

Patch Management Reference

ZENworks® 11 SP3

February 2014

Novell.



Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2007-2011 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

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

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide	7
1 What's New in ZENworks 11 SP3	9
1.1 Subscription Download	9
1.1.1 Platform to Download	9
1.1.2 RPM Dependency	9
1.1.3 Download Location For Patch Content	10
1.1.4 Select Vendors To Use In The System	10
1.2 Email Notification	11
1.3 Deployment Options	11
1.4 Patch Management License	12
2 Patch Management Overview	13
2.1 Product Overview	13
2.2 Patch Management Process	14
2.3 Features of Patch Management	15
2.4 Supported ZENworks Server and Agent Environments	16
3 Getting Started with ZENworks 11 SP3 Patch Management	21
3.1 Downloading Patches	21
3.2 Deploying a Patch	21
3.3 Setting a Baseline	22
3.4 Dashboard	22
3.5 Patch Download Status	23
3.6 Patch Wizard	23
4 Using Patch Management	25
4.1 Viewing Subscription Service Information	25
4.2 Configuring the Schedule for Discover Applicable Update Bundles	28
4.2.1 DAU Schedule: Date Specific	31
4.2.2 DAU Schedule: Recurring	32
4.3 DAU Schedule: Set DAU at Folder Level	37
4.4 Configuring HTTP Proxy Detail	39
4.5 Configuring Subscription Download Details	42
4.6 Configuring Patch Subscription Credentials	45
4.6.1 Adding a Credential	47
4.7 Configuring Mandatory Baseline Settings	49
4.8 Configuring Email Notification Details	51
4.9 Configuring Patch Dashboard and Trending Behavior	53
4.10 Patch Management Licensing	57
5 Using the Patch Management Tab	61
5.1 Viewing Patches	61
5.2 Dashboard	62

5.3	Status	65
5.3.1	Status	65
5.3.2	Cache Status	65
5.4	Using the Patches Page	66
5.4.1	Patches	66
5.4.2	Patch Information	77
5.4.3	Searching for a Patch	78
5.4.4	Patch Management	80
5.5	Patch Management BOE Reports	81

6 Using the Deploy Remediation Wizard 83

6.1	Creating a Deployment Schedule	83
6.2	Confirm Devices	84
6.2.1	Confirm Devices: All Non-patched Devices	85
6.2.2	Confirm Devices: Select Applicable Devices	85
6.2.3	Confirm Devices: Select Devices, Folders, and Groups	86
6.3	License Agreement	87
6.4	Remediation Schedule	87
6.4.1	Remediation Schedule: Now	88
6.4.2	Remediation Schedule: Date Specific	89
6.4.3	Remediation Schedule: Recurring	90
6.4.4	Remediation Schedule: Wake On LAN	95
6.5	Deployment Order and Behavior	96
6.6	Remediation Options	97
6.7	Advanced Remediation Options	98
6.8	Pre Install Notification Options	100
6.9	Distribution Schedule	103
6.9.1	Distribution Schedule: No Schedule	103
6.9.2	Distribution Schedule: Date Specific	104
6.9.3	Distribution Schedule: Recurring	105
6.10	Notification and Reboot Options	110
6.10.1	11.3 New variables	112
6.11	Choose Deployment Name	114
6.12	Deployment Summary	115

7 Using Mandatory Baselines 117

7.1	About Mandatory Baselines	117
7.1.1	Viewing Mandatory Baselines	118
7.1.2	Using the Mandatory Baseline Page	120
7.2	Working with Mandatory Baselines	121
7.2.1	Assigning or Managing a Mandatory Baseline	122
7.2.2	Removing a Mandatory Baseline	123
7.2.3	Using Update Cache	124

8 Patch Management for a Device 127

8.1	Accessing the Patches Tab for a Device	127
8.2	Using the Patches Tab for a Device	130
8.2.1	Patches	130
8.2.2	Patch Name	130
8.2.3	Total Number of Patches Available	131
8.2.4	Patch Impacts	131
8.2.5	Patch Statistics	132
8.2.6	Action Menu Items	132
8.2.7	Searching Patches	133

8.2.8	Patch Information	135
8.2.9	Workstation Device Patches	136
9	Patch Management for a Device Group	139
9.1	Using the Patches Tab within a Server Group	139
9.2	Using the Patches Tab within a Workstation Group	141
10	License Behaviour of ZPM	145
10.1	ZCM Only State	145
10.2	Trial State	145
10.3	Trial Expired State	146
10.4	Licensed State	147
10.5	License Expired State	147
11	ZENworks Reporting Reports	149
11.1	Viewing the Predefined Report	149
12	Best Practice with ZENworks 11 SP3 Patch Management	151
12.1	Testing Patches	152
12.2	Deploying Patches in a Controlled Way	152
12.3	Setting a Baseline	153
12.4	Monitoring	153
13	Patch Policy	155
13.1	Setting up a Patch Policy	155
13.2	Publishing Patch Policy	158
13.3	Advanced Configuration for Patch Policy	159
13.4	Testing a Policy before deploying to Live Environment	164
13.5	Scheduling a Patch Policy	165
13.6	Patch Policy Assignment Wizard	165
13.7	Patch Policy Enforcement	166
13.8	Patch Policy Distribution	169
13.9	Patch Policy - Best Practice	171
A	Troubleshooting Patch Management	173
A.1	Patch Management Issues	173
A.2	Configuration Issues	179
A.3	Error Codes	179

About This Guide

This *ZENworks 11 SP3 Patch Management Reference* includes information to help you successfully install a Novell ZENworks 11 SP3 Patch Management system. The information in this guide is organized as follows:

- ◆ Chapter 1, “What’s New in ZENworks 11 SP3,” on page 9
- ◆ Chapter 2, “Patch Management Overview,” on page 13
- ◆ Chapter 3, “Getting Started with ZENworks 11 SP3 Patch Management,” on page 21
- ◆ Chapter 4, “Using Patch Management,” on page 25
- ◆ Chapter 5, “Using the Patch Management Tab,” on page 61
- ◆ Chapter 6, “Using the Deploy Remediation Wizard,” on page 83
- ◆ Chapter 7, “Using Mandatory Baselines,” on page 117
- ◆ Chapter 8, “Patch Management for a Device,” on page 127
- ◆ Chapter 9, “Patch Management for a Device Group,” on page 139
- ◆ Chapter 10, “License Behaviour of ZPM,” on page 145
- ◆ Chapter 11, “ZENworks Reporting Reports,” on page 149
- ◆ Chapter 12, “Best Practice with ZENworks 11 SP3 Patch Management,” on page 151
- ◆ Chapter 13, “Patch Policy,” on page 155
- ◆ Appendix A, “Troubleshooting Patch Management,” on page 173

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 SP3 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 SP3 documentation Web site \(http://www.novell.com/documentation/zenworks113\)](http://www.novell.com/documentation/zenworks113).

1 What's New in ZENworks 11 SP3

The following sections describe the new features and enhancement in Novell ZENworks 11 SP3:

- ♦ [Section 1.1, "Subscription Download," on page 9](#)
- ♦ [Section 1.2, "Email Notification," on page 11](#)
- ♦ [Section 1.3, "Deployment Options," on page 11](#)
- ♦ [Section 1.4, "Patch Management License," on page 12](#)

1.1 Subscription Download

The following sections provide more information on the new features in the subscription download page:

- ♦ [Section 1.1.1, "Platform to Download," on page 9](#)
- ♦ [Section 1.1.2, "RPM Dependency," on page 9](#)
- ♦ [Section 1.1.3, "Download Location For Patch Content," on page 10](#)
- ♦ [Section 1.1.4, "Select Vendors To Use In The System," on page 10](#)

1.1.1 Platform to Download

A new platform has been added to the ZENworks 11 SP3 which is the Mac platform.

This new option will enable you to select the operating system platform for Mac which was not present in the previous version. Now you can select the *Mac* check box, for Mac patches to be downloaded, as shown in the following image:

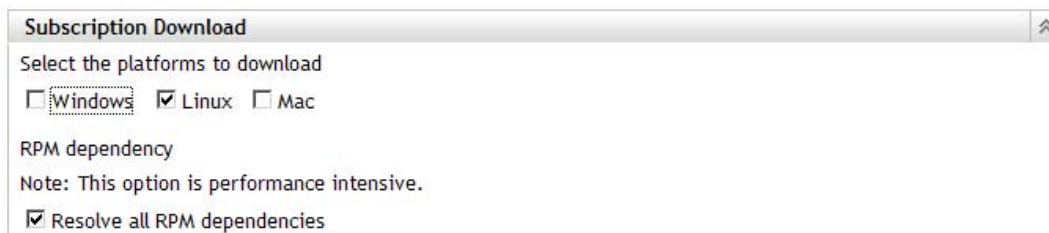
Figure 1-1 Mac Checkbox

Mac

1.1.2 RPM Dependency

The RPM package manager (RPM) is a new feature which will only be enabled when you select the operating system platform for Linux. Now you can select the *Linux* check box, then you can select the *Resolve all RPM Dependencies* to download all the patches, as shown in the following image;

Figure 1-2 RPM Dependency



The check box should only be selected if you want to resolve all the root level dependency as it is very time consuming and performance intensive. It will download all the RPM that are required to patch the particular vulnerabilities.

This is an improvement compared to the previous version. By default it will only download the RPM files required at the top level unless you select the check box to resolve the RPM dependencies.

1.1.3 Download Location For Patch Content

Another new feature that was added is the Download location for patch content. For Linux systems there is not always enough disk space allocated, now you can select the files to be downloaded to the Bundle content directory.

By default it will automatically use ZPM Directory but if you wish to download it to the Bundle content directory just select the radio button.

Figure 1-3 Download location for patch content

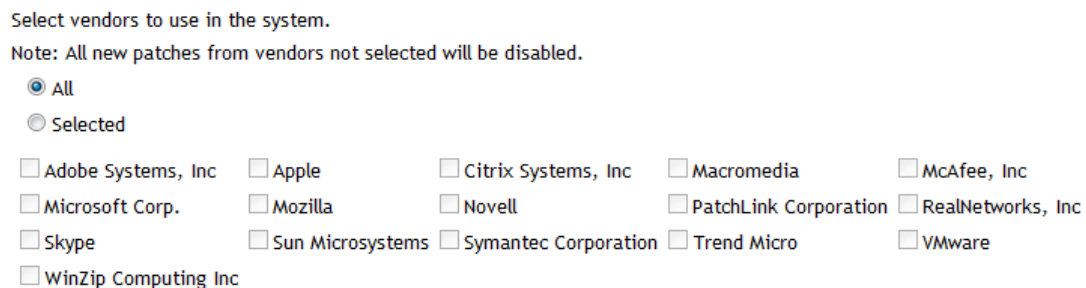


1.1.4 Select Vendors To Use In The System

ZENworks 11 SP3 prompts the user to download only the necessary updates when doing a subscription update. Basically it will only download any new files that are available.

By default the selection is All, but if necessary you can select the particular vendor or bundles that you want to download by selecting the individual check boxes as shown in the following image:

Figure 1-4 Select vendors to use in the system



1.2 Email Notification

ZENworks 11 SP3 has a new feature that allows the users to test if the email server has been configured correctly or not. The user can enter the email addresses to the required fields and then select the Send test email button, which will send a mail to the user.

This new feature will help prevent patch subscription failure. There was previously no option to test whether the email had been configured correctly. The notification process is shown below:

Figure 1-5 Send Test Email

The screenshot shows the 'Email Notification' configuration window. At the top, there is a breadcrumb trail: 'Configuration > Email Notification'. The window title is 'Email Notification' and it contains the instruction: 'Setup email notifications to be delivered when new patches are discovered.' Below this, there is a note: 'Note: The SMTP settings are configured in the log settings section. Separate multiple email addresses with commas.' The form includes three input fields for 'From:', 'To:', and 'Cc:'. A 'Send test email' button is located below the 'Cc:' field. At the bottom of the window, there are four buttons: 'OK', 'Apply', 'Reset', and 'Cancel'.

This email notification page allows you to configure the email notification options when the patch management server detects a new patch. The next time the patch management server detects a new patch, the recipients will receive an email informing them of the same.

1.3 Deployment Options

ZENworks 11 SP3 has a new feature that allows the users to see a message that appears when a it needs to reboot or install.

The administrator can specify the amount of time to allocate to users after this pop-up, before the system will reboot or install, as shown in the following image:

Figure 1-6 Deployment Options

The screenshot shows the 'Deployment Options' configuration window. The window title is 'Deployment Options'. It contains a single input field for 'Time to snooze agent popup' with the value '120' and a unit label 'Seconds'. Below the input field, there are four buttons: 'OK', 'Apply', 'Reset', and 'Cancel'.

A message will pop up in the bottom right hand corner of the screen.

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.

1.4 Patch Management License

ZENworks 11 SP3 now allows the users to add 5 new serial numbers whereas the previous version allowed the user to add only 1 Serial number.

In the image below we can see there are 2 serial numbers that have been added:

Figure 1-7 Multiple patch management license

The user cannot add an invalid serial number and expect it to show up. Only a valid serial number will show up on this page.

If you enter an invalid serial number then you will only be able to enter 3 serial numbers every 10 minutes, as shown in the following image:

Figure 1-8 Entering invalid serial number will allow you to try 3 licenses every 10 minutes.



Error: Only 3 licenses can be entered within a 10 minute period.

2 Patch Management Overview

Novell ZENworks 11 SP3 Patch Management is a part of the ZENworks 11 SP3 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.

- ♦ [Section 2.1, "Product Overview," on page 13](#)
- ♦ [Section 2.2, "Patch Management Process," on page 14](#)
- ♦ [Section 2.3, "Features of Patch Management," on page 15](#)
- ♦ [Section 2.4, "Supported ZENworks Server and Agent Environments," on page 16](#)

2.1 Product Overview

Patch Management is a fully integrated feature of the ZENworks 11 SP3 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 SP3 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.

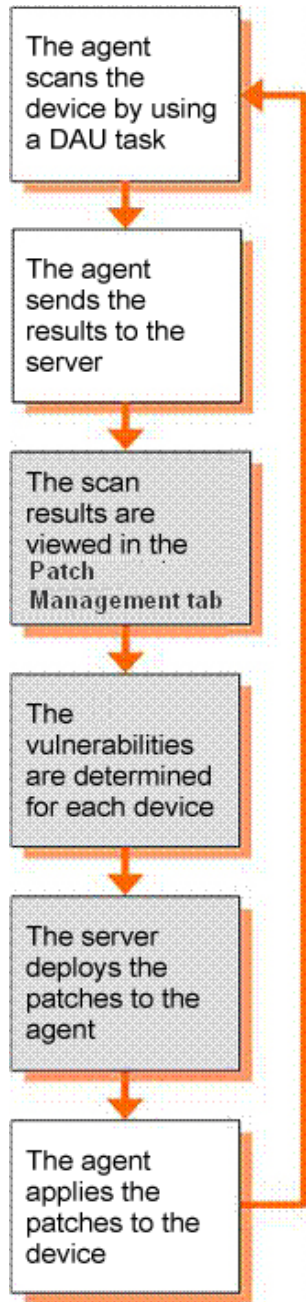
The Patch Management feature stays current with the latest patches and fixes by regular communication with the ZENworks Patch Subscription Network through a secure connection. After the initial 60-day free trial period, the Patch Management feature requires a paid subscription to continue its daily download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

2.2 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 Discover Applicable Updates (DAU) task is scheduled for all ZENworks managed devices (servers and workstations).

For all patches in the DAU 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.

2.3 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.

2.4 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 and Satellite Server Environments

Platform	Version
SUSE Linux Enterprise Server (SLES)	SLES 10 SP3 x86
	SLES 10 SP3 x86_64
	SLES 10 SP3 x86
	SLES 10 SP3 x86_64
	SLES 11 x86
	SLES 11 x86_64
	SLES 11 SP3 x86
	SLES 11 SP3 x86_64
Novell Open Enterprise Server Linux (OES-Linux)	OES 2 SP3 x86
	OES 2 SP3 x86_64
	OES 2 SP3 x86
	OES 2 SP3 x86_64
Microsoft Windows Server	Windows Server 2003 SP3 Standard x86
	Windows Server 2003 SP3 Standard x86_64
	Windows Server 2003 SP3 Enterprise x86
	Windows Server 2003 SP3 Enterprise x86_64
	Windows Server 2008 SP3 Standard x86
	Windows Server 2008 SP3 Standard x86_64
	Windows Server 2008 SP3 Enterprise x86
	Windows Server 2008 SP3 Enterprise x86_64
Windows Server 2008 SP3 Standard x86	

Platform	Version
Red Hat Enterprise Linux (RHEL)	Windows Server 2008 SP3 Standard x86_64
	Windows Server 2008 SP3 Enterprise x86
	Windows Server 2008 SP3 Enterprise x86_64
	Windows Server 2008 R2 Standard x86
	Windows Server 2008 R2 Standard x86_64
	Windows Server 2008 R2 Enterprise x86
	Windows Server 2008 R2 Enterprise x86_64
	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

Table 2-3 Supported ZENworks Satellite Server Environments

Platform	Version
Microsoft Windows	Windows XP SP3 x86
	Windows XP SP3 x86
	Embedded XP SP3
	Windows XP Tablet PC Edition (SP3)
	Windows Vista x86 Enterprise
	Windows Vista x86_64 Enterprise
	Windows Vista x86 Business
	Windows Vista x86_64 Business
	Windows Vista x86 Ultimate
	Windows Vista x86_64 Ultimate
	Embedded Vista
	Windows Vista SP3 x86 Enterprise
	Windows Vista SP3 x86_64 Enterprise
	Windows Vista SP3 x86 Business
	Windows Vista SP3 x86_64 Business
	Windows Vista SP3 x86 Ultimate
	Windows Vista SP3 x86_64 Ultimate

Platform	Version
	Embedded Vista SP3
	Windows Vista SP3 x86 Enterprise
	Windows Vista SP3 x86_64 Enterprise
	Windows Vista SP3 x86 Business
	Windows Vista SP3 x86_64 Business
	Windows Vista SP3 x86 Ultimate
	Windows Vista SP3 x86_64 Ultimate
	Embedded Vista SP3
	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

The following environments support installation of the ZENworks agent:

Table 2-4 Supported Agent Environments

Platform	Version
Microsoft Windows Server	Windows Server 2003 SP3 Standard x86
	Windows Server 2003 SP3 Standard x86_64
	Windows Server 2003 SP3 Enterprise x86
	Windows Server 2003 SP3 Enterprise x86_64
	Windows Server 2008 SP3 Standard x86
	Windows Server 2008 SP3 Standard x86_64
	Windows Server 2008 SP3 Enterprise x86
	Windows Server 2008 SP3 Enterprise x86_64
	Windows Server 2008 SP3 Standard x86
	Windows Server 2008 SP3 Standard x86_64
	Windows Server 2008 SP3 Enterprise x86
	Windows Server 2008 SP3 Enterprise x86_64
	Windows Server 2008 R2 Standard x86
	Windows Server 2008 R2 Standard x86_64
	Windows Server 2008 R2 Enterprise x86

Platform	Version
Microsoft Windows	Windows Server 2008 R2 Enterprise x86_64
	Windows XP SP3 x86
	Windows XP SP3 x86
	Embedded XP SP3
	Windows XP Tablet PC Edition (SP3)
	Embedded Vista
	Windows Vista SP3 x86 Enterprise
	Windows Vista SP3 x86_64 Enterprise
	Windows Vista SP3 x86 Business
	Windows Vista SP3 x86_64 Business
	Windows Vista SP3 x86 Ultimate
	Windows Vista SP3 x86_64 Ultimate
	Embedded Vista SP3
	Windows Vista SP3 x86 Enterprise
	Windows Vista SP3 x86_64 Enterprise
	Windows Vista SP3 x86 Business
	Windows Vista SP3 x86_64 Business
	Windows Vista SP3 x86 Ultimate
	Windows Vista SP3 x86_64 Ultimate
	Embedded Vista SP3
	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	
SUSE Linux Enterprise Desktop (SLED)	SLED 10 x86
	SLED 10 x86_64
	SLED 11 x86
	SLED 11 x86_64
SUSE Linux Enterprise Server (SLES)	SLES 10 SP3 x86
	SLES 10 SP3 x86_64
	SLES 10 SP3 x86

Platform	Version
	SLES 10 SP3 x86_64
	SLES 11 x86
	SLES 11 x86_64
	SLES 11 SP3 x86
	SLES 11 SP3 x86_64
Novell Open Enterprise Server Linux (OES-Linux)	OES 2 SP3 x86
	OES 2 SP3 x86_64
	OES 2 SP3 x86
	OES 2 SP3 x86_64
Red Hat Enterprise Linux (RHEL)	RHEL 4.6 x86
	RHEL 4.6 x86_64
	RHEL 4.7 x86
	RHEL 4.7 x86_64
	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

3 Getting Started with ZENworks 11 SP3 Patch Management

Patch Management is a fully integrated feature of Novell ZENworks 11 SP3 that provides the same agent-based patch, vulnerability patch, and compliance management solution that was used in prior versions.

The ZENworks Server schedules a Discover Applicable Updates (DAU) 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 ZENworks 11 SP3 Patch Management:

- [Section 3.1, "Downloading Patches," on page 21](#)
- [Section 3.2, "Deploying a Patch," on page 21](#)
- [Section 3.3, "Setting a Baseline," on page 22](#)
- [Section 3.4, "Dashboard," on page 22](#)
- [Section 3.5, "Patch Download Status," on page 23](#)
- [Section 3.6, "Patch Wizard," on page 23](#)

3.1 Downloading Patches

Before you start downloading a patch, configure the downloading options in the *Configuration* tab. For more information, see [Section 4.5, "Configuring Subscription Download Details," on page 42](#).

3.2 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 83](#).

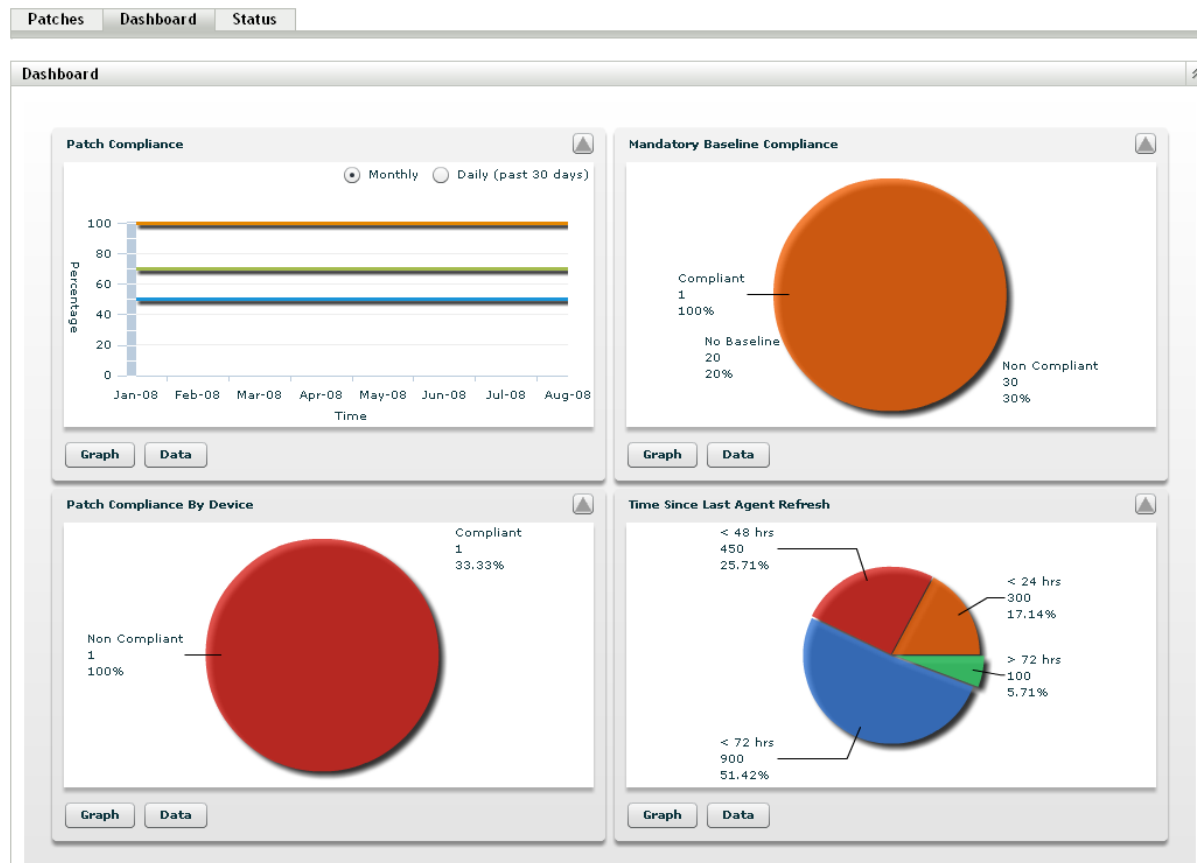
3.3 Setting a Baseline

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 117.

3.4 Dashboard

The Dashboard tab contains graphs that allow users a direct overview of the devices in the network. For more information, see [Section 5.2, "Dashboard,"](#) on page 62.

Figure 3-1 Dashboard Page



3.5 Patch Download Status

The Status page consists of the system and cache statuses, which show the overall patch information. For more information, see [Section 5.3, “Status,” on page 65](#).

