

## Reference

# **Novell® ZENworks® 10 Configuration Management Patch Management Services**

**10.1**

August 6, 2008

[www.novell.com](http://www.novell.com)



## 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 © 2007-2008 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. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the [Novell Legal Patents Web page \(http://www.novell.com/company/legal/patents/\)](http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.  
404 Wyman Street, Suite 500  
Waltham, MA 02451  
U.S.A.  
[www.novell.com](http://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

<b>About This Guide</b>	<b>7</b>
<b>1 Patch Management Services Overview</b>	<b>9</b>
1.1 Product Overview . . . . .	9
1.2 ZENworks Server and Adaptive Agent Process . . . . .	10
1.3 Features of ZENworks Patch Management Services . . . . .	11
<b>2 Using Patch Management Services</b>	<b>13</b>
2.1 Viewing Subscription Service Information . . . . .	13
2.2 Activating Your Paid Subscription or Viewing the Subscription Serial Number . . . . .	16
2.3 Configuring HTTP Proxy Details . . . . .	19
2.4 Configuring Subscription Download Details . . . . .	22
<b>3 Using Vulnerabilities</b>	<b>25</b>
3.1 Viewing Vulnerabilities . . . . .	25
3.2 Using the Vulnerabilities Page . . . . .	26
3.2.1 Vulnerabilities . . . . .	26
3.2.2 Vulnerability Information . . . . .	31
3.2.3 Searching Vulnerability . . . . .	32
3.2.4 Vulnerability Tasks . . . . .	33
<b>4 Using the Deploy Remediation Wizard</b>	<b>37</b>
4.1 Confirm Devices . . . . .	37
4.2 License Agreement . . . . .	39
4.3 Remediation Schedule . . . . .	40
4.3.1 Remediation Schedule – Date Specific . . . . .	41
4.3.2 Remediation Schedule – Recurring . . . . .	43
4.3.3 Remediation Schedule – Event . . . . .	48
4.4 Remediation Options . . . . .	49
4.5 Advanced Remediation Options . . . . .	50
4.6 Deployment Order and Behavior . . . . .	53
4.7 Notification and Reboot Options . . . . .	54
4.8 Deployment Summary . . . . .	56
<b>5 Using Mandatory Baselines</b>	<b>57</b>
5.1 About Mandatory Baselines . . . . .	57
5.1.1 Viewing Mandatory Baselines . . . . .	58
5.1.2 Using the Mandatory Baseline Page . . . . .	60
5.2 Working with Mandatory Baselines . . . . .	61
5.2.1 Assigning or Managing a Mandatory Baseline . . . . .	61
5.2.2 Removing a Mandatory Baseline . . . . .	63
5.2.3 Using Update Cache . . . . .	65

<b>6</b>	<b>Using Devices</b>	<b>67</b>
6.1	Server Device Vulnerabilities . . . . .	67
6.2	Using the Vulnerabilities Page for the Selected Device . . . . .	69
6.2.1	Vulnerabilities . . . . .	69
6.2.2	Vulnerability Name. . . . .	69
6.2.3	Total Number of Vulnerabilities Available . . . . .	70
6.2.4	Vulnerability Impacts . . . . .	70
6.2.5	Vulnerability Statistics . . . . .	71
6.2.6	Action Menu Items . . . . .	71
6.2.7	Vulnerability Information . . . . .	72
6.2.8	Searching Vulnerabilities . . . . .	74
6.2.9	Workstation Device Vulnerabilities . . . . .	75
<b>7</b>	<b>Using Device Group Vulnerabilities</b>	<b>77</b>
7.1	Server Group Vulnerabilities . . . . .	77
7.2	Workstation Group Vulnerabilities . . . . .	79

# About This Guide

This *Patch Management Services Reference* includes information to help you successfully install a Novell® ZENworks® 10 Configuration Management (10.1) system. The information in this guide is organized as follows:

- ♦ Chapter 1, “Patch Management Services Overview,” on page 9
- ♦ Chapter 2, “Using Patch Management Services,” on page 13
- ♦ Chapter 3, “Using Vulnerabilities,” on page 25
- ♦ Chapter 4, “Using the Deploy Remediation Wizard,” on page 37
- ♦ Chapter 5, “Using Mandatory Baselines,” on page 57
- ♦ Chapter 6, “Using Devices,” on page 67
- ♦ Chapter 7, “Using Device Group Vulnerabilities,” on page 77

## 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, or go to the [Novell Documentation Feedback site \(http://www.novell.com/documentation/feedback.html\)](http://www.novell.com/documentation/feedback.html) and enter your comments there.

## Additional Documentation

ZENworks 10 Configuration Management 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 10 Configuration Management with SP1 \(10.1\) documentation Web site \(http://www.novell.com/documentation/zcm10\)](http://www.novell.com/documentation/zcm10).

## Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (\*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux\*, should use forward slashes as required by your software.





# Patch Management Services Overview

# 1

Novell® ZENworks® 10 Configuration Management Patch Management Services is the core product of the leading patch and vulnerability management solution for medium and large enterprise networks. Patch Management Services enables customers to easily translate security 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, ZENworks Patch Management Services ensures that policy measurement and security audits are a true representation of network security status.

This section contains the following information:

- ♦ [Section 1.1, “Product Overview,” on page 9](#)
- ♦ [Section 1.2, “ZENworks Server and Adaptive Agent Process,” on page 10](#)
- ♦ [Section 1.3, “Features of ZENworks Patch Management Services,” on page 11](#)

## 1.1 Product Overview

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

ZENworks Patch Management Services provides rapid patch management, 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 management tool known as ZENworks Control Center, which is a centralized Web interface that allows you to monitor and maintain patch compliance throughout the whole enterprise. The ZENworks Server can deploy a ZENworks Adaptive Agent on every client system in the target network, ensuring that all systems are protected with the latest vulnerability patches, software updates, and service packs.

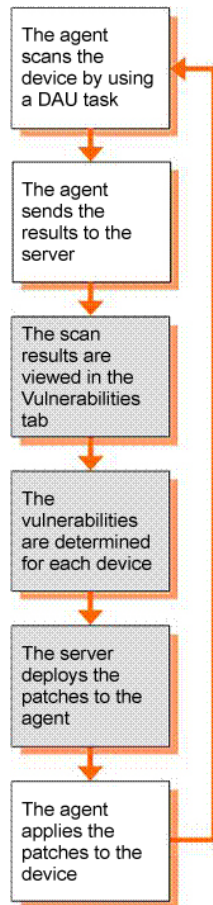
The ZENworks Patch Management Services feature stays current with the latest patches and fixes by regular communication with the ZENworks Patch Subscription Network through a secure connection. After the initial 60-day free trial period, the ZENworks Patch Management Services feature requires a paid subscription to continue its daily download of the latest vulnerability and patch 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 new patch and the list of devices that require deployment can be viewed easily along with the description and business impact. At this time, the administrator can choose to deploy the patch to devices or disregard the patch.

## 1.2 ZENworks Server and Adaptive Agent Process

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

**Figure 1-1** Process Map



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 Vulnerabilities section or in the Device section under the *Vulnerabilities* tab even if a workstation is disconnected from your network.

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

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

## 1.3 Features of ZENworks Patch Management Services

ZENworks Patch Management Services has the world's largest repository of patches, including more than 10,000 patches for major operating systems and applications. ZENworks Patch Management Services 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. ZENworks Patch Management Services continuously monitors end points to ensure that they get patched and stay patched.

With Novell ZENworks Patch Management Services, you can be sure that your systems are effectively patched and compliant for successful IT and regulatory audits. ZENworks Patch Management Services 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 remedy end points that do not meet defined patch levels—a key aspect of regulatory compliance. In addition, because many organizations need to demonstrate patch compliance, ZENworks Patch Management Services includes standard reports that document changes and demonstrate progress toward internal and external audit and compliance requirements.

The following table describes the salient features of ZENworks Patch Management Services:

**Table 1-1** *ZENworks Patch Management Services 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 (2008 feature).
Patch fingerprint accuracy	Ensures the highest level of accuracy in the detection of security vulnerabilities.
Multi-patch deployments	Delivers multiple patches to multiple computers in one distribution to increase IT productivity.

Feature	Description
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.

# Using Patch Management Services

# 2

Novell® ZENworks® Patch Management Services 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 Services:

- ♦ [Section 2.1, “Viewing Subscription Service Information,” on page 13](#)
- ♦ [Section 2.2, “Activating Your Paid Subscription or Viewing the Subscription Serial Number,” on page 16](#)
- ♦ [Section 2.3, “Configuring HTTP Proxy Details,” on page 19](#)
- ♦ [Section 2.4, “Configuring Subscription Download Details,” on page 22](#)

## 2.1 Viewing Subscription Service Information

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

The Configuration page appears as shown in the following figure:

Configuration	Registration	System Information	Asset Inventory	Asset Management	System Updates
Management Zone Settings					
Content					
Device Management					
Discovery and Deployment					
Event and Messaging					
Infrastructure Management					
Inventory					
Reporting Services					
Asset Management					
Patch Management Services					
Server Hierarchy					
Administrators					
Roles					
User Sources					
Licenses					
Credential Vault					

- 2 Click *Patch Management Services*.

Four links—*Subscription Service Information*, *Product Serial Number*, *Configure HTTPProxy*, and *Subscription Download*—are displayed:

Configuration	Registration	System Information	Asset Inventory	Asset Management	System Updates
Management Zone Settings					⌵
Content					⌵
Device Management					⌵
Discovery and Deployment					⌵
Event and Messaging					⌵
Infrastructure Management					⌵
Inventory					⌵
Reporting Services					⌵
Asset Management					⌵
Patch Management Services					⌵
Category	Description				Is Configured
<a href="#">Subscription Service Information</a>	View subscription log and update subscription settings				Yes
<a href="#">Product Serial Number</a>	Configure the subscription Serial Number.				No
<a href="#">Configure Http Proxy</a>	Configure HTTP Proxy for access to the Internet patch subscription				No
<a href="#">Subscription Download</a>	Configure subscription download options				No
Server Hierarchy					⌵
Administrators					⌵
Roles					⌵
User Sources					⌵

### 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/zcm-server

Service Running

Last Subscription Poll

3/16/08 10:39 PM

Subscription Replication Status

Complete

Subscription Host

novell.patchlink.com

Subscription Communication Interval(Every Day at)

03:30

Update Now

Subscription Service History

Action						
Type	Status	Start Date	End Date	Duration	Successful	
Vulnerabilities	Complete	3/16/08 10:39 PM	3/16/08 10:55 PM	00:16:19	true	
Licenses	Complete	3/16/08 10:39 PM	3/16/08 10:39 PM	00:00:00	false	
Bundles	Complete	3/16/08 11:23 PM	3/16/08 11:23 PM	00:00:00	true	

1 - 3 of 3

show 10 items

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:



You can choose the number of items to be displayed per page by clicking the *show items* drop-down list and selecting the desired number, 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 need to 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"> <li>◆ After the subscription service starts running, the <i>Start</i> button reads <i>Service Running</i>.</li> <li>◆ If there are multiple ZENworks Servers in your management zone, you can select any one of them to be the Patch Management Server. However, this must be decided only once per zone in this release.</li> </ul>
Last Subscription Poll	The date and time of the last successful update.
Subscription Replication Status	Latest status of the process of replication.
Subscription Host	The URL of the ZENworks Patch Subscription Network.
Subscription Communication Interval (Every Day at)	The frequency of ZENworks Server communication with the ZENworks Patch Subscription Network for retrieving updates.

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 ZENworks Patch Subscription Network and forces an immediate download of patch subscription
<i>Cancel</i>	Enables you to cancel the last action performed

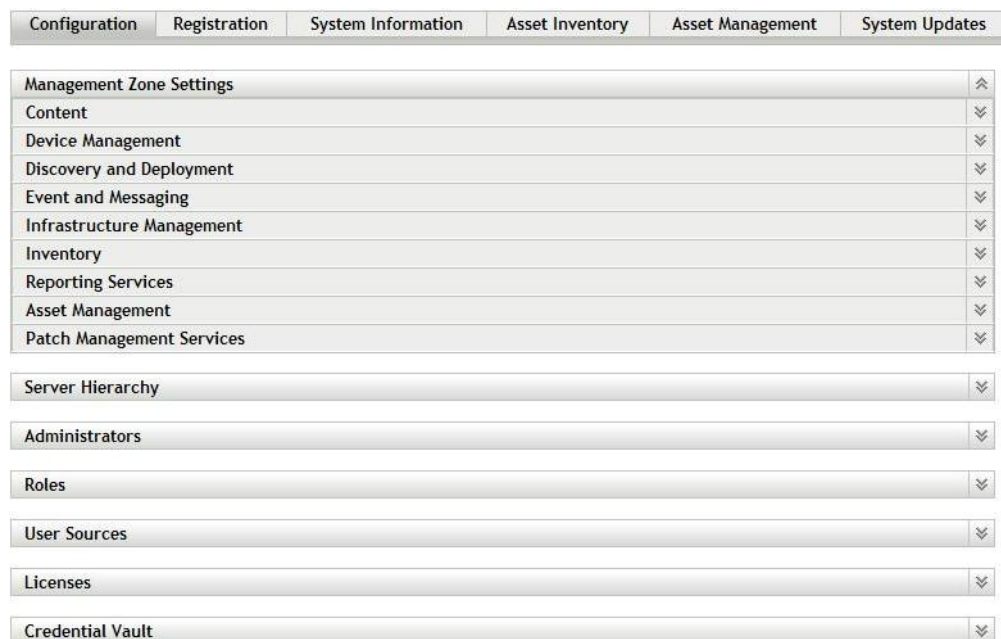
The *Subscription Service History* section displays the activity log of the subscription activities. The following table describes each item featured in this section.

