asset Inventory	Asset Management	System Updates	Locations	Administrators	Certificates
Management Zone Settings							
Content							
Device Management							
Discovery and Deployment							
Event and Messaging							
Infrastructure Management							
Inventory							
Asset Management							
Service Desk Management							
Mobile Management							
Audit Management							
Patch Management							
Category	Description						
Subscription Service Settings	ZPM server with any HTTP proxy and 3rd party subscription settings						
Subscription Service Content Download	Patch subscription content download settings						
Email Notification	Email notifications to be delivered when new patches are discovered						
Dashboard and Trending	Configure patch dashboard and trending behavior						
Vulnerability Detection Schedule	Update vulnerability data and detection schedule						
Patch Policy Settings	Distribution and execution of patch policies						
Mandatory Baseline Settings	Set global values for how mandatory baseline installs will behave						

- 3 Click the **Subscription Service Settings** link. The Subscription Service Settings page appears.

[Configuration](#) > Subscription Service Settings

Subscription Service Settings

ZPM server with any HTTP proxy and 3rd party subscription settings

Start the Subscription Service /Devices/Servers/az-tp-win2008r2 Service Running

Last Subscription Poll 3/31/15 12:00 AM

Subscription Replication Status Complete

Subscription Host novell.patchlink.com



Subscription Communication Interval(Every Day at) 00:00 Update Now

[Reset ZENworks Patch Management Settings](#) [Reset Subscription Service](#)



HTTP Proxy Server Details



Proxy Host

Port

Http Credential  

Patch Subscription Credentials


RedHat Network Credentials  

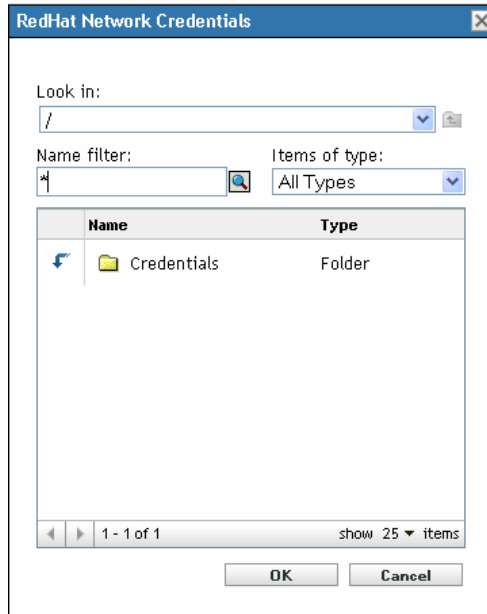
SUSE Network Credentials  

OK Apply Reset Cancel

The Subscription Service Settings page allows you to specify the network credentials associated with Linux subscription providers such as Red Hat and SUSE. Credentials are stored in the Credential Vault and are used by actions and tasks that require authentication to access a particular resource. If you do not specify the patch subscription credentials, you cannot successfully download and install patches for your Red Hat and SUSE servers and agents.

To configure the credentials for a subscription provider:

- 1 Click  next to the provider whose credentials you want to specify. The following window appears:



- 2 Click the arrow next to the **Credentials** option to display the list of available credentials for that subscription provider.

Operating System	Description
RedHat Network Credentials	Credentials that authenticate with the RedHat network.
SUSE Network Credentials	Credentials that authenticate with SUSE Customer Center for SUSE 11.
SLED12 Network Credentials	Credentials that authenticate with SUSE Customer Center for SUSE Linux Enterprise Desktop 12.
SLES12 Network Credentials	Credentials that authenticate with SUSE Customer Center for SUSE Linux Enterprise Server 12.

- 3 Click the desired credential. Click **OK** to confirm credential selection.

The window closes and the Subscription Service Settings page displays the selection.

The Subscription Service Settings page also contains the following buttons:

Button	Action
OK	Takes you back to the Configuration page.
Apply	Saves the changes made to the page.
Reset	Resets the selected options.
Cancel	Cancels the last action.

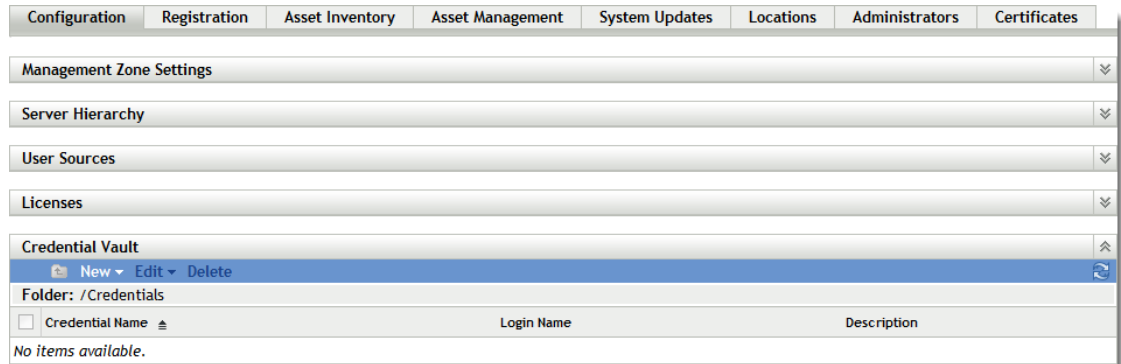
Adding a Credential

The Credential Vault stores the credentials used by Novell ZENworks 11 SP4 actions and tasks that require authentication to access a particular resource.

For example, if you want to create a third-party Imaging bundle by using the image files stored in a shared-network image repository that requires authentication, you can add a credential that includes the login name and password for the repository in the credential vault. During the creation of the third-party Imaging bundle, you can specify the credential name to access the repository.

You can use ZENworks Control Center to add credentials to the Credential Vault as follows:

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



- 2 In the Credential Vault panel, click **New > Credential** to display the Add Credential dialog box.

The screenshot shows the 'Add Credential' dialog box. It has a title bar with a question mark and a close button. The dialog contains five input fields: 'Credential Name:', 'Login Name:', 'Password:', 'Reenter Password:', and 'Description:'. The 'Credential Name:', 'Login Name:', and 'Password:' fields have an asterisk next to them, indicating they are required. The 'Description:' field has a small up/down arrow next to it. Below the fields is a note: 'Fields marked with an asterisk are required.' At the bottom are 'OK' and 'Cancel' buttons.

- 3 Fill in the fields.

If you need help, click the **Help** button.

Configuring Subscription Service Content Download Details

- 1 Click the **Configuration** tab in the left panel to display the Configuration page:

Configuration	Registration	Asset Inventory	Asset Management	System Updates	Locations	Administrators	Certificates
Management Zone Settings							
Content							⌵
Device Management							⌵
Discovery and Deployment							⌵
Event and Messaging							⌵
Infrastructure Management							⌵
Inventory							⌵
Asset Management							⌵
Service Desk Management							⌵
Mobile Management							⌵
Audit Management							⌵
Patch Management							⌵

- 2 Click **Patch Management** to display the seven links (Subscription Service Settings, Subscription Service Content Download, Email Notification, Dashboard and Trending, Vulnerability Detection Schedule, Patch Policy Settings, Mandatory Baseline Settings):

Configuration	Registration	Asset Inventory	Asset Management	System Updates	Locations	Administrators	Certificates
Management Zone Settings							
Content							⌵
Device Management							⌵
Discovery and Deployment							⌵
Event and Messaging							⌵
Infrastructure Management							⌵
Inventory							⌵
Asset Management							⌵
Service Desk Management							⌵
Mobile Management							⌵
Audit Management							⌵
Patch Management							⌵
Category							
Description							
Subscription Service Settings		ZPM server with any HTTP proxy and 3rd party subscription settings					
Subscription Service Content Download		Patch subscription content download settings					
Email Notification		Email notifications to be delivered when new patches are discovered					
Dashboard and Trending		Configure patch dashboard and trending behavior					
Vulnerability Detection Schedule		Update vulnerability data and detection schedule					
Patch Policy Settings		Distribution and execution of patch policies					
Mandatory Baseline Settings		Set global values for how mandatory baseline installs will behave					

3 Click the **Subscription Service Content Download** link to display the Subscription Service Content Download page:

The screenshot shows a configuration window titled "Subscription Service Content Download" with a subtitle "Patch subscription content download settings". The window is divided into several sections with orange borders:

- Select the platforms to download:** Includes checkboxes for Windows (checked), Linux, and Mac.
- RPM dependency:** Includes a note "Note: This option is performance intensive." and a checkbox for "Resolve all RPM dependencies".
- Choose your language options for Windows operating systems:** Includes a note "These languages are for Operating Systems prior to Vista and other third party patches. For the best performance results select only the languages used by your organization." and a grid of checkboxes for various languages: English (checked), Japanese, Spanish, Danish, Portuguese (Portugal), Portuguese (Brazil), Korean, Dutch, Hungarian, French, Traditional Chinese, Swedish, Norwegian, Italian, Simplified Chinese, Russian, German, Hong Kong Chinese, Czech, and Polish.
- Select the option below to combine all languages into each Patch Detection assignment. (Not Recommended):** Includes a checkbox for "Mix Multiple Languages".
- Specify whether to use a secure channel when communicating with the Patch Subscription:** Includes a checked checkbox for "SSL".
- Specify whether patch bundle content will automatically replicate to other servers:** Includes checkboxes for "Cache patch bundles to satellite servers" and "Cache patch bundles to primary servers".
- Download location for patch content:** Includes radio buttons for "ZPM directory" (selected) and "Bundle content directory".
- Select the option below to enable not applicable patches. This may significantly decrease performance for systems with a large number of devices.** Includes a checked checkbox for "Enable not applicable patches".
- Use local cache for faster Patch Detection results (NOTE: workstation users must not have access to ZENworks agent directory):** Includes a checked checkbox for "Enable PD caching".
- Select vendors to use in the system.** Includes a note "Note: All new patches from vendors not selected will be disabled." and radio buttons for "All" (selected) and "Selected". Below are checkboxes for various vendors: 7-Zip.org, Audacity Team, The, Foxit Corporation, Martin Prikryl, Novell, Inc., Riverbed Technology, TeamViewer, VMware, Inc., Yahoo! Inc., Adobe Systems, Inc., Citrix Systems, Inc., Google Inc., McAfee, Inc., Oracle Corporation, Skype, Tim Kosse, VideoLAN, dotPDN LLC, Apache Software Foundation, Document Foundation, The, Inkscape Team, The, Microsoft Corp., PatchLink Corporation, Sophos, Trend Micro, VlnZip Computing Inc., Apple, Don Ho, Lightning UK!, Mozilla, RealNetworks, Inc., Sun Microsystems, UltraVNC, VlnZip Computing, S.L., Apple Inc., F-Secure, Macromedia, Symantec Corporation, RealVNC Ltd., Viresearch Foundation, and VMware.
- When building a patch policy use only the applicable patches in the system. Note: Any new patches will not be rebuilt into the policy until at least one device has determined it is applicable:** Includes a checked checkbox for "Patch Policy uses only applicable patches".
- Patch feed filtering:** Includes checkboxes for "Disable legacy patches that were updated with a newly issued duplicate patch", "Disable obsolete security patches", "Detect only the current supported Service Packs", and "Disable older patches by age". Below are dropdown menus for "OS Vendor" and "Third Party Vendor" for "Critical", "Recommended", and "Software Installers" categories. The "Disable patches for specific cultures" section includes checked checkboxes for "United Kingdom English" and "South African English".

At the bottom of the window are buttons for "OK", "Apply", "Reset", and "Cancel".

The Subscription Service Content Download Options page allows you to configure the subscription download options for the Patch Management Server. You can select the languages that are used within your network to ensure that you only download the patches that are most

applicable for your organization. The next time patch replication occurs, only those patches specific to the selected languages are downloaded, thereby saving download time and disk space on your Patch Management Server.

NOTE: Novell does not recommend selecting all languages because each language can represent hundreds of patches. Downloading unnecessary languages can result in thousands of unused patch definitions within your ZENworks Primary Server database that would then need to be disabled in the **Patch Management** tab.

EXPECTED RESULTS: From version ZCM 11.1 onwards, the administrators are allowed to select the Primary servers that should receive the patch bundles compared to the forced rollout to all servers in prior releases.

The following table describes each option on the Subscription Download Options page:

Item	Description
Select the platforms to download	Enables you to select the operating system platform for which you want to download patches. For example, if you select the Windows check box, only Windows patches are downloaded.
RPM Dependency	This Option will be enabled ONLY when the LINUX platform is selected. Selecting this check box will download all the root level dependencies that will be necessary to resolve any vulnerabilities.
Choose Windows your language options	Enables you to select the language of patches you want to download. For example, if you select the French check box, only French language patches are downloaded.
Mix Multiple Languages	Enables you to combine all languages into each Patch Detection Assignment (not recommended).
SSL	Enables you to turn secured downloading on or off.
Cache patch bundles to satellite servers	Enables you to cache patch bundles to the servers or workstations that are managed by primary servers.
Cache patch bundles to primary servers	Enables you to cache patch bundles to primary servers only.
Download location for patch content	<p>By default all the patches will be downloaded to the ZPM directory which is enabled, but, if necessary, select the radio button for Bundle content directory to download it there.</p> <ul style="list-style-type: none">♦ ZPM directory: Downloads patch content to installpath\zenworks\zpm (Windows) or /var/opt/Novell/zenworks/zpm (Linux)♦ Bundle content directory: Downloads patch content to installationpath\zenworks\work\content-repo (Windows) or /var/opt/Novell/zenworks/content-repo (Linux)
Enable not applicable patches	Enables patches that aren't applicable to your enterprise. This option may slow performance if enabled.

Item	Description
Enable PD caching	Enables local cache for faster Patch Detection results, which eliminates the decryption and decompression of Vulnerability Detections. Only use this feature if you trust end users to stay out of the ZENWorks Agent directory, ideally, workstations users shouldn't have access to Zenworks agent directory.
Select vendors to use in the system	<p>Enables you to select the vendors to use in the system. By default it is ALL. For example, if you want to select the patches only for Novell not the rest available. Select the radio button Selected and then select the Novell check box, only Novell patches are downloaded.</p> <p>NOTE: This list of vendors will not be populated until the initial subscription update has completed.</p>
Patch Policy uses only applicable patches	Configures the system to only have applicable patches available for selection when building patch policies.
Patch feed filtering	Disables content within the system based on the criteria you select. These options are useful for filtering out obsolete content. ALL options are selected by default.
Enable clean up of content for disabled patches	<p>Deletes the patch listing and any cached bundles for that patch that meet the following conditions:</p> <ul style="list-style-type: none"> ♦ The patch is disabled. ♦ The patch has been disabled longer than the time duration selected from the drop-down. <p>NOTE: The bundles are not deleted until the next subscription update.</p>

IMPORTANT: Customers with larger network environments should select both **Cache Patch Bundles to Satellites** and **Cache Patch Bundles to Primary Servers** for optimal distribution of patches and the daily Discover Applicable Updates task within their environment. Not selecting these options could cause very slow and inefficient delivery of these patch bundles within a highly distributed WAN environment.

Within an enterprise network environment, the customer usually installs more than one ZENworks 11 SP4 Primary Server. Although only one of these servers can be used to download patches, every Primary Server has a cache of patch bundle content for distribution to the agents that are closest to it within the zone. Thus, when an agent wants to get a bundle, it can get the bundle directly from its closest Primary Server rather than the Primary Server where the patches were downloaded.

In addition, the satellites that are installed within the customer network can also serve as a cache for bundle content. If an agent is at a remote branch office with a satellite, it can get its content directly from the satellite rather than the Primary Server where patches were downloaded.

The following table describes the action of each button on the page:

Button	Action
OK	Enables you to go back to the Configuration page.
Apply	Enables you to save the changes made to the page.
Reset	Enables you to reset the selected options.
Cancel	Enables you to cancel the last action performed.

Best practices recommendations for using the patch subscription:

- ♦ Customers should always disable patches that they no longer require, because this minimizes the volume of patch scan data stored each day, as well as the time taken to scan each of the endpoint devices.
- ♦ We highly recommend that customers cache only the patches they need. When a patch is cached to the Primary Server where patches are downloaded, it needs to be copied to all Primary Servers and satellites within the zone. Downloading all patches wastes space and bandwidth within the ZENworks 11 SP4 content distribution network.

Configuring Email Notification Details

- 1 Click the **Configuration** tab in the left panel to display the Configuration page:

Configuration	Registration	Asset Inventory	Asset Management	System Updates	Locations	Administrators	Certificates
Management Zone Settings							
Content							
Device Management							
Discovery and Deployment							
Event and Messaging							
Infrastructure Management							
Inventory							
Asset Management							
Service Desk Management							
Mobile Management							
Audit Management							
Patch Management							

- Click **Patch Management** to display the seven links (Subscription Service Settings, Subscription Service Content Download, Email Notification, Dashboard and Trending, Vulnerability Detection Schedule, Patch Policy Settings, Mandatory Baseline Settings):

Configuration	Registration	Asset Inventory	Asset Management	System Updates	Locations	Administrators	Certificates
Management Zone Settings							
Content							⌵
Device Management							⌵
Discovery and Deployment							⌵
Event and Messaging							⌵
Infrastructure Management							⌵
Inventory							⌵
Asset Management							⌵
Service Desk Management							⌵
Mobile Management							⌵
Audit Management							⌵
Patch Management							⌵
Category	Description						
Subscription Service Settings	ZPM server with any HTTP proxy and 3rd party subscription settings						
Subscription Service Content Download	Patch subscription content download settings						
Email Notification	Email notifications to be delivered when new patches are discovered						
Dashboard and Trending	Configure patch dashboard and trending behavior						
Vulnerability Detection Schedule	Update vulnerability data and detection schedule						
Patch Policy Settings	Distribution and execution of patch policies						
Mandatory Baseline Settings	Set global values for how mandatory baseline installs will behave						

- Click the **Email Notification** link to open the Email Notification page.

[Configuration](#) > **Email Notification** ⌵

Email Notification
✕

Setup email notifications to be delivered when new patches are discovered.

Email Notification
⌵

Note: The SMTP settings are configured in the log settings section. Separate multiple email addresses with commas.

From:

To:

Cc:

The Email Notification page allows you to configure the email notification options when the Patch Management Server detects a new patch. You can decide which email address is used to send notifications as well as specify the recipients. The next time the Patch Management Server detects a patch, the recipients will receive an email informing them of the same.

The following table describes each option on the Email Notification page:

Item	Description
From	The email address the notification will be sent from.
To	The email address the notification will be sent to.
Cc	The email address the notification will be carbon-copied to.

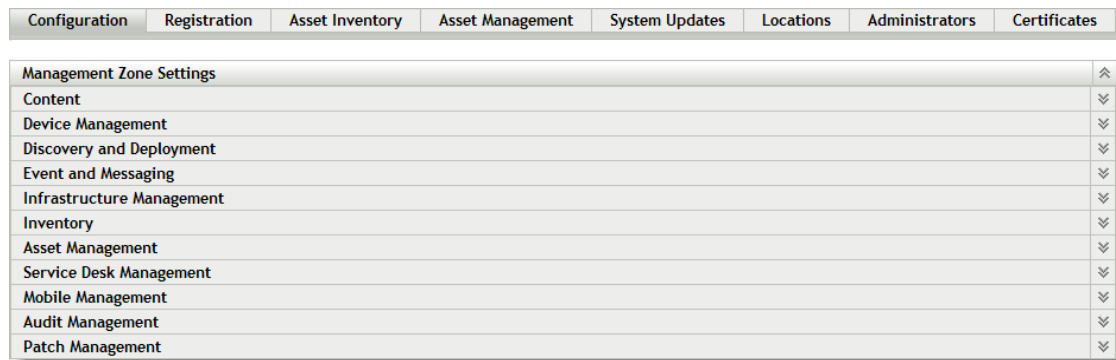
TIP: You can add multiple email addresses in the **To** and **Cc** fields. Separate each address with a comma.

The following table describes the action of each button on the page:

Button	Action
OK	Enables you to go back to the Configuration page.
Apply	Enables you to save the changes made to the page.
Reset	Enables you to reset the selected options.
Cancel	Enables you to cancel the last action performed.
Send test email	Enables you to send a test email. For more information, see “Configuring Email Notification Details” on page 43 .

Configuring Patch Dashboard and Trending Behavior

- 1 Click the **Configuration** tab in the left panel to display the Configuration page:



- 2 Click **Patch Management** to display the seven links (Subscription Service Settings, Subscription Service Content Download, Email Notification, Dashboard and Trending, Vulnerability Detection Schedule, Patch Policy Settings, Mandatory Baseline Settings):

Configuration	Registration	Asset Inventory	Asset Management	System Updates	Locations	Administrators	Certificates
Management Zone Settings							
Content							
Device Management							
Discovery and Deployment							
Event and Messaging							
Infrastructure Management							
Inventory							
Asset Management							
Service Desk Management							
Mobile Management							
Audit Management							
Patch Management							
Category		Description					
Subscription Service Settings		ZPM server with any HTTP proxy and 3rd party subscription settings					
Subscription Service Content Download		Patch subscription content download settings					
Email Notification		Email notifications to be delivered when new patches are discovered					
Dashboard and Trending		Configure patch dashboard and trending behavior					
Vulnerability Detection Schedule		Update vulnerability data and detection schedule					
Patch Policy Settings		Distribution and execution of patch policies					
Mandatory Baseline Settings		Set global values for how mandatory baseline installs will behave					

- 3 Click the **Dashboard and Trending** link to open the Dashboard and Trending page.

Dashboard and Trending

Configure patch dashboard and trending behavior

Dashboard and Trending

Days to store data in database 90

☐ Save patch status history (Warning: This can cause large database usage)

Impacts to include

☒ Critical

☐ Recommended

☐ Informational

☐ Software Installer

The Dashboard and Trending page allows you to configure the Patch Dashboard and trending behavior for the Patch Management Server, according to the patch impact status. You can decide the time when the Dashboard receives daily updates. This page also enables you to specify the number of days the Patch Management Server database stores Dashboard and Trending information.

The following table describes each option on the Dashboard and Trending page:

Item	Description
Dashboard and Trending	<p>Enables you to specify for how many days the database stores Dashboard information. This information is then used to create dashboard and graph information. If you want to turn off data collection for the dashboard, select 0 days.</p> <p>This section also includes a check box for saving a record of patch status history for every day in your database (this data is also used to show trends in the Patch Compliance dashboard graph). Enterprises with 10k+ nodes shouldn't use this option because when the data for all nodes and patches is saved, it can consume a large amount of your database very quickly.</p>
Impacts to include	<p>Lets you select the impact status of patches for which Dashboard information will be collected. Depending on the impacts you select, the Patch Compliance by Device Dashboard report will display the data.</p>
Custom Patch Agent Status report Filter time	<p>The interval at which the Patch Agent status report refilters itself.</p>
Dashboard Report Schedule	<p>The schedule by which the patch Dashboard retrieves updates. You can either choose the Default option (which will update the dashboard once daily) or Select a schedule to generate dashboard report (which lets you choose a custom schedule).</p>

If you want to turn off data collection for the dashboard, select 0 days in the **Days to store data** in database field.

The following table describes the action of each button on the page:

Button	Action
OK	Enables you to go back to the Configuration page.
Apply	Enables you to save the changes made to the page.
Reset	Enables you to reset the selected options.
Cancel	Enables you to cancel the last action performed.

Dashboard Report Schedule

☐ Default (Run once per day at time chosen by Patch Subscription Service).
 ☒ Select a schedule to generate dashboard report

Schedule Type:

Recurring

☒ When a device is refreshed

☐ Delay execution after refresh:

0

 Days

0

 Hours

0

 Minutes

☐ Days of the week

Sun	Mon	Tue	Wed	Thu	Fri	Sat
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Time:

1

 :

00

[More Options](#)

☐ Monthly

☒ Day of the month:

1

☐ Last day of the month
 ☐

First

Sunday

+

Start Time:

1

 :

00

[More Options](#)

☐ Fixed Interval

0

 Months

0

 Weeks

0

 Days

0

 Hours

0

 Minutes

Start Date:

9/26/2012

 Start Time:

1

 :

00

[More Options](#)

OK

Apply

Reset

Cancel

The Dashboard report can be scheduled in the same way as a Deployment. There are 3 ways to generate a schedule for the Dashboard Report

- ♦ Default: Selecting **Default** schedules the report at a time chosen by the Patch Subscription Service.
- ♦ Date Specific: Selecting **Date Specific** schedules the report according to the selected date. Further options can set the time and frequency of the report
- ♦ Recurring: Selecting **Recurring** schedules the report on the selected day at the selected time, and produces the report: On Refresh, Every day/week/month, and if defined, ends on a specific date. There are also options for producing the report on a Fixed Interval.

Configuring the Schedule for Vulnerability Detections

- 1 Click the **Configuration** tab in the left panel to display the Configuration page:

Configuration	Registration	Asset Inventory	Asset Management	System Updates	Locations	Administrators	Certificates
Management Zone Settings							
Content							⌵
Device Management							⌵
Discovery and Deployment							⌵
Event and Messaging							⌵
Infrastructure Management							⌵
Inventory							⌵
Asset Management							⌵
Service Desk Management							⌵
Mobile Management							⌵
Audit Management							⌵
Patch Management							⌵

- 2 Click **Patch Management** to display the seven links (Subscription Service Settings, Subscription Service Content Download, Email Notification, Dashboard and Trending, Vulnerability Detection Schedule, Patch Policy Settings, Mandatory Baseline Settings):

Configuration	Registration	Asset Inventory	Asset Management	System Updates	Locations	Administrators	Certificates
Management Zone Settings							
Content							⌵
Device Management							⌵
Discovery and Deployment							⌵
Event and Messaging							⌵
Infrastructure Management							⌵
Inventory							⌵
Asset Management							⌵
Service Desk Management							⌵
Mobile Management							⌵
Audit Management							⌵
Patch Management							⌵
Category							
Description							
Subscription Service Settings		ZPM server with any HTTP proxy and 3rd party subscription settings					
Subscription Service Content Download		Patch subscription content download settings					
Email Notification		Email notifications to be delivered when new patches are discovered					
Dashboard and Trending		Configure patch dashboard and trending behavior					
Vulnerability Detection Schedule		Update vulnerability data and detection schedule					
Patch Policy Settings		Distribution and execution of patch policies					
Mandatory Baseline Settings		Set global values for how mandatory baseline installs will behave					

- 3 Click the **Vulnerability Detection Schedule** link. The Vulnerability Detection Schedule page appears:

[Configuration](#) > Vulnerability Detection Schedule ⌵

Vulnerability Detection Schedule ✕

Update vulnerability data and detection schedule

Schedule Vulnerability Definition Content ⌵

☒ Distribute vulnerability definition before scan

☐ Distribute vulnerability definition content on a schedule

Schedule Type:
Date Specific ▼

Start Date(s): *

☐ Run event every year

☐ Process immediately if device unable to execute on schedule

Select when schedule execution should start:

☒ Start immediately at Start Time

☐ Start at a random time between Start and End Times

Start Time: 1 ▼ : 00 ▼ End Time: 1 ▼ : 00 ▼

☐ Use Coordinated Universal Time (Current UTC 4:25 PM)

Schedule Vulnerability Check ⌵

☒ Check for vulnerabilities on device refresh

☐ Check for vulnerabilities on a schedule

Schedule Type:
Date Specific ▼

Start Date(s): *

☐ Run event every year

☐ Process immediately if device unable to execute on schedule

Select when schedule execution should start:

☒ Start immediately at Start Time

☐ Start at a random time between Start and End Times

Start Time: 1 ▼ : 00 ▼ End Time: 1 ▼ : 00 ▼

☐ Use Coordinated Universal Time (Current UTC 4:25 PM)

OK

Apply

Reset

Cancel

The Vulnerability Detection Schedule page enables you to configure Vulnerability Detection schedules for the devices in your network. You can decide when to run the Vulnerability Detection on network devices as well as specify when to distribute bundle content through the Vulnerability Detection.

The following table describes the main options on the Vulnerability Detection Schedule page:

Item	Description
Run Vulnerability Detection on refresh	Lets you initiate Vulnerability Detection action when the Agents on the managed devices are refreshed.
Select a schedule to launch Vulnerability Detection on patch devices	Lets you specify a schedule when the Vulnerability Detection will run.
Distribute Vulnerability Detection on launch	Lets you deploy bundle content immediately.
Select a schedule to distribute the Vulnerability Detection content	Lets you specify a schedule when Vulnerability Detection bundles will be distributed to devices.

The following table describes the action of each button on the page:

Button	Action
OK	Enables you to go back to the Configuration page.
Apply	Enables you to save the data entered in the text fields.
Reset	Enables you to reset the data entered in the text fields.
Cancel	Enables you to cancel the last action performed.

If you decide to set a schedule for running the Vulnerability Detection and distributing bundle content, you will need to select a schedule type as follows:

Schedule Type:

Date Specific	▼
Date Specific	
Recurring	

Patch Management offers two types of schedules to determine when a Vulnerability Detection is run and bundle content is distributed.

- ♦ Select **Date Specific** to schedule the deployment to your selected devices according to the selected date.
- ♦ Select **Recurring** to start the deployment on the selected day at a selected time, repeat the deployment every day/week/month, and if defined, end on a specific date.

The following sections provide more information on schedule types:

- ♦ [“Vulnerability Detection Schedule: Date Specific” on page 52](#)
- ♦ [“Vulnerability Detection Schedule: Recurring” on page 53](#)

Vulnerability Detection Schedule: Date Specific

When you select **Date Specific**, the selected Vulnerability Detection Schedule section appears as shown in the following figure:

Figure 4-1 Vulnerability Detection Schedule Section for the Date Specific Schedule Type

Schedule Vulnerability Check

☐ Check for vulnerabilities on device refresh

☒ Check for vulnerabilities on a schedule

Schedule Type:
Date Specific

Start Date(s): *

☐ Run event every year

☐ Process immediately if device unable to execute on schedule

Select when schedule execution should start:

☒ Start immediately at Start Time

☐ Start at a random time between Start and End Times

Start Time: 1 : 00 End Time: 1 : 00

☐ Use Coordinated Universal Time (Current UTC 4:25 PM)

Use this page to set the following options:

- ♦ **Start Date:** Enables you to pick the date when you need to start the desired action. To do so, click the icon to open the calendar and pick the date. To remove the selected date, click the icon.
- ♦ **Run event every year:** Ensures that the desired action starts on a selected date at a selected time, repeats every year, and if defined, ends on a specific date.
- ♦ **Process immediately if device unable to execute on schedule:** Ensures that the desired action starts immediately if the device could not execute on the selected schedule.
- ♦ **Select when schedule execution should start:** There are two options to enable you to select the start time of the schedule execution namely:
 - ♦ **Start immediately at Start Time:** Deactivates the **End Time** panel and starts the action at the start time specified. In this option, you must set the start time in the **Start Time** panel:

Start Time: 1 : 00

- ♦ **Start at a random time between Start Time and End Times:** Activates the **End Time** panel next to the **Start Time** panel. You can specify the end time and the start time so that the action occurs at a random time between them. The **End Time** panel appears as follows:

End Time: 1 : 00

In both time panels, the first drop-down list enables you to select the hour, the second drop-down list enables you to select the minute, and the third drop-down list enables you to select **am** and **pm**.

Selecting the **Use Coordinated Universal Time** check box enables you to schedule the desired action at the same time, regardless of time zone differences. Coordinated Universal Time (UTC), also known as World Time, Z Time, or Zulu Time, is a standardized measurement of time that is not dependent upon the local time zone. Deselecting UTC schedules the distribution at the local time.

Vulnerability Detection Schedule: Recurring

When you select **Recurring**, the selected Vulnerability Detection Schedule section appears as shown in the following figure:

Figure 4-2 Vulnerability Detection Schedule Section for the Recurring Schedule Type

The screenshot shows a window titled "Schedule Vulnerability Check". At the top, there are two radio buttons: "Check for vulnerabilities on device refresh" (selected) and "Check for vulnerabilities on a schedule". Below these is a "Schedule Type:" dropdown menu set to "Recurring". The main content area is divided into four sections, each with a radio button:

- When a device is refreshed:** Includes a checkbox for "Delay execution after refresh:" followed by input fields for "0" Days, "0" Hours, and "0" Minutes.
- Days of the week:** Includes a row of checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, and Sat. Below this is a "Start Time:" dropdown set to "1" and a time dropdown set to ":00". A link "More Options" is present.
- Monthly:** Includes three radio buttons: "Day of the month:" (selected, with input "1"), "Last day of the month", and "First" (with a dropdown set to "Sunday" and a calendar icon). Below this is a "Start Time:" dropdown set to "1" and a time dropdown set to ":00". A link "More Options" is present.
- Fixed Interval:** Includes input fields for "0" Months, "0" Weeks, "0" Days, "0" Hours, and "0" Minutes. Below this is a "Start Date:" field set to "4/6/2015" and a "Start Time:" dropdown set to "1" and a time dropdown set to ":00". A link "More Options" is present.

In this page, you can set the following options for a recurring deployment:

- ♦ [“When a Device Is Refreshed” on page 54](#)
- ♦ [“Days of the Week” on page 55](#)
- ♦ [“Monthly” on page 56](#)
- ♦ [“Fixed Interval” on page 57](#)

When a Device Is Refreshed

This option enables you to schedule a recurring deployment whenever the device is refreshed. In this option, you can choose to delay the next deployment until after a specific time.

To set the delay, select the **Delay execution after refresh** check box as shown in the following image, and specify the days, hours, and minutes of the time to delay the deployment:

Figure 4-3 Delay Execution After Refresh Check Box

A screenshot of a user interface element. It features a checked checkbox labeled "Delay execution after refresh:". To the right of the checkbox are three input fields for time delay: "0" Days, "0" Hours, and "0" Minutes. The entire element is set against a light blue background.☒ Delay execution after refresh: Days Hours Minutes

NOTE: The device is refreshed based on the settings in the **Device Management** tab under the **Configuration** tab. Click the **Device Refresh Schedule** link under the **Device Management** tab to open the page displaying the option for either a **Manual Refresh** or **Timed Refresh**. Alternatively, you can refresh the device by selecting a device under the **Devices** tab and clicking the **Refresh Device** option under the **Quick Tasks** menu.

Days of the Week

This option enables you to schedule the deployment on selected days of the week:

Figure 4-4 Weekly Options - Default

Days of the week

*

Sun	Mon	Tue	Wed	Thu	Fri	Sat
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Time: :

[More Options](#)

- ♦ To set the day of deployment, select the **Days of the week** button, select the required day of the week, and set the start time of deployment.

If you click the **More Options** link, additional deployment options appear as shown in the following figure. Click the **Hide Options** link to hide the additional deployment options and show only the default deployment options:

Days of the week

*

Sun	Mon	Tue	Wed	Thu	Fri	Sat
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Time: :

[Hide Options](#)

☐ Process immediately if device unable to execute on schedule

☐ Use Coordinated Universal Time (Current UTC 8:19 AM)

☐ Start at a random time between Start and End Times

End Time: :


☐ Restrict schedule execution to the following date range:

Start Date:

End Date:

Selecting the **Use Coordinated Universal Time** check box enables you to schedule the deployment of all devices at the same time, regardless of time zone differences. Coordinated Universal Time (UTC), also known as World Time, Z Time, or Zulu Time, is a standardized measurement of time that is not dependent upon the local time zone. Deselecting UTC schedules the distribution at local time.

Selecting the **Start at a random time between Start Time and End Times** check box activates the **End Time** panel in addition to the **Start Time** panel. You can specify the end time and the start time so that the deployment occurs at any random time between the start and end times.

The **Restrict schedule execution to the following date range** option enables you to schedule a recurring deployment at the selected time, repeat the deployment on the days specified, and, if defined, end at the specific time. This option also enables you to restrict the deployment to the period between the start date and the end date. To set this option, select the **Restrict schedule execution to the following date range** check box and click the  icon to open the calendar and pick a start date or end date. Click the **Close** button when you have finished selecting the date.

Monthly

This option enables you to specify the monthly deployment options:

Figure 4-5 Monthly Options – Default

☒ Monthly

☒ Day of the month:


☐ Last day of the month


☐ 

Start Time: :


[More Options](#)

- ◆ In the **Monthly** deployment option, you can specify the following:
 - ◆ **Days of the month:** Enables you to schedule the deployment on a specific day of the month. You can specify any number between 1 and 31.
 - ◆ **Last day of the month:** Enables you to schedule the deployment on the last day of the month.
 - ◆ **Particular days of the month:** Enables you to schedule the deployment on specific days of every month. The valid options for the day are first, second, third, fourth, and fifth. The valid options for the weekday are Sunday through Saturday. To select one particular day of the month, use the drop-down arrows. An example is shown as follows.

☒ 

To select an additional day of the month, click the  icon and use the drop-down arrows in the second row shown as follows.

☒ 
 

NOTE: To remove a particular day from the list, click the  icon.

If you click the **More Options** link, additional deployment options appear as shown in the following figure. Clicking the **Hide Options** link hides the additional deployment options and shows only the default deployment options:

Monthly

☒ Day of the month:

☐ Last day of the month

☐ First

Start Time: :

[Hide Options](#)

☐ Process immediately if device unable to execute on schedule

☐ Use Coordinated Universal Time (Current UTC 8:19 AM)

☐ Start at a random time between Start and End Times

End Time: :

☒ Restrict schedule execution to the following date range:

Start Date:

End Date:

NOTE: The **Restrict schedule execution to the following date range** option enables you to schedule a recurring deployment at the selected time, repeat the deployment on the days specified, and, if defined, end on the specific time. This option also enables you to restrict the deployment to the period between the **Start Date** and the **End Date**. To set this option, select the **Restrict schedule execution to the following date range** check box and click the icon to open the calendar and pick a start date or end date. Click the **Close** button when you have finished selecting the date.