Figure 3-2 Status Page

Patches Dashboard Status		
Status		
Name	Status	
Signature Download	Complete	
Last Signature Download Time	Apr/02/2009 09:45:24	
Bundle Download	In Progress	
Last Patch Download	Apr/02/2009 09:45:29	
Number of Failed Download(s)	9	
Number of Patches Queued for Caching	103	
Number of Active Patches	1268	
Number of New Patches(less than 30 days)	77	
Latest Patch Released On	Apr/01/2009 00:00:00	
Cache Status		
Name	Status	Error Detail (if any)
Adobe APSB09-03 APSB09-04 Reader (English) 9.1 Security Update for Windows (Rev 2)	Queued	
F-Secure Anti-Virus DEF File (March 25, 2009)	Queued	
MS09-007 Security Update for Windows 2000 (KB960225)	Queued	
MS09-008 Security Update for Windows 2000 (KB961063)	Queued	
Symantec Norton AntiVirus Def files x86 version (March 30, 2009)	Queued	
MS09-008 Security Update for Windows Server 2008 (KB961063)	Queued	
MS09-008 Security Update for Windows Server 2003 (KB961064)	Queued	
MS08-052 Security Update for Windows Server 2003 (KB938464)	Queued	
MS09-008 Security Update for Windows Server 2003 (KB961063)	Queued	
Adobe APSB09-03 APSB09-04 Reader 7.1.1 Security Update for Windows (All Languages)	Queued	
1 - 10 of 112		show 10 items

3.6 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 72](#)

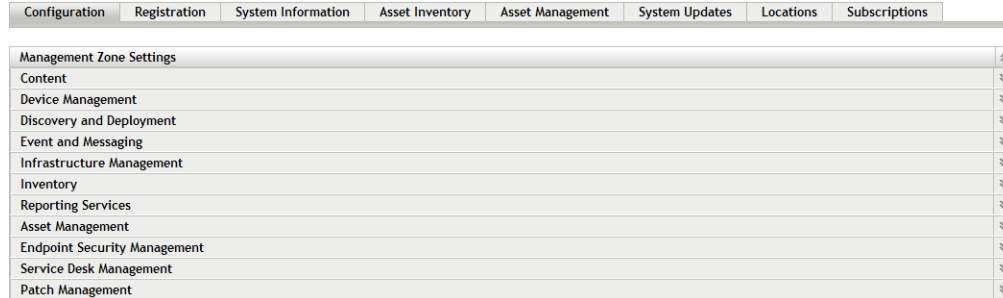
4 Using Patch Management

Novell ZENworks 11 SP3 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:

- [Section 4.1, “Viewing Subscription Service Information,” on page 25](#)
- [Section 4.2, “Configuring the Schedule for Discover Applicable Update Bundles,” on page 28](#)
- [Section 4.3, “DAU Schedule: Set DAU at Folder Level,” on page 37](#)
- [Section 4.4, “Configuring HTTP Proxy Detail,” on page 39](#)
- [Section 4.5, “Configuring Subscription Download Details,” on page 42](#)
- [Section 4.6, “Configuring Patch Subscription Credentials,” on page 45](#)
- [Section 4.7, “Configuring Mandatory Baseline Settings,” on page 49](#)
- [Section 4.8, “Configuring Email Notification Details,” on page 51](#)
- [Section 4.9, “Configuring Patch Dashboard and Trending Behavior,” on page 53](#)
- [Section 4.10, “Patch Management Licensing,” on page 57](#)

4.1 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*.

Eight links—*Subscription Service Information, Schedule Discover Applicable Update Bundles, Schedule Discover Applicable Update Bundles Install, Schedule Discover Applicable Update Bundles Distribution, Configure HTTP Proxy, Subscription Download, Patch Subscription Credentials, Mandatory Baseline Settings, Email Notification, Dashboard and Trending, and Deployment Options*—are displayed:

Configuration	Registration	System Information	Asset Inventory	Asset Management	System Updates	Locations	Subscriptions
Management Zone Settings							
Content							
Device Management							
Discovery and Deployment							
Event and Messaging							
Infrastructure Management							
Inventory							
Reporting Services							
Asset Management							
Endpoint Security Management							
Service Desk Management							
Patch Management							
Category		Description					
Subscription Service Information		View subscription log and update subscription settings					
Schedule Discover Applicable Update Bundles Install		This will allow the DAU Bundle to be configured on when to install fingerprints.					
Schedule Discover Applicable Update Bundles Distribution		This will allow the DAU Bundle to be configured on when to distribute fingerprints.					
Configure HTTP Proxy		Configure HTTP Proxy for access to the Internet patch subscription					
Subscription Download		Configure subscription download options					
Patch Subscription Credentials		Configure the credentials for each of the Subscription providers					
Mandatory Baseline Settings		Set global values for how mandatory baseline installs will behave.					
Email Notification		Setup email notifications to be delivered when new patches are discovered.					
Dashboard and Trending		Configure Patch Dashboard and Trending behavior					

3 Click the *Subscription Service Information* link.

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

[Configuration](#) > **Subscription Service Information** 🔍

Subscription Service Information ✕

View subscription log and update subscription settings

Subscription Service Information ⤴

Start the Subscription Service /Devices/Servers/airgap ▾ Service Running

Last Subscription Poll 11/10/09 10:12 PM

Subscription Replication Status Complete

Subscription Host novell.patchlink.com

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

Reset ZENworks Patch Management Settings

Subscription Service History ⤴

Action ▾						
Type	Status	Start Date	End Date	Duration	Successful	Error Detail (if any)
Licenses	Complete	11/10/09 10:29 PM	11/10/09 10:29 PM	00:00:00	false	
Bundles	In Progress	11/10/09 10:07 PM		01:30:55	true	
Patches	Complete	11/10/09 10:12 PM	11/10/09 10:23 PM	00:11:25	true	

OK Apply Reset Cancel

The Subscription Service Information page displays all the information about your subscription, including the status. You can also update your subscription settings on this page.

You can refresh the subscription information by clicking the *Action* drop-down list on the Subscription Information page and selecting the *Refresh* option, as shown in the following figure:



The following table describes each status item featured on the Subscription Service Information page:

Status Item	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 <i>Start</i> button to start the subscription service.</p> <ul style="list-style-type: none"> ◆ After the subscription service starts running, the <i>Start</i> button reads <i>Service Running</i>. ◆ 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 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.

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

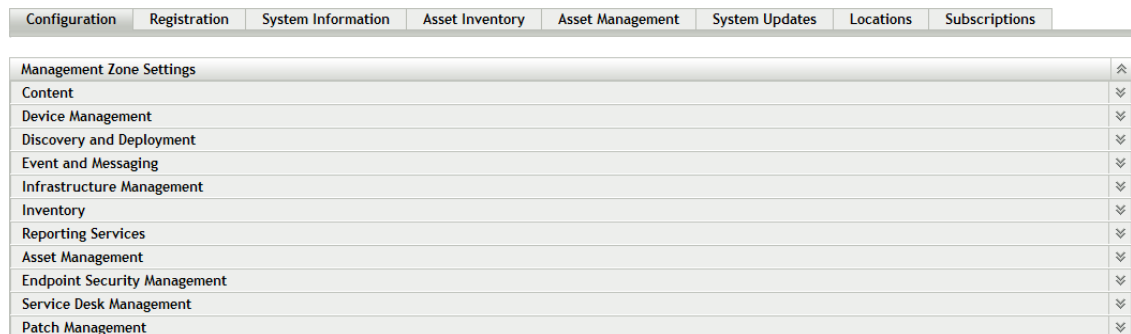
Button	Action
<i>OK</i>	Enables you to go back to the Configuration page.
<i>Apply</i>	Enables you to save the changes made to the Subscription Communication Interval.
<i>Reset</i>	Enables you to reset the replication status and initiate a complete replication with the ZENworks Patch Subscription Network.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

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

4.2 Configuring the Schedule for Discover Applicable Update Bundles

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



- Click *Patch Management* to display the eight links (*Subscription Service Information, Schedule Discover Applicable Update Bundles, Configure HTTP Proxy, Subscription Download, Patch Subscription Credentials, Mandatory Baseline Settings, Email Notification, and Dashboard and Trending*):

Configuration		Registration	System Information	Asset Inventory	Asset Management	System Updates	Locations	Subscriptions
Management Zone Settings								
Content								
Device Management								
Discovery and Deployment								
Event and Messaging								
Infrastructure Management								
Inventory								
Reporting Services								
Asset Management								
Endpoint Security Management								
Service Desk Management								
Patch Management								
Category	Description							
Subscription Service Information	View subscription log and update subscription settings							
Schedule Discover Applicable Update Bundles Install	This will allow the DAU Bundle to be configured on when to install fingerprints.							
Schedule Discover Applicable Update Bundles Distribution	This will allow the DAU Bundle to be configured on when to distribute fingerprints.							
Configure Http Proxy	Configure HTTP Proxy for access to the Internet patch subscription							
Subscription Download	Configure subscription download options							
Patch Subscription Credentials	Configure the credentials for each of the Subscription providers							
Mandatory Baseline Settings	Set global values for how mandatory baseline installs will behave.							
Email Notification	Setup email notifications to be delivered when new patches are discovered.							
Dashboard and Trending	Configure Patch Dashboard and Trending behavior							

- Click the *Schedule Discover Applicable Update Bundles* link. The Schedule Discover Applicable Update Bundles page appears:

[Configuration](#) > [Schedule Discover Applicable Update Bundles Install](#) ES ▾

Schedule Discover Applicable Update Bundles Install ✕

This will allow the DAU Bundle to be configured on when to install fingerprints.

Schedule ⤴

Run DAU on refresh

Select a schedule to launch DAU on patch 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 8:40 AM)

Schedule Discover Applicable Update Bundles Distribution ✕

This will allow the DAU Bundle to be configured on when to distribute fingerprints.

Schedule ⤴

Distribute DAU on Launch

Select a schedule to distribute the DAU content

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 8:43 AM)

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

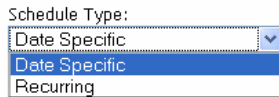
The following table describes the main options on the Schedule Discover Applicable Update Bundles page:

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

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

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

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



Patch Management offers two types of schedules to determine when a DAU 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.

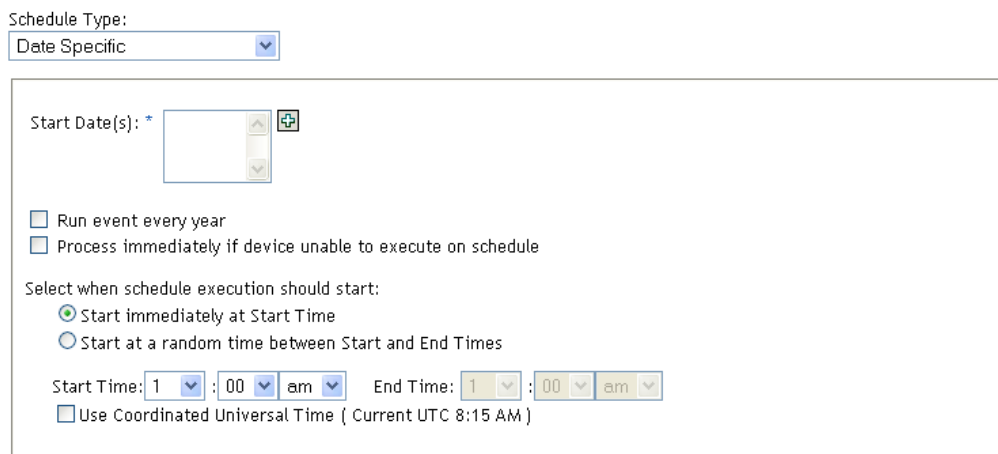
The following sections provide more information on schedule types:

- ◆ [Section 4.2.1, “DAU Schedule: Date Specific,” on page 31](#)
- ◆ [Section 4.2.2, “DAU Schedule: Recurring,” on page 32](#)



4.2.1 DAU Schedule: Date Specific

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

Figure 4-1 DAU Schedule Section for the Date Specific Schedule Type

A screenshot of the DAU Schedule section for the 'Date Specific' schedule type. The 'Schedule Type' dropdown is set to 'Date Specific'. Below it, there is a 'Start Date(s): *' field with a calendar icon and a remove icon. There are two checkboxes: 'Run event every year' and 'Process immediately if device unable to execute on schedule'. Under the heading 'Select when schedule execution should start:', there are two radio buttons: 'Start immediately at Start Time' (selected) and 'Start at a random time between Start and End Times'. Below this, there are time selection fields for 'Start Time' (1:00 am) and 'End Time' (1:00 am). At the bottom, there is a checkbox for 'Use Coordinated Universal Time (Current UTC 8:15 AM)'.

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: :

- ♦ **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: :

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.

4.2.2 DAU Schedule: Recurring

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

Figure 4-2 DAU Schedule Section for the Recurring Schedule Type

Schedule Type:

When a device is refreshed

Delay execution after refresh: Days Hours 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: :

[More Options](#)

Monthly

Day of the month:

Last day of the month

First

Start Time: :

[More Options](#)

Fixed Interval

Months Weeks Days Hours Minutes

Start Date: Start Time: :

[More Options](#)

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

- ◆ [“When a Device Is Refreshed” on page 33](#)
- ◆ [“Days of the Week” on page 34](#)
- ◆ [“Monthly” on page 35](#)
- ◆ [“Fixed Interval” on page 36](#)

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*



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

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

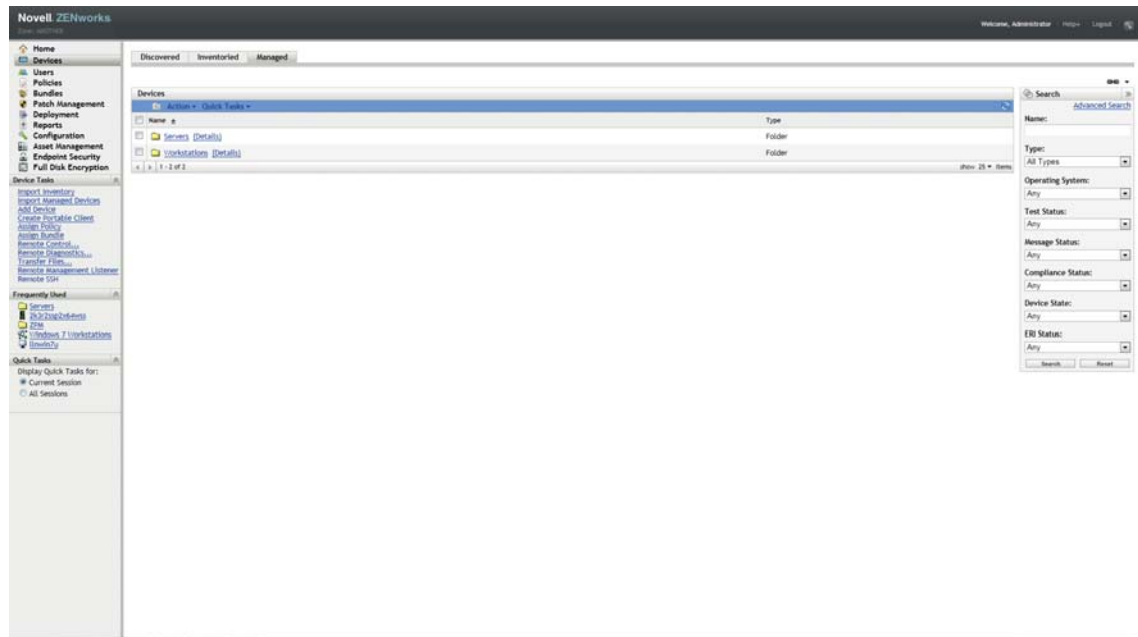
0 Months 0 Weeks 0 Days 0 Hours 0 Minutes
Start Date: 10/25/2011 Start Time: 1 :00
[Hide Options](#)

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)

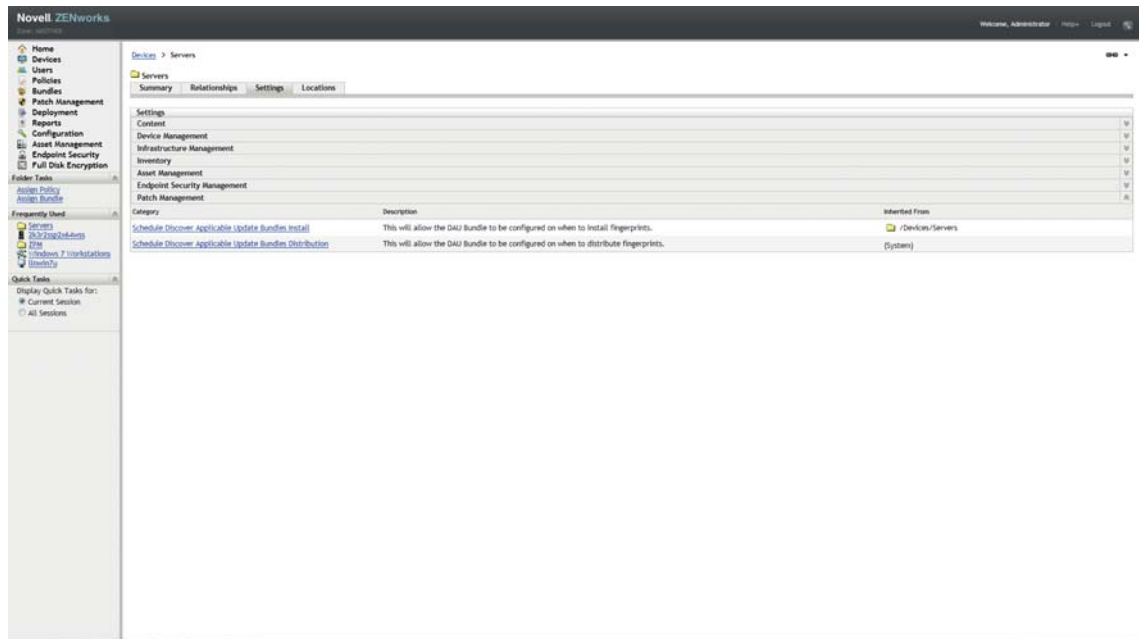
4.3 DAU Schedule: Set DAU at Folder Level

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

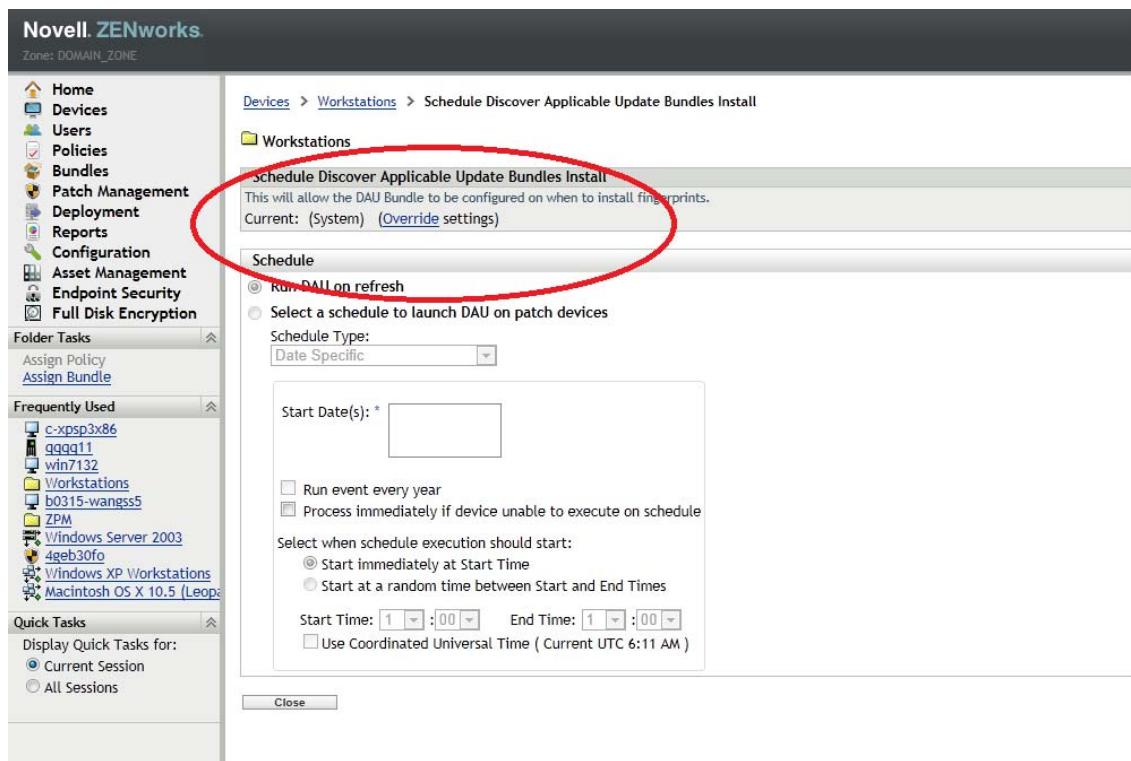
- 1 Click the Devices tab in the left panel to display the Devices page. This will present a choice between Servers and Workstations.



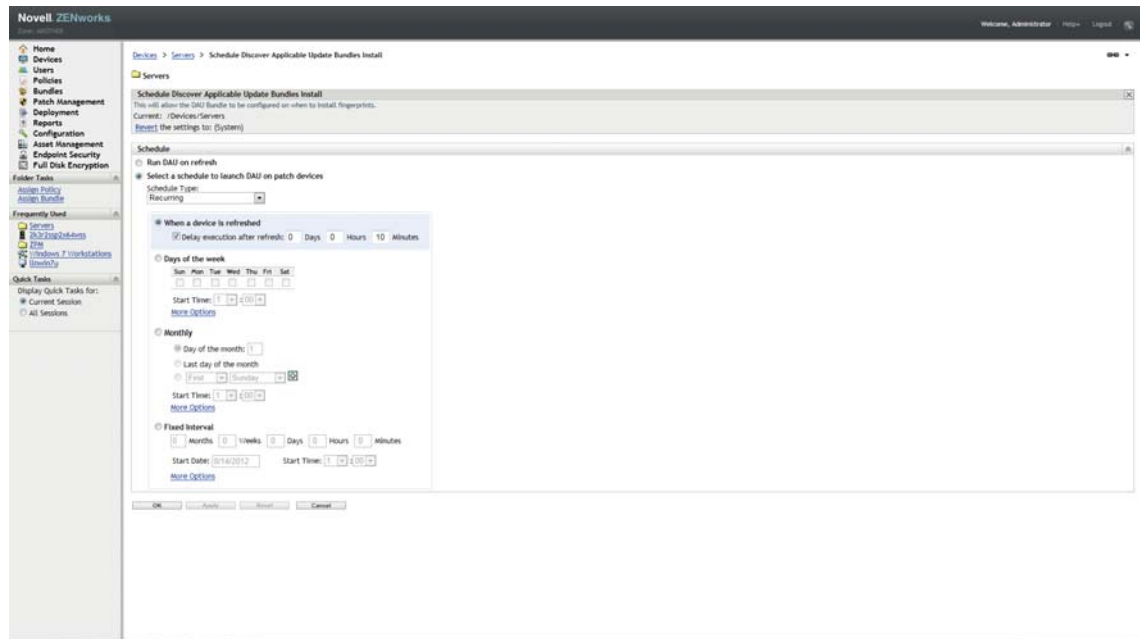
- 2 Choose the Devices that you want to set a schedule for and click on the Details link. Then select the Settings tab. This will present two options for scheduling Install and Distribution. Select which schedule you would like to change.



- 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.



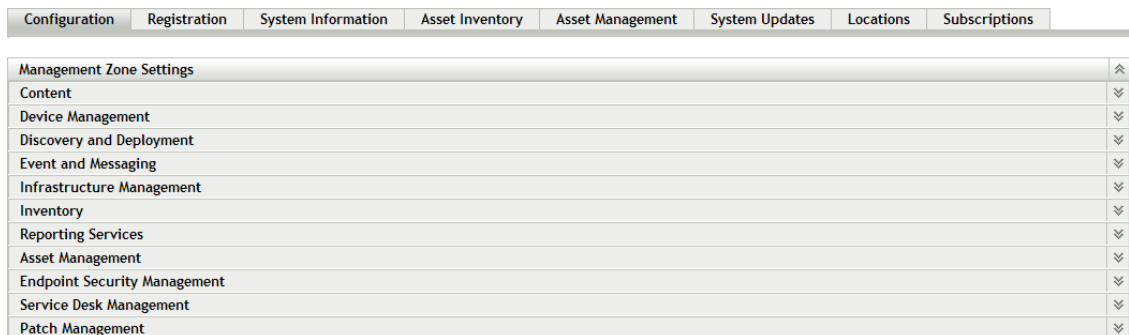
- Select your desired schedule for the DAU, as described in the previous section.



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

4.4 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 eight links (*Subscription Service Information, Schedule Discover Applicable Update Bundles Install, Schedule Discover Applicable Update Bundles Distribution, Configure HTTP Proxy, Subscription Download, Patch Subscription Credentials, Mandatory Baseline Settings, Email Notification, Dashboard and Trending, and Deployment Options*): *Schedule Discover Applicable Update Bundles*,

Configuration	Registration	System Information	Asset Inventory	Asset Management	System Updates	Locations	Subscriptions
Management Zone Settings							
Content							
Device Management							
Discovery and Deployment							
Event and Messaging							
Infrastructure Management							
Inventory							
Reporting Services							
Asset Management							
Endpoint Security Management							
Service Desk Management							
Patch Management							
Category		Description					
Subscription Service Information		View subscription log and update subscription settings					
Schedule Discover Applicable Update Bundles Install		This will allow the DAU Bundle to be configured on when to install fingerprints.					
Schedule Discover Applicable Update Bundles Distribution		This will allow the DAU Bundle to be configured on when to distribute fingerprints.					
Configure Http Proxy		Configure HTTP Proxy for access to the Internet patch subscription					
Subscription Download		Configure subscription download options					
Patch Subscription Credentials		Configure the credentials for each of the Subscription providers					
Mandatory Baseline Settings		Set global values for how mandatory baseline installs will behave.					
Email Notification		Setup email notifications to be delivered when new patches are discovered.					
Dashboard and Trending		Configure Patch Dashboard and Trending behavior					

Configuration	Registration	System Information	Asset Inventory	Asset Management	System Updates	Locations	Subscriptions
Management Zone Settings							
Content							
Device Management							
Discovery and Deployment							
Event and Messaging							
Infrastructure Management							
Inventory							
Reporting Services							
Asset Management							
Endpoint Security Management							
Service Desk Management							
Patch Management							
Category		Description					
Subscription Service Information		View subscription log and update subscription settings					
Schedule Discover Applicable Update Bundles Install		This will allow the DAU Bundle to be configured on when to install fingerprints.					
Schedule Discover Applicable Update Bundles Distribution		This will allow the DAU Bundle to be configured on when to distribute fingerprints.					
Configure Http Proxy		Configure HTTP Proxy for access to the Internet patch subscription					
Subscription Download		Configure subscription download options					
Patch Subscription Credentials		Configure the credentials for each of the Subscription providers					
Mandatory Baseline Settings		Set global values for how mandatory baseline installs will behave.					
Email Notification		Setup email notifications to be delivered when new patches are discovered.					
Dashboard and Trending		Configure Patch Dashboard and Trending behavior					

3 Click the *Configure HTTP Proxy* link. The Proxy Server Details page appears:

[Configuration](#) > [Configure Http Proxy](#)

Configure Http Proxy
Configure HTTP Proxy for access to the Internet patch subscription

HTTP Proxy Server Details

Proxy Host

Port

Requires Authentication?

User Name

Password

Confirm Password

OK Apply Reset Cancel

The Proxy Server Details 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 field on the Proxy Server Details page:

Item	Description
<i>Proxy Host</i>	The proxy address used to connect to the ZENworks Patch Subscription Network.
<i>Port</i>	The proxy port used to connect to ZENworks Patch Subscription Network.
<i>Requires Authentication</i>	Selecting this check box ensures that the Proxy server can be used only after user authentication. If you select the check box, the <i>User Name</i> and <i>Password</i> fields are enabled.
<i>User Name</i>	User's name used for authentication.
<i>Password</i>	User's password used for authentication.
<i>Confirm Password</i>	User's password for confirmation.