Item	Definition
Type	Subscription type defined for your account: Vulnerability (Subscription Replication), Bundles (Subscription Replication), and Licenses.
Status	Status of replication. When replication begins, the status reads <i>In Progress</i> . When replication ends, the status reads <i>Completed</i> .  <b>NOTE:</b> 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.
Start Date	The date and time at which replication started.
End Date	The date and time at which replication ended.
Duration	The length of time for which replication has been going on.
Successful	Indicates whether the replication was successful or not. <i>True</i> indicates successful replication and <i>False</i> indicates incomplete or failed replication.

## 2.2 Activating Your Paid Subscription or Viewing the Subscription Serial Number

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

The Configuration page appears as shown in the following figure:



- 2 Click *Patch Management Services*.



Four links—*Subscription Service Information*, *Product Serial Number*, *Configure HTTPProxy*, and *Subscription Download*—are displayed:



### 3 Click the *Product Serial Number* link.

The Subscription Serial Number page appears:

Configuration > Product Serial Number

Product Serial Number

Configure the subscription Serial Number.

Product Serial Number

Serial Number

XXXXXXXX-XXXXXXX

Company Name

Email Address

Account Id

Total Non-Expired Licenses

Product Serial Number

Action ▾

Description	Status	Vendor	Expiration	Purchased
No items available.				

OK

Apply

Reset

Cancel

The Subscription Serial Number 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 in case it has expired. The page provides a summary of all subscription elements that are part of your patch management activities. This information is updated after each replication with the ZENworks Patch Management Subscription Service.

---

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

---

ZENworks Patch Management Services provides a 60-day free trial period. You need not enter a serial number unless you purchase the product or the 60-day free trial has expired.

- 1 Specify the subscription serial number, which is valid only for a 60-day trial.  
The *Product Serial Number* panel does not display any details because the product is in trial mode.
- 2 To continue using the patch management features of the ZENworks Control Center after your 60-day free trial has ended, you must enter a valid subscription serial number for ZENworks Patch Management Services along with the company name and e-mail address.
- 3 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.lumension.com/update>.

The ZENworks Patch Management Services 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>.

To download patches, you must provide Internet access to both [novell.lumension.com](http://novell.lumension.com) and [novell.cdn.lumension.com](http://novell.cdn.lumension.com) through the external firewall or proxy infrastructure.

You should use `nslookup` to discover the local IP address for your nearest content distribution node. For example, entering `nslookup novell.cdn.lumension.com` displays the local IP address for the content distribution node. Allow access to that specific local address through the firewall.

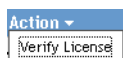
The following table describes each field on the Subscription Serial Number page.

**Table 2-1** ZENworks Subscription Serial Number Items

Item	Definition
<i>Serial Number</i>	ZENworks Patch Management Services license number (serial number).
<i>Company Name</i>	Name of the company that ZENworks Patch Management Services is registered to.
<i>Email Address</i>	E-mail address, which you can use for receiving alerts and for future communication.
<i>Account ID</i>	Key created by the ZENworks Server, which is passed to the ZENworks 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 from where the license was purchased.
<i>Expiration</i>	The date the license expires. Typically, licenses expire one calendar year from the date of purchase.
<i>Purchased</i>	The total number of licenses purchased with the product.

The ZENworks Patch Management Services serial number can be entered only once. After you have entered the serial number, you can verify the license by clicking *Action* on the Subscription Serial Number page and selecting *Verify License*. Automatic verification of the license happens every day with the replication process.

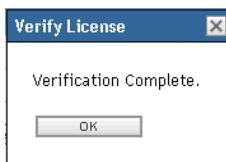
**Figure 2-1** Verify License option



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

The *Verify License* message box appears, as shown in the following figure:

**Figure 2-2** *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 Subscription Serial Number page:

**Table 2-2** *Buttons on the Subscription Serial Number Page*

Button	Action
<i>OK</i>	Enables you to go back to the <i>Configuration</i> 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

## 2.3 Configuring HTTP Proxy Details

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

The Configuration page appears as shown in the following figure:

Configuration	Registration	System Information	Asset Inventory	Asset Management	System Updates
Management Zone Settings					
Content					
Device Management					
Discovery and Deployment					
Event and Messaging					
Infrastructure Management					
Inventory					
Reporting Services					
Asset Management					
Patch Management Services					
Server Hierarchy					
Administrators					
Roles					
User Sources					
Licenses					
Credential Vault					

## 2 Click *Patch Management Services*.

Four links—*Subscription Service Information*, *Product Serial Number*, *Configure HTTPProxy*, and *Subscription Download*—are displayed:

Configuration	Registration	System Information	Asset Inventory	Asset Management	System Updates
Management Zone Settings					
Content					
Device Management					
Discovery and Deployment					
Event and Messaging					
Infrastructure Management					
Inventory					
Reporting Services					
Asset Management					
Patch Management Services					
Category	Description	Is Configured			
<a href="#">Subscription Service Information</a>	View subscription log and update subscription settings	Yes			
<a href="#">Product Serial Number</a>	Configure the subscription Serial Number.	No			
<a href="#">Configure Http Proxy</a>	Configure HTTP Proxy for access to the Internet patch subscription	No			
<a href="#">Subscription Download</a>	Configure subscription download options	No			
Server Hierarchy					
Administrators					
Roles					
User Sources					

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

**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 subscription. The HTTP proxy server allows ZENworks Patch Management Services to download 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 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.

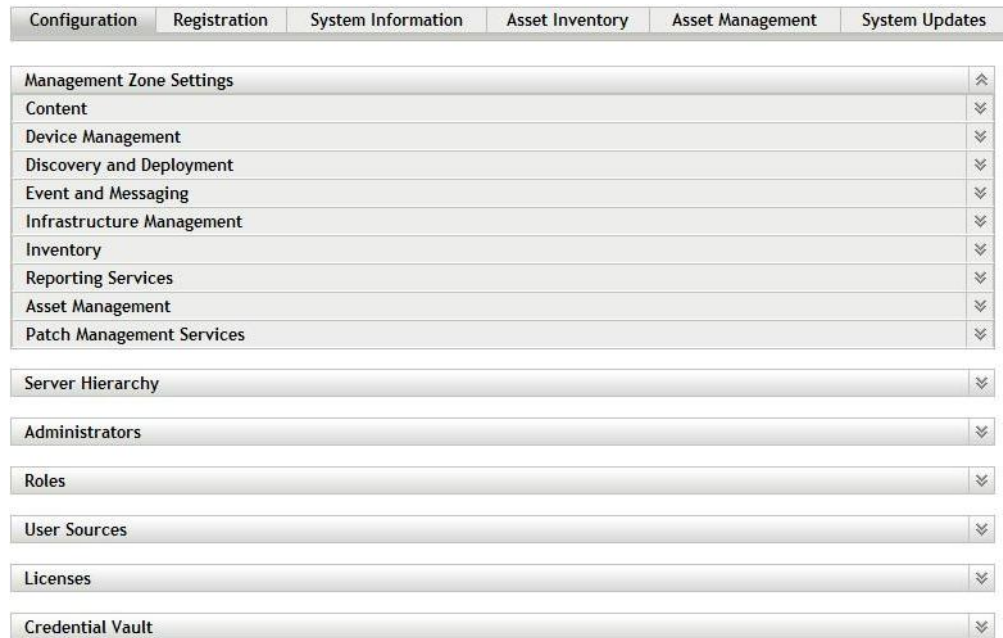
The following table describes the action of each button on the page:

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

## 2.4 Configuring Subscription Download Details

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

The Configuration page appears as shown in the following figure:



- 2 Click *Patch Management Services*.

Four links—*Subscription Service Information*, *Product Serial Number*, *Configure HTTPProxy*, and *Subscription Download*—are displayed:

Configuration	Registration	System Information	Asset Inventory	Asset Management	System Updates	
Management Zone Settings					⌵	
Content					⌵	
Device Management					⌵	
Discovery and Deployment					⌵	
Event and Messaging					⌵	
Infrastructure Management					⌵	
Inventory					⌵	
Reporting Services					⌵	
Asset Management					⌵	
Patch Management Services					⌵	
Category					Description	Is Configured
<a href="#">Subscription Service Information</a>					View subscription log and update subscription settings	Yes
<a href="#">Product Serial Number</a>					Configure the subscription Serial Number.	No
<a href="#">Configure Http Proxy</a>					Configure HTTP Proxy for access to the Internet patch subscription	No
<a href="#">Subscription Download</a>					Configure subscription download options	No
Server Hierarchy					⌵	
Administrators					⌵	
Roles					⌵	
User Sources					⌵	

### 3 Click the *Subscription Download* link.

The Subscription Download Options page appears:

[Configuration](#) > [Subscription Download](#)

Subscription Download

Configure subscription download options

Subscription Download

Choose your language options

For Vista all languages are supported. These languages are for Operating Systems prior to Vista and other non Microsoft components. For the best performance results select only the languages used by your organization.

☒ English
 ☐ Portuguese (Brazil)
 ☐ French
 ☐ Italian
 ☐ German

☐ Japanese
 ☐ Korean
 ☐ Traditional Chinese
 ☐ Simplified Chinese
 ☐ Hong Kong Chinese

☐ Spanish
 ☐ Dutch
 ☐ Swedish
 ☐ Finnish
 ☐ Czech

☐ Danish
 ☐ Hungarian
 ☐ Norwegian
 ☐ Russian
 ☐

Select the option below to combine all languages into each Discover Applicable Updates Assignment. (Not Recommended)

☐ Mix Multiple Languages

The Subscription Download Options page allows you to configure the subscription download options for the ZENworks Primary 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 replication occurs, only those patches specific to the languages are downloaded, thereby saving time and duration of replication and disk space on your ZENworks Primary Server.

---

**NOTE:** Novell does not recommend the selection of all languages because each language can represent hundreds of patches. Downloading unwanted languages may result in thousands of useless vulnerability definitions within your ZENworks Primary Server database that would then need to be disabled in the *Vulnerabilities* tab.

---

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

Item	Description
<i>Choose 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).

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



# Using Vulnerabilities

# 3

The Vulnerabilities page is where the majority of patch management activities are performed. This page lists all patch-related vulnerabilities across all systems registered to the ZENworks® Server. The page displays the name, description, impact, and statistics of the vulnerabilities.

The following sections provide more information on the Vulnerabilities page:

- ♦ [Section 3.1, “Viewing Vulnerabilities,” on page 25](#)
- ♦ [Section 3.2, “Using the Vulnerabilities Page,” on page 26](#)

## 3.1 Viewing Vulnerabilities

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

The Vulnerabilities page displays a complete list of all known patches and updates reported by various software vendors. After they are reported and analyzed, the vulnerabilities are registered for distribution to your ZENworks Server through the ZENworks Patch Subscription Network. The ZENworks Adaptive Agent installed on each device checks for known vulnerabilities. A bundle called Discover Applicable Updates (DAU) is then run on each device on a daily basis to scan for known vulnerabilities. This task returns the results that are then displayed on the Vulnerabilities page. The results are presented in a table of vulnerability patch status. The total number of vulnerabilities is displayed below the table in the bottom left corner.

To view the vulnerabilities in ZENworks Patch Management Services, click the *Vulnerabilities* tab on the left panel, as shown in the following figure:

**Figure 3-1** *Vulnerabilities Tab*



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

Action	Vulnerability Name	Impact	Patched	Not Patched
<input type="checkbox"/>	<a href="#">Internet Explorer 6.0 Service Pack 1 (Rev 2)</a>	Software Installer	<a href="#">1</a>	<a href="#">0</a>
<input type="checkbox"/>	<a href="#">Internet Explorer 7 Blocker Toolkit (SEE NOTES)</a>	Software Installer	<a href="#">0</a>	<a href="#">2</a>
<input type="checkbox"/>	<a href="#">Internet Explorer 7.0 (SEE NOTES)</a>	Software Installer	<a href="#">1</a>	<a href="#">1</a>
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 6 patch release R65 for IE</a>	Critical	<a href="#">1</a>	<a href="#">0</a>
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 7.0.r19 for IE</a>	Software Installer	<a href="#">0</a>	<a href="#">2</a>
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 7.0.r61 for IE</a>	Software Installer	<a href="#">0</a>	<a href="#">2</a>
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 7.0.r63 for IE</a>	Software Installer	<a href="#">0</a>	<a href="#">2</a>
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 8.0.r22 for IE</a>	Software Installer	<a href="#">0</a>	<a href="#">2</a>
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 9.0.r28 for IE</a>	Software Installer	<a href="#">0</a>	<a href="#">2</a>
<input type="checkbox"/>	<a href="#">Microsoft .NET Framework 2.0 SP1 (See Notes)</a>	Critical	<a href="#">0</a>	<a href="#">2</a>

1 - 10 of 210 show 10 items

**Vulnerability Information**

**Search**

Vulnerability Name

Search Reset

**Status**

☒ Patched

☒ Not Patched

☐ Not Applicable

☒ Include Disabled

**Impact**

☒ Critical

☒ Recommended

☒ Informational

☒ Software Installers

## 3.2 Using the Vulnerabilities Page

The following sections provide more information on the Vulnerabilities page:

- ♦ [Section 3.2.1, “Vulnerabilities,” on page 26](#)
- ♦ [Section 3.2.2, “Vulnerability Information,” on page 31](#)
- ♦ [Section 3.2.3, “Searching Vulnerability,” on page 32](#)
- ♦ [Section 3.2.4, “Vulnerability Tasks,” on page 33](#)

### 3.2.1 Vulnerabilities

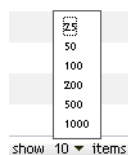
This section of the Vulnerabilities page provides the following information about vulnerabilities:

- ♦ Name of the vulnerability
- ♦ Total number of vulnerabilities available
- ♦ Impact of the vulnerability
- ♦ Statistics of the vulnerability

This section features the *Action* menu that enables you to perform any of the four actions related to vulnerabilities, namely *Deploy Remediation*, *Enable*, *Disable*, and *Update Cache*. For more information on these actions, see [“Action Menu Items” on page 30](#).

