

# Novell ZENworks® Patch Management

10

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

REFERENCE

September 21, 2007



Novell®

## Legal Notices

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

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

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

Copyright © 2007 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 Novell ZENworks Patch Management Overview</b>	<b>9</b>
1.1 Product Overview	9
1.1.1 ZENworks Server and Adaptive Agent Process	10
1.1.2 Features of ZENworks Patch Management	11
<b>2 Using Novell ZENworks Patch Management</b>	<b>13</b>
2.1 Using the ZENworks Patch Management Home Page	13
2.1.1 Viewing and Configuring Subscription Information	13
<b>3 Using Vulnerabilities</b>	<b>27</b>
3.1 About Vulnerabilities	27
3.1.1 Viewing Vulnerabilities	27
3.2 Using the Vulnerabilities Page	28
3.2.1 Vulnerabilities	28
3.2.2 Vulnerability Information	31
3.2.3 Searching Vulnerability	33
<b>4 Working with Deployments</b>	<b>35</b>
4.1 Using the Deploy Remediation Wizard	35
4.1.1 Confirming the Device	36
4.1.2 Accepting License Agreement	37
4.1.3 Setting Remediation Schedule	38
4.1.4 Setting Remediation Options	48
4.1.5 Setting Advanced Remediation Options	49
4.1.6 Setting Deployment Order and Behavior	51
4.1.7 Notification and Reboot Options	52
4.1.8 Deployment Summary	53
<b>5 Mandatory Baselines</b>	<b>55</b>
5.1 About Mandatory Baselines	55
5.1.1 Viewing Mandatory Baselines	55
5.1.2 Using the Mandatory Baseline Page	58
5.2 Working with Mandatory Baselines	59
5.2.1 Assigning or Managing a Mandatory Baseline	60
5.2.2 Removing a Mandatory Baseline	61
5.2.3 Using Update Cache	61
<b>6 Using Devices</b>	<b>63</b>
6.1 About Devices	63
6.1.1 Device Vulnerabilities	63

**7 Device Group Vulnerabilities 75**

7.1 Server Group Vulnerabilities . . . . . 75

7.2 Workstation Group Vulnerabilities . . . . . 77

# About This Guide

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

- ♦ Chapter 1, “Novell ZENworks Patch Management Overview,” on page 9
- ♦ Chapter 2, “Using Novell ZENworks Patch Management,” on page 13
- ♦ Chapter 3, “Using Vulnerabilities,” on page 27
- ♦ Chapter 4, “Working with Deployments,” on page 35
- ♦ Chapter 5, “Mandatory Baselines,” on page 55
- ♦ Chapter 6, “Using Devices,” on page 63
- ♦ Chapter 7, “Device Group Vulnerabilities,” on page 75

## Audience

This guide is intended for ZENworks Configuration Management 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 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 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.





# Novell ZENworks Patch Management Overview

# 1

Novell® ZENworks® Patch Management is the core product of the leading patch and vulnerability management solution for medium and large enterprise networks. ZENworks Patch Management enables customers to easily translate security policies into automated and continuous protection against over 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 ensures that policy measurement and security audits are a true representation of network security posture.

## In this chapter

- ♦ [Section 1.1, “Product Overview,” on page 9](#)
- ♦ [Section 1.1.1, “ZENworks Server and Adaptive Agent Process,” on page 10](#)
- ♦ [Section 1.1.2, “Features of ZENworks Patch Management,” on page 11](#)

## 1.1 Product Overview

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

The ZENworks Patch Management 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.

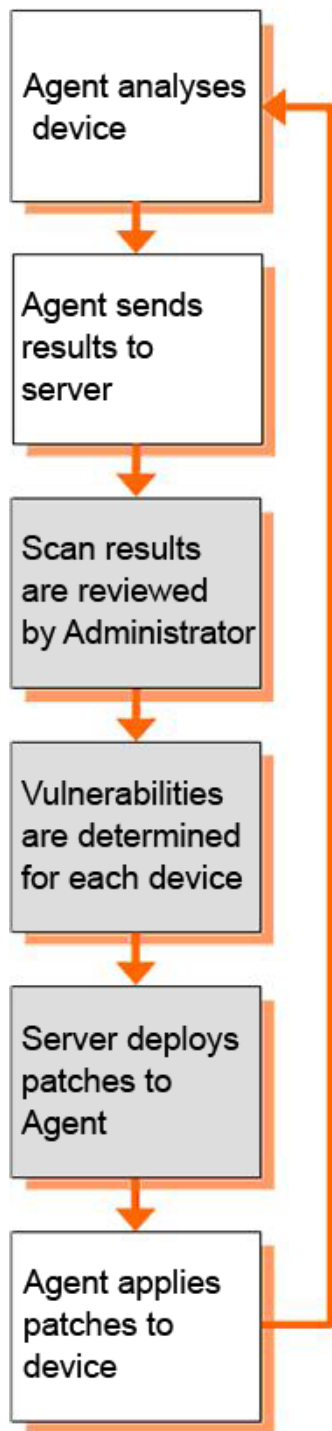
The core component of the system is the ZENworks Control Center (ZCC), from which you can monitor and maintain patch compliance throughout the whole enterprise through a centralized Web-interface. ZENworks Server can deploy a ZENworks Adaptive Agent on every client system in the target network ensuring that all systems are protected with the latest vulnerability patches, software updates, and service packs.

The ZENworks Patch Management feature stays current with the latest patches and fixes by regular communication with the Patchlink Patch Subscription Service through a connection to the Internet. After the initial 60-day free trial period, the ZENworks Patch Management 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 Management subscription, it is downloaded automatically to the ZENworks server and an e-mail is sent to the Administrator. When the Administrator logs onto the ZENworks Control Center, the new patch and the list of devices that require deployment can be viewed easily in the Web-based management interface along with the description and business impact. At this time, the Administrator can choose to deploy the patch to devices or disregard the patch.

### 1.1.1 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.



The ZENworks server schedules an “analyze” scan of all ZENworks Patch Management devices (Servers and Workstations) and compiles information on 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 under 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 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 "Analyze" process are posted to the Vulnerabilities tab of the ZENworks Control Center (ZCC), for review by an Administrator.

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

## 1.1.2 Features of ZENworks Patch Management

ZENworks Patch Management has the world's largest repository of patches, including more than 10,000 patches for major operating systems and applications. ZENworks Patch Management features an agent-based architecture, patch package pre-testing, highly scalable software, and easy-to-use features that allow customers to patch 13 times faster than the industry average.

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

With Novell® ZENworks Patch Management, you can be sure that your systems are effectively patched and compliant for successful IT and regulatory audits. ZENworks Patch Management creates a Patch Fingerprint Profile that includes all missing patches for that machine, ensuring the continued compliance of each end-point. Each end-point is then continually monitored to make sure it stays patched. Administrators can also establish a mandatory baseline to automatically 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 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.

**Table 1-1** ZENworks Patch Management Features

Feature	Description
Patented multi-platform patch management	Enables security of all operating systems and applications within heterogeneous networks, including Windows (32 and 64-bit) and Linux distributions later this year. 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

Feature	Description
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 administrator(s) for proactive security and administrative management
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
Flexible application reporting	Delivers multiple patches to multiple computers in one distribution to increase IT productivity
Flexible application reporting	Audits and reports on the status of the organization's security
Policy-based administration	Ensures that all systems meet a mandatory baseline policy—a key aspect of regulatory compliance

# Using Novell ZENworks Patch Management

# 2

## 2.1 Using the ZENworks Patch Management Home Page

### 2.1.1 Viewing and Configuring Subscription Information

ZENworks® Configuration Management provides current information about your subscription status and allows you to activate and configure your subscription. The following sections further introduce you to the capabilities of ZENworks Configuration Management:

- ♦ “Viewing Subscription Service Information” on page 14
- ♦ “Activating/Viewing the Subscription Serial Number” on page 18
- ♦ “Configuring Http Proxy Details” on page 22
- ♦ “Configuring Subscription Download Details” on page 24

## Viewing Subscription Service Information

To view the current subscription service information:

1. Click the *Configuration* tab in the left panel. The *Configuration* page appears as shown in the following figure.

**Figure 2-1** Configuration Page

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

- Click *Patch Management Services*. Four hyperlinks—*Subscription Service Information*, *Product Serial Number*, *Configure Http Proxy*, and *Subscription Download*—are displayed as shown in the following figure.