Fixed Interval

This option enables you to schedule a recurring deployment that runs after a fixed duration on a regular basis. You can choose the number of months, weeks, days, hours, and minutes of the interval and the start date for the deployment schedule, as shown in the following figure:

Figure 4-6 Fixed Interval Deployment Options - Default

Fixed Interval

Months Weeks Days Hours Minutes

Start Date: Start Time: :

[More Options](#)

If you click the **More Options** link, additional deployment options appear as shown in the following figure. Clicking the **Hide Options** link hides the additional deployment options and shows only the default deployment options:

Figure 4-7 Fixed Interval Options - All

Fixed Interval

Months
 Weeks
 Days
 Hours
 Minutes

Start Date:
 Start Time: :

[Hide Options](#)

☐ Process immediately if device unable to execute on schedule
☐ Use Coordinated Universal Time
☐ Restrict schedule execution to the following date range:

End Date:
 End Time: : (Current UTC 8:19 AM)

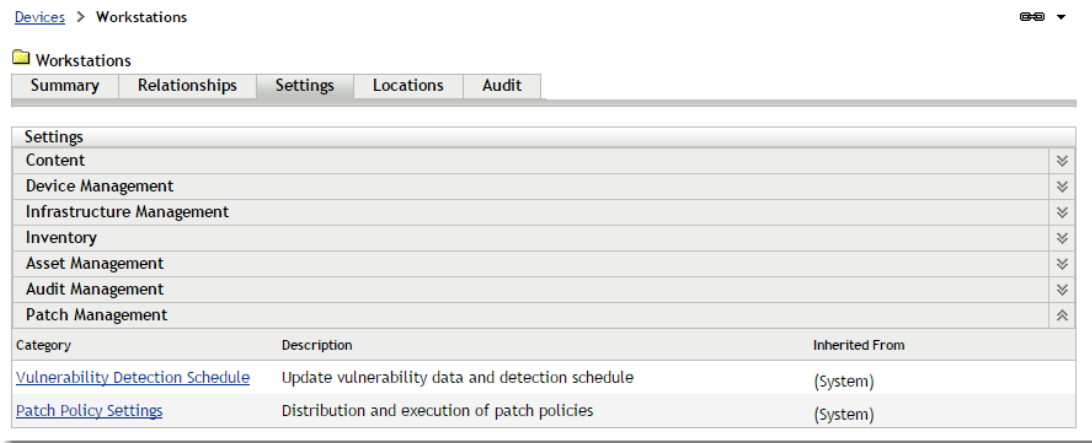
Vulnerability Detection Schedule: Set Vulnerability Detection at Folder Level

The Vulnerability Detection schedule can be set at folder level which enables you to set the deployment options for Vulnerability Detection for the Server or Workstation estate. This means that the System settings (configured in the Configuration tab) can be overridden.

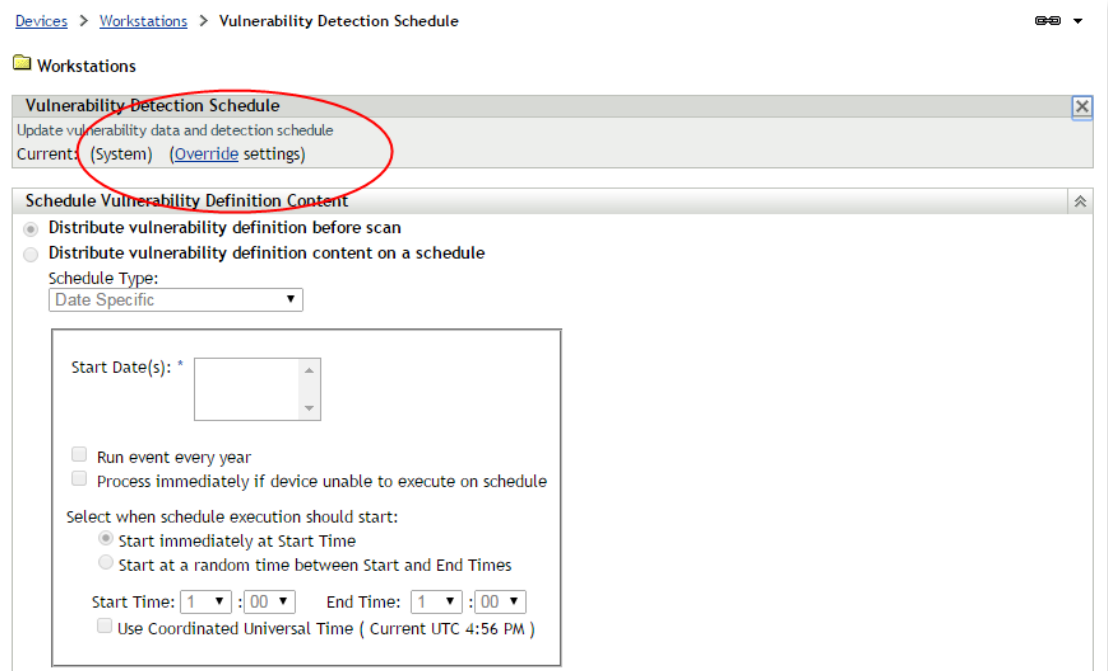
- 1 Click the Devices tab in the left panel to display the Devices page. This will present a choice between Servers and Workstations.

The screenshot shows the ZENworks 11 SP4 Patch Management interface. At the top, there are tabs for 'Discovered', 'Inventoried', and 'Managed'. Below these, the 'Devices' tab is selected, displaying a table with columns 'Name' and 'Type'. The table lists two folders: 'Servers (Details)' and 'Workstations (Details)'. To the right of the table is a search panel with various filters: 'Name', 'Type' (set to 'All Types'), 'Operating System' (set to 'Any'), 'Test Status' (set to 'Any'), 'Message Status' (set to 'Any'), 'Compliance Status' (set to 'Any'), and 'Device State' (set to 'Any'). There are 'Search' and 'Reset' buttons at the bottom of the search panel.

- 2 Choose the Devices that you want to set a schedule for and click on the Details link. Then select the Settings tab. This will present two options for scheduling Install and Distribution. Select which schedule you would like to change.



- 3 At the top of the page there is an option to Override the System settings, select this to begin making changes. This option can be used to revert to System settings if you need to change back.



- 4 Select your desired schedule for the Vulnerability Detection, as described in the previous section.

Workstations

Vulnerability Detection Schedule

Update vulnerability data and detection schedule
 Current: /Devices/Workstations
[Revert the settings to: \(System\)](#)

Schedule Vulnerability Definition Content

☒ Distribute vulnerability definition before scan
☐ Distribute vulnerability definition content on a schedule

Schedule Type:
 Date Specific

Start Date(s): *

☐ Run event every year
☐ Process immediately if device unable to execute on schedule

Select when schedule execution should start:

☒ Start immediately at Start Time
☐ Start at a random time between Start and End Times

Start Time: 1 :00 End Time: 1 :00
☐ Use Coordinated Universal Time (Current UTC 4:58 PM)

NOTE: These settings will override the System settings, as selected from the configuration tab. To switch back follow the instructions in Step 3.

Configuring Mandatory Baseline Settings

- 1 Click the **Configuration** tab in the left panel to display the Configuration page:

Configuration	Registration	Asset Inventory	Asset Management	System Updates	Locations	Administrators	Certificates
Management Zone Settings							
Content							
Device Management							
Discovery and Deployment							
Event and Messaging							
Infrastructure Management							
Inventory							
Asset Management							
Service Desk Management							
Mobile Management							
Audit Management							
Patch Management							

- Click **Patch Management** to display the seven links (Subscription Service Settings, Subscription Service Content Download, Email Notification, Dashboard and Trending, Vulnerability Detection Schedule, Patch Policy Settings, Mandatory Baseline Settings):

Configuration	Registration	Asset Inventory	Asset Management	System Updates	Locations	Administrators	Certificates
Management Zone Settings							
Content							⌵
Device Management							⌵
Discovery and Deployment							⌵
Event and Messaging							⌵
Infrastructure Management							⌵
Inventory							⌵
Asset Management							⌵
Service Desk Management							⌵
Mobile Management							⌵
Audit Management							⌵
Patch Management							⌵
Category	Description						
Subscription Service Settings	ZPM server with any HTTP proxy and 3rd party subscription settings						
Subscription Service Content Download	Patch subscription content download settings						
Email Notification	Email notifications to be delivered when new patches are discovered						
Dashboard and Trending	Configure patch dashboard and trending behavior						
Vulnerability Detection Schedule	Update vulnerability data and detection schedule						
Patch Policy Settings	Distribution and execution of patch policies						
Mandatory Baseline Settings	Set global values for how mandatory baseline installs will behave						

- Click the **Mandatory Baseline Settings** link to open the Mandatory Baseline Settings page.

Mandatory Baseline Settings
Set global values for how mandatory baseline installs will behave

Mandatory Baseline Settings

- ☒ Use default reboot and deployment behavior
- ☐ Modify mandatory baseline reboot and deployment behavior

Description Text

To complete the installation of mandatory patches on your computer, it is now necessary to reboot. If you require any additional information, please contact your Novell ZENworks Patch Management administrator.

Options

	Yes	No
Suppress reboot	<input type="radio"/>	<input checked="" type="radio"/>
Allow user to cancel	<input checked="" type="radio"/>	<input type="radio"/>
Allow user to snooze	<input checked="" type="radio"/>	<input type="radio"/>
Snooze interval	<input type="text" value="10"/>	Minutes ▾
Reboot within	<input type="text" value="2"/>	Hours ▾

Show tray notification
☒

Tray notification duration
 Seconds ▾

Tray notification text

Important patches have been installed. In order for these patches to be applied a reboot is required. Please click here to reboot now.

The Mandatory Baseline Settings page allows you to completely control deployment of mandatory baseline patches. For example, you can decide whether or not to automatically reboot the machine when a baseline patch is applied. The page also enables you to set global options for installation of mandatory baseline patches.

The page displays the following options:

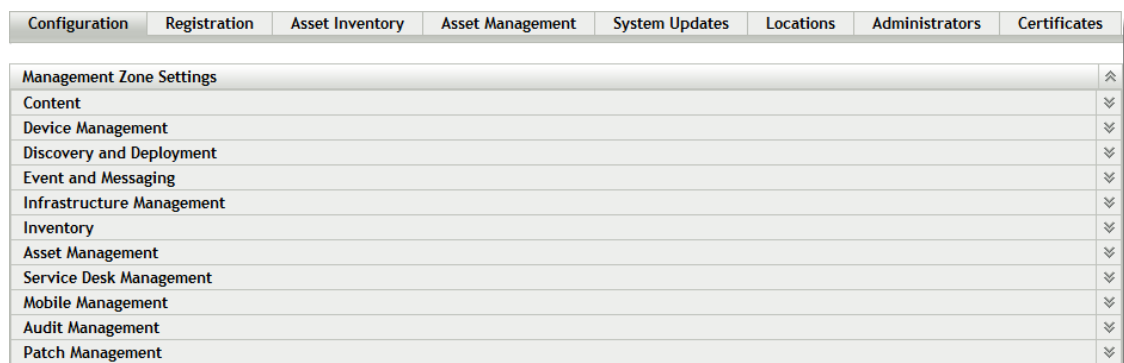
- ♦ **Use default reboot and deployment behavior:** Uses the default mandatory baseline default reboot and deployment behavior.
- ♦ **Modify mandatory baseline reboot and deployment behavior:** Allows you to use customized mandatory baseline reboot and deployment behaviors. After you select this option, the options below become available.
 - ♦ **Description text:** The text of the notification message.
 - ♦ **Options:** When you define auto reboot options, you can specify whether to use the values in the default settings or the custom settings. There are four options:
 - ♦ **Suppress Reboot:** Allows the user to prevent rebooting after installation of a patch.
 - ♦ **Allow user to cancel:** Allows the user to cancel the reboot process.
 - ♦ **Allow user to snooze:** Allows the user to delay the reboot.
 - ♦ **Snooze Interval:** Sets the amount of time before the reboot is delayed before the user is prompted to reboot again.
 - ♦ **Reboot Within:** Sets the amount of time before the user is forced to reboot.
 - ♦ **Show tray notification:** Enables a pop-up window in the system tray that notifies users of a pending reboot.
 - ♦ **Tray notification duration:** The amount of time the tray notification is displayed before it dismisses itself.
 - ♦ **Tray notification text:** The text displayed in the tray notification.

The page also contains the following buttons:

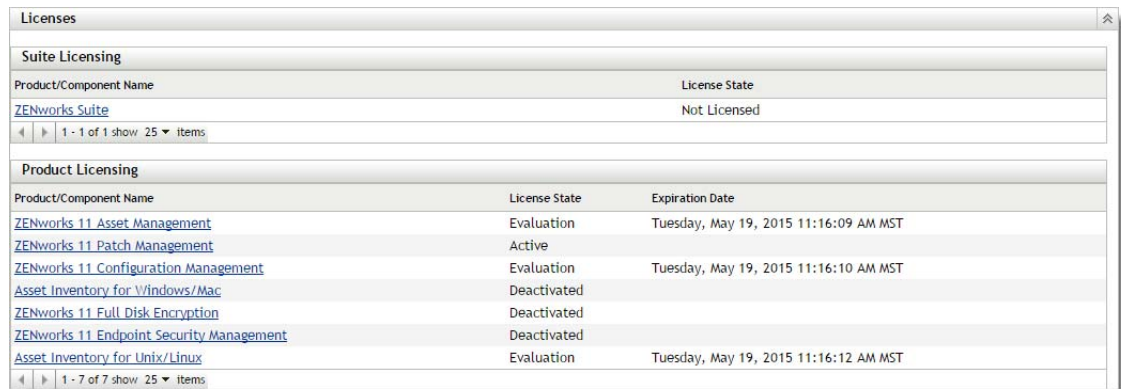
Button	Action
OK	Takes you back to the Configuration page.
Apply	Saves the changes made to the page.
Reset	Resets the selected options.
Cancel	Cancels the last action.

Patch Management Licensing

- 1 Click the **Configuration** tab in the left panel to display the Configuration page:



2 If necessary, expand the **Licenses** section:



The screenshot shows a window titled "Licenses" with two main sections: "Suite Licensing" and "Product Licensing".

Suite Licensing

Product/Component Name	License State
ZENworks Suite	Not Licensed

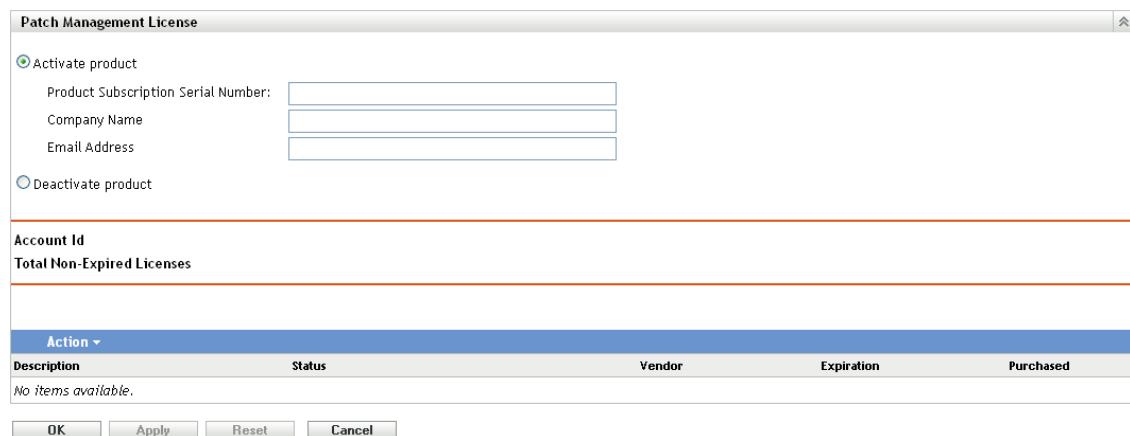
1 - 1 of 1 show 25 items

Product Licensing

Product/Component Name	License State	Expiration Date
ZENworks 11 Asset Management	Evaluation	Tuesday, May 19, 2015 11:16:09 AM MST
ZENworks 11 Patch Management	Active	
ZENworks 11 Configuration Management	Evaluation	Tuesday, May 19, 2015 11:16:10 AM MST
Asset Inventory for Windows/Mac	Deactivated	
ZENworks 11 Full Disk Encryption	Deactivated	
ZENworks 11 Endpoint Security Management	Deactivated	
Asset Inventory for Unix/Linux	Evaluation	Tuesday, May 19, 2015 11:16:12 AM MST

1 - 7 of 7 show 25 items

3 Click **ZENworks 11 Patch Management**.



The screenshot shows the "Patch Management License" dialog box. It has two radio buttons: "Activate product" (selected) and "Deactivate product".

Product Subscription Serial Number:

Company Name:

Email Address:

Account Id

Total Non-Expired Licenses

Action ▼

Description	Status	Vendor	Expiration	Purchased
No items available.				

OK Apply Reset Cancel

The Patch Management License page allows you to view and verify the patch management subscription for the ZENworks Primary Server. The page also allows you to activate or renew your paid subscription if it has expired, and provides a summary of all subscription elements that are part of your patch management activities. This information is updated after each replication with the Patch Management Subscription Service.

IMPORTANT: If you are upgrading from a prior version of Patch Management, you can use your existing Patch Management subscription serial number after your Patch Management 10.1 server has been uninstalled.

Patch Management offers the following licenses:

Table 4-1 Patch Management Licenses

License Type	Description
Trial	Denotes trial access to all features of Patch Management for 60 days.
Extended Trial	Denotes continued access to some Patch Management features after the initial 60-day trial, up to 12 months since ZENworks service is installed.
Valid	Denotes a valid subscription license.
Trial Expired	Denotes that the initial 60-day trial period or the extended trial period has ended, depending on the license in use earlier.
License Expired	Denotes expiry of the current Patch Management license.

Depending on the type of license you use, Patch Management functions are enabled as follows:

- ♦ **Trial:** All Patch Management capabilities are free to use.
- ♦ **Extended Trial:** During this license period, only Windows devices have Patch Management support. You can only download new patches released by Microsoft and run Vulnerability Detection for those patches. Patches that were cached previously will have their content cleared so you cannot deploy them. Other features disabled are patch caching, remediation, generation of reports, and the ability to set mandatory baseline patches. In addition, a message appears, asking you to purchase a Patch Management license.
- ♦ **Valid:** All Patch Management functions are available.
- ♦ **Trial Expired:** After the trial ends, the Server will not download any new patches. All Patch Management functionalities are disabled and you will receive a message asking you to purchase a Patch Management license.
- ♦ **License Expired:** After the license expires, the Server will not download any new patches. However, you can continue to use all Patch Management features on the patches downloaded prior to license expiry.

Patch Management provides a 60-day free trial period. You do not need to enter a serial number unless you have purchased the product or the 60-day free trial has expired.

To continue using the patch management features of the ZENworks Control Center after your 60-day free trial has ended:

- 1 Enter a valid subscription serial number for Patch Management along with the company name and e-mail address.
- 2 Revalidate the subscription serial number.

The license record is now valid, and displays its description, purchase date, vendor, effective date, and expiration date.

To validate the serial number and obtain the authorization to download patches, the Primary Server on which patch subscription is being downloaded must have port 443 (HTTPS) access to <https://novell.patchlink.com/update>.

The Patch Management content distribution network is a global cache infrastructure with many servers. Downloading patches from this network requires port 80 (HTTP) access to <http://novell.cdn.lumension.com/novell/baretta.xml>. For security reasons, it is also recommended that SSL access to the internet should be allowed. The **SSL** option is enabled by default and downloads the lists of patches from a secure and trusted site.

You should use nslookup to discover the local IP address for your nearest content distribution node. The content distribution network has over 40,000 cache distribution servers worldwide, plus multiple redundant cache servers in each geographic location. It is important to allow access to a range of addresses through the firewall.

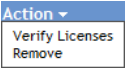
The following table describes each field on the Subscription Serial Number page:

Table 4-2 Patch Management License Items

Item	Definition
Activate product	Activates the patch management service. The Patch Management tab is restored in the main panel and the Patch Management section is restored in the Configuration panel.
Deactivate product	Deactivates the patch management service. The Patch Management tab is removed from the main panel and the Patch Management section is removed from the Configuration page.
Product Subscription Serial Number	Patch Management license number (serial number).
Company Name	Name of the company that Patch Management Service is registered to.
Email Address	E-mail address that you can use for receiving alerts and for future communications.
Account ID	Key created by the ZENworks Server, which is passed to the Patch Management Subscription Service and used to validate the update request.
Total Non-Expired Licenses	Total number of active licenses. Each registered device requires one license.
Description	The description of the license or the name of the license.
Status	Status of license verification. When verification begins, the status reads Initializing Verification . When replication ends, the status reads Completed .
Vendor	The source where the license was purchased.
Expiration	The date the licenses expire. Typically, licenses expire one calendar year from the date of purchase.
Purchased	The total number of licenses purchased with the product.

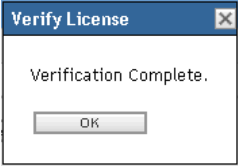
The Patch Management serial number can be entered only once. When you have entered the serial number, you can verify the license by clicking the **Action** drop-down list on the Patch Management License page and selecting **Verify License**. To start the license verification process, click **Apply**. Automatic verification of the license happens every day with the replication process.

Figure 4-8 Verify License option



To start the license verification process, click **Apply**.

Figure 4-9 Verify License message box



The **Verify License** message box indicates that the verification of the subscription license is complete or the license has expired.

NOTE: You can check the resultant license verification status under the **Subscription Service History** panel on the Subscription Service Information page. When verification begins, the status column reads **Initializing Verification**. When verification ends, the status column reads **Completed**. The **Successful** column indicates whether the verification was successful or not. **True** indicates successful verification and **False** indicates incomplete or failed verification.

The following table describes the action of each button on the Patch Management License page:

Table 4-3 Buttons on the Patch Management License Page

Button	Action
OK	Enables you to go back to the Configuration page.
Apply	Enables you to start the license verification process.
Reset	Enables you to reset the data entered in the text fields.
Cancel	Enables you to cancel the last action performed.

5 Using the Patch Management Tab

The Patch Management page is where the majority of Novell ZENworks 11 SP4 Patch Management activities are performed. This page lists all patches across all systems registered to the ZENworks Server. The page displays the name, description, impact, and statistics of the patches.

The following sections provide more information on the Patches page:

- ♦ [“Viewing Patches” on page 67](#)
- ♦ [“Dashboard” on page 68](#)
- ♦ [“Status” on page 72](#)
- ♦ [“Using the Patches Page” on page 73](#)
- ♦ [“Patch Management Reports” on page 88](#)

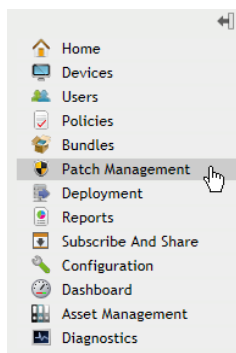
Viewing Patches

A patch consists of a description, signatures, and fingerprints required to determine whether the patch is applied or not patched. A patch also consists of associated patch bundles for deploying the patch.

The Patches page displays a complete list of all known patches reported by various software vendors. After they are reported and analyzed, the patches are registered for distribution to your ZENworks Server through the ZENworks Patch Subscription Network. The ZENworks Adaptive Agent should be installed on each device to check for known patches. A patch bundle called Vulnerability Detection is then assigned to run on each device on a daily basis to scan for known patches. This task returns the results that are displayed on the Patches page. The results are presented in a table of patch status. The total number of patches is displayed below the table in the bottom left corner.

To view the patches in Patch Management, click the **Patch Management** tab on the left panel, as shown in the following figure:

Figure 5-1 Patch Management Tab



The patches are displayed, as shown in the following figure:

Figure 5-2 Patches Listed on the Patches Page

Dashboard Patch Policies Patches Status					
Patches					
New Delete Action					
<input type="checkbox"/>	Patch Name	Impact	Patched	Not Patched	Released On
<input type="checkbox"/>	Update for Windows Server 2008 R2 x64 (KB2990214)	Recommended	0	1	Apr-14-2015
<input type="checkbox"/>	Windows Malicious Software Removal Tool - April 2015 (KB890830)	Software Installer	0	1	Apr-14-2015
<input type="checkbox"/>	MS15-032 Cumulative Security Update for Internet Explorer 8 for Windows Server 2008 R2 x64 (KB3038314)	Critical	0	1	Apr-14-2015
<input type="checkbox"/>	MS15-038 Security Update for Windows Server 2008 R2 x64 (KB3045999)	Critical	0	1	Apr-14-2015
<input type="checkbox"/>	MS15-041 Security Update for .NET Framework 4 on Win 2003, Vista, Win 7, Server 2008, Server 2008 R2 x64 (KB3037578)	Critical	0	1	Apr-14-2015
<input type="checkbox"/>	MS15-035 Security Update for Windows Server 2008 R2 x64 (KB3046306)	Critical	0	1	Apr-14-2015
<input type="checkbox"/>	Windows Malicious Software Removal Tool x64 - April 2015 (KB890830)	Software Installer	0	1	Apr-14-2015
<input type="checkbox"/>	MS15-038 Security Update for Windows Server 2008 R2 x64 (KB3045685)	Critical	0	1	Apr-14-2015
<input type="checkbox"/>	MS15-037 Security Update for Windows Server 2008 R2 x64 (KB3046269)	Critical	0	1	Apr-14-2015
<input type="checkbox"/>	MS15-034 Security Update for Windows Server 2008 R2 x64 (KB3042553)	Critical	0	1	Apr-14-2015
<input type="checkbox"/>	MS15-039 Security Update for Windows Server 2008 R2 x64 (KB3046482)	Critical	0	1	Apr-14-2015
<input type="checkbox"/>	MS15-041 Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 SP1 x64 (KB3037574)	Critical	0	1	Apr-14-2015
<input type="checkbox"/>	custom	Recommended	1	1	Apr-10-2015
<input type="checkbox"/>	Microsoft Skype Business 7.3.32.101 for Windows (See Notes)	Recommended	0	1	Apr-01-2015
<input type="checkbox"/>	MS15-023 Security Update for Windows Server 2008 R2 x64 (KB3034344)	Critical	0	1	Mar-10-2015
<input type="checkbox"/>	Update for Windows Server 2008 R2 x64 (KB3006137)	Recommended	0	1	Feb-24-2015
<input type="checkbox"/>	Update for Windows Server 2008 R2 x64 (KB3005788)	Recommended	0	1	Feb-10-2015
<input type="checkbox"/>	Security Update for Windows Server 2008 R2 x64 (KB3004375)	Critical	0	1	Feb-10-2015
<input type="checkbox"/>	MS15-011 Security Update for Windows Server 2008 R2 x64 (KB3000483)	Critical	0	1	Feb-10-2015

Search
Patch Name
Search Reset
Status
☐ Patched
☒ Not Patched
☐ Not Applicable
☐ Include Disabled
Impact
☒ Critical
☒ Recommended
☒ Informational
☒ Software Installers
Platform:
Windows
Vendor:
All
Cache Status:
All
CVE Identifier:

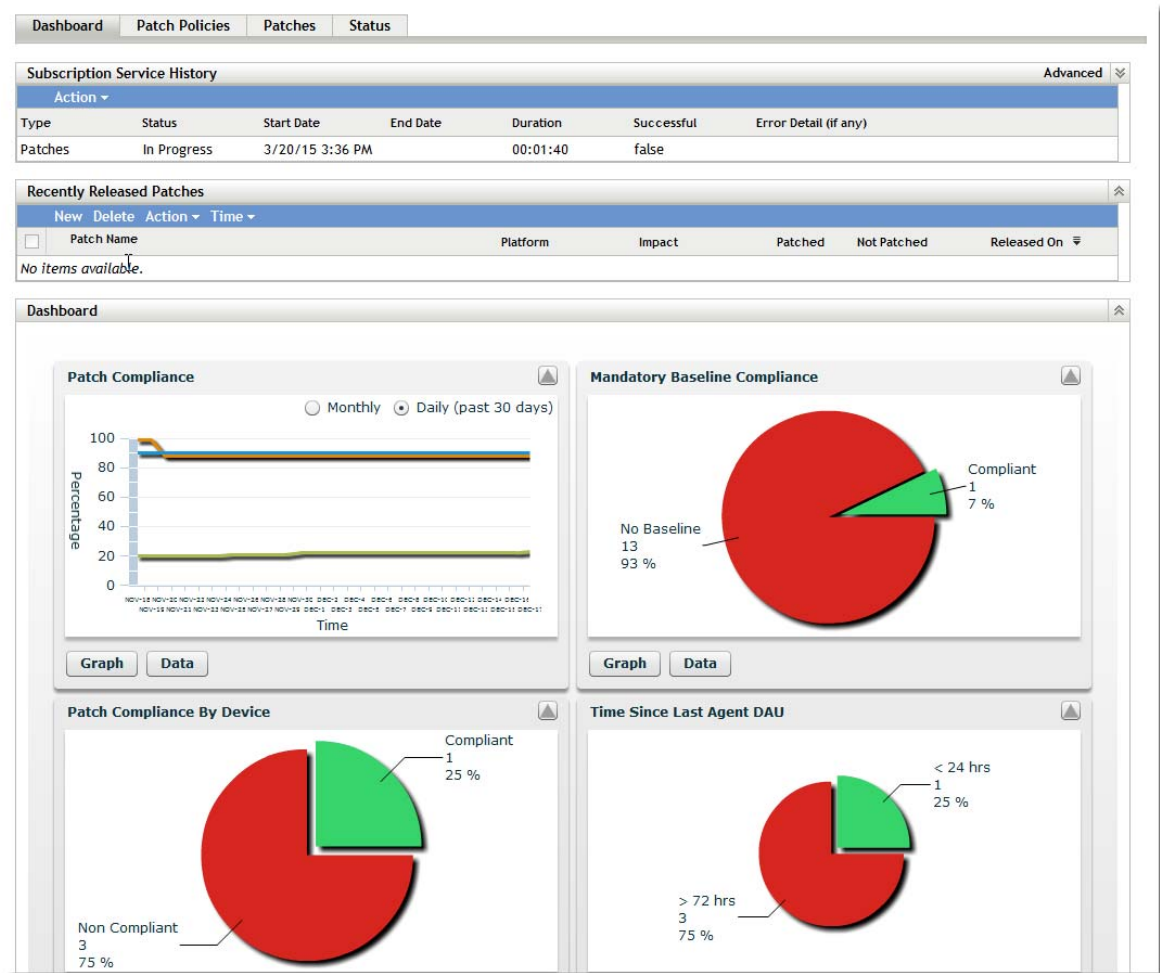
NOTE: The Patches page downloads and displays patches only for the operating systems that are running on your managed devices. This process prevents wastage of bandwidth and disk space required to store thousands of unneeded patches in the ZENworks Primary Server database. If you connect a device running a previously undetected operating system, you must initiate replication again so that the Patch Management Server downloads patches for that operating system.

Dashboard

NOTE: To use patch management effectively, customers should disable the patches that are irrelevant to their environment, so that the daily compliance statistics are based only on patches relevant to their network of devices, giving the percentage of enabled patches actually applied on a given day.

Following is an illustration of the Dashboard page:

Figure 5-3 Dashboard Page



The **Subscription Service History** section displays the activity log of the subscription activities. The following table describes each item featured in this section.

Item	Definition
Type	Subscription type defined for your account: Patches (Subscription Replication), Bundles (Subscription Replication), and Licenses.
Status	Status of the replication. When replication begins, the status reads In Progress . When replication ends, the status reads Complete . NOTE: If the replication process is interrupted, the status reads Resetting . This indicates that the replication process has continued from the point where it was interrupted.
Start Date	The date and time when replication started.
End Date	The date and time when replication ended.
Duration	The length of time the replication has been going on.
Successful	Indicates whether the replication was successful or not. True indicates successful replication and False indicates incomplete or failed replication.
Error Detail (if any)	Details of any error encountered during the patch download process.

Recently Released Patches lists the last ten patches that were downloaded by the subscription service.

item	Definition
Patch Name	The name of the patch.
Platform	The operating system that the patch applies to.
Impact	The impact of the patch.
Patched	The number of devices that the patch has been installed on.
Not Patched	The number of devices that the patch has not been installed on.
Released On	The date that the patch was released.

The **Dashboard** addresses operational, management, and compliance reporting needs with a graphical dashboard and four standard reports that document patches, patch deployments, patch status, trends, inventory and more, at individual machine or aggregated levels. This provides a unified view to demonstrate progress toward internal and external audit and compliance requirements. Clicking a dashboard report will display more information about that report in tabular form. You can update the dashboard by clicking the **Update Dashboard Report** button in the **Action** menu of the **Patch Management** tab.

The dashboard reporting thread captures daily statistics concerning the overall percentage of enabled patches that are actually patched on a given day. It will take at least 24 hours for the initial dashboard reports to be generated.

- ♦ **Patch Compliance:** Displays the monthly [or daily] trend of overall compliance for each patch impact category.

Patch Management best practices recommend that an organization should monitor compliance reports over time to ensure that the intended patches are deployed regularly and the patch management solution is being used correctly. Mouse over the trend lines to see the actual calculated percentages for each impact category (Critical, Software, or Optional). Detailed drill-down information showing the individual patched / not patched totals per patch can be seen on the **Patches** tab of **Patch Management**.

- ◆ Month [or Day]: Time period
- ◆ Critical Patch: Percentage of critical patches that are patched
- ◆ Optional Patch: Percentage of Recommended and Informational patches that are patched
- ◆ Software Patch: Percentage of Software patches that are patched
- ◆ **Mandatory Baseline Compliance:** Displays the percentage of device groups that are currently in mandatory baseline compliance.

Establishing a mandatory baseline policy allows the administrator to auto-deploy patches to device groups very quickly and easily, and to ensure that known vulnerabilities do not return when a new computer is purchased or re-imaged. Each group is evaluated as being in mandatory baseline compliance if all enabled baseline patches for that group are currently in a patched status for all group member devices.

- ◆ Status: Compliant, Non-Compliant or No Baseline
- ◆ Group Count: Number of groups in each state
- ◆ **Patch Compliance By Device:** Displays the overall patch compliance of the devices that ZENworks Patch Management is monitoring.

Each device will only be evaluated as “compliant” if it has a patched status for all of the active patches currently available within Patch Management. It is recommended that patches that are not applicable should always be disabled within Patch Management so that this metric can track only the relevant patches for the managed network of devices.



- ◆ Status: Compliant or Non-Compliant
- ◆ Device Count: Total number of devices in each state
- ◆ **Time Since Last Agent DAU:** Displays the elapsed time since the last refresh cycle for all managed devices within the network.

Within a patch management system, it is vital to ensure that all devices are scanned regularly for missing patches. Even with a regular daily refresh cycle, it is very likely that some laptops or workstations will be offline during any given day.

- ◆ Elapsed Time: < 24 hrs, < 48 hrs, < 72 hrs, > 72 hrs, above custom time
- ◆ Device Count: Total number of devices in each category

The following table describes the action of each button on the page:

Button Name	Action
Graph	Displays the details graphically.
Data	Displays the details in tabular form.
Zoom Control	Enlarges or reduces a single graph into the full page size or restores it to the original size.
Update Dashboard Report	Refreshes the Dashboard page to show the updated information.

When you click the  button, the corresponding graph is in full page size mode; when you click the  button, the corresponding graph is restored to its former size.

Status

This page displays the download status for patches and bundles in table form, and also displays the details of patch caching and queuing status.

- ♦ [“Status” on page 72](#)
- ♦ [“Cache Status” on page 73](#)

Status

Table 5-1 Status Table Items

Item Name	Item Status
Signature Download	Indicates whether downloading of the signature has finished or is in progress.
Signature Download Time	Indicates the last time the local server contacted and downloaded the signature from the Patch Subscription server.
Bundle Download	Indicates whether the patch bundle download is finished or is in progress.
Last Patch Download	Indicates the last time the local server contacted and downloaded a patch from the Patch Subscription server.
Number of Failed Download(s)	Indicates the number of patches that failed to download from the Patch Subscription server.
Number of Patches Queued for Caching	Indicates the number of patches that are queued for download from the Patch Subscription server.
Number of Active Patches	Indicates the number of patches that are available for download from the Patch Subscription server.
Number of New Patches (less than 30 days)	Indicates the number of patches that have been uploaded to the Patch Subscription server in the last 30 days and are available for download.
Latest Patch Released On	Indicates the time when the latest patches were released.

Cache Status

Table 5-2 Cache Status Table Items

Item	Definition
Action > Cancel Pending Downloads	Cancels the download of any patches in the process of being cached.
Name	The name of a patch.
Status	Whether the patch has been successfully downloaded.
Error Detail (if any)	Details of any error that occurred during the download process.

Using the Patches Page

The following sections provide more information on the Patches page:

- ♦ [“Patches” on page 73](#)
- ♦ [“Patch Information” on page 84](#)
- ♦ [“Searching for a Patch” on page 85](#)
- ♦ [“Patch Management” on page 87](#)

Patches

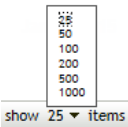
This section of the Patches page provides the following information about patches:

- ♦ Name of the patch
- ♦ Total number of patches available
- ♦ Impact of the patch
- ♦ Statistics of the patch
- ♦ Date when the patch was released

This section features the **Action** menu, which enables you to perform any of the five actions related to patches: **Deploy Remediation**, **Enable**, **Disable**, **Update Cache**, and **Update Dashboard Report**. For more information on these actions, see [“Action Menu Items” on page 83](#).