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

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

4.5 Configuring Subscription Download Details

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

Configuration	Registration	System Information	Asset Inventory	Asset Management	System Updates	Locations	Subscriptions
Management Zone Settings							
Content							
Device Management							
Discovery and Deployment							
Event and Messaging							
Infrastructure Management							
Inventory							
Reporting Services							
Asset Management							
Endpoint Security Management							
Service Desk Management							
Patch Management							

- 2 Click *Patch Management* to display the eight links (Subscription Service Information, Schedule Discover Applicable Update Bundles Install, Schedule Discover Applicable Update Bundles Distribution, Configure HTTP Proxy, Subscription Download, Patch Subscription Credentials, Mandatory Baseline Settings, Email Notification, Dashboard and Trending, and Deployment Options):

Configuration	Registration	System Information	Asset Inventory	Asset Management	System Updates	Locations	Subscriptions
Management Zone Settings							
Content							
Device Management							
Discovery and Deployment							
Event and Messaging							
Infrastructure Management							
Inventory							
Reporting Services							
Asset Management							
Endpoint Security Management							
Service Desk Management							
Patch Management							
Category	Description						
Subscription Service Information	View subscription log and update subscription settings						
Schedule Discover Applicable Update Bundles Install	This will allow the DAU Bundle to be configured on when to install fingerprints.						
Schedule Discover Applicable Update Bundles Distribution	This will allow the DAU Bundle to be configured on when to distribute fingerprints.						
Configure Http Proxy	Configure HTTP Proxy for access to the Internet patch subscription						
Subscription Download	Configure subscription download options						
Patch Subscription Credentials	Configure the credentials for each of the Subscription providers						
Mandatory Baseline Settings	Set global values for how mandatory baseline installs will behave.						
Email Notification	Setup email notifications to be delivered when new patches are discovered.						
Dashboard and Trending	Configure Patch Dashboard and Trending behavior						

3 Click the *Subscription Download* link to display the Subscription Download Options page:

[Configuration](#) > Subscription Download ⌵

Subscription Download ✕

Configure subscription download options

Subscription Download ⌵

Select the platforms to download

Windows Linux Mac

RPM dependency

Note: This option is performance intensive.

Resolve all RPM dependencies

Choose Windows your language options

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.

<input checked="" type="checkbox"/> English	<input type="checkbox"/> Portuguese (Brazil)	<input type="checkbox"/> French	<input type="checkbox"/> Italian	<input type="checkbox"/> German
<input type="checkbox"/> Japanese	<input type="checkbox"/> Korean	<input type="checkbox"/> Traditional Chinese	<input type="checkbox"/> Simplified Chinese	<input type="checkbox"/> Hong Kong Chinese
<input type="checkbox"/> Spanish	<input type="checkbox"/> Dutch	<input type="checkbox"/> Swedish	<input type="checkbox"/> Finnish	<input type="checkbox"/> Czech
<input type="checkbox"/> Danish	<input type="checkbox"/> Hungarian	<input type="checkbox"/> Norwegian	<input type="checkbox"/> Russian	<input type="checkbox"/> Polish
<input type="checkbox"/> Portugese (Portugal)				

The Subscription 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
<i>Select the platforms to download</i>	Enables you to select the operating system platform for which you want to download patches. For example, if you select the <i>Windows</i> check box, only Windows patches are downloaded.
<i>Choose Windows your language options</i>	Enables you to select the language of patches you want to download. For example, if you select the <i>French</i> check box, only French language patches are downloaded.
<i>Mix Multiple Languages</i>	Enables you to combine all languages into each Discover Applicable Updates Assignment (not recommended).
<i>SSL</i>	Enables you to turn secured downloading of patch list information on or off. The recommended setting is On.
<i>Cache patch bundles to satellites</i>	Enables you to cache patch bundles to the servers or workstations that are managed by Primary Servers.
<i>Cache patch bundles to primary servers</i>	Enables you to cache patch bundles to Primary Servers only.

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 SP3 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 SP3 content distribution network.

4.6 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 eight links (Subscription Service Information, Schedule Discover Applicable Update Bundles Install, Schedule Discover Applicable Update Bundles Distribution, Configure HTTP Proxy, Subscription Download, Patch Subscription Credentials, Mandatory Baseline Settings, Email Notification, Dashboard and Trending, and Deployment Options):

Configuration	Registration	System Information	Asset Inventory	Asset Management	System Updates	Locations	Subscriptions
Management Zone Settings							
Content							
Device Management							
Discovery and Deployment							
Event and Messaging							
Infrastructure Management							
Inventory							
Reporting Services							
Asset Management							
Endpoint Security Management							
Service Desk Management							
Patch Management							
Category		Description					
Subscription Service Information		View subscription log and update subscription settings					
Schedule Discover Applicable Update Bundles Install		This will allow the DAU Bundle to be configured on when to install fingerprints.					
Schedule Discover Applicable Update Bundles Distribution		This will allow the DAU Bundle to be configured on when to distribute fingerprints.					
Configure Http Proxy		Configure HTTP Proxy for access to the Internet patch subscription					
Subscription Download		Configure subscription download options					
Patch Subscription Credentials		Configure the credentials for each of the Subscription providers					
Mandatory Baseline Settings		Set global values for how mandatory baseline installs will behave.					
Email Notification		Setup email notifications to be delivered when new patches are discovered.					
Dashboard and Trending		Configure Patch Dashboard and Trending behavior					

- 3 Click the *Patch Subscription Credentials* link. The Patch Subscriptions Credentials page appears.

[Configuration](#) > **Patch Subscription Credentials** 🔒 ▼

Patch Subscription Credentials ✕

Configure the credentials for each of the Subscription providers

Patch Subscription Credentials ⤴

RedHat Network Credentials


🔍

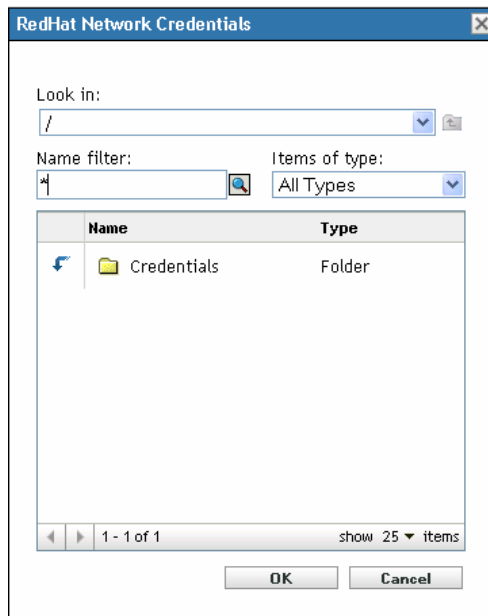
SUSE Network Credentials

🔍

The Patch Subscription Credentials 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.
 - 3 Click the desired credential. Click *OK* to confirm credential selection.
- The window closes and the Patch Subscription Credentials page displays the selection.

The Patch Subscription Credentials page also contains the following buttons:

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

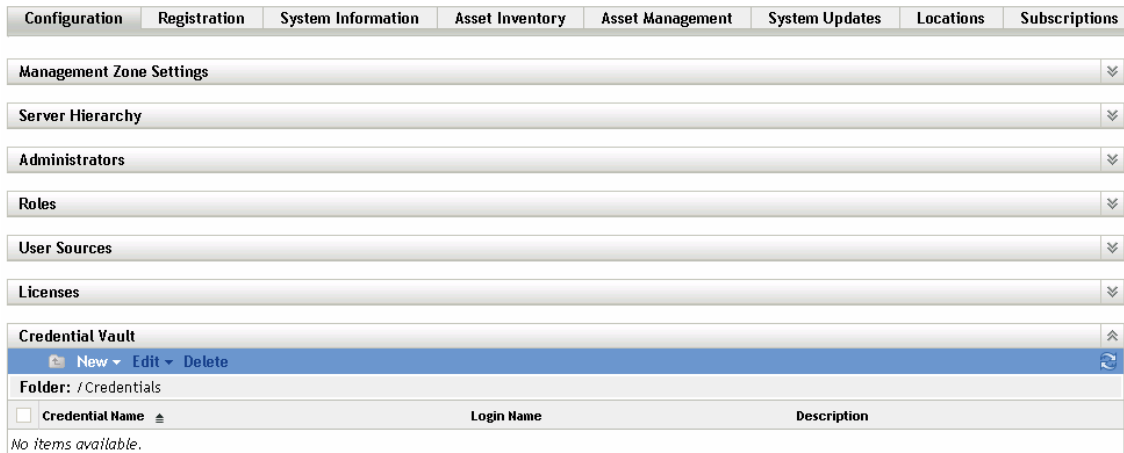
4.6.1 Adding a Credential

The Credential Vault stores the credentials used by Novell ZENworks 11 SP3 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 close button. The dialog contains the following fields: Credential Name (required), Login Name (required), Password, Reenter Password, and Description. A note at the bottom states "Fields marked with an asterisk are required." There are OK and Cancel buttons at the bottom.

- 3 Fill in the fields.
If you need help, click the *Help* button.

4.7 Configuring Mandatory Baseline Settings

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

Configuration	Registration	System Information	Asset Inventory	Asset Management	System Updates	Locations	Subscriptions
Management Zone Settings							
Content							
Device Management							
Discovery and Deployment							
Event and Messaging							
Infrastructure Management							
Inventory							
Reporting Services							
Asset Management							
Endpoint Security Management							
Service Desk Management							
Patch Management							

- 2 Click *Patch Management* to display the eight links (Subscription Service Information, Schedule Discover Applicable Update Bundles Install, Schedule Discover Applicable Update Bundles Distribution, Configure HTTP Proxy, Subscription Download, Patch Subscription Credentials, Mandatory Baseline Settings, Email Notification, Dashboard and Trending, and Deployment Options):

Configuration	Registration	System Information	Asset Inventory	Asset Management	System Updates	Locations	Subscriptions
Management Zone Settings							
Content							
Device Management							
Discovery and Deployment							
Event and Messaging							
Infrastructure Management							
Inventory							
Reporting Services							
Asset Management							
Endpoint Security Management							
Service Desk Management							
Patch Management							
Category	Description						
Subscription Service Information	View subscription log and update subscription settings						
Schedule Discover Applicable Update Bundles Install	This will allow the DAU Bundle to be configured on when to install fingerprints.						
Schedule Discover Applicable Update Bundles Distribution	This will allow the DAU Bundle to be configured on when to distribute fingerprints.						
Configure Http Proxy	Configure HTTP Proxy for access to the Internet patch subscription						
Subscription Download	Configure subscription download options						
Patch Subscription Credentials	Configure the credentials for each of the Subscription providers						
Mandatory Baseline Settings	Set global values for how mandatory baseline installs will behave.						
Email Notification	Setup email notifications to be delivered when new patches are discovered.						
Dashboard and Trending	Configure Patch Dashboard and Trending behavior						

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

[Configuration](#) > Mandatory Baseline Settings 🔍 ▼

Mandatory Baseline Settings ✕

Set global values for how mandatory baseline installs will behave.

Mandatory Baseline Settings ⤴

Modify mandatory baseline reboot and deployment behavior

Popup text

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

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 type="radio"/>	<input checked="" type="radio"/>	
Time to show dialog before reboot	<input type="radio"/>	<input checked="" type="radio"/>	120 <input style="width: 30px; border: 1px solid #ccc;" type="text"/>
Allow User to snooze	<input type="radio"/>	<input checked="" type="radio"/>	<input style="width: 30px; border: 1px solid #ccc;" type="text"/> Days <input style="width: 30px; border: 1px solid #ccc;" type="text"/> Hours <input style="width: 30px; border: 1px solid #ccc;" type="text"/> Minutes

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:

- ◆ **Enable auto reboot of mandatory baseline:** Select this option to enable an automatic reboot of the machine when a mandatory baseline patch is applied.

NOTE: The auto reboot option is not applied to patches that do not require rebooting after installation.

- ◆ **Popup text:** The text of the popup window that appears before patch installation completes and the computer reboots.
- ◆ **Description text:** The text of the notification message.

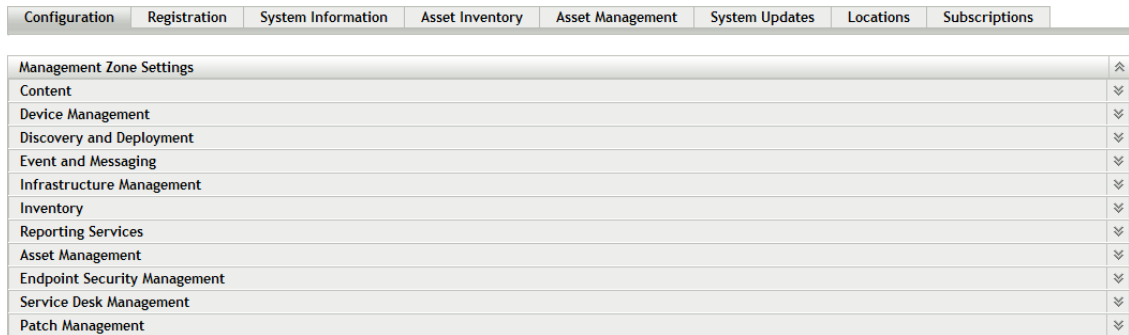
- ◆ **Options:** When you define auto reboot options, you can specify whether to use the values in the default settings or the custom settings. There are four options:
 - ◆ **Suppress Reboot:** Allows the user to prevent rebooting after installation of a patch.
 - ◆ **Allow User to cancel:** Allows the user to cancel the reboot process.
 - ◆ **Time to show dialog before reboot:** The time in seconds for users to choose whether to reboot the machine after installation of a patch.
 - ◆ **Allow User to snooze:** This option allows the user to snooze the reboot.

The page also contains the following buttons:

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

4.8 Configuring Email Notification Details

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



- Click *Patch Management* to display the eight links (Subscription Service Information, Schedule Discover Applicable Update Bundles Install, Schedule Discover Applicable Update Bundles Distribution, Configure HTTP Proxy, Subscription Download, Patch Subscription Credentials, Mandatory Baseline Settings, Email Notification, Dashboard and Trending, and Deployment Options):

Configuration	Registration	System Information	Asset Inventory	Asset Management	System Updates	Locations	Subscriptions
Management Zone Settings							
Content							
Device Management							
Discovery and Deployment							
Event and Messaging							
Infrastructure Management							
Inventory							
Reporting Services							
Asset Management							
Endpoint Security Management							
Service Desk Management							
Patch Management							
Category		Description					
Subscription Service Information		View subscription log and update subscription settings					
Schedule Discover Applicable Update Bundles Install		This will allow the DAU Bundle to be configured on when to install fingerprints.					
Schedule Discover Applicable Update Bundles Distribution		This will allow the DAU Bundle to be configured on when to distribute fingerprints.					
Configure Http Proxy		Configure HTTP Proxy for access to the Internet patch subscription					
Subscription Download		Configure subscription download options					
Patch Subscription Credentials		Configure the credentials for each of the Subscription providers					
Mandatory Baseline Settings		Set global values for how mandatory baseline installs will behave.					
Email Notification		Setup email notifications to be delivered when new patches are discovered.					
Dashboard and Trending		Configure Patch Dashboard and Trending behavior					

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

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

Email Notification [X]

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
<i>From</i>	The email address the notification will be sent from.
<i>To</i>	The email address the notification will be sent to.
<i>Cc</i>	The email address the notification will be carbon-copied to.

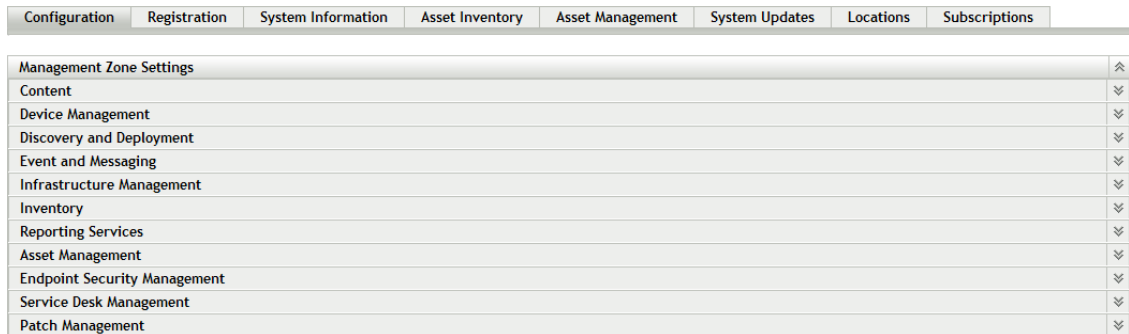
TIP: You can add multiple email addresses in the *To* and *Cc* fields. Separate each address with a comma.

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

Button	Action
<i>OK</i>	Enables you to go back to the Configuration page.
<i>Apply</i>	Enables you to save the changes made to the page.
<i>Reset</i>	Enables you to reset the selected options.
<i>Cancel</i>	Enables you to cancel the last action performed.
Send test email	Enables you to send a test email. For more information, see Section 1.2, "Email Notification," on page 11

4.9 Configuring Patch Dashboard and Trending Behavior

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



- Click *Patch Management* to display the eight links (Subscription Service Information, Schedule Discover Applicable Update Bundles Install, Schedule Discover Applicable Update Bundles Distribution, Configure HTTP Proxy, Subscription Download, Patch Subscription Credentials, Mandatory Baseline Settings, Email Notification, Dashboard and Trending, and Deployment Options):

Configuration	Registration	System Information	Asset Inventory	Asset Management	System Updates	Locations	Subscriptions
Management Zone Settings							
Content							
Device Management							
Discovery and Deployment							
Event and Messaging							
Infrastructure Management							
Inventory							
Reporting Services							
Asset Management							
Endpoint Security Management							
Service Desk Management							
Patch Management							
Category		Description					
Subscription Service Information		View subscription log and update subscription settings					
Schedule Discover Applicable Update Bundles Install		This will allow the DAU Bundle to be configured on when to install fingerprints.					
Schedule Discover Applicable Update Bundles Distribution		This will allow the DAU Bundle to be configured on when to distribute fingerprints.					
Configure Http Proxy		Configure HTTP Proxy for access to the Internet patch subscription					
Subscription Download		Configure subscription download options					
Patch Subscription Credentials		Configure the credentials for each of the Subscription providers					
Mandatory Baseline Settings		Set global values for how mandatory baseline installs will behave.					
Email Notification		Setup email notifications to be delivered when new patches are discovered.					
Dashboard and Trending		Configure Patch Dashboard and Trending behavior					

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

[Configuration](#) > **Dashboard and Trending** 🔍

Dashboard and Trending ✕

Configure Patch Dashboard and Trending behavior

Dashboard and Trending ⤴

Dashboard Update Interval(Every Day at)

Days to store data in database

Criticalities 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 criticality 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
<i>Dashboard Update Interval (Every Day at)</i>	The time at which the patch Dashboard retrieves updates.
<i>Days to store data in database</i>	Enables you to specify for how many days the database stores Dashboard information.
<i>Criticalities to include</i>	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.

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
<i>OK</i>	Enables you to go back to the Configuration page.
<i>Apply</i>	Enables you to save the changes made to the page.
<i>Reset</i>	Enables you to reset the selected options.
<i>Cancel</i>	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:

When a device is refreshed

Delay execution after refresh: Days Hours 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: :

[More Options](#)

Monthly

Day of the month:
 Last day of the month

Start Time: :

[More Options](#)

Fixed Interval

Months Weeks Days Hours Minutes

Start Date: Start Time: :

[More Options](#)

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.

4.10 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 the expanded Licenses section. It contains a table with the following data:

Product/Component Name	License State	Expiration Date
ZENworks 11 Patch Management	Active	
Asset Inventory for Unix/Linux	Evaluation	Thursday, May 13, 2010 10:35:21 PM GMT-07:00
ZENworks 11 Asset Management	Evaluation	Thursday, May 13, 2010 10:35:23 PM GMT-07:00
Asset Inventory for Windows/Mac	Deactivated	
ZENworks Endpoint Security Management	Evaluation	Thursday, May 13, 2010 10:35:23 PM GMT-07:00
ZENworks 11 Configuration Management	Evaluation	Thursday, May 13, 2010 10:35:25 PM GMT-07:00

At the bottom of the table, there is a pagination control showing "1 - 5 of 6" and a "show 5 items" dropdown.

- 3 Click *ZENworks 11 SP3 Patch Management*.

The screenshot shows the Patch Management License dialog box. It has two radio buttons: "Activate product" (selected) and "Deactivate product". Below the "Activate product" radio button, there are three input fields: "Product Subscription Serial Number:", "Company Name", and "Email Address". Below the "Deactivate product" radio button, there is a section for "Account Id" and "Total Non-Expired Licenses". At the bottom, there is a table with the following columns: "Action", "Description", "Status", "Vendor", "Expiration", and "Purchased". The table is currently empty, with the text "No items available." below it. At the very bottom, there are four buttons: "OK", "Apply", "Reset", and "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 functionalities 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 DAU 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.

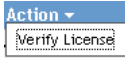
The following table describes each field on the Subscription Serial Number page:

Table 4-2 Patch Management License Items

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

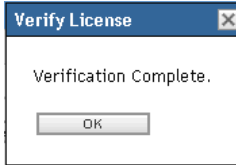
The Patch Management serial number can be entered only once. When you have entered the serial number, you can verify the license by clicking the *Action* drop-down list on the Patch Management License page and selecting *Verify License*. To start the license verification process, click *Apply*. Automatic 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
<i>OK</i>	Enables you to go back to the Configuration page.
<i>Apply</i>	Enables you to start the license verification process.
<i>Reset</i>	Enables you to reset the data entered in the text fields.
<i>Cancel</i>	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 SP3 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:

- ◆ [Section 5.1, “Viewing Patches,” on page 61](#)
- ◆ [Section 5.2, “Dashboard,” on page 62](#)
- ◆ [Section 5.3, “Status,” on page 65](#)
- ◆ [Section 5.4, “Using the Patches Page,” on page 66](#)
- ◆ [Section 5.5, “Patch Management BOE Reports,” on page 81](#)

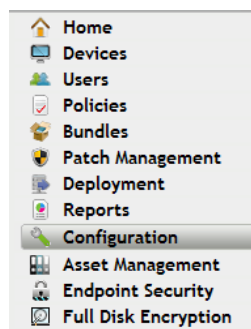
5.1 Viewing Patches

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 Discover Applicable Updates (DAU) 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

Patches					
New Delete Action					
<input type="checkbox"/>	Patch Name	Impact	Patched	Not Patched	Released On
<input type="checkbox"/>	MS11-075 Security Update for Windows XP (KB2564958)	Critical	0	1	Oct-11-2011
<input type="checkbox"/>	MS11-077 Security Update for Windows XP (KB2567053)	Critical	0	1	Oct-11-2011
<input type="checkbox"/>	890830 Windows Malicious Software Removal Tool - October 2011 (KB890830)	Software Installer	0	2	Oct-11-2011
<input type="checkbox"/>	MS11-080 Security Update for Windows Server 2003 (KB2592799)	Critical	0	1	Oct-11-2011
<input type="checkbox"/>	MS11-081 Cumulative Security Update for Internet Explorer 7 for Windows Server 2003 (KB2586448)	Critical	0	1	Oct-11-2011
<input type="checkbox"/>	MS11-075 Security Update for Windows Server 2003 (KB2564958)	Critical	0	1	Oct-11-2011
<input type="checkbox"/>	MS11-078 2604930 2572073 2572075 Security Update for .NET Framework 2.0 SP2 and 3.5 SP1 (All Languages)	Critical	0	2	Oct-11-2011
<input type="checkbox"/>	MS11-077 Security Update for Windows Server 2003 (KB2567053)	Critical	0	1	Oct-11-2011
<input type="checkbox"/>	MS11-081 Cumulative Security Update for Internet Explorer 6 for Windows XP (KB2586448)	Critical	0	1	Oct-11-2011
<input type="checkbox"/>	MS11-080 Security Update for Windows XP (KB2592799)	Critical	0	1	Oct-11-2011
<input type="checkbox"/>	Adobe Flash Player 11.0.1.152 (Other Browsers) for Windows (Full/Upgrade) (All Languages)	Software Installer	0	2	Oct-03-2011
<input type="checkbox"/>	Adobe Flash Player 11.0.1.152 (Internet Explorer) for Windows (Full/Upgrade) (All Languages)	Software Installer	0	2	Oct-03-2011
<input type="checkbox"/>	Adobe AIR 3.0.0.4080 for Windows (Full/Upgrade) (All Languages)	Software Installer	0	2	Oct-03-2011
<input type="checkbox"/>	Mozilla Firefox (English) 3.6.23 for Windows (Full/Upgrade) (See Notes)	Software Installer	0	2	Sep-27-2011
<input type="checkbox"/>	Mozilla Firefox (English) 7.0 for Windows (Full/Upgrade) (See Notes)	Software Installer	0	2	Sep-27-2011
<input type="checkbox"/>	Adobe Flash Player 10.3.183.10 (Internet Explorer) for Windows (Full/Upgrade) (All Languages)	Software Installer	0	2	Sep-21-2011
<input type="checkbox"/>	MS11-071 Security Update for Windows Server 2003 (KB2570947)	Critical	0	1	Sep-13-2011
<input type="checkbox"/>	MS 2616676 Update for Untrusted Certificates for Windows XP and Windows Server 2003 (See Note)	Critical	0	2	Sep-13-2011
<input type="checkbox"/>	MS11-071 Security Update for Windows XP (KB2570947)	Critical	0	1	Sep-13-2011
<input type="checkbox"/>	Mozilla Firefox (English) 6.0.2 for Windows (Full/Upgrade) (See Notes)	Software Installer	0	2	Sep-06-2011
<input type="checkbox"/>	MS 2607712 Update for Untrusted Certificates for Windows XP and Windows Server 2003	Critical	0	2	Sep-06-2011
<input type="checkbox"/>	2570791 Update for Windows Server 2003 (KB2570791)	Recommended	0	1	Aug-23-2011
<input type="checkbox"/>	2570791 Update for Windows XP (KB2570791)	Recommended	0	1	Aug-23-2011
<input type="checkbox"/>	MS11-062 Security Update for Windows XP (KB2566454)	Critical	0	1	Aug-09-2011
<input type="checkbox"/>	Adobe Shockwave Player 11.6.1.629 for Windows (Full/Upgrade) (All Languages)	Software Installer	0	2	Aug-09-2011

1 - 25 of 422
show 25 items

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

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.

5.2 Dashboard

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.