**Figure 2-2** *Patch Management Services*

Configuration	Registration	System Information	Asset Inventory	System Updates
Management Zone Settings				
Content				
Device Management				
Discovery and Deployment				
Event and Messaging				
Infrastructure Management				
Inventory				
Reporting Services				
Patch Management Services				
Category	Description			Is Configured
<a href="#">Subscription Service Information</a>	View subscription log and update subscription settings			No
<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				Advanced
User Sources				

- Click the *Subscription Service Information* hyperlink. The *Subscription Information* page appears, as shown in the following figure.

**Figure 2-3** Figure 2-3 Subscription Information Page

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

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

The following table describes each status item featured on the *Subscription Information* page.

**Table 2-1** Subscription Service Information Status Items

Status Item	Definition
Start the Subscription Service	Enables you to select a server from multiple servers in your management zone. You need to select a server from the drop-down and click the Start button to start the subscription service.  <b>NOTE:</b> Once the subscription service starts running, the Start button reads Service Running.
Last Subscription Poll	The time of the last successful update
Subscription Replication Status	Latest status of the process of replication
Account Id	Key created by the ZENworks Server, which is passed to the ZENworks Patch Management Subscription Service and used to validate the update request
Subscription Host	The address of the ZENworks Patch Management Subscription Service



Status Item	Definition
Subscription Communication Interval (Every Day at)	The frequency of agent communication with ZENworks Patch Management Subscription Service for retrieving updates

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

**Table 2-2** Buttons on the Subscription Information Page

Button	Action
OK	Enables you to go back to the Configuration page
Apply	Enables you to save the changes made to the Subscription Communication Interval
Reset	Enables you to reset the replication status and initiates a complete replication with the ZENworks Patch Management Subscription Service
Cancel	Enables you to cancel the last action performed

The *Subscription Service History* section displays the activity log of the subscription activities. Table 2-3 describes each item featured in this section.

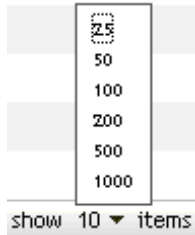
**Table 2-3** Table 2-3 ZENworks Subscription Service History Items

Item	Definition
Type	Subscription type defined for your account namely Vulnerability (Subscription Replication) and License.
Status	Status of replication—when replication begins, the status reads <i>Initializing Replication</i> . When replication ends, the status reads <i>Completed</i> .
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.

You can refresh the subscription information by clicking the Action drop-down 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 on the show items drop-down and selecting the desired number, as shown in the following figure.



## Activating/Viewing the Subscription Serial Number

To activate your paid subscription or view your subscription serial number, repeat steps 1 and 2 in the *Viewing Subscription Service Information* section mentioned earlier and do as follows:

- Click the *Product Serial Number* hyperlink. The *Subscription Serial Number* page appears, as shown in the following figure.

**Figure 2-4** Subscription Serial Number Page

[Configuration](#) > **Subscription Serial Number**

Subscription Serial Number

Please enter your ZENworks Patch Management serial number, company name and email address in order to activate your paid subscription

Product Serial Number

Serial Number

Company Name

Email Address

Total Non-Expired Licenses

Product Serial Number

Action

Description	Purchase Date	Vendor	Effective Date	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.

**NOTE:** ZENworks Configuration Management provides a 60-day free trial. Therefore, during the trial period the *Product Serial Number* panel will not display any details. To continue using the

patch management features of the ZENworks Control Center, at the end of your 60-day free trial, you must enter a valid subscription serial number for ZENworks Patch Management along with the company name and email address. On entering the required details, the license record will be displayed with its description, purchase date, vendor, effective date, and expiration date.

---

**NOTE:**

- ♦ 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 the following URL: <https://novell.patchlink.com/update>.
  - ♦ The ZENWorks Patch Management content distribution network is a global cache infrastructure with many servers. Downloading patches from this network requires port 80 (HTTP) access to the following URL: <http://cdn.patchlink.com/novell>.
  - ♦ To download patches, you must provide Internet access to both [novell.patchlink.com](https://novell.patchlink.com) and [cdn.patchlink.com](http://cdn.patchlink.com) through the external firewall / proxy infrastructure.
  - ♦ It is recommended that you use nslookup to discover the local IP address for your nearest content distribution node. For example, typing “nslookup [cdn.patchlink.com](http://cdn.patchlink.com)” will display the local IP address for the content distribution node. Allow access to that specific local address through the firewall. These IP addresses will be in the 208.111.128.0/18 range.
- 

**IMPORTANT:** If you are upgrading from a prior version of ZENworks Patch Management, you can use your existing patch management subscription serial number once your ZENworks Patch Management 6.3 server has been uninstalled.

---

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

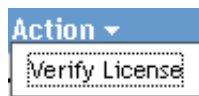
**Table 2-4** ZENworks Subscription Serial Number Items

Item	Definition
Serial Number	ZENworks Patch Management license number (serial number)
Company Name	Name of the company that ZENworks Patch Management is registered to
Email Address	Email address, which you can use for receiving alerts and for future communication
Total Non-Expired Licenses	Total number of active licenses. Each registered device requires one license
Description	The description of the license or the name of the license

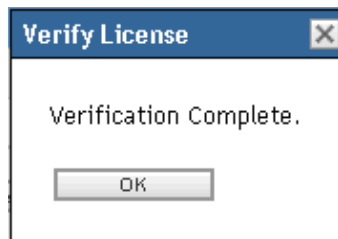
---

Item	Definition
Purchase Date	The date the license group was purchased
	<p><b>NOTE:</b> A license group is a block of licenses purchased at a time. For example, you can have 3 license groups comprising 500 total licenses with a group of 300 licenses purchased initially, and two additional groups of 100 licenses each added each subsequent quarter.</p>
Vendor	The source from where the license was purchased
Effective Date	The date the license(s) come into effect. This date may not necessarily be the installation date.
Expiration	The date the license(s) expire(s). Typically, licenses expire one calendar year from the date of purchase
Purchased	The total number of licenses purchased with the product

You can verify the license by clicking the Action drop-down on the *Subscription Serial Number* page and selecting *Verify License*. The *Verify License* message box appears, as shown in the following figures.



**Figure 2-5** *Verify License Message Box*



This *Verify License* message box indicates that the verification of the subscription license is complete.

**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 2-5** *Buttons on the Subscription Serial Number Page*

Button	Action
OK	Enables you to go back to the Configuration page
Apply	Enables you to save the information entered in the page
Reset	Enables you to reset the replication status and initiates a complete replication with the ZENworks Patch Management Subscription Service
Cancel	Enables you to cancel the last action performed

## Configuring Http Proxy Details

To configure Proxy Server details, repeat steps 1 and 2 in the *Viewing Subscription Service Information* section mentioned earlier and do as follows:

- Click the *Configure Http Proxy* hyperlink. The *Proxy Server Details* page appears, as shown in the following figure.

**Figure 2-6** Proxy Server Details Page

[Configuration](#) > **Proxy Server Details**

**Proxy Server Details**

Configure Proxy Server to allow PatchManagement to download subscription services over internet.

**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 to download subscription service over the Internet.

The following table describes each field on the *Proxy Server Details* page.

**Table 2-6** Items in Proxy Server Details Page

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

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

**Table 2-7** *Buttons on the Proxy Server Details Page*

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

## Configuring Subscription Download Details

To configure the Subscription Download details, repeat steps 1 and 2 in the *Viewing Subscription Service Information* section earlier and do as follows:

- Click the *Subscription Download* hyperlink. The *Subscription Download Options* page appears, as shown in the following figure.

**Figure 2-7** *Subscription Download Options Page*

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

**Subscription Download Options** [X]

Configure download options for all the supported platforms.

---

**Subscription Download** [^]

☒ **Microsoft Windows (X86)**

**Select Operating System**

☒ XP ☐ 2000 ☐ 2003 ☐ Vista

**Choose your language options**

☒ English(en) ☐ Portuguese(pt) ☐ French(fr) ☐ Italian(it) ☐ German(de)

☐ Spanish(es) ☐ Japanese(jp) ☐ Taiwanese(zh\_tw) ☐ Chinese(zh\_cn) ☐ Korean(ko)

☐ **Microsoft Windows (X86-64)**

**Select Operating System**

☒ XP ☐ 2000 ☐ 2003 ☐ Vista

**Choose your language options**

☒ English(en) ☐ Portuguese(pt) ☐ French(fr) ☐ Italian(it) ☐ German(de)

☐ Spanish(es) ☐ Japanese(jp) ☐ Taiwanese(zh\_tw) ☐ Chinese(zh\_cn) ☐ Korean(ko)

OK Apply Reset Cancel

The *Subscription Download Options* page allows you to configure the subscription download options for the ZENworks primary server. You can select the operating system(s) and the language(s) 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 selected operating system (s) and language (s) will be 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 as 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 have to be disabled in the *Vulnerabilities* tab.