The section also features the **show items** drop-down list that enables you to select the number of items to be displayed in this section, as shown in the following image:

Figure 5-4 Show Items Drop-Down List



The following sections explain the information on the Patches page:

- ♦ [“Patch Name” on page 74](#)
- ♦ [“Total Patches Available” on page 74](#)

- ♦ “Patch Impacts” on page 75
- ♦ “Patch Statistics” on page 76
- ♦ “Patch Release Date” on page 79
- ♦ “Sorting of patches by released date” on page 79
- ♦ “Patches released within the last 30 days are displayed in bold font” on page 79
- ♦ “Patch Creation” on page 79
- ♦ “Patch Deletion” on page 82
- ♦ “Action Menu Items” on page 83

Patch Name

This is the name that identifies a patch. This name typically includes the vendor or manufacturer of the patch, the specific application, and version information.

An example of a patch name is shown as follows. It indicates that Adobe is the vendor, Acrobat Reader is the application, and 6.0.6 is the version information:

Figure 5-5 Example of a Patch Name

Adobe Acrobat Reader 6.0.6 Update

- ♦ All Microsoft security patches are titled with their Microsoft Security Bulletin number in the format MS0x-yyy, where 0x indicates the year the patch was released and yyy indicates the sequential number of the released patch. These patches are critical and must be installed as soon as possible.
- ♦ Names of all Microsoft non-security patches include the Knowledge Base (KB) article number. These patches can be installed at your discretion.
- ♦ The names of Microsoft service packs and third-party patches do not usually contain a KB number, and never a Microsoft Security Bulletin number. Test these service packs thoroughly to ensure that they have the expected results.

For more information on the naming conventions for patches, refer to [Comprehensive Patches and Exposures \(CVE\)](http://cve.mitre.org/) (<http://cve.mitre.org/>), which is a list of standardized names for patches and other information exposures. Another useful resource is the [National Patch Database](http://nvd.nist.gov/) (<http://nvd.nist.gov/>), which is the U.S. government repository of standards-based patch management data.

Total Patches Available

The total number of patches that are available for deployment is displayed in the bottom left corner of the table. In the following figure, the total number of available patches is 979:

Figure 5-6 Show Items Drop-down List

1 - 25 of 138

Patch Impacts

The type of patch defined on the basis of the severity of the patch; the type can be Critical, Recommended, Informational, or Software Installers. Each impact is described as follows:

- ♦ **Critical:** Novell has determined that this type of patch is critical, and should be installed as soon as possible. Most of the recent security updates fall in this category. ZENworks Server automatically downloads and saves the patches that have critical impact.
- ♦ **Recommended:** Novell has determined that this patch, although not critical or security related, is useful and should be applied to maintain the health of your computers. You should install patches that fall into this category.
- ♦ **Software Installers:** These types of patches are software applications. Typically, this includes software installers. The patches show **Not Patched** if the application has not been installed on a machine.
- ♦ **Informational:** This type of patch detects a condition that Novell has determined is informational. Informational patches are used for information only. There is no actual patch to be installed.

Patch Management impact terminology for its patch subscription service closely follows the vendor impact terminology for patch criticality. Each operating system has a vendor-specific impact rating and that impact is mapped to a Novell rating as described in this section. Patch Management, following the recommendations of Lumension Security, increases or steps up the severity of the impact rating. For example, Microsoft classifications for Critical, Important, and Moderate patches are all classified as Critical by Novell.

The following table lists the mapping between Novell and Microsoft patch classification terminology:

Table 5-3 Novell and Microsoft Patch Impact Mapping

Novell Patch Impacts	Windows	Other
Critical	Critical Security	NA
	Important	
	Moderate	
Recommended	Recommended	NA
	Low	
	Example: Microsoft Outlook 2003 Junk E-mail Filter Update	
Software Installers	Software Distribution	Adobe 8.1 software installer
	Example: Microsoft Windows Malicious Software Removal Tool (Virus Removal)	
Informational	NA	NA

Source: Lumension Security

Patch Statistics

Patch statistics show the relationship between a specific patch and the total number of devices (or groups) within ZENworks Server that meet a specific status. The patch statistics appear in two columns on the far right side of the Patches page. Each column status is described as follows:

- ♦ **Patched:** Displays a link indicating the total number of devices to which the corresponding patch has been applied.

Clicking this link displays a page that lists the patched devices, in alphabetical order.

Dashboard







Patch Policies

Patches

Status

Patches

New Delete Action

	Patch Name	Impact	Patched	Not Patched	Released On
<input type="checkbox"/>	 MS15-028 Security Update for Windows Server 2008 R2 x64 (KB3030377)	Critical	0	1	Mar-10-2015
<input type="checkbox"/>	 MS15-027 Security Update for Windows Server 2008 R2 x64 (KB3002657)	Critical	0	1	Mar-10-2015
<input type="checkbox"/>	 MS15-020 Security Update for Windows Server 2008 R2 x64 (KB3039066)	Critical	0	1	Mar-10-2015
<input type="checkbox"/>	 MS15-031 Security Update for Windows Server 2008 R2 x64 (KB3046049)	Critical	0	1	Mar-10-2015
<input type="checkbox"/>	 MS15-021 Security Update for Windows Server 2008 R2 x64 (KB3032323)	Critical	0	1	Mar-10-2015
<input type="checkbox"/>	 MS15-029 Security Update for Windows Server 2008 R2 x64 (KB3035126)	Critical	0	1	Mar-10-2015

If a patch does not support uninstallation, the **Remove** option in the **Action** menu is disabled.

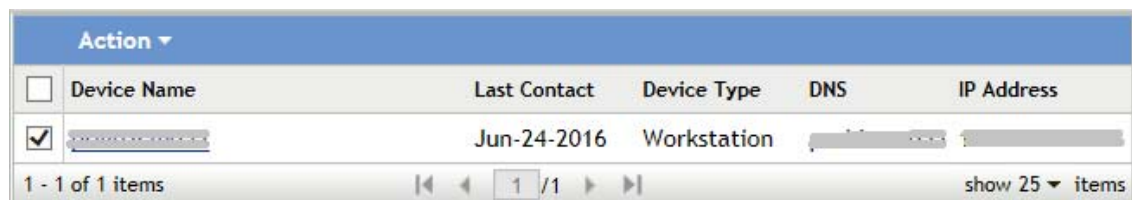
The Patched page provides the following information about the devices to which a patch has been applied.

Item	Definition
Device Name	The name of the device registered with Novell ZENworks 11 SP4 Patch Management to which the patch is to be deployed.
Last Contact	The last time the device contacted the Patch Management Server.
Device Type	Server or Workstation.
DNS	The name of the DNS server.
IP Address	The IP address of the device.

You can uninstall the patch by using the **Remove** option in the **Action** menu.

- ♦ **Not Patched:** Displays a link indicating the total number of devices to which the corresponding patch has not been applied.

Clicking this link displays a page that lists these devices, in alphabetical order.



Action ▾					
<input type="checkbox"/>	Device Name	Last Contact	Device Type	DNS	IP Address
<input checked="" type="checkbox"/>	[Device Name]	Jun-24-2016	Workstation	[DNS]	[IP Address]
1 - 1 of 1 items					
show 25 ▾ items					

The Not Patched page provides the following information about the devices to which a patch has been applied.

Item	Definition
Device Name	The name of the device registered with Novell ZENworks 11 SP4 Patch Management to which the patch is to be deployed.
Last Contact	The last time the device contacted the Patch Management Server.
Device Type	Server or Workstation.
DNS	The name of the DNS server.
IP Address	The IP address of the device.

You can deploy the patch to these devices by using the **Deploy Remediation** option in the **Action** menu.

- ♦ **Information:** The Information page displays detailed information for a selected patch.

Patched	Not Patched	Information
<div> <div>Property Name</div> <div>Details</div> </div>		
Name		
Update for Windows Server 2008 R2 x64 (KB2990214)		
Impact		
Recommended		
Status		
Enabled		
Vendor		
Microsoft Corp.		
Released On		
Apr-14-2015		
Vendor Product ID		
KB2990214		
Description		
LSAC(v3) Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.		
Number of Devices Patched		
0		
Number of Devices Not Patched		
1		
Number of Devices Not Applicable		
0		
CVE Code		
URL		
http://support.microsoft.com/kb/2990214		
Size		
3053KB		







You can view the following information for a patch:

Property Name	Definition
Name	The name of the patch.
Impact	The impact of the patch as determined by Novell. See Patch Impacts .
Status	Status of the patch; can be Enabled , Disabled (Superseded) or Disabled (By User) .
Vendor	The name of the vendor.
Released on	The date the patch was released by the vendor.

Property Name	Definition
Vendor Product ID	The ID number given to the product by the vendor.
Description	The description of the patch; includes detailed information concerning the defect or issue resolved by this patch, deployment notes, and the prerequisites for deployment.
Number of Devices Patched	The number of devices to which the patch has been applied.
Number of Devices Not Patched	The number of devices to which the patch has not been applied.
Number of Devices Not Applicable	The number of devices to which the patch does not apply.
CVE Code	The Common Vulnerabilities and Exposures ID for the patch, if applicable.
URL	A URL that has more information about the patch.
Size	The size of the patch.

The patches shown in the Patches page have different icons indicating their current status. The following table describes the icons for each patch:

Table 5-4 Patch Icons

Patch Icon	Significance
	Indicates the patches that are disabled. Disabled patches are hidden by default. Use the Include Disabled filter in the Search panel to show these items.
	Indicates that only the fingerprint information for the patch has been brought down from the ZENworks Patch Subscription Network. This icon represents the patches that are not cached.
	Indicates that a download process for the bundles associated with the selected patch is pending.
	Indicates that a download process for the bundles associated with the selected patch has started. This process caches those bundles on your ZENworks Server.
	Indicates that the fingerprints and remediation patch bundles that are necessary to address the patch have been cached in the system. This icon represents the patches that are cached and ready for deployment.
	Indicates that an error has occurred while trying to download the bundle associated with the selected patch.

Patch Release Date

The date the patch was released by the vendor is displayed in columnar form. The latest released patches are displayed in bold font and the released date is displayed under the Released On column.

Sorting of patches by released date

Clicking the Released On column lets you sort patches by their release date.

Patches released within the last 30 days are displayed in bold font

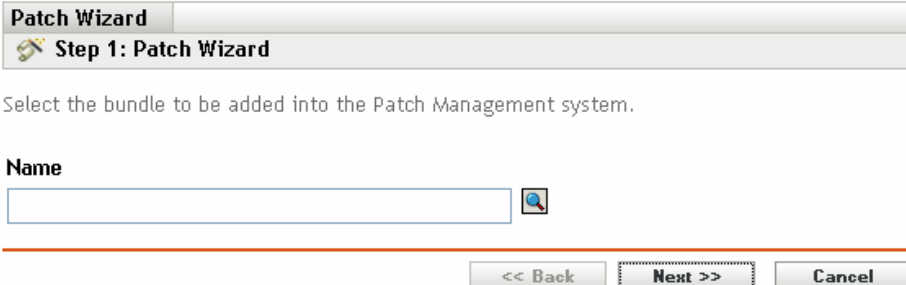
All the patches released in last 30 days are displayed in bold font.

Patch Creation

The Patches section features a Patch Wizard, which enables you to create custom patches for your devices. The wizard assists in selecting patch bundles and modifying patch details.

When you select the **New** menu item on the Patches page, the Patch Wizard appears as shown in the following figure:

Figure 5-7 Patch Wizard



The screenshot shows a window titled "Patch Wizard" with a subtitle "Step 1: Patch Wizard". Below the title bar, there is a text instruction: "Select the bundle to be added into the Patch Management system." Underneath this, there is a label "Name" followed by a text input field and a magnifying glass icon. At the bottom of the window, there are three buttons: "<< Back", "Next >>" (which is highlighted with a dashed border), and "Cancel".


The following sections provide more information on each step of the wizard:

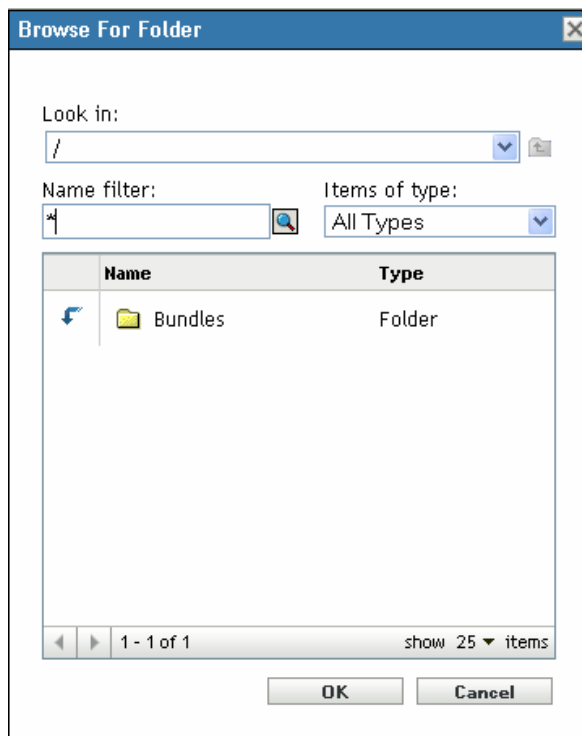
- ♦ [“Add Patch Bundle” on page 79](#)
- ♦ [“Modify Patch Details” on page 81](#)
- ♦ [“Export Patches Summary” on page 82](#)

Add Patch Bundle

Adding a bundle to the existing Patch Management System is the first step in creating a patch using the Patch Wizard.

To add one or more bundles to a patch:

- 1 Click the **New** menu item on the Patches page to open the Patch Wizard.
- 2 Click the  icon. The following window appears:



- 3 Click the arrow next to the **Bundles** option to display the available bundles in the **ZPM** folder.

TIP: You can add your own bundles, not just the ones in the ZPM folder.

- 4 Click the arrow next to a vendor to display the available bundles of that vendor.
- 5 Click the desired bundle.
- 6 Click **OK** to confirm bundle selection.
- 7 The window closes and the Select Bundles page displays the selection.

NOTE: You can associate only one bundle with a patch.

After selecting the bundle to add to the patch, click the **Next** button to modify the patch details. Click **Cancel** to exit the wizard.

Modify Patch Details

The Modify Details page allows you to add information relevant to the created patch. Modifying patch details is the second step in creating a patch using the Patch Wizard.

Figure 5-8 Modify Patch Details

The screenshot shows the 'Patch Wizard' window with 'Step 2: Patch Wizard' selected. Below the title bar, it says 'Modify the details of the patch.' The form contains the following fields:

- Name:** A text box containing 'Novell Linux 2008-11-22 SLE 10 x86 Security update'.
- Impact:** A dropdown menu with 'Recommended' selected.
- Vendor:** A text box containing 'Custom'.
- Vendor Product ID:** An empty text box.
- Requires Reboot:** A checkbox that is currently unchecked.
- Description:** A text area containing 'Patch data do not remove: Patch Remediation Bundle'.

At the bottom of the form, there are three buttons: '<< Back', 'Next >>', and 'Cancel'.

You can modify the following information for a patch:

Property Name	Definition
Name	The name of the patch.
Impact	The impact of the patch as determined by Novell. See Patch Impacts .
Vendor	The name of the vendor.
Vendor Product ID	The ID number given to the product by the vendor.
Requires Reboot	Whether a reboot is required after patch deployment
Description	The description of the patch; includes detailed information concerning the defect or issue resolved by this patch, deployment notes, and the prerequisites for deployment.
CVE Code	The Common Vulnerabilities and Exposures ID for the patch, if applicable.
URL	A URL that has more information about the patch.
Size	The size of the patch.

Click the **Next** button to open the Export Patches Summary page. Click the **Back** button to return to the previous page. Click **Cancel** to exit the wizard.

Export Patches Summary

The Export Patches Summary page of the Patch Wizard displays the summary of the patch creation you have scheduled in the previous steps. Summarizing the important points of the creation is the last and third step in creating a patch.

Figure 5-9 Export Patches Summary

Patch Wizard

Step 3: Export Patches Summary

The selected bundle will show up as 'Software Installer' patch after it's created. Applicability of the new patches will be based upon the bundle system requirements.

Patch Name

PatchCompatibilityActions

<< Back Finish Cancel

The Export Patches Summary page displays the name of the patch.

Click the **Finish** button to complete the process of creating a patch. Click the **Back** button to return to the previous page. Click **Cancel** to exit the wizard.

NOTE: After creating a new patch, you cannot immediately deploy it to any devices. This is because the Patch Management Server does not recognize the patch yet. To enable deployment, perform a subscription update after the new patch is created.

Patch Deletion

The Patches section enables you to remove patches from the Patch Management System.

To delete a patch:

- 1 Select the check boxes for the patches you want to delete and click the **Delete** menu item.
A message appears, asking you to confirm patch deletion.

Delete Patches

Deleting patches will delete all bundles associated with the selected patches until the next subscription update. Are you sure you want to delete the selected patches?

Note: Bundles associated with patches that have been deployed may not be deleted.

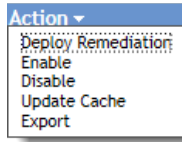
Yes No

- 2 Click Yes to confirm the deletion. Click No to return to the Patches page.

Choosing to delete patches also removes all the bundles associated with the selected patches from the Patch Management System. Performing a subscription update adds the deleted bundles to the Patch Management System.

Action Menu Items

The **Patches** section also features an **Action** menu, which enables you to perform one of five actions on the patches listed on the page. The following figure shows the five options in the **Action** menu:





The **Action** menu consists of the following five options:

- ♦ **Deploy Remediation:** Enables you to deploy a patch. To use this option, select the check boxes for the patches you want to deploy and select **Deploy Remediation** from the **Action** menu options to open the Deploy Remediation Wizard. For more information, see [Chapter 6, “Using the Deploy Remediation Wizard,” on page 91](#).
- ♦ **Enable:** Allows you to enable a disabled patch.
- ♦ **Disable:** Allows you to disable a patch. To use this option, select the check box for the desired patch and select **Disable**. The selected patch is removed from the list.
- ♦ **Update Cache:** Initiates the download process for the bundles associated with the selected patch and caches those bundles on your ZENworks Server.

The remediation patch bundles must be cached before they are installed on the target device.

To use this option:

- ♦ Select one or more patches in the patches list.
- ♦ In the **Action** menu, click **Update Cache**.

The patch icon changes to . While the download is in progress, the icon changes to . When caching is complete, the color of the patch icon changes to green. This indicates that the patch remediation is ready to be deployed.

You can sort the patches in ascending and descending alphabetical order. To sort, click the arrow in the column heading **Patch Name** as shown below.

Figure 5-10 Patch Name Column



- ♦ **Export:** Exports the page data to a comma separated value file.

NOTE: To know when a patch was downloaded, view the **Message Log** panel for that patch in the **Bundles** section.

Patch Information

You can view detailed information for a selected patch in the **Patch Information** section. Clicking the name of a patch displays the details of that patch.

For example, if you select the patch called **Windows Malicious Software Removal Tool- February 2009 (KB890830)** from the list of patches, the **Patch Information** section displays the result of a patch analysis for the selected patch, as shown in the following figure:

Figure 5-11 Patch Information for a Selected Patch

Patch Information	
Name	Windows Malicious Software Removal Tool - April 2015 (KB890830)
Impact	Software Installer
Status	Enabled
Vendor	Microsoft Corp.
Released On	Apr-14-2015
Vendor Product ID	KB890830
Description	LSAC(v2)/LSAC(v3) After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.
Requires Reboot	Yes
Supports Uninstall	No
CVE Code	
URL	http://support.microsoft.com/kb/890830
Size	43132KB

The following table defines each property name in the **Patch Information** section:

Table 5-5 Property Names in the Patch Information Section

Property Name	Definition
Name	The name of the patch.
Impact	The impact of the patch as determined by Novell. See Patch Impacts .
Status	Status of the patch; can be Enabled , Disabled (Superseded) , or Disabled (By User) .
Vendor	The name of the vendor or manufacturer.
Released on	The date the patch was released by the vendor.
Vendor Product ID	The ID number given to the product by the vendor.
Description	The description of the patch; it includes the advantages of deploying the patch and the prerequisites for deployment.
Requires Reboot	Whether a reboot is required after patch deployment
Supports Uninstall	Whether the patch supports an uninstall after installation
CVE Code	The Common Vulnerabilities and Exposures ID for the patch, if applicable.

Property Name	Definition
URL	A URL that has more information about the patch.
Size	The size of the patch.

Searching for a Patch

The **Search** section on the Patches page offers extensive search and data filtering options that allow you to search for specific patches and filter result sets based on the status and impact of the patches. Searching and filtering can be performed independently of each other or can be combined to provide extensive drill-down capabilities. The following figure shows the **Search** section:

Figure 5-12 Search Section on the Patches page

The screenshot shows a 'Search' dialog box with the following fields and options:

- Patch Name:** A text input field with 'Search' and 'Reset' buttons below it.
- Status:**
 - ☐ Patched
 - ☒ Not Patched
 - ☐ Not Applicable
 - ☐ Include Disabled
- Impact:**
 - ☒ Critical
 - ☒ Recommended
 - ☒ Informational
 - ☒ Software Installers
- Platform:** A drop-down menu currently showing 'Windows'.
- Vendor:** A drop-down menu currently showing 'All'.
- Cache Status:** A drop-down menu currently showing 'All'.
- CVE Identifier:** A text input field.

To search for a patch:

- 1 Type all or part of the patch name in the **Patch Name** text box.
- 2 Select the desired check box under **Status** and **Impact**.
- 3 Select the platform in the **Platform** drop-down list.
- 4 Select the vendor in the **Vendor** drop-down list.
- 5 Select the cache status in the **Cache Status** drop-down list.
- 6 Type a common vulnerabilities and exposures ID for a patch.
- 7 Click **Search**.

NOTE: Click **Reset** to return to the default settings.

The following table describes the result of selecting each filter option under **Status**:

Table 5-6 Status Filters in Search

Status Filter	Result
Patched	Search results include all the patches in the patch list that have been applied to one or more devices.
Not Patched	Search results include all the patches in the patch list that have not been applied to any device.
Not Applicable	Search results include all the patches in the patch list that do not apply to the device.
Include Disabled	Search results include all the patches in the patch list that have been disabled by the administrator.

The following table describes the result of selecting each filter option under **Impact**:

Table 5-7 Impact Filters in Search

Impact Filter	Result
Critical	Search results include all the patches in the patch list that are classified as Critical by Novell.
Recommended	Search results include all the patches in the patch list that are classified as Recommended by Novell.
Informational	Search results include all the patches in the patch list that are classified as Informational by Novell.
Software Installers	Search results include all the patches in the patch list that are classified as Software Installers by Novell.

Table 5-8 Vendor Filters and Cache Status Filter in Search

Filter	Result
Platform	Search results include all the patches relevant to the operating system in the patch list.
Vendor	Search results include all the patches relevant to the vendor in the patch list.
Cache Status	Search results include all the patches relevant to their cache status on the local server.
CVE Identifier	Search results include all the patches that have the common vulnerabilities and exposures ID that you type.

Patch Management

The following sections provide more information on the different options in the Patch Management pane:

- ♦ [“Deploy Remediation” on page 87](#)
- ♦ [“Export Patches” on page 87](#)
- ♦ [“View a Patch” on page 88](#)

Deploy Remediation

This option enables you to deploy a patch. To use this option, select the check boxes for the patches you want to deploy and click the **Deploy Remediation** link to open the Deploy Remediation Wizard. For more information, see [Chapter 6, “Using the Deploy Remediation Wizard,” on page 91](#).

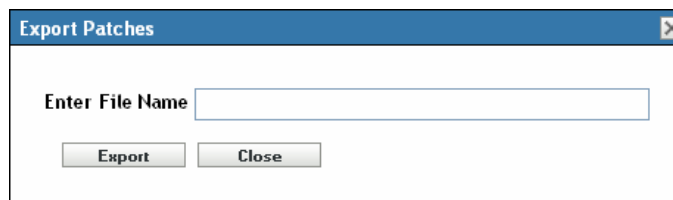
Export Patches

Details such as the status and impact of all patches can be exported into a comma-separated value (CSV) file. You can choose to save the file in a different file format after opening it from the download option.

- 1 Click the **Export Patches** link in the left pane.

This exports all data results, not just selected results. However, some data might not export or translate into .csv format in a readable format.

- 2 In the **Export Patches** dialog box, click **Export**.



- 3 In the **File Download** dialog box, select from the available options:

- ♦ **Open:** Creates the file and opens it in your Web browser. From the browser, you can save to a variety of file formats, including CSV, XML, text, and numerous spreadsheet applications.
- ♦ **Save:** Creates the file and saves it to a local folder. The file is saved in Microsoft Office Excel CSV format. The file is named `ZPMPatchesList.csv` by default.

- ♦ **Cancel:** The report is not created or saved.

	A	B	C	D	E
1	#Status	Patch Name	Impact	Patched C	Not Patched
2	Active	Adobe Acrobat Reader 6.0.2 update	Critical	0	0
3	Active	Adobe Acrobat Reader 6.0.3 Update	Critical	0	0
4	Active	Adobe Acrobat Reader 6.0.4 Update	Critical	0	0
5	Active	Adobe Acrobat Reader 6.0.5 Update	Critical	0	0
6	Active	Adobe Acrobat Reader 6.0.6 Update	Recommended	0	0
7	Active	Adobe Acrobat Reader 7.0.1 Update	Critical	0	0
8	Active	Adobe Acrobat Reader 7.0.2 Update	Critical	0	0
9	Active	Adobe Acrobat Reader 7.0.5 Update (SEE NOTES)	Critical	0	0
10	Active	Adobe Acrobat Reader 7.0.7 Update (SEE NOTES)	Critical	0	0
11	Active	Adobe Acrobat Reader 7.0.8 (Update) (Rev 4)	Critical	0	0
12	Active	Adobe APSB06-07 Dreamweaver Server Behavior SQL Injection vulnerability	Critical	0	0
13	Active	Adobe APSB07-12 Flash Player 9.0.r47 for FireFox (Upgrade) (All Languages)	Critical	0	0
14	Active	Adobe APSB07-12 Flash Player 9.0.r47 for IE (Upgrade) (All Languages) (Rev 3)	Critical	0	2
15	Active	Adobe APSB07-12 Flash Player 9.0.r47 for IE (Upgrade) (All Languages) (Rev 3)	Critical	0	0
16	Active	Adobe APSB07-12 Flash Player 9.0.r47 for Netscape (Upgrade) (All Languages) (Rev 2)	Critical	0	0
17	Active	Adobe APSB07-12 Flash Player 9.0.r47 for Netscape (Upgrade) (All Languages) (Rev 2)	Critical	0	0
18	Active	Adobe APSB07-13 Photoshop CS3 Update for Windows	Critical	0	0
19	Active	Adobe APSB07-20 Flash Player 9.0.r115 for IE (Upgrade) (All Languages)	Critical	0	0
20	Active	Adobe APSB07-20 Flash Player 9.0.r115 for IE (Upgrade) (All Languages)	Critical	0	2
21	Active	Adobe APSB08-01 Contribute CS3 update FLVPlayer_Progressive.swf file for Windows	Critical	0	0
22	Active	Adobe APSB08-01 Dreamweaver CS3 update FLVPlayer_Progressive.swf file for Windows	Critical	0	0

View a Patch

Select a patch and click the **View Patch** link to display a page that provides details for that patch. The page provides three tabs as follows:

- ♦ **Patched:** Displays the patched devices for that patch.
- ♦ **Not Patched:** Displays all the devices that are not patched for that patch.
- ♦ **Information:** Displays detailed information for that patch.

Patch Management Reports

Reports are available to customers who install ZENworks Reporting Services (ZRS) inside ZENworks 11 SP4. The following predefined reports are included for Patch Management:

- ♦ **Application Discovery Not Deployed:** Displays information on Application Discovery that have not deployed. This report lists the device name, OS name, ZENworks Agent version and last contact.
- ♦ **Application Discovery Not Run in a Specified Time:** Displays information on Device Patch Status by Vendor. This report lists the device name, OS name, ZENworks Agent version and last contact.
- ♦ **Baseline Report:** Displays information on a patch that assigned to a device. This report lists device group name, agent name, patch name, and patch status.
- ♦ **Bundle Deployment Summary:** Displays only the devices on which the patch bundle have been deployed. This report lists deployment name, patch name, assigned device name, and patch device status.
- ♦ **Critical Patch Report:** Displays information on critical patches that are assigned to the devices. This report displays the total summary of the patch status and lists patched, not patched, not applicable, Error, and total devices.
- ♦ **Device Patch Status by Vendor:** Displays information on device patch status. This report lists agent name, vendor, patched, not patched, not applicable, released on, is patch enabled, and patch impact.
- ♦ **Mandatory Baseline By Patch:** Displays information on patch that have been assigned as mandatory baseline on a device. This report lists group name, patch name, criticality, vendor, released on, enabled status, cached status, patched, host name, DNS, and patch device status.

- ♦ **Mandatory Baseline Details:** Displays information on the device group name and device name on which mandatory baseline patch have been applied. This report lists device group name, criticality, name, device name, and patch device status.
- ♦ **Mandatory Baseline Summary:** Displays information on patch assigned as mandatory baseline on a device. This report lists vulnerability name, released on, criticality, group name, applicable, devices, patched, and not patched.
- ♦ **Patch Analysis:** Displays information on patch assigned as mandatory baseline on a device. This report lists vendor, patch name, released date, criticality, applicable, patched, not patched, and %patched.
- ♦ **Patch Assessment Report:** Displays information on all released patches and their impact. This report lists vendor, released patches, and patch impact.
- ♦ **Patch Bundle Deployment Status:** Displays information on all released patch bundles and their status. This report lists admin initiated remediation bundle, deployed patch bundle, event type, and event status.
- ♦ **Patch Deployment Summary:** Displays information on all released patch bundles and their status. This report lists admin initiated remediation bundle, deployed patch bundle, event type, and event status.
- ♦ **Patch Detail Report:** Displays detailed information on patches. This report lists patch name, patched status, total devices, and %patched.
- ♦ **Patch Release Report:** Displays information on released patches. This report lists, patch device status, and device name.
- ♦ **Patch Tuesday Report:** Displays information on Tuesday's released patches. This report lists, patch name, patch status, and total devices.
- ♦ **Top 10 Not Patched Critical Patches:** Displays information on the most critical patches that are not deployed. This report lists patch name and patch impact.

6 Using the Deploy Remediation Wizard

The Deploy Remediation Wizard provides an interface to create or edit patch deployment schedules for multiple recipients or devices. The wizard assists in selecting devices, scheduling deployment of patches, and if required, setting recurrence.

You can access the Deploy Remediation Wizard from the **Devices** or **Patch Management** tab.

If you select multiple patches in the Deployment Remediation Wizard, the wizard automatically selects all the applicable devices and packages. If any device is selected, the wizard automatically selects all patches that are applicable for that device. If a group is selected, the wizard includes all patches applicable for the devices in that particular group.

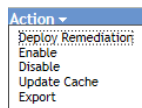
The following sections provide more information on each step of the wizard:

- ♦ [“Creating a Deployment Schedule” on page 91](#)
- ♦ [“Confirm Devices” on page 92](#)
- ♦ [“License Agreement” on page 95](#)
- ♦ [“Remediation Schedule” on page 95](#)
- ♦ [“Deployment Order and Behavior” on page 105](#)
- ♦ [“Remediation Options” on page 106](#)
- ♦ [“Advanced Remediation Options” on page 107](#)
- ♦ [“Pre Install Notification Options” on page 108](#)
- ♦ [“Distribution Schedule” on page 110](#)
- ♦ [“Notification and Reboot Options” on page 118](#)
- ♦ [“Choose Deployment Name” on page 121](#)
- ♦ [“Deployment Summary” on page 122](#)

Creating a Deployment Schedule

To create a deployment schedule for a patch for one or more devices:

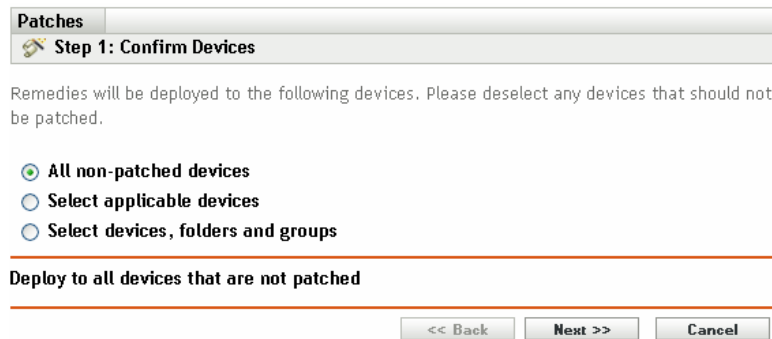
- 1 Click the **Patch Management** tab and select the patch that you want to deploy to one or more devices.
- 2 Select **Deploy Remediation** from the **Action** menu on the Patches page, as shown in the following figure. Alternatively, you can click the **Deploy Remediation** link in the **Patch Management** pane on the left side of the Patches page:



Confirm Devices

The Confirm Devices page allows you to select and confirm the devices for which you need to schedule a deployment. Confirming the device is the first step in scheduling a deployment for a selected patch.

Figure 6-1 Confirm Devices Page



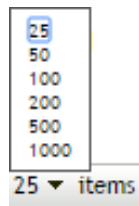
The page indicates the total number of devices to which the selected patch will be deployed. In the following example, two devices will receive the patch:

Figure 6-2 Total Number of Devices



You can choose the total number of items to be displayed on the page by using the **show items** drop-down list:

Figure 6-3 Show Items



- 1 Select the devices for deployment, then click the **Next** button to open the License Agreement page.
- 2 Select one of the following options to determine the devices to which the patches are to be deployed.
 - ♦ Choose **All non-patched** devices to deploy the patch to those devices that are in a non-patched state, then continue with [“Confirm Devices: All Non-patched Devices” on page 93](#).
 - ♦ Choose **Select applicable devices** to deploy the patch to specific devices, then continue with [“Confirm Devices: Select Applicable Devices” on page 93](#).
 - ♦ Choose **Select devices, folders and groups** to deploy the patch to specific devices, folders, or groups that are in a non-patched state. Then, continue with [“Confirm Devices: Select Devices, Folders, and Groups” on page 94](#).

Confirm Devices: All Non-patched Devices

Selecting this option deploys the patch to all the devices that are not patched. This option is enabled by default.

Confirm Devices: Select Applicable Devices

When you select **Select applicable devices**, the Confirm Devices page appears as shown in the following figure:

Figure 6-4 Confirm Devices Page for the Select Applicable Devices Type

Patches

Step 1: Confirm Devices

Remedies will be deployed to the following devices. Please deselect any devices that should not be patched.

All non-patched devices

Select applicable devices

Select devices, folders and groups

<input type="checkbox"/>	Device Name	Last Contact	Platform	DNS	IP Address
<input checked="" type="checkbox"/>	2k3er2zcm1	Oct-24-2011	Windows	2K3ER2zcm1.symbio.com	172.16.46.168
<input checked="" type="checkbox"/>	xpagent	Oct-24-2011	Windows	xpagent.symbio.com	172.16.46.158

1 - 2 of 2

show 25 items

<< Back

Next >>

Cancel

Selecting this option deploys the patch to the devices you select from the devices list. You can deploy a patch to a device regardless of its existing patch status, which can be patched or not patched.

NOTE: If you deploy a patch from the Patch Management page, the list of devices that appears is based on the patch **Status** filter you choose.

Table 6-1 Confirm Devices Page Column Headings

Column Heading	Description
Device Name	The name of the device. The name of the device registered with Novell ZENworks 11 SP4 Patch Management to which the patch is to be deployed.
Last Contact	The status of the device when they were last contacted.
Platform	The operating system of the device.
DNS	The name of the DNS server.
IP Address	The IP address of the device.

Confirm Devices: Select Devices, Folders, and Groups

When you select **Select devices, folders and groups**, the Confirm Devices page appears as shown in the following figure:

Figure 6-5 Confirm Devices Page for the Select Devices, Folders and Groups Type

Patches

Step 1: Confirm Devices

Remedies will be deployed to the following devices. Please deselect any devices that should not be patched.

☐ All non-patched devices

☐ Select applicable devices

☒ Select devices, folders and groups

Add	Remove
Name	In Folder

No items selected, click add to select items

<< Back Next >> Cancel

To select a device, folder, or group for deployment:

- 1 Click the **Add** menu item on the Confirm Devices page. The following window appears:

Look in: /

Name filter: Items of type: All Types

Name	Type
Devices	Folder

1 - 1 of 1 show 25 items

Select All 0 Items Selected Remove All

OK Cancel

- 2 Click the arrow next to the **Devices** option on the left side of the window to display the available devices, folders, and groups.
- 3 Click the desired device to add it to the **Selected** panel on the right side of the window.
or
To remove a device from the panel, click the **Delete** button in the **Remove** column for that device.
- 4 Click **OK** to confirm device selection.

The window closes and the Confirm Devices page displays the selection.

You can remove a device from the list by selecting it and clicking the **Remove** menu item.

License Agreement

The License Agreement page displays all the third-party licensing information associated with the selected patches. Accepting or declining the license agreement of the patch is the second step in scheduling a deployment for a selected patch.