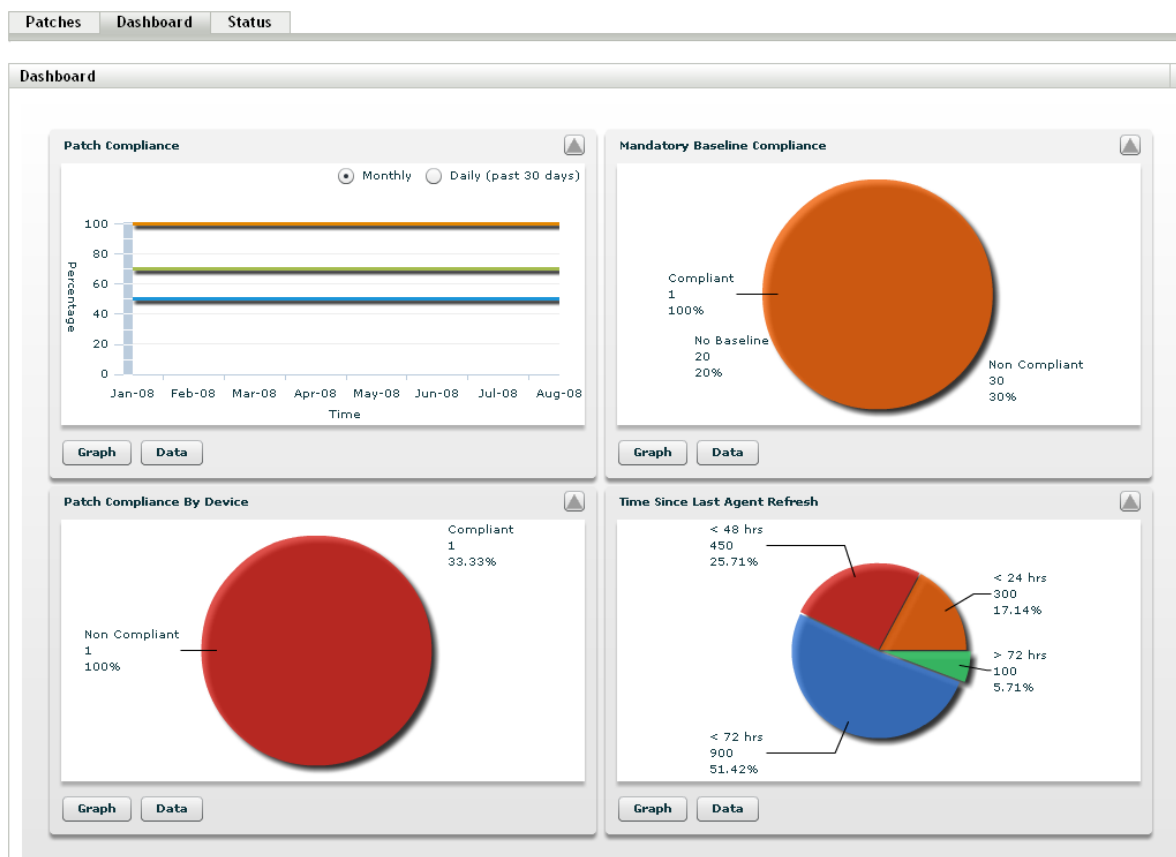
Clicking a dashboard report will display more information about that report in tabular form. You can update the dashboard by clicking the *Update Dashboard Report* button in the *Action* menu of the *Patch Management* tab.

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.

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



- ◆ **Patch Compliance:** Displays the monthly/daily trend of overall compliance for each patch impact category.

Patch Management best practices recommend that an organization should monitor compliance 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 information that shows the individual patched/not patched totals per patch is seen on the *Patches* tab of *Patch Management*.

- ◆ **Monthly/Daily:** Time period for the compliance trend data.

- ◆ **Critical Patched:** Percentage of Critical patches that are applied.
- ◆ **Optional Patched:** Percentage of Recommended and Informational patches that are applied.
- ◆ **Software Patched:** Percentage of Software patches that are applied
- ◆ **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 quickly and easily, and to ensure that known vulnerabilities do not return when a new computer is purchased or re-imaged. Each group is only 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 Patch Management is monitoring.

Each device is evaluated as compliant only if it has a patched status for all of the active patches currently available within Patch Management. Patches that are not applicable should always be disabled within Patch Management so that this metric can be tracked only on 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:** Displays the elapsed time since the last DAU cycle for all managed devices within the network.

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

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

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

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

5.3 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.

- ♦ [Section 5.3.1, “Status,” on page 65](#)
- ♦ [Section 5.3.2, “Cache Status,” on page 65](#)

5.3.1 Status

Table 5-1 Status Table Items

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

5.3.2 Cache Status

Table 5-2 Cache Status Table Column Headings

Item	Definition
<i>Name</i>	The name of a patch.
<i>Status</i>	Whether the patch has been successfully downloaded.
<i>Error Detail (if any)</i>	Details of any error that occurred during the download process.

5.4 Using the Patches Page

The following sections provide more information on the Patches page:

- ◆ [Section 5.4.1, “Patches,” on page 66](#)
- ◆ [Section 5.4.2, “Patch Information,” on page 77](#)
- ◆ [Section 5.4.3, “Searching for a Patch,” on page 78](#)
- ◆ [Section 5.4.4, “Patch Management,” on page 80](#)

5.4.1 Patches

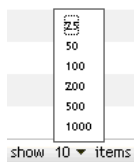
This section of the Patches page provides the following information about patches:

- ◆ 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 76](#).

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 67](#)
- ◆ [“Total Patches Available” on page 67](#)
- ◆ [“Patch Impacts” on page 67](#)
- ◆ [“Patch Statistics” on page 68](#)
- ◆ [“Patch Release Date” on page 72](#)
- ◆ [“Sorting of patches by released date” on page 72](#)
- ◆ [“Patches released within the last 30 days are displayed in bold font” on page 72](#)
- ◆ [“Patch Creation” on page 72](#)
- ◆ [“Patch Deletion” on page 75](#)
- ◆ [“Action Menu Items” on page 76](#)

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/>), 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/>), 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 - 10 of 979

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	
Software Installers	Software Distribution	Adobe 8.1 software installer
	Example: Microsoft Windows Malicious Software Removal Tool (Virus Removal)	
Informational	NA	NA

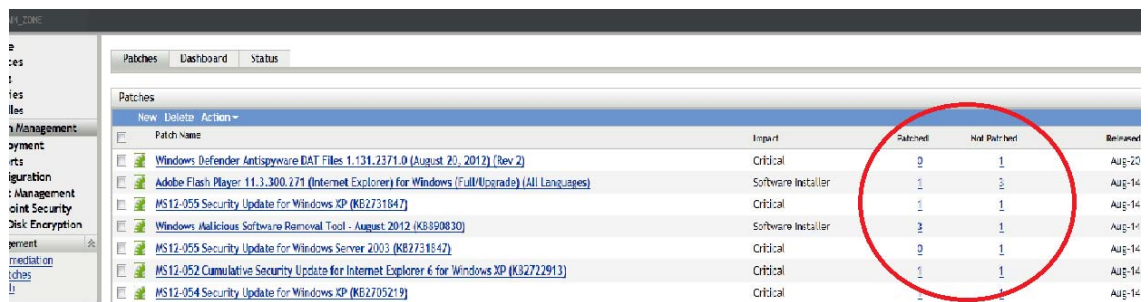
Source: Lumension Security

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.



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

Patched	Not Patched	Information												
<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #4f81bd; color: white; padding: 2px;">Action ▾</div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;"><input type="checkbox"/></th> <th style="width: 40%;">Device Name</th> <th style="width: 15%;">Last Contact</th> <th style="width: 15%;">Platform</th> <th style="width: 15%;">DNS</th> <th style="width: 15%;">IP Address</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>xp-professional-agent</td> <td>May-27-2010</td> <td>Windows</td> <td>XP-Professional-Agent</td> <td>192.168.1.147</td> </tr> </tbody> </table> </div>			<input type="checkbox"/>	Device Name	Last Contact	Platform	DNS	IP Address	<input checked="" type="checkbox"/>	xp-professional-agent	May-27-2010	Windows	XP-Professional-Agent	192.168.1.147
<input type="checkbox"/>	Device Name	Last Contact	Platform	DNS	IP Address									
<input checked="" type="checkbox"/>	xp-professional-agent	May-27-2010	Windows	XP-Professional-Agent	192.168.1.147									

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

Item	Definition
<i>Device Name</i>	The name of the device registered with Novell ZENworks 11 SP3 Patch Management to which the patch is to be deployed.
<i>Last Contact</i>	The last time the device contacted the Patch Management Server.
<i>Platform</i>	The operating system of the device.
<i>DNS</i>	The name of the DNS server.
<i>IP Address</i>	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.

Patched	Not Patched	Information												
<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #4f81bd; color: white; padding: 2px;">Action ▾</div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;"><input type="checkbox"/></th> <th style="width: 40%;">Device Name</th> <th style="width: 15%;">Last Contact</th> <th style="width: 15%;">Platform</th> <th style="width: 15%;">DNS</th> <th style="width: 15%;">IP Address</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>new-zcm-server</td> <td>May-27-2010</td> <td>Windows</td> <td>NEW-ZCM-SERVER</td> <td>192.168.1.150</td> </tr> </tbody> </table> </div>			<input type="checkbox"/>	Device Name	Last Contact	Platform	DNS	IP Address	<input checked="" type="checkbox"/>	new-zcm-server	May-27-2010	Windows	NEW-ZCM-SERVER	192.168.1.150
<input type="checkbox"/>	Device Name	Last Contact	Platform	DNS	IP Address									
<input checked="" type="checkbox"/>	new-zcm-server	May-27-2010	Windows	NEW-ZCM-SERVER	192.168.1.150									

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

Item	Definition
<i>Device Name</i>	The name of the device registered with Novell ZENworks 11 SP3 Patch Management to which the patch is to be deployed.
<i>Last Contact</i>	The last time the device contacted the Patch Management Server.
<i>Platform</i>	The operating system of the device.
<i>DNS</i>	The name of the DNS server.
<i>IP Address</i>	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
⌵		
Property Name	Details	
Name	890830 Windows Malicious Software Removal Tool - November 2009 (KB890830)	
Impact	Software Installer	
Status	Enabled	
Vendor	Microsoft Corp.	
Released On	2009-11-10 00:00:00.0	
Vendor Product ID	Windows Vista, Windows 2000, Windows XP, Windows Server 2003, Datacenter Edition, Windows Server 2008, Windows 7	
Description	LSAC(v2) 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.	
Number of Devices Patched	0	
Number of Devices Not Patched	2	
Number of Devices Not Applicable	0	

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 <i>Enabled</i> , <i>Disabled</i> (<i>Superseded</i>) or <i>Disabled (By User)</i> .
Vendor	The name of the vendor.
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; 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.

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 <i>Include Disabled</i> filter in the <i>Search</i> 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

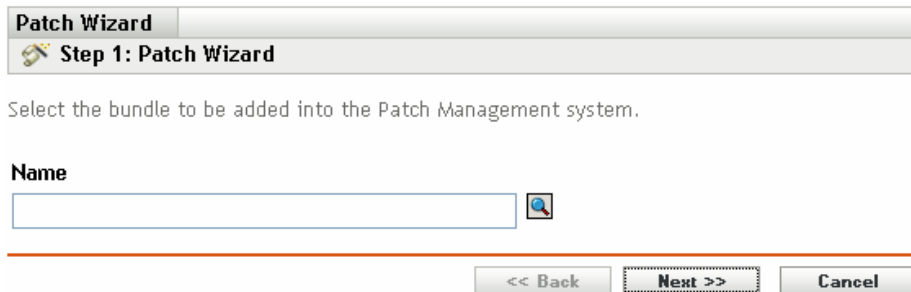
All the patches released in last 30 days are displayed in bold font.

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 sub-header "Step 1: Patch Wizard". Below the header, there is a text prompt: "Select the bundle to be added into the Patch Management system." Underneath, 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:

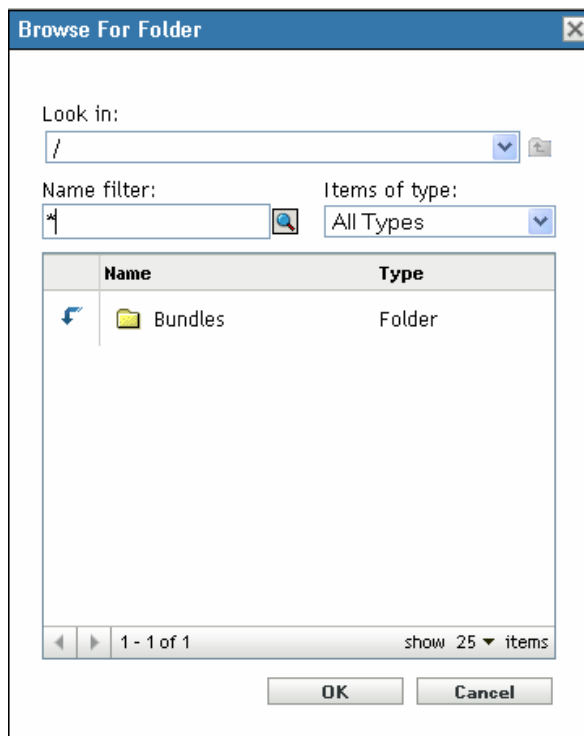
- ◆ [“Add Patch Bundle” on page 72](#)
- ◆ [“Modify Patch Details” on page 74](#)
- ◆ [“Export Patches Summary” on page 75](#)

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.
- 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 a web-based form titled "Patch Wizard" with a sub-header "Step 2: Patch Wizard". Below the header is the instruction "Modify the details of the patch." The form contains several fields: "Name" with the value "Novell Linux 2008-11-22 SLE 10 x86 Security update"; "Impact" with a dropdown menu set to "Recommended"; "Vendor" with the value "Custom"; "Vendor Product ID" which is empty; "Requires Reboot" with an unchecked checkbox; and "Description" with the text "Patch data do not remove: Patch Remediation Bundle". At the bottom of the form are three buttons: "<< Back", "Next >>" (which is highlighted with a dashed border), and "Cancel".

You can modify the following information for a patch:

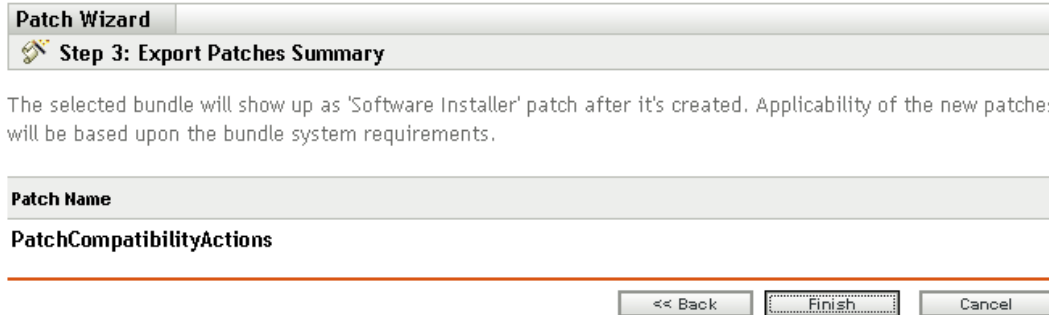
Property Name	Definition
<i>Name</i>	The name of the patch.
<i>Impact</i>	The impact of the patch as determined by Novell. See Patch Impacts .
<i>Vendor</i>	The name of the vendor.
<i>Vendor Product ID</i>	The ID number given to the product by the vendor.
<i>Requires Reboot</i>	Whether a reboot is required after patch deployment
<i>Description</i>	The description of the patch; includes detailed information concerning the defect or issue resolved by this patch, deployment notes, and the prerequisites for deployment.

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



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.

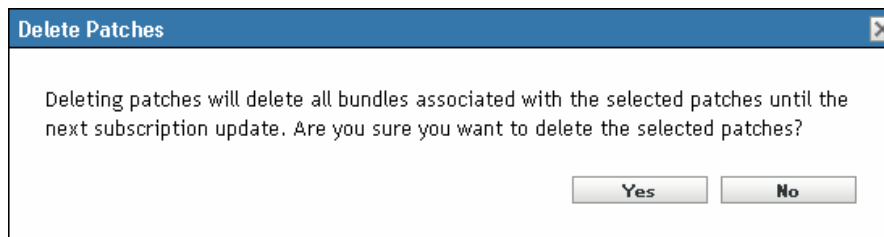
NOTE: After creating a new patch, you cannot immediately deploy it to any devices. This is because the Patch Management Server does not recognize the patch yet. To enable deployment, perform a subscription update after the new patch is created.

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.

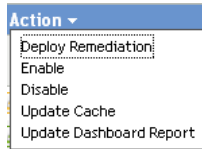


- 2 Click Yes to confirm the deletion. Click No to return to the Patches page.

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 83](#).
- ◆ **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.
Disabling a patch also disables all the bundles associated with it.
- ◆ **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



- ◆ **Update Dashboard Report:** Enables you to update the dashboard report with the latest statistics.

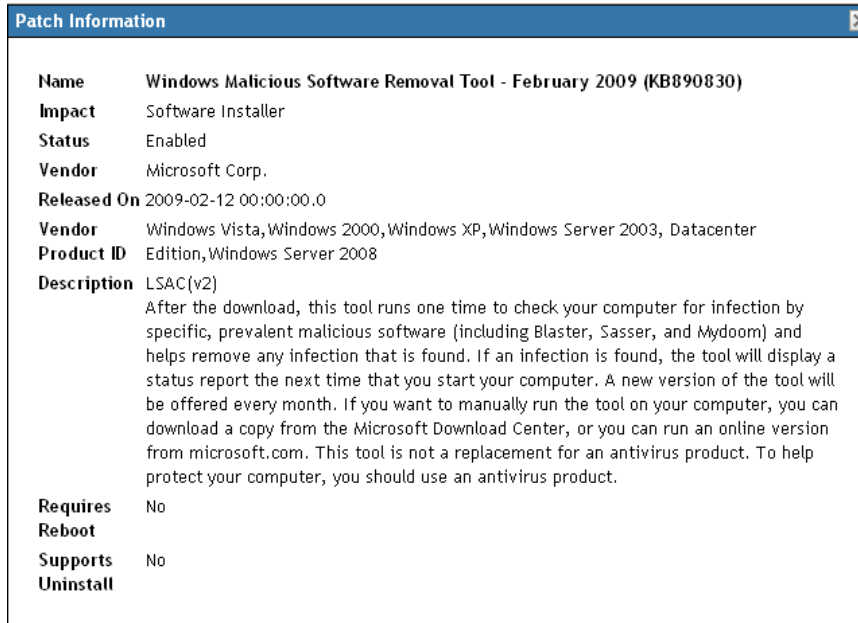
NOTE: To know when a patch was downloaded, view the *Message Log* panel for that patch in the *Bundles* section.

5.4.2 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



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

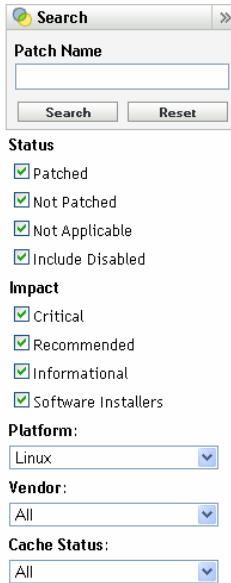
Table 5-5 Property Names in the Patch Information Section

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 <i>Enabled</i> , <i>Disabled (Superseded)</i> , or <i>Disabled (By User)</i> .
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

5.4.3 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 interface with the following elements:

- Search** (title)
- Patch Name**: A text input field.
- Search** and **Reset** buttons.
- Status** section with four checked checkboxes:
 - Patched
 - Not Patched
 - Not Applicable
 - Include Disabled
- Impact** section with four checked checkboxes:
 - Critical
 - Recommended
 - Informational
 - Software Installers
- Platform:** A drop-down menu with "Linux" selected.
- Vendor:** A drop-down menu with "All" selected.
- Cache Status:** A drop-down menu with "All" selected.

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 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
<i>Patched</i>	Search results include all the patches in the patch list that have been applied to one or more devices.
<i>Not Patched</i>	Search results include all the patches in the patch list that have not been applied to any device.
<i>Not Applicable</i>	Search results include all the patches in the patch list that do not apply to the device.
<i>Include Disabled</i>	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
<i>Critical</i>	Search results include all the patches in the patch list that are classified as Critical by Novell.
<i>Recommended</i>	Search results include all the patches in the patch list that are classified as Recommended by Novell.
<i>Informational</i>	Search results include all the patches in the patch list that are classified as Informational by Novell.
<i>Software Installers</i>	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
<i>Vendor</i>	Search results include all the patches relevant to the vendor in the patch list.
<i>Cache Status</i>	Search results include all the patches relevant to their cache status on the local server.
<i>Platform</i>	Search results include all the patches relevant to the operating system in the patch list.

5.4.4 Patch Management

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

- ◆ “Deploy Remediation” on page 80
- ◆ “Export Patches” on page 80
- ◆ “View Patch” on page 81

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 83](#).

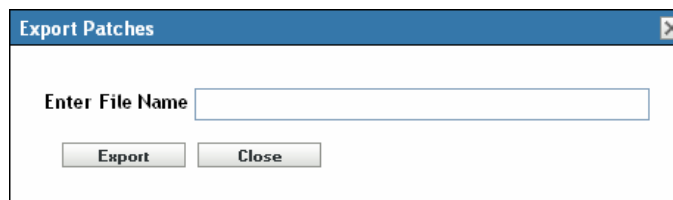
Export Patches

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	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 APSS06-07 Dreamweaver Server Behavior SQL Injection vulnerability	Critical	0	0
13	Active	Adobe APSS07-12 Flash Player 9.0.r47 for FireFox (Upgrade) (All Languages)	Critical	0	0
14	Active	Adobe APSS07-12 Flash Player 9.0.r47 for IE (Upgrade) (All Languages) (Rev 3)	Critical	0	2
15	Active	Adobe APSS07-12 Flash Player 9.0.r47 for IE (Upgrade) (All Languages) (Rev 3)	Critical	0	0
16	Active	Adobe APSS07-12 Flash Player 9.0.r47 for Netscape (Upgrade) (All Languages) (Rev 2)	Critical	0	0
17	Active	Adobe APSS07-12 Flash Player 9.0.r47 for Netscape (Upgrade) (All Languages) (Rev 2)	Critical	0	0
18	Active	Adobe APSS07-13 Photoshop CS3 Update for Windows	Critical	0	0
19	Active	Adobe APSS07-20 Flash Player 9.0.r115 for IE (Upgrade) (All Languages)	Critical	0	0
20	Active	Adobe APSS07-20 Flash Player 9.0.r115 for IE (Upgrade) (All Languages)	Critical	0	2
21	Active	Adobe APSS08-01 Contribute CS3 update FLYPlayer_Progressive.swf file for Windows	Critical	0	0
22	Active	Adobe APSS08-01 Dreamweaver CS3 update FLYPlayer_Progressive.swf file for Windows	Critical	0	0

View 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.

5.5 Patch Management BOE Reports

Business Objects Enterprise (BOE) reports are available to customers who install ZENworks Reporting Services (ZRS) inside ZENworks 11 SP3. The following predefined reports are included for Patch Management:

- ◆ **Mandatory Baseline Details:** Displays the applicable device names and patch statuses for the patches within the selected mandatory baseline. This report also helps you to monitor and communicate the compliance level for mandatory patches in the environment.
- ◆ **Mandatory Baseline Summary:** Displays the applicable device names and patch statuses for the patches. It also displays the criticality and the percentage of patched and not patched devices.
- ◆ **Vulnerability Analysis:** Displays the criticality level for patches that are applicable in an enterprise. It also displays the number of devices applicable to the patch, and the percentage of patched devices. This report is designed to assist in showing adherence to various compliances that require a level of patching efforts.

NOTE: On a Linux server, the Vulnerability Analysis and the Mandatory Baseline Summary reports display blank columns even though the reports have data. To view the data, modify the reports and set the text color to black in the Formatting toolbar, then save the reports. You need to do this only once.

- ◆ **Patch Assessment Report:** Displays the patches released by vendors, and the number of patched, not patched, and not applicable devices.
- ◆ **Patch Release Report:** Displays the number of patches released by vendors. The details section displays the patch name and percentage patched by impact and vendor.

- ◆ **Top 10 Not Patched Critical Patches:** Displays the 10 most critical patches that have not been applied to any device.
- ◆ **Patch Bundle Assignment Summary**
 - ◆ **Summary Report:** Displays the patched, not patched, not applicable, and patch percentage statuses by bundle name and patch name.
 - ◆ **Detail Report:** Displays the devices, device patch status, and deployment state by Bundle and Patch.
- ◆ **Patch Analysis**
 - ◆ **Dashboard:** Displays the patch status by vendor for the selected deployment status and impact.
 - ◆ **Detail Page:** Displays the patch name, release date, impact, deployment state, and patch status.
- ◆ **Patch Detail Report:** Displays the devices and patch status for the selected vendors, patches, impact, and patch status.

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.

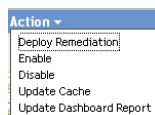
The following sections provide more information on each step of the wizard:

- ◆ [Section 6.1, “Creating a Deployment Schedule,” on page 83](#)
- ◆ [Section 6.2, “Confirm Devices,” on page 84](#)
- ◆ [Section 6.3, “License Agreement,” on page 87](#)
- ◆ [Section 6.4, “Remediation Schedule,” on page 87](#)
- ◆ [Section 6.5, “Deployment Order and Behavior,” on page 96](#)
- ◆ [Section 6.6, “Remediation Options,” on page 97](#)
- ◆ [Section 6.7, “Advanced Remediation Options,” on page 98](#)
- ◆ [Section 6.8, “Pre Install Notification Options,” on page 100](#)
- ◆ [Section 6.9, “Distribution Schedule,” on page 103](#)
- ◆ [Section 6.10, “Notification and Reboot Options,” on page 110](#)
- ◆ [Section 6.11, “Choose Deployment Name,” on page 114](#)
- ◆ [Section 6.12, “Deployment Summary,” on page 115](#)

6.1 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:



6.2 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 screenshot shows the 'Confirm Devices' page. At the top, there is a 'Patches' tab and a sub-header 'Step 1: Confirm Devices'. Below this, a message states: 'Remedies will be deployed to the following devices. Please deselect any devices that should not be patched.' There are three radio button options: 'All non-patched devices' (which is selected), 'Select applicable devices', and 'Select devices, folders and groups'. A red horizontal line separates the options from the deployment target text: 'Deploy to all devices that are not patched'. At the bottom, there are three buttons: '<< Back', 'Next >>', and 'Cancel'.