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

**Table 2-8** *ZENworks Subscription Download Option Items*

Item	Description
Microsoft Windows (X86)	Family of Operating Systems that include XP, 2000, 2003, and Vista



Item	Description
Choose your language options	Enables you to select the language of patches you wish to download. For example, if you select the French (fr) check box, only French language patches will be downloaded.
Microsoft Windows (X86-64)	Family of Operating Systems that include XP, 2000, 2003, and Vista
Choose your language options	Enables you to select the language of patches you wish to download. For example, if you select the French (fr) check box, only the French language Patches will be downloaded

The following figure describes the action of each button on the page.

**Table 2-9** *Buttons on the Subscription Download Options Page*

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



# Using Vulnerabilities

# 3

The Vulnerabilities page (see Figure 3-1) is where the majority of patch management activities are performed. This page lists all patch-related vulnerabilities across all systems registered to the ZENworks® Patch Management Server. The page displays the name, description, impact, and statistics of the vulnerabilities.

- ♦ [Section 3.1, “About Vulnerabilities,” on page 27](#)
- ♦ [Section 3.2, “Using the Vulnerabilities Page,” on page 28](#)

## 3.1 About Vulnerabilities

A vulnerability is a patch that a software or application in a network device requires to keep it updated and secure. 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 software vendors. Once reported and analyzed, the vulnerabilities are registered for distribution to your ZENworks Patch Management Server through the ZENworks Patch Subscription Service. The ZENworks Adaptive Agent installed on each device checks for known vulnerabilities. Called the Discover Applicable Updates (DAU), this task returns the results 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.

- ♦ [Section 3.1.1, “Viewing Vulnerabilities,” on page 27](#)

### 3.1.1 Viewing Vulnerabilities

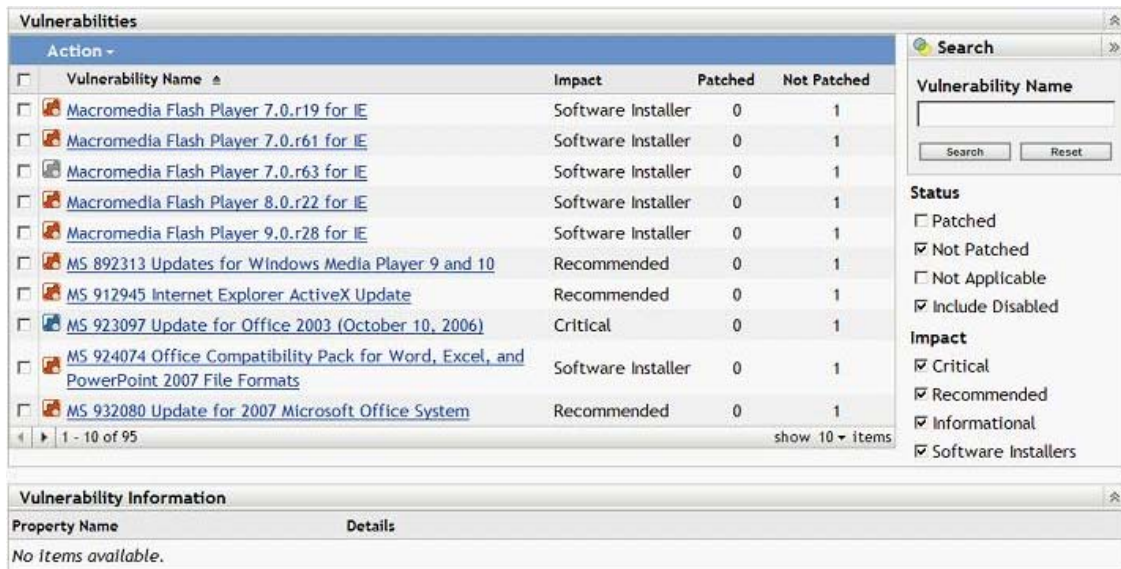
To view the vulnerabilities in ZENworks Configuration Management:

1. Click the Vulnerabilities tab on the left panel, as shown in the following figure.



The vulnerabilities are displayed in a page, as shown in Figure 3-1.

Figure 3-1 Vulnerabilities Page



## 3.2 Using the Vulnerabilities Page

The Vulnerabilities Page comprises the following three sections:

- ♦ Vulnerabilities
- ♦ Vulnerabilities Information
- ♦ Search
- ♦ Section 3.2.1, “Vulnerabilities,” on page 28
- ♦ Section 3.2.2, “Vulnerability Information,” on page 31
- ♦ Section 3.2.3, “Searching Vulnerability,” on page 33

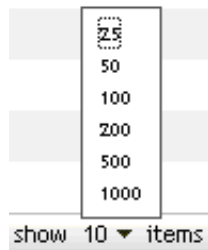
### 3.2.1 Vulnerabilities

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.

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



## Vulnerability Name

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.

[Adobe Acrobat Reader 6.0.6 Update](#)

## 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 example, the total number of available vulnerabilities is 979.

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 therefore, should be installed as soon as possible. Most of the recent security updates fall in to this category. ZENworks Patch Management 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 specially recommends vulnerabilities that fall in to this category.
- ♦ Informational: This type of vulnerability detects a condition that Novell has determined as informational. However, you can install it at your discretion if this type of vulnerability has an associated bundle.
- ♦ Software Installers: These types of vulnerabilities are software applications. Typically, this includes software installers. The vulnerabilities will show not patched if the application has not been installed on a machine.

## Vulnerability Statistics




Vulnerability statistics shows the relationship between a specific vulnerability and the total number of devices (or groups) within ZENworks Patch Management Server that meet a specific status. The

vulnerability statistics appear in two columns on the extreme right side of the Vulnerability Page. Each column status is described as follows.

- ♦ Patched: This column displays the total number of devices to which the corresponding vulnerability has been applied or patched.
- ♦ Not Patched: This column displays the total number of devices to which the corresponding vulnerability has not been applied or patched.

The Vulnerabilities shown in the Vulnerabilities page have different icons against their names indicating their current status. The following table describes the significance of the icons that appear against each Vulnerability.

**Table 3-1** *Vulnerability Icons*

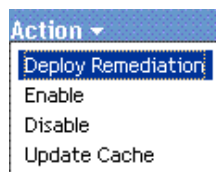
Vulnerability Icon	Significance
	Indicates the Vulnerabilities that are disabled.
	Indicates that the fingerprint information for the vulnerability has been brought down. Therefore, this icon represents the Vulnerabilities that are not cached.
	Indicates that the fingerprints and packages necessary to address the vulnerability have been cached into the system. Therefore, this icon represents the Vulnerabilities that are cached and ready for deployment.

**NOTE:** If you choose a vulnerability that does not have cached files, it is not automatically deployed to devices. You must download the files from the patch repository 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 Actions menu.

### Action Menu Items

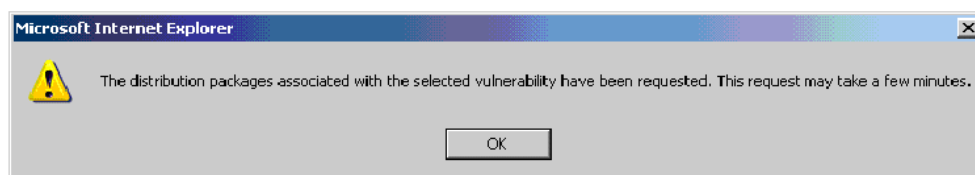
The Vulnerabilities section also features an Action menu, which enables you to perform one of four actions on the vulnerabilities listed in the page. Figure 3-2 shows the four options in the Action menu.

**Figure 3-2** *Action Menu Items*



The Action menu consists of the following four options:

- ◆ **Deploy Remediation:** This option enables you to deploy a patch. To use this option, select the checkbox/s for the vulnerability/s you require to deploy and select Deploy Remediation from the Action menu options to open the Deploy Remediation Wizard.
- ◆ **Enable:** This option allows you to enable a disabled vulnerability.
- ◆ **Disable:** This option enables you to disable a vulnerability. To use this option, select the checkbox for the required vulnerability and select Disable. The selected vulnerability is removed from the list.
- ◆ **Update Cache:** This option initiates a process that gathers the bundles associated with the selected vulnerability and places those bundles on your ZENworks Patch Management Server. To use this option:
  - ◆ Select one or multiple vulnerabilities in the Vulnerabilities list.
  - ◆ In the Action menu, click Update Cache. A Warning dialog box appears as shown in the following figure prompting you to confirm the request for update and informing you that this action may take an extended period of time.