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 3-2** Show Items drop-down List



The following sections explain the information on the Vulnerabilities page:

- ♦ “Vulnerability Name” on page 27
- ♦ “Total Vulnerabilities Available” on page 27
- ♦ “Vulnerability Impacts” on page 28
- ♦ “Vulnerability Statistics” on page 29
- ♦ “Action Menu Items” on page 30

### Vulnerability Name

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

An example of a vulnerability name is shown as follows. In the following vulnerability name, Adobe is the vendor, Acrobat Reader is the application, and 6.0.6 is the version information.

**Figure 3-3** Example of a Vulnerability Name

[Adobe Acrobat Reader 6.0.6 Update](#)

---

#### NOTE:

- ♦ 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 expected results.
- 

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

### Total Vulnerabilities Available

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

**Figure 3-4** *Show Items Drop-down List*

1 - 10 of 979

## Vulnerability Impacts

A type of the vulnerability defined on the basis of the release date of the vulnerability; the type can be Critical, Recommended, Informational, or Software Installers. Each impact is described as follows.

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

Novell ZENworks Patch Management impact terminology for its patch subscription closely follows the vendor impact terminology for vulnerability criticality. Each operating system has a vendor-specific impact rating and that impact is mapped to a Novell rating as described in this section. Novell ZENworks 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’s and Microsoft’s patch classification terminology:

**Table 3-1** *Novell and Microsoft Patch Impact Mapping*

Novell Patch Impacts	Windows	Other
Critical	Critical Security	Example: AV Updates (Critical-01)
	Important	
	Moderate	
	Example: Service Packs (Critical-01)	
Recommended	Recommended	NA
	Low	
	Example: Microsoft Outlook 2003 Junk E-mail Filter Update	

Novell Patch Impacts	Windows	Other
Software Installers	Software Distribution Example: Microsoft Windows Malicious Software Removal Tool (Virus Removal)	Adobe* 8.1 software installer
Informational	NA	NA

Source: Lumension Security




## Vulnerability Statistics




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

- ♦ **Patched:** This column displays a link indicating the total number of devices to which the corresponding vulnerability has been applied or patched.  
  
Clicking this link displays a page that lists the patched devices. You can uninstall the patch by using the *Remove* option in the *Action* menu.
- ♦ **Not Patched:** This column displays a link indicating the total number of devices to which the corresponding vulnerability has not been applied or patched.  
  
Clicking this link displays a page that lists these devices. You can deploy the patch to these devices by using the *Deploy Remediation* option in the *Action* menu.

The vulnerabilities shown on the Vulnerabilities page have different icons next to their names, indicating their current status. The following table describes the significance of the icons that appear against each vulnerability:

**Table 3-2** Vulnerability Icons

Vulnerability Icon	Significance
	Indicates the vulnerabilities that are disabled.  <b>NOTE:</b> Disabled vulnerabilities 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 vulnerability has been brought down from the ZENworks Patch Subscription Network. Therefore, this icon represents the vulnerabilities that are not cached.
	Indicates that a download process for the bundles associated with the selected vulnerability is pending.

Vulnerability Icon	Significance
	Indicates that a download process for the bundles associated with the selected vulnerability has started. This process caches those bundles on your ZENworks Server.
	Indicates that the fingerprints and remediation bundles necessary to address the vulnerability have been cached into the system. Therefore, this icon represents the vulnerabilities that are cached and ready for deployment.
	Indicates that an error has occurred while trying to download the bundle associated with the selected vulnerability.

**NOTE:** If you choose a vulnerability that does not have cached remediation bundles, the deployment process might fail until the cache download is complete. You should download the files from the patch subscription and they must be packaged by ZENworks Configuration Management. Then the icon turns blue. To initiate an immediate download of these packages, select the *Update Cache* option from the *Action* menu.

## Action Menu Items

The *Vulnerabilities* section also features an *Action* menu, which enables you to perform one of four actions on the vulnerabilities listed on the page. The following figure shows the four options in the *Action* menu.

**Figure 3-5** Action Menu Items



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

- ♦ **Deploy Remediation:** Enables you to deploy a patch. To use this option, select the check boxes for the vulnerabilities you want to deploy and select *Deploy Remediation* from the *Action* menu options to open the Deploy Remediation Wizard. For more information, see [Chapter 4, “Using the Deploy Remediation Wizard,” on page 37](#).
- ♦ **Enable:** Allows you to enable a disabled vulnerability.
- ♦ **Disable:** Enables you to disable a vulnerability. To use this option, select the check box for the desired vulnerability and select *Disable*. The selected vulnerability is removed from the list.



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

- ♦ **Update Cache:** Initiates a download process for the bundles associated with the selected vulnerability and caches those bundles on your ZENworks Server.

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

To use this option:

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

The vulnerability icon changes to . While the download is in progress, the icon changes to . When the caching is complete, the color of the vulnerability icon changes to blue.

This indicates that the patch remediation is ready to be deployed.

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

**Figure 3-6** *Vulnerability Name Column*

Vulnerability Name ▾

---

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

---

## 3.2.2 Vulnerability Information

You can view detailed information of a selected vulnerability in the *Vulnerability Information* section. Clicking the name of a vulnerability displays the details of that vulnerability.

For example, if you select the vulnerability called *(EC) Microsoft.NET Framework 2.0 Service Pack 1 (KB110806) (x86)* from the list of vulnerabilities, the *Vulnerability Information* section displays the result of a vulnerability analysis for the selected vulnerability, as shown in the following figure:

**Figure 3-7** *Vulnerability Information for a Selected Vulnerability*

Vulnerability Information	
Property Name	Details
Name	Adobe Acrobat Reader 7.0.1 Update
Type	Unknown
Remediation Bundles	-1
Impact	Critical
Distribution Package Status	Active
Status	Enabled
Vendor	Adobe Systems, Inc
Modified On	
Released On	
Vulnerability Results	Unknown
Vendor Product ID	AdbeRdr701
Description	This multilingual Adobe Reader 7.0.1 update addresses sev can be applied to Adobe Reader 7.0 in any of the 15 primar that all users of Adobe Reader 7.0 apply this update as a pr improved security and support for hyperlinks to PDF files in issues associated with the Swedish language version of Rea files that contain 3D content generated in 3D CAD or model

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

**Table 3-3** *Property Names in the Vulnerability Information Section*

Property Name	Definition
Name	The name of the vulnerability.
Impact	The impact of the vulnerability as determined by Novell. See <a href="#">Section , "Vulnerability Impacts," on page 28</a> .
Status	Status of the vulnerability. It can be <i>Enabled</i> or <i>Disabled</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 vulnerability; it includes the advantages of deploying the vulnerability and the prerequisites for deployment.

### 3.2.3 Searching Vulnerability

The *Search* section on the Vulnerabilities page offers extensive search and data filtering options that allow you to search for specific vulnerabilities and filter result sets based on the status and impact of the vulnerabilities. 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 3-8** *Search Section on the Vulnerabilities Page*

The screenshot shows a web interface for searching vulnerabilities. At the top is a search bar with the label 'Vulnerability Name' and a magnifying glass icon. Below the search bar are two buttons: 'Search' and 'Reset'. Underneath the search bar are two sections of filters. The first section is labeled 'Status' and contains four checkboxes: 'Patched', 'Not Patched', 'Not Applicable', and 'Include Disabled'. The second section is labeled 'Impact' and contains four checkboxes: 'Critical', 'Recommended', 'Informational', and 'Software Installers'.

To search for a vulnerability:

- 1 Type all or part of the vulnerability name in the *Vulnerability Name* text box.
- 2 Select the desired check box under *Status* and *Impact*.
- 3 Click *Search*.



---

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

---

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

**Table 3-4** *Status Filters in Search*

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

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

**Table 3-5** *Impact Filters in Search*

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

## 3.2.4 Vulnerability Tasks

The following sections provide more information on the different options in the *Vulnerabilities Tasks* pane:

- ♦ [“Deploy Remediation” on page 33](#)
- ♦ [“Export Vulnerabilities” on page 34](#)
- ♦ [“View Vulnerability” on page 34](#)

### Deploy Remediation

This option enables you to deploy a patch. To use this option, select the check boxes for the vulnerabilities you want to deploy and click the *Deploy Remediation* link to open the Deploy Remediation Wizard. For more information, see [Chapter 4, “Using the Deploy Remediation Wizard,” on page 37](#).

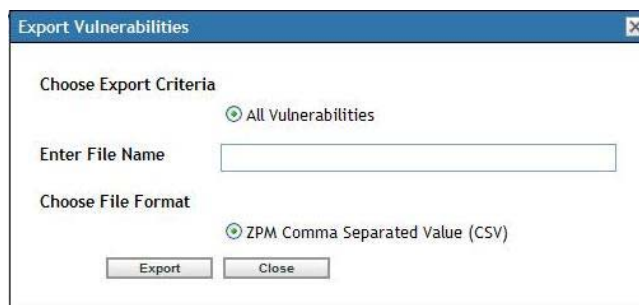
## Export Vulnerabilities

Details such as the status and impact of all vulnerabilities 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 Vulnerabilities* link in the left pane.

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

- 2 In the *Export Vulnerabilities* 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 `ZPMVulnerabilitiesList.csv` by default.
- ♦ **Cancel:** The report is not created or saved.

	A	B	C	D	E
1	#Status	Vulnerability Name	Impact	Patched Count	Not Patched Count
2	Active	MS04-027 (EC) Security Update for Office XP: WordPerfect 5.x Converter (K	Critical	0	0
3	In Active	MS05-005 (EC) Security Update for Office XP (KB873352)	Critical	0	0
4	Active	MS05-021 (EC) Security Update for Exchange 2000 Server Service Pack 3 (	Critical	0	0
5	Active	MS05-021 (EC) Security Update for Exchange Server 2003 (KB894549)	Critical	0	0
6	Active	MS05-021 (EC) Security Update for Exchange Server 2003 Service Pack 1 (	Critical	0	0
7	Active	MS05-048 (EC) Security Update for Exchange 2000 Server (KB906780)	Critical	0	0
8	Active	MS06-003 (EC) Security Update for Exchange 2000 Server (KB894689)	Critical	0	0
9	In Active	MS06-003 (EC) Security Update for Office 2003 Multilingual User Interface P	Critical	0	0
10	In Active	MS06-003 (EC) Security Update for Office XP Multilingual User Interface Pac	Critical	0	0
11	In Active	MS06-009 (EC) Security Update for Office 2003 Multilingual User Interface P	Critical	0	0
12	Active	MS06-009 (EC) Security Update for Office 2003 Proofing Tools (KB905645)	Critical	0	0
13	Active	MS06-012 (EC) Security Update for Office XP Multilingual User Interface Pac	Critical	0	0
14	Active	MS06-019 (EC) Security Update for Exchange 2000 Server Service Pack 3 (	Critical	0	0
15	Active	MS06-019 (EC) Security Update for Exchange Server 2003 Service Pack 1 (	Critical	0	0
16	Active	MS06-019 (EC) Security Update for Exchange Server 2003 Service Pack 2 (	Critical	0	0
17	Active	MS06-029 (EC) Security Update for Exchange 2000 Server Service Pack 3 (	Critical	0	0
18	Active	MS06-029 (EC) Security Update for Exchange Server 2003 Service Pack 1 (	Critical	0	0
19	Active	MS06-029 (EC) Security Update for Exchange Server 2003 Service Pack 2 (	Critical	0	0
20	Active	MS06-033 (EC) Security Update for Microsoft .NET Framework, Version 2.0	Critical	0	0
21	In Active	MS06-038 (EC) Security Update for Office 2003 (KB917151)	Critical	0	0
22	In Active	MS06-038 (EC) Security Update for Office XP (KB917150)	Critical	0	0

## View Vulnerability

Selecting a vulnerability and clicking the *View Vulnerability* link displays a page that provides details for that vulnerability. The page provides three tabs as follows:

- ♦ **Patched:** Click this tab to view the patched devices for that vulnerability.

- ♦ **Not Patched:** Click this tab to view all the devices that are not patched for that vulnerability.
- ♦ **Information:** Click this tab to view detailed information of that vulnerability.



# 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 *Vulnerabilities* tab.

---

**NOTE:** In the Deploy Remediation Wizard, if you select multiple vulnerabilities, the wizard automatically selects all the applicable devices and packages. If any device is selected, the wizard automatically selects all vulnerabilities that are applicable for that device. If a group is selected, the wizard includes all vulnerabilities applicable for the devices in that particular group.

---

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

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



---

**NOTE:** Disabling a vulnerability also disables all the bundles associated with it. Although you can deploy a disabled vulnerability to a device, the deployment does not occur because the associated bundle is disabled.