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

1 - 2 of 2

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

The screenshot shows a dropdown menu for 'show items'. The current selection is '10'. The menu is open, showing the following options: 25, 50, 100, 200, 500, and 1000.

- 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 [Section 6.2.1, “Confirm Devices: All Non-patched Devices,”](#) on page 85.
 - ♦ Choose *Select applicable devices* to deploy the patch to specific devices, then continue with [Section 6.2.2, “Confirm Devices: Select Applicable Devices,”](#) on page 85.
 - ♦ 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 [Section 6.2.3, “Confirm Devices: Select Devices, Folders, and Groups,”](#) on page 86.

6.2.1 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.

6.2.2 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

<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

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
<i>Device Name</i>	The name of the device. The name of the device registered with Novell ZENworks 11 SP3 Patch Management to which the patch is to be deployed.
<i>Last Contact</i>	The status of the device when they were last contacted.
<i>Platform</i>	The operating system of the device.
<i>DNS</i>	The name of the DNS server.
<i>IP Address</i>	The IP address of the device.

6.2.3 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

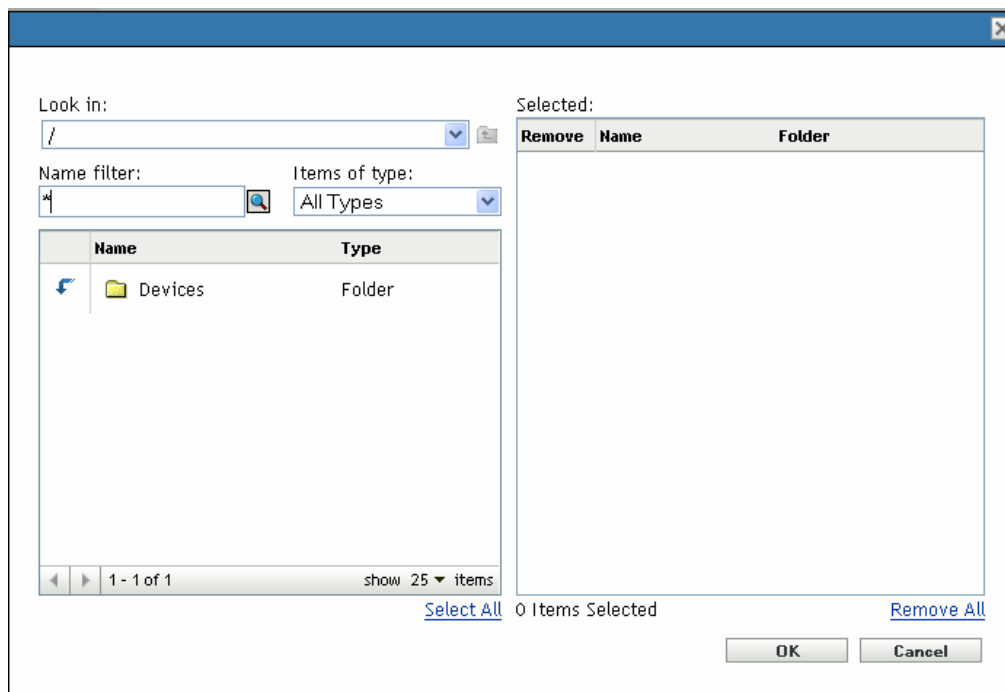
Add	Remove
<input type="checkbox"/>	
Name	In Folder

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:



- 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.

6.3 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 'Step 2: License Agreement' page. At the top, there is a breadcrumb 'Patches' and a title bar 'Step 2: License Agreement'. Below the title bar, a message reads: '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 the following structure:

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

Below the table, the text 'License Agreement' is displayed. At the bottom of the page, there are three buttons: '<< Back', 'Next >>', and 'Cancel'.

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.

6.4 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 'Step 3: Remediation Schedule' page. At the top, there is a breadcrumb 'Patches' and a title bar 'Step 3: Remediation Schedule'. Below the title bar, a message reads: 'Please select the schedule for deployment of remediation to your selected devices'. A 'Schedule Type:' label is followed by a dropdown menu with the following options:

- Now
- Now
- Date Specific
- Recurring

At the bottom of the page, 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.

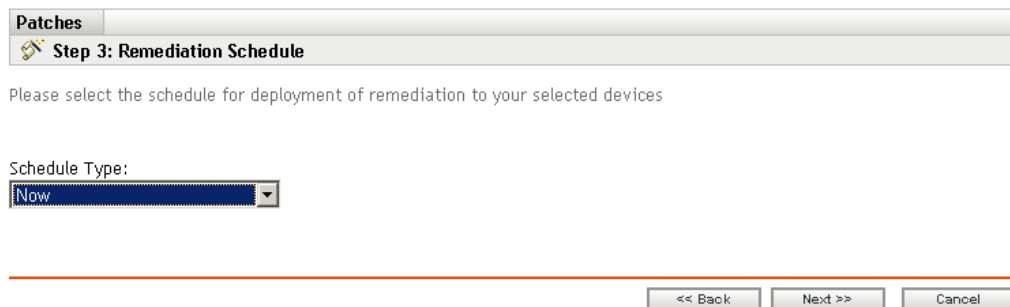
The following sections provide more information on schedule types:

- ♦ [Section 6.4.1, “Remediation Schedule: Now,” on page 88](#)
- ♦ [Section 6.4.2, “Remediation Schedule: Date Specific,” on page 89](#)
- ♦ [Section 6.4.3, “Remediation Schedule: Recurring,” on page 90](#)
- ♦ [Section 6.4.4, “Remediation Schedule: Wake On LAN,” on page 95](#)

6.4.1 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 wizard window titled "Patches" with a sub-header "Step 3: Remediation Schedule". Below the header, there is a prompt: "Please select the schedule for deployment of remediation to your selected devices". Underneath, there is a "Schedule Type:" label followed by a dropdown menu where "Now" is selected. 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.



6.4.2 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 is a breadcrumb trail: "Patches" > "Step 3: Remediation Schedule". Below this, a message reads: "Please select the schedule for deployment of remediation to your selected devices". The "Schedule Type:" dropdown menu is set to "Date Specific". The main configuration area includes a "Start Date(s):" field with a calendar icon, two checkboxes: "Run event every year" and "Process immediately if device unable to execute on schedule", and a section titled "Select when schedule execution should start:" with two radio buttons: "Start immediately at Start Time" (selected) and "Start at a random time between Start and End Times". Below the radio buttons are "Start Time:" and "End Time:" fields, each with hour and minute dropdown menus. A checkbox "Use Coordinated Universal Time (Current UTC 8:08 AM)" is also present. 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.

6.4.3 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

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
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: 10/25/2011 Start Time: 1 :00
[More Options](#)

<< Back Next >> Cancel

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 the *Actions* tab for the particular patch bundle assignment.
- 2 Click *Options*. This opens the Install Options window.
- 3 Select *Install always* and click *OK*.
- 4 Click *Apply*.

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

- ♦ “When a Device Is Refreshed” on page 91
- ♦ “Days of the Week” on page 92

- ♦ “Monthly” on page 93
- ♦ “Fixed Interval” on page 94

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 6-11 *Delay Execution After Refresh Check Box*



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 6-12 Weekly Deployment 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 6-13 Monthly Deployment 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 6-14 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 6-15 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)

6.4.4 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 6-16 Remediation Schedule Page with Wake On LAN option

Schedule Type:

When a device is refreshed

Delay execution after refresh: Days Hours 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: :

[More Options](#)

Monthly

Day of the month:
 Last day of the month
 First

Start Time: :

[More Options](#)

Fixed Interval

Months Weeks Days Hours Minutes
 Start Date: Start Time: :

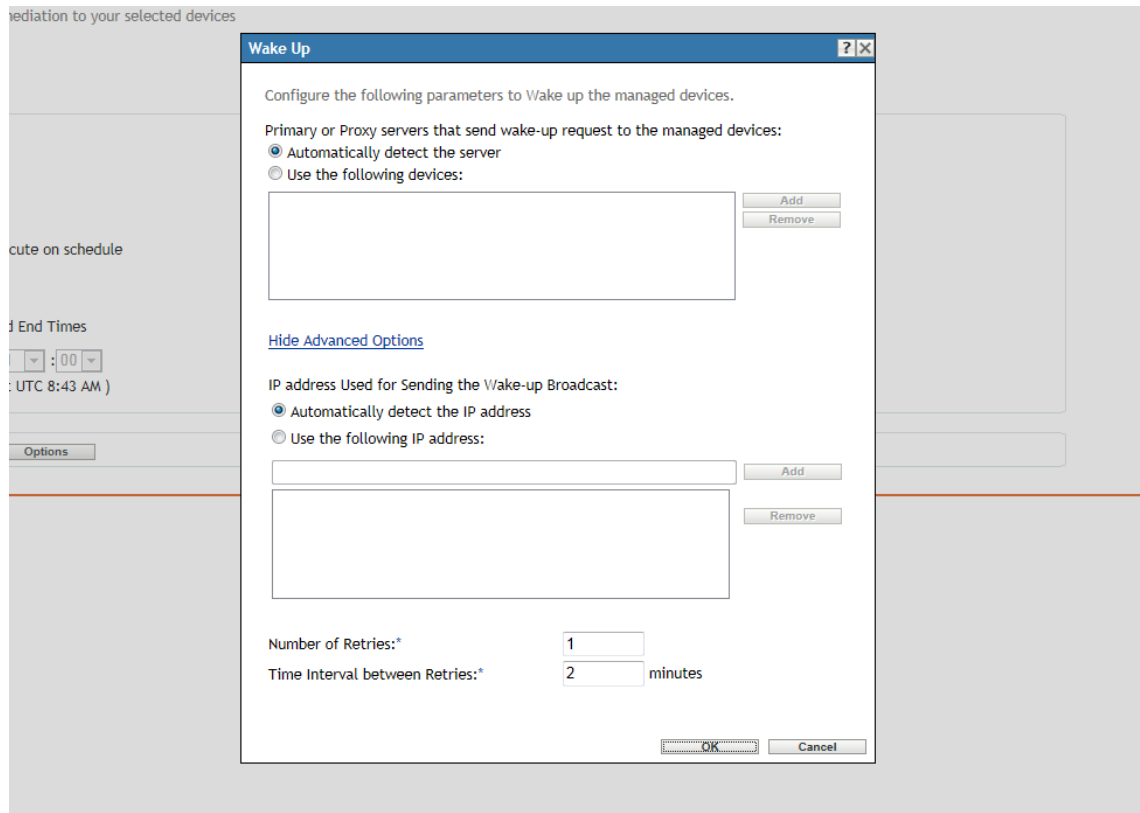
[More Options](#)

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

To change the parameters:

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

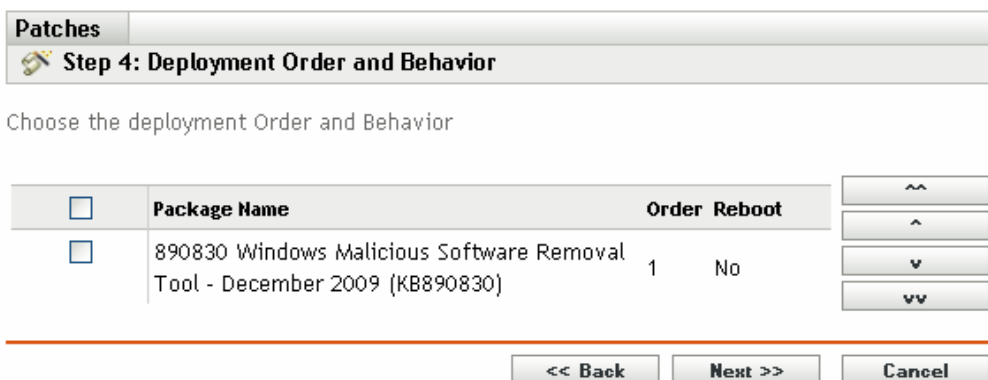
When you select Wake On LAN options, the Advanced settings page appears as shown in the following figure:



6.5 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 6-17 Deployment Order and Behavior Page







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.

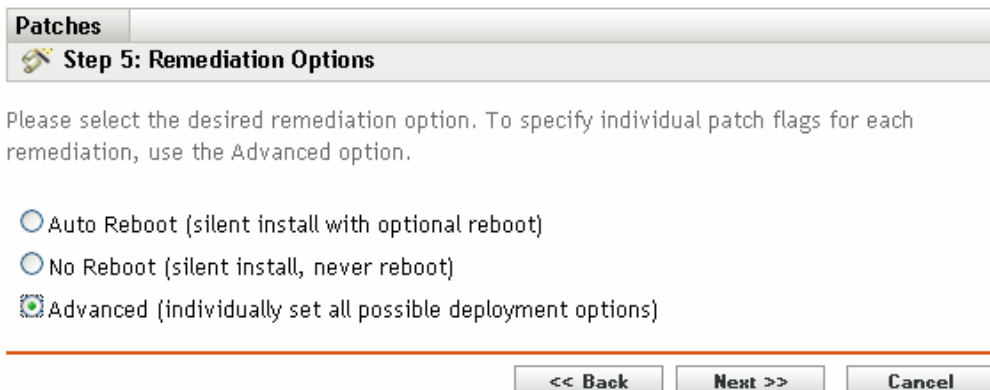
Click the *Next* button to open the Remediation Options page. Click the *Back* button to return to the previous page. Click *Cancel* to exit the wizard.

6.6 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 6-18 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)

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

Table 6-3 *The Remediation Options*

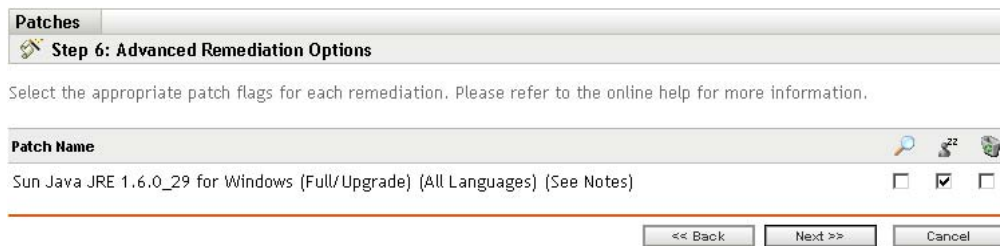
Remediation Option	Functionality
Auto Reboot (silent install with optional reboot)	Automatically sets all possible patches to deploy with QChain enabled. Allows the administrator to set the patch deployment flags as desired, using the default QChain (http://articles.techrepublic.com.com/5100-10878_11-1048774.html) 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.

6.7 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 6-19 *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
	<i>Uninstall</i>	Uninstalls the packages.
	<i>Force Shutdown</i>	Forces all applications to close if the package causes a reboot.
	<i>Do Not Back Up</i>	Does not back up files for uninstalling.
	<i>Suppress Reboot</i>	Prevents the computer from rebooting after installation of the package.

Icon	Name	Functionality
	<i>Quiet Mode</i>	Sets the installer to function in quiet mode. Quiet mode suppresses any user interfaces (if a user is logged in) during the remediation.
	<i>Unattended Setup</i>	Installs the packages in the Unattended Setup mode.
	<i>List Hot Fixes</i>	Returns a list of the hot fixes installed on the target computers.
	<i>Force Reboot</i>	Forces the computer to reboot regardless of package requirements.
	<i>Reboot is Required</i>	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.
	<i>Chain Packages</i>	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.
	<i>Suppress Chained Reboot</i>	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.
	<i>Repair File Permissions</i>	Repairs file permissions after package installation.
	<i>Download Only</i>	Distributes the package without running the package installation script.
	<i>Suppress Notification</i>	Suppresses any user notifications during installations.
	<i>Debug Mode</i>	Runs the package installation in debug mode.
	<i>Do Not Repair Permissions</i>	Suppresses the repair of filename permissions after the reboot.
	<i>May Reboot</i>	Allows the package to force a reboot if required.
	<i>Multi-User Mode</i>	Performs the installation in Multi-User mode.
	<i>Single-User Mode</i>	Performs the installation in Single-User mode.
	<i>Restart Service</i>	Restarts the service following the deployment.
	<i>Do Not Restart Service</i>	Does not restart the service following the deployment.
	<i>Reconfigure</i>	Performs the system reconfigure task following the deployment.
	<i>Do Not Reconfigure</i>	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 98](#) 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.

6.8 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.

Figure 6-20 Pre Install Notification Options Page

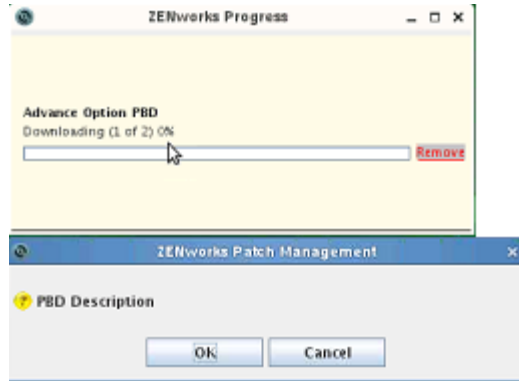
The screenshot shows the 'Step 7: Pre Install Notification Options' page. At the top, there is a breadcrumb trail: 'Patches > Step 7: Pre Install Notification Options'. Below this, the instruction 'Select Pre Install Notification Options' is displayed. The main section is titled 'Define Pre Install Options' and contains two radio button options: 'Use values assigned to system variables or defaults' (which is selected) and 'Override Settings'. Underneath, there is a checked checkbox for 'Notify Users of Patch Install', with two sub-options: 'Prompt before download' and 'Prompt before install' (which is selected). Below these are two text areas: 'Popup text' containing the message 'There are important patches that need to be applied to your device. Click here to install patches now.' and 'Description text' containing the message 'The download and installation of patches is ready to begin. If you require any additional information, please contact your Novell ZENworks Patch Management administrator.' At the bottom, there are three sections: 'Options' with radio buttons for 'Allow User to cancel' (selected), 'Time to show dialog before install' (set to 120 seconds), and 'Allow User to snooze' (set to 0 days, 2 hours, 0 minutes). At the very bottom, there are three buttons: '<< Back', 'Next >>', and '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:

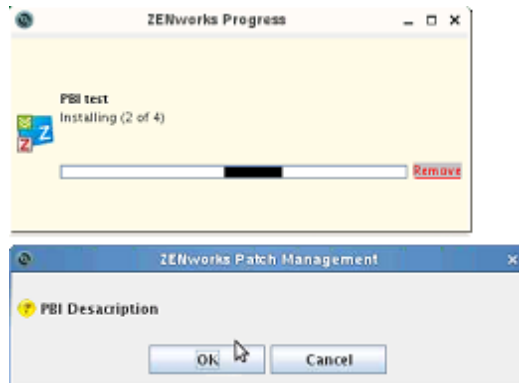
- ◆ **Prompt before download:** Select this option to notify the user when the patch download process begins.

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.



- ◆ **Popup Text:** The text of the popup window that appears before patch installation or patch download begins.
- ◆ **Description Text:** The text of the notification message.
- ◆ **Use values assigned to system variables or defaults:** Select this option to use the default settings for each agent. This option disables all other installation and notification options.

TIP: System variables or defaults are defined to configure the agent settings at the system level in the properties file, such as pre-install notification options. If the *Use values assigned to system variables or defaults* option is selected, the settings for the current agent are taken directly from system variables or defaults; otherwise, the settings customized by the user take effect only for the current agent.

The following table describes system variables or defaults for pre-install notification options:

System Variable	Variable Value
Notify Users of Patch Install	Not selected
Prompt before download	Not selected
Prompt before install	Selected
Popup text	There are important patches that need to be applied to your device. Click here to install patches now.
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.
Allow User to cancel	No
Time to show dialog before install	No 120 seconds
Allow User to snooze	Yes 0 Days 2 Hours 0 Minutes

- ◆ **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 defining 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 installation.
 - ◆ **Time to show dialog before install:** The time in seconds for users to choose whether to download and install patch.
 - ◆ **Allow User to snooze:** This option allows the user to snooze the installation.

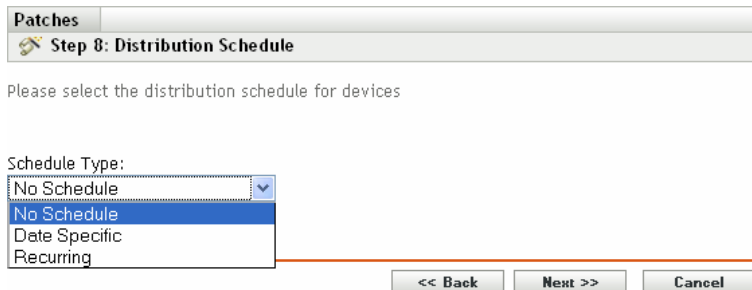
NOTE: Even if you choose to snooze the installation, the pop-up window continues to appear every few seconds until you proceed with or cancel the installation.

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.

6.9 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 6-21 Distribution Schedule Page



The screenshot shows the 'Patches' window with 'Step 8: Distribution Schedule' selected. Below the window title bar, it says 'Please select the distribution schedule for devices'. The 'Schedule Type:' dropdown menu is open, showing three options: 'No Schedule' (selected), 'Date Specific', and 'Recurring'. At the bottom of the window are three buttons: '<< Back', 'Next >>', and '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.

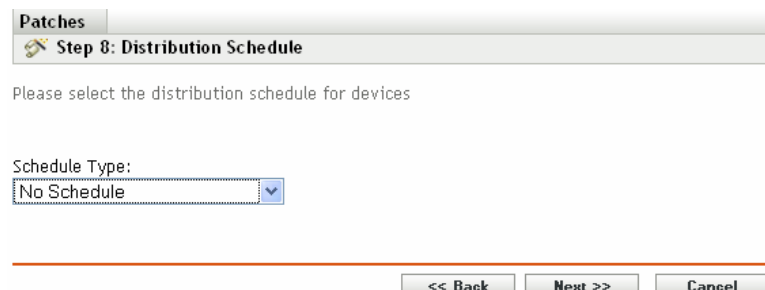
The following sections provide more information on schedule types:

- ◆ [Section 6.9.1, “Distribution Schedule: No Schedule,” on page 103](#)
- ◆ [Section 6.9.2, “Distribution Schedule: Date Specific,” on page 104](#)
- ◆ [Section 6.9.3, “Distribution Schedule: Recurring,” on page 105](#)

6.9.1 Distribution Schedule: No Schedule

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

Figure 6-22 Distribution Schedule Page for the No Schedule Type



The screenshot shows the 'Patches' window with 'Step 8: Distribution Schedule' selected. Below the window title bar, it says 'Please select the distribution schedule for devices'. The 'Schedule Type:' dropdown menu is set to 'No Schedule'. At the bottom of the window 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.



6.9.2 Distribution Schedule: Date Specific

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

Figure 6-23 Distribution Schedule Page for the Date Specific Schedule Type

The screenshot shows the 'Step 8: Distribution Schedule' page. At the top, there is a breadcrumb 'Patches' and a title bar 'Step 8: Distribution Schedule'. Below the title bar, the instruction reads: 'Please select the distribution schedule for devices'. The 'Schedule Type:' dropdown menu is set to 'Date Specific'. The main configuration area contains a 'Start Date(s):' field with a calendar icon and a clear icon. Below this are two checkboxes: 'Run event every year' and 'Process immediately if device unable to execute on schedule'. The 'Select when schedule execution should start:' section has two radio buttons: 'Start immediately at Start Time' (selected) and 'Start at a random time between Start and End Times'. The 'Start Time:' is set to '1:00' and the 'End Time:' is set to '1:00'. There is also a checkbox for 'Use Coordinated Universal Time (Current UTC 10:19 AM)'. At the bottom of the page, 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.

6.9.3 Distribution Schedule: Recurring

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

Figure 6-24 Distribution Schedule Page for the Recurring Schedule Type

Schedule Type:

When a device is refreshed

Delay execution after refresh: Days Hours 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: :

[More Options](#)

Monthly

Day of the month:

Last day of the month

First

Start Time: :

[More Options](#)

Fixed Interval

Months Weeks Days Hours Minutes

Start Date: Start Time: :

[More Options](#)

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

- ◆ [“When a Device Is Refreshed” on page 106](#)
- ◆ [“Days of the Week” on page 107](#)
- ◆ [“Monthly” on page 108](#)
- ◆ [“Fixed Interval” on page 109](#)

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 6-25 *Delay Execution After Refresh Check Box*



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 6-26 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 6-27 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 6-28 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 6-29 Fixed Interval Distribution 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)

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.

6.10 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 6-30 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

Popup text

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

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 type="radio"/>
Allow User to cancel	<input type="radio"/>	<input type="radio"/>
Time to show dialog before reboot	<input type="radio"/>	<input type="radio"/> <input type="text" value="120"/> Seconds
Allow User to snooze	<input type="radio"/>	<input type="radio"/> <input type="text" value="0"/> Days <input type="text" value="2"/> Hours <input type="text" value="0"/> Minutes

The page provides the following options:

- ◆ **Notify Users:** Select this option to notify the user when patch installation completes.

- ◆ **Popup Text:** The text of the popup window that appears before patch installation completes and the computer reboots.
- ◆ **Description text:** The text of the notification message.
- ◆ **Use values assigned to system variables or defaults:** Select this option to use the default settings for each agent. This option disables all other reboot notification options.

The following table describes system variables or defaults for notification and reboot options:

System Variable	Variable Value
Notify Users	Selected
Popup text	Important patches have been installed. In order for these patches to be applied a reboot is required. Please click here to reboot now.
Description text	To complete the installation of patches to your computer, it is now necessary to reboot. If you require any additional information, please contact your Novell ZENworks Patch Management administrator.
Suppress Reboot	No
Allow User to cancel	No
Time to show dialog before reboot	No 120 seconds
Allow User to snooze	Yes 0 Days 2 Hours 0 Minutes

- ◆ **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.

For eg. Select this option and customize the settings by changing the Popup text to “Custom Reboot Popup text” and the Description text to “Custom Reboot Description text”. Also change the options settings as shown in the figure below.

Define Reboot Options

Use values assigned to system variables or defaults
 Override Settings

Notify Users

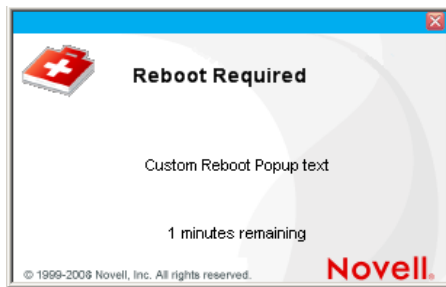
Popup text
 Custom Reboot Popup text

Description text
 Custom Reboot Description text

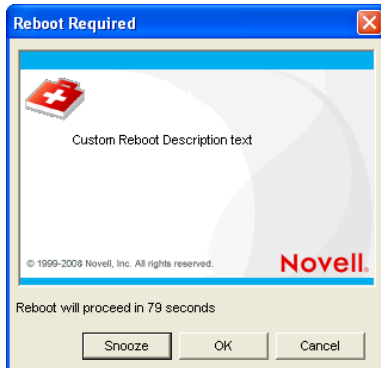
Options

	Yes	No
Suppress Reboot	<input type="radio"/>	<input checked="" type="radio"/>
Allow User to cancel	<input checked="" type="radio"/>	<input type="radio"/>
Time to show dialog before reboot	<input checked="" type="radio"/>	80 Seconds
Allow User to snooze	<input checked="" type="radio"/>	0 Days 0 Hours 2 Minutes

A popup text will be displayed when the reboot will be required as shown in the figure below.