- ◆ Click OK.

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.



### 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 that vulnerability in the Vulnerability Information section.

For example, if you select the vulnerability called Adobe Acrobat Reader 7.0.1 Update from the list of vulnerabilities, the Vulnerability Information section displays the result of a vulnerability analysis for the selected vulnerability, as shown in Figure 3-3.

**Figure 3-3** *Vulnerability Information for 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

Table 3-2 below defines each property name in the Vulnerability Information section.

**Table 3-2** *Property Names in Vulnerability Information Section*

Property Name	Definition
Name	The name of the vulnerability
Remediation Bundles	The number of bundles associated with each vulnerability
Impact	The impact of the vulnerability as determined by Novell. See Vulnerability Impacts
Distribution Bundle Status	The status of the bundle – can be Cached or Not Cached
Status	Status of the vulnerability - can be "Enabled" or "Disabled"
Vendor	The name of the vendor or manufacturer
Modified On	The date the vulnerability was last modified
Released On	The date the vulnerability was released
Vendor Product ID	The ID number given to the product by the vendor



Property Name	Definition
Description	The description of the vulnerability; includes the advantages of deploying the vulnerability and the pre-requisites for deployment

### 3.2.3 Searching Vulnerability

The Search section in the Vulnerabilities page offers extensive search and data filtering options that allow you to search for specific vulnerabilities and filter result sets based on "Status" and "Impact" of the vulnerabilities. Searching and filtering can be performed independent of each other or can be combined to provide extensive drill-down capabilities. Figure 3-4 shows the Vulnerability Search section.

To search a vulnerability:

1. Enter full or part of the vulnerability name in the Vulnerability Name textbox.
2. Select the required checkbox under "Status" and "Impact."
3. Click Search.

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

**Figure 3-4** Search Section in Vulnerabilities Page

The screenshot shows a web interface for searching vulnerabilities. At the top is a 'Search' window with a title bar. Inside, there's a 'Vulnerability Name' label above a text input field. Below the input field are two buttons: 'Search' and 'Reset'. Underneath the search window, there are two sections: 'Status' and 'Impact'. The 'Status' section has four checkboxes: 'Patched', 'Not Patched', 'Not Applicable', and 'Include Disabled'. The 'Impact' section has four checkboxes: 'Critical', 'Recommended', 'Informational', and 'Software Installers'.

Table 3-3 describes the result of selecting each filter option under Status.

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

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

Table 3-4 describes the result of selecting each filter option under Impact.

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

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

# Working with Deployments

# 4

## 4.1 Using the Deploy Remediation Wizard

The Deploy Remediation Wizard provides an interface to create or edit deployment schedules for multiple recipients or devices. The Wizard assists in device selection, deployment scheduling, and if required, setting recurrences.

You can access the Deploy Remediation Wizard from the Device or Vulnerabilities tab.

- ♦ [Section 4.1.1, “Confirming the Device,” on page 36](#)
- ♦ [Section 4.1.2, “Accepting License Agreement,” on page 37](#)
- ♦ [Section 4.1.3, “Setting Remediation Schedule,” on page 38](#)
- ♦ [Section 4.1.4, “Setting Remediation Options,” on page 48](#)
- ♦ [Section 4.1.5, “Setting Advanced Remediation Options,” on page 49](#)
- ♦ [Section 4.1.6, “Setting Deployment Order and Behavior,” on page 51](#)
- ♦ [Section 4.1.7, “Notification and Reboot Options,” on page 52](#)
- ♦ [Section 4.1.8, “Deployment Summary,” on page 53](#)

---

**NOTE:** Using the Deployment wizard, you can select multiple vulnerabilities, and the wizard will automatically select all of the devices and vulnerabilities required and if devices are selected, the wizard will automatically select all vulnerabilities.

---

---

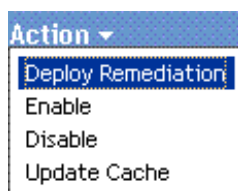
**NOTE:** In the case, you select a single vulnerability and choose "View Vulnerability" from the task menu, and from the next page onwards you select a device and click "Deploy Remediation", the first page in the Wizard is not displayed since the device has already been selected.

---

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

1. Click the Vulnerabilities tab and select the vulnerability that you require to deploy to one or more devices.
2. Select Deploy Remediation from the Action menu in the Vulnerabilities page, as shown in Figure 4-1. The Confirm Devices page appears as shown in Figure 4-2.

**Figure 4-1** Action Menu Items



### 4.1.1 Confirming the Device

The Confirm Devices page (see Figure 4-2) allows you to select and confirm the devices to which you require to schedule a deployment. Confirming the device is the first step in scheduling a deployment for a selected vulnerability and therefore, the Confirm Devices page says 'Step 1'.

**Figure 4-2** *Confirm Devices Page*

The screenshot shows the 'Confirm Devices' page. At the top, there's a tab labeled 'Vulnerabilities' and a sub-header 'Step 1: Confirm Devices' with a small icon. Below this, a message states: 'Remedies will be deployed to the following devices. Please deselect any devices that should not be patched.' A table follows with columns: Device Name, Status, Platform, DNS, and IP Address. The first row shows a device named 'zpmbeta4' with status 'Online', platform 'Windows', DNS 'ZPMBETA4', and IP '192.168.1.145'. Below the table, it says '1 - 1 of 1' and 'show 10 items'. At the bottom, there are three buttons: '<< Back', 'Next >>', and 'Cancel'.

<input type="checkbox"/>	Device Name	Status	Platform	DNS	IP Address
<input checked="" type="checkbox"/>	zpmbeta4	Online	Windows	ZPMBETA4	192.168.1.145

1 - 1 of 1 show 10 items

<< Back Next >> Cancel

Table 4-1 describes the column headings in the Confirm Devices page.

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

Column Heading	Description
Device Name	The name of the device registered with ZENworks® (to which the vulnerability is to be deployed)
Status	The status of the device. The status can be 'Offline' or 'Online'.
Platform	The Operating System of the device
DNS	The IP address of the DNS server
IP Address	The IP address of the device

The total number of devices to which the selected vulnerability would be deployed is displayed in the page. In the following example, the total number of devices is 5.

**Figure 4-3** *Total Number of Vulnerabilities*

The screenshot shows a small box containing the text '1 - 5 of 5'.

1 - 5 of 5

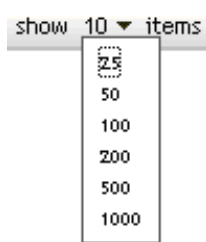
You can sort the devices in ascending and descending alphabetical order. To sort, click the arrow in the column heading "Device Name" as shown in Figure 4-4.

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



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

**Figure 4-5** *Show Items*



3. Deselect the devices to which you do not require to deploy the vulnerability.

---

**NOTE:** By default, all the devices are selected for deployment

---

4. Click the Next button. The License Agreement page appears as shown in Figure 4-6.

---

**NOTE:** If you click the Cancel button, the Wizard will abort and you will go back to the Vulnerabilities page.

---


### 4.1.2 Accepting License Agreement

The License Agreement page displays all the 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 and therefore, the License Agreement page says 'Step 2'.


**Figure 4-6** License Agreement Page



[Vulnerabilities](#) > **Deploy Remediation**


Vulnerabilities

 **Step 2: License Agreement**

Please review all the licenses individually and accept or decline. Only patches with accepted license agreement will be deployed. You must accept at least one license agreement.

Required license lists 	Accept	Decline
<a href="#">Adobe Acrobat Reader 6.0.2 update</a>	<input type="radio"/>	<input checked="" type="radio"/>

  1 - 1 of 1

show 10  items

License Agreement

<< Back

Next >>

Cancel

5. Select the Accept radio button for the license agreements you require to accept.

---

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

---

---

**NOTE:** If you want to return to the previous page, click the Back button.

---

---

**NOTE:** If you want to abort the Wizard, click the Cancel button.

---

6. Click the Next button. The Remediation Schedule page appears as shown in Figure 4-7.


### 4.1.3 Setting 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 and therefore, the Remediation Schedule page says 'Step 3'. See Figure 4-7.