Figure 6-6 License Agreement Page

The screenshot shows the 'Patches' tab with 'Step 2: License Agreement' selected. Below the tab, a message states: 'Please review all the license agreements below. You must accept all of the licenses before you will be able to proceed to the next step.' A table follows with three columns: 'Required license lists', 'Accept', and 'Decline'. The first row contains the text 'Windows Malicious Software Removal Tool - February 2009 (KB890830)' under the first column, an empty circle under 'Accept', and a circle with a green checkmark under 'Decline'. Below the table, the text 'License Agreement' is displayed. At the bottom right, there are three buttons: '<< Back', 'Next >>', and 'Cancel'.

Required license lists	Accept	Decline
Windows Malicious Software Removal Tool - February 2009 (KB890830)	<input type="radio"/>	<input checked="" type="radio"/>

Select **Accept** for the license agreements you want to accept. To view the license agreement details, click the name of the patch.

NOTE: All license agreements must be accepted before the deployment wizard allows you to proceed.

Click the **Next** button to open the Remediation Schedule page. Click the **Back** button to return to the previous page. Click **Cancel** to exit the wizard.

Remediation Schedule

The Remediation Schedule page allows you to select how a patch is scheduled and deployed for selected devices. Setting various deployment options for a selected patch is the third step in scheduling a deployment for the selected patch.

Figure 6-7 Remediation Schedule Page

The screenshot shows the 'Patches' tab with 'Step 3: Remediation Schedule' selected. Below the tab, a message states: 'Please select the schedule for deployment of remediation to your selected devices'. A 'Schedule Type:' label is followed by a dropdown menu. The dropdown menu is open, showing three options: 'Now', 'Date Specific' (which is highlighted), and 'Recurring'. At the bottom right, there are three buttons: '<< Back', 'Next >>', and 'Cancel'.

To start setting the remediation schedule, you need to select the schedule type. Patch Management offers three types of schedules to determine when the patches are actually applied to the target device:

- ♦ Select **Now** to schedule the deployment to your selected devices immediately after you complete all the steps in the Deployment Remediation Wizard.
- ♦ Select **Date Specific** to schedule the deployment to your selected devices according to the selected date.
- ♦ Select **Recurring** to start the deployment on the selected day at a selected time, repeat the deployment every day/week/month, and if defined, end on a specific date.

By default, the Device Refresh Schedule is set to twice a day. For testing and demonstration purposes, you could increase the frequency to once every five to fifteen minutes.

The following sections provide more information on schedule types:

- ♦ [“Remediation Schedule: Now” on page 96](#)
- ♦ [“Remediation Schedule: Date Specific” on page 97](#)
- ♦ [“Remediation Schedule: Recurring” on page 98](#)
- ♦ [“Remediation Schedule: Wake On LAN” on page 103](#)

Remediation Schedule: Now

When you select **Now**, the Remediation Schedule page appears as shown in the following figure:

Figure 6-8 Remediation Schedule Page for the Now Schedule Type

The screenshot shows a software window titled "Patches" with a sub-header "Step 3: Remediation Schedule". Below the header is a message: "Please select the schedule for deployment of remediation to your selected devices". Underneath, there is a label "Schedule Type:" followed by a dropdown menu. The dropdown menu is open, showing "Now" as the selected option. At the bottom of the window, there are three buttons: "<< Back", "Next >>", and "Cancel".

In this page, you can directly schedule deployment after completing the remaining steps in the Deployment Remediation Wizard.

Remediation Schedule: Date Specific

When you select **Date Specific**, the Remediation Schedule page appears as shown in the following figure:

Figure 6-9 Remediation Schedule Page for the Date Specific Schedule Type

The screenshot shows a web interface for configuring a remediation schedule. At the top, there's a tab labeled 'Patches' and a sub-header 'Step 3: Remediation Schedule'. Below this, a message says 'Please select the schedule for deployment of remediation to your selected devices'. The 'Schedule Type' dropdown is set to 'Date Specific'. The 'Start Date(s)' field is empty, with a calendar icon to its right. There are two checkboxes: 'Run event every year' (unchecked) and 'Process immediately if device unable to execute on schedule' (unchecked). Under 'Select when schedule execution should start:', 'Start immediately at Start Time' is selected. Below this, 'Start Time' and 'End Time' are both set to '1:00'. A checkbox for 'Use Coordinated Universal Time (Current UTC 8:08 AM)' is unchecked. At the bottom right, there are three buttons: '<< Back', 'Next >>', and 'Cancel'.

Use this page to set the following deployment options:

- ♦ **Start Date:** Enables you to pick the date when you need to start the deployment. To do so, click the icon to open the calendar and pick the date. To remove the selected date, click the icon.
- ♦ **Run event every year:** Ensures that the deployment starts on a selected date at a selected time, repeats every year, and if defined, ends on a specific date.
- ♦ **Process immediately if device unable to execute on schedule:** Ensures that the deployment starts immediately if the device could not execute on the selected schedule.
- ♦ **Select when schedule execution should start:** There are two options to enable you to select the start time of the schedule execution namely:
 - ♦ **Start immediately at Start Time:** Deactivates the **End Time** panel and starts the deployment at the start time specified. In this option, you must set the start time in the **Start Time** panel:

Start Time:

- ♦ **Start at a random time between Start Time and End Times:** Activates the **End Time** panel next to the **Start Time** panel. You can specify the end time and the start time so that the deployment occurs at a random time between them. The **End Time** panel appears as follows:

End Time:

In both time panels, the first drop-down list enables you to select the hour, the second drop-down list enables you to select the minute, and the third drop-down list enables you to select **am** and **pm**.

Selecting the **Use Coordinated Universal Time** check box enables you to schedule the deployment of all devices at the same time, regardless of time zone differences. Coordinated Universal Time (UTC), also known as World Time, Z Time, or Zulu Time, is a standardized measurement of time that is not dependent upon the local time zone. Deselecting UTC schedules the distribution at the local time.

Click the **Next** button to open the Deployment Order and Behavior page. Click the **Back** button to return to the previous page. Click **Cancel** to exit the wizard.

Remediation Schedule: Recurring

When you select **Recurring**, the Remediation Schedule page appears as shown in the following figure:

Figure 6-10 Remediation Schedule Page for the Recurring Schedule Type

The screenshot shows the 'Step 3: Remediation Schedule' page. At the top, there's a tab labeled 'Patches' and a sub-header 'Step 3: Remediation Schedule'. Below this is a instruction: 'Please select the schedule for deployment of remediation to your selected devices'. The 'Schedule Type' dropdown is set to 'Recurring'. Under this, there are three main options: 'When a device is refreshed' (selected), 'Days of the week', and 'Monthly'. The 'When a device is refreshed' section includes a checkbox for 'Delay execution after refresh' and input fields for '0 Days', '0 Hours', and '0 Minutes'. The 'Days of the week' section shows a grid for Sun through Sat, all of which are currently unchecked. It also has a 'Start Time' set to '1 :00' and a 'More Options' link. The 'Monthly' section has three radio buttons: 'Day of the month' (selected with value '1'), 'Last day of the month', and 'First' (with a dropdown set to 'Sunday' and a calendar icon). It also has a 'Start Time' set to '1 :00' and a 'More Options' link. The 'Fixed Interval' section has input fields for '0 Months', '0 Weeks', '0 Days', '0 Hours', and '0 Minutes', along with a 'Start Date' of '5/13/2016' and a 'Start Time' of '1 :00', with a 'More Options' link. At the bottom, there is a checkbox for 'Wake-on-LAN (Applies to Devices only)' and an 'Options' button.

NOTE: By default, the bundle install frequency is set to **Install once per device**. For a recurring deployment, change it to **Install always**.

To change the schedule:

- 1 Click **Bundles** in the ZENworks navigation panel, and locate the particular patch bundle assignment.
- 2 Click the patch bundle, and select **Actions** tab > **Install** tab > **Options**.
- 3 Select **Install always** and click **OK**.
- 4 Click **Apply**.

In the Recurring Remediation Schedule, you can set the following options for a recurring deployment:

- ♦ [“When a Device Is Refreshed” on page 99](#)
- ♦ [“Days of the Week” on page 100](#)
- ♦ [“Monthly” on page 101](#)
- ♦ [“Fixed Interval” on page 102](#)

When a Device Is Refreshed

This option enables you to schedule a recurring deployment whenever the device is refreshed. In this option, you can choose to delay the next deployment until after a specific time.

To set the delay, select the **Delay execution after refresh** check box, and specify the days, hours, and minutes of the time to delay the deployment:

NOTE: The device is refreshed based on the settings in the **Device Management** tab under the **Configuration** tab. Click the **Device Refresh Schedule** link under the **Device Management** tab to open the page displaying the option for either a **Manual Refresh** or **Timed Refresh**. Alternatively, you can refresh the device by selecting a device under the **Devices** tab and clicking the **Refresh Device** option under the **Quick Tasks** menu.

Days of the Week

This option enables you to schedule the deployment on selected days of the week:

To set the day of deployment, select the **Days of the week** button, select the required day of the week, and set the start time of deployment.

If you click the **More Options** link, additional deployment options appear as shown in the following figure. Click the **Hide Options** link to hide the additional deployment options and show only the default deployment options:

Days of the week

*

Sun	Mon	Tue	Wed	Thu	Fri	Sat
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Time: :

[Hide Options](#)

☐ Process immediately if device unable to execute on schedule

☐ Use Coordinated Universal Time (Current UTC 8:19 AM)

☐ Start at a random time between Start and End Times

End Time: :


☐ Restrict schedule execution to the following date range:

Start Date:

End Date:

Selecting the **Use Coordinated Universal Time** check box enables you to schedule the deployment of all devices at the same time, regardless of time zone differences. Coordinated Universal Time (UTC), also known as World Time, Z Time, or Zulu Time, is a standardized measurement of time that is not dependent upon the local time zone. Deselecting UTC schedules the distribution at local time.

Selecting the **Start at a random time between Start Time and End Times** check box activates the **End Time** panel in addition to the **Start Time** panel. You can specify the end time and the start time so that the deployment occurs at any random time between the start and end times.

The **Restrict schedule execution to the following date range** option enables you to schedule a recurring deployment at the selected time, repeat the deployment on the days specified, and, if defined, end at the specific time. This option also enables you to restrict the deployment to the period between the start date and the end date. To set this option, select the **Restrict schedule execution to the following date range** check box and click the  icon to open the calendar and pick a start date or end date. Click the **Close** button when you have finished selecting the date.

Monthly

This option enables you to specify the monthly deployment options:

Figure 6-11 Monthly Deployment Options – Default

The screenshot shows the 'Monthly' deployment options interface. It features a radio button labeled 'Monthly' which is selected. Below it are three options: 'Day of the month:' with a text input field containing '1', 'Last day of the month', and 'Particular days of the month' which consists of a dropdown menu showing 'First' and another dropdown showing 'Sunday', followed by a plus icon. Below these is a 'Start Time:' section with a dropdown for '1' and a dropdown for ':00'. At the bottom is a link labeled 'More Options'.

In the **Monthly** deployment option, you can specify the following:

- **Days of the month:** Enables you to schedule the deployment on a specific day of the month. You can specify any number between 1 and 31.
- **Last day of the month:** Enables you to schedule the deployment on the last day of the month.
- **Particular days of the month:** Enables you to schedule the deployment on specific days of every month. The valid options for the day are first, second, third, fourth, and fifth. The valid options for the weekday are Sunday through Saturday. To select one particular day of the month, use the drop-down arrows. An example is shown as follows.

This screenshot shows a close-up of the 'Particular days of the month' section. It displays a radio button, a dropdown menu with 'Second' selected, another dropdown menu with 'Sunday' selected, and a plus icon to the right.

To select an additional day of the month, click the **Plus** icon and use the drop-down arrows in the second row.

This screenshot shows the 'Particular days of the month' section with two rows. The first row has a radio button, a dropdown with 'Second', a dropdown with 'Sunday', and a minus icon. The second row has a dropdown with 'First', a dropdown with 'Monday', a minus icon, and a plus icon.

To remove a particular day from the list, click the **Minus** icon.

If you click the **More Options** link, additional deployment options appear as shown in the following figure. Clicking the **Hide Options** link hides the additional deployment options and shows only the default deployment options.

☛ Monthly

- ☒ Day of the month:
- ☐ Last day of the month
- ☐ 
- Start Time: :

[Hide Options](#)

- ☐ Process immediately if device unable to execute on schedule
- ☐ Use Coordinated Universal Time (Current UTC 8:19 AM)
- ☐ Start at a random time between Start and End Times

End Time: :

- ☒ Restrict schedule execution to the following date range:

Start Date: 

End Date: 

NOTE: The **Restrict schedule execution to the following date range** option enables you to schedule a recurring deployment at the selected time, repeat the deployment on the days specified, and if defined, end on the specific time. This option also enables you to restrict the deployment to the period between the Start Date and the End Date. To set this option, select the **Restrict schedule execution to the following date range** check box and click the **Time** icon to open the calendar and pick a start date or end date. Click the **Close** button when you have finished selecting the date.


Fixed Interval

This option enables you to schedule a recurring deployment that runs after a fixed duration on a regular basis. You can choose the number of months, weeks, days, hours, and minutes of the interval and the start date for the deployment schedule, as shown in the following figure:

Figure 6-12 Fixed Interval Deployment Options - Default

☛ Fixed Interval

Months Weeks Days Hours Minutes

Start Date:  Start Time: :


[More Options](#)

If you click the **More Options** link, additional deployment options appear as shown in the following figure. Clicking the **Hide Options** link hides the additional deployment options and shows only the default deployment options:

Figure 6-13 Fixed Interval Deployment Options - All

☒ **Fixed Interval**

Months Weeks Days Hours Minutes

Start Date:  Start Time: :

[Hide Options](#)

☐ Process immediately if device unable to execute on schedule
☐ Use Coordinated Universal Time
☐ Restrict schedule execution to the following date range:


End Date: End Time: : (Current UTC 8:19 AM)

Remediation Schedule: Wake On LAN

The Wake on LAN function is an option in Remediation schedule. It can be used to set a deployment even if the managed devices are powered off. By default the settings will automatically detect the Primary server, the parameters can be changed by pressing the (options) button, where you can select different servers for the wake up request and wake up broadcast.


Figure 6-14 Remediation Schedule Page with Wake On LAN option

Patches

 **Step 3: Remediation Schedule**

Please select the schedule for deployment of remediation to your selected devices

Schedule Type:

Start Date(s): * 


☐ Run event every year
☐ Process immediately if device unable to execute on schedule

Select when schedule execution should start:

☒ Start immediately at Start Time
☐ Start at a random time between Start and End Times

Start Time: : End Time: :

☐ Use Coordinated Universal Time (Current UTC 5:32 PM)

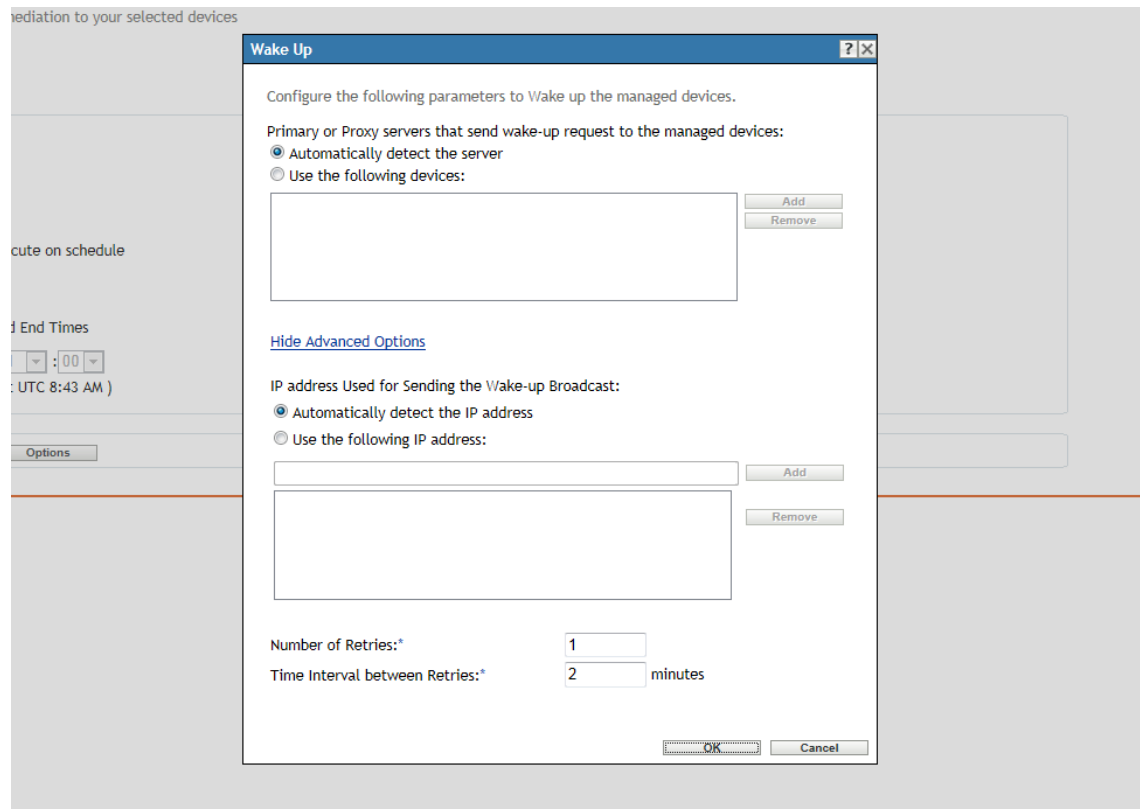
☒ Wake-on-LAN (Applies to Devices only) 

NOTE: The default settings for this function are to automatically detect the Primary server.

To change the parameters:

- 1 Select the Wake On LAN check box.
- 2 Click **Options**. This opens the Options window.
- 3 Select desired parameters and click **OK**.

When you select Wake On LAN options, the Advanced settings page appears as shown in the following figure:




Deployment Order and Behavior

The Deployment Order and Behavior page of the Deploy Remediation Wizard enables you to set the order and behavior for each deployment schedule. Setting the order and behavior of deployment for a selected patch is the fourth step in scheduling a deployment for a selected patch.

Figure 6-15 Deployment Order and Behavior Page

Patches

 Step 4: Deployment Order and Behavior

Choose the deployment Order and Behavior

<input type="checkbox"/>	Package Name	Order	Reboot	
<input type="checkbox"/>	890830 Windows Malicious Software Removal Tool - December 2009 (KB890830)	1	No	<div>^^ ^ v vv</div>

<< Back

Next >>





Cancel

The Deployment Order and Behavior page features the following:

- ♦ **Package Name:** The name of the patch that has been selected for deployment.
- ♦ **Order:** The order of execution of the deployment. The arrow appearing next to the column heading enables you to sort in ascending or descending order.
- ♦ **Reboot:** The reboot settings applicable for the corresponding patch.

The following table describes the actions of the various buttons in the Deployment Order and Behavior page:

Table 6-2 Buttons in the Deployment Order and Behavior Page

Button	Action
	Moves the patch to the top of all non-chained deployments
	Moves the patch up one place
	Moves the patch down one place
	Moves the patch to the bottom of the listing

NOTE: Chained patches can be moved only after removing their chained status.

Click the **Next** button to open the Remediation Options page. Click the **Back** button to return to the previous page. Click **Cancel** to exit the wizard.


Remediation Options

The Remediation Options page enables you to select the required remediation option for each deployment schedule. Setting the remediation options for a selected patch is the fifth step in scheduling a deployment for a selected patch.

NOTE: The **Advanced** option enables you to specify individual patch flags for each remediation.

Figure 6-16 Remediation Options Page

Patches

 **Step 5: Remediation Options**

Please select the desired remediation option. To specify individual patch flags for each remediation, use the Advanced option.

☐

Auto Reboot (silent install with optional reboot)

☐

No Reboot (silent install, never reboot)

☒

Advanced (individually set all possible deployment options)

<< Back

Next >>

Cancel

The following table describes the functionality of each option available in the Remediation Options page:

Table 6-3 The Remediation Options

Remediation Option	Functionality
Auto Reboot (silent install with optional reboot)	Automatically sets all possible patches to deploy with QChain enabled. Allows the administrator to set the patch deployment flags as desired, using the default and reboot settings defined for each patch.
No Reboot (silent install, never reboot)	Automatically sets all possible patches to deploy with QChain enabled. All necessary reboots must be performed manually.
Advanced (individually set all possible deployment options)	Allows the administrator to set the patch deployment flags as desired, using the default QChain and reboot settings defined for each patch.

Click the **Next** button to open the Advanced Remediation Options page. Click the **Back** button to return to the previous page. Click **Cancel** to exit the wizard.











Advanced Remediation Options














The Advanced Remediation Options page enables you to set patch flags for each remediation. Setting the patch flags for a selected patch is the sixth step in scheduling a deployment for the selected patch. The icons displayed on the page represent the patch flags that can be set for each package.

Figure 6-17 Advanced Remediation Options Page

The following table describes the functionality of each icon on the Advanced Remediation Options page:

Table 6-4 The Advanced Remediation Options Page

Icon	Name	Functionality
	Uninstall	Uninstalls the packages.
	Force Shutdown	Forces all applications to close if the package causes a reboot.
	Do Not Back Up	Does not back up files for uninstalling.
	Suppress Reboot	Prevents the computer from rebooting after installation of the package.
	Quiet Mode	Sets the installer to function in quiet mode. Quiet mode suppresses any user interfaces (if a user is logged in) during the remediation.
	Unattended Setup	Installs the packages in the Unattended Setup mode.
	List Hot Fixes	Returns a list of the hot fixes installed on the target computers.
	Force Reboot	Forces the computer to reboot regardless of package requirements.
	Reboot is Required	Indicates that this package requires a reboot prior to completing the installation. Selecting this option reboots the device even if the specific bundle does not require a reboot.
	Chain Packages	Sets the package as chainable (if the package supports chaining). This option cannot be modified in this release; the package is always installed with the “chain” option.

Icon	Name	Functionality
	Suppress Chained Reboot	Suppress the reboot, allowing other chained packages to be sent following this package You should suppress the final reboot for all chained packages, then send a reboot deployment when all packages are finished.
	Repair File Permissions	Repairs file permissions after package installation.
	Download Only	Distributes the package without running the package installation script.
	Suppress Notification	Suppresses any user notifications during installations.
	Debug Mode	Runs the package installation in debug mode.
	Do Not Repair Permissions	Suppresses the repair of filename permissions after the reboot.
	May Reboot	Allows the package to force a reboot if required.
	Multi-User Mode	Performs the installation in Multi-User mode.
	Single-User Mode	Performs the installation in Single-User mode.
	Restart Service	Restarts the service following the deployment.
	Do Not Restart Service	Does not restart the service following the deployment.
	Reconfigure	Performs the system reconfigure task following the deployment.
	Do Not Reconfigure	Does not perform the system reconfigure task following the deployment.

NOTE: Depending on the type of patch you select, the icons displayed in [Table 6-4 on page 107](#) change dynamically, so you might not be able to select some of the options described in the table.

Click the **Next** button to open the Pre Install Notification Options page. Click the **Back** button to return to the previous page. Click **Cancel** to exit the wizard.

Pre Install Notification Options

The Pre Install Notification Options page of the Deploy Remediation Wizard allows you to define whether users receive any notification when patches are downloaded and installed, and to customize the notification. Setting the notification and allowing users to cancel options is the seventh step in scheduling a deployment for a selected patch.

NOTE: The **Pre Install Notification Option** only displays if the **Advanced** option is selected in the **Step 5: Remediation Options** page.

Figure 6-18 Pre Install Notification Options Page

Patches
Step 7: Pre Install Notification Options

Select Pre Install Notification Options

Define Pre Install Options

☒ Use values assigned to system variables or defaults
☐ Override Settings

☒ Notify Users of Patch Install

☒ Prompt before download
☐ Prompt before install

Description Text

The download and installation of patches is ready to begin. If you require any additional information, please contact your Novell ZENworks Patch Management administrator.

Options

	Yes	No
Allow user to cancel	<input type="radio"/>	<input checked="" type="radio"/>
Allow user to snooze	<input checked="" type="radio"/>	<input type="radio"/>
Snooze interval	10	Minutes
Install within	2	Hours

Show tray notification ☒ ☐

Tray notification duration 20 Seconds

Tray notification text

There are important patches that need to be applied to your device. Click here to install patches now.

<< Back Next >> Cancel

The page provides the following options:

- ♦ **Notify Users Of Patch Install:** Select this option to notify the user prior to the installation of the patch. There are two options:
 - ♦ **Prompt before download:** Select this option to notify the user when the patch download process begins.
For eg. select Prompt before download and change the text in the Popup text as PBD and the Description text as PBD Description. Then refresh the agent and then we will see this pop up box that was selected.
 - ♦ **Prompt before install:** Select this option to notify the user when the patch installation process begins.
For eg. select Prompt before install and change the text in the Popup text as PBI and the Description text as PBI Description. Then refresh the agent and then we will see this pop up box that was selected.
- ♦ **Description text:** The text of the notification message. You can edit this field only if you override the default settings.
- ♦ **Override Settings:** Select this option to use the settings chosen by users for each agent. Selecting this option enables all other notification options and enables you to edit the default settings.

- ♦ **Options:** When you define installation options, you can specify whether to use the values in the default settings (the **Use values assigned to system variables or defaults** check box) or the custom settings. There are three options:

- ♦ **Allow User to cancel:** Allows the user to cancel the patch installation.
- ♦ **Allow User to snooze:** Allows the user to pause the installation.

NOTE: Even if you snooze the installation, the popup window will continue to appear every few seconds until you proceed with or cancel the installation.

- ♦ **Show tray notification:** On selecting this option, a notification for a pending installation is displayed in the system tray. If you select this option, define the following options:
 - ♦ **Tray notification text:** Option to select how long the system tray notification is displayed before being hidden.
 - ♦ **Tray notification duration:** Option for text that appears in the notification.

Click the **Next** button to proceed to the Notification and Reboot Options Distribution Schedule page. Click the **Back** button to return to the previous page. Click **Cancel** to exit the wizard.

Distribution Schedule

The Distribution Schedule page of the Deployment Remediation Wizard allows you to determine when a patch will be distributed to and installed on the devices. Setting a distribution schedule is the eighth step in scheduling a deployment for a selected patch.

Figure 6-19 Distribution Schedule Page

Patches

Step 8: Distribution Schedule

Please select the distribution schedule for devices

Schedule Type:

No Schedule

No Schedule

Date Specific

Recurring

<< Back Next >> Cancel

To start setting the distribution schedule, you need to select the schedule type. Patch Management offers three types of schedules to determine when the patches are actually distributed to the target device:

- ♦ Select **No Schedule** to schedule the distribution to your selected devices immediately after you complete all the steps in the Deployment Remediation Wizard.
- ♦ Select **Date Specific** to schedule the distribution to your selected devices according to the selected date.
- ♦ Select **Recurring** to start the distribution on the selected day at a selected time, repeat the deployment every day/week/month, and if defined, end on a specific date.

By default, the Device Refresh Schedule is set to twice a day. For testing and demonstration purposes, you could increase the frequency to once every five to fifteen minutes.

The following sections provide more information on schedule types:

- ♦ “Distribution Schedule: No Schedule” on page 111
- ♦ “Distribution Schedule: Date Specific” on page 111
- ♦ “Distribution Schedule: Recurring” on page 113

Distribution Schedule: No Schedule

When you select **Now**, the Distribution Schedule page appears as shown in the following figure:

Figure 6-20 Distribution Schedule Page for the No Schedule Type

The screenshot shows a wizard window titled "Patches" with a sub-header "Step 8: Distribution Schedule". Below the header, it says "Please select the distribution schedule for devices". There is a "Schedule Type:" label followed by a dropdown menu currently showing "No Schedule". At the bottom of the window, there are three buttons: "<< Back", "Next >>", and "Cancel".

In this page, you can directly schedule distribution after completing the remaining steps in the Deployment Remediation Wizard.



Distribution Schedule: Date Specific



When you select **Date Specific**, the Distribution Schedule page appears as shown in the following figure:

Figure 6-21 Distribution Schedule Page for the Date Specific Schedule Type

The screenshot shows a wizard window titled "Patches" with a sub-header "Step 8: Distribution Schedule". Below the header, it says "Please select the distribution schedule for devices". There is a "Schedule Type:" label followed by a dropdown menu currently showing "Date Specific". Below this, there is a large rectangular area containing several options: "Start Date(s):" with a text box and a calendar icon; two checkboxes, "Run event every year" and "Process immediately if device unable to execute on schedule"; a section titled "Select when schedule execution should start:" with two radio buttons, "Start immediately at Start Time" (which is selected) and "Start at a random time between Start and End Times"; "Start Time:" and "End Time:" labels followed by time selection dropdowns (1:00); and a checkbox "Use Coordinated Universal Time (Current UTC 10:19 AM)". At the bottom of the window, there are three buttons: "<< Back", "Next >>", and "Cancel".

Use this page to set the following deployment options:

- ♦ **Start Date:** Enables you to pick the date when you need to start the distribution. To do so, click the  icon to open the calendar and pick the date. To remove the selected date, click the  icon.
- ♦ **Run event every year:** Ensures that the distribution starts on a selected date at a selected time, repeats every year, and if defined, ends on a specific date.
- ♦ **Process immediately if device unable to execute on schedule:** Ensures that the distribution starts immediately if the device could not execute on the selected schedule.
- ♦ **Select when schedule execution should start:** There are two options to enable you to select the start time of the schedule execution namely:
 - ♦ **Start immediately at Start Time:** Deactivates the **End Time** panel and starts the distribution at the start time specified. In this option, you must set the start time in the **Start Time** panel:

Start Time:  : 

- ♦ **Start at a random time between Start Time and End Times:** Activates the **End Time** panel next to the **Start Time** panel. You can specify the end time and the start time so that the distribution occurs at a random time between them. The **End Time** panel appears as follows:

End Time:  : 

In both time panels, the first drop-down list enables you to select the hour, the second drop-down list enables you to select the minute, and the third drop-down list enables you to select **am** and **pm**.

Selecting the **Use Coordinated Universal Time** check box enables you to schedule the distribution to all devices at the same time, regardless of time zone differences. Coordinated Universal Time (UTC), also known as World Time, Z Time, or Zulu Time, is a standardized measurement of time that is not dependent upon the local time zone. Deselecting UTC schedules the distribution at the local time.

Distribution Schedule: Recurring

When you select **Recurring**, the Distribution Schedule page appears as shown in the following figure:

Figure 6-22 Distribution Schedule Page for the Recurring Schedule Type

The screenshot shows the 'Schedule Vulnerability Check' window. At the top, there are two radio buttons: 'Check for vulnerabilities on device refresh' and 'Check for vulnerabilities on a schedule'. The 'Schedule Type' dropdown is set to 'Recurring'. Below this, there are three main sections: 'When a device is refreshed', 'Days of the week', and 'Monthly'. The 'When a device is refreshed' section is selected, showing a checkbox for 'Delay execution after refresh' with input fields for 0 Days, 0 Hours, and 0 Minutes. The 'Days of the week' section has a table with checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, and Sat. The 'Monthly' section has three options: 'Day of the month' (set to 1), 'Last day of the month', and 'First' (set to Sunday). Each section has a 'Start Time' dropdown set to 1:00 and a 'More Options' link.

In this page, you can set the following options for a recurring deployment:

- ♦ “When a Device Is Refreshed” on page 113
- ♦ “Days of the Week” on page 114
- ♦ “Monthly” on page 115
- ♦ “Fixed Interval” on page 116

When a Device Is Refreshed

This option enables you to schedule a recurring distribution whenever the device is refreshed. In this option, you can choose to delay the next distribution until after a specific time.

To set the delay, select the **Delay execution after refresh** check box as shown in the following image, and specify the days, hours, and minutes of the time to delay the distribution:

Figure 6-23 Delay Execution After Refresh Check Box

The close-up shows the 'Delay execution after refresh' checkbox checked. To its right are input fields for 0 Days, 0 Hours, and 0 Minutes.

NOTE: The device is refreshed based on the settings in the **Device Management** tab under the **Configuration** tab. Click the **Device Refresh Schedule** link under the **Device Management** tab to open the page displaying the option for either a **Manual Refresh** or **Timed Refresh**. Alternatively, you can refresh the device by selecting a device under the **Devices** tab and clicking the **Refresh Device** option under the **Quick Tasks** menu.

Days of the Week

This option enables you to schedule the distribution on selected days of the week:

Figure 6-24 Weekly Distribution Options - Default

☒ Days of the week

*

Sun	Mon	Tue	Wed	Thu	Fri	Sat
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Time: :

[More Options](#)

- ♦ To set the day of distribution, select the **Days of the week** button, select the required day of the week, and set the start time of distribution.

If you click the **More Options** link, additional distribution options appear as shown in the following figure. Click the **Hide Options** link to hide the additional distribution options and show only the default distribution options:

☒ Days of the week

*

Sun	Mon	Tue	Wed	Thu	Fri	Sat
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Time: :

[Hide Options](#)

☐ Process immediately if device unable to execute on schedule

☐ Use Coordinated Universal Time (Current UTC 8:19 AM)

☐ Start at a random time between Start and End Times

End Time: :


☐ Restrict schedule execution to the following date range:

Start Date:

End Date:

Selecting the **Use Coordinated Universal Time** check box enables you to schedule the distribution to all devices at the same time, regardless of time zone differences. Coordinated Universal Time (UTC), also known as World Time, Z Time, or Zulu Time, is a standardized measurement of time that is not dependent upon the local time zone. Deselecting UTC schedules the distribution at local time.

Selecting the **Start at a random time between Start Time and End Times** check box activates the **End Time** panel in addition to the **Start Time** panel. You can specify the end time and the start time so that the distribution occurs at any random time between the start and end times.

The **Restrict schedule execution to the following date range** option enables you to schedule a recurring distribution at the selected time, repeat the distribution on the days specified, and, if defined, end at the specific time. This option also enables you to restrict the distribution to the period between the start date and the end date. To set this option, select the **Restrict schedule execution to the following date range** check box and click the  icon to open the calendar and pick a start date or end date. Click the **Close** button when you have finished selecting the date.

Monthly

This option enables you to specify the monthly distribution options:

Figure 6-25 Monthly Distribution Options – Default

☒ **Monthly**

☒ Day of the month:

☐ Last day of the month

☐

Start Time: :

[More Options](#)

- ◆ In the **Monthly** distribution option, you can specify the following:
 - ◆ **Days of the month:** Enables you to schedule the distribution on a specific day of the month. You can specify any number between 1 and 31.
 - ◆ **Last day of the month:** Enables you to schedule the distribution on the last day of the month.
 - ◆ **Particular days of the month:** Enables you to schedule the distribution on specific days of every month. The valid options for the day are first, second, third, fourth, and fifth. The valid options for the weekday are Sunday through Saturday. To select one particular day of the month, use the drop-down arrows. An example is shown as follows.

☒

To select an additional day of the month, click the icon and use the drop-down arrows in the second row shown as follows.

☒

NOTE: To remove a particular day from the list, click the icon.

If you click the **More Options** link, additional distribution options appear as shown in the following figure. Clicking the **Hide Options** link hides the additional distribution options and shows only the default distribution options:

☒ **Monthly**

☒ Day of the month:

☐ Last day of the month

☐ First

Start Time: :

[Hide Options](#)

☐ Process immediately if device unable to execute on schedule

☐ Use Coordinated Universal Time (Current UTC 8:19 AM)

☐ Start at a random time between Start and End Times

End Time: :

☒ Restrict schedule execution to the following date range:

Start Date:

End Date:

NOTE: The **Restrict schedule execution to the following date range** option enables you to schedule a recurring distribution at the selected time, repeat the distribution on the days specified, and, if defined, end on the specific time. This option also enables you to restrict the distribution to the period between the **Start Date** and the **End Date**. To set this option, select the **Restrict schedule execution to the following date range** check box and click the icon to open the calendar and pick a start date or end date. Click the **Close** button when you have finished selecting the date.

Fixed Interval

This option enables you to schedule a recurring distribution that runs after a fixed duration on a regular basis. You can choose the number of months, weeks, days, hours, and minutes of the interval and the start date for the distribution schedule, as shown in the following figure:

Figure 6-26 Fixed Interval Distribution Options - Default

☒ **Fixed Interval**

Months Weeks Days Hours Minutes

Start Date: Start Time: :

[More Options](#)

If you click the **More Options** link, additional distribution options appear as shown in the following figure. Clicking the **Hide Options** link hides the additional distribution options and shows only the default distribution options:

Figure 6-27 *Fixed Interval Distribution Options - All*

Fixed Interval

0 Months 0 Weeks 0 Days 0 Hours 0 Minutes

Start Date: 10/25/2011 Start Time: 1:00

[Hide Options](#)

☐ Process immediately if device unable to execute on schedule

☐ Use Coordinated Universal Time

☐ Restrict schedule execution to the following date range:

End Date: 10/25/2011 End Time: 1:00 (Current UTC 8:19 AM)

Click the **Next** button to open the Notification and Reboot Options page. Click the **Back** button to return to the previous page. Click **Cancel** to exit the wizard.

Notification and Reboot Options

The Notification and Reboot Options page of the Deploy Remediation Wizard allows you to define whether users receive notification of patch deployments and reboots, and to customize the notification. Setting the notification and reboot options is the ninth step in scheduling a deployment for a selected patch.

Figure 6-28 Notification and Reboot Options Page

Patches

Step 9: Notification and Reboot Options

Select Notification and Reboot Options

Define Reboot Options

☒ Use values assigned to system variables or defaults
☐ Override Settings

☒ Notify Users

Description Text

To complete the installation of patches on your computer, it is now necessary to reboot. If you require any additional information, please contact your Novell ZENworks Patch Management administrator.