A popup will be displayed containing the customized description 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 four options:
 - ◆ **Suppress Reboot:** Prevents a reboot even if the patch bundle requires a reboot.
 - ◆ **Allow User to cancel:** Allows the user to cancel the reboot.
 - ◆ **Time to show dialog before reboot:** The time in seconds that allows user to choose whether to reboot after installation of a patch.
 - ◆ **Allow User to snooze:** Allows the user to snooze the reboot.

NOTE: Even if you choose to snooze the reboot, the pop-up window continues to appear every few seconds until you proceed with or cancel 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.

6.10.1 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

6.11 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 6-31 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.

6.12 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 6-32 Deployment Summary Page

Patches

Step 9: Deployment Summary

Please review summary and then press finish.

Property Name	Details
Schedule	Event
Total selected packages	3

Order	Package Name	Reboot
1	Adobe APSB07-12 Flash Player 9.0.r47 for IE (Upgrade) (All Languages) (Rev 3)	No
2	Adobe APSB08-11 Flash Player 9.0.r124 for FireFox (Rev 2)	No
3	Adobe APSB07-20 Flash Player 9.0.r115 for IE (Upgrade) (All Languages)	No

<< Back Finish Cancel

Figure 6-33 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:

- ♦ **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.
- ♦ **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.

- ♦ [Section 7.1, “About Mandatory Baselines,” on page 117](#)
- ♦ [Section 7.2, “Working with Mandatory Baselines,” on page 121](#)

7.1 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 Discover Applicable Updates (DAU) task for all devices in that group.
- ♦ Every few hours, depending on the results of the DAU 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.

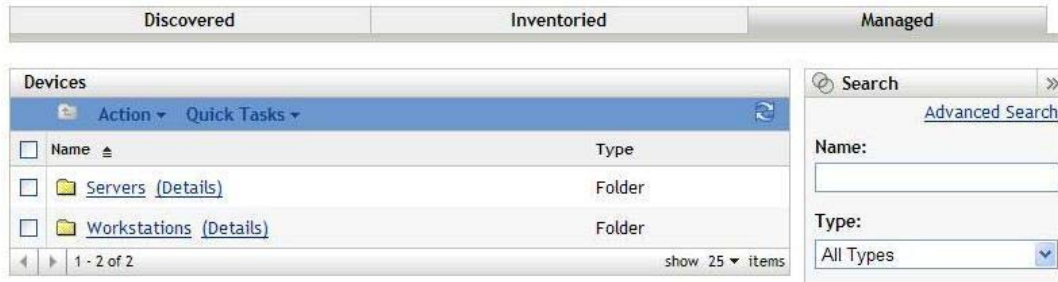
The following sections provide more information on mandatory baselines:

- ♦ [Section 7.1.1, “Viewing Mandatory Baselines,” on page 118](#)
- ♦ [Section 7.1.2, “Using the Mandatory Baseline Page,” on page 120](#)

7.1.1 Viewing Mandatory Baselines

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

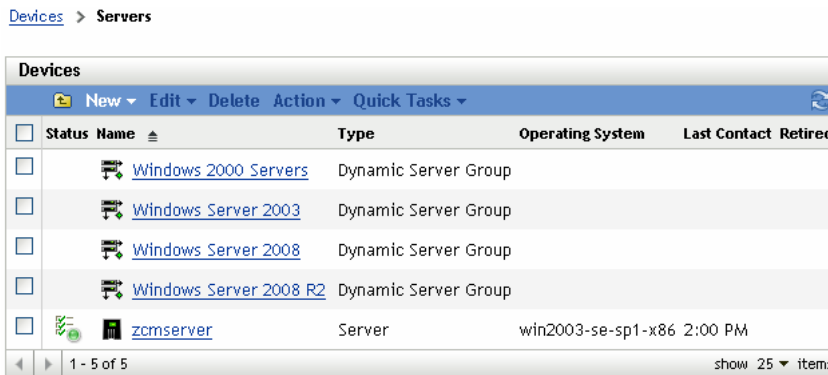
A page displaying the root folders for each type of device appears, as shown in the following figure:



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.

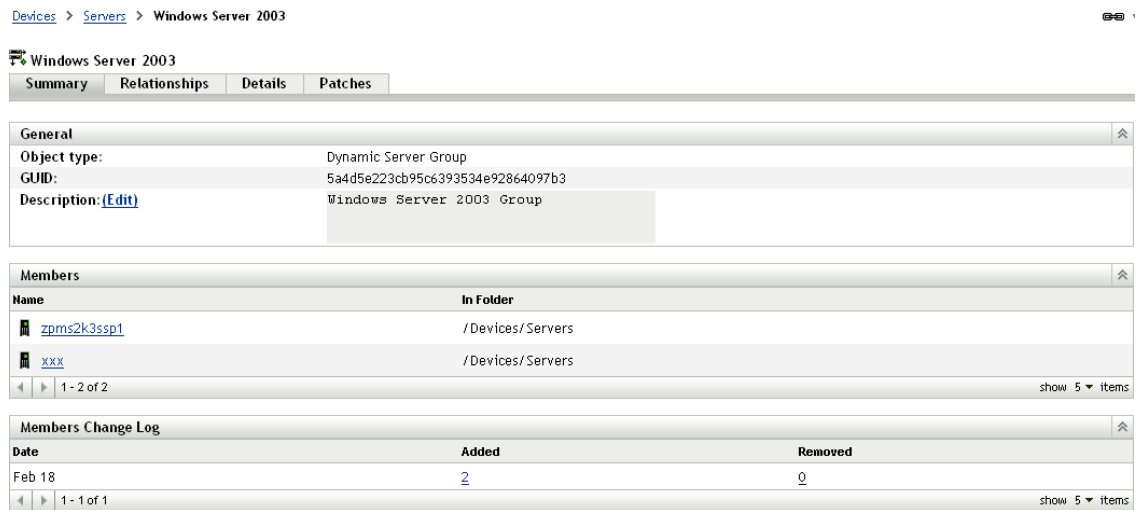
- 2 Click the *Servers* or *Workstations* link.

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:



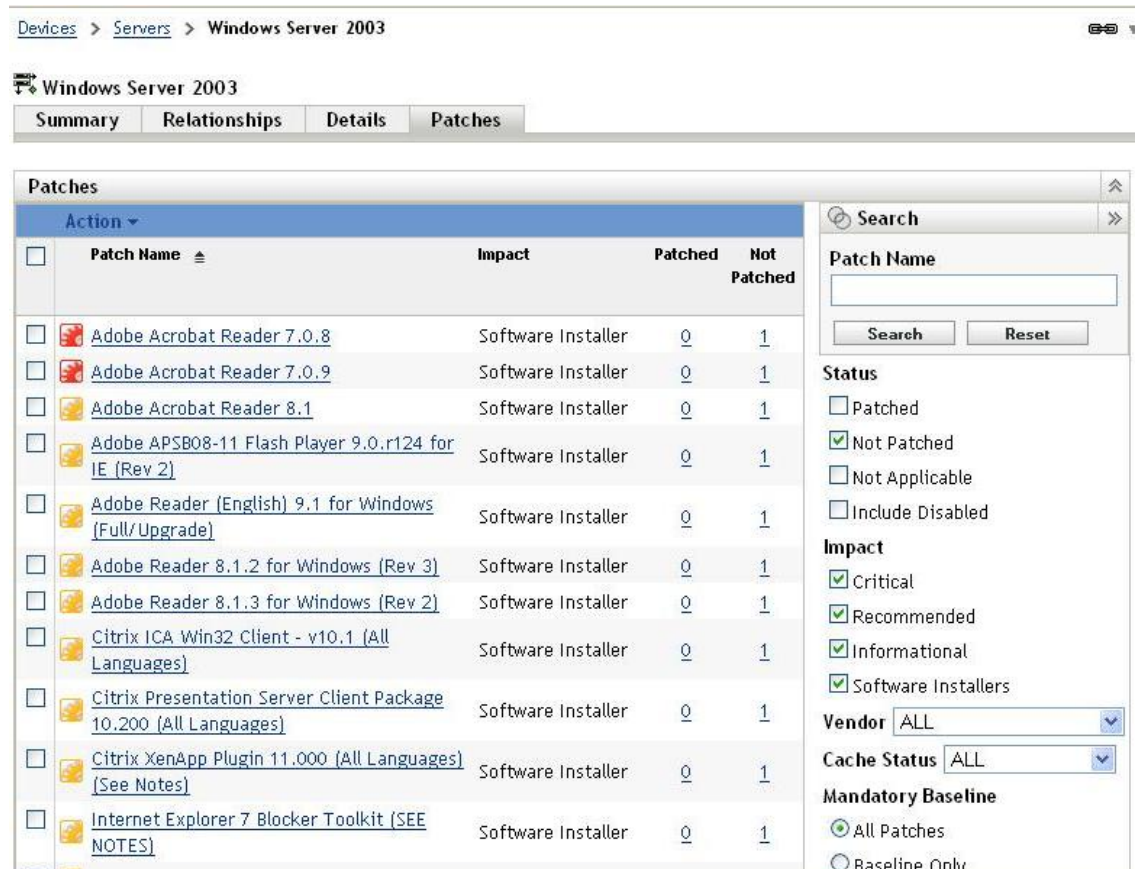
3 On the Servers or Workstation page (in this case, it is the Servers page), select any group.


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 2003* is selected:



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 2003*, the *Patches* tab displays all the patches applicable to the member devices within the group *Windows Server 2003*, as shown in the following figure:



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.

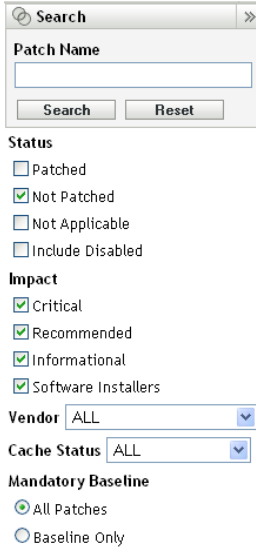
For detailed information on *Patches* and *Patches Information* panels, refer to [Chapter 5, “Using the Patch Management Tab,”](#) on page 61.

7.1.2 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 panel with the following elements:

- Search** (panel title)
- Patch Name** (input field)
- Search** and **Reset** (buttons)
- Status** (checkboxes):
 - Patched
 - Not Patched
 - Not Applicable
 - Include Disabled
- Impact** (checkboxes):
 - Critical
 - Recommended
 - Informational
 - Software Installers
- Vendor** (dropdown menu): ALL
- Cache Status** (dropdown menu): ALL
- Mandatory Baseline** (radio buttons):
 - All Patches
 - Baseline Only

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

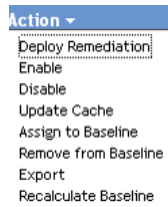
- ◆ **All Patches:** Displays all patches, including mandatory baseline items.

- ♦ **Baseline Only:** Displays only those patches that are marked as “mandatory baseline” for the group.

7.2 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 [Section 7.2.3, “Using Update Cache,” on page 124](#).
- ♦ The *Assign to Baseline* option enables you to assign a baseline to a patch. For more information, see [Section 7.2.1, “Assigning or Managing a Mandatory Baseline,” on page 122](#).
- ♦ The *Remove from Baseline* option enables you to remove a patch from a baseline. See [Section 7.2.2, “Removing a Mandatory Baseline,” on page 123](#) 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:

- ♦ [Section 7.2.1, “Assigning or Managing a Mandatory Baseline,” on page 122](#)
- ♦ [Section 7.2.2, “Removing a Mandatory Baseline,” on page 123](#)
- ♦ [Section 7.2.3, “Using Update Cache,” on page 124](#)

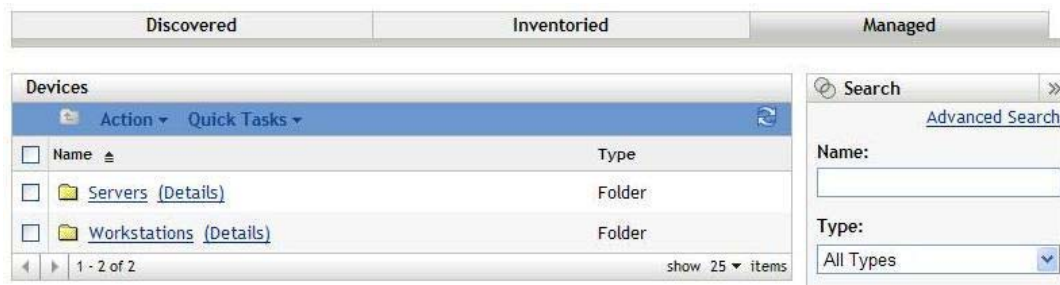
7.2.1 Assigning or Managing a Mandatory Baseline

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.

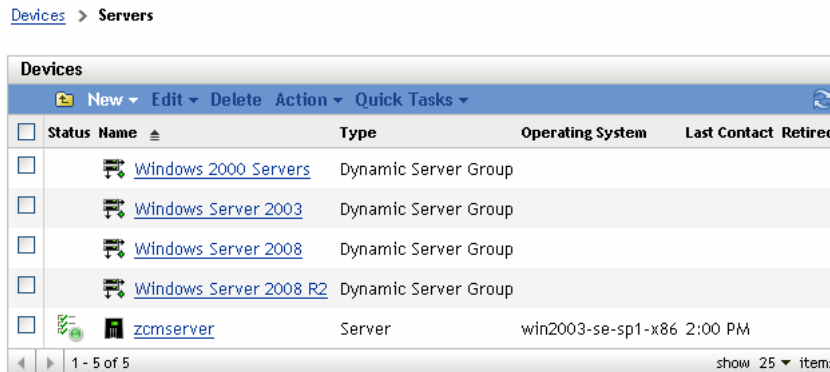
A page displaying the root folders for each type of device appears, as shown in the following figure:



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.

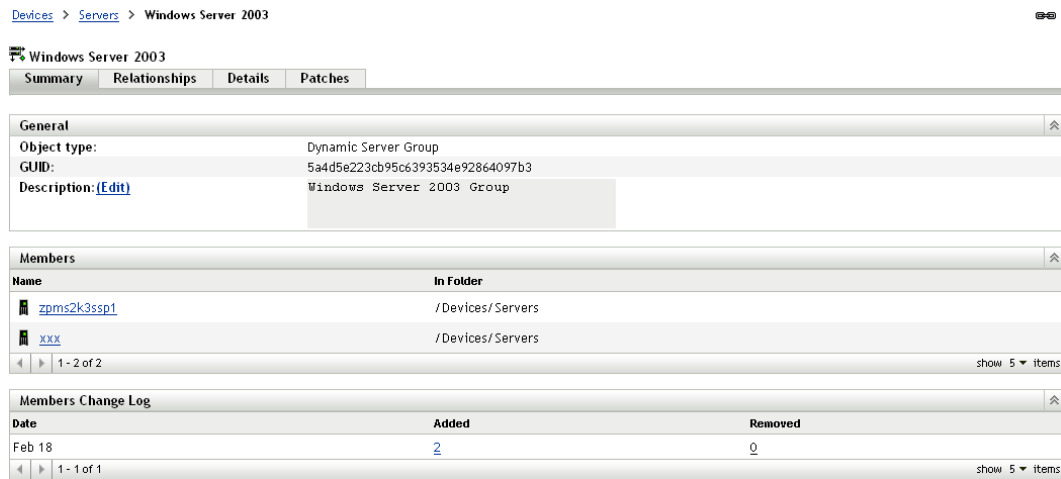
- 2 Click the *Servers* or *Workstations* link.

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:



- 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 2003* 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.

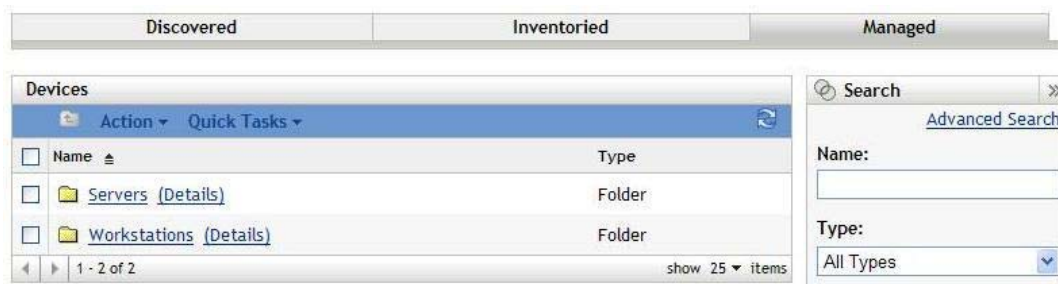
After a patch has been assigned to the baseline, the following process takes place:

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 DAU 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.

7.2.2 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:

[Devices](#) > [Servers](#)

Status	Name	Type	Operating System	Last Contact	Retired
<input type="checkbox"/>	Windows 2000 Servers	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"/>	zcmserver	Server	win2003-se-sp1-x86	2:00 PM	

1 - 5 of 5 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 2003* is selected:

[Devices](#) > [Servers](#) > [Windows Server 2003](#)

Windows Server 2003

Summary Relationships Details Patches

General	
Object type:	Dynamic Server Group
GUID:	5a4d5e223cb95c6393534e92864097b3
Description: (Edit)	Windows Server 2003 Group

Members	
Name	In Folder
zpm2k3ssp1	/Devices/Servers
xxx	/Devices/Servers

1 - 2 of 2 show 5 items

Members Change Log		
Date	Added	Removed
Feb 18	2	0

1 - 1 of 1 show 5 items

- 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.



7.2.3 Using Update Cache

The *Action* menu *Update Cache* option (see [Figure 7-2 on page 121](#)) 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 SP3 Patch Management:

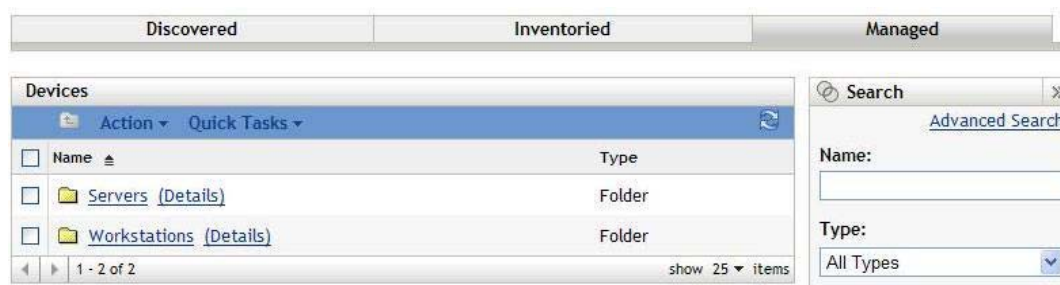
- ♦ [Section 8.1, “Accessing the Patches Tab for a Device,” on page 127](#)
- ♦ [Section 8.2, “Using the Patches Tab for a Device,” on page 130](#)

8.1 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 ▾						
<input type="checkbox"/>	Status	Name	Type	Operating System	Last Contact	Retired
<input type="checkbox"/>		Windows 2000 Servers	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"/>		zcmserver	Server	win2003-se-sp1-x86	2:00 PM	

1 - 5 of 5 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.
Operating System	Searches for devices running a particular operating system.
Message Status	Searches for devices that display a particular message status.
Compliance Status	Searches for devices based on their compliance status, such as <i>Yes</i> or <i>No</i> .
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 `zpmS2k3sSP3` for the managed device is an example. The network administrator decides the name of the managed device.

[Devices](#) > [Servers](#) > `zpmS2k3ssp1`

zpmS2k3ssp1

Summary	Inventory	Relationships	Settings	Content	Statistics	Patches
---------	-----------	---------------	----------	---------	------------	---------

General

Alias:	zpmS2k3ssp1
Host Name:	zpmS2k3Ssp1
IP Address:	172.16.11.134
Last Full Refresh:	9:42 AM
Last Contact:	1:42 PM
ZENworks Configuration Management Version:	10.2.0.0
ZENworks Asset Management Version:	10.2.0.16026
ZENworks Patch Management Version:	
ZENworks Agent Version:	10.2.0.16030
ZENworks Agent Status:	●
Operating System:	Microsoft Windows Server 2003 5.2.1 3790
Number of errors not acknowledged:	1
Number of warnings not acknowledged:	0
Primary User:	No user sources configured
Owner:	(Edit)
Serial Number:	(Edit) b5b246af5b22dd98974fad6fc77ecdac
GUID:	b5b246af5b22dd98974fad6fc77ecdac
Department:	(Edit)
Site:	(Edit)
Location:	(Edit)

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

[Devices](#) > [Servers](#) > `zpmS2k3ssp1`

zpmS2k3ssp1

Summary	Inventory	Relationships	Settings	Content	Statistics	Patches
---------	-----------	---------------	----------	---------	------------	---------

Patches

Action	Patch Name	Impact	Patched
<input type="checkbox"/>	Adobe Acrobat Reader 6.0.2 Update	Critical	No
<input type="checkbox"/>	Adobe Acrobat Reader 6.0.3 Update	Critical	No
<input type="checkbox"/>	Adobe Acrobat Reader 6.0.4 Update	Critical	No
<input type="checkbox"/>	Adobe Acrobat Reader 6.0.5 Update	Critical	No
<input type="checkbox"/>	Adobe Acrobat Reader 6.0.6 Update	Recommended	No
<input type="checkbox"/>	Adobe Acrobat Reader 7.0.1 Update	Critical	No
<input type="checkbox"/>	Adobe Acrobat Reader 7.0.2 Update	Critical	No
<input type="checkbox"/>	Adobe Acrobat Reader 7.0.5 Update [SEE NOTES]	Critical	No
<input type="checkbox"/>	Adobe Acrobat Reader 7.0.7 Update [SEE NOTES]	Critical	No
<input type="checkbox"/>	Adobe Acrobat Reader 7.0.8 (Update) [Rev 4]	Critical	No
<input type="checkbox"/>	Adobe APSB06-07 Dreamweaver Server Behavior SQL Injection vulnerability	Critical	No
<input type="checkbox"/>	Adobe APSB07-12 Flash Player 9.0.r47 for FireFox (Upgrade) (All Languages)	Critical	No
<input type="checkbox"/>	Adobe APSB07-12 Flash Player 9.0.r47 for IE (Upgrade) (All Languages) [Rev 3]	Critical	No
<input type="checkbox"/>	Adobe APSB07-12 Flash Player 9.0.r47 for Netscape (Upgrade) (All Languages) [Rev 2]	Critical	No

Search

Patch Name:

Status

Patched

Not Patched

Not Applicable

Include Disabled

Impact

Critical

Recommended

Informational

Software Installers

Vendor:

Cache Status:

8.2 Using the Patches Tab for a Device

- ◆ [Section 8.2.1, “Patches,” on page 130](#)
- ◆ [Section 8.2.2, “Patch Name,” on page 130](#)
- ◆ [Section 8.2.3, “Total Number of Patches Available,” on page 131](#)
- ◆ [Section 8.2.4, “Patch Impacts,” on page 131](#)
- ◆ [Section 8.2.5, “Patch Statistics,” on page 132](#)
- ◆ [Section 8.2.6, “Action Menu Items,” on page 132](#)
- ◆ [Section 8.2.7, “Searching Patches,” on page 133](#)
- ◆ [Section 8.2.8, “Patch Information,” on page 135](#)
- ◆ [Section 8.2.9, “Workstation Device Patches,” on page 136](#)

8.2.1 Patches

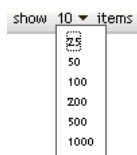
This section of the Patches page provides the following information about patches:

- ◆ 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 [Section 8.2.6, “Action Menu Items,” on page 132](#).

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

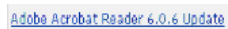


8.2.2 Patch Name

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



8.2.3 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

1 - 10 of 979

8.2.4 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)	

Novell Patch Impacts	Windows	Other
Informational	NA	NA

Source: Lumension Security

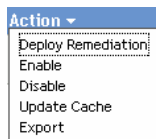
8.2.5 Patch Statistics

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*.

8.2.6 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.

NOTE: Disabling a patch also disables all the bundles associated with it.

- ◆ **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*.

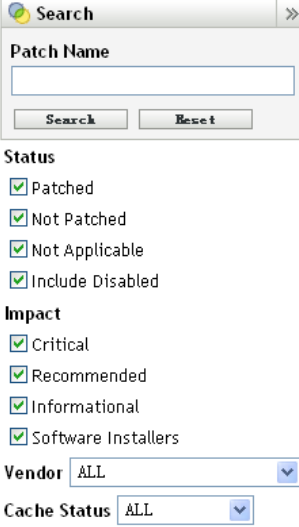
The patch icon changes to . While the download is in progress, the icon changes to . When the caching is complete, the color of the patch icon changes to green. This indicates that the patch remediation is ready to be deployed.

- ◆ **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.

8.2.7 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 interface with the following elements:

- Search** window title with a close button (X) and a right arrow (>).
- Patch Name** text input field.
- Search** and **Reset** buttons.
- Status** section with four checked checkboxes: Patched, Not Patched, Not Applicable, and Include Disabled.
- Impact** section with four checked checkboxes: Critical, Recommended, Informational, and Software Installers.
- Vendor** drop-down menu set to **ALL**.
- Cache Status** drop-down menu set to **ALL**.