**Figure 4-7** Remediation Schedule Page

[Vulnerabilities](#) > **Deploy Remediation**

Vulnerabilities

 **Step 3: Remediation Schedule**

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

Schedule Type:

---

To start with setting the remediation options, you need to select the Schedule type. ZENworks Configuration Management offers three types of schedules to determine when the patch(s) will actually be applied to the target device:


- ◆ **Date Specific:** Selecting Date Specific will schedule the deployment of remediation to your selected devices according to the selected date.
- ◆ **Recurring:** Selecting Recurring will start the deployment on the selected day at selected time, repeat the deployment every day/week/month, and if defined, end on a specific date.
- ◆ **Event:** Selecting the Event will trigger the scheduled deployment when a particular event (chosen from a given list of events) takes place.

#### 4.4.4.1 Setting Remediation Schedule – Date Specific

When you select Date Specific, the Remediation Schedule page appears as shown in Figure 4-8.

**Figure 4-8** Remediation Schedule Page for Date Specific Schedule Type


**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 2:11 PM )

<< Back

Next >>

Cancel

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

- ◆ Start Date(s): This option enables you to pick the date on which you require to start the deployment. To do so, click the symbol  to open up the calendar and pick the date on which you require to schedule the deployment. To remove the selected date, click the symbol .
- ◆ Run event every year: Selecting this check box will ensure 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 will ensure 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 to enable you to select the start time of the schedule execution namely, Start immediately at Start Time and Start at a random time between Start Time and End Time.
  - ◆ 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 require to set the start time in the start time panel shown as follows.



Start Time: 1 : 00 am

- ♦ Start at a random time between Start Time and End Time: Selecting this option activates the End Time panel besides the Start Time panel. You can specify the end time and the start time such that the deployment will occur at any random time between them. The End Time panel is shown as follows:

End Time: 1 : 00 am

---

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

---

**NOTE:** 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 local time.

---

#### 4.4.4.2 Setting Remediation Schedule – Recurring

When you select Recurring, the Remediation Schedule page appears as shown in Figure 4-9.

**Figure 4-9** Remediation Schedule Page for Recurring Schedule Type

---

Schedule Type:  
Recurring

☒ **When a device is refreshed**

☐ Delay execution after refresh: 0 Days, 0 Hours, 0 Minutes

☐ **Days of the week**

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

Start Time: 1 : 00 am

[More Options](#)

☐ **Monthly**

☒ Day of the month: 1

☐ Last day of the month

☐ First Sunday +

Start Time: 1 : 00 am

[More Options](#)

☐ **Fixed Interval**

0 Months, 0 Weeks, 0 Days, 0 Hours, 0 Minutes

Start Date: 5/17/07 📅 Start Time: 1 : 00 am

[More Options](#)

---

<< Back Next >> Cancel

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

- ◆ **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 after a specific time. The check box Delay execution after refresh enables you to set the 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.

☒ Delay execution after refresh: 0 Days, 0 Hours, 0 Minutes

**NOTE:** The device will be refreshed based on the settings mentioned in 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. See Figure 4-10.

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

☒ **Days of the week**

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

Start Time:  :

[More Options](#)

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

If you click the link More Options shown in Figure 4-10, additional deployment options will appear as shown in Figure 4-11. Clicking the link Hide Options will hide the additional deployment options and show only the default deployment options.

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

☒ **Days of the week**

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

Start Time:  :

[Hide Options](#)


☐ Process immediately if device unable to execute on schedule


☐ Use Coordinated Universal Time ( Current UTC 2:25 PM )

☐ Start at a random time between Start and End Times

End Time:  :

☐ Restrict schedule execution to the following date range:

Start Date:  

End Date:  


**NOTE:** 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 local time.

---

**NOTE:** Selecting the Start at a random time between Start Time and End Time check box activates the End Time panel besides the Start Time panel. You can specify the end time and the start time such that the deployment will occur at any random time between them.

---

**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 day(s) 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.

---


- ♦ Monthly: This option enables you to specify the monthly deployment options. See Figure 4-12.

**Figure 4-12** Monthly Deployment Options – Default

☒ **Monthly**

☒ Day of the month:

☐ Last day of the month


☐   


Start Time:  :

[More Options](#)

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

- ♦ Days of the month: 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.

☒   

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

<input checked="" type="radio"/>	Second	Sunday	
	First	Sunday	

---

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

---

If you click the link More Options in Figure 4-12, additional deployment options will appear as shown in Figure 4-13. Clicking the link Hide Options will hide the additional deployment options and show only the default deployment options.

**Figure 4-13** *Monthly Deployment Options – All*

☒ **Monthly**

☒ Day of the month:

☐ Last day of the month

☐

First	Sunday	
-------	--------	--

Start Time: 

1	:00	am
---	-----	----

[Hide Options](#)

☐ Process immediately if device unable to execute on schedule

☐ Use Coordinated Universal Time ( Current UTC 2:25 PM )

☐ Start at a random time between Start and End Times

End Time: 

1	:00	am
---	-----	----

☐ Restrict schedule execution to the following date range:

Start Date: 

7/1/07	
--------	--

End Date: 

7/1/07	
--------	--

---

**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 day(s) 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 Interval:** This option enables you to schedule a recurring deployment at a fixed time interval. In this option, you can specify both the monthly and weekly intervals. 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 Figure 4-14.

**Figure 4-14** Fixed Deployment Options - Default

☒ **Fixed Interval**

Months,  Weeks,  Days,  Hours,  Minutes

Start Date:   Start Time:  :  :


[More Options](#)

If you click the link More Options in Figure 4-14, additional deployment options will appear as shown in Figure 4-15. Clicking the link Hide Options will hide the additional deployment options and show only the default deployment options.

**Figure 4-15** Fixed Deployment Options - All

☒ **Fixed Interval**

Months,  Weeks,  Days,  Hours,  Minutes


Start Date:   Start Time:  :  :

[Hide Options](#)

☐ Process immediately if device unable to execute on schedule

☐ Use Coordinated Universal Time

☐ Restrict schedule execution to the following date range:


End Date:   End Time:  :  :   
( Current UTC 2:25 PM )

#### 4.4.4.3 Setting Remediation Schedule – Event

When you select Event, the Remediation Schedule page appears as shown in Figure 4-16.

**Figure 4-16** Remediation Schedule Page for Event Schedule Type

**Vulnerabilities**

 **Step 3: Remediation Schedule**

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

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 schedule type 'Event' features a list of events from which you can select one such that when the selected event occurs, the deployment is executed.

Table 4-2 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 ZENworks Configuration Management.

Event	Action
ZENworks – Logout	Deployment remediation occurs whenever the user logs out of ZENworks Configuration Management.
Device Connecting to Network (Windows Only)	Deployment remediation occurs whenever the device tries to connect to any machine (Windows Only) in the network.

8. Click the Next button. The *Remediation Options* page appears as shown in Figure 4-17

**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) time and time zone settings are correct.

**NOTE:** To return to the previous page click the Back button. To abort the Deployment Remediation Wizard, click the Cancel button.

#### 4.1.4 Setting 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.

**Figure 4-17** Remediation Options Page

**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 Options	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 will remain in a dirty state until you perform a reboot.
Advanced (Standard - Set Individually)	Uses the QChain and reboot settings defined for each vulnerability.

**NOTE:** If the deployment is not QChain enabled and the reboot is suppressed then the agent will be in the Dirty R state. Agents in the Dirty R state will only accept one of the reboot deployments. Therefore, for uninterrupted mandatory baseline patching, ensure you do not select the without reboot option. In addition, you should ensure there are no patches in the baseline that require a login after patch installation.


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

## 4.1.5 Setting Advanced Remediation Options




The Advanced Remediation Options page as shown in Figure 4-18 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 in the page represent the patch flags that can be set for each package.