Options	Yes	No
Suppress reboot	<input type="radio"/>	<input checked="" type="radio"/>
Allow user to cancel	<input type="radio"/>	<input checked="" type="radio"/>
Allow user to snooze	<input checked="" type="radio"/>	<input type="radio"/>

Snooze interval: 10 Minutes

Reboot within: 2 Hours

Show tray notification: ☐ ☒

Tray notification duration: 20 Seconds

Tray notification text

Important patches have been installed. In order for these patches to be applied a reboot is required. Please click here to reboot now.

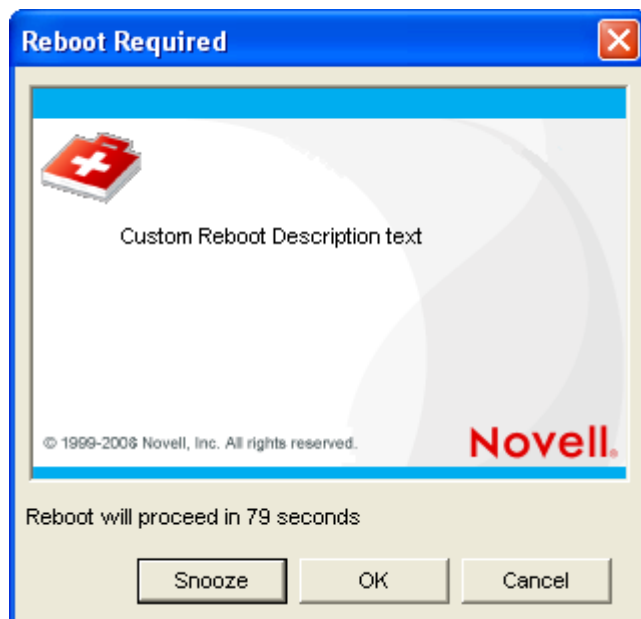
<< Back Next >> Cancel

The page provides the following options:

- ♦ **Define Reboot Options:** Allows you to use the default reboot options you've set in options or override them and set them manually for the deployment.
 - ♦ **Use values assigned to system variables or defaults:** Uses reboot options set for deployments.
 - ♦ **Override Settings:** Overrides the default reboot settings and lets you choose from the options below.
- ♦ **Notify Users:** Select this option to notify the user prior to a reboot required for installation of the patch.

- ♦ **Description Text:** The text of the message that appears before patch installation completes and the computer reboots. You can edit this field only if you override the default settings.
- ♦ **Options:** When you define reboot options, you can specify whether to use the values in the default settings (the **Use values assigned to system variables or defaults** check box) or the custom settings. There are four options:
 - ♦ **Suppress Reboot:** If a patch requires a reboot by default, and no reboot is desired, select the **Suppress Reboot** option to stop this action. This will prevent a reboot after installation.
 - ♦ **Allow User to cancel:** On selecting this option, the user is allowed to cancel the reboot option.
 - ♦ **Allow User to snooze:** On selecting this option, the user is allowed to snooze (pause) the reboot for a particular time.
 - ♦ **Snooze interval:** The amount of time before a user is prompted again to reboot after snoozing.
 - ♦ **Reboot within:** The amount of time before a user is forced to reboot for the deployment.
 - ♦ **Show tray notification:** On selecting this option, a notification for a pending reboot is displayed in the system tray. If you select this option, define the following options
 - ♦ **Tray notification duration:** Option to select how long the system tray notification is displayed before being hidden.
 - ♦ **Tray notification text:** Option for text that appears in the notification.

A description text will be displayed when a reboot is required, as shown in the figure below.



- ♦ **Options:** When defining reboot options, you can specify whether to use the values in the default settings (the **Use values assigned to system variables or defaults** check box) or in the custom settings. There are three options:
 - ♦ **Snooze:** Prevents a reboot even if the patch bundle requires a reboot. The notification will continue to appear occasionally until the reboot occurs.
 - ♦ **OK:** Proceeds with the reboot. Be sure to tell users to save their work before rebooting.
 - ♦ **Cancel:** Completely cancels the reboot.

Click the **Next** button to proceed to the Deployment Summary page. Click the **Back** button to return to the previous page. Click **Cancel** to exit the wizard.

11.3 New variables

The following is a list of the system variables which can be used through the console. These are the calls made to set the defaults. Each Variable has the variable name and the default setting. The values can be set by the user depending on their requirements.

- **ConfigManager.SetDefaultConfigValue(PATCH_MANDATORY_NOTIFY_REBOOT_REBOOT_TIMEOUT, "7200");** Time to do prompts before rebooting In Seconds
- **ConfigManager.SetDefaultConfigValue(PATCH_MANDATORY_NOTIFY_REBOOT_POPUP_SHOW_TRAY, "true");** Whether to show the popup in the corner.
- **ConfigManager.SetDefaultConfigValue(PATCH_MANDATORY_NOTIFY_REBOOT_POPUP_DURATION, "20");** How long to display the popup. In seconds.
- **ConfigManager.SetDefaultConfigValue(PATCH_MANDATORY_NOTIFY_REBOOT_SNOOZE_INTERVAL, "600");** The time to wait before showing popup again. In seconds.
- **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_REBOOT_REBOOT_TIMEOUT, "7200");** The time to wait before the system notifies a time out, In seconds.
- **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_REBOOT_POPUP_SHOW_TRAY, "true");** The value indicates whether or not the system will show a popup before reboot.
- **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_REBOOT_POPUP_DURATION, "20");** This value indicates the length of time for the popup to remain.
- **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_REBOOT_SNOOZE_INTERVAL, "600");** The value sets the length of time for the snooze interval before reboot prompt. In seconds.
- **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_INSTALL_REBOOT_TIMEOUT, "7200");** The value shows the amount of time before the system reboots after an install timeout. In Seconds.
- **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_INSTALL_POPUP_SHOW_TRAY, "true");** The value determines whether a popup appears to notify of install.
- **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_INSTALL_POPUP_DURATION, "20");** This value sets the length of time that the popup will show for on install. In seconds.
- **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_INSTALL_SNOOZE_INTERVAL, "600");** The value sets the length of time for the snooze interval after install. In seconds.

The following are no longer used:

- PATCH_NOTIFY_REBOOT_SNOOZE_TIMETOLIVE
- PATCH_NOTIFY_REBOOT_DIALOG_TIMEOUT
- PATCH_NOTIFY_INSTALL_SNOOZE_TIMETOLIVE
- PATCH_NOTIFY_INSTALL_DIALOG_TIMEOUT
- PATCH_MANDATORY_NOTIFY_ALLOW_SNOOZE
- PATCH_MANDATORY_NOTIFY_DIALOG_TIMEOUT
- PATCH_MANDATORY_NOTIFY_DIALOG_TIMEOUT_ENABLED
- PATCH_MANDATORY_NOTIFY_SNOOZE_HOURS

- ♦ PATCH_MANDATORY_NOTIFY_SNOOZE_MINUTES
- ♦ PATCH_MANDATORY_NOTIFY_SNOOZE_DAYS

Choose Deployment Name

The Choose Deployment Name of the Deploy Remediation Wizard lets you customize the name of the deployment you have scheduled. Setting a deployment name is the tenth step in scheduling a deployment for a selected patch.

Figure 6-29 Choose Deployment Name Page

Patches

Step 10: Choose deployment name

Creates deployment using the name chosen here

Deployment Name *

Folder: *

/Bundles/ZPM

Description:

Fields marked with an asterisk are required.

<< Back Next >> Cancel

The page provides the following options:

- ♦ **Deployment Name:** The name you give to the deployment.
- ♦ **Folder:** The location where the deployment is saved. The default location is /Bundles/ZPM.
- ♦ **Description:** The description of the scheduled deployment.

Deployment Summary

The Deployment Summary page of the Deploy Remediation Wizard displays the summary of the deployment you have scheduled in the previous steps. Summarizing the important points of the deployment is the last step in scheduling a deployment for a selected patch.

Figure 6-30 Deployment Summary Page

Patches

Step 11: Deployment Summary

Please review summary and then press finish.

Property Name	Details
Deployment Name	AdobePatch
Delviery Schedule	No Schedule
Deployment Schedule	Now
Total selected packages	2

Order	Package Name	Reboot
1	Adobe Flash Player 10.2.152.26 (Other Browsers) for Windows (Full/Upgrade) (All Languages)	No

<< Back

Finish

Cancel

The Deployment Summary page displays the following details about the deployment you have scheduled:

- ◆ **Deployment Name:** The name of the deployment as defined on the Choose Deployment Name page.
- ◆ **Delivery Schedule:** The schedule selected for distribution of patches as defined on the Distribution Schedule page.
- ◆ **Deployment Schedule:** The schedule selected for the deployments as defined on the Remediation Schedule page.
- ◆ **Total Selected Packages:** The total number of patches selected for deployment.
- ◆ **Order:** The order of deployment of the patches as defined on the Deployment Order and Behavior page.
- ◆ **Package Name:** The name of the patch you have selected for deployment.
- ◆ **Reboot:** The reboot setting of the selected patch as defined in the Deployment Order and Behavior page.

Click the **Finish** button to complete the process of scheduling the deployment of a selected patch. Click the **Back** button to return to the previous page. Click **Cancel** to exit the wizard.

7 Using Mandatory Baselines

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

- ♦ [“About Mandatory Baselines” on page 123](#)
- ♦ [“Working with Mandatory Baselines” on page 128](#)

About Mandatory Baselines

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

IMPORTANT: Mandatory baselines are an automatic enforcement method based on the most recent discovery scan results, so there is no control over the deployment time or order for patches applied in this manner. Unless a stringent Content Blackout Schedule is in effect, do not apply mandatory baselines to groups of mission-critical servers or other devices where unscheduled patch deployments would disrupt daily operations.

The Content Blackout Schedule panel lets you define times when content (bundles, policies, configuration settings, etc.) will not be delivered to the devices.

When a mandatory baseline is created or modified:

- ♦ The ZENworks Server automatically schedules a daily Vulnerability Detection task for all devices in that group.
- ♦ Every few hours, depending on the results of the Vulnerability Detection task, the ZENworks Server determines the devices that are applicable and out of compliance (based upon the patches added to the baseline).
- ♦ Necessary bundles, as defined in the baseline, are then deployed as soon as possible for each device.
- ♦ After patches have been deployed, it might be necessary to reboot those devices for them to be detected as patched.

The baseline function does not auto-reboot devices that have been patched.

NOTE: Some patches, such as MDAC and IE, require both a reboot and an administrator level login to complete. If these or similar patches are added to a baseline, the deployment stops until the login occurs.

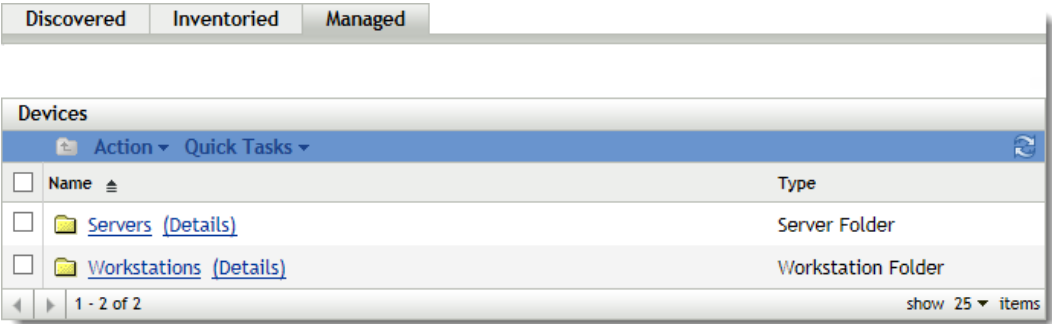
The following sections provide more information on mandatory baselines:

- ♦ [“Viewing Mandatory Baselines” on page 124](#)
- ♦ [“Using the Mandatory Baseline Page” on page 127](#)

Viewing Mandatory Baselines

- 1 Click the **Devices** tab in the left panel.





















A page displaying the root folders for each type of device appears, as shown in the following figure:



The **Servers** folder is the root folder for all managed servers and the **Workstations** folder is the root folder for all managed workstations in the network.

- 2 Click the **Servers** or **Workstations** link.

A list of server or workstation groups classified on the basis of their operating systems appears. The following figure shows a list of server groups:

Devices						
New Edit Delete Action Quick Tasks Export						
<input type="checkbox"/>	Status	Name	Type	Operating System	Last Contact	Retired
<input type="checkbox"/>		 Apple OS X 10.10 Server (Yosemite)	Dynamic Server Group			
<input type="checkbox"/>		 Apple OS X 10.8 Server (Mountain Lion)	Dynamic Server Group			
<input type="checkbox"/>		 Apple OS X 10.9 Server (Mavericks)	Dynamic Server Group			
<input type="checkbox"/>		 Open Enterprise Server 11	Dynamic Server Group			
<input type="checkbox"/>		 Open Enterprise Server 2	Dynamic Server Group			
<input type="checkbox"/>		 Red Hat Enterprise Linux Server 4	Dynamic Server Group			
<input type="checkbox"/>		 Red Hat Enterprise Linux Server 5	Dynamic Server Group			
<input type="checkbox"/>		 Red Hat Enterprise Linux Server 6	Dynamic Server Group			
<input type="checkbox"/>		 Red Hat Enterprise Linux Server 7	Dynamic Server Group			
<input type="checkbox"/>		 server	Server Group			
<input type="checkbox"/>		 SUSE Linux Enterprise Server 10	Dynamic Server Group			
<input type="checkbox"/>		 SUSE Linux Enterprise Server 11	Dynamic Server Group			
<input type="checkbox"/>		 SUSE Linux Enterprise Server 12	Dynamic Server Group			
<input type="checkbox"/>		 Windows Server 2003	Dynamic Server Group			
<input type="checkbox"/>		 Windows Server 2008	Dynamic Server Group			
<input type="checkbox"/>		 Windows Server 2008 R2	Dynamic Server Group			
<input type="checkbox"/>		 Windows Server 2012	Dynamic Server Group			
<input type="checkbox"/>		 Windows Server 2012 R2	Dynamic Server Group			
<input type="checkbox"/>		 az-tp-win2008r2	Server	win2008r2-ee-sp1-x64	4:05 AM	
1 - 19 of 19						show 25 items

- 3 On the Servers or Workstation page (in this case, it is the Servers page), select any group.

A page displaying the general details of the group and the members in the group appears. The following figure shows such a page that appears when a Dynamic Server Group called **Windows Server 2008 R2** is selected:

The screenshot shows the Zenworks interface for the 'Windows Server 2008 R2' group. The breadcrumb navigation at the top reads 'Devices > Servers > Windows Server 2008 R2'. Below the title bar, there are tabs for 'Summary', 'Relationships', 'Details', 'Audit', and 'Patches'. The 'Summary' tab is active, displaying the following information:

- General**
 - Object type: Dynamic Server Group
 - GUID: 677c3c2dca7cfd30c1cabf5315ada028
 - Description: [\(Edit\)](#) Windows Server 2008 R2 Group
- Members**

Name	In Folder
az-tp-win2008r2	/Devices/Servers

1 - 1 of 1 items
- Members Change Log**

Date	Added	Removed
Mar 21	1	0

1 - 1 of 1 items

- 4 Click the **Patches** tab.

The patches applicable to the member devices of the selected group are displayed. If the selected group is **Windows Server 2008 R2**, the **Patches** tab displays all the patches applicable to the member devices within the group **Windows Server 2008 R2**, as shown in the following figure:

Windows Server 2008 R2

Summary Relationships Details Audit Patches

Patches

Action	Patch Name	Impact	Patched	Not Patched	Released On
	Update for Windows Server 2008 R2 x64 (KB2990214)	Recommended	0	1	Apr-14-2015
	MS15-032 Cumulative Security Update for Internet Explorer 8 for Windows Server 2008 R2 x64 (KB3038314)	Critical	0	1	Apr-14-2015
	MS15-038 Security Update for Windows Server 2008 R2 x64 (KB3045999)	Critical	0	1	Apr-14-2015
	MS15-041 Security Update for .NET Framework 4 on Win 2003, Vista, Win 7, Server 2008, Server 2008 R2 x64 (KB3037578)	Critical	0	1	Apr-14-2015
	MS15-035 Security Update for Windows Server 2008 R2 x64 (KB3046306)	Critical	0	1	Apr-14-2015
	Windows Malicious Software Removal Tool x64 - April 2015 (KB890830)	Software Installer	0	1	Apr-14-2015
	MS15-038 Security Update for Windows Server 2008 R2 x64 (KB3045685)	Critical	0	1	Apr-14-2015
	MS15-037 Security Update for Windows Server 2008 R2 x64 (KB3046269)	Critical	0	1	Apr-14-2015

Search

Patch Name

Search Reset

Status

☐ Patched

☒ Not Patched

☐ Not Applicable

☐ Include Disabled

Impact

☒ Critical

☒ Recommended

☒ Informational

☒ Software Installers

Vendor All

Cache Status All

CVE Identifier

Mandatory Baseline

☒ All Patches

☐ Baseline Only

A patch that has been assigned to the baseline (also called the mandatory baseline patch) has the icon displayed next to its name, as shown in the above figure.

Alternatively, you can view the baseline patches by using the **Search** panel on the Patches page to search for mandatory baseline patches.

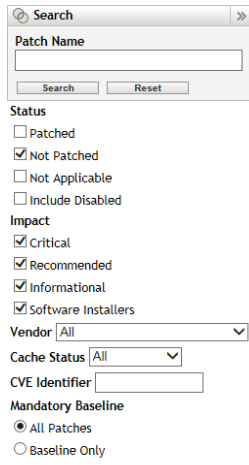
For detailed information on **Patches** and **Patches Information** panels, refer to [Chapter 5, “Using the Patch Management Tab,”](#) on page 67.

Using the Mandatory Baseline Page

You can use the **Search** panel on the Mandatory Baseline page to view the baseline patches.

The **Search** panel on the Device Group Patches page, as shown in [Figure 7-1](#), enables you to search for mandatory baseline patches. The **Search** panel also enables you to search for other patches based on the status and impact of the patches.

Figure 7-1 Mandatory Baseline Search

The screenshot shows a 'Search' dialog box with a 'Patch Name' text field at the top, followed by 'Search' and 'Reset' buttons. Below these are several filter sections: 'Status' with checkboxes for 'Patched', 'Not Patched' (checked), 'Not Applicable', and 'Include Disabled'; 'Impact' with checkboxes for 'Critical' (checked), 'Recommended' (checked), 'Informational' (checked), and 'Software Installers' (checked); a 'Vendor' dropdown menu set to 'All'; a 'Cache Status' dropdown menu set to 'All'; a 'CVE Identifier' text field; and a 'Mandatory Baseline' section with radio buttons for 'All Patches' (selected) and 'Baseline Only'.

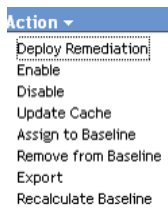
You can search for the mandatory baseline patches based on the following filter options:

- ♦ **All Patches:** Displays all patches, including mandatory baseline items.
- ♦ **Baseline Only:** Displays only those patches that are marked as “mandatory baseline” for the group.

Working with Mandatory Baselines

The **Action** menu on the Device Group Patches page enables you to perform various actions concerning mandatory baseline patches. The **Action** menu options also assist you in managing and deploying patches in a consistent and uniform manner across groups. The following figure shows the various menu options that help you work with mandatory baselines:

Figure 7-2 Action Menu Items



- ♦ The **Deploy Remediation** option enables you to deploy a patch. To use this option, select the check boxes for the patches you want to deploy and select **Deploy Remediation** from the **Action** menu options to open the Deploy Remediation Wizard.
- ♦ The **Enable** option allows you to enable a disabled patch.
- ♦ The **Disable** option enables you to disable a patch. To use this option, select the check box for the required patch and select **Disable**. The selected patch is removed from the list.
- ♦ The **Update Cache** option initiates a download process for the bundles associated with a selected patch and caches those bundles on your ZENworks Server. See [“Using Update Cache” on page 134](#).
- ♦ The **Assign to Baseline** option enables you to assign a baseline to a patch. For more information, see [“Assigning or Managing a Mandatory Baseline” on page 129](#).

- ♦ The **Remove from Baseline** option enables you to remove a patch from a baseline. See [“Removing a Mandatory Baseline” on page 132](#) for more information.
- ♦ The **Export** option enables you to export details such as the status and impact of selected patches into a comma-separated value (CSV) file. You can choose to save the file in a different file format after opening it from the download option.
- ♦ The **Recalculate Baseline** option enables you to start the thread that normally runs automatically about every four hours, which, in turn, creates baseline deployments to the relevant devices without waiting for four hours.

The following sections provide more information on mandatory baselines:

- ♦ [“Assigning or Managing a Mandatory Baseline” on page 129](#)
- ♦ [“Removing a Mandatory Baseline” on page 132](#)
- ♦ [“Using Update Cache” on page 134](#)

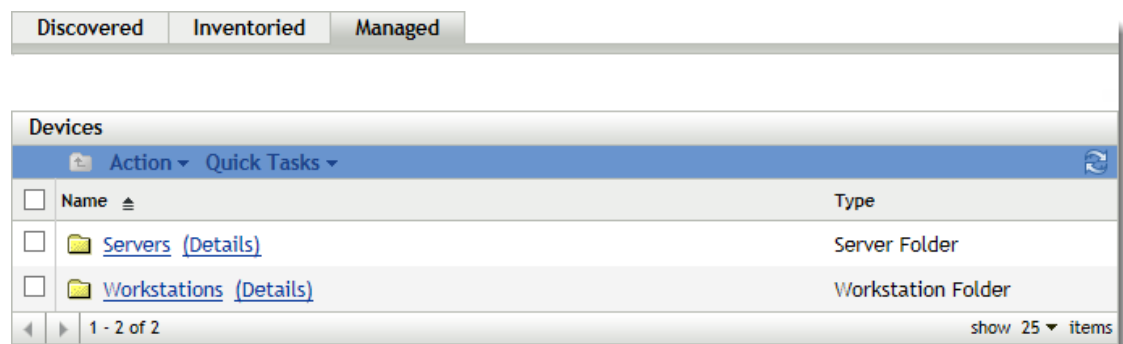
Assigning or Managing a Mandatory Baseline

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

To create or manage a mandatory baseline:

- 1 Click the **Devices** tab in the left panel.

A page displaying the root folders for each type of device appears, as shown in the following figure:



The **Servers** folder is the root folder for all managed servers and the **Workstations** folder is the root folder for all managed workstations in the network.

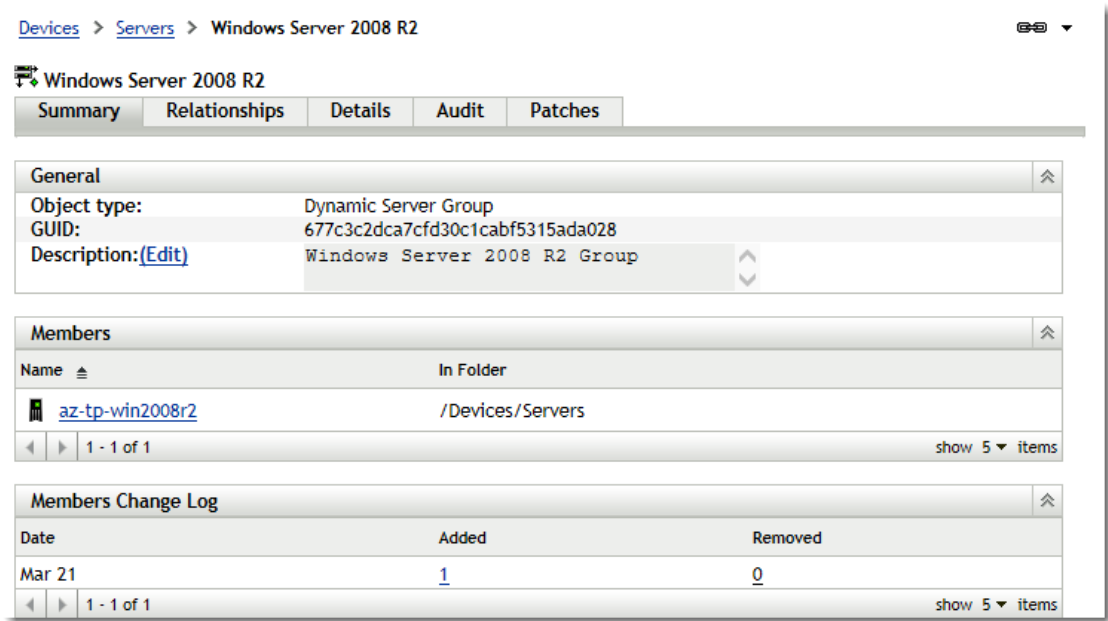
- 2 Click the **Servers** or **Workstations** link.

A list of server or workstation groups classified on the basis of their operating systems appears. The following figure shows a list of server groups:

Devices						
New ▾ Edit ▾ Delete Action ▾ Quick Tasks ▾ Export ▾						
<input type="checkbox"/>	Status	Name	Type	Operating System	Last Contact	Retired
<input type="checkbox"/>		Apple OS X 10.10 Server (Yosemite)	Dynamic Server Group			
<input type="checkbox"/>		Apple OS X 10.8 Server (Mountain Lion)	Dynamic Server Group			
<input type="checkbox"/>		Apple OS X 10.9 Server (Mavericks)	Dynamic Server Group			
<input type="checkbox"/>		Open Enterprise Server 11	Dynamic Server Group			
<input type="checkbox"/>		Open Enterprise Server 2	Dynamic Server Group			
<input type="checkbox"/>		Red Hat Enterprise Linux Server 4	Dynamic Server Group			
<input type="checkbox"/>		Red Hat Enterprise Linux Server 5	Dynamic Server Group			
<input type="checkbox"/>		Red Hat Enterprise Linux Server 6	Dynamic Server Group			
<input type="checkbox"/>		Red Hat Enterprise Linux Server 7	Dynamic Server Group			
<input type="checkbox"/>		server	Server Group			
<input type="checkbox"/>		SUSE Linux Enterprise Server 10	Dynamic Server Group			
<input type="checkbox"/>		SUSE Linux Enterprise Server 11	Dynamic Server Group			
<input type="checkbox"/>		SUSE Linux Enterprise Server 12	Dynamic Server Group			
<input type="checkbox"/>		Windows Server 2003	Dynamic Server Group			
<input type="checkbox"/>		Windows Server 2008	Dynamic Server Group			
<input type="checkbox"/>		Windows Server 2008 R2	Dynamic Server Group			
<input type="checkbox"/>		Windows Server 2012	Dynamic Server Group			
<input type="checkbox"/>		Windows Server 2012 R2	Dynamic Server Group			
<input type="checkbox"/>		az-tp-win2008r2	Server	win2008r2-ee-sp1-x64	4:05 AM	
1 - 19 of 19						show 25 items

- On the Servers or Workstation page (in this case, it is the Servers page), select any group.

A page displaying the general details of the group and the members in the group appears. The following figure shows such a page that appears when a Dynamic Server Group called **Windows Server 2008 R2** is selected:



- 4 Select the required patch and choose **Assign to Baseline** from the **Action** menu. An icon appears next to the patch, indicating that it has been assigned to the baseline.

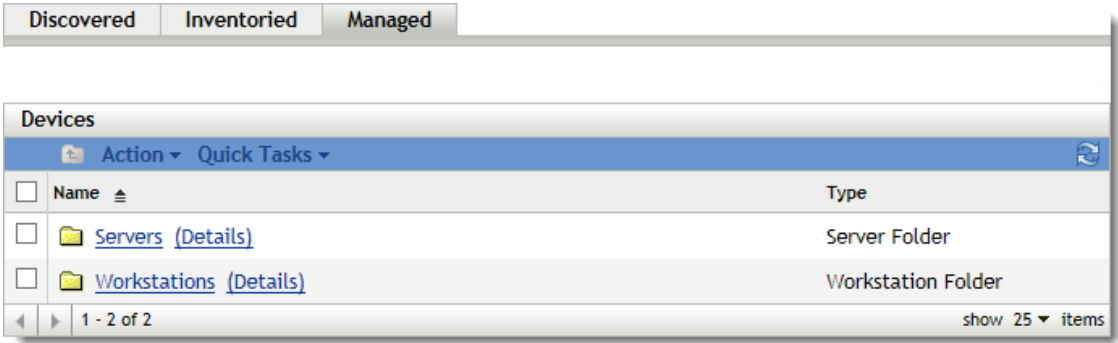
After a patch has been assigned to the baseline, the following process takes place:

1. The ZENworks Server automatically schedules a daily Discover Applicable Updates task for all devices in that group.
2. Every few hours, depending on the results of the Vulnerability Detection task, the ZENworks Server determines the devices that are applicable and out of compliance (based upon the patches added to the baseline).
3. Necessary bundles, as defined in the baseline, are deployed as soon as possible for each device.
4. After patches have been deployed, it might be necessary to reboot those devices for them to be detected as patched.

NOTE: The baseline function does not auto-reboot devices that have been patched.

Removing a Mandatory Baseline

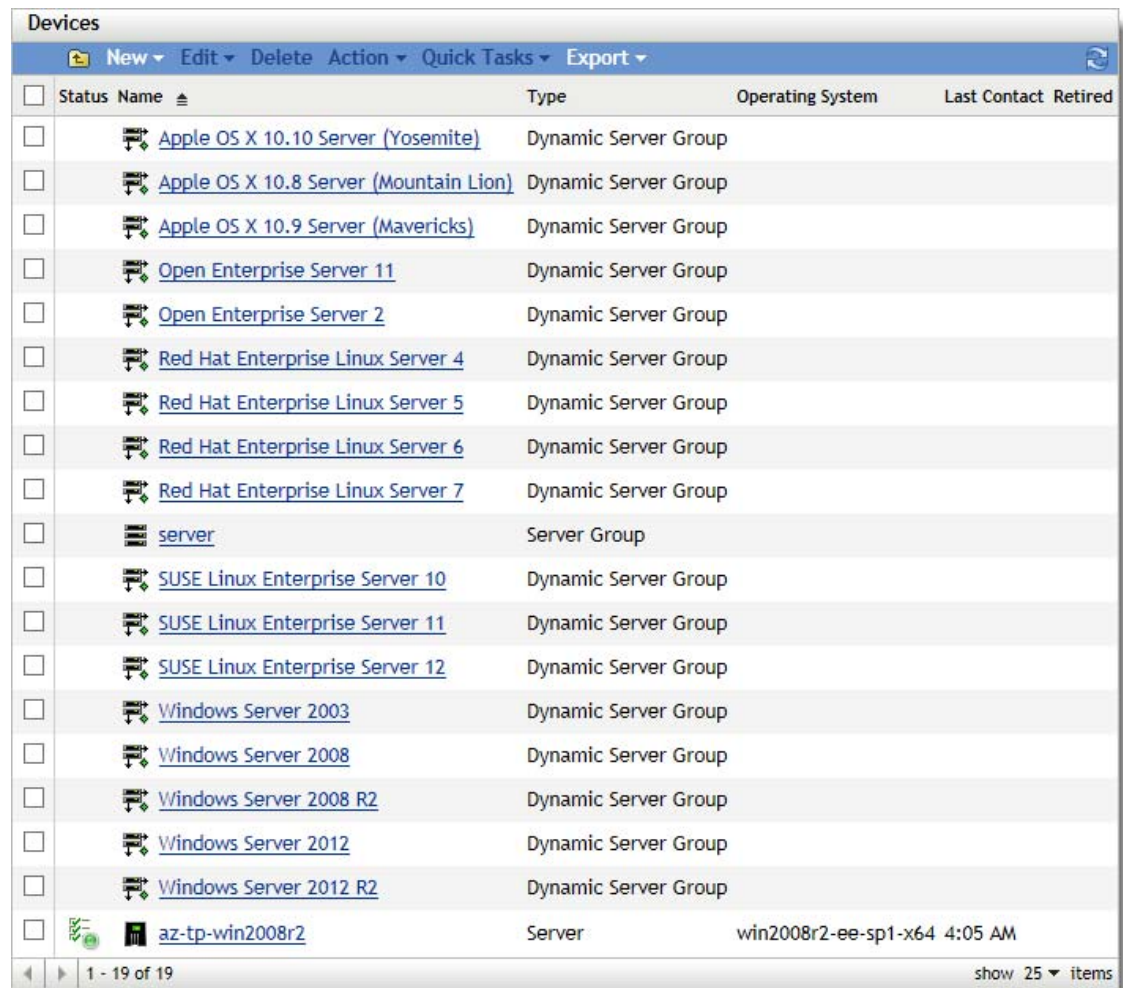
- 1 Click the **Devices** tab in the left panel to display the Devices page, which shows the root folders for each type of device:























The **Servers** folder is the root folder for all managed servers and the **Workstations** folder is the root folder for all managed workstations in the network.

2 Click the **Servers** or **Workstations** link.

A list of server or workstation groups classified on the basis of their operating systems appears. The following figure shows a list of server groups:

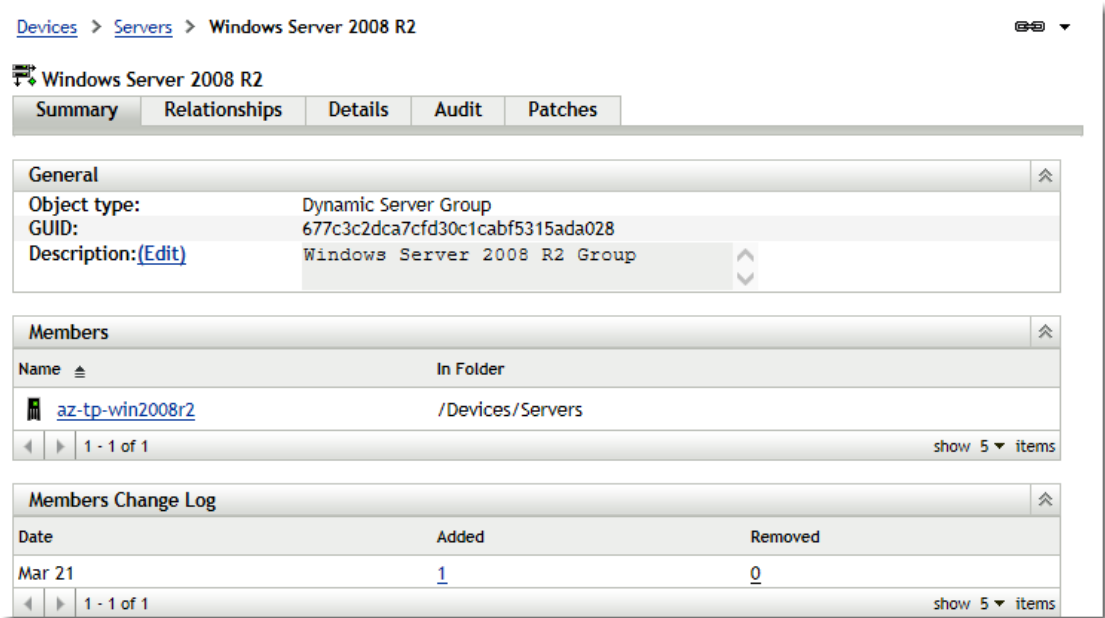


<input type="checkbox"/>	Status	Name	Type	Operating System	Last Contact	Retired
<input type="checkbox"/>		 Apple OS X 10.10 Server (Yosemite)	Dynamic Server Group			
<input type="checkbox"/>		 Apple OS X 10.8 Server (Mountain Lion)	Dynamic Server Group			
<input type="checkbox"/>		 Apple OS X 10.9 Server (Mavericks)	Dynamic Server Group			
<input type="checkbox"/>		 Open Enterprise Server 11	Dynamic Server Group			
<input type="checkbox"/>		 Open Enterprise Server 2	Dynamic Server Group			
<input type="checkbox"/>		 Red Hat Enterprise Linux Server 4	Dynamic Server Group			
<input type="checkbox"/>		 Red Hat Enterprise Linux Server 5	Dynamic Server Group			
<input type="checkbox"/>		 Red Hat Enterprise Linux Server 6	Dynamic Server Group			
<input type="checkbox"/>		 Red Hat Enterprise Linux Server 7	Dynamic Server Group			
<input type="checkbox"/>		 server	Server Group			
<input type="checkbox"/>		 SUSE Linux Enterprise Server 10	Dynamic Server Group			
<input type="checkbox"/>		 SUSE Linux Enterprise Server 11	Dynamic Server Group			
<input type="checkbox"/>		 SUSE Linux Enterprise Server 12	Dynamic Server Group			
<input type="checkbox"/>		 Windows Server 2003	Dynamic Server Group			
<input type="checkbox"/>		 Windows Server 2008	Dynamic Server Group			
<input type="checkbox"/>		 Windows Server 2008 R2	Dynamic Server Group			
<input type="checkbox"/>		 Windows Server 2012	Dynamic Server Group			
<input type="checkbox"/>		 Windows Server 2012 R2	Dynamic Server Group			
<input type="checkbox"/>		 az-tp-win2008r2	Server	win2008r2-ee-sp1-x64	4:05 AM	

1 - 19 of 19 show 25 items

- 3 On the Servers or Workstation page (in this case, it is the Servers page), select any group.

A page displaying the general details of the group and the members in the group appears. The following figure shows such a page that appears when a Dynamic Server Group called **Windows Server 2008 R2** is selected:



- 4 Select the mandatory baseline item (the patch that has been assigned to baseline) and select the **Remove from Baseline** option from the **Action** menu.

The patch is removed from the baseline.

NOTE: The **Remove from Baseline** menu option is enabled for a patch only if the patch has been added to the baseline.



Using Update Cache

The **Action** menu **Update Cache** option (see [Figure 7-2 on page 128](#)) initiates a download process for the bundles associated with a selected patch and caches those bundles on your ZENworks Server.