---

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

- ♦ [Section 4.1, “Confirm Devices,” on page 37](#)
- ♦ [Section 4.2, “License Agreement,” on page 39](#)
- ♦ [Section 4.3, “Remediation Schedule,” on page 40](#)
- ♦ [Section 4.4, “Remediation Options,” on page 49](#)
- ♦ [Section 4.5, “Advanced Remediation Options,” on page 50](#)
- ♦ [Section 4.6, “Deployment Order and Behavior,” on page 53](#)
- ♦ [Section 4.7, “Notification and Reboot Options,” on page 54](#)
- ♦ [Section 4.8, “Deployment Summary,” on page 56](#)

## 4.1 Confirm Devices

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

The following sections provide more information on the other steps of the wizard:

- ◆ [Section 4.2, “License Agreement,” on page 39](#)
- ◆ [Section 4.3, “Remediation Schedule,” on page 40](#)
- ◆ [Section 4.4, “Remediation Options,” on page 49](#)
- ◆ [Section 4.5, “Advanced Remediation Options,” on page 50](#)
- ◆ [Section 4.6, “Deployment Order and Behavior,” on page 53](#)
- ◆ [Section 4.7, “Notification and Reboot Options,” on page 54](#)
- ◆ [Section 4.8, “Deployment Summary,” on page 56](#)

**Figure 4-1** *Confirm Devices Page*

The following table describes the column headings on the Confirm Devices page.

**Table 4-1** *Confirm Devices Page Column Headings*

Column Heading	Description
<i>Device Name</i>	The name of the device registered with ZENworks® Patch Management Services (to which the vulnerability is to be deployed).
<i>Status</i>	The status of the device. The status can be offline or online.
<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.

The total number of devices to which the selected vulnerability would be deployed is displayed on the page. In the following example, the total number of devices is five.

**Figure 4-2** *Total Number of Devices*

1 - 5 of 5

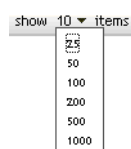
You can sort the devices in ascending and descending alphabetical order. To sort, click the arrow in the *Device Name* column heading as shown in the following figure:

**Figure 4-3** *Sorting Devices*



You can choose the total number of items to be displayed on the page by using the *show items* drop-down list, as shown in the following figure:

**Figure 4-4** *Show Items*



By default, all the devices are selected for deployment. Deselect the devices to which you do not want to deploy the vulnerability and click the *Next* button to open the License Agreement page.

## 4.2 License Agreement

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

The following sections provide more information on the other steps of the wizard:

- ♦ [Section 4.1, “Confirm Devices,” on page 37](#)
- ♦ [Section 4.3, “Remediation Schedule,” on page 40](#)
- ♦ [Section 4.4, “Remediation Options,” on page 49](#)
- ♦ [Section 4.5, “Advanced Remediation Options,” on page 50](#)
- ♦ [Section 4.6, “Deployment Order and Behavior,” on page 53](#)
- ♦ [Section 4.7, “Notification and Reboot Options,” on page 54](#)
- ♦ [Section 4.8, “Deployment Summary,” on page 56](#)

**Figure 4-5** *License Agreement Page*



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

---

**NOTE:** Only those vulnerabilities are deployed for which you have accepted license agreements. At least one license agreement must be accepted for the deployment 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.

## 4.3 Remediation Schedule

The Remediation Schedule page allows you to select the schedule and manner of deployment of remediation to your selected devices. Setting various deployment options for a selected vulnerability is the third step in scheduling a deployment for a selected vulnerability.

The following sections provide more information on the other steps of the wizard:

- ♦ [Section 4.1, “Confirm Devices,” on page 37](#)
- ♦ [Section 4.2, “License Agreement,” on page 39](#)
- ♦ [Section 4.4, “Remediation Options,” on page 49](#)
- ♦ [Section 4.5, “Advanced Remediation Options,” on page 50](#)
- ♦ [Section 4.6, “Deployment Order and Behavior,” on page 53](#)
- ♦ [Section 4.7, “Notification and Reboot Options,” on page 54](#)
- ♦ [Section 4.8, “Deployment Summary,” on page 56](#)

**Figure 4-6** Remediation Schedule Page

Devices > Servers > Vulnerabilities

Vulnerabilities

Step 3: Remediation Schedule

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

Schedule Type:

- Date Specific
- Date Specific
- Recurring
- Event

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

- ♦ 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 selected time, repeats the deployment every day/week/month, and if defined, ends on a specific date.
- ♦ Select *Event* to trigger the scheduled deployment when a particular event (chosen from a given list of events) takes place.



---

**TIP:** For an immediate installation of a patch, select the *Recurring* schedule type, and choose the *When a device is refreshed* option. This forces the installation of the patches during the next Device Refresh Schedule (the frequency of communication between the ZENworks Adaptive Agent and the ZENworks Server). This option is typically used when testing a patch. For remediation to a group of devices, select the *Date Specific* schedule type.

---

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 4.3.1, “Remediation Schedule – Date Specific,” on page 41](#)
- ♦ [Section 4.3.2, “Remediation Schedule – Recurring,” on page 43](#)
- ♦ [Section 4.3.3, “Remediation Schedule – Event,” on page 48](#)

## 4.3.1 Remediation Schedule – Date Specific

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

**Figure 4-7** Remediation Schedule Page for the Date Specific Schedule Type

Devices > Servers > Vulnerabilities

Vulnerabilities

Step 3: Remediation Schedule

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

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 am End Time: 1 : 00 am  
☐ Use Coordinated Universal Time ( Current UTC 7:24 AM )

<< Back Next >> Cancel

In this page, you can set the following options of deployment:

- ♦ **Start Date:** This option enables you to pick the date on which you want 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:** Selecting this check box ensures that the deployment starts on a selected date at selected time and repeats every year and, if defined, ends on a specific date.
- ♦ **Process immediately if device unable to execute on schedule:** Selecting this check box ensures that the deployment starts immediately after it has failed to execute as per the specified schedule.
- ♦ **Select when schedule execution should start:** There are two options that enable you to select the start time of the schedule execution: *Start immediately at Start Time* and *Start at a random time between Start Time and End Times*.
  - ♦ *Start immediately at Start Time:* Selecting this option deactivates the *End Time* panel and starts the deployment at the start time specified. In this option, you set the start time in the start time panel.

Start Time: 1 :00 am

- ♦ *Start at a random time between Start Time and End Times:* Selecting this option 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 *End Time* panel appears as follows:

End Time: 1 :00 am

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 for 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 deployment at the local time.

## 4.3.2 Remediation Schedule – Recurring

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

**Figure 4-8** Remediation Schedule Page for the Recurring Schedule Type

The screenshot shows the 'Remediation Schedule' page for the 'Recurring' schedule type. At the top, 'Schedule Type:' is set to 'Recurring'. Below this, there are four radio button options for scheduling: 'When a device is refreshed', 'Days of the week', 'Monthly', and 'Fixed Interval'. The 'When a device is refreshed' option is selected. It includes a checkbox for 'Delay execution after refresh:' with input fields for 0 Days, 0 Hours, and 0 Minutes. The 'Days of the week' option shows a grid for Sun through Sat, all of which are currently unchecked. It also has a 'Start Time' field set to 1:00 am and a 'More Options' link. The 'Monthly' option has three sub-options: 'Day of the month:' (set to 1), 'Last day of the month', and 'First' (set to Sunday). It also has a 'Start Time' field set to 1:00 am and a 'More Options' link. The 'Fixed Interval' option has input fields for 0 Months, 0 Weeks, 0 Days, 0 Hours, and 0 Minutes. It also has a 'Start Date' field set to 3/17/08 and a 'Start Time' field set to 1:00 am, along with a 'More Options' link. At the bottom of the page, there are three buttons: '<< Back', 'Next >>', and '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 bundle assignment.
- 2 Click *Options* to open the *Install Options* window.
- 3 Select the *Install always* button 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 44
- ♦ “Days of the week” on page 45
- ♦ “Monthly” on page 46
- ♦ “Fixed” on page 47

## 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 by which you require delaying the deployment.

**Figure 4-9** *Delay Execution After Refresh Check Box*

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

---

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

---

## Days of the week

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

**Figure 4-10** Weekly Deployment Options - Default

The screenshot shows a panel titled "Days of the week" with a sub-header "\*". Below this is a row of seven checkboxes corresponding to the days of the week: Sun, Mon, Tue, Wed, Thu, Fri, and Sat. All checkboxes are currently unchecked. Below the checkboxes is a "Start Time" field with three dropdown menus: the first shows "1", the second shows ":00", and the third shows "am". At the bottom of the panel is a link labeled "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.

**Figure 4-11** Weekly Deployment Options - All

This screenshot shows the same "Days of the week" panel as Figure 4-10, but with the "More Options" link expanded. The "Start Time" field remains at "1 :00 am". Below the "Start Time" field is a link labeled "Hide Options". Underneath this link are four unchecked checkboxes with the following labels: "Process immediately if device unable to execute on schedule", "Use Coordinated Universal Time ( Current UTC 7:03 AM )", "Start at a random time between Start and End Times", and "Restrict schedule execution to the following date range:". Below the "Start at a random time..." checkbox is an "End Time" field with three dropdown menus showing "1", ":00", and "am". Below the "Restrict schedule execution..." checkbox are two date fields: "Start Date" and "End Date", both showing "3/17/08". Each date field has a calendar icon to its right.

Selecting the *Use Coordinated Universal Time* check box enables you to schedule the deployment for all agents 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 will schedule the deployment at the 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 and 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 4-12** Monthly Deployment Options – Default

The screenshot shows the 'Monthly' deployment options interface. It includes three radio buttons: 'Day of the month' (selected), 'Last day of the month', and 'Particular days of the month'. The 'Day of the month' option has a text input field with the value '1'. The 'Particular days of the month' option has two dropdown menus, the first set to 'First' and the second to 'Sunday', followed by a plus icon. Below these is a 'Start Time' section with dropdowns for hour (1), minute (:00), and period (am). A 'More Options' link is at the bottom.


- ♦ In the *Monthly* deployment option, you can specify the following:
  - ♦ **Days of the month:** This option 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:** This option enables you to schedule the deployment on the last day of the month.
  - ♦ **Particular days of the month:** This option 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 and the valid options for the weekday are Sunday through Saturday. To select one particular day of the month, use the drop-down arrows. An example is shown as follows.

This screenshot shows the 'Particular days of the month' selection interface. It features a radio button, a dropdown menu set to 'Second', another dropdown menu set to 'Sunday', and a plus icon.

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

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

---


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

---

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

This screenshot shows the 'Monthly' deployment options interface with the 'More Options' section expanded. It includes the same radio buttons and 'Start Time' section as the previous figure. Below the 'More Options' link, there are four checkboxes: 'Process immediately if device unable to execute on schedule', 'Use Coordinated Universal Time ( Current UTC 7:03 AM )', 'Start at a random time between Start and End Times', and 'Restrict schedule execution to the following date range:'. The 'End Time' field is set to 1:00 am. The 'Restrict schedule execution' section has 'Start Date' and 'End Date' both set to 3/17/08.

---

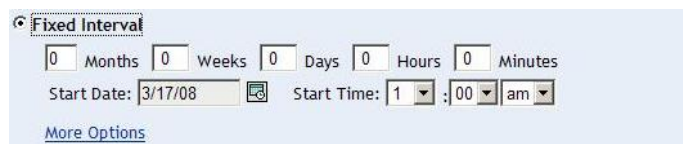
**NOTE:** The option *Restrict schedule execution to the following date range* enables you to schedule a recurring deployment at the selected time and repeat the deployment on the days specified, and if defined, end on the specific time. This option also enables you to restrict the deployment to the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

---

## Fixed

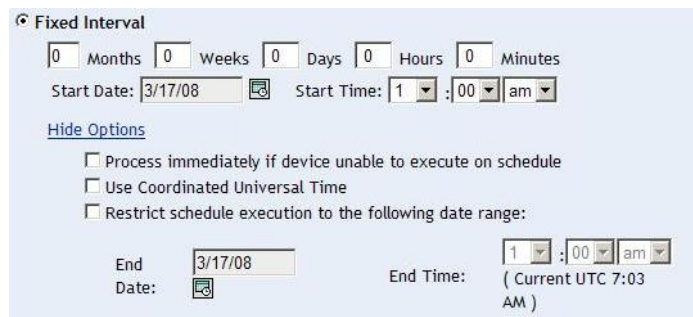
This option enables you to schedule a recurring deployment that runs after a fixed duration on a regular basis. You can choose the number of months, weeks, days, hours, and minutes of the interval and the start date for the deployment schedule, as shown in the following figure.

**Figure 4-13** Fixed Interval Deployment Options - Default



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 4-14** Fixed Interval Deployment Options - All



### 4.3.3 Remediation Schedule – Event

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

**Figure 4-15** Remediation Schedule Page for the Event Schedule Type

Schedule Type:  
Event

Select the event that this schedule should be triggered on:

- ☐ User Login
- ☐ User Logout
- ☐ Device Boot
- ☐ On Device Lock
- ☐ On Device Unlock
- ☐ ZENworks - Login
- ☐ ZENworks - Logout
- ☐ Device Connecting to Network (Windows Only)

<< Back    Next >>    Cancel

The Remediation Schedule page for the *Event* schedule type features a list of events to select so that when the selected event occurs, the deployment is executed.

The following table describes the result of selecting each event featured in the Remediation Schedule page:

**Table 4-2** Events that Can Trigger Remediation

Event	Action
User Login	Deployment remediation occurs whenever the user logs into the device.
User Logout	Deployment remediation occurs whenever the user logs out of the device.
Device Boot	Deployment remediation occurs whenever the device boots.
On Device Lock	Deployment remediation occurs whenever the user locks the device.
On Device Unlock	Deployment remediation occurs whenever the user unlocks the device.
ZENworks – Login	Deployment remediation occurs whenever the user logs into the ZENworks user source account. This option is not applicable if no user sources are configured.
ZENworks – Logout	Deployment remediation occurs whenever the user logs out of the ZENworks user source account. This option is not applicable if no user sources are configured.
Device Connecting to Network (Windows Only)	Deployment remediation occurs whenever the device obtains access to the network.

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.