**Figure 4-18** Advanced Remediation Options Page

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			
Macromedia Flash Player 7.0.r61 for IE	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Macromedia Flash Player 7.0.r63 for IE	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Macromedia Flash Player 8.0.r22 for IE	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Macromedia Flash Player 9.0.r28 for IE	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

◀

▶

1 - 4 of 4








show 10 ▼ items

<< Back

Next >>

Cancel

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

Icon	Behavior Functionality
	Sets the vulnerability as chainable (provided the vulnerability supports chaining)
(Chain Packages)	
	Runs the vulnerability installation in debug mode
(Debug Mode)	
	Sets the installer to function in quiet mode. Quiet mode suppresses any user interfaces (in the event a user is logged in) during the remediation
(Quiet Mode)	
	Indicates that this vulnerability requires a reboot prior to completing the installation
(Reboot is Required)	
	Suppresses the reboot, allowing other chained vulnerabilities to be sent following this vulnerability
(Suppress Chained Reboot)	<p><b>TIP:</b> It is recommended that you suppress the final reboot for all chained packages, then send a reboot deployment when all packages are finished</p>
	Prevents the computer from rebooting after installation of the package
(Suppress Reboot)	
	Uninstalls the packages instead of an installation.
(Uninstall)	

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 abort the Wizard.

## 4.1.6 Setting 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. See Figure 4-19.

**Figure 4-19** *Deployment Order and Behavior Page*

**Vulnerabilities**

**Step 6: Deployment Order and Behavior**

Choose the deployment Order and Behavior

<input type="checkbox"/>	Package Name	Order	Reboot
<input type="checkbox"/>	Macromedia Flash Player 7.0.r61 for IE	1	No

1 - 1 of 1      show 10 ▼ items

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 besides 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.

Table 4-4 describes the actions of the various buttons in the Deployment Order and Behavior page.

**Table 4-4** *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 by one place
	Moves the Vulnerability down by one place
	Moves the Vulnerability to the bottom of the listing

9. Click the *Next* button. The Notification and Reboot Options page appears as shown in Figure 4-20.

---

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

---

To return to the previous page click the *Back* button. To abort the Wizard click *Cancel*.

### 4.1.7 Notification and Reboot Options

The Notification and Reboot Options page of the Deploy Remediation Wizard, allows you to define whether users will receive notification of these deployments and/or reboots, and if so, what the notification will contain. Setting the notification and reboot options is the seventh step in scheduling a deployment for a selected vulnerability. See Figure 4-20.

**Figure 4-20** Notification and Reboot Options Page

**Vulnerabilities**

**Step 7: Notification and Reboot Options**

Select Notification and Reboot Options

**Define Reboot Options**

☒ Notify Users

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

☒ Edit Default Settings

Options	Yes	No
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 checked="" type="radio"/>	<input type="radio"/>

<< Back   Next >>   Cancel

**Notify Users:** If selected, the user will be notified prior to the installation of this deployment. The user will see a message when notified about this deployment.

**Message Box:** This field contains the message you will see when notified about this deployment.

**Edit Default Settings:** When selected, the default settings for each agent will be used. Selection of this option disables all other reboot notification options and enables you to edit the default settings.

**Options:** When defining reboot options you can specify, for each option, whether

to use the values defined in the default settings (by selecting the Edit Default Settings check box) or the custom settings. There are three options available as follows:

- ♦ 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 allows the user to ensure that notifications will be given by the Novell® 'Z' agent.

---

**NOTE:** To return to the previous page click the *Back* button. To abort the Deployment Remediation Wizard, click the *Cancel* button.

---

10. Click the *Next* button to proceed to the Deployment Summary page as shown in Figure 4-21.

### 4.1.8 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. See Figure 4-21.

**Figure 4-21** Deployment Summary Page

**Vulnerabilities**

**Step 8: Deployment Summary**

Please review summary and then press finish.

Property Name	Details
<b>Schedule</b>	Recurring
<b>Total selected packages</b>	1
<b>Total selected devices or groups</b>	1

Order	Package Name	Reboot	Total Devices
1	Macromedia Flash Player 7.0.r61 for IE	No	1

<< Back   Finish   Cancel

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

- ♦ Schedule: This is the schedule selected for the deployments (as defined under the Remediation Schedule page).
- ♦ Total Selected Packages: This is the total number of vulnerabilities selected for the deployment.
- ♦ Total Selected Devices or Groups: This is the total number of devices selected for deployment.
- ♦ Order: This is the deployment order selected for deployment of the vulnerabilities as defined under the Deployment Order and Behavior page.

- ♦ **Total Devices:** This is the total number of devices to which the selected vulnerability has been deployed.
- ♦ **Package Name:** This is the name of the vulnerability you have selected for deployment.
- ♦ **Reboot:** This is the reboot setting of the selected vulnerability as defined in the Deployment Order and Behavior page.

11. Click the *Finish* button to complete the process of scheduling the deployment of a selected vulnerability.

---

**NOTE:** To return to the previous page click the *Back* button. To abort the Deployment Remediation Wizard, click the *Cancel* button.

---

# 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 the Novell® ZENworks® Patch Management mandatory baselines:

- ♦ [Section 5.1, “About Mandatory Baselines,” on page 55](#)
- ♦ [Section 5.2, “Working with Mandatory Baselines,” on page 59](#)

## 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 the device is patched back into compliance.

---

**NOTE:** 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 stringent *Content Blackout Schedule* is in effect, do not apply mandatory baselines to groups of mission critical servers or other devices where unscheduled reboots would disrupt daily operations.

---

---

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

---

When a mandatory baseline is created or modified:

- ♦ The ZENworks® Patch Management Server automatically schedules a *Discover Applicable Updates (DAU)* task for all machines in that group.
- ♦ Patch Management Server determines which systems are applicable and out of compliance (based upon the vulnerabilities added to the baseline) following the *DAU* task.
- ♦ Necessary bundles, as defined in the baseline, are deployed as soon as possible for each machine.

---

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



---

### 5.1.1 Viewing Mandatory Baselines

To view 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 Figure 5-1.

**Figure 5-1** Root Folders of Device Groups

Discovered			Inventoried	Managed
Devices				
<div> <div></div> <div>Action ▾ Quick Tasks ▾</div> <div></div> </div>				
<input type="checkbox"/>	Name ▲	Type	Last Contact	
<input type="checkbox"/>	 <a href="#">Servers (Details)</a>	Folder		
<input type="checkbox"/>	 <a href="#">Workstations (Details)</a>	Folder		
1 - 2 of 2			show 25 ▾ items	

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.

- Click the *Server* or *Workstation* link. A list of server or workstation groups classified on the basis of their operating systems appears. Figure 5-2 shows a list of server groups, by way of an example.

**Figure 5-2** List of Server Groups

Servers

New ▾

Edit ▾

Delete

Action ▾

Quick Tasks ▾

<input type="checkbox"/>	Status	Name ▲	Operating System	Type	Last Contact
<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="#">zenbeta3</a>	win2003-ee-sp1-x86	Server	5/18/07 4:57 PM

1 - 3 of 3

show 25 ▾ items

- In 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. Figure 5-3 shows such a page that appears when a Dynamic Server Group called 'Windows Server 2003' is selected.



**Figure 5-3** General Details and Member(s) of the Windows Server 2003 Group















4. Click the *Vulnerabilities* tab. The vulnerabilities applicable to the member device (s) 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 Figure 5-4.

**Figure 5-4** Device Group Vulnerabilities Page for the Selected Server Group

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

 **Windows Server 2003**

Summary Relationships Details <b>Vulnerabilities</b>				
Vulnerabilities				
Action ▾				
<input type="checkbox"/>	Vulnerability Name 	Impact	Patched	Not Patched
<input type="checkbox"/>	 <a href="#">Macromedia Flash Player 7.0.r19 for IE</a>	Software Installer	0	1
<input type="checkbox"/>	 <a href="#">Macromedia Flash Player 7.0.r61 for IE</a>	Software Installer	0	1
<input type="checkbox"/>	 <a href="#">Macromedia Flash Player 7.0.r63 for IE</a>	Software Installer	0	1
<input type="checkbox"/>	 <a href="#">Macromedia Flash Player 8.0.r22 for IE</a>	Software Installer	0	1
<input type="checkbox"/>	 <a href="#">Macromedia Flash Player 9.0.r28 for IE</a>	Software Installer	0	1
<input type="checkbox"/>	 <a href="#">MS 892313 Updates for Windows Media Player 9 and 10</a>	Recommended	0	1
<input type="checkbox"/>	 <a href="#">MS 912945 Internet Explorer ActiveX Update</a>	Recommended	0	1
<input type="checkbox"/>	 <a href="#">MSXML 6.0</a>	Software Installer	0	1
<input type="checkbox"/>	 <a href="#">MS 910437 Resolves Access Violation Errors for WU and AU</a>	Recommended	0	1
<input type="checkbox"/>	 <a href="#">MS 913538 Update for Windows Management Instrumentation</a>	Recommended	0	1
1 - 10 of 74			show 10 ▾ items	

A vulnerability, which has been assigned to the baseline (also called the mandatory baseline vulnerability), has the icon  displayed next to its name, as shown in Figure 5-4.