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*

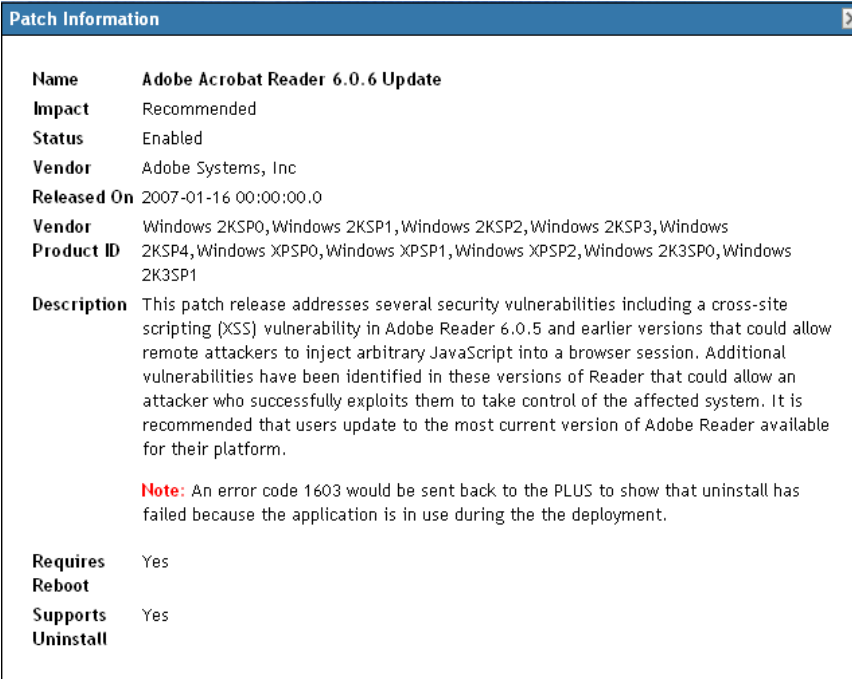
Filter	Result
Vendor	Search results include all the patches relevant to the vendor.
Cache Status	Search results include all the patches that have been cached, not been cached, or whose caching process has failed on the local server.

8.2.8 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 *Adobe Acrobat Reader 6.0.6 Update* 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



The screenshot shows a window titled "Patch Information" with a close button in the top right corner. The window contains the following details:

Name	Adobe Acrobat Reader 6.0.6 Update
Impact	Recommended
Status	Enabled
Vendor	Adobe Systems, Inc
Released On	2007-01-16 00:00:00.0
Vendor	Windows 2KSP0, Windows 2KSP1, Windows 2KSP2, Windows 2KSP3, Windows
Product ID	2KSP4, Windows XPSP0, Windows XPSP1, Windows XPSP2, Windows 2K3SP0, Windows 2K3SP1
Description	This patch release addresses several security vulnerabilities including a cross-site scripting (XSS) vulnerability in Adobe Reader 6.0.5 and earlier versions that could allow remote attackers to inject arbitrary JavaScript into a browser session. Additional vulnerabilities have been identified in these versions of Reader that could allow an attacker who successfully exploits them to take control of the affected system. It is recommended that users update to the most current version of Adobe Reader available for their platform. Note: An error code 1603 would be sent back to the PLUS to show that uninstall has failed because the application is in use during the the deployment.
Requires Reboot	Yes
Supports Uninstall	Yes

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.
Impact	The impact of the patch as determined by Novell. See Section 8.2.4, "Patch Impacts," on page 131.
Status	Status of the patch; can be <i>Enabled</i> , <i>Disabled (Superseded)</i> or <i>Disabled (By User)</i> .
Vendor	The name of the vendor or manufacturer.
Released on	The date the patch was released.
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 uninstallation.

8.2.9 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:

[Devices](#) > **Workstations**

Devices					
New Edit Delete Action Quick Tasks					
<input type="checkbox"/>	Status	Name	Type	Operating System	Last Contact Retired
<input type="checkbox"/>		Windows 2000 Workstations	Dynamic Workstation Group		
<input type="checkbox"/>		Windows 7 Workstations	Dynamic Workstation Group		
<input type="checkbox"/>		Windows Vista Workstations	Dynamic Workstation Group		
<input type="checkbox"/>		Windows XP Workstations	Dynamic Workstation Group		
<input type="checkbox"/>		w2adxps2	Workstation	winxp-pro-sp2-x86	2:41 PM

1 - 5 of 5 show 25 items

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 128).

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

[Devices](#) > [Workstations](#) > [w2adxpsp2](#)

 w2adxpsp2

Summary	Inventory	Relationships	Settings	Content	Patches
General					
Alias:	w2adxpsp2				
Host Name:	W2AdxPsp2				
IP Address:	172.16.11.49				
Last Full Refresh:	1:28 PM				
Last Contact:	1:28 PM				
ZENworks Agent Version:	10.2.0.16030				
ZENworks Agent Status:					
Operating System:	Microsoft Windows XP Professional 5.1 2 2600				
Number of errors not acknowledged:	0				
Number of warnings not acknowledged:	0				
Primary User:	No user sources configured				
Owner:	(Edit)				
Serial Number:	(Edit) d69e308e2fd9e3418f828206eb15a03e				
GUID:	d69e308e2fd9e3418f828206eb15a03e				
Department:	(Edit)				
Site:	(Edit)				
Location:	(Edit)				

- Click the *Patches* tab.















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

Devices > Servers > zpms2k3ssp1

zpms2k3ssp1

Summary Inventory Relationships Settings Content Statistics Patches

Patches

Action	Patch Name	Impact	Patched
<input type="checkbox"/>	 Adobe Acrobat Reader 6.0.2 Update	Critical	No
<input type="checkbox"/>	 Adobe Acrobat Reader 6.0.3 Update	Critical	No
<input type="checkbox"/>	 Adobe Acrobat Reader 6.0.4 Update	Critical	No
<input type="checkbox"/>	 Adobe Acrobat Reader 6.0.5 Update	Critical	No
<input type="checkbox"/>	 Adobe Acrobat Reader 6.0.6 Update	Recommended	No
<input type="checkbox"/>	 Adobe Acrobat Reader 7.0.1 Update	Critical	No
<input type="checkbox"/>	 Adobe Acrobat Reader 7.0.2 Update	Critical	No
<input type="checkbox"/>	 Adobe Acrobat Reader 7.0.5 Update (SEE NOTES)	Critical	No
<input type="checkbox"/>	 Adobe Acrobat Reader 7.0.7 Update (SEE NOTES)	Critical	No
<input type="checkbox"/>	 Adobe Acrobat Reader 7.0.8 (Update) (Rev 4)	Critical	No
<input type="checkbox"/>	 Adobe APSB06-07 Dreamweaver Server Behavior SQL Injection vulnerability	Critical	No
<input type="checkbox"/>	 Adobe APSB07-12 Flash Player 9.0.r47 for FireFox (Upgrade) (All Languages)	Critical	No
<input type="checkbox"/>	 Adobe APSB07-12 Flash Player 9.0.r47 for IE (Upgrade) (All Languages) (Rev 3)	Critical	No
<input type="checkbox"/>	 Adobe APSB07-12 Flash Player 9.0.r47 for Netscape (Upgrade) (All Languages) (Rev 2)	Critical	No

Search

Patch Name

Search Reset

Status

Patched

Not Patched

Not Applicable

Include Disabled

Impact

Critical

Recommended

Informational

Software Installers

Vendor ALL

Cache Status ALL

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.

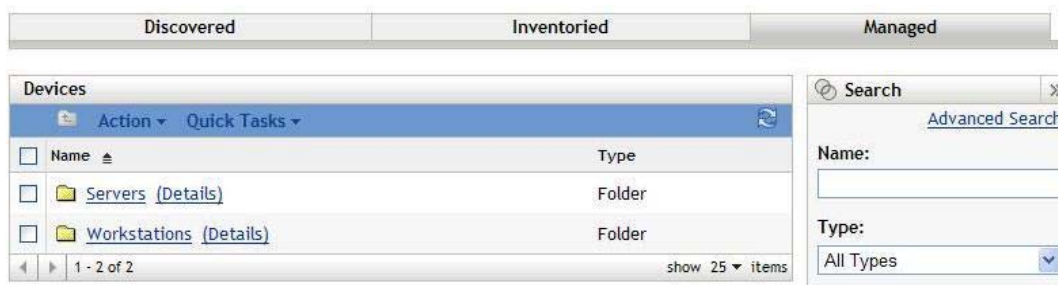
- ♦ Section 9.1, “Using the Patches Tab within a Server Group,” on page 139
- ♦ Section 9.2, “Using the Patches Tab within a Workstation Group,” on page 141

9.1 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 ▾						
<input type="checkbox"/>	Status	Name	Type	Operating System	Last Contact	Retired
<input type="checkbox"/>		Windows 2000 Servers	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"/>		zcmserver	Server	win2003-se-sp1-x86	2:00 PM	

1 - 5 of 5 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 2003* type is selected:

[Devices](#) > [Servers](#) > [Windows Server 2003](#) @ 1

Windows Server 2003

Summary Relationships Details Patches

General ⌵

Object type: Dynamic Server Group
 GUID: 5a4d5e223cb95c6393534e92864097b3
 Description: [\(Edit\)](#) Windows Server 2003 Group

Members ⌵

Name	In Folder
zprms2k3ssp1	/Devices/Servers
xxx	/Devices/Servers

1 - 2 of 2 show 5 ▾ items

Members Change Log ⌵

Date	Added	Removed
Feb 18	<u>2</u>	<u>0</u>

1 - 1 of 1 show 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 Server 2003*, the *Patches* tab displays all the patches applicable to the member devices within the group *Windows Server 2003*, as shown in the following figure:

Devices > Servers > Windows Server 2003

Windows Server 2003

Summary Relationships Details Patches

Patches

Action	Patch Name	Impact	Patched	Not Patched
<input type="checkbox"/>	Adobe APSB08-11 Flash Player 9.0.r124 for IE (Rev 2)	Software Installer	0	2
<input type="checkbox"/>	Adobe Reader 9.0 for Windows (Full/Upgrade) (Rev 2)	Software Installer	0	2
<input type="checkbox"/>	Citrix Presentation Server Client Package 10.200 (All Languages)	Software Installer	0	2
<input type="checkbox"/>	Citrix XenApp Plugin 11.000 (All Languages) (See Notes)	Software Installer	0	2
<input type="checkbox"/>	Macromedia Flash Player 7.0.r19 for IE	Software Installer	0	1
<input type="checkbox"/>	Macromedia Flash Player 7.0.r61 for IE	Software Installer	0	1
<input type="checkbox"/>	Macromedia Flash Player 7.0.r63 for IE	Software Installer	0	1
<input type="checkbox"/>	Macromedia Flash Player 8.0.r22 for IE	Software Installer	0	1
<input type="checkbox"/>	Microsoft (English) XML Paper Specification Essentials Pack 1.0 (Rev 2)	Software Installer	0	2
<input type="checkbox"/>	Microsoft (English/MUI) Excel Viewer 2003	Software Installer	0	2
<input type="checkbox"/>	Microsoft (English/MUI) Word Viewer 2003	Software Installer	0	2
<input type="checkbox"/>	Microsoft .NET Framework 1.0 (Rev 2)	Software Installer	0	1
<input type="checkbox"/>	Microsoft .NET Framework 2.0 SP1 (See Notes) (Rev 3)	Critical	0	2
<input type="checkbox"/>	Microsoft .NET Framework 3.5 (Rev 3)	Software Installer	0	2
<input type="checkbox"/>	Microsoft .NET Framework 3.5 SP1 (All Languages) (See Notes)	Software Installer	0	2
<input type="checkbox"/>	Mozilla Firefox (English) 3.0 for Windows (Full/Upgrade) (Rev 2)	Software Installer	0	2

Search

Patch Name

Search Reset

Status

Patched

Not Patched

Not Applicable

Include Disabled

Impact

Critical

Recommended

Informational

Software Installers

Vendor ALL

Cache Status ALL

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 117](#).

9.2 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:

[Devices](#) > **Workstations**

Devices					
New ▾ Edit ▾ Delete Action ▾ Quick Tasks ▾					
<input type="checkbox"/>	Status	Name	Type	Operating System	Last Contact Retired
<input type="checkbox"/>		Windows 2000 Workstations	Dynamic Workstation Group		
<input type="checkbox"/>		Windows 7 Workstations	Dynamic Workstation Group		
<input type="checkbox"/>		Windows Vista Workstations	Dynamic Workstation Group		
<input type="checkbox"/>		Windows XP Workstations	Dynamic Workstation Group		
<input type="checkbox"/>		w2adxpsp2	Workstation	winxp-pro-sp2-x86	2:41 PM

1 - 5 of 5 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 XP Workstations* is selected:

[Devices](#) > [Workstations](#) > **Windows XP Workstations** @ 1

Windows XP Workstations

Summary Relationships Details Patches

General	
Object type:	Dynamic Workstation Group
GUID:	97454fc02e7481834f3339a2a80946b5
Description: (Edit)	Windows XP Workstation Group

Members	
Name	In Folder
xp-p-sp3-001	/ Devices/ Workstations
w2adxpsp2	/ Devices/ Workstations

1 - 2 of 2 show 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 XP Workstations, the *Patches* tab displays all the patches applicable to the member devices within the group Windows XP Workstations, as shown in the following figure:

Devices > Workstations > Windows XP Workstations

Windows XP Workstations

Summary Relationships Details Patches

Patches

Action	Patch Name	Impact	Patched	Not Patched
<input type="checkbox"/>	Adobe Acrobat Reader 6.0.2 update	Critical	0	0
<input type="checkbox"/>	Adobe Acrobat Reader 6.0.2 update	Critical	0	0
<input type="checkbox"/>	Adobe Acrobat Reader 6.0.2 update	Critical	0	0
<input type="checkbox"/>	Adobe Acrobat Reader 6.0.2 update	Critical	0	0
<input type="checkbox"/>	Adobe Acrobat Reader 6.0.3 Update	Critical	0	0
<input type="checkbox"/>	Adobe Acrobat Reader 6.0.3 Update	Critical	0	0
<input type="checkbox"/>	Adobe Acrobat Reader 6.0.3 Update	Critical	0	0
<input type="checkbox"/>	Adobe Acrobat Reader 6.0.4 Update	Critical	0	0
<input type="checkbox"/>	Adobe Acrobat Reader 6.0.4 Update	Critical	0	0
<input type="checkbox"/>	Adobe Acrobat Reader 6.0.4 Update	Critical	0	0
<input type="checkbox"/>	Adobe Acrobat Reader 6.0.4 Update	Critical	0	0
<input type="checkbox"/>	Adobe Acrobat Reader 6.0.4 Update	Critical	0	0
<input type="checkbox"/>	Adobe Acrobat Reader 6.0.5 Update	Critical	0	0
<input type="checkbox"/>	Adobe Acrobat Reader 6.0.5 Update	Critical	0	0
<input type="checkbox"/>	Adobe Acrobat Reader 6.0.5 Update	Critical	0	0

Search

Patch Name

Search Reset

Status

- Patched
- Not Patched
- Not Applicable
- Include Disabled

Impact

- Critical
- Recommended
- Informational
- Software Installers

Vendor ALL

Cache Status ALL

Mandatory Baseline

- All Patches
- Baseline Only

For information on the features of the Device Group Patches page for the selected workstations group, see “[About Mandatory Baselines](#)” on page 117.

10 License Behaviour of ZPM

This chapter describes the various ZPM license states and the functionalities available in the various states. The following sections describe the possible License states in Novell ZENworks 11 SP3:

- ♦ [Section 10.1, “ZCM Only State,” on page 145](#)
- ♦ [Section 10.2, “Trial State,” on page 145](#)
- ♦ [Section 10.3, “Trial Expired State,” on page 146](#)
- ♦ [Section 10.4, “Licensed State,” on page 147](#)
- ♦ [Section 10.5, “License Expired State,” on page 147](#)

10.1 ZCM Only State

ZPM will be in the ZCM only state when the state is in trial/valid ZCM. The license of the ZPM does not affect this state.

The capabilities that are supported:

- ♦ **Patches:** Only the Microsoft patch scanning is supported and Microsoft patches will be downloaded.
- ♦ **Scan result:** The DAU 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.

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

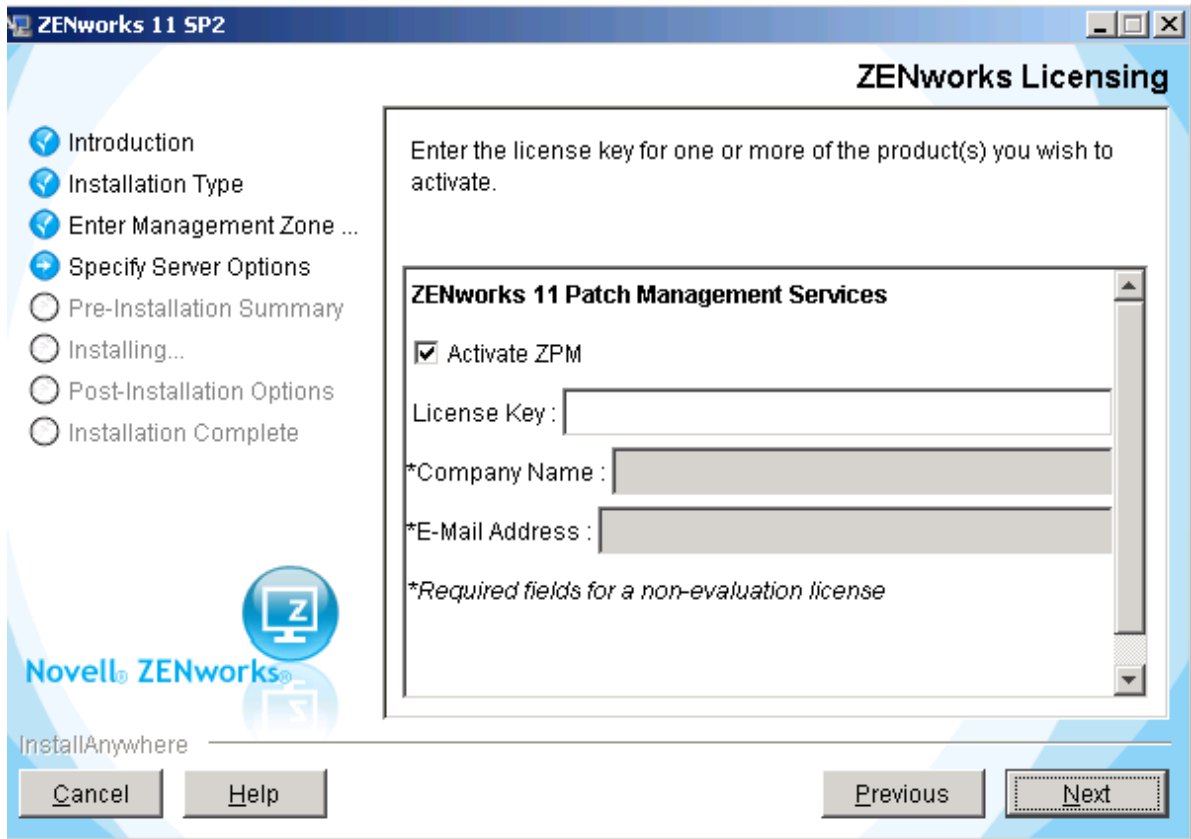
10.2 Trial State

ZENworks 11 SP3 allows the ZPM to have two(2) active trial states which are mentioned below:

- ♦ **Keyless trial:** During the installation when you select the “Activate ZPM” button it enables the keyless trial. It can be disabled during the installation and can be enabled at any later stage while using the application. This will allow 60 day full functionality trial of the ZPM.
- ♦ **Key based trial:** During the installation a valid license key of ZPM trial subscription can be entered or at any later stage while using the application. All the functionality of the ZPM will be allowed during this evaluation period.

NOTE: Only Microsoft patch scanning is allowed of ZPM. Enabling the ZPM trial will allow the application to function as a full functioning product. Also to use the ZPM the ZCM does not have to be licensed.

Figure 10-1 Activate ZPM during Installation



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.

10.3 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 [Section 9.1, “Using the Patches Tab within a Server Group,” on page 139.](#)

10.4 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 DAU 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.

10.5 License Expired State

When the ZPM license expires the functionality of the ZPM will behave in the same manner as “ZCM-Only State. See [Section 9.1, “Using the Patches Tab within a Server Group,” on page 139.](#)

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

- ♦ **Patches:** It will revert to supporting Microsoft patch scanning only, and Microsoft patches will be downloaded.

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](#).

- ♦ [Section 11.1, “Viewing the Predefined Report,” on page 149](#)

11.1 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:
 - ♦ **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.

For more information about ZENworks Reporting, see the [ZENworks Reporting 5 System Reference](#).

12 Best Practice with ZENworks 11 SP3 Patch Management

Patch Management is a fully integrated feature of Novell ZENworks 11 SP3 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 Discover Applicable Updates (DAU) 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.

12.1 Testing Patches

Before you start downloading a patch, configure the downloading options in the *Configuration* tab. For more information, see [Section 4.5, "Configuring Subscription Download Details," on page 42](#).

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.

12.2 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 83](#).

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 SP3 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

12.3 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 117](#).

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.

12.4 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.

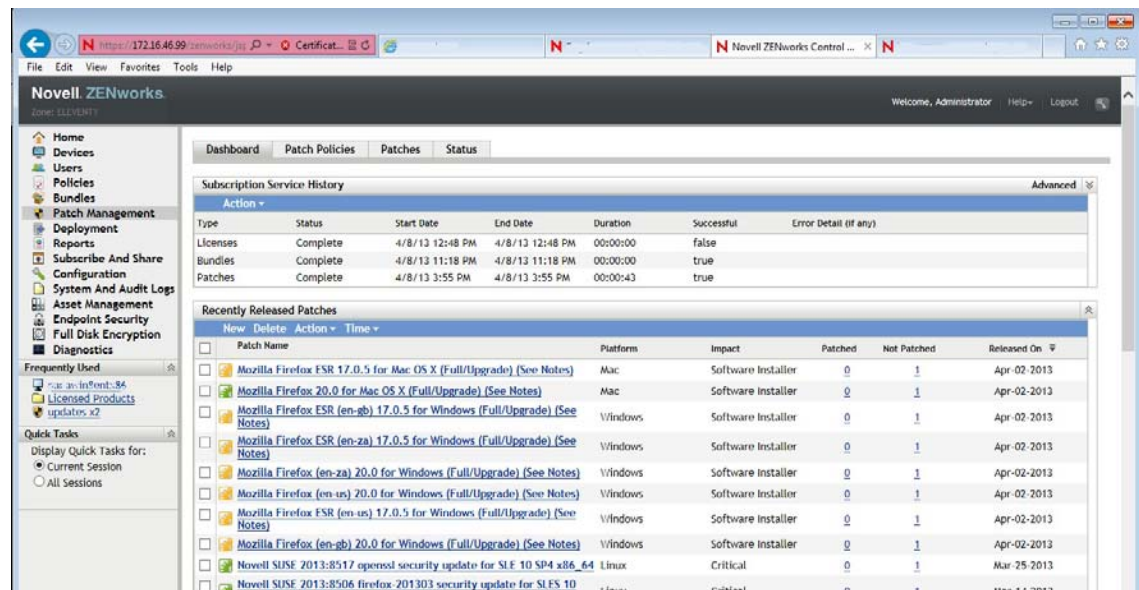
13.1 Setting up a Patch Policy

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:

- Linux
- Mac
- Windows

Description:

Linux - Create a patch policy for Linux devices.

<< 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:

Create New Patch Policy
Step 3: Define Rules

Enter the rules for the patch policy.

Patch Policy Rules
Specify the patch conditions for the patches you wish to enforce on the assigned devices.

Add Filter Add Filter Set Insert Filter ▾ Delete

Combine Filters using: and ▾

Select--
Age
Architecture
CVE Identifier
Impact
Patch Name
Release Date
Vendor

Only the t that meet these conditions will be enforced. Testing patches will be enforced only on assigned devices with

Incl

Patch Name	Impact	Released On ▾
No items available.		

<< Back Next >> Cancel

The following filters are available:

Filter Item	Result
Age	Select by age of patch: in days, weeks, months etc.
Architecture	Toggle between 32bit and 64bit
CVE Identifier	Insert a relevant CVE code
Impact	Choose Impact of patch ie 'Critical', 'Recommended' etc.
Patch Name	Filter by Patch Name ie: MSxxx xxx
Release date	Select by Patch Release date
Vendor	Select by Patch Vendor

It is also possible to add multiple filters, by clicking Add Filter Set, you can add a number of extra levels to further refine the patch cadre. For example, you could filter by Age + Architecture + Vendor.

Once the selection is made click Apply, the box below the selection tool will be populated with relevant patches (assuming that you have an agent attached and have also replicated) Review the Patches in the Included Patches box, and if satisfied to continue, click Next.

- 5 Review the Patch Policy in the *Patches* tab and if satisfied with the results proceed to the *Summary* tab

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 1 day(s)

Recalculate after 30 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

13.2 Publishing Patch Policy

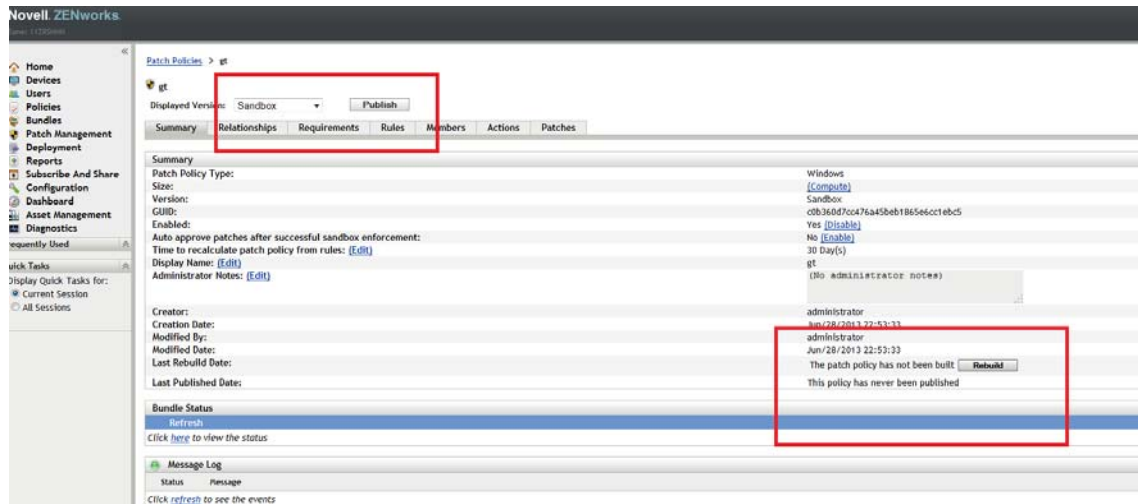
Once the Policy is created, you can further fine tune the parameters and even test it out before publishing it to a live environment.

- 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.