---

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

---

## 4.4 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 vulnerability is the fourth step in scheduling a deployment for a selected vulnerability.

---

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

---

The following sections provide more information on the other steps of the wizard:

- ♦ [Section 4.1, “Confirm Devices,” on page 37](#)
- ♦ [Section 4.2, “License Agreement,” on page 39](#)
- ♦ [Section 4.3, “Remediation Schedule,” on page 40](#)
- ♦ [Section 4.5, “Advanced Remediation Options,” on page 50](#)
- ♦ [Section 4.6, “Deployment Order and Behavior,” on page 53](#)
- ♦ [Section 4.7, “Notification and Reboot Options,” on page 54](#)
- ♦ [Section 4.8, “Deployment Summary,” on page 56](#)

**Figure 4-16** Remediation Options Page

Devices > Servers > Vulnerabilities

Vulnerabilities

Step 4: Remediation Options

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

☐ Quiet(Auto QChain With Automatic Reboot)

☒ Default(Auto QChain With Manual Reboot)

☐ Advanced(Standard - Set Individually)

<< Back   Next >>   Cancel

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

**Table 4-3** Functionalities of the Remediation Options

Remediation Option	Functionality
Quiet (Auto QChain With Automatic Reboot)	Automatically sets all possible vulnerabilities to deploy with QChain enabled. All necessary reboots are performed automatically.
Default (Auto QChain With Manual Reboot)	Automatically sets all possible vulnerabilities to deploy with QChain enabled. When a reboot is required, the agent remains in a dirty state until you perform a reboot.

Remediation Option	Functionality
Advanced (Standard - Set Individually)	Allows the administrator to set the patch deployment flags as desired, using the default QChain and reboot settings defined for each vulnerability.

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.

## 4.5 Advanced Remediation Options

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

The following sections provide more information on the other steps of the wizard:

- ♦ [Section 4.1, “Confirm Devices,” on page 37](#)
- ♦ [Section 4.2, “License Agreement,” on page 39](#)
- ♦ [Section 4.3, “Remediation Schedule,” on page 40](#)
- ♦ [Section 4.4, “Remediation Options,” on page 49](#)
- ♦ [Section 4.6, “Deployment Order and Behavior,” on page 53](#)
- ♦ [Section 4.7, “Notification and Reboot Options,” on page 54](#)
- ♦ [Section 4.8, “Deployment Summary,” on page 56](#)

**Figure 4-17** Advanced Remediation Options Page

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

**Vulnerabilities**

Step 5: Advanced Remediation Options











Select the appropriate patch flags for each remediation. Please refer to the online help for more information.












Vulnerability Name								
(EC) Microsoft .NET Framework 2.0 Service Pack 1 (KB110806) (x86)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(EC) Windows Malicious Software Removal Tool - May 2008 (KB890830)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
MS05-026 (EC) Security Update for Windows Server 2003 (KB896358)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



1 - 3 of 3 show 10 ▼ items

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

**Table 4-4** Functionalities of the Advanced Remediations Options Page

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

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

Icon	Behavior Functionality
	Performs the system reconfigure task following the deployment.
(Reconfigure)	
	Does not perform the system reconfigure task following the deployment.
(Do Not Reconfigure)	

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.

## 4.6 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 vulnerability is the sixth step in scheduling a deployment for a selected vulnerability.


The following sections provide more information on the other steps of the wizard:

- ♦ [Section 4.1, “Confirm Devices,” on page 37](#)
- ♦ [Section 4.2, “License Agreement,” on page 39](#)
- ♦ [Section 4.3, “Remediation Schedule,” on page 40](#)
- ♦ [Section 4.4, “Remediation Options,” on page 49](#)
- ♦ [Section 4.5, “Advanced Remediation Options,” on page 50](#)
- ♦ [Section 4.7, “Notification and Reboot Options,” on page 54](#)
- ♦ [Section 4.8, “Deployment Summary,” on page 56](#)

**Figure 4-18** Deployment Order and Behavior Page

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

**Vulnerabilities**

 Step 6: Deployment Order and Behavior

Choose the deployment Order and Behavior

<input type="checkbox"/>	Package Name	Order	Reboot	
<input type="checkbox"/>	MS05-026 (EC) Security Update for Windows Server 2003 (KB896358)	1	Yes	<input type="button" value="AA"/> <input type="button" value="A"/> <input type="button" value="V"/> <input type="button" value="VV"/>
<input type="checkbox"/>	(EC) Windows Malicious Software Removal Tool - May 2008 (KB890830)	2	No	
<input type="checkbox"/>	(EC) Microsoft .NET Framework 2.0 Service Pack 1 (KB110806) (x86)	3	Yes	




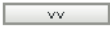
The Deployment Order and Behavior page features the following:

- ♦ **Package Name:** This column displays the name of the vulnerability that has been selected for deployment.

- ♦ **Order:** This column displays the order of execution of the deployment. The arrow appearing next to the column heading enables you to sort the order in ascending or descending order.
- ♦ **Reboot:** This column displays the reboot settings applicable for the corresponding vulnerability.

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

**Table 4-5** Buttons in the Deployment Order and Behavior Page

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

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

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.

## 4.7 Notification and Reboot Options

The Notification and Reboot Options page of the Deploy Remediation Wizard allows you to define whether users receive notification of these deployments and/or reboots, and if so, what the notification contains. Setting the notification and reboot options is the seventh step in scheduling a deployment for a selected vulnerability.

The following sections provide more information on the other steps of the wizard:

- ♦ [Section 4.1, “Confirm Devices,” on page 37](#)
- ♦ [Section 4.2, “License Agreement,” on page 39](#)
- ♦ [Section 4.3, “Remediation Schedule,” on page 40](#)
- ♦ [Section 4.4, “Remediation Options,” on page 49](#)
- ♦ [Section 4.5, “Advanced Remediation Options,” on page 50](#)
- ♦ [Section 4.6, “Deployment Order and Behavior,” on page 53](#)
- ♦ [Section 4.8, “Deployment Summary,” on page 56](#)

**Figure 4-19** Notification and Reboot Options Page

Devices > Servers > Vulnerabilities

Vulnerabilities

Step 7: Notification and Reboot Options

Choose the deployment Order and Behavior

Define Reboot Options

☒ Notify Users

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. This machine will reboot in {0} seconds.

☐ Edit Default Settings

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"/>
Notification on top	<input type="radio"/>	<input checked="" type="radio"/>
Seconds to wait before forcing reboot	<input type="text" value="120"/>	<input type="button" value="Up"/> <input type="button" value="Down"/>

<< Back   Next >>   Cancel

The page provides the following options:

- ♦ **Notify Users:** If selected, the user is notified prior to the installation of this deployment. The user sees a message when notified about this deployment.
- ♦ **Message Box:** This field contains the message you see when notified about this deployment.
- ♦ **Edit Default Settings:** When selected, the default settings for each agent are used. Selecting this option disables all other reboot notification options and enables you to edit the default settings.
- ♦ **Options:** When defining reboot options you can specify whether to use the values defined in the default settings for each option by selecting the *Edit Default Settings* check box or the custom settings. There are five options available:
  - ♦ *Suppress Reboot:* This option prevents a reboot even if the bundle requires a reboot.
  - ♦ *Allow User to cancel:* This option allows the user to cancel the reboot.
  - ♦ *Allow User to snooze:* This option allows the user to snooze the reboot.
  - ♦ *Notification on top:* This option ensures that notifications are given by the ZENworks Adaptive Agent.
  - ♦ *Seconds to wait before forcing reboot:* This option allows you to set an interval after which the device is forced to 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.

## 4.8 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 and eighth step in scheduling a deployment for a selected vulnerability.

The following sections provide more information on the other steps of the wizard:

- ♦ [Section 4.1, “Confirm Devices,” on page 37](#)
- ♦ [Section 4.2, “License Agreement,” on page 39](#)
- ♦ [Section 4.3, “Remediation Schedule,” on page 40](#)
- ♦ [Section 4.4, “Remediation Options,” on page 49](#)
- ♦ [Section 4.5, “Advanced Remediation Options,” on page 50](#)
- ♦ [Section 4.6, “Deployment Order and Behavior,” on page 53](#)
- ♦ [Section 4.7, “Notification and Reboot Options,” on page 54](#)

**Figure 4-20** *Deployment Summary Page*

Devices > Servers > Vulnerabilities

Vulnerabilities

Step 8: Deployment Summary

Please review summary and then press finish.

Property Name	Details
Schedule	Event
Total selected packages	3

Order	Package Name	Reboot
1	MS05-026 (EC) Security Update for Windows Server 2003 (KB896358)	Yes
2	(EC) Windows Malicious Software Removal Tool - May 2008 (KB890830)	No
3	(EC) Microsoft .NET Framework 2.0 Service Pack 1 (KB110806) (x86)	Yes

<< 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 vulnerabilities selected for the deployment.
- ♦ **Order:** The deployment order selected for deployment of the vulnerabilities as defined on the Deployment Order and Behavior page.
- ♦ **Package Name:** The name of the vulnerability you have selected for deployment.
- ♦ **Reboot:** The reboot setting of the selected vulnerability as defined in the Deployment Order and Behavior page.

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



# Using Mandatory Baselines

# 5

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

The following sections provide information on mandatory baselines:

- ♦ [Section 5.1, “About Mandatory Baselines,” on page 57](#)
- ♦ [Section 5.2, “Working with Mandatory Baselines,” on page 61](#)

## 5.1 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, and therefore there is no control over the deployment time or order for vulnerabilities resolved in this manner. Therefore, 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.) are will not 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 vulnerabilities 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.

---

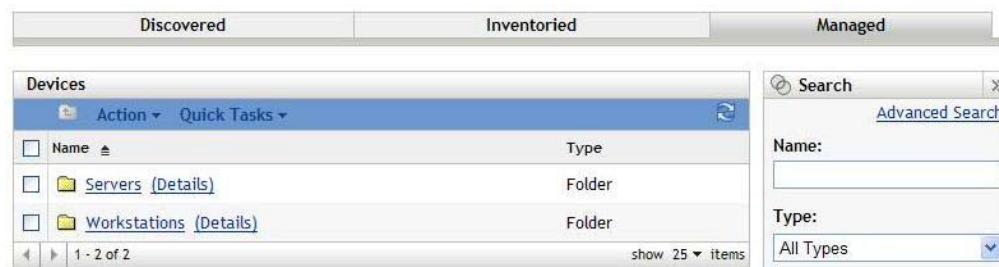
The following sections provide more information on mandatory baselines:

- ♦ [Section 5.1.1, “Viewing Mandatory Baselines,” on page 58](#)
- ♦ [Section 5.1.2, “Using the Mandatory Baseline Page,” on page 60](#)

## 5.1.1 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:

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

Devices						
New ▾ Edit ▾ Delete ▾ Action ▾ Quick Tasks ▾						
<input type="checkbox"/>	Status	Name	Type	Operating System	Last Contact	Retired
<input type="checkbox"/>		<a href="#">Windows 2000 Servers</a>	Dynamic Server Group			
<input type="checkbox"/>		<a href="#">Windows Server 2003</a>	Dynamic Server Group			
<input type="checkbox"/>		<a href="#">Windows Server 2008</a>	Dynamic Server Group			
<input type="checkbox"/>		<a href="#">zcm-server</a>	Server	win2003-se-sp1-x86	Mar 17	
1 - 4 of 4						
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	Vulnerabilities									
<b>General</b> Object type: Dynamic Server Group GUID: 73f4ced49feb837b42f742a586a717c4 Description: <a href="#">(Edit)</a> Windows Server 2003 Group												
<b>Members</b> <table border="1"> <thead> <tr> <th>Name</th> <th>In Folder</th> </tr> </thead> <tbody> <tr> <td><a href="#">zcm-server</a></td> <td>/Devices/Servers</td> </tr> <tr> <td><a href="#">w2k3sp2</a></td> <td>/Devices/Servers</td> </tr> </tbody> </table>				Name	In Folder	<a href="#">zcm-server</a>	/Devices/Servers	<a href="#">w2k3sp2</a>	/Devices/Servers			
Name	In Folder											
<a href="#">zcm-server</a>	/Devices/Servers											
<a href="#">w2k3sp2</a>	/Devices/Servers											
<b>Members Change Log</b> <table border="1"> <thead> <tr> <th>Date</th> <th>Added</th> <th>Removed</th> </tr> </thead> <tbody> <tr> <td>Jun 15</td> <td>1</td> <td>0</td> </tr> <tr> <td>Jun 10</td> <td>1</td> <td>0</td> </tr> </tbody> </table>				Date	Added	Removed	Jun 15	1	0	Jun 10	1	0
Date	Added	Removed										
Jun 15	1	0										
Jun 10	1	0										