NOTE: The remediation bundles must be cached before they are installed on the target device.

To update caching of patch data:

- 1 In the **Patches** list, select one or more patches.
- 2 In the **Action** menu, click **Update Cache**.

The icon changes to . While the download is in progress, the icon changes to . When the caching is complete, the color of the patch icon changes to green. This indicates that the patch remediation is ready to be deployed.

8 Patch Management for a Device

Device patches are the patches associated with a selected device (a server or a workstation). The patches listed for a specific device are the ones that are applicable only for that device. The following sections describe device patch information for Novell ZENworks 11 SP4 Patch Management:

- ♦ “Accessing the Patches Tab for a Device” on page 135
- ♦ “Using the Patches Tab for a Device” on page 138

Accessing the Patches Tab for a Device

To view the patches for a specific server device:

- 1 Click the **Device** tab on the left panel.


A page displaying the root folders for each type of device appears, as shown in the following figure:







The **Servers** folder is the root folder for all managed servers and the **Workstations** folder is the root folder for all managed workstations.

- 2 Click the **Servers** link.

A list of server groups classified on the basis of their operating systems appears, as shown in the following figure:

Devices						
New Edit Delete Action Quick Tasks Export						
<input type="checkbox"/>	Status	Name	Type	Operating System	Last Contact	Retired
<input type="checkbox"/>		Apple OS X 10.10 Server (Yosemite)	Dynamic Server Group			
<input type="checkbox"/>		Apple OS X 10.8 Server (Mountain Lion)	Dynamic Server Group			
<input type="checkbox"/>		Apple OS X 10.9 Server (Mavericks)	Dynamic Server Group			
<input type="checkbox"/>		Open Enterprise Server 11	Dynamic Server Group			
<input type="checkbox"/>		Open Enterprise Server 2	Dynamic Server Group			
<input type="checkbox"/>		Red Hat Enterprise Linux Server 4	Dynamic Server Group			
<input type="checkbox"/>		Red Hat Enterprise Linux Server 5	Dynamic Server Group			
<input type="checkbox"/>		Red Hat Enterprise Linux Server 6	Dynamic Server Group			
<input type="checkbox"/>		Red Hat Enterprise Linux Server 7	Dynamic Server Group			
<input type="checkbox"/>		server	Server Group			
<input type="checkbox"/>		SUSE Linux Enterprise Server 10	Dynamic Server Group			
<input type="checkbox"/>		SUSE Linux Enterprise Server 11	Dynamic Server Group			
<input type="checkbox"/>		SUSE Linux Enterprise Server 12	Dynamic Server Group			
<input type="checkbox"/>		Windows Server 2003	Dynamic Server Group			
<input type="checkbox"/>		Windows Server 2008	Dynamic Server Group			
<input type="checkbox"/>		Windows Server 2008 R2	Dynamic Server Group			
<input type="checkbox"/>		Windows Server 2012	Dynamic Server Group			
<input type="checkbox"/>		Windows Server 2012 R2	Dynamic Server Group			
<input type="checkbox"/>		az-tp-win2008r2	Server	win2008r2-ee-sp1-x64	1:26 AM	
1 - 19 of 19 show 25 items						

You see the following icons on the Servers page:

Icon	Status
	Message Status: Normal Device Status: Bundle and policy enforcement successful
	Message Status: Warning Device Status: Bundle and policy enforcement successful
	Message Status: Error Device Status: Bundle and policy enforcement successful
	Message Status: Error Device Status: Bundle and/or policy enforcement failed on one or more bundles or policies.

Devices can also be found by searching. The following filters are available:

Filter Item	Result
Name	Searches for devices with a particular name.
Type	Searches for devices of a specific type.
Server Type	Searches for devices based on whether it is a ZCM primary or satellite server.
Operating System	Searches for devices running a particular operating system.
Test Status	Searches for devices based on its ZCM test status.
Message Status	Searches for devices that display a particular message status.
Compliance Status	Searches for devices based on their compliance status, such as Yes or No .
Device Status	Searches for devices based on the device status.
Include subfolders	The search is also executed in the subfolders.

- Click the required group (Server or Dynamic Server Group) to view details of the group and the members of the group. Alternatively, you can click the managed device.

A page displaying details about the managed device or member is displayed, as shown in the following figure, where the name `az-tp-win2008r2` for the managed device is an example. The network administrator decides the name of the managed device.

The screenshot displays the ZENworks management console interface. At the top, there is a navigation bar with tabs: Summary, Inventory, Relationships, Settings, Content, Statistics, Locations, Audit, and Patches. The 'Summary' tab is selected. Below the navigation bar, the 'General' section is expanded, showing various system and configuration details for the device 'az-tp-win2008r2'.

General	
Alias:	az-tp-win2008r2
Host Name:	AZ-TP-WIN2008R2
IP Address:	10.19.0.151
Last Full Refresh:	1:26 AM
Last Contact:	1:26 PM
ZENworks Configuration Management Version:	11.4.0.0
ZENworks Asset Management Version:	11.4.0.2973
ZENworks Patch Management Version:	11.4.0.379
ZENworks EndPoint Security Management Version:	11.4.0.2973
ZENworks Full Disk Encryption Version:	11.4.0.2973
ZENworks Agent Version:	11.4.0.2973
ZENworks Updater Service Version:	11.4.0.2973
ZENworks Agent Status:	
Operating System:	Microsoft Windows Server 2008 R2 SP1 Enterprise x64 Edition 6.1.7601 Service Pack 1 Build 7601
Number of errors not acknowledged:	0
Number of warnings not acknowledged:	0
Primary User:	No user sources configured
Owner:	(Edit)
Serial Number	422f920aa8c346973c42c930b387652c
GUID:	1af8ab908ca4088c670b65a11f85583a
Department:	(Edit)
Site:	(Edit)
Location:	(Edit)

- Click the **Patches** tab to display the patches associated with the server device:

Patches - Last PD time: Mar/31/2015 01:30:09

Action	Patch Name	Impact	Patched	Released On
<input type="checkbox"/>	MS15-028 Security Update for Windows Server 2008 R2 x64 (KB3030377)	Critical	No	Mar-10-2015
<input type="checkbox"/>	MS15-027 Security Update for Windows Server 2008 R2 x64 (KB3002657)	Critical	No	Mar-10-2015
<input type="checkbox"/>	MS15-020 Security Update for Windows Server 2008 R2 x64 (KB3039066)	Critical	No	Mar-10-2015
<input type="checkbox"/>	MS15-031 Security Update for Windows Server 2008 R2 x64 (KB3046049)	Critical	No	Mar-10-2015
<input type="checkbox"/>	MS15-021 Security Update for Windows Server 2008 R2 x64 (KB3032323)	Critical	No	Mar-10-2015
<input type="checkbox"/>	MS15-029 Security Update for Windows Server 2008 R2 x64 (KB3035126)	Critical	No	Mar-10-2015
<input type="checkbox"/>	MS15-018 Cumulative Security Update for Internet Explorer 8 for Windows Server 2008 R2 x64 (KB3032359)	Critical	No	Mar-10-2015

Search

Patch Name

Status

☐ Patched

☒ Not Patched

☐ Not Applicable

☐ Include Disabled

Impact

☒ Critical

☒ Recommended

☒ Informational

☒ Software Installers

Vendor

Cache Status

CVE Identifier

Using the Patches Tab for a Device

- “Patches” on page 138
- “Patch Name” on page 139
- “Total Number of Patches Available” on page 139
- “Patch Impacts” on page 139
- “Patch Statistics” on page 140
- “Action Menu Items” on page 140
- “Searching Patches” on page 141
- “Patch Information” on page 143
- “Workstation Device Patches” on page 144

Patches

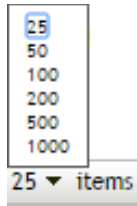
This section of the Patches page provides the following information about patches:

- Name of the patch
- Total number of patches available
- Impact of the patch
- Statistics of the patch

This section features the **Action** menu, which enables you to perform any of the following actions related to patches: **Deploy Remediation**, **Enable**, **Disable**, **Scan Now**, **Update Cache**, and **Export**. For more information on these actions, see “[Action Menu Items](#)” on page 140.

The **Patches** section also features the **show items** option that enables you to select the number of items to be displayed in this section:

Figure 8-1 Show Items drop-down List



Patch Name

The patch name typically includes the vendor or manufacturer of the patch, the specific application, and version information.

An example of a patch name is shown in the following figure, where patch name is given, Adobe is the vendor, Acrobat Reader is the application, and 6.0.6 is the version information:

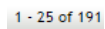
Figure 8-2 Example of a Patch Name



Total Number of Patches Available

The total number of available patches is displayed in the bottom left corner of the table. In the following example, there are 979 patches available:

Figure 8-3 Total Number of Patches



Patch Impacts

Based on the release date and impact, a patch can be classified as Critical, Recommended, Informational, or Software Installers:

- ♦ **Critical:** Novell has determined that this type of patch is critical, and should be installed as soon as possible. Most of the recent security updates fall into this category. ZENworks Server automatically downloads and saves the patches that have critical impact.
- ♦ **Recommended:** Novell has determined that this patch, although not critical or security related, is useful and should be applied to maintain the health of your computers. Therefore, Novell recommends that you implement patches that fall in this category.
- ♦ **Informational:** This type of patch detects a condition that Novell has determined as informational. Informational patches are used for information only. There is no actual patch to be installed.
- ♦ **Software Installers:** These types of patches are software applications. Typically, they include installers. The patches show **Not Patched** if the application has not been installed on a machine.

Patch Management impact terminology for its patch subscription closely follows the vendor impact terminology for patch criticality. Each operating system has a vendor-specific impact rating and that impact is mapped to a Novell rating as described in this section. Patch Management, following the

recommendations of Lumension Security, increases or steps up the severity of the impact rating. For example, Microsoft classifications for “Critical,” “Important,” and “Moderate” patches are all classified as “Critical” by Novell.

The following table lists the mapping between Novell and Microsoft patch classification terminology:

Table 8-1 Novell and Microsoft Patch Impact Mapping

Novell Patch Impacts	Windows	Other
Critical	Critical Security	NA
	Important	
	Moderate	
Recommended	Recommended	NA
	Low	
	Example: Microsoft Outlook 2003 Junk E-mail Filter Update	
Software Installers	Software Distribution	Adobe 8.1 software installer
	Example: Microsoft Windows Malicious Software Removal Tool (Virus Removal)	
Informational	NA	NA

Source: Lumension Security

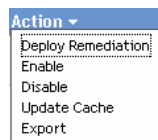
Patch Statistics

Patch statistics show the relationship between a specific patch and the selected device. The patch statistics appear in the **Patched** column on the far right side of the Patch page. This column indicates whether the selected device has been successfully patched or not. If the device has been patched, this column shows **Yes**; if the device has not been patched, this column shows **No**.

Action Menu Items

The **Action** menu on the Patches page for a selected device consists of the following six options:

Figure 8-4 Action Menu





- ♦ **Deploy Remediation:** Enables you to deploy a patch. To use this option, select the check box for the patch you want to deploy and select **Deploy Remediation** to open the Deploy Remediation Wizard.
- ♦ **Enable:** Allows you to enable a disabled patch. To use this option, select it from the **Action** menu.

- ♦ **Disable:** Enables you to disable a patch. To use this option, select the check box for the required patch and select **Disable**. The selected patch is removed from the list.
- ♦ **Update Cache:** Initiates a download process for the bundles associated with the selected patch and caches those bundles on your ZENworks Server.

NOTE: The remediation bundles must be cached before they are installed on the target device.

To use this option:

1. Select one or more patches in the patches list.
2. In the **Action** menu, click **Update Cache**.

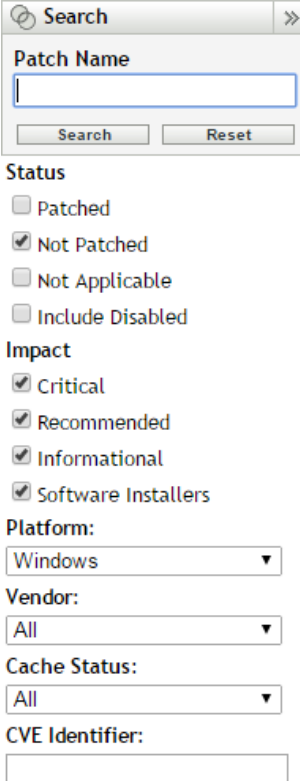
The patch icon changes to . While the download is in progress, the icon changes to . When the caching is complete, the color of the patch icon changes to green. This indicates that the patch remediation is ready to be deployed.

- ♦ **Export:** Enables you to export the details such as the status and impact of selected patches into a comma-separated value (CSV) file. You can choose to save the file in a different file format after opening it from the download option.

Searching Patches

The **Search** section on the Patches page offers extensive search and data filtering options that allow you to search for specific patches and filter result sets based on the status and impact of the patches. Searching and filtering can be performed independently of each other or can be combined to provide extensive drill-down capabilities. The following figure shows the **Patch Search** section:

Figure 8-5 Search Section on the Patches Page



The screenshot shows a 'Search' window with the following components:

- Search Bar:** Labeled 'Patch Name' with a text input field and 'Search' and 'Reset' buttons.
- Status:** A group of checkboxes:
 - ☐ Patched
 - ☒ Not Patched
 - ☐ Not Applicable
 - ☐ Include Disabled
- Impact:** A group of checkboxes:
 - ☒ Critical
 - ☒ Recommended
 - ☒ Informational
 - ☒ Software Installers
- Platform:** A dropdown menu currently showing 'Windows'.
- Vendor:** A dropdown menu currently showing 'All'.
- Cache Status:** A dropdown menu currently showing 'All'.
- CVE Identifier:** A text input field.

To search for a patch:

- 1 Type all or part of the patch name in the **Patch Name** text box.
- 2 Select the desired check box under **Status** and **Impact**.
- 3 Select the vendor in the **Vendor** drop-down list.
- 4 Select the cache status in the **Cache Status** drop-down list.
- 5 Click **Search**.

Clicking **Reset** enables you to return to the default settings.

The following table describes the result of selecting each filter option under **Status**:

Table 8-2 Status Filters in Search

Status Filter	Result
Patched	Search results include all the patches in the patch list that have been applied to one or more devices.
Not Patched	Search results include all the patches in the patch list that have not been applied to any device.
Not Applicable	Search results include all the patches in the patch list that do not apply to the device.
Include Disabled	Search results include all the patches in the patch list that have been disabled by the administrator.

The following table describes the result of selecting each filter option under **Impact**:

Table 8-3 Impact Filters in Search

Impact Filter	Result
Critical	Search results include all the patches in the patch list that are classified as Critical by Novell.
Recommended	Search results include all the patches in the patch list that are classified as Recommended by Novell.
Informational	Search results include all the patches in the patch list that are classified as Informational by Novell.
Software Installers	Search results include all the patches in the patch list that are classified as Software Installers by Novell.

Table 8-4 Vendor Filters and Cache Status Filter in search

Filter	Result
Platform	Search results include all the patches relevant to the operating system.
Vendor	Search results include all the patches relevant to the vendor.
Cache Status	Search results include all the patches that have been cached, not been cached, or whose caching process has failed on the local server.
CVE Identifier	Search results include all the patches for the Common Vulnerabilities and Exposures ID entered.

Patch Information

You can view detailed information for a selected patch in the **Patch Information** section. Clicking the name of a patch displays the details of that patch.

For example, if you select the patch called **Windows Malicious Software Removal Tool** from the list of patches, the **Patch Information** section displays the result of a patch analysis for the selected patch, as shown in the following figure:

Figure 8-6 Patch Information for a Selected Patch

Patch Information	
Name	Windows Malicious Software Removal Tool - April 2015 (KB890830)
Impact	Software Installer
Status	Enabled
Vendor	Microsoft Corp.
Released On	Apr-14-2015
Vendor Product ID	KB890830
Description	LSAC(v2)/LSAC(v3) After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.
Requires Reboot	Yes
Supports Uninstall	No
CVE Code	
URL	http://support.microsoft.com/kb/890830
Size	43132KB

The following table defines each property name in the **Patch Information** section:

Table 8-5 Property Names in the Patch Information Section

Property Name	Definition
Name	The name of the patch.

Property Name	Definition
Impact	The impact of the patch as determined by Novell. See "Patch Impacts" on page 75 .
Status	Status of the patch; can be Enabled , Disabled (Superseded) , or Disabled (By User) .
Vendor	The name of the vendor or manufacturer.
Released on	The date the patch was released by the vendor.
Vendor Product ID	The ID number given to the product by the vendor.
Description	The description of the patch; it includes the advantages of deploying the patch and the prerequisites for deployment.
Requires Reboot	Whether a reboot is required after patch deployment
Supports Uninstall	Whether the patch supports an uninstall after installation
CVE Code	The Common Vulnerabilities and Exposures ID for the patch, if applicable.
URL	A URL that has more information about the patch.
Size	The size of the patch.

Workstation Device Patches

To view the patches for a specific workstation device:

- 1 Click the **Workstation** link on the Devices page.

A list of workstation groups classified on the basis of their operating systems appears, as shown in the following figure:

Status	Name	Type	Operating System	Last Contact	Retired
	Apple OS X 10.10 (Yosemite)	Dynamic Workstation Group			
	Apple OS X 10.8 (Mountain Lion)	Dynamic Workstation Group			
	Apple OS X 10.9 (Mavericks)	Dynamic Workstation Group			
	Mac OS X 10.5 (Leopard)	Dynamic Workstation Group			
	Mac OS X 10.6 (Snow Leopard)	Dynamic Workstation Group			
	Mac OS X 10.7 (Lion)	Dynamic Workstation Group			
	my endpoints	Workstation Group			
	Red Hat Enterprise Linux Desktop 4	Dynamic Workstation Group			
	Red Hat Enterprise Linux Desktop 5	Dynamic Workstation Group			
	Red Hat Enterprise Linux Desktop 6	Dynamic Workstation Group			
	Red Hat Enterprise Linux Desktop 7	Dynamic Workstation Group			
	SUSE Linux Enterprise Desktop 10	Dynamic Workstation Group			
	SUSE Linux Enterprise Desktop 11	Dynamic Workstation Group			
	SUSE Linux Enterprise Desktop 12	Dynamic Workstation Group			
	Windows 7 Workstations	Dynamic Workstation Group			
	Windows 8 Workstations	Dynamic Workstation Group			
	Windows 8.1 Workstations	Dynamic Workstation Group			
	Windows Vista Workstations	Dynamic Workstation Group			
	Windows XP Workstations	Dynamic Workstation Group			
	TP-Windows7	Workstation	windows7-ent-x86	11:07 AM	

You see the following icons on the Workstations page:

Icon	Status
	Message Status: Normal Device Status: Bundle and policy enforcement successful
	Message Status: Warning Device Status: Bundle and policy enforcement successful
	Message Status: Error Device Status: Bundle and policy enforcement successful
	Message Status: Error Device Status: Bundle and/or policy enforcement failed on one or more bundles or policies.

Devices can also be found by using **Search** (see section “[Filter Item](#)” on page 137).

- Click the required group (Workstation or Dynamic Workstation Group) to view the details of the group and its members.

3 Click the required member or workstation device.

A page displaying the member's details is displayed. The following figure shows the page displaying details for the workstation device **w2adxpSP3**:

TP-Windows7

Summary Inventory Relationships Settings Content Locations Audit Patches

General

Alias: TP-Windows7

Host Name: TP-Windows7

IP Address: 10.19.0.126

Test Device: No (Set)

Last Full Refresh: 12:19 AM

Last Contact: 11:07 AM

ZENworks Agent Version: 11.4.0.2973

ZENworks Updater Service Version: 11.4.0.2973

ZENworks Agent Status:

Operating System: Microsoft Windows 7 Enterprise 6.1.7600 N/A Build 7600

Number of errors not acknowledged: 0

Number of warnings not acknowledged: 0

Primary User: No user sources configured

Owner: (Edit)

Serial Number: 422f98cc27c51f5bbea4bd765571c9e5

GUID: 05ff8f0a0d141345a51a4c69f336bc9f

Department: (Edit)

Site: (Edit)

Location: (Edit)

Message Log

Advanced

Status	Message	Date
Click refresh to see the events		

4 Click the **Patches** tab.

The patches associated with the workstation device appear as shown in the following figure:

Patches - Last PD time: Mar/31/2015 01:30:09

Summary Inventory Relationships Settings Content Statistics Locations Audit Patches

Action	Patch Name	Impact	Patched	Released On
<input type="checkbox"/>	MS15-028 Security Update for Windows Server 2008 R2 x64 (KB3030377)	Critical	No	Mar-10-2015
<input type="checkbox"/>	MS15-027 Security Update for Windows Server 2008 R2 x64 (KB3002657)	Critical	No	Mar-10-2015
<input type="checkbox"/>	MS15-020 Security Update for Windows Server 2008 R2 x64 (KB3039066)	Critical	No	Mar-10-2015
<input type="checkbox"/>	MS15-031 Security Update for Windows Server 2008 R2 x64 (KB3046049)	Critical	No	Mar-10-2015
<input type="checkbox"/>	MS15-021 Security Update for Windows Server 2008 R2 x64 (KB3032323)	Critical	No	Mar-10-2015
<input type="checkbox"/>	MS15-029 Security Update for Windows Server 2008 R2 x64 (KB3035126)	Critical	No	Mar-10-2015
<input type="checkbox"/>	MS15-018 Cumulative Security Update for Internet Explorer 8 for Windows Server 2008 R2 x64 (KB3032359)	Critical	No	Mar-10-2015

Search

Patch Name

Search Reset

Status

☐ Patched

☒ Not Patched

☐ Not Applicable

☐ Include Disabled

Impact

☒ Critical

☒ Recommended

☒ Informational

☒ Software Installers

Vendor All

Cache Status All

CVE Identifier

9 Patch Management for a Device Group

Device group patches refers to the patches that have been assigned to members of the server group or the workstation group of devices in the network and displays the status of each patch for the devices. This view displays only the patches applicable to the member devices of the selected group.

- ♦ [“Using the Patches Tab within a Server Group” on page 147](#)
- ♦ [“Using the Patches Tab within a Workstation Group” on page 150](#)

Using the Patches Tab within a Server Group

This view displays the patches applicable to the member devices of the selected server group.

- 1 Click the **Devices** tab on the left panel.


















A page displaying the root folders for each type of device appears, as shown in the following figure:



The **Servers** folder is the root folder for all managed servers and the **Workstations** folder is the root folder for all managed workstations in the network.

- 2 Click the **Servers** link.

A list of server groups classified on the basis of their operating systems appears, as shown in the following figure:

Devices						
New Edit Delete Action Quick Tasks Export						
<input type="checkbox"/>	Status	Name	Type	Operating System	Last Contact	Retired
<input type="checkbox"/>		 Apple OS X 10.10 Server (Yosemite)	Dynamic Server Group			
<input type="checkbox"/>		 Apple OS X 10.8 Server (Mountain Lion)	Dynamic Server Group			
<input type="checkbox"/>		 Apple OS X 10.9 Server (Mavericks)	Dynamic Server Group			
<input type="checkbox"/>		 Open Enterprise Server 11	Dynamic Server Group			
<input type="checkbox"/>		 Open Enterprise Server 2	Dynamic Server Group			
<input type="checkbox"/>		 Red Hat Enterprise Linux Server 4	Dynamic Server Group			
<input type="checkbox"/>		 Red Hat Enterprise Linux Server 5	Dynamic Server Group			
<input type="checkbox"/>		 Red Hat Enterprise Linux Server 6	Dynamic Server Group			
<input type="checkbox"/>		 Red Hat Enterprise Linux Server 7	Dynamic Server Group			
<input type="checkbox"/>		 server	Server Group			
<input type="checkbox"/>		 SUSE Linux Enterprise Server 10	Dynamic Server Group			
<input type="checkbox"/>		 SUSE Linux Enterprise Server 11	Dynamic Server Group			
<input type="checkbox"/>		 SUSE Linux Enterprise Server 12	Dynamic Server Group			
<input type="checkbox"/>		 Windows Server 2003	Dynamic Server Group			
<input type="checkbox"/>		 Windows Server 2008	Dynamic Server Group			
<input type="checkbox"/>		 Windows Server 2008 R2	Dynamic Server Group			
<input type="checkbox"/>		 Windows Server 2012	Dynamic Server Group			
<input type="checkbox"/>		 Windows Server 2012 R2	Dynamic Server Group			
<input type="checkbox"/>		 az-tp-win2008r2	Server	win2008r2-ee-sp1-x64	1:26 AM	
1 - 19 of 19 show 25 items						

3 Click the required group (Server or Dynamic Server Group).

A page displaying the general details of the group and the members in the group appears. The following figure shows the page that appears when the **Windows Server 2008 R2** type is selected:

The screenshot shows a web-based management interface for a group named "Windows Server 2008 R2". The breadcrumb navigation at the top reads "Devices > Servers > Windows Server 2008 R2". Below the title, there are five tabs: "Summary", "Relationships", "Details", "Audit", and "Patches". The "Summary" tab is active and displays the following information:

- General** section:
 - Object type: Dynamic Server Group
 - GUID: 677c3c2dca7cfd30c1cabf5315ada028
 - Description: (Edit) Windows Server 2008 R2 Group
- Members** section:

Name	In Folder
az-tp-win2008r2	/Devices/Servers
- Members Change Log** section:

Date	Added	Removed
Mar 21	1	0

Each section includes a "show 5 items" link and a "1 - 1 of 1" indicator.

4 Click the **Patches** tab.

The patches applicable to the member devices of the selected group are displayed. If the selected group is **Windows Server 2008 R2**, the **Patches** tab displays all the patches applicable to the member devices within the group **Windows Server 2008 R2**, as shown in the following figure:

Devices > Servers > Windows Server 2008 R2

Windows Server 2008 R2

Summary Relationships Details Audit Patches

Patches

Action	Patch Name	Impact	Patched	Not Patched	Released On
<input type="checkbox"/>	Update for Windows Server 2008 R2 x64 (KB2990214)	Recommended	0	1	Apr-14-2015
<input type="checkbox"/>	MS15-032 Cumulative Security Update for Internet Explorer 8 for Windows Server 2008 R2 x64 (KB3038314)	Critical	0	1	Apr-14-2015
<input type="checkbox"/>	MS15-038 Security Update for Windows Server 2008 R2 x64 (KB3045999)	Critical	0	1	Apr-14-2015
<input type="checkbox"/>	MS15-041 Security Update for .NET Framework 4 on Win 2003, Vista, Win 7, Server 2008, Server 2008 R2 x64 (KB3037578)	Critical	0	1	Apr-14-2015
<input type="checkbox"/>	MS15-035 Security Update for Windows Server 2008 R2 x64 (KB3046306)	Critical	0	1	Apr-14-2015
<input type="checkbox"/>	Windows Malicious Software Removal Tool x64 - April 2015 (KB890830)	Software Installer	0	1	Apr-14-2015
<input type="checkbox"/>	MS15-038 Security Update for Windows Server 2008 R2 x64 (KB3045685)	Critical	0	1	Apr-14-2015
<input type="checkbox"/>	MS15-037 Security Update for Windows Server 2008 R2 x64 (KB3046269)	Critical	0	1	Apr-14-2015

Search

Patch Name

Search Reset

Status

☐ Patched

☒ Not Patched

☐ Not Applicable

☐ Include Disabled

Impact

☒ Critical

☒ Recommended

☒ Informational

☒ Software Installers

Vendor All

Cache Status All

CVE Identifier

Mandatory Baseline

☒ All Patches

☐ Baseline Only

For information on the features of the Device Group Patches page for the selected server group, see [“About Mandatory Baselines” on page 123](#).

Using the Patches Tab within a Workstation Group

This view displays the patches applicable to the member devices of the selected workstation group.

- 1 Click the **Devices** tab on the left panel.
A page displaying the root folders for each type of device appears
- 2 Click the **Workstations** link.

A list of workstation groups classified on the basis of their operating systems appears, as shown in the following figure:

Status	Name	Type	Operating System	Last Contact	Retired
<input type="checkbox"/>	Apple OS X 10.10 (Yosemite)	Dynamic Workstation Group			
<input type="checkbox"/>	Apple OS X 10.8 (Mountain Lion)	Dynamic Workstation Group			
<input type="checkbox"/>	Apple OS X 10.9 (Mavericks)	Dynamic Workstation Group			
<input type="checkbox"/>	Mac OS X 10.5 (Leopard)	Dynamic Workstation Group			
<input type="checkbox"/>	Mac OS X 10.6 (Snow Leopard)	Dynamic Workstation Group			
<input type="checkbox"/>	Mac OS X 10.7 (Lion)	Dynamic Workstation Group			
<input type="checkbox"/>	my endpoints	Workstation Group			
<input type="checkbox"/>	Red Hat Enterprise Linux Desktop 4	Dynamic Workstation Group			
<input type="checkbox"/>	Red Hat Enterprise Linux Desktop 5	Dynamic Workstation Group			
<input type="checkbox"/>	Red Hat Enterprise Linux Desktop 6	Dynamic Workstation Group			
<input type="checkbox"/>	Red Hat Enterprise Linux Desktop 7	Dynamic Workstation Group			
<input type="checkbox"/>	SUSE Linux Enterprise Desktop 10	Dynamic Workstation Group			
<input type="checkbox"/>	SUSE Linux Enterprise Desktop 11	Dynamic Workstation Group			
<input type="checkbox"/>	SUSE Linux Enterprise Desktop 12	Dynamic Workstation Group			
<input type="checkbox"/>	Windows 7 Workstations	Dynamic Workstation Group			
<input type="checkbox"/>	Windows 8 Workstations	Dynamic Workstation Group			
<input type="checkbox"/>	Windows 8.1 Workstations	Dynamic Workstation Group			
<input type="checkbox"/>	Windows Vista Workstations	Dynamic Workstation Group			
<input type="checkbox"/>	Windows XP Workstations	Dynamic Workstation Group			
<input checked="" type="checkbox"/>	TP-Windows7	Workstation	windows7-ent-x86	11:07 AM	

1 - 20 of 20 show 25 items

3 Click the required group (Workstation or Dynamic Workstation Group).

A page displaying the general details of the group and the members in the group appears. The following figure shows the page that appears when the Dynamic Workstation Group called **Windows 7 Workstations** is selected:

Devices > Workstations > Windows 7 Workstations

Windows 7 Workstations

SummaryRelationshipsDetailsAuditPatches

General

Object type:Dynamic Workstation Group

GUID:f360bbcd2846a91d62f582d28d80cc28

Description:(Edit)Windows 7 Workstation Group

Members

Name	In Folder
TP-Windows7	/Devices/Workstations

1 - 1 of 1show 5 items

Members Change Log

Date	Added	Removed
Mar 27	1	0

1 - 1 of 1show 5 items

4 Click the **Patches** tab.

The patches applicable to the member devices of the selected group are displayed. If the selected group is Windows 7 Workstations, the **Patches** tab displays all the patches applicable to the member devices within the group Windows 7 Workstations, as shown in the following figure:

The screenshot shows the ZENworks 11 SP4 Patch Management interface. The breadcrumb navigation at the top indicates the path: **Devices > Workstations > Windows 7 Workstations**. Below this, the **Windows 7 Workstations** group is selected, and the **Patches** tab is active. The main area displays a table of patches with the following columns: **Patch Name**, **Impact**, **Patched**, **Not Patched**, and **Released On**. The table lists 15 patches, including **Windows Malicious Software Removal Tool - April 2015 (KB890830)**, **Microsoft Skype Business 7.3.32.101 for Windows**, and various Microsoft security updates. The right sidebar contains a **Search** section with a text input and **Search** and **Reset** buttons. Below the search section are filter options for **Status** (Patched, Not Patched, Not Applicable, Include Disabled), **Impact** (Critical, Recommended, Informational, Software Installers), **Vendor** (All), **Cache Status** (All), **CVE Identifier** (input field), and **Mandatory Baseline** (All Patches, Baseline Only).

Patch Name	Impact	Patched	Not Patched	Released On
Windows Malicious Software Removal Tool - April 2015 (KB890830)	Software Installer	0	1	Apr-14-2015
custom	Recommended	0	1	Apr-10-2015
Microsoft Skype Business 7.3.32.101 for Windows (See Notes)	Recommended	0	1	Apr-01-2015
Microsoft Enhanced Mitigation Evaluation Toolkit (EMET) 4.1 Update 1 (See Notes)	Software Installer	0	1	Apr-30-2014
MS 2905247 2894842 Security Update for .NET Framework 4.0 (All Languages)	Recommended	0	1	Dec-10-2013
MS 2841134 Internet Explorer 11.0 (All Languages) (See Note)	Software Installer	0	1	Nov-07-2013
MS 2896666 Workaround for Vulnerability in Microsoft Graphics component (Enabled) (See Notes)	Recommended	0	1	Nov-05-2013
MS 2896666 Workaround for Vulnerability in Microsoft Graphics component (Disabled) (See Notes)	Recommended	0	1	Nov-05-2013
MS 2887505 Workaround for Vulnerability in Internet Explorer (Enabled) (See Notes)	Recommended	0	1	Sep-17-2013
MS 2847140 Workaround for Vulnerability in Internet Explorer (Enabled) (See Notes)	Recommended	0	1	May-08-2013
MS 2799926 Update for Windows 7 and Windows Server 2008 R2 (All Languages)	Recommended	0	1	Apr-08-2013
MS 2791765 Application Compatibility Update for Windows 7 and Windows Server 2008 R2 (March 2013) (All Languages)	Recommended	0	1	Mar-12-2013
MS 2794119 Update for Windows 7 and Windows Server 2008 R2 (All Languages) (See Notes) (Rev. 2)	Recommended	0	1	Jan-21-2013

For information on the features of the Device Group Patches page for the selected workstations group, see [“About Mandatory Baselines” on page 123](#).

10 License Behavior of ZPM

This chapter describes the various ZPM license states and the functions available in the various states. The following sections describe the possible License states in Novell ZENworks 11 SP4:

- ♦ “ZCM Only State” on page 153
- ♦ “Trial State” on page 153
- ♦ “Trial Expired State” on page 154
- ♦ “Licensed State” on page 154
- ♦ “License Expired State” on page 154

ZCM Only State

The ZCM only states indicates that you are not licensed for ZPM.

The following list describes ZPM capability behavior while you are in a ZCM only state:

- ♦ **Patches:** Regardless of platform, you cannot use ZPM patch deployment features.
- ♦ **Scan result:** The Vulnerability Detection runs on each device daily, scanning for known patches. This task returns the results that are displayed on the Patches page. The results are presented in a table of patch status.

NOTE: When the user tries to perform any of the ZPM functionality a red error message will be displayed.

Trial State

After installing ZENworks 11 SP4, it enters a 60 trial state. During this trial, all ZPM functions are available for use.

When the trial expires, you must enter a valid serial number to continue using ZPM (**Configuration > Product Licensing > ZENworks Patch Management**).

NOTE: Only patch scanning is allowed of ZPM. Also to use the ZPM the ZCM does not have to be licensed.

The capabilities that are supported:

- ♦ **ZPM functionality:** This will allow you to perform all the security, patch and configuration management tasks.
- ♦ **Patches:** Patches of all the platforms and vendors will be supported for scanning and downloading.

NOTE: If trial has been used then it will request the user to purchase the subscription after it has expired.

Trial Expired State

The ZPM reports this state in the following cases:

- ♦ **Keyless trial expires:** Activating the ZPM without a key will allow ZPM to run in keyless trial, after the 60 day trial the keyless trial will expire.
- ♦ **Key based trial expires:** Once you enter a valid trial key the ZPM will be activated as a key based trial. Once the license of the trial key has expired it will behave as an expired key based trial.

When the ZPM trial state expires after the allotted period it returns to “ZCM Only State”. See [“Using the Patches Tab within a Server Group” on page 147](#).

Licensed State

ZPM in licensed state is not hindered by the license state of ZCM. The ZPM needs to be active and it should have a valid ZPM license to continue in this state.

In a licensed ZPM all the functions work as mentioned below:

- ♦ **ZPM functionality:** This will allow you to perform all the security, patch, and configuration management tasks.
- ♦ **Patches:** Patches of all the platforms and vendors will be supported for scanning and downloading.
- ♦ **Scan result:** The Vulnerability Detection is assigned to run on each device on a daily basis to scan for known patches. This task returns the results that are displayed on the Patches page. The results are presented in a table of patch status.

License Expired State

When the ZPM license expires the functionality of the ZPM will behave in the same manner as “ZCM-Only State”. See [“Using the Patches Tab within a Server Group” on page 147](#).

In a license Expired ZPM, the limitations of the ZPM are mentioned below:

- ♦ **Patches:** Only patch scanning is supported and deployment of cached patches is supported, regardless of platform (including Linux and Mac). You cannot cache additional uncached patches.

NOTE: The Administrator will be able to review the patches that were cached. The cached patches can be used for deployment, but no new patch subscription will be downloaded until the license is renewed.

The bundles or patches that were downloaded before the license expired will not be disabled nor deleted.

11 ZENworks Reporting Reports

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

- ♦ [“Viewing the Predefined Report” on page 155](#)

Viewing the Predefined Report

You must have installed ZENworks Reporting to view the predefined reports.