Alternatively, you can view the baseline vulnerabilities by using the *Search* panel in the Vulnerabilities page that allows you to search for mandatory baseline vulnerabilities. See Figure 5-5.

For detailed information on Vulnerabilities and Vulnerabilities Information panels, refer Using Vulnerabilities.

## 5.1.2 Using the Mandatory Baseline Page

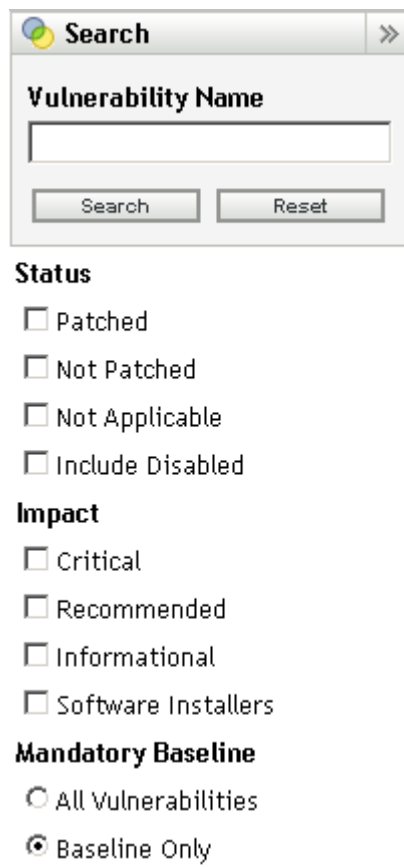
You can use the Search panel in the Mandatory Baseline page to view the baseline vulnerabilities.

The Search panel in the Device Group Vulnerabilities page, as shown in Figure 5-5 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:** Selecting this filter option displays only those vulnerabilities, which are marked as “mandatory baseline” items for the group.

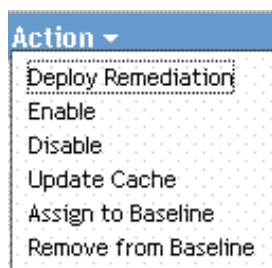
**Figure 5-5** Mandatory Baseline Search

The image shows a 'Search' dialog box with a title bar containing a search icon and the word 'Search'. Below the title bar is a section labeled 'Vulnerability Name' with a text input field and 'Search' and 'Reset' buttons. Below this is a 'Status' section with four checkboxes: 'Patched', 'Not Patched', 'Not Applicable', and 'Include Disabled'. Next is an 'Impact' section with four checkboxes: 'Critical', 'Recommended', 'Informational', and 'Software Installers'. Finally, there is a 'Mandatory Baseline' section with two radio buttons: 'All Vulnerabilities' and 'Baseline Only', with 'Baseline Only' being selected.

## 5.2 Working with Mandatory Baselines

The *Action* menu in 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. Figure 5-6 shows the various menu options that help you work with Mandatory baselines.

**Figure 5-6** Action Menu Items



The *Deploy Remediation* option enables you to deploy a patch. To use this option, select the checkbox/s for the vulnerability/s you require 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. To use this option, select it from the Action menu.

The *Disable* option enables you to disable a vulnerability. To use this option, select the checkbox for the required vulnerability and select *Disable*. The selected vulnerability is removed from the list.

To learn more about the *Update Cache*, *Assign to Baseline*, and *Remove from Baseline* options see the following three sections.

### 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, repeat steps 1 to 4 in *Viewing Mandatory Baseline* section and then do as follows:

- ♦ Select the required vulnerability and choose the option ‘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 once a vulnerability has been assigned to the baseline:

1. The ZENworks Patch Management Server automatically schedules a *Discover Applicable Updates* task for all machines in that group.
2. ZENworks Patch Management Server also determines which systems are applicable and out of compliance (based on the vulnerabilities added to the baseline) following the *DAU* task.
3. Necessary bundles, as defined in the baseline, are deployed as soon as possible for each machine.

## 5.2.2 Removing a Mandatory Baseline

To remove patches from a mandatory baseline, repeat steps 1 through 4 in *Viewing Mandatory Baseline* section and then do as follows.

- ◆ Select the mandatory baseline item (vulnerability that have been assigned to baseline) and choose the option 'Remove from Baseline' from the *Action* menu. The vulnerability is removed from baseline and therefore is not mandatory for that group anymore.

---

**NOTE:** The 'Remove from Baseline' menu option will be 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 5-6**) initiates a process that gathers the bundles associated with a selected vulnerability and places those bundles on your ZENworks Patch Management Server.

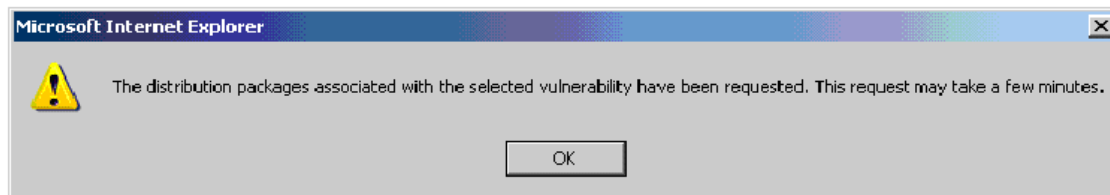
---

**NOTE:** If there are multiple ZCM servers in your management zone, you can select any one of them to be your current Patch Management Server.

---

To update caching of vulnerability data:

1. In the *Vulnerabilities* list, select one or multiple vulnerabilities.
2. In the Action menu, click *Update Cache*. A *Warning* dialog box appears as shown in the following image, prompting you to confirm the update request and informing you that this action may take an extended period of time.



3. Click *OK*.



# Using Devices

# 6

The following sections describe device vulnerability information for Novell® ZENworks® Configuration Management:

- ♦ [Section 6.1, “About Devices,” on page 63](#)

## 6.1 About Devices

### 6.1.1 Device Vulnerabilities

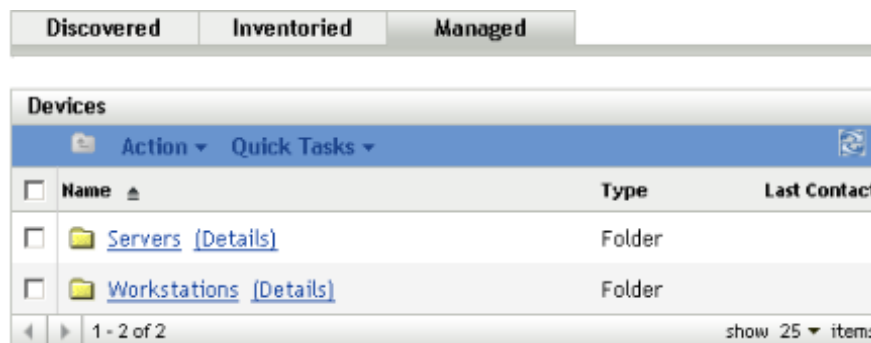
*Device Vulnerabilities* refers to the vulnerability information associated with a selected device - a server or a workstation. The vulnerabilities listed for a specific device are the ones that are applicable only for that device.

#### Server Device Vulnerabilities

To view the vulnerabilities for a specific server device:

1. Click the *Device* tab in the left panel. A page displaying the root folders for each type of device appears as shown in Figure 6-1.

**Figure 6-1** Root Folders in Devices Tab







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 Figure 6-2. Along with the server groups, the default agent is also displayed.

**Figure 6-2** *The List of Server Groups*

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

Servers					
New ▾ Edit ▾ Delete Action ▾ Quick Tasks ▾					
<input type="checkbox"/>	Status	Name ▲	Operating System	Type	Last Contact
<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="#">zenbeta3</a>	win2003-ee-sp1-x86	Server	5/18/07 4:57 PM
1 - 3 of 3					show 25 ▾ items

- Click the required group (Server Group or Dynamic Server Group) to view details of the group and the members of the group. Alternatively, you can click the default agent. A page displaying details about the agent or member appears. See Figure 6-3.

---

**NOTE:** The name "zenbeta3" for the default agent is by way of an example. The network administrator will decide the name of the default agent.


---

Figure 6-3 shows the page displaying details for the default agent named "zenbeta3."