#### 4 Click the *Vulnerabilities* tab.

The vulnerabilities applicable to the member devices of the selected group are displayed. If the selected group is *Windows Server 2003*, the *Vulnerabilities* tab displays all the vulnerabilities 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	Vulnerabilities																																																							
<b>Vulnerabilities</b> <table border="1"> <thead> <tr> <th>Action</th> <th>Vulnerability Name</th> <th>Impact</th> <th>Patched</th> <th>Not Patched</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td><a href="#">Internet Explorer 7 Blocker Toolkit (SEE NOTES)</a></td> <td>Software Installer</td> <td>0</td> <td>3</td> </tr> <tr> <td><input type="checkbox"/></td> <td><a href="#">Internet Explorer 7.0 (SEE NOTES)</a></td> <td>Software Installer</td> <td>0</td> <td>4</td> </tr> <tr> <td><input type="checkbox"/></td> <td><a href="#">Macromedia Flash Player 7.0.r19 for IE</a></td> <td>Software Installer</td> <td>0</td> <td>4</td> </tr> <tr> <td><input type="checkbox"/></td> <td><a href="#">Macromedia Flash Player 7.0.r61 for IE</a></td> <td>Software Installer</td> <td>0</td> <td>4</td> </tr> <tr> <td><input type="checkbox"/></td> <td><a href="#">Macromedia Flash Player 7.0.r63 for IE</a></td> <td>Software Installer</td> <td>0</td> <td>4</td> </tr> <tr> <td><input type="checkbox"/></td> <td><a href="#">Macromedia Flash Player 8.0.r22 for IE</a></td> <td>Software Installer</td> <td>0</td> <td>4</td> </tr> <tr> <td><input type="checkbox"/></td> <td><a href="#">Macromedia Flash Player 9.0.r28 for IE</a></td> <td>Software Installer</td> <td>0</td> <td>4</td> </tr> <tr> <td><input type="checkbox"/></td> <td><a href="#">MS 890830 Microsoft Windows Malicious Software Removal Tool (February 2008)</a></td> <td>Software Installer</td> <td>0</td> <td>4</td> </tr> <tr> <td><input type="checkbox"/></td> <td><a href="#">MS 892313 Updates for Windows Media Player 9 and 10</a></td> <td>Recommended</td> <td>1</td> <td>3</td> </tr> <tr> <td><input type="checkbox"/></td> <td><a href="#">MS 898715 Update for Windows Server 2003 Service Pack 1</a></td> <td>Critical</td> <td>0</td> <td>3</td> </tr> </tbody> </table>				Action	Vulnerability Name	Impact	Patched	Not Patched	<input type="checkbox"/>	<a href="#">Internet Explorer 7 Blocker Toolkit (SEE NOTES)</a>	Software Installer	0	3	<input type="checkbox"/>	<a href="#">Internet Explorer 7.0 (SEE NOTES)</a>	Software Installer	0	4	<input type="checkbox"/>	<a href="#">Macromedia Flash Player 7.0.r19 for IE</a>	Software Installer	0	4	<input type="checkbox"/>	<a href="#">Macromedia Flash Player 7.0.r61 for IE</a>	Software Installer	0	4	<input type="checkbox"/>	<a href="#">Macromedia Flash Player 7.0.r63 for IE</a>	Software Installer	0	4	<input type="checkbox"/>	<a href="#">Macromedia Flash Player 8.0.r22 for IE</a>	Software Installer	0	4	<input type="checkbox"/>	<a href="#">Macromedia Flash Player 9.0.r28 for IE</a>	Software Installer	0	4	<input type="checkbox"/>	<a href="#">MS 890830 Microsoft Windows Malicious Software Removal Tool (February 2008)</a>	Software Installer	0	4	<input type="checkbox"/>	<a href="#">MS 892313 Updates for Windows Media Player 9 and 10</a>	Recommended	1	3	<input type="checkbox"/>	<a href="#">MS 898715 Update for Windows Server 2003 Service Pack 1</a>	Critical	0	3
Action	Vulnerability Name	Impact	Patched	Not Patched																																																						
<input type="checkbox"/>	<a href="#">Internet Explorer 7 Blocker Toolkit (SEE NOTES)</a>	Software Installer	0	3																																																						
<input type="checkbox"/>	<a href="#">Internet Explorer 7.0 (SEE NOTES)</a>	Software Installer	0	4																																																						
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 7.0.r19 for IE</a>	Software Installer	0	4																																																						
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 7.0.r61 for IE</a>	Software Installer	0	4																																																						
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 7.0.r63 for IE</a>	Software Installer	0	4																																																						
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 8.0.r22 for IE</a>	Software Installer	0	4																																																						
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 9.0.r28 for IE</a>	Software Installer	0	4																																																						
<input type="checkbox"/>	<a href="#">MS 890830 Microsoft Windows Malicious Software Removal Tool (February 2008)</a>	Software Installer	0	4																																																						
<input type="checkbox"/>	<a href="#">MS 892313 Updates for Windows Media Player 9 and 10</a>	Recommended	1	3																																																						
<input type="checkbox"/>	<a href="#">MS 898715 Update for Windows Server 2003 Service Pack 1</a>	Critical	0	3																																																						

Search

Vulnerability Name

Search Reset

Status

☐ Patched

☒ Not Patched

☐ Not Applicable

☐ Include Disabled

Impact

☒ Critical

☒ Recommended


☒ Informational

☒ Software Installers

Mandatory Baseline

☒ All Vulnerabilities

☐ Baseline Only

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

Alternatively, you can view the baseline vulnerabilities by using the *Search* panel on the Vulnerabilities page that allows you to search for mandatory baseline vulnerabilities.

For detailed information on *Vulnerabilities* and *Vulnerabilities Information* panels, refer to [Chapter 3, “Using Vulnerabilities,” on page 25](#).

## 5.1.2 Using the Mandatory Baseline Page

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

The *Search* panel on the Device Group Vulnerabilities page, as shown in [Figure 5-1](#), enables you to search for mandatory baseline vulnerabilities. The *Search* panel also enables you to search for other vulnerabilities based on status and impact of the vulnerabilities.

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

- ♦ **All Vulnerabilities:** Selecting this filter option displays all vulnerabilities and including the mandatory baseline items.
- ♦ **Baseline Only:** *Baseline Only*: Selecting this filter option displays only those vulnerabilities that are marked as “mandatory baseline” items for the group.

**Figure 5-1** Mandatory Baseline Search

Search

Vulnerability Name

Search Reset

Status

☐ Patched

☐ Not Patched

☐ Not Applicable

☐ Include Disabled

Impact

☐ Critical

☐ Recommended

☐ Informational

☐ Software Installers

Mandatory Baseline

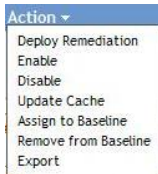
☒ All Vulnerabilities

☐ Baseline Only

## 5.2 Working with Mandatory Baselines

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

**Figure 5-2** Action Menu Items



- ♦ The *Deploy Remediation* option enables you to deploy a patch. To use this option, select the check boxes for the vulnerabilities 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 vulnerability.
- ♦ The *Disable* option enables you to disable a vulnerability. To use this option, select the check box for the required vulnerability and select *Disable*. The selected vulnerability is removed from the list.
- ♦ The *Update Cache* option initiates a download process for the bundles associated with a selected vulnerability and caches those bundles on your ZENworks Server. See [Section 5.2.3, “Using Update Cache,” on page 65](#).
- ♦ The *Assign to Baseline* option enables you to assign a baseline to a vulnerability. For more information, see [Section 5.2.1, “Assigning or Managing a Mandatory Baseline,” on page 61](#)
- ♦ The *Remove from Baseline* option enables you to remove a vulnerability from a baseline. See [Section 5.2.2, “Removing a Mandatory Baseline,” on page 63](#) for more information.
- ♦ The *Export* option enables you to export details such as the status and impact of selected vulnerabilities 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 following sections provide more information on mandatory baselines:

- ♦ [Section 5.2.1, “Assigning or Managing a Mandatory Baseline,” on page 61](#)
- ♦ [Section 5.2.2, “Removing a Mandatory Baseline,” on page 63](#)
- ♦ [Section 5.2.3, “Using Update Cache,” on page 65](#)

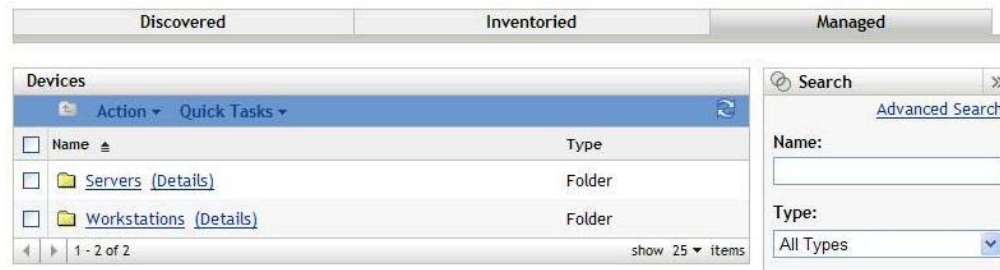
### 5.2.1 Assigning or Managing a Mandatory Baseline

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.

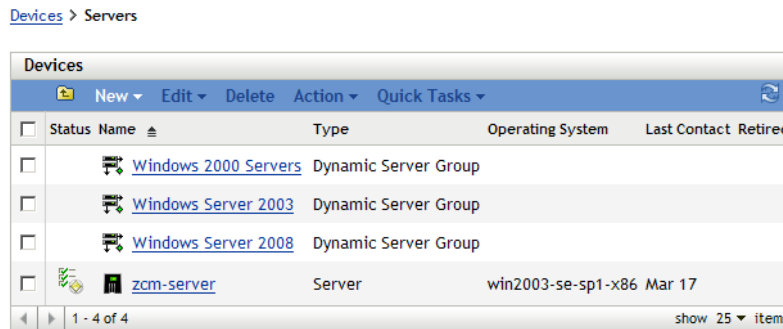
A page displaying the root folders for each type of device appears, as shown in the following figure.



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:

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

Windows Server 2003

Summary	Relationships	Details	Vulnerabilities									
<b>General</b> <div> Object type: Dynamic Server Group  GUID: 73f4ced49feb837b42f742a586a717c4  Description: <a href="#">(Edit)</a> Windows Server 2003 Group </div>												
<b>Members</b> <table border="1"> <thead> <tr> <th>Name</th> <th>In Folder</th> </tr> </thead> <tbody> <tr> <td> <a href="#">zcm-server</a></td> <td>/Devices/Servers</td> </tr> <tr> <td> <a href="#">w2k3sp2</a></td> <td>/Devices/Servers</td> </tr> </tbody> </table> <div> 1 - 2 of 2 show 5 items </div>				Name	In Folder	<a href="#">zcm-server</a>	/Devices/Servers	<a href="#">w2k3sp2</a>	/Devices/Servers			
Name	In Folder											
<a href="#">zcm-server</a>	/Devices/Servers											
<a href="#">w2k3sp2</a>	/Devices/Servers											
<b>Members Change Log</b> <table border="1"> <thead> <tr> <th>Date</th> <th>Added</th> <th>Removed</th> </tr> </thead> <tbody> <tr> <td>Jun 15</td> <td><a href="#">1</a></td> <td><a href="#">0</a></td> </tr> <tr> <td>Jun 10</td> <td><a href="#">1</a></td> <td><a href="#">0</a></td> </tr> </tbody> </table> <div> 1 - 2 of 2 show 5 items </div>				Date	Added	Removed	Jun 15	<a href="#">1</a>	<a href="#">0</a>	Jun 10	<a href="#">1</a>	<a href="#">0</a>
Date	Added	Removed										
Jun 15	<a href="#">1</a>	<a href="#">0</a>										
Jun 10	<a href="#">1</a>	<a href="#">0</a>										

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

This is what happens after a vulnerability has been assigned to the baseline:

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 vulnerabilities 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.

---

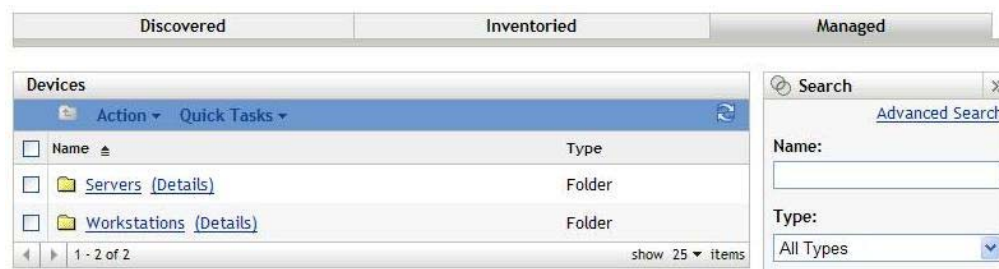
**NOTE:** The baseline function does not auto-reboot devices that have been patched.

---

## 5.2.2 Removing a Mandatory Baseline

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

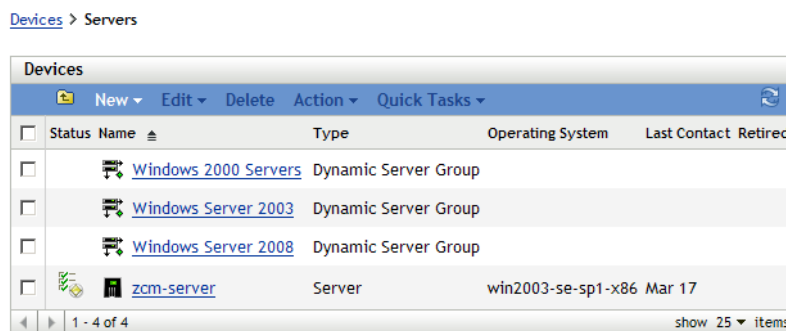
A page displaying the root folders for each type of device appears, as shown in the following figure.



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.