13.3 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 SP3 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

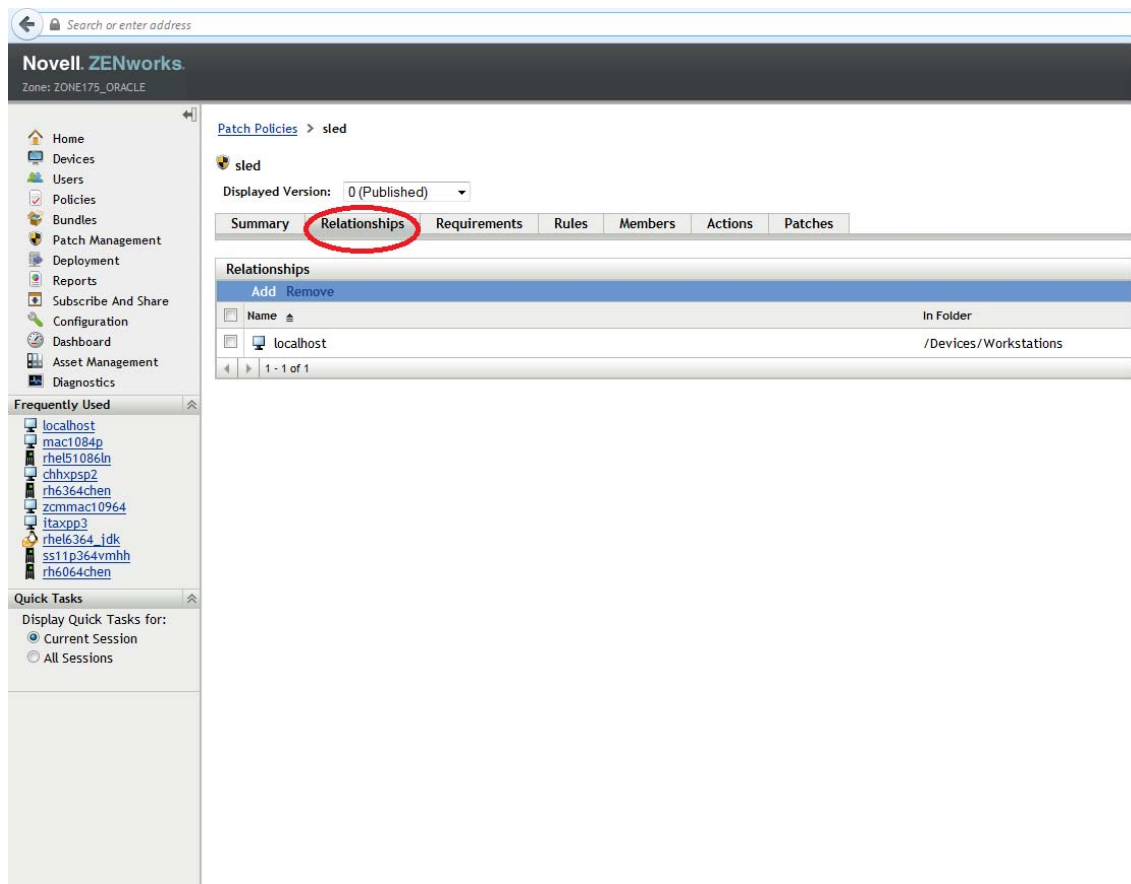
A selection of pre-made policies should be in the list

- 2 Choose a Policy to edit.

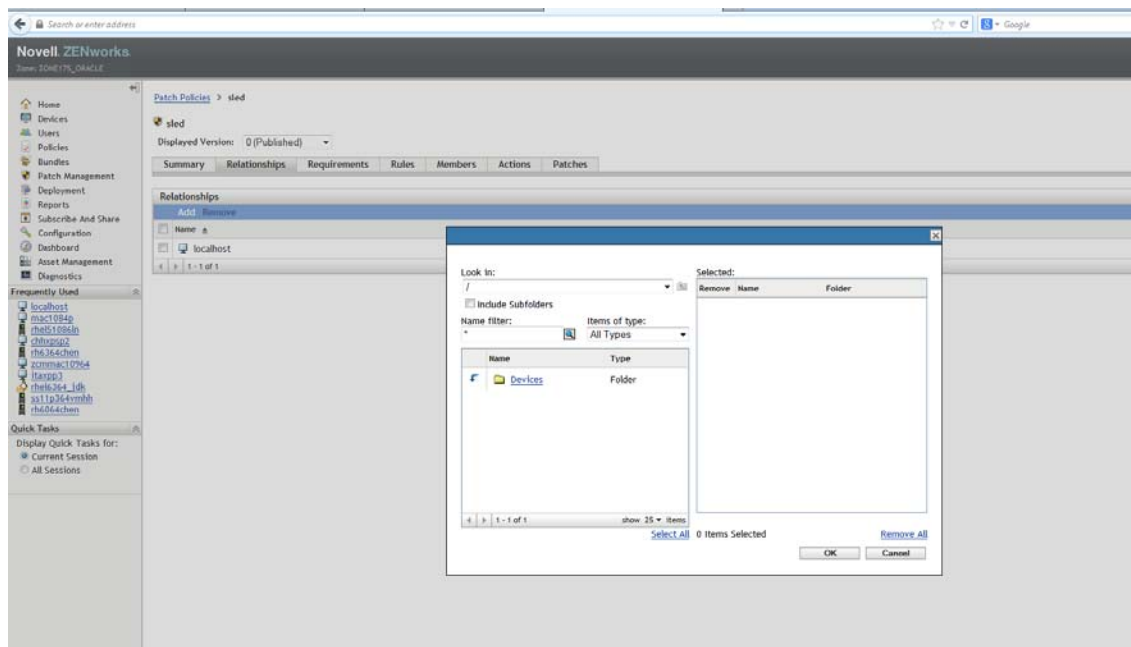
You should be presently on the Patch Policies dashboard, there are 4 tabs for Advanced settings: Relationships, Requirements, Members and Actions.

Remember, each selection will further define the list of patches that the policy produces

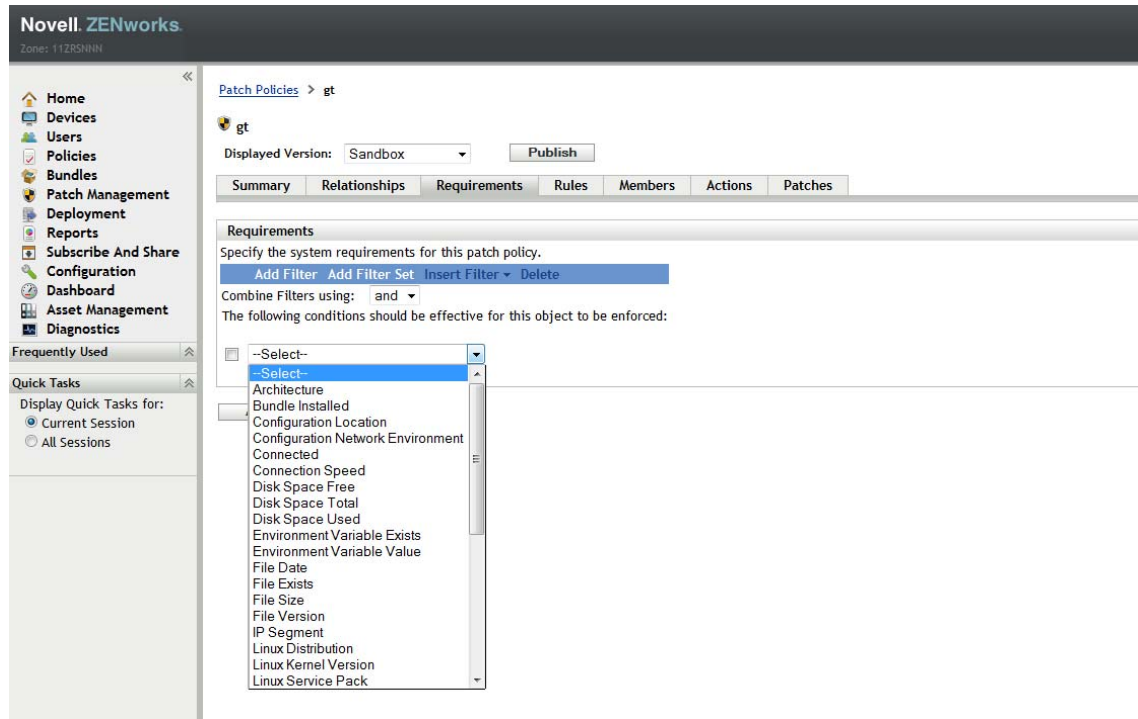
- 3 Click on the *Relationships* tab



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. Choose the appropriate device and click OK to set changes.



4 Click on the *Requirements* tab.

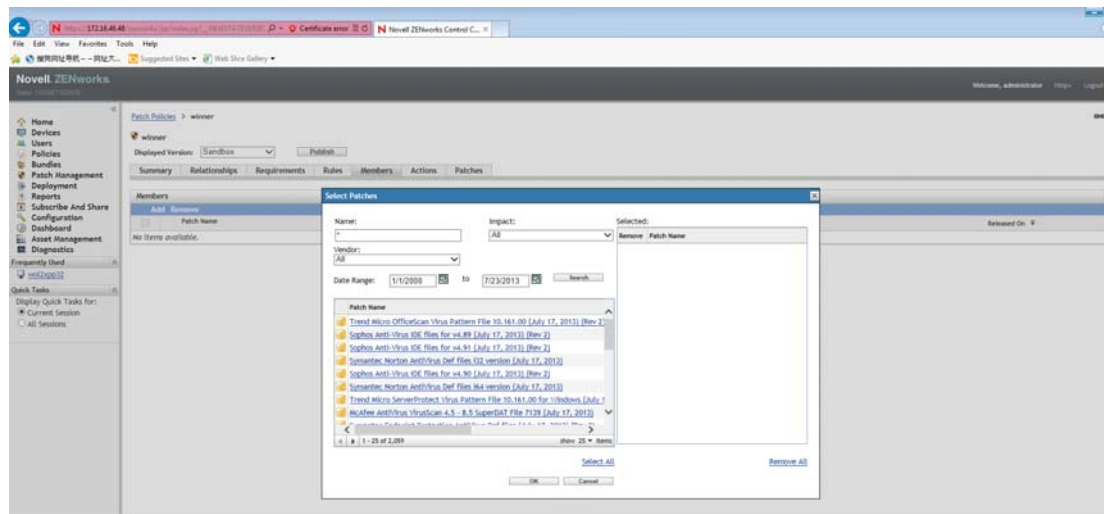


The Requirements tab has a lot of variables to choose from, as listed below:

Filter Item	Result
Architecture	Toggle between 32bit and 64bit
Bundle Installed	Choose between installed bundles
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

Filter Item	Result
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

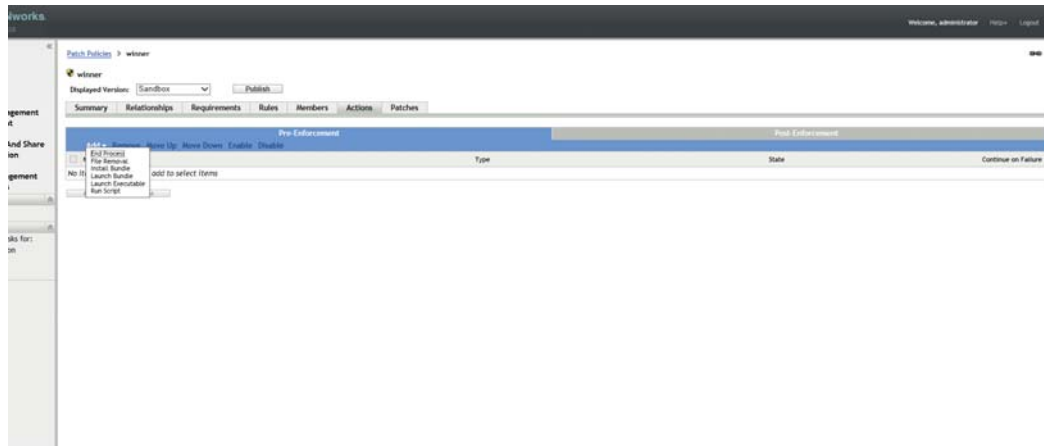
5 Click the *Members* tab.



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.

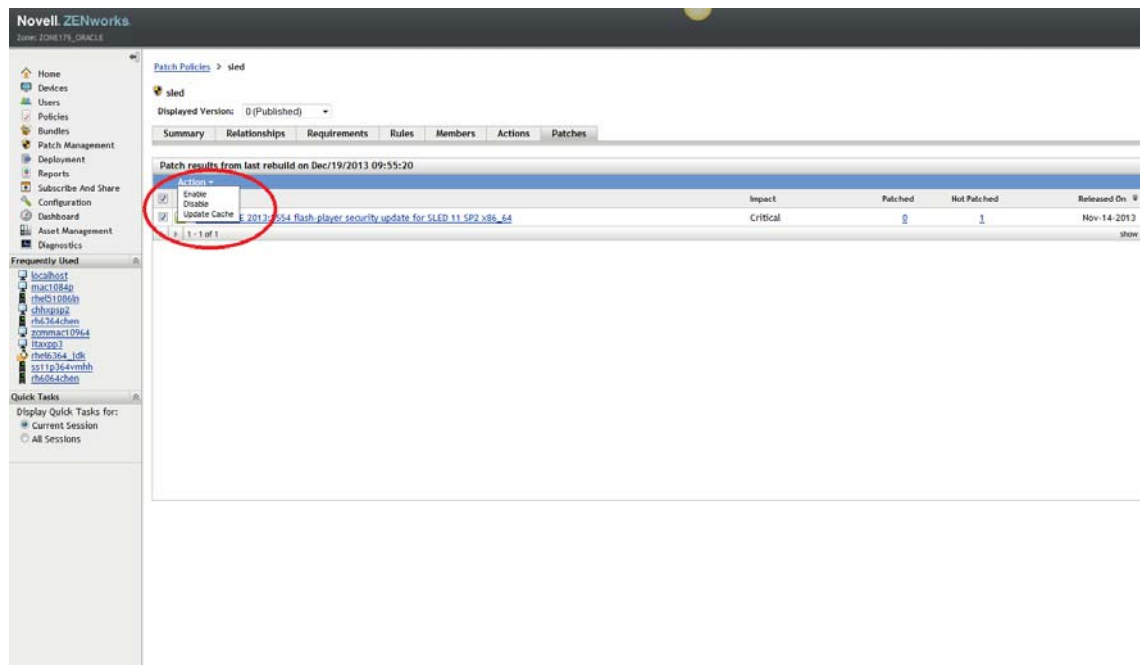
The available Actions are:

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.

13.4 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.

13.5 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.

13.6 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.

13.7 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 separate selection boxes, one controls the Schedule and the other sets the Reboot behavior, as below.

Novell. ZENworks
Zone: ZONE175_ORACLE

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)
 Hours Minutes

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 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	<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	<input checked="" type="radio"/>	<input type="radio"/>
Tray notification duration	<input type="text" value="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.
```


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'.

13.8 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:

Novell. ZENworks
Zone: ZONE175_ORACLE

Configuration > Patch Policy Distribution Settings

Patch Policy Distribution Settings
Configure the distribution time for patch policies

Schedule

Default (Distribution and enforcement will apply on enforcement schedule)
 Schedule Patch Policy Distribution

Restrict Duration (stop sending files 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 10:52 PM)

OK Apply Reset Cancel

- 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.

13.9 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.

A Troubleshooting Patch Management

The following sections contain detailed explanations of the error messages you might receive or problems you might encounter when using Novell ZENworks 11 SP3 Patch Management.

- ◆ Section A.1, “Patch Management Issues,” on page 173
- ◆ Section A.2, “Configuration Issues,” on page 179
- ◆ Section A.3, “Error Codes,” on page 179

A.1 Patch Management Issues

- ◆ “Patches are unavailable because of the CDN switch to Akamai for ZENworks Patch Management” on page 173
- ◆ “No patches are shown in the Patches tab” on page 176
- ◆ “Patches do not seem to be deployed on the target device” on page 176
- ◆ “The Cancel button disappears in the Reboot Required dialog box” on page 176
- ◆ “Superseded patches are shown as NOT APPLICABLE” on page 176
- ◆ “Patch deployment might not start when scheduled” on page 177
- ◆ “Microsoft System Installer (MSI) might need to be updated for some patches” on page 177
- ◆ “Remediation of Linux patches displays an error on the SLES 11 SP1 agent” on page 177
- ◆ ““Failed but set to continue” error shows in progress bar” on page 178
- ◆ “Patch Policy assignment: Bundle stays in ‘Pending’ state forever” on page 178
- ◆ “Patch Policy assignment: Error Message should be displayed for (failed) assignment to older agents” on page 178
- ◆ “Linux - Custom Patches: Bundles fail to launch” on page 179

Patches are unavailable because of the CDN switch to Akamai for ZENworks Patch Management

Source: ZENworks 11 SP3; Patch Management.

Explanation: In the week of 18 February 2008, the hosting infrastructure for the patch content Web site used by ZENworks 11 SP3 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
 - ◆ cdn.lumension.com.edgesuite.net
 - ◆ cache.lumension.com
 - ◆ a1533.g.akamai.net

- ◆ www.download.windowsupdate.com
- ◆ www.download.windowsupdate.nsatc.net
- ◆ download.windowsupdate.chinacache.net
- ◆ download.windowsupdate.com
- ◆ cc00022.h.cnssr.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
- ◆ e4579.c.akamaiedge.net
- ◆ nu.novell.com

NOTE: Adding hosts on ZENworks server, please use "nslookup" on command to get the IP address for each URLs.

- 2 Turn off *SSL Download* on the Configuration page (see [“Configuring Subscription Download Details”](#) on page 42).
- 3 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 a1533.g.akamai.net [12.37.74.25] with 32 bytes of
data:                               Replyfrom 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 SP3:

ZENworks 11 SP3 Patch Management license replication goes to the following servers:

206.16.247.2

206.16.45.34

Port 443

ZENworks 11 SP3 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 SP3; 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 SP3; 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 SP3; 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 SP3; 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 SP3:

- ◆ 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 SP3; 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 SP3; 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 \(http://www.microsoft.com/downloads/details.aspx?familyid=889482fc-5f56-4a38-b838-de776fd4138c&displaylang=en\)](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 SP3; 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 SP3; 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 recognised in older versions. Functionality is NOT affected.

Action: Nothing that can be done on agent side. However on the server side, while creating the bundle a action level system requirement can be added to the patchReportResult action not to execute on older agents. With this change only benefit is the error "Action handler not found" wont get reported to server.

Otherwise functionality wise there nothing that can be done to make the action run on older agents. For Linux patch bundles the action level system requirement that can be used is:

```
"Version of RPM" with values "novell-zenovell-patch-management-agent" ">="  
"11.3.0"
```

Patch Policy assignment: Bundle stays in ‘Pending’ state forever

Source: ZENworks 11 SP3; 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 SP3; 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 SP3; 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..

A.2 Configuration Issues

- ♦ [“Deploying patches with Auto Reboot causes the device to shut down” on page 179](#)

Deploying patches with Auto Reboot causes the device to shut down

Source: ZENworks 11 SP3; 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.

A.3 Error Codes

- ♦ [“ERROR CODE: ERR = 40” on page 180](#)
- ♦ [“ERROR CODE: PPX_ERROR_ARCHIVE_EXTRACT = 2” on page 180](#)
- ♦ [“ERROR CODE: PPX_ERROR_PACKAGE_ARCHIVE_INITIALIZE = 8” on page 181](#)
- ♦ [“ERROR CODE: PPX_ERROR_EXTRACT_FILE = 20” on page 181](#)
- ♦ [“ERROR CODE: PPX_ERROR_PACKAGE_REIMPORT = 40” on page 181](#)
- ♦ [“ERROR CODE: PPX_ERROR_EXPIRED_LICENSE_KEY = 27” on page 181](#)
- ♦ [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1” on page 181](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 3” on page 181](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 4” on page 181](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_MANY_APPLICABLE_SIGNATURES = 5” on page 181](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 6” on page 182](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 7” on page 182](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 9” on page 182](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 10” on page 182](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 11” on page 182](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 12” on page 182](#)
- ♦ [“ERROR CODE: PPX_ERROR_SIGNATURE_PREREQ_CACHE_EXHAUSTED = 13” on page 182](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 14” on page 182](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 15” on page 182](#)

- ◆ “ERROR CODE: PPX_ERROR_FINGERPRINT_EXPRESSION_SYNTAX = 16” on page 182
- ◆ “ERROR CODE: PPX_ERROR_FINGERPRINT_FILEROOT_UNSUPPORTED = 17” on page 183
- ◆ “ERROR CODE: PPX_ERROR_FINGERPRINT_TYPE_UNSUPPORTED = 18” on page 183
- ◆ “ERROR CODE: PPX_ERROR_SCRIPT_BAD_FILEHANDLE = 19” on page 183
- ◆ “ERROR CODE: PPX_ERROR_WMI_FINGERPRINT_UNSUPPORTED = 22” on page 183
- ◆ “ERROR CODE: PPX_ERROR_JAVASCRIPT_UNSUPPORTED = 23” on page 183
- ◆ “ERROR CODE: PPX_ERROR_MISSING_PREREQ_SIGNATURE = 25” on page 183
- ◆ “ERROR CODE: PPX_ERROR_INVALID_PREREQ_LANGUAGE = 26” on page 183
- ◆ “ERROR CODE: PPX_ERROR_INVALID_ROOT_HKEY = 21” on page 183
- ◆ “ERROR CODE: PPX_ERROR_FINGERPRINT_INVALID_SYSINFO = 31” on page 183
- ◆ “ERROR CODE: PPX_ERROR_FINGERPRINT_EXPRESSION_MISSING_VARIABLE = 32” on page 184
- ◆ “ERROR CODE: PPX_ERROR_FINGERPRINT_FILESCAN_UNSUPPORTED = 34” on page 184
- ◆ “ERROR CODE: PPX_ERROR_FINGERPRINT_WMI_ERROR = 35” on page 184
- ◆ “ERROR CODE: PPX_ERROR_RELEVANCE_SCRIPT_SYNTAX = 36” on page 184
- ◆ “ERROR CODE: PPX_ERROR_ENTITLED_FILE_INVALID = 41” on page 184
- ◆ “ERROR CODE: PPX_ERROR_ENTITLED_FILE_MISSING = 28” on page 184
- ◆ “ERROR CODE: PPX_ERROR_ENTITLED_FILE_BAD_CHECKSUM = 29” on page 184
- ◆ “ERROR CODE: PPX_ERROR_ENTITLED_FILE_WRONG_SIZE = 30” on page 185
- ◆ “ERROR CODE: PPX_ERROR_OUT_OF_MEMORY = 24” on page 185
- ◆ “ERROR CODE: PPX_ERROR_PACKAGE_MKDIR_FAILURE = 33” on page 185
- ◆ “ERROR CODE: PPX_ERROR_UNKNOWN” on page 185
- ◆ “ERROR CODE: 41” on page 185
- ◆ “ERROR CODE: 142” on page 185
- ◆ “ERROR CODE: 143” on page 186
- ◆ “ERROR CODE: 144” on page 186
- ◆ “ERROR CODE: 145” on page 186
- ◆ “ERROR MESSAGE: “There is an issue with checksum metadata at CDN”” on page 186
- ◆ “ERROR : zman prb "<baseline_patch_name>" - java.lang.NullPointerException when trying to get the DefaultHibernateSessionManager” on page 186
- ◆ “OTHER ERROR CODES” on page 188

ERROR CODE: ERR = 40

Source: ZENworks 11 SP3; 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_ARCHIVE_EXTRACT = 2

Source: ZENworks 11 SP3; 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 180.

ERROR CODE: PPX_ERROR_EXTRACT_FILE = 20

Source: See [“ERROR CODE: PPX_ERROR_ARCHIVE_EXTRACT = 2”](#) on page 180.

ERROR CODE: PPX_ERROR_PACKAGE_REIMPORT = 40

Source: See [“ERROR CODE: PPX_ERROR_ARCHIVE_EXTRACT = 2”](#) on page 180.

ERROR CODE: PPX_ERROR_EXPIRED_LICENSE_KEY = 27

Source: ZENworks 11 SP3; 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 SP3; 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 181.

ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 4

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

ERROR CODE:

PPX_ERROR_PATCH_MANY_APPLICABLE_SIGNATURES = 5

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 6

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 7

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 9

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 10

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 11

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 12

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

ERROR CODE:

PPX_ERROR_SIGNATURE_PREREQ_CACHE_EXHAUSTED = 13

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 14

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 15

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

ERROR CODE: PPX_ERROR_FINGERPRINT_EXPRESSION_SYNTAX = 16

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

**ERROR CODE:
PPX_ERROR_FINGERPRINT_FILEROOT_UNSUPPORTED = 17**

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

ERROR CODE: PPX_ERROR_FINGERPRINT_TYPE_UNSUPPORTED = 18

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

ERROR CODE: PPX_ERROR_SCRIPT_BAD_FILEHANDLE = 19

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

ERROR CODE: PPX_ERROR_WMI_FINGERPRINT_UNSUPPORTED = 22

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

ERROR CODE: PPX_ERROR_JAVASCRIPT_UNSUPPORTED = 23

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

ERROR CODE: PPX_ERROR_MISSING_PREREQ_SIGNATURE = 25

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

ERROR CODE: PPX_ERROR_INVALID_PREREQ_LANGUAGE = 26

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

ERROR CODE: PPX_ERROR_INVALID_ROOT_HKEY = 21

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

ERROR CODE: PPX_ERROR_FINGERPRINT_INVALID_SYSINFO = 31

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

**ERROR CODE:
PPX_ERROR_FINGERPRINT_EXPRESSION_MISSING_VARIABLE = 32**

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

**ERROR CODE:
PPX_ERROR_FINGERPRINT_FILESCAN_UNSUPPORTED = 34**

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

ERROR CODE: PPX_ERROR_FINGERPRINT_WMI_ERROR = 35

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

ERROR CODE: PPX_ERROR_RELEVANCE_SCRIPT_SYNTAX = 36

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 181.

ERROR CODE: PPX_ERROR_ENTITLED_FILE_INVALID = 41

Source: ZENworks 11 SP3; 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 184.

ERROR CODE: PPX_ERROR_ENTITLED_FILE_BAD_CHECKSUM = 29

Source: See [“ERROR CODE: PPX_ERROR_ENTITLED_FILE_INVALID = 41”](#) on page 184.

ERROR CODE: PPX_ERROR_ENTITLED_FILE_WRONG_SIZE = 30

Source: See [“ERROR CODE: PPX_ERROR_ENTITLED_FILE_INVALID = 41”](#) on page 184.

ERROR CODE: PPX_ERROR_OUT_OF_MEMORY = 24

Source: ZENworks 11 SP3; 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 SP3; 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 SP3; 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 Open a support ticket with Lumension.
- 2 Contact Novell Support.

ERROR CODE: 41

Source: ZENworks 11 SP3; 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 SP3; 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 SP3; 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 SP3; 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 SP3; 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 SP3; 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 SP3; 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(DelegatingMethodAccesso
rImpl.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(DelegatingMethodAccesso
rImpl.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 SP3; Patch Management.

Action: Contact Novell Support.