To view the Predefined reports for Patch Management, do the following:

- 1 Log in to ZENworks Reporting.
- 2 Navigate to the **View** > Repository > Folders > Organization > Reports > ZENworks > Predefined Reports > **Patch Management** folder.
- 3 The following Predefined reports are included for Bundles and Policies:
 - ♦ **Baseline Report:** Displays information on a patch that assigned to a device. This report lists device group name, agent name, patch name, and patch status.
 - ♦ **Bundle Deployment Summary:** Displays only the devices on which the patch bundle have been deployed. This report lists deployment name, patch name, assigned device name, and patch device status.
 - ♦ **Critical Patch Status Report:** Displays information on critical patches that are assigned to the devices. This report displays the total summary of the patch status and lists patched, not patched, not applicable, Error, and total devices.
 - ♦ **Device Patch Status by Vendor:** Displays information on device patch status. This report lists agent name, vendor, patched, not patched, not applicable, released on, is patch enabled, and patch impact.
 - ♦ **Mandatory Baseline By Patch:** Displays information on patch that have been assigned as mandatory baseline on a device. This report lists group name, patch name, criticality, vendor, released on, enabled status, cached status, patched, host name, DNS, and patch device status.
 - ♦ **Mandatory Baseline Details:** Displays information on the device group name and device name on which mandatory baseline patch have been applied. This report lists device group name, criticality, name, device name, and patch device status.
 - ♦ **Mandatory Baseline Summary:** Displays information on patch assigned as mandatory baseline on a device. This report lists vulnerability name, released on, criticality, group name, applicable, devices, patched, and not patched.
 - ♦ **Patch Analysis:** Displays information on patch assigned as mandatory baseline on a device. This report lists vendor, patch name, released date, criticality, applicable, patched, not patched, and %patched.
 - ♦ **Patch Assement Report:** Displays information on all released patches and their impact. This report lists vendor, released patches, and patch impact.

- ♦ **Patch Bundle Deployment Status:** Displays information on all released patch bundles and their status. This report lists admin initiated remediation bundle, deployed patch bundle, event type, and event status.
- ♦ **Patch Deployment Summary:** Displays information on all released patch bundles and their status. This report lists admin initiated remediation bundle, deployed patch bundle, event type, and event status.
- ♦ **Patch Detail Report:** Displays detailed information on patches. This report lists patch name, patched status, total devices, and %patched.
- ♦ **Patch Detection Not Deployed:** Displays information on Patch Detections that have not deployed. This report lists the device name, OS name, ZENworks Agent version and last contact.
- ♦ **Patch Detection Not Run in a Specified Time:** Displays information on Patch Detections not run within a time period. This report lists the device name, OS name, ZENworks Agent version and last contact.
- ♦ **Patch Release Report:** Displays information on released patches. This report lists, patch device status, and device name.
- ♦ **Patch Tuesday Report:** Displays information on Tuesday's released patches. This report lists, patch name, patch status, and total devices.
- ♦ **Top 10 Not Patched Critical Patches:** Displays information on the most critical patches that are not deployed. This report lists patche name, and patch impact.

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

12 Best Practice with ZENworks 11 SP4 Update 2 Patch Management

Patch Management is a fully integrated feature of Novell ZENworks 11 SP4 that provides the same agent-based patch, vulnerability patch, and compliance management solution that was used in prior versions.

It is recommended that all moderate to large-size organizations should be using enterprise patch management tools for the majority of their computers. Even small organizations should be migrating to some form of automated patching tool. Widespread manual patching of computers is becoming ineffective as the number of patches that need to be installed grows and as attackers continue to develop and exploit code more rapidly. Only uniquely configured computers and other computers that cannot be updated effectively through automated means, such as many appliance-based devices, should continue to be patched manually.

The ZENworks Server schedules a Vulnerability Detection task for all ZENworks managed devices (servers and workstations) and compiles information on the operating system, hardware, and software.

The results of the scan are sent to the ZENworks Server and can be viewed anytime in the Patches section under the **Patch Management** tab or in the **Devices** tab even if a workstation is disconnected from your network.

Timely patching of security issues is generally recognized as critical to maintaining the operational availability, confidentiality, and integrity of information technology (IT) systems. However, failure to keep operating system and application software patched is one of the most common issues identified by security and IT professionals. New patches are released daily, and it is often difficult for even experienced system administrators to keep abreast of all the new patches and ensure proper deployment in a timely manner. Most major attacks in the past few years have targeted known vulnerabilities for which patches existed before the outbreaks. Indeed, the moment a patch is released, attackers make a concerted effort to reverse engineer the patch swiftly (measured in days or even hours), identify the vulnerability, and develop and release exploit code. Thus, the time immediately after the release of a patch is ironically a particularly vulnerable moment for most organizations due to the time lag in obtaining, testing, and deploying a patch.

It is highly recommended that before any Patch management takes place, that within your company or organization you set up a Patch and Vulnerability Group (PVG) to manage the patching process. This group should be concerned with the Patching and Vulnerability operation across the organization, and should therefore be an exclusive group with ties to your security, asset management and network control groups.

The PVG should be specially tasked to implement the patch and vulnerability management program throughout the organization. The PVG is the central point for vulnerability remediation efforts, such as OS and application patching and configuration changes. Since the PVG needs to work actively with local administrators, large organizations may need to have several PVGs; they could work together or be structured hierarchically with an authoritative top-level PVG. The duties of a PVG should include the following:

1. Inventory the organization's IT resources to determine which hardware equipment, operating systems, and software applications are used within the organization.

2. Monitor security sources for vulnerability announcements, patch and non-patch remediations, and emerging threats that correspond to the software within the PVG's system inventory.
3. Prioritize the order in which the organization addresses remediating vulnerabilities.
4. Create a database of remediations that need to be applied to the organization.
5. Conduct testing of patches and non-patch remediations on IT devices that use standardized configurations.
6. Oversee vulnerability remediation.
7. Distribute vulnerability and remediation information to local administrators.
8. Perform automated deployment of patches to IT devices using enterprise patch management tools.
9. Configure automatic update of applications whenever possible and appropriate.
10. Verify vulnerability remediation through network and host vulnerability scanning.
11. Train administrators on how to apply vulnerability remediations.

Testing Patches

Before you start downloading a patch, configure the downloading options in the **Configuration** tab. For more information, see [“Configuring Subscription Service Content Download Details” on page 39](#).

It is important that your PVG determines a strategy for testing patches before release, this will vary from organization to organization, but should be in line with your current security policies. How you decide to test your patches before deployment will depend on your current architecture and policy. In some organizations it may be required to review your policies in order to effectively use this method.

However, it is highly recommended that patches are tested prior to deployment.

Deploying Patches in a Controlled Way

To deploy a patch, you can use the Deploy Remediation Wizard. For more information, see [Chapter 6, “Using the Deploy Remediation Wizard,” on page 91](#).

Patches are released frequently, and it is possible to automate the entire release process by using the deployment settings. Whilst this may suit some smaller companies, in a large organization with multiple platforms and sites, we recommend that the PVG designs a strategy for deployment. Each patch for each software update will behave differently, which is why it is necessary to control the process. For example, some software will require a reboot after updating, and although Zenworks 11 SP4 can manage this process on your behalf, your PVG should determine the details of this, and be aware of any other software or processes which are running, or patches that are being installed concurrently. The Best Practice recommendation for controlling these processes is to use a phased approach.

Implementing patch management tools in phases allows process and user communication issues to be addressed with a small group before deploying the patch application universally. Most organizations deploy patch management tools first to standardized desktop systems and single-platform server farms of similarly configured servers. Once this has been accomplished, organizations should address the more difficult issue of integrating multi-platform environments, nonstandard desktop systems, legacy computers, and computers with unusual configurations. Manual methods may need to be used for operating systems and applications not supported by automated patching tools, as well as some computers with unusual configurations; examples include

embedded systems, industrial control systems, medical devices, and experimental systems. For such computers, there should be a written and implemented procedure for the manual patching process, and the PVG should coordinate local administrator efforts

Setting a Baseline

To set a baseline, you must ensure that a group of devices is protected and that all the devices in the group are patched consistently. For more information, see [Chapter 7, "Using Mandatory Baselines," on page 123](#).

It is also highly recommended that the customer does NOT deploy all patches using mandatory baseline. As stated above, some patches can require a reboot, if an attempt was made to deploy all patches via the baseline, without being aware of the consequences of each individual patch, then your system could become unstable, or the patch updating process could be compromised.

It is of vital importance that this method is discussed by the PVG, and a suitable strategy is agreed upon. Industry recommendations are to use a standardized configuration to manage IT resources.

Monitoring

Patch and vulnerability metrics fall into three categories: susceptibility to attack, mitigation response time, and cost, which includes a metric for the business impact of program failures. The emphasis on patch and vulnerability metrics being taken for a system or IT security program should reflect the patch and vulnerability management maturity level. For example, attack susceptibility metrics such as the number of patches, vulnerabilities, and network services per system are generally more useful for a program with a low maturity level than a high maturity level. Organizations should document what metrics will be taken for each system and the details of each of those metrics. Realistic performance targets for each metric should be communicated to system owners and system security officers. Once these targets have been achieved, more ambitious targets can be set. It is important to carefully raise the bar on patch and vulnerability security to avoid overwhelming system security officers and system administrators.

Organizations should consistently measure the effectiveness of their patch and vulnerability management program and apply corrective actions as necessary.

13 Patch Policy

Patch Policy is a new feature designed to make deployment of multiple patches easier across large estates. It can be used as a testing ground for new patches before they are released onto the network, and it can also be used to filter content, so that some devices can be selected or omitted as part of the remediation.

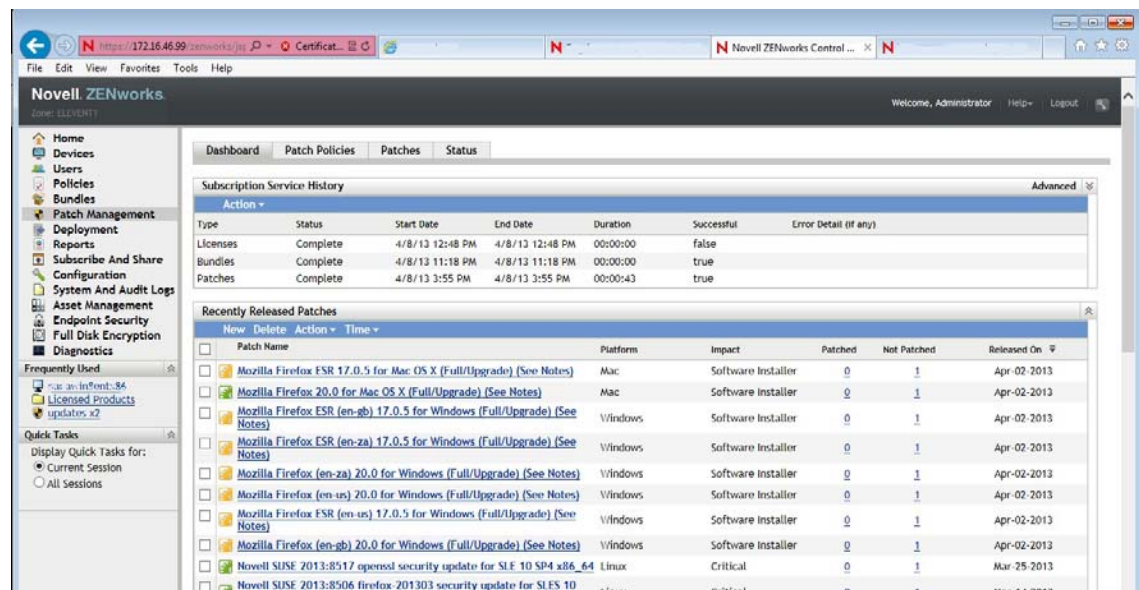
Setting up a Patch Policy

Before setting up a patch policy it is important to plan your deployment, and ensure that you know the devices you would like to reach and the remediations you would like to deliver.

It is recommended that you setup a test machine to test the efficacy of the patch before deploying across a global environment.

- 1 Click the Patch Management tab on the left panel.

A page displaying the tabs for controlling patch management appears, as shown in the following figure:



Open the Patch Policies tab.

- 2 Click the New link.

A list of device groups classified on the basis of their operating systems appears, as shown in the following figure:

Create New Patch Policy

Step 1: Select Platform

Select the platform for which you want to create a patch policy.

Platform:	Description:
Linux	Linux - Create a patch policy for Linux devices.
Mac	
Windows	

<< Back Next >> Cancel

3 Click the required Platform

A page appears asking to define details, here you can name your policy and make some administrative notes, then click Next.

Create New Patch Policy

Step 2: Define Details

Enter the details for the patch policy.

Patch Policy Name: *

Administrator Notes:

Fields marked with an asterisk are required.

<< Back Next >> Cancel

4 Next you should define the Patch Policy Rules.

Click Add Filter and a drop down menu appears, here you can choose the filter by which to select the appropriate patches, as shown in the figure below:

5 Review the Patch Policy in the **Patches** tab and select from the following options.

Option	Description
Auto approve patches after	Approve patches after they've been successfully tested in the sandbox.
Approve after x days	Approve patches the number of days specified after a successful test.
Recalculate after x days	Reapplies the patch filters you've selected after a number of specified days.
Rebuild policy on creation	Rebuilds the policy to include the patches included after recalculation.
Define additional properties	Defines additional properties.

The final step in creating the patch policy is to click the Rebuild button. This can be achieved by selecting the **Rebuild Patch Policy On Creation** checkbox or by returning to the Patch Policy Summary page and clicking **Rebuild Now**. This will finalize the Policy and create it in Sandbox.

Create New Patch Policy

Step 4: Summary

Review the information and click "Finish" to create the new patch policy.

Platform:

Windows

Patch Policy Name:

test

Administrator Notes:

☒ Create as Sandbox

☐ Auto approve patches after successful test enforcements

Approve after day(s)

Recalculate after day(s)

☐ Rebuild policy on creation

☐ Define Additional Properties

<< Back

Finish

Cancel

NOTE: Every time that you make a change to the Patch Policy you must click the **Rebuild** button to secure the changes

IMPORTANT: If you delete an old patch policy from an endpoint and then publish a new policy to replace it, the endpoint may list a Device-Assigned Bundle Status of Not Installed for an indefinite period of time. If you encounter this endpoint status, reboot the endpoint to complete publication of the patch policy.

Publishing Patch Policy

Once the Policy is created, you can further fine tune the parameters and even test it out before publishing it to a live environment.

- 1 Go to the Patch Policy Summary page

This should display the current attributes for the Policy that you have created

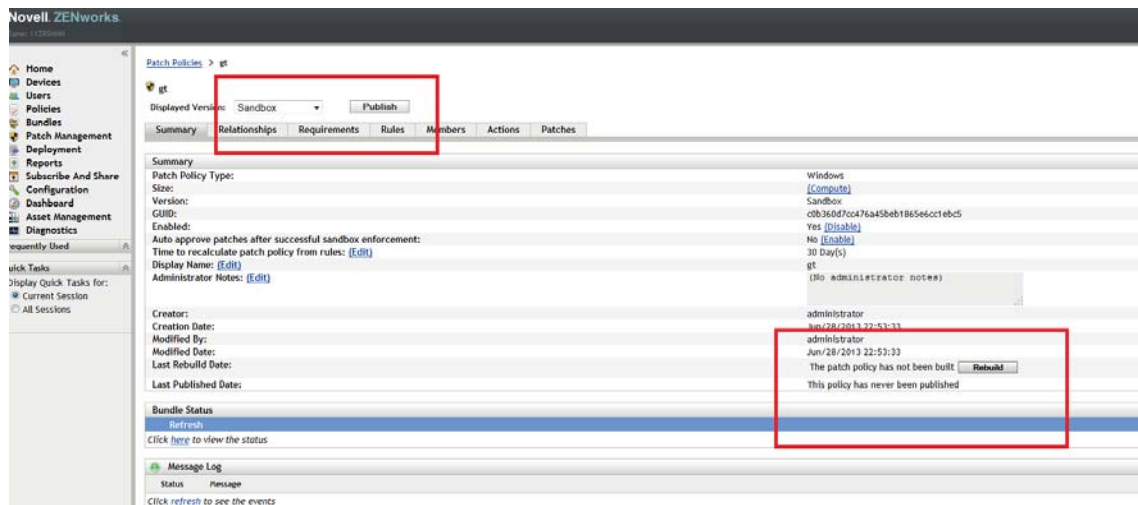
- 2 Click the **Rebuild** button

This will build the Policy, you will notice in the below figure that the Policy is defined as unpublished.

- 3 In the drop down menu at the top of the page you can choose where to publish the Policy to: when the Policy is created its default status is Sandbox.

All that is needed to achieve this is to click the **Publish** button, this will update the information in the summary box, and publish the policy, if you return to your agent device and refresh it you will see the Policy in the Agent Window.

IMPORTANT: If you delete an old patch policy from an endpoint and then publish a new policy to replace it, the endpoint may list a Device-Assigned Bundle Status of Not Installed for an indefinite period of time. If you encounter this endpoint status, reboot the endpoint to complete publication of the patch policy.



Advanced Configuration for Patch Policy

To achieve an even more targeted remediation within the Patch Policy function there are a number of Advanced settings for the ZENworks 11 SP4 user. It should be noted that we advise ZENworks Administrators to dry run their Policies on a Test device before releasing to a Live environment (see next section)

- 1 Click the **Patch Policy** tab on the Patch Management Dashboard

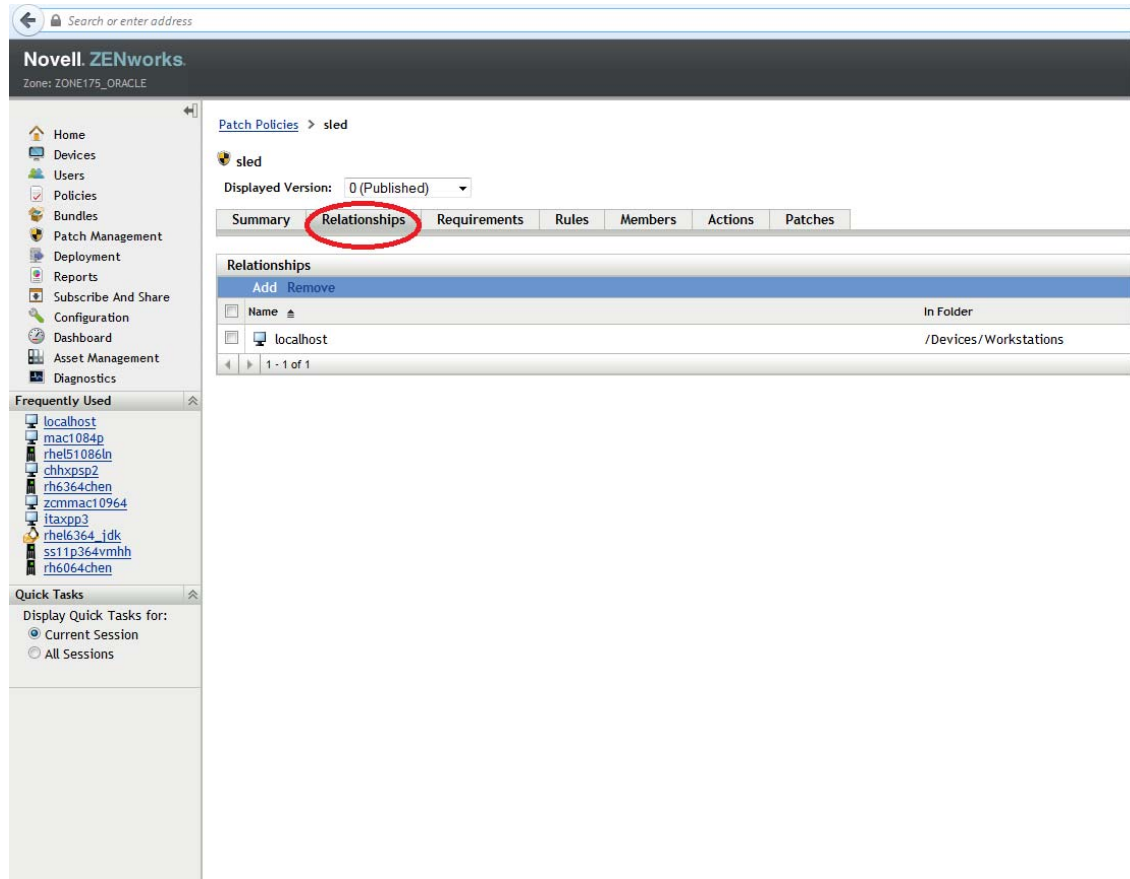
A selection of pre-made policies should be in the list

- 2 Choose a Policy to edit.

You should be presently on the Patch Policies dashboard, there are 4 tabs for Advanced settings: Relationships, Requirements, Members and Actions.

Remember, each selection will further define the list of patches that the policy produces

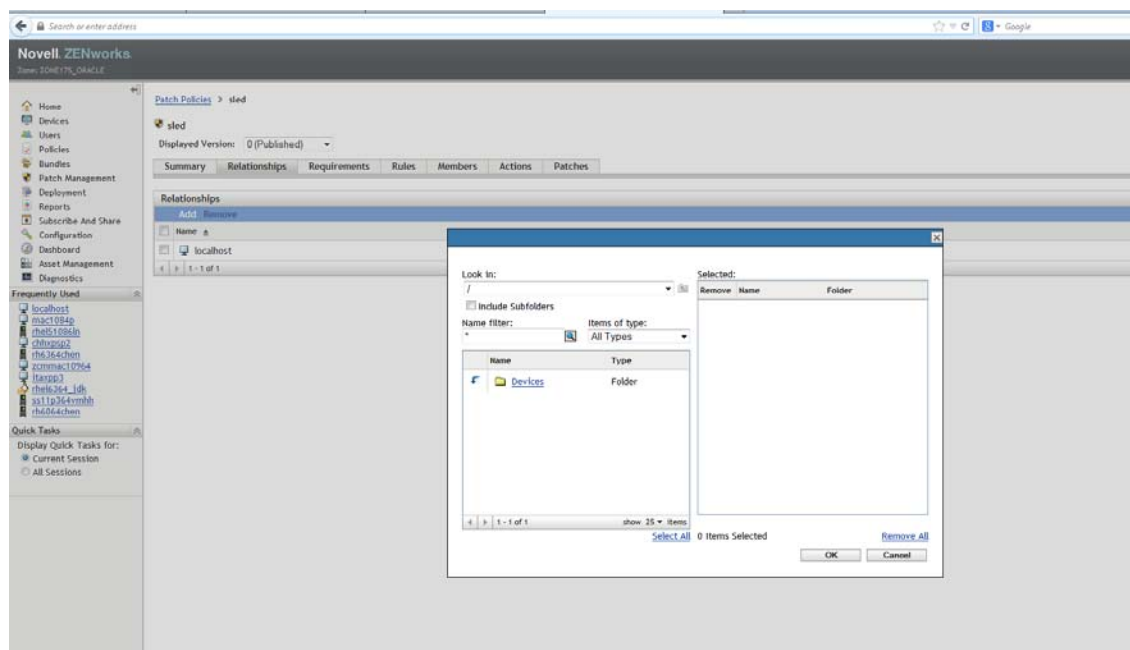
3 Click on the **Relationships** tab



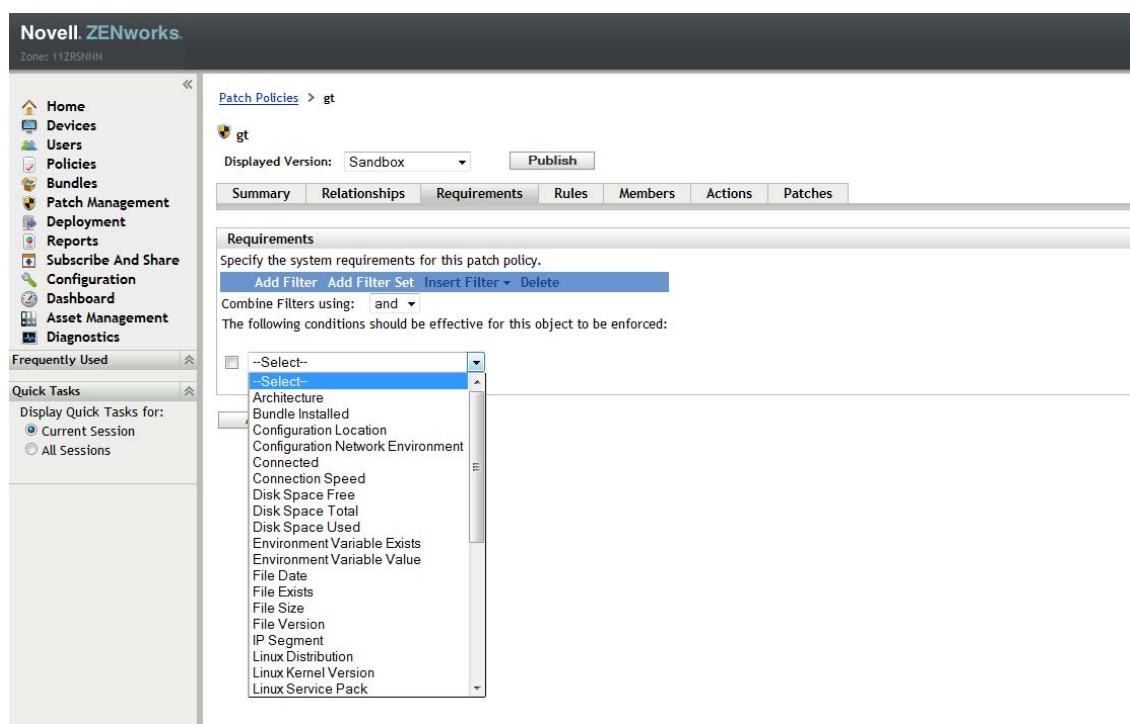
Here you can define which devices that this policy has a relationship to, to proceed click **Add**. A dialog box will open up where you can select the device(s) from your network, as below.

IMPORTANT: If you delete an old patch policy from an endpoint and then publish a new policy to replace it, the endpoint may list a Device-Assigned Bundle Status of Not Installed for an indefinite period of time. If you encounter this endpoint status, reboot the endpoint to complete publication of the patch policy.

Choose the appropriate device and click OK to set changes.



4 Click on the **Requirements** tab.

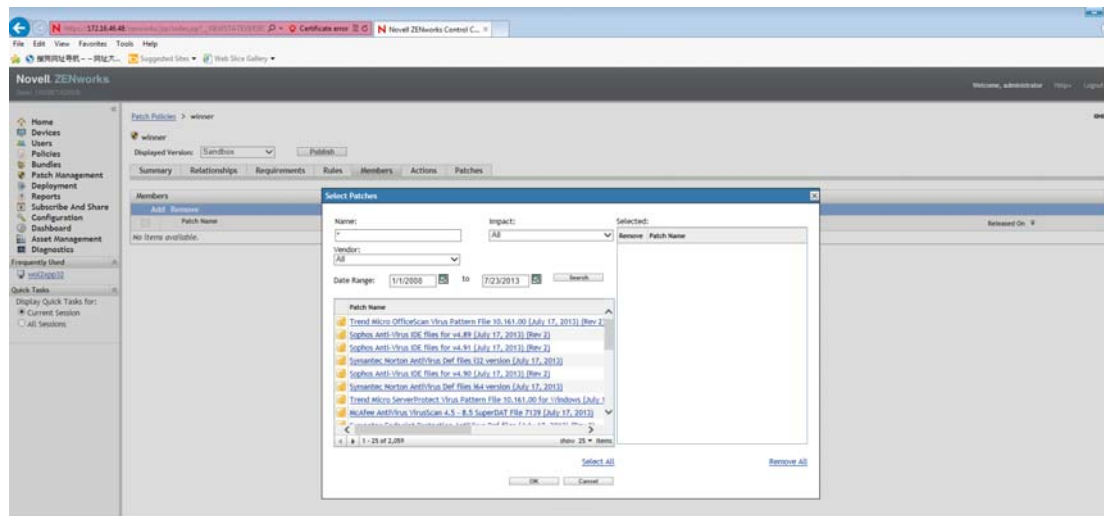


The Requirements tab has a lot of variables to choose from, as listed below:

Filter Item	Result
Architecture	Toggle between 32bit and 64bit
Bundle Installed	Choose between installed bundles

Filter Item	Result
Configuration Location	The location of the server
Configuration Network Environment	Select the network environment
Connected	Connected or Not Connected
Connection Speed	Choose the speed of the connection
Disk Space Free	Select by Disk space available
Disk Space Total	Select by Disk space total
Disk Space Used	Select by Disk space used
Environment Variable Exists	Is there a pre-existing variable
Environment Variable Value	The value of the pre-existing variable
File Date	Select by File date
File Exists	Select by pre-existing File name
IP Segment	Select by pre-existing File date
Linux Distribution	Select the Linux variants to target
Linux Kernel version	Select the Linux Kernel version to target
Linux Service Pack	Select the Service pack version to target
Logged on to Primary Workstation	Select Logged on or not Logged on
Mac Distribution	Select the Mac OS version
Memory	Choose the memory
Novell Client Installed	Novell client installed - yes or no
Operating System- Windows	Choose the Windows variant
Primary User is Logged In	Primary user logged in -yes or no
Processor Family	Select by Processor
Processor Speed	Select by Processor speed
Registry Key Exists	Add a Registry Key and choose yes or no
Registry Key Value	Add a Registry Key value and yes or no
Registry Key and Value Exists	Add a Registry Key and Value and yes or no
Service Exists	Insert a Service name and yes or no
Specified Devices	Add specific devices (has search function)
Version of Application	Select by Application Version
Version of RPM	Select by RPM Version

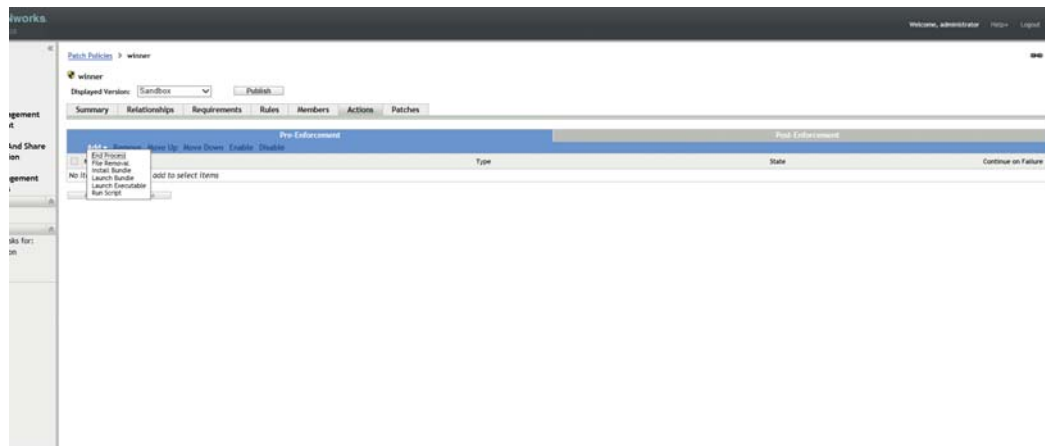
5 Click the **Members** tab.



The Members tab can be used to add additional patches to the Policy.

The patches can be selected by Name, Impact, Date and Vendor, and either added or removed, if you are using this feature in conjunction with other settings it will ensure no duplication of caching, the patch selected will stay as a member of the Policy until it is removed.

6 Click on the **Actions** tab



The Actions tab can be used to specify administrative action before or after a deployment. There are 2 tabs in this menu: Pre-Enforcement and Post-Enforcement.

Click on the **Add** button to open the selection menu, each selection has its own set of custom parameters.

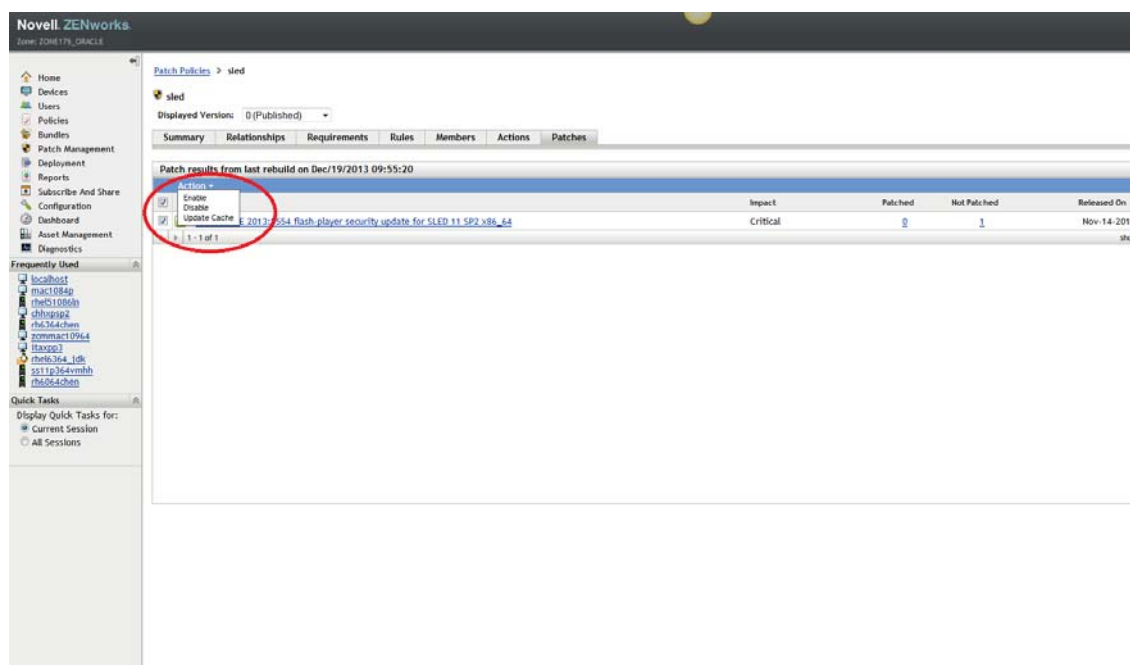
The available Actions are:

End Process	Choose to end a process -i.e. Notepad
File Removal	Choose to remove a file
Install Bundle	Select to install a bundle
Launch Bundle	Select to launch a bundle
Launch Executable	Launch an executable
Run Script	Run a custom script

7 Click on the **Patches** tab

The Patches tab can be used to further refine the choice of patches for deployment.

After a Policy is created the final step is to press the **Rebuild** button. Once this button has been pressed the list of patches in the Patches tab should populate. The purpose of the patches tab is for the user to have control over the deployment of these patches.



Once the list has some patches in it, click **Actions** and it will open a small menu. The options available are **Enable**, **Disable** and **Update Cache**. Check the box next to the patch you wish to take action with and select the appropriate action. Also in the Patches tab there is the usual information about Patch deployment status, impact and Release date.

Testing a Policy before deploying to Live Environment

We advise ZENworks Administrators to always dry run their Policies on a Test device before releasing to a Live environment. Once a Policy is released in a Live environment, rescinding the changes that have been made can be difficult and time consuming.

- 1 First, we need to create the test device:

In the ZCC go to the Devices tab (on the left hand side)

You are presented with a choice of Workstations or Servers, depending on your intentions, choose a device for testing purposes, only Workstations or satellite servers can be configured for test, a Primary Server, whilst operating as such, cannot be used for testing.

- 2 When you have selected the device, check the box and go to the **Actions** menu. Select **Set as Test**.

Once you have made the selection a small yellow arrow will appear on the workstation icon, if you hover the mouse over the workstation icon an info box will appear which says 'Test Workstation'.

- 3 Next, follow the instructions for creating a Patch Policy with the option "Auto approve patches after successful test enforcement". When you have selected the various remediations go to the Relationships tab. Scroll through the list of devices until you find your pre-selected test device.

- 4 Click on the Test device, return to the **Policy Summary** tab and click on the **Rebuild** button

Now you don't need to publish the Patch Policy, only refresh on test device, using the test device will enable the user to measure any changes to the environment, or the functionality of the device before deploying a Policy en masse. This is Best Practice and we recommend the use of test devices prior to all major deployments. The Patch Policy will auto publish to others devices after all patches are applying in Patch Policy.

Scheduling a Patch Policy

Another new feature of Patch Policy is the scheduling function. This is designed to deploy remediation at suitable times to decrease network traffic and strain on the network. The idea is that a policy can be scheduled to be released at different times, or even out of hours. This setting will affect all the policies that are setup and will set the schedule for the deployment.

- 1 Click on "Patch Management" tab.
- 2 Click on Dashboard tab, there are 4 modules. Open the Patch Policy tab. Click New > Patch Policy, or open a previously created policy. Refresh client agent, allowing time for patches to download.

- 3 Return to the ZCC homepage and select the folder 'Configuration'. Click on 'Patch Management Enforcement Settings'. Select 'Schedule Patch Policy Application Time' (Note: Selecting Default setting will require manual intervention)
- 4 Choose a schedule type (Recurring or Date Specific) and choose some parameters for your policy. Select a Reboot Behavior (Default= disabled / Enabled= active) and choose whether Reboot, Cancel or Snooze option will be available to the end user. Click 'Apply' to set the changes.
- 5 Navigate to Agent Device and refresh. The Policy should be deployed in line with the settings that you have specified.

Patch Policy Assignment Wizard

Another new feature of Patch Policy is the scheduling function. This is designed to deploy remediation at suitable times to decrease network traffic and strain on the network. The idea is that a policy can be scheduled to be released at different times, or even out of hours. This setting will affect all the policies that are setup and will set the schedule for the deployment.

- 1 Click on "Patch Management" tab.
- 2 Click on Dashboard tab, there are 4 modules. Open the Patch Policy tab. Click New > Patch Policy, or open a previously created policy. Refresh client agent, allowing time for patches to download.
- 3 Return to the ZCC homepage and select the folder 'Configuration'. Click on 'Patch Management Enforcement Settings'. Select 'Schedule Patch Policy Application Time' (Note: Selecting Default setting will require manual intervention)
- 4 Choose a schedule type (Recurring or Date Specific) and choose some parameters for your policy. Select a Reboot Behavior (Default= disabled / Enabled= active) and choose whether Reboot, Cancel or Snooze option will be available to the end user. Click 'Apply' to set the changes.
- 5 Navigate to Agent Device and refresh. The Policy should be deployed in line with the settings that you have specified.