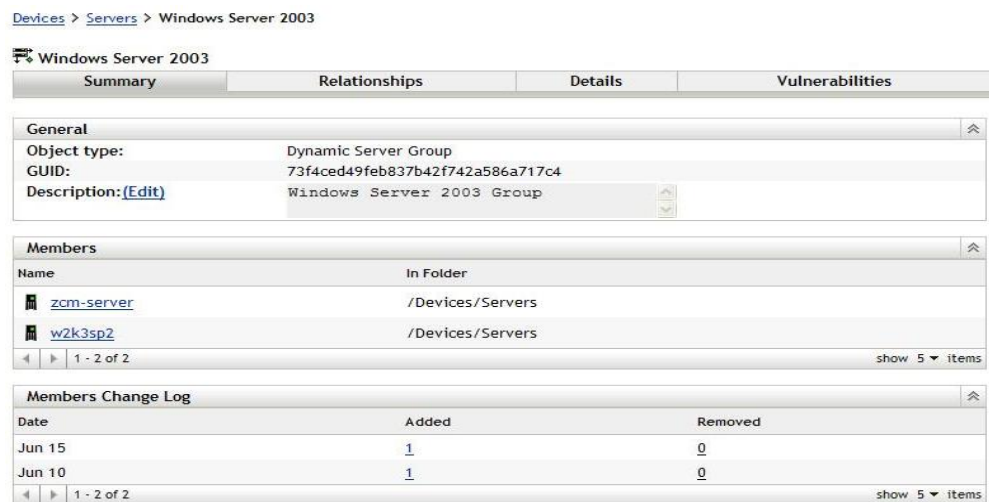
A list of server or workstation groups classified on the basis of their operating systems appears. The following figure shows a list of server groups:



**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 mandatory baseline item (vulnerability that has been assigned to baseline) and choose the option *Remove from Baseline* from the *Action* menu.

The vulnerability is removed from baseline.

---

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

---

### 5.2.3 Using Update Cache

The *Action* menu option *Update Cache* (see [Figure 5-2 on page 61](#)) initiates a download process for the bundles associated with a selected vulnerability and caches those bundles on your ZENworks Server.

---

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

---

To update caching of vulnerability data:

- 1 In the *Vulnerabilities* list, select one or multiple vulnerabilities.
- 2 In the *Action* menu, click *Update Cache*.

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



# Using Devices

# 6

Device vulnerabilities refers to the vulnerability information associated with a selected device—a server or a workstation. The vulnerabilities listed for a specific device are the ones that are applicable only for that device. The following sections describe device vulnerability information for Novell® ZENworks® Patch Management Services:

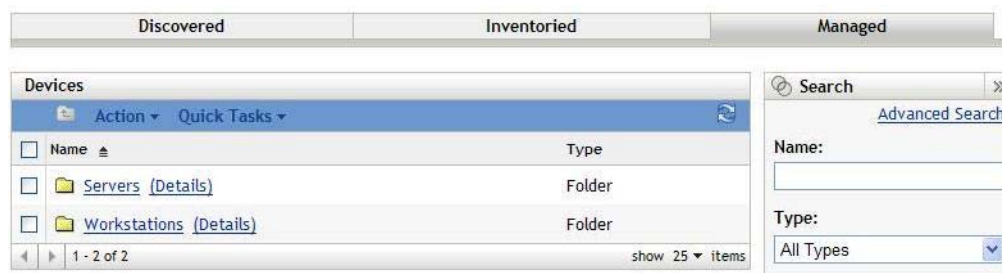
- ♦ [Section 6.1, “Server Device Vulnerabilities,” on page 67](#)
- ♦ [Section 6.2, “Using the Vulnerabilities Page for the Selected Device,” on page 69](#)

## 6.1 Server Device Vulnerabilities

To view the vulnerabilities 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](#) > [Servers](#)

Devices					
New Edit Delete Action Quick Tasks					
<input type="checkbox"/>	Status Name	Type	Operating System	Last Contact	Retired
<input type="checkbox"/>	 <a href="#">Windows 2000 Servers</a>	Dynamic Server Group			
<input type="checkbox"/>	 <a href="#">Windows Server 2003</a>	Dynamic Server Group			
<input type="checkbox"/>	 <a href="#">Windows Server 2008</a>	Dynamic Server Group			
<input type="checkbox"/>	 <a href="#">zcm-server</a>	Server	win2003-se-sp1-x86	Mar 17	
1 - 4 of 4 show 25 items					

- 3 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 appears, as shown in the following figure.

The name "zcm-server" for the managed device is an example. The network administrator decides the name of the managed device.

The following figure shows the page displaying details for the managed device named *zcm-server*:

[Devices](#) > [Servers](#) > zcm-server

**zcm-server**

Summary	Inventory	Relationships	Settings	Content	Statistics	Vulnerabilities
---------	-----------	---------------	----------	---------	------------	-----------------

**General**

Alias: zcm-server

Host Name: ZCM-SERVER

IP Address: 192.168.1.145

Last Full Refresh: 1:50 AM

Last Contact: 1:50 AM

ZENworks Agent Status:

Operating System: Microsoft Windows Server 2003 5.2 1 3790

Number of errors not acknowledged: 2

Number of warnings not acknowledged: 14

Primary User: No user sources configured

Owner: [\(Edit\)](#)

GUID: b9e131e7fb3ad21130aab433ea5eea89

Department: [\(Edit\)](#)

Site: [\(Edit\)](#)

Location: [\(Edit\)](#)

**Upcoming Events**

3/17/08

[Refresh](#)

Type	Name	Time
Click <a href="#">refresh</a> to see upcoming events		

**Logged In Users** [Advanced](#)

Name	In Folder
No items available.	

**Imaging Work** [Advanced](#)

Scheduled Work: None

Applied Image Files: None

Type	Name
No items available.	

#### 4 Click the *Vulnerabilities* tab.

The vulnerabilities associated with the server device appear, as shown in the following figure:

[Devices](#) > [Workstations](#) > zcm-agent

**zcm-agent**

Summary	Inventory	Relationships	Settings	Content	Vulnerabilities
---------	-----------	---------------	----------	---------	-----------------

**Vulnerabilities**

Action	Vulnerability Name	Impact	Patched
<input type="checkbox"/>	Internet Explorer 6.0 Service Pack 1 (Rev 2)	Software Installer	Yes
<input type="checkbox"/>	Internet Explorer 7 Blocker Toolkit (SEE NOTES)	Software Installer	No
<input type="checkbox"/>	Internet Explorer 7.0 (SEE NOTES)	Software Installer	No
<input type="checkbox"/>	Macromedia Flash Player 6 patch release R65 for IE	Critical	Yes
<input type="checkbox"/>	Macromedia Flash Player 7.0.r19 for IE	Software Installer	No
<input type="checkbox"/>	Macromedia Flash Player 7.0.r61 for IE	Software Installer	No
<input type="checkbox"/>	Macromedia Flash Player 7.0.r63 for IE	Software Installer	No
<input type="checkbox"/>	Macromedia Flash Player 8.0.r22 for IE	Software Installer	No
<input type="checkbox"/>	Macromedia Flash Player 9.0.r28 for IE	Software Installer	No
<input type="checkbox"/>	Microsoft .NET Framework 2.0 SP1 (See Notes)	Critical	No

1 - 10 of 186 show 10 items

**Search**

Vulnerability Name

[Search](#) [Reset](#)

**Status**

☒ Patched

☒ Not Patched

☐ Not Applicable

☒ Include Disabled

**Impact**

☒ Critical

☒ Recommended

☒ Informational

☒ Software Installers

## 6.2 Using the Vulnerabilities Page for the Selected Device

The following sections provide more information on the Vulnerabilities page:

- ♦ [Section 6.2.1, “Vulnerabilities,” on page 69](#)
- ♦ [Section 6.2.2, “Vulnerability Name,” on page 69](#)
- ♦ [Section 6.2.3, “Total Number of Vulnerabilities Available,” on page 70](#)
- ♦ [Section 6.2.4, “Vulnerability Impacts,” on page 70](#)
- ♦ [Section 6.2.5, “Vulnerability Statistics,” on page 71](#)
- ♦ [Section 6.2.6, “Action Menu Items,” on page 71](#)
- ♦ [Section 6.2.7, “Vulnerability Information,” on page 72](#)
- ♦ [Section 6.2.8, “Searching Vulnerabilities,” on page 74](#)
- ♦ [Section 6.2.9, “Workstation Device Vulnerabilities,” on page 75](#)

### 6.2.1 Vulnerabilities

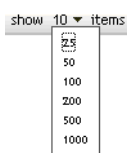
This section of the Vulnerabilities page provides the following information about vulnerabilities:

- ♦ Name of the vulnerability
- ♦ Total number of vulnerabilities available
- ♦ Impact of the vulnerability
- ♦ Statistics of the vulnerability

This section features the *Action* menu that enables you to perform any of the five actions related to vulnerabilities: *Deploy Remediation*, *Enable*, *Disable*, *Scan Now*, *Update Cache*, and *Export*. For more information on these actions, see [Section 6.2.6, “Action Menu Items,” on page 71](#).

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

**Figure 6-1** *Show Items drop-down List*



### 6.2.2 Vulnerability Name

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

An example of a vulnerability name is shown in the following figure, where vulnerability name is given, Adobe\* is the vendor, Acrobat Reader\* is the application, and 6.0.6 is the version information.

**Figure 6-2** Example of a Vulnerability Name

Adobe Acrobat Reader 6.0.6 Update

### 6.2.3 Total Number of Vulnerabilities Available

The total number of available vulnerabilities is displayed in the bottom left corner of the table. In the following example, the total number of available vulnerabilities is 979.

**Figure 6-3** Total Number of Vulnerabilities

1 - 10 of 979

### 6.2.4 Vulnerability Impacts

Based on the release date and impact, a vulnerability can be classified as Critical, Recommended, Informational, or Software Installers. Each impact is described as follows:

- ♦ **Critical:** Novell has determined that this type of vulnerability 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 vulnerabilities that have critical impact.
- ♦ **Recommended:** Novell has determined that this vulnerability, 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 vulnerabilities that fall in this category.
- ♦ **Informational:** This type of vulnerability 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 vulnerabilities are software applications. Typically, they include installers. The vulnerabilities show *Not Patched* if the application has not been installed on a machine.

Novell ZENworks Patch Management impact terminology for its patch subscription closely follows the vendor impact terminology for vulnerability criticality. Each operating system has a vendor-specific impact rating and that impact is mapped to a Novell rating as described in this section. Novell ZENworks 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's and Microsoft's patch classification terminology:

**Table 6-1** *Novell and Microsoft Patch Impact Mapping*

Novell Patch Impacts	Windows	Other
Critical	Critical Security	Example: AV Updates (Critical-01)
	Important	
	Moderate	
	Example: Service Packs (Critical-01)	
Recommended	Recommended	NA
	Low	
	Example: Microsoft Outlook 2003 Junk E-mail Filter Update	
Software Installers	Software Distribution	Adobe* 8.1 software installer
	Example: Microsoft Windows Malicious Software Removal Tool (Virus Removal)	
Informational	NA	NA

Source: Lumension Security

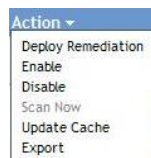
## 6.2.5 Vulnerability Statistics

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

## 6.2.6 Action Menu Items

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

**Figure 6-4** *Action Menu*



- ♦ **Deploy Remediation:** This option enables you to deploy a patch. To use this option, select the check box for the vulnerability you want to deploy and select *Deploy Remediation* to open the Deploy Remediation Wizard.

- ♦ **Enable:** This option allows you to enable a disabled vulnerability. To use this option, select it from the *Action* menu.
- ♦ **Disable:** This option enables you to disable a vulnerability. To use this option, select the check box for the required vulnerability and select *Disable*. The selected vulnerability is removed from the list.

---

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

---

- ♦ **Scan Now:** This option enables you to reschedule the Discover Applicable Updates (DAU) task for immediate execution. The DAU runs on a predefined interval schedule. A manual scan schedules the task for immediate execution.
- ♦ **Update Cache:** This option initiates a download process for the bundles associated with the selected vulnerability and caches those bundles on your ZENworks Server.



---

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

---

To use this option:

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

The vulnerability icon changes to . While the download is in progress, the icon changes to . When the caching is complete, the color of the vulnerability icon changes to blue.

This indicates that the patch remediation is ready to be deployed.

- ♦ **Export:** This option enables you to export the details such as the status and impact of selected vulnerabilities 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.

## 6.2.7 Vulnerability Information

You can view detailed information of a selected vulnerability in the *Vulnerability Information* section. Clicking the name of a vulnerability displays the details of that vulnerability.



For example, if you select the vulnerability called *Macromedia Flash Player 7.0.r19 for IE* from the list of vulnerabilities, the *Vulnerability Information* section displays the result of a vulnerability analysis for the selected vulnerability, as shown in the following figure:

**Figure 6-5** *Vulnerability Information for a Selected Vulnerability*

Vulnerability Information	
Property Name	Details
Name	Macromedia Flash Player 7.0.r19 for IE
Impact	Software Installer
Status	Enabled
Vendor	Macromedia
Released On	2004-06-17 00:00:00.0
Vendor Product ID	MP7.0r19
Description	<p>Macromedia added two new restrictions to the Macromedia Flash security model, starting with Macromedia Flash Player 7:</p> <ul style="list-style-type: none"> <li>• All operations require an exact domain match. Similar domains, such as <code>www.mysite.com</code> and <code>store.mysite.com</code>, are no longer considered a match. Domains must now match exactly.</li> <li>• Macromedia Flash movies served over HTTP (or other insecure protocols) are no longer allowed to access movies or data served over HTTPS.</li> </ul> <p>In version 7r19 of the Flash Player, Macromedia added the ActionScript API <code>System.security.loadPolicyFile</code>. Using this API, you can place policy files in arbitrary locations, rather than just the default location at the server root. With this API, you can also serve policy files directly from XMLSocket servers and specify XMLSocket connections to ports below 1024.</p> <p>For information on the latest patch revision, see <a href="#">Patch Applicability Fingerprint Improvements</a>.</p>

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

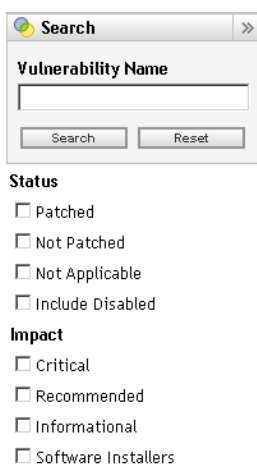
**Table 6-2** *Property Names in the Vulnerability Information Section*

Property Name	Definition
Name	The name of the vulnerability.
Impact	The impact of the vulnerability as determined by Novell. See <a href="#">Section 6.2.4, "Vulnerability Impacts," on page 70</a> .
Status	Status of the vulnerability. It can be <i>Enabled</i> or <i>Disabled</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 vulnerability; it includes the advantages of deploying the vulnerability and the prerequisites for deployment.