Patch Policy Enforcement

Another new feature of Patch Policy is the Enforcement function. This is designed to give the user power over the installation time and reboot behaviors for each Patch policy

- 1 Click on **Configuration** tab.
- 2 Navigate down the list to Patch Policy Enforcement settings and enter the page.

- 3 You will be presented with 2 seperate selection boxes, one controls the Schedule and the other sets the Reboot behavior, as below.

Novell. ZENworks

Zone: ZONE175_ORACLE

Home

Devices

Users

Policies

Bundles

Patch Management

Deployment

Reports

Subscribe And Share

Configuration

Dashboard

Asset Management

Diagnostics

Configuration Tasks

[Message Cleanup](#)
[Password Key Generator](#)

Frequently Used

localhost
mac1084p
rhel51086ln
chh:psp2
rh6364chen
zcmmac10964
itax:pp3
rhel6364_jdk
ss11p364vmhh
rh6064chen

Quick Tasks

Display Quick Tasks for:

☒ Current Session
☐ All Sessions

Configuration > Patch Policy Enforcement Settings

Patch Policy Enforcement Settings

Configure the installation time and reboot behavior for patch policies

Schedule

☒ Default (Manually apply patches on the agent using "zac pap")
☐ Schedule patch policy application time

☐ Restrict Duration (stop applying policies after this amount of time)

0 Hours 0 Minutes

Schedule Type:

Date Specific

Start Date(s): *

☐ Run event every year
☐ Process immediately if device unable to execute on schedule

Select when schedule execution should start:

☒ Start immediately at Start Time
☐ Start at a random time between Start and End Times

Start Time:

1 : 00

End Time:

1 : 00

☐ Use Coordinated Universal Time (Current UTC 10:38 PM)

Patch Policy Reboot Behavior

☒ Default Disabled (No reboots or prompts)
☐ Enabled

☒ Notify Users

Description Text

To complete the installation of mandatory patches on your computer, it is now necessary to reboot. If you require any additional information, please contact your Novell ZENworks Patch Management administrator.

Options

Yes

No

Suppress reboot

☐ Yes
☒ No

Allow user to cancel

☒ Yes
☐ No

Allow user to snooze

☒ Yes
☐ No

Snooze interval

10

Minutes

Reboot within

2

Hours

Show tray notification

☒ Yes
☐ No

Tray notification duration

20

Seconds

Tray notification text

Important patches have been installed. In order for these patches to be applied a reboot is required. Please click here to reboot now.

174 ZENworks 11 SP4 Patch Management Reference

The Schedule can be set in 2 ways:

Default, this will require a manual intervention to trigger the policy once its delivered to the target device, this is achieved by opening a command shell and typing 'zac pap'

or

Schedule Patch Policy Application Time. This works in the same way as a normal schedule, as follows:

- 4 Choose a schedule type (Recurring or Date Specific) and choose some parameters for your policy. Select a Reboot Behavior (Default= disabled / Enabled= active) and choose whether Reboot, Cancel or Snooze option will be available to the end user. Click 'Apply' to set the changes. Once completed and deployed navigate to the Agent Device and refresh. The Policy should be deployed in line with the settings that you have specified.
- 5 Reboot Behavior. This can be setup as a preference to when you may require the reboot process to occur. Some patches do require a reboot in order to complete their deployment. As with normal reboot behavior, you are presented with a short list of choices. Once you have made the selection, please click 'Apply'.

Patch Policy Distribution

Further control over the Patch Policy can be exerted in the Patch Policy Distribution settings

- 1 Click on **Configuration** tab.
- 2 Navigate to the Patch Policy Distribution Settings, click and enter the page. You should be presented with a selection menu as below:



- 3 There are 2 choices on this menu.

The Default Setting will make no change, and the behavior will follow that which is set in the Patch Policy Enforcement schedule.

The Schedule setting enables further manipulation and can be set up as below:

- 4 Choose a schedule type (Recurring or Date Specific) and choose some parameters for your policy. Select a Reboot Behavior (Default= disabled / Enabled= active) and choose whether Reboot, Cancel or Snooze option will be available to the end user. Click 'Apply' to set the changes.
- 5 Complete your policy deployment and navigate to Agent Device and refresh. The Policy should be deployed in line with the settings that you have specified.

Patch Policy - Best Practice

In general use the 11.3 Patch Policy function is the most effective and labor saving way to deploy patch remediations across large estates. Once set up it can deliver the patches to the target machines with little fuss and requiring much less oversight than previous incarnations.

Whilst we advocate the automated setup that this function delivers, it is important to remember not to overstretch your systems or the capabilities of the product. So with that in mind we have some Best Practice advice, to enable you to get the best value and least hassle from Zenworks 11.3:

- 1 Keep the policies reasonably simple, try to organise individual Patch Policies around a common outcome, for example: Assuming some of your stock is comprised of Windows 7 machines; setup a policy called Win7 and use this to deliver all MS update remediation to those targets. Similarly, you could organise Policies by Vendor, or Architecture.
- 2 Devise a naming convention for your Policies, this will enable you to track Policies more easily, and will also make it simpler to make changes to individual policies.
- 3 When you are setting up individual Policies try to plan into the Policy. For example: In real terms how often a policy will be deployed, whether that specific vendor has regular updates, what would your expectation be for throughput? It is our general recommendation that you should have a Patch and Vulnerability group to steer your approach to this. This is in line with NIST recommendations.
- 4 When you are designing you policies be careful not to apply conflicting statements. There are a lot of different settings built in to ensure that Policies can perform some very useful tasks, but be aware that changing **Rules, Requirements, Actions, Relationships and Members** may bring your policy into conflict with previously defined settings.
- 5 Choose a schedule type based on network load, for example: it might be advisable to schedule Policy deployments out of hours, or at times when you know that your network will be least busy.
- 6 Use the Patch Policy Enforcement and Distribution settings in **ZCC > Configuration** to their full extent, especially around Reboot settings, why reboot if the patch does not require this?
- 7 Use the Sandbox function to its full extent. We cannot stress how important it is to test patches before deploying them, especially over big networks. It is therefore prudent to set up a test server or a proving ground and deploy to this in the first instance, once there has been a clean and issue free deployment, then you are ready to release to the wider network.
- 8 Don't overload the Policy: we recommend that you don't have more than 50 patches in the rules, this is to keep the policies within a manageable parameter.
- 9 Continually monitor Patch Policies, ensuring that you have the available space and bandwidth to avoid any calamity on your network. If you have large groupings amongst your assets, it may be necessary to stagger deployments, this way you will not impact the integrity of your network, and normal operating can continue alongside the task of protecting against future problems.

- 10 If you delete an old patch policy from an endpoint and then publish a new policy to replace it, the endpoint may list a Device-Assigned Bundle Status of Not Installed for an indefinite period of time. If you encounter this endpoint status, reboot the endpoint to complete publication of the patch policy.

A Patch Management Appendix

The following sections contain detailed explanations of the error messages you might receive or problems you might encounter when using Novell ZENworks 11 SP4 Patch Management.

- ♦ [“Patch Management Issues” on page 179](#)
- ♦ [“Configuration Issues” on page 186](#)
- ♦ [“Error Codes” on page 186](#)
- ♦ [“Patch Management System Variables” on page 195](#)

Patch Management Issues

- ♦ [“Patches are unavailable because of the CDN switch to Akamai for ZENworks Patch Management” on page 179](#)
- ♦ [“No patches are shown in the Patches tab” on page 182](#)
- ♦ [“No vendors are shown in the Select vendors to use in the system options” on page 183](#)
- ♦ [“Patches do not seem to be deployed on the target device” on page 183](#)
- ♦ [“The Cancel button disappears in the Reboot Required dialog box” on page 183](#)
- ♦ [“Superseded patches are shown as NOT APPLICABLE” on page 183](#)
- ♦ [“Patch deployment might not start when scheduled” on page 184](#)
- ♦ [“Microsoft System Installer \(MSI\) might need to be updated for some patches” on page 184](#)
- ♦ [“Remediation of Linux patches displays an error on the SLES 11 SP1 agent” on page 184](#)
- ♦ [““Failed but set to continue” error shows in progress bar” on page 184](#)
- ♦ [“Patch Policy assignment: Bundle stays in ‘Pending’ state forever” on page 185](#)
- ♦ [“Patch Policy assignment: Error Message should be displayed for \(failed\) assignment to older agents” on page 185](#)
- ♦ [“Linux - Custom Patches: Bundles fail to launch” on page 185](#)
- ♦ [“Airgap Server: User receives trial license email after adding the license info to system variables” on page 185](#)

Patches are unavailable because of the CDN switch to Akamai for ZENworks Patch Management

Source: ZENworks 11 SP4; Patch Management.

Explanation: In the week of 18 February 2008, the hosting infrastructure for the patch content Web site used by ZENworks 11 SP4 Patch Management was migrated to Akamai as the new host provider. This switch was done through a global DNS change.

Action: Follow the steps below:

1 Open access to the following Web sites:

- ♦ novell.cdn.lumension.com
- ♦ novell.cdn.heatsoftware.com
- ♦ cdn.lumension.com.edgesuite.net
- ♦ cache.lumension.com
- ♦ a1533.g.akamai.net
- ♦ go.microsoft.com
- ♦ www.download.windowsupdate.com
- ♦ www.download.windowsupdate.nsatc.net
- ♦ download.windowsupdate.chinacache.net
- ♦ download.windowsupdate.com
- ♦ download.skype.com
- ♦ download.microsoft.com
- ♦ cc00022.h.cnccsr.chinacache.net
- ♦ a26.ms.akamai.net
- ♦ wsus.ds.download.windowsupdate.com
- ♦ a767.dscd.akamai.net
- ♦ fg.ds.dl.windowsupdate.com.nsatc.net
- ♦ main-ds.dl.windowsupdate.com.nsatc.net
- ♦ ds.download.windowsupdate.com.edgesuite.net
- ♦ xmlrpc.rhn.redhat.com
- ♦ a248.e.akamai.net
- ♦ cache.patchlinksecure.net
- ♦ rhn.redhat.com
- ♦ www.redhat.com
- ♦ wildcard.redhat.com.edgekey.net
- ♦ wildcard.redhat.com.edgekey.net.globalredir.akadns.net
- ♦ linux-update.oracle.com
- ♦ itrc.hp.com
- ♦ ftp.itrc.hp.com
- ♦ mirror.centos.org
- ♦ vault.centos.org
- ♦ https://getupdates.oracle.com
- ♦ e4579.c.akamaiedge.net
- ♦ nu.novell.com
- ♦ ardownload.adobe.com
- ♦ armdl.adobe.com
- ♦ download.adobe.com
- ♦ swupdl.adobe.com

- ♦ www.adobe.com
- ♦ <http://ftp.mozilla.org>
- ♦ <http://support1.uvnc.com>
- ♦ <http://downloads.sourceforge.net>
- ♦ <http://download.viedolan.org>

NOTE: Adding hosts on ZENworks server, please use "nslookup" on command to get the IP address for each URLs.

2 Test your connectivity to the new hosting provider from your ZENworks Primary Server that the Patch Management feature is currently running on:

- ♦ Ping test:

Log in to the server console, and launch a command prompt or shell window:

```
ping novell.cdn.lumension.com
```

If your server is able to connect to the Akamai hosting network without a problem, you see a response similar to the one shown below:

```
Pinging al533.g.akamai.net [12.37.74.25] with 32 bytes of
data:                                Reply from 12.37.74.25:
bytes=32 time=14ms TTL=55
Reply from 12.37.74.25: bytes=32 time=14ms TTL=55
Reply from 12.37.74.25: bytes=32 time=14ms TTL=55
Reply from 12.37.74.25: bytes=32 time=13ms TTL=55
Ping statistics for 12.37.74.25:      Packets:
    Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds: Minimum =
    13ms, Maximum = 14ms, Average = 13ms
```

The ping command shows you the address of the nearest AKAMAI server to your current location.

If you receive the following message:

```
Ping request could not find host novell.cdn.lumension.com.
Please check the name and try again.
```

The firewall administrator needs to open access to the Akamai network for both ping and HTTP (TCP port 80) traffic.

NOTE: Ping test is a simple way to establish that a server has a route available to reach the server, it is not used by Patch Management in normal operations.

Ping (ICMP) may be blocked by your corporate firewall, or the server may need to pass through a proxy to reach the hosting provider: In these circumstances the Ping test will fail, so other tests will be needed.

- ♦ Browser test:

Using a Web browser, type in the following URL:

```
http://novell.cdn.lumension.com/novell/pulsar.xml
```

The browser should display formatted output from the Web site, as shown in the figure below:

```
- <sub>
- <os name="Windows">
- <arch name="x86">
- <lang name="English">
  <lst> windows/x86/en/applications.lst </lst>
  <lst> windows/x86/en/software.lst </lst>
  <lst ver="XP" spack="3"> windows/x86/en/xpsp3.lst </lst>
  <lst ver="XP" spack="2" legacy="Y"> windows/x86/en/xpsp2.lst </lst>
  <lst ver="XP" spack="1" legacy="Y"> windows/x86/en/xpsp1.lst </lst>
  <lst ver="2000" spack="4"> windows/x86/en/2ksp4.lst </lst>
  <lst ver="2000" spack="3" legacy="Y"> windows/x86/en/2ksp3.lst </lst>
  <lst ver="2003" spack="2"> windows/x86/en/2k3sp2.lst </lst>
  <lst ver="2003" spack="1" legacy="Y"> windows/x86/en/2k3sp1.lst </lst>
  <lst ver="2003" spack="0" legacy="Y"> windows/x86/en/2k3sp0.lst </lst>
  <lst ver="VISTA" spack="0" legacy="Y"> windows/x86/en/vistasp0.lst </lst>
  <lst ver="VISTA" spack="1"> windows/x86/en/vistasp1.lst </lst>
</lang>
```

If your browser cannot access the XML file, you experience a browser timeout and receive some kind of error message. If the ping test succeeds and the browser test fails, this indicates that the firewall administrator has limited access to the Akamai network, but that the HTTP (TCP port 80) is blocked.

The license server is still using the same address as in ZENworks Patch Management 6.4. If you want to enter a serial number to register your Patch Management usage, you need to leave the IP addresses of our old servers in your firewall rules.

NOTE: The server needs to use a proxy to get to the outside world, and the browser isn't configured for the same proxy, then the test in the mentioned would fail.

◆ Firewall information for ZENworks 11 SP4:

ZENworks Patch Management license replication goes to the following servers:

206.16.247.1

206.16.45.33

206.16.45.34

Port 443

ZENworks 11 SP4 Patch Management content replication goes to the following DNS name:

<http://novell.cdn.lumension.com/novell>

To find out what IP your specific server is using, ping novell.cdn.lumension.com from several machines and enter the applicable address range into your firewall rules.

No patches are shown in the Patches tab

Source: ZENworks 11 SP4; Patch Management.

Possible Cause: The server has just been installed.

Action: You need to start the patch subscription download, and then wait twenty minutes or more for patches to be downloaded automatically from novell.patchlink.com.

No vendors are shown in the Select vendors to use in the system options

Source: ZENworks 11 SP4; Patch Management.

Possible Cause: The server has just been installed.

Action: You need to start the patch subscription download, and then wait twenty minutes or more for patches to be downloaded automatically from novell.patchlink.com.

Patches do not seem to be deployed on the target device

Source: ZENworks 11 SP4; Patch Management.

Possible Cause: The ZENworks administrator hasn't deployed the patches into the applicable devices in the ZENworks server, or the patches have been deployed in the server but the device refresh schedule hasn't been triggered in the ZENworks adaptive agent.

Actions: Check to see if the **Device Refresh Schedule** option is set as **Manual Refresh** or **Timed Refresh** on the Configuration tab, and wait for the specified interval.

The Cancel button disappears in the Reboot Required dialog box

Source: ZENworks 11 SP4; Patch Management.

Explanation: When two or more patches are deployed, if the **Allow User to Cancel** option is set as No on the Pre Install Notification Options page and the Notification and Reboot Options page of the server, the **Cancel** button disappears in the Reboot Required dialog box for all patches of the agent.

Action: None necessary.

Superseded patches are shown as NOT APPLICABLE

Source: ZENworks 11 SP4; Patch Management.

Explanation: In earlier releases of Patch Management, a patch showed its status as PATCHED or NOT PATCHED, regardless of whether the patch was new or outdated. This often caused many more patches to show as NOT PATCHED than were actually necessary for deployment to a given target device. This issue has been addressed in many of the new advanced content patches provided with ZENworks 11 SP4:

- ♦ When a patch is superseded, it is automatically disabled.
- ♦ If the patch is re-enabled and detected, in most cases the patch shows as NOT APPLICABLE because it has been replaced by a more recent patch.

Although this is inconsistent with the behavior of earlier versions of Patch Management, this change is an improvement because only the patches that currently need to be installed are reported or analyzed on each device.

Action: None necessary.

Patch deployment might not start when scheduled

Source: ZENworks 11 SP4; Patch Management.

Possible Cause: If the deployment schedule type includes both the **Recurring** and **Process Immediately If the Device Is Unable to Execute** options, when the device becomes active, the deployment of the patch does not start on the first of its scheduled recurring dates. However, the patch is deployed when the next recurring date occurs.

Action: Instead of selecting a recurring schedule, select a date-specific schedule so that the patch is applied when the device becomes active.

Microsoft System Installer (MSI) might need to be updated for some patches

Source: ZENworks 11 SP4; Patch Management.

Explanation: Deployment of certain .NET patches might require that the latest MSI is installed. Otherwise, you might receive errors when deploying those patches.

Action: Prior to deploying .NET patches, verify whether an MSI version is a prerequisite. If necessary, create a bundle to deploy the latest MSI (version 3.1 or later) to your systems. MSIs are available from Microsoft (<http://www.microsoft.com/downloads/details.aspx?familyid=889482fc-5f56-4a38-b838-de776fd4138c&displaylang=en>).

Remediation of Linux patches displays an error on the SLES 11 SP1 agent

Source: ZENworks 11 SP4; Patch Management

Explanation: On a SUSE Linux Enterprise Server (SLES) 11 SP1 x86, when you apply some patches, though they get applied successfully, an error is reported in the bundle system.

Possible Cause: This is a reporting error, related to patches that have java dependencies.

Action: In the jexec script installed by the sun/oracle java rpm in the /etc/init.d folder, after the # Required-Start: \$local_fs line, add the following line: # Required-Stop.

“Failed but set to continue” error shows in progress bar

Source: ZENworks 11 SP4; Patch Management

Explanation: After an 11.2.4 server and agents are set up and some deployments are made, and then following an upgrade from 11.2.4 to 11.3, this error will be shown in the progress bar. The patches ARE installed, but the system can not ‘see’ this. patchReportResult does not action on older agents.

Possible Cause: Mismatch, new actions from the newer architecture are not recognized in older versions. Functionality is NOT affected.

Action: Disable the action in both the deployment and remediation bundles, and immediately refresh the agents to avoid the error.

Patch Policy assignment: Bundle stays in 'Pending' state forever

Source: ZENworks 11 SP4; Patch Management.

Possible Cause: There are issues between bundles and older agents

Action: Bundle Assignment having State as "Not Effective" has a reason associated like "System requirement failed", "Unsociable Type", "Blocked", "Wrong Platform" etc. Similarly we have to define a new State like "Not Effective because Older Agent" and then update the existing logic to set that State while filtering the assignments.

Adding / defining new State for Bundle Assignment has more impact as other components on server might be using the value of Effective State for other computations.

Patch Policy assignment: Error Message should be displayed for (failed) assignment to older agents

Source: ZENworks 11 SP4; Patch Management.

Possible Cause: "Patch bundles assigned through patch policies don't flow down to older version agents than 11.3" message should be displayed on assignment of patch to older version agents.

Action: Assignment can be done from the device side as well as from the object (patch policy/bundle) side. So, various checks are required here i.e. whether the device is an older agent and whether the object type is patch policy.

Also, since multiple objects can be assigned to multiple devices (including folders and groups), the checks need to be iterative which further increases the complexity.

Linux - Custom Patches: Bundles fail to launch

Source: ZENworks 11 SP4; Patch Management.

Possible Cause: RPM Application Bundle and Custom RPM Bundle fails on both SUSE as well as Redhat when it is assigned to the device with Launch Schedule On Device Refresh.

Action: Work around for the custom patch: Add 1-2 minutes of delay execution after refresh for "Remediation Schedule" to resolve it.

Airgap Server: User receives trial license email after adding the license info to system variables

Source: ZENworks 11 SP4; Patch Management.

Explanation: After setting up an airgap server, you receive trial license emails from the server although you've added your license to the airgap server system variables.

Possible Cause: The airgap server requires the Patch Management license file from the connected server.

Action: Contact Novell Support.

Configuration Issues

- ♦ [“Deploying patches with Auto Reboot causes the device to shut down” on page 186](#)

Deploying patches with Auto Reboot causes the device to shut down

Source: ZENworks 11 SP4; Patch Management.

Possible Cause: Trying to deploy patches with auto-reboot might shut down the machine instead of rebooting. It might also fail to report patch results to the ZENworks Server.

Action: Perform reboots with a Quick Task rather than using the Auto Reboot option.

Error Codes

- ♦ [“ERROR CODE: ERROR = 40” on page 187](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_MORE_THAN_MAXAPPLICABLE SIGS = 45” on page 187](#)
- ♦ [“ERROR CODE: PPX_ERROR_ARCHIVE_EXTRACT = 2” on page 188](#)
- ♦ [“ERROR CODE: PPX_ERROR_PACKAGE_ARCHIVE_INITIALIZE = 8” on page 188](#)
- ♦ [“ERROR CODE: PPX_ERROR_EXTRACT_FILE = 20” on page 188](#)
- ♦ [“ERROR CODE: PPX_ERROR_PACKAGE_REIMPORT = 40” on page 188](#)
- ♦ [“ERROR CODE: PPX_ERROR_EXPIRED_LICENSE_KEY = 27” on page 188](#)
- ♦ [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1” on page 188](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 3” on page 188](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 4” on page 188](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_MANY_APPLICABLE_SIGNATURES = 5” on page 189](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 6” on page 189](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 7” on page 189](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 9” on page 189](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 10” on page 189](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 11” on page 189](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 12” on page 189](#)
- ♦ [“ERROR CODE: PPX_ERROR_SIGNATURE_PREREQ_CACHE_EXHAUSTED = 13” on page 189](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 14” on page 189](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 15” on page 189](#)
- ♦ [“ERROR CODE: PPX_ERROR_FINGERPRINT_EXPRESSION_SYNTAX = 16” on page 190](#)
- ♦ [“ERROR CODE: PPX_ERROR_FINGERPRINT_FILEROOT_UNSUPPORTED = 17” on page 190](#)
- ♦ [“ERROR CODE: PPX_ERROR_FINGERPRINT_TYPE_UNSUPPORTED = 18” on page 190](#)
- ♦ [“ERROR CODE: PPX_ERROR_SCRIPT_BAD_FILEHANDLE = 19” on page 190](#)
- ♦ [“ERROR CODE: PPX_ERROR_WMI_FINGERPRINT_UNSUPPORTED = 22” on page 190](#)

- ♦ “ERROR CODE: PPX_ERROR_JAVASCRIPT_UNSUPPORTED = 23” on page 190
- ♦ “ERROR CODE: PPX_ERROR_MISSING_PREREQ_SIGNATURE = 25” on page 190
- ♦ “ERROR CODE: PPX_ERROR_INVALID_PREREQ_LANGUAGE = 26” on page 190
- ♦ “ERROR CODE: PPX_ERROR_INVALID_ROOT_HKEY = 21” on page 190
- ♦ “ERROR CODE: PPX_ERROR_FINGERPRINT_INVALID_SYSINFO = 31” on page 191
- ♦ “ERROR CODE: PPX_ERROR_FINGERPRINT_EXPRESSION_MISSING_VARIABLE = 32” on page 191
- ♦ “ERROR CODE: PPX_ERROR_FINGERPRINT_FILESCAN_UNSUPPORTED = 34” on page 191
- ♦ “ERROR CODE: PPX_ERROR_FINGERPRINT_WMI_ERROR = 35” on page 191
- ♦ “ERROR CODE: PPX_ERROR_RELEVANCE_SCRIPT_SYNTAX = 36” on page 191
- ♦ “ERROR CODE: PPX_ERROR_ENTITLED_FILE_INVALID = 41” on page 191
- ♦ “ERROR CODE: PPX_ERROR_ENTITLED_FILE_MISSING = 28” on page 191
- ♦ “ERROR CODE: PPX_ERROR_ENTITLED_FILE_BAD_CHECKSUM = 29” on page 192
- ♦ “ERROR CODE: PPX_ERROR_ENTITLED_FILE_WRONG_SIZE = 30” on page 192
- ♦ “ERROR CODE: PPX_ERROR_OUT_OF_MEMORY = 24” on page 192
- ♦ “ERROR CODE: PPX_ERROR_PACKAGE_MKDIR_FAILURE = 33” on page 192
- ♦ “ERROR CODE: PPX_ERROR_UNKNOWN” on page 192
- ♦ “ERROR CODE: 41” on page 192
- ♦ “ERROR CODE: 142” on page 192
- ♦ “ERROR CODE: 143” on page 193
- ♦ “ERROR CODE: 144” on page 193
- ♦ “ERROR CODE: 145” on page 193
- ♦ “ERROR MESSAGE: “There is an issue with checksum metadata at CDN”” on page 193
- ♦ “ERROR : zman prb "<baseline_patch_name>" - java.lang.NullPointerException when trying to get the DefaultHibernateSessionManager” on page 193
- ♦ “OTHER ERROR CODES” on page 195

ERROR CODE: ERROR = 40

Source: ZENworks 11 SP4; Patch Management.

Possible Cause: The patch file cached to the ZCM Server is corrupt.

Action: Try recaching the patch to the ZCM Server.

ERROR CODE:

PPX_ERROR_PATCH_MORE_THAN_MAXAPPLICABLE SIGS = 45

Source: ZENWorks 11 SP4; Patch Management.

Possible Cause: The patch file contains more than the maximum applicable signatures.

Action: Notify Novell Support of the error. We will fix the problem with the patch and notify you when it's fixed.

ERROR CODE: PPX_ERROR_ARCHIVE_EXTRACT = 2

Source: ZENworks 11 SP4; Patch Management.

Possible Cause: Extraction of the .cab file or its contents fails.

Action: Follow the steps below.

- 1 Make sure that CABARC runs on the endpoint where the error message appears.
- 2 Check the available disk space on the endpoint.
- 3 Re-cache the patch to the ZCM Server.
- 4 If the issue persists, contact Novell Support.

ERROR CODE: PPX_ERROR_PACKAGE_ARCHIVE_INITIALIZE = 8

Source: See [“ERROR CODE: PPX_ERROR_ARCHIVE_EXTRACT = 2” on page 188.](#)

ERROR CODE: PPX_ERROR_EXTRACT_FILE = 20

Source: See [“ERROR CODE: PPX_ERROR_ARCHIVE_EXTRACT = 2” on page 188.](#)

ERROR CODE: PPX_ERROR_PACKAGE_REIMPORT = 40

Source: See [“ERROR CODE: PPX_ERROR_ARCHIVE_EXTRACT = 2” on page 188.](#)

ERROR CODE: PPX_ERROR_EXPIRED_LICENSE_KEY = 27

Source: ZENworks 11 SP4; Patch Management.

Possible Cause: The .plk license file you are using is outdated or has expired. This error code might also appear if the license file is erased or did not get decrypted properly.

Action: Ensure that you have the latest System Update installed.

ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1

Source: ZENworks 11 SP4; Patch Management.

Possible Cause: You might encounter any of these error codes if a patch has bad metadata.

Action: Contact Novell Support.

ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 3

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1” on page 188.](#)

ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 4

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1” on page 188.](#)

ERROR CODE:**PPX_ERROR_PATCH_MANY_APPLICABLE_SIGNATURES = 5**

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 6

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 7

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 9

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 10

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 11

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 12

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE:**PPX_ERROR_SIGNATURE_PREREQ_CACHE_EXHAUSTED = 13**

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 14

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 15

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE: PPX_ERROR_FINGERPRINT_EXPRESSION_SYNTAX = 16

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE: PPX_ERROR_FINGERPRINT_FILEROOT_UNSUPPORTED = 17

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE: PPX_ERROR_FINGERPRINT_TYPE_UNSUPPORTED = 18

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE: PPX_ERROR_SCRIPT_BAD_FILEHANDLE = 19

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE: PPX_ERROR_WMI_FINGERPRINT_UNSUPPORTED = 22

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE: PPX_ERROR_JAVASCRIPT_UNSUPPORTED = 23

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE: PPX_ERROR_MISSING_PREREQ_SIGNATURE = 25

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE: PPX_ERROR_INVALID_PREREQ_LANGUAGE = 26

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE: PPX_ERROR_INVALID_ROOT_HKEY = 21

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE: PPX_ERROR_FINGERPRINT_INVALID_SYSINFO = 31

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE:

PPX_ERROR_FINGERPRINT_EXPRESSION_MISSING_VARIABLE = 32

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE:

PPX_ERROR_FINGERPRINT_FILESCAN_UNSUPPORTED = 34

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE: PPX_ERROR_FINGERPRINT_WMI_ERROR = 35

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE: PPX_ERROR_RELEVANCE_SCRIPT_SYNTAX = 36

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 188.

ERROR CODE: PPX_ERROR_ENTITLED_FILE_INVALID = 41

Source: ZENworks 11 SP4; Patch Management.

Possible Cause: These error codes indicate possible problems in bundle distribution. The ZCM server might not be able to access a third-party Web site where bundles are located.

Action: Follow the steps below.

- 1 Check your Internet connection and firewall settings.
- 2 Check that the ZCM Server can access a third-party Web site such as the [Microsoft Download Center \(http://www.microsoft.com/downloads/en/default.aspx\)](http://www.microsoft.com/downloads/en/default.aspx).
- 3 Download patches from the third-party Web site.
- 4 Recache the downloaded patches.

ERROR CODE: PPX_ERROR_ENTITLED_FILE_MISSING = 28

Source: See [“ERROR CODE: PPX_ERROR_ENTITLED_FILE_INVALID = 41”](#) on page 191.

ERROR CODE: PPX_ERROR_ENTITLED_FILE_BAD_CHECKSUM = 29

Source: See [“ERROR CODE: PPX_ERROR_ENTITLED_FILE_INVALID = 41” on page 191](#).

ERROR CODE: PPX_ERROR_ENTITLED_FILE_WRONG_SIZE = 30

Source: See [“ERROR CODE: PPX_ERROR_ENTITLED_FILE_INVALID = 41” on page 191](#).

ERROR CODE: PPX_ERROR_OUT_OF_MEMORY = 24

Source: ZENworks 11 SP4; Patch Management.

Possible Cause: This error arises when there is a deficiency in system resources, such as insufficient disk space, low available memory, and so on.

Action: Check the available disk space and memory, then verify that it is sufficient to meet the ZCM Server and Agent requirements.

ERROR CODE: PPX_ERROR_PACKAGE_MKDIR_FAILURE = 33

Source: ZENworks 11 SP4; Patch Management.

Possible Cause: The user has insufficient permissions to carry out the specified action.

Action: Check whether you have appropriate system rights or permissions.

ERROR CODE: PPX_ERROR_UNKNOWN

Source: ZENworks 11 SP4; Patch Management.

Possible Cause: This error is a a general exception. If logging is enabled, the error is recorded in the `.log` file.

Action: Follow the steps below:

- 1 Open a support ticket with Lumension.
- 2 Contact Novell Support.

ERROR CODE: 41

Source: ZENworks 11 SP4; Patch Management.

Possible Cause: This error code implies that ZENworks Patch Management was unable to perform patch remediation. This error occurs when deployment of a different version of the same patch is in progress.

Action: Wait for the previous deployment to complete, then deploy the patch again.

ERROR CODE: 142

Source: ZENworks 11 SP4; Patch Management.

Possible Cause: The selected patch requires certain prerequisites before the patch can be deployed. This error can also occur when package files for a patch are unavailable.

Action: Contact Novell Support and report the patch name. This is most likely a bad patch.

ERROR CODE: 143

Source: ZENworks 11 SP4; Patch Management.

Possible Cause: This error is a general exception. If logging is enabled, the error is recorded in the `.log` file.

Action: Follow the steps below:

- 1 Redeploy the patch.
- 2 If the error persists, file an incident report with Novell.

ERROR CODE: 144

Source: ZENworks 11 SP4; Patch Management.

Possible Cause: This error code appears if there are errors in the patch deployment script. If logging is enabled, the error is recorded in the `.log` file.

Action: File an incident report with Novell.

ERROR CODE: 145

Source: ZENworks 11 SP4; Patch Management.

Possible Cause: The script failed to open the registry. This issue is most probably associated with timing.

Action: Deploy the patch again.

ERROR MESSAGE: "There is an issue with checksum metadata at CDN"

Source: ZENworks 11 SP4; Patch Management.

Possible Cause: There is a problem with not having access to the VEGA content path.

Action: Check the following URL's and see if you can download them:

<http://cache.patchlinksecure.net/PatchComponents/OSPXSet.xml>

<http://cache.lumension.com/patchcomponents/1f12ad89-5711-41ce-ae84-9df6487153f3/win8x64.ospx>

ERROR : zman prb "<baseline_patch_name>" - java.lang.NullPointerException when trying to get the DefaultHibernateSessionManager

Source: ZENworks 11 SP4; Patch Management.

Possible Cause: zman prb "<baseline_patch_name>" is throwing a java.lang.NullPointerException.

This is being caused by code returning a null DefaultHibernateSessionManager.

The following error will be seen:.

Code:

```
com.novell.zenworks.zman.commands.PatchHandler.patchRemoveBaseline()
```

```
Line: 123    DirectServiceStoreImpl dssi = (DirectServiceStoreImpl) store;
```

```
Line: 124    DefaultHibernateSessionManager dsm =  
(DefaultHibernateSessionManager) ((HibernateAbstractSession)  
dssi.getSession()).getSessionManager();
```

```
Line: 125    session = dsm.openSession();
```

StackTrace:

```
java.lang.NullPointerException
```

```
(java.lang.StackTraceElement[])
```

```
[com.novell.zenworks.zman.commands.PatchHandler.patchRemoveBaseline(P  
atchHandler.java:125),
```

```
sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method),
```

```
sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:  
57),
```

```
sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessori  
mpl.java:43),
```

```
java.lang.reflect.Method.invoke(Method.java:606),
```

```
com.novell.zenworks.zman.CommandRunner.execute(CommandRunner.java:9  
4),
```

```
com.novell.zenworks.zman.ZMan.executeRunner(ZMan.java:328),
```

```
com.novell.zenworks.zman.ZMan.runCommand(ZMan.java:531),
```

```
com.novell.zenworks.zman.ZMan.main(ZMan.java:465),
```

```
com.novell.zenworks.zman.ZManExecutor.execute(ZManExecutor.java:101),
```

```
com.novell.zenworks.zman.ZManExecutor.main(ZManExecutor.java:41),
```

```
sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method),
```

```
sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:  
57),
```

```
sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43),
java.lang.reflect.Method.invoke(Method.java:606),
com.novell.zenworks.zman.ZManLoader.loadZMan(ZManLoader.java:59),
com.novell.zenworks.zman.ZManLoader.main(ZManLoader.java:143)]
```

Action: Increase memory size as follows:

modify "JVM_STARTUP_OPTIONS=-Xms64m -Xmx128m" to

"JVM_STARTUP_OPTIONS=-Xms64m -Xmx1024m" in the zman-config.properties file. The

the error disappears and indicates the baseline clears successfully.

Then,

1. Assign a baseline in a group.
2. Refresh agent to receive the baseline.
3. Remove the baseline on the server.
4. Refresh agent again and notice the baseline should remain.
5. Modify memory in the file "zman-config.properties file."
6. Run zman prb "patch name" on the server machine.
5. Refresh agent again

OTHER ERROR CODES

Source: ZENworks 11 SP4; Patch Management.

Action: Contact Novell Support.

Patch Management System Variables

Within ZCC, you can enter system variables to enable/disable certain Patch Management behaviors. See below for a list of variables and how to enter them. You can enter these variables by selecting [Configuration > Configuration Tab > Device Management > System Variables](#).

NOTE: All system variables are case-sensitive.

PATCH_SHOW_BLANK_POLICY

This variable, when set to `true`, opens the Patches tab in a policy that is blank.

Default Value: `false`

Valid Values: `true`, `false`

CONNECTION_TIMEOUT

Enables the adjustment of URL connection timeout duration when downloading patch files (signatures, packages & payloads). Using this system variable can be beneficial when operating in a slow or intermittent network environment.

Default Value: 180 seconds

Valid Range: 0 (infinite) to 3600 seconds (1 hour)

PATCH_POLICY_ACTIONS_LIMIT

Enables adjustments of the maximum number of patch policy actions. Thus, using this system variable allows users finer control of patch policy child bundle actions.

Default Value: 1500 actions

Valid Range: 100 to 99999 actions

PATCH_DAU_SYSTEM_CONTENT

If that is set to `true` then DAU bundles are created with content type of Patch System.

NOTE: If this is not set prior to existing DAU bundles being created, it is necessary to delete the existing DAU bundles and then re-download the subscription update.

Default Value: `false`

Valid Values: `true`, `false`