## 6.2.8 Searching Vulnerabilities

The *Search* section on the Vulnerabilities page offers extensive search and data filtering options that allow you to search for specific vulnerabilities and filter result sets based on the status and impact of the vulnerabilities. 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 *Vulnerability Search* section:

**Figure 6-6** *Search Section on the Vulnerabilities Page*



**Search** >>

**Vulnerability Name**

**Status**

☐ Patched

☐ Not Patched

☐ Not Applicable

☐ Include Disabled

**Impact**

☐ Critical

☐ Recommended

☐ Informational

☐ Software Installers

To search for a vulnerability:

- 1 Type all or part of the vulnerability name in the *Vulnerability Name* text box.
- 2 Select the desired check box under *Status* and *Impact*.
- 3 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 6-3** *Status Filters in Search*

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

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

**Table 6-4** *Impact Filters in Search*

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

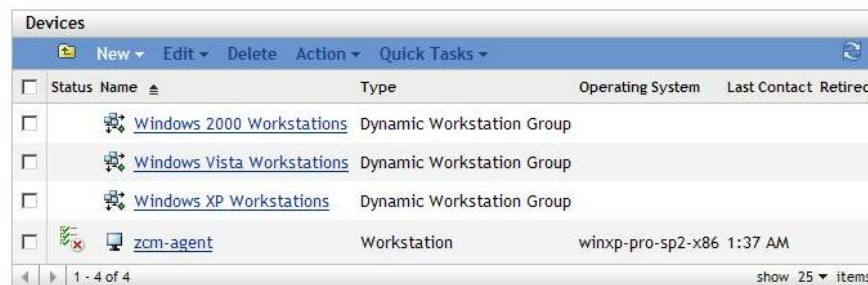
## 6.2.9 Workstation Device Vulnerabilities

To view the vulnerabilities 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					
<a href="#">New</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Action</a> <a href="#">Quick Tasks</a>					
<input type="checkbox"/>	Status	Name	Type	Operating System	Last Contact Retired
<input type="checkbox"/>		<a href="#">Windows 2000 Workstations</a>	Dynamic Workstation Group		
<input type="checkbox"/>		<a href="#">Windows Vista Workstations</a>	Dynamic Workstation Group		
<input type="checkbox"/>		<a href="#">Windows XP Workstations</a>	Dynamic Workstation Group		
<input type="checkbox"/>		<a href="#">zcm-agent</a>	Workstation	winxp-pro-sp2-x86	1:37 AM

1 - 4 of 4 show 25 items

- 2 Click the required group (Workstation or Dynamic Workstation Group) to view details of the group and the members of the group.
- 3 Click the required member or workstation device.

A page displaying details of the member appears. See the following figure.

**NOTE:** The name *zcm-agent* is an example.

The following figure shows the page displaying details for the workstation device *zcm-agent*:

Devices > Workstations > zcm-agent

zcm-agent

Summary	Inventory	Relationships	Settings	Content	Vulnerabilities
---------	-----------	---------------	----------	---------	-----------------

**General**

Alias: zcm-agent

Host Name: ZCM-AGENT

IP Address: 192.168.1.135

Last Full Refresh: 1:49 AM

Last Contact: 1:51 AM

ZENworks Agent Status:

Operating System: Microsoft Windows XP Professional 5.1 2 2600

Number of errors not acknowledged: 18

Number of warnings not acknowledged: 18

Primary User: No user sources configured

Owner: [\(Edit\)](#)

GUID: a23083509433d8478906d750aeffa7ae

Department: [\(Edit\)](#)

Site: [\(Edit\)](#)

Location: [\(Edit\)](#)

**Upcoming Events**

3/17/08

Refresh

Type	Name	Time
Click <a href="#">refresh</a> to see upcoming events		

**Logged In Users** [Advanced](#)

Name	In Folder
No items available.	

**Imaging Work** [Advanced](#)

Scheduled Work: None

Applied Image Files: None

Type	Name
No items available.	

#### 4 Click the *Vulnerabilities* tab.

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

Devices > Workstations > zcm-agent

zcm-agent

Summary	Inventory	Relationships	Settings	Content	Vulnerabilities
---------	-----------	---------------	----------	---------	-----------------

**Vulnerabilities**

Action	Vulnerability Name	Impact	Patched
<input type="checkbox"/>	<a href="#">Internet Explorer 6.0 Service Pack 1 (Rev 2)</a>	Software Installer	Yes
<input type="checkbox"/>	<a href="#">Internet Explorer 7 Blocker Toolkit (SEE NOTES)</a>	Software Installer	No
<input type="checkbox"/>	<a href="#">Internet Explorer 7.0 (SEE NOTES)</a>	Software Installer	No
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 6 patch release R65 for IE</a>	Critical	Yes
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 7.0.r19 for IE</a>	Software Installer	No
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 7.0.r61 for IE</a>	Software Installer	No
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 7.0.r63 for IE</a>	Software Installer	No
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 8.0.r22 for IE</a>	Software Installer	No
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 9.0.r28 for IE</a>	Software Installer	No
<input type="checkbox"/>	<a href="#">Microsoft .NET Framework 2.0 SP1 (See Notes)</a>	Critical	No

1 - 10 of 186 show 10 items

**Search**

Vulnerability Name

Search Reset

**Status**

☒ Patched

☒ Not Patched

☐ Not Applicable

☒ Include Disabled

**Impact**

☒ Critical

☒ Recommended

☒ Informational

☒ Software Installers

# Using Device Group Vulnerabilities

# 7

Device group vulnerabilities refers to the vulnerabilities that have been assigned to the members the servers group or the workstations group of devices in the network and displays the status of each vulnerability for the devices. This view only displays the vulnerabilities applicable to the member devices of the selected group.

- [Section 7.1, “Server Group Vulnerabilities,” on page 77](#)
- [Section 7.2, “Workstation Group Vulnerabilities,” on page 79](#)

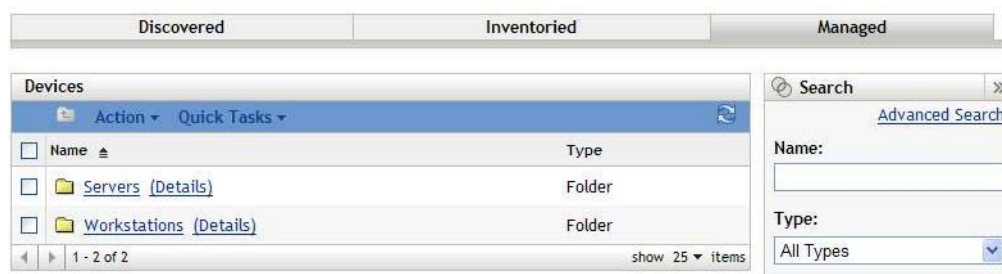
## 7.1 Server Group Vulnerabilities

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

To view the vulnerabilities for a specific group of servers:

- 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](#) > [Servers](#)

Devices					
New Edit Delete Action Quick Tasks					
Status	Name	Type	Operating System	Last Contact	Retired
<input type="checkbox"/>	<a href="#">Windows 2000 Servers</a>	Dynamic Server Group			
<input type="checkbox"/>	<a href="#">Windows Server 2003</a>	Dynamic Server Group			
<input type="checkbox"/>	<a href="#">Windows Server 2008</a>	Dynamic Server Group			
<input type="checkbox"/>	<a href="#">zcm-server</a>	Server	win2003-se-sp1-x86	Mar 17	

**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 below shows such a page that appears when the *Windows Server 2003* type is selected:

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

Windows Server 2003

Summary	Relationships	Details	Vulnerabilities
---------	---------------	---------	-----------------

**General**

Object type: Dynamic Server Group

GUID: 73f4ced49feb837b42f742a586a717c4

Description: [\(Edit\)](#) Windows Server 2003 Group

**Members**

Name	In Folder
<a href="#">zcm-server</a>	/Devices/Servers
<a href="#">w2k3sp2</a>	/Devices/Servers

1 - 2 of 2

show 5 items

**Members Change Log**

Date	Added	Removed
Jun 15	<a href="#">1</a>	<a href="#">0</a>
Jun 10	<a href="#">1</a>	<a href="#">0</a>

1 - 2 of 2

show 5 items

**4** Click the *Vulnerabilities* tab.

The vulnerabilities applicable to the member devices of the selected group are displayed. If the selected group is *Windows Server 2003*, the *Vulnerabilities* tab displays all the vulnerabilities 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	<b>Vulnerabilities</b>
---------	---------------	---------	------------------------

**Vulnerabilities**

Action	Vulnerability Name	Impact	Patched	Not Patched
<input type="checkbox"/>	<a href="#">Internet Explorer 7 Blocker Toolkit (SEE NOTES)</a>	Software Installer	<a href="#">0</a>	<a href="#">3</a>
<input type="checkbox"/>	<a href="#">Internet Explorer 7.0 (SEE NOTES)</a>	Software Installer	<a href="#">0</a>	<a href="#">4</a>
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 7.0.r19 for IE</a>	Software Installer	<a href="#">0</a>	<a href="#">4</a>
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 7.0.r61 for IE</a>	Software Installer	<a href="#">0</a>	<a href="#">4</a>
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 7.0.r63 for IE</a>	Software Installer	<a href="#">0</a>	<a href="#">4</a>
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 8.0.r22 for IE</a>	Software Installer	<a href="#">0</a>	<a href="#">4</a>
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 9.0.r28 for IE</a>	Software Installer	<a href="#">0</a>	<a href="#">4</a>
<input type="checkbox"/>	<a href="#">MS 890830 Microsoft Windows Malicious Software Removal Tool (February 2008)</a>	Software Installer	<a href="#">0</a>	<a href="#">4</a>
<input type="checkbox"/>	<a href="#">MS 892313 Updates for Windows Media Player 9 and 10</a>	Recommended	<a href="#">1</a>	<a href="#">3</a>
<input type="checkbox"/>	<a href="#">MS 898715 Update for Windows Server 2003 Service Pack 1</a>	Critical	<a href="#">0</a>	<a href="#">3</a>

1 - 10 of 144      show 10 items

**Search**

Vulnerability Name

Search    Reset

**Status**

☐ Patched

☒ Not Patched

☐ Not Applicable

☐ Include Disabled

**Impact**

☒ Critical

☒ Recommended

☒ Informational

☒ Software Installers

**Mandatory Baseline**

☒ All Vulnerabilities

☐ Baseline Only

For information on the features of the Device Group Vulnerabilities page for the selected server group, see [“About Mandatory Baselines” on page 57](#).

## 7.2 Workstation Group Vulnerabilities

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

To view the vulnerabilities for a specific 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				
<a href="#">New</a> ▾ <a href="#">Edit</a> ▾ <a href="#">Delete</a> <a href="#">Action</a> ▾ <a href="#">Quick Tasks</a> ▾				
<input type="checkbox"/>	Status	Name	Type	Operating System
<input type="checkbox"/>		<a href="#">Windows 2000 Workstations</a>	Dynamic Workstation Group	
<input type="checkbox"/>		<a href="#">Windows Vista Workstations</a>	Dynamic Workstation Group	
<input type="checkbox"/>		<a href="#">Windows XP Workstations</a>	Dynamic Workstation Group	
<input type="checkbox"/>		<a href="#">zcm-agent</a>	Workstation	winxp-pro-sp2-x86 1:37 AM

1 - 4 of 4 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 such a page that appears when the Dynamic Workstation Group called *Windows XP Workstations* is selected:

[Devices](#) > [Workstations](#) > [Windows XP Workstations](#)

[Windows XP Workstations](#)

Summary	Relationships	Details	Vulnerabilities
---------	---------------	---------	-----------------

Members	
Name	In Folder
<a href="#">zcm-agent</a>	/Devices/Workstations

1 - 1 of 1 show 5 ▾ items

### 4 Click the *Vulnerabilities* tab.

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

Summary	Relationships	Details	Vulnerabilities
---------	---------------	---------	-----------------

Vulnerabilities				
Action ▾	Vulnerability Name	Impact	Patched	Not Patched
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 7.0.r19 for IE</a>	Critical	0	1
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 7.0.r61 for IE</a>	Critical	0	1
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 7.0.r63 for IE</a>	Critical	0	1
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 8.0.r22 for IE</a>	Critical	0	1
<input type="checkbox"/>	<a href="#">Macromedia Flash Player 9.0.r28 for IE</a>	Critical	0	1
<input type="checkbox"/>	<a href="#">MS 890830 Microsoft Windows Malicious Software Removal Tool (March 13 2007)</a>	Critical	0	1
<input type="checkbox"/>	<a href="#">MS 892313 Updates for Windows Media Player 9 and 10</a>	Critical	0	1
<input type="checkbox"/>	<a href="#">MS 912946 Internet Explorer ActiveX Update</a>	Critical	0	1
<input type="checkbox"/>	<a href="#">MS04L 6.0</a>	Critical	0	1
<input type="checkbox"/>	<a href="#">MS 913538 Update for Windows Management Instrumentation</a>	Critical	0	1

1 - 10 of 66 show 10 ▾ items

For information on the features of the Device Group Vulnerabilities page for the selected workstations group, see “[About Mandatory Baselines](#)” on page 57.