**Figure 6-3** Device Details Page for the Default Agent

[Devices](#) > [Servers](#) > zenbeta3

 **zenbeta3**

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

General

Alias:

zenbeta3

Host Name:

ZENBETA3

IP Address:

192.168.1.144


Last Full Refresh:

May 18, 2007 11:27:52 AM

Last Contact:

May 18, 2007 6:53:37 PM

ZENworks Agent Status:



Operating System:

Microsoft Windows Server 2003 Enterprise Edition 5.02 13790

Number of errors not acknowledged:


0

Number of warnings not acknowledged:

5


Primary User:

No user sources configured



Owner:

[\(Edit\)](#)



GUID:

4f8d7955779852f8ca09050afea49693

Department:

[\(Edit\)](#)

Site:

[\(Edit\)](#)

Location:

[\(Edit\)](#)

- Click the *Vulnerabilities* tab. The vulnerabilities associated with the server device appear as shown in Figure 6-4.

**Figure 6-4** Vulnerabilities Associated with Default Agent

Vulnerabilities			
Action ▾			
<input type="checkbox"/>	Vulnerability Name ▲	Impact	Patched
<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="#">MS 892313 Updates for Windows Media Player 9 and 10</a>	Recommended	No
<input type="checkbox"/>	 <a href="#">MS 912945 Internet Explorer ActiveX Update</a>	Recommended	No
<input type="checkbox"/>	 <a href="#">MSXML 6.0</a>	Software Installer	No
<input type="checkbox"/>	 <a href="#">MS 910437 Resolves Access Violation Errors for WU and AU</a>	Recommended	No
<input type="checkbox"/>	 <a href="#">MS 913538 Update for Windows Management Instrumentation</a>	Recommended	No
1 - 10 of 74		show 10 ▾ items	

Figure 6-4 displays vulnerability information associated with the default agent.

### Using the Vulnerabilities Page for the Selected Device

The *Vulnerabilities* Page for a selected server device comprises the following three sections:

- ♦ Vulnerabilities
- ♦ Vulnerabilities Information
- ♦ Search

#### 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

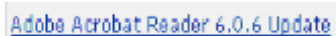
This section features the Action menu that enables you to perform any of the five actions related to vulnerabilities, namely, Deploy Remediation, Enable, Disable, Scan Now, and Update Cache. For more information on these actions, see [Action Menu Items](#).

The *Vulnerabilities* section also features the "show items" drop-down that enables you to select the number of items to be displayed in this section. See the following image.

### Vulnerability Name

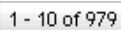
The name that identifies a vulnerability. This name typically includes the vendor or manufacturer of the vulnerability, the specific application, and version information.

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.

A screenshot of a vulnerability name displayed in a table. The text "Adobe Acrobat Reader 6.0.6 Update" is shown in a blue, underlined font, indicating it is a hyperlink.

### 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.

A screenshot of a table's bottom-left corner showing the text "1 - 10 of 979" in a small, grey box, indicating the current page and total number of vulnerabilities.

### 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 therefore, should be installed as soon as possible. Most of the recent security updates fall in to this category. ZENworks Patch Management 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 specially recommends vulnerabilities that fall in to this category.
- ♦ **Informational:** This type of vulnerability detects a condition that Novell has determined as informational. However, you can install it at your discretion if this type of vulnerability has an associated bundle.
- ♦ **Software Installers:** These types of vulnerabilities are software applications. Typically, this includes software installers. The vulnerabilities will show not patched if the application has not been installed on a machine.

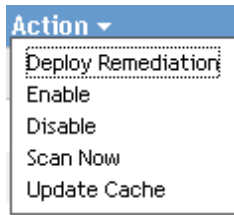
### Vulnerability Statistics

Vulnerability statistics shows the relationship between a specific vulnerability and the selected device. The vulnerability statistics appear in the last column on the extreme right side of the Vulnerability Page. The column status is described as follows.

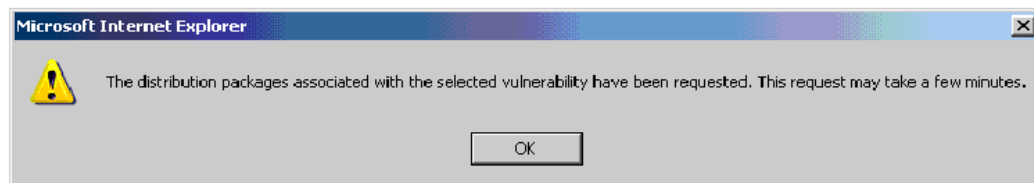
- ♦ **Patched:** This column indicates whether the selected device has been successfully patched or not. If the device has been patched this column shows "yes" and if the device has not been patched this column shows "no".

## Action Menu Items

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



- ♦ **Deploy Remediation:** This option enables you to deploy a patch. To use this option, select the checkbox for the vulnerability you require 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 checkbox for the required vulnerability and select Disable. The selected vulnerability is removed from the list.
- ♦ **Scan Now:** This option enables you to reschedule the Discover Applicable Updates System Task (DAU) 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 process that gathers the bundles associated with the selected vulnerability and places those bundles on your ZENworks Patch Management Server. To use this option:
  - a. Select one or multiple vulnerabilities in the *Vulnerabilities* list.
  - b. In the Action menu, click *Update Cache*. A *Warning* dialog box appears as shown in the following figure prompting you to confirm the request for update and informing you that this action may take an extended period of time.
  - c. Click *OK*.



---

**NOTE:** If there are multiple ZCM servers in your management zone, you can select any one of them to be your current Patch Management Server.

---

## 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 in the Vulnerability Information section.

For example, if you select the vulnerability called MSXML 6.0 from the list of vulnerabilities, the *Vulnerability Information* section displays the result of a vulnerability analysis for the selected vulnerability, as shown in Figure 6-5.

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

Vulnerability Information	
Property Name	Details
Name	MSXML 6.0
Impact	Software Installer
Status	Enabled
Vendor	Microsoft Corp.
Vendor Product ID	MSXML6.0
Description	<p>&lt;b&gt;Windows Installer 3.1 or higher must be present on the machine to allow this installation to proceed correctly.&lt;/b&gt;&lt;P&gt;The Microsoft Core XML Services (MSXML) 6.0 release provides standards-conformant implementations of: &lt;ul&gt;&lt;li&gt;XML 1.0 (DOM &amp; SAX2 APIs)&lt;/li&gt; XML Schema (XSD) 1.0&lt;li&gt;XPath 1.0&lt;li&gt;XSLT 1.0 &lt;/li&gt;&lt;/ul&gt;In addition, it offers client and server-safe components for XML over HTTP. MSXML6 is intended as an upgrade path for existing MSXML3 and MSXML4 users except for users that leverage some of the older ProgIDs and technologies in MSXML3 and MSXML4. The following are not supported in MSXML6: &lt;ul&gt;&lt;li&gt;DSOControl&lt;li&gt;XML Data Islands&lt;li&gt;XMLHTTP10, DOMDocument10, FreeThreadedDOMDocument10&lt;li&gt;XDR Schemas&lt;/li&gt;&lt;/ul&gt; These technologies are currently in maintenance mode in MSXML3 and MSXML4 but will be phased out according to the life-cycle for those components. MSXML6 will install side by side with MSXML 3 and MSXML4 and will not impact existing applications that use MSXML3 and MSXML4 (version independent ProgIDs will not point to MSXML6). Developers must move to the new '60' ProgIDs to use MSXML6 in their applications.&lt;p&gt;For information on the latest patch revision, see &lt;a href='http://support.patchlink.com/scripts/rightnow.cfg/php.exe/enduser/std_adp.php?p_faqid=361' target='_blank'&gt;Patch Applicability Fingerprint Improvements&lt;/a&gt;.&lt;br /&gt;</p>

Table 6-1 below defines each property name in the Vulnerability Information section.

**Table 6-1** *Property Names in Vulnerability Information Section*

Property Name	Definition
Name	The name of the vulnerability
Impact	The impact of the vulnerability as determined by Novell. See <i>Vulnerability Impacts</i>
Status	Status of the vulnerability - can be "Enabled" or "Disabled"
Vendor	The name of the vendor or manufacturer
Vendor Product ID	The ID number given to the product by the vendor
Description	The description of the vulnerability; includes the advantages of deploying the vulnerability and the pre-requisites for deployment

## Searching Vulnerabilities

The *Search* section in the Vulnerabilities page offers extensive search and data filtering options that allow you to search for specific vulnerabilities and filter result sets based on "Status" and "Impact" of the vulnerabilities. Searching and filtering can be performed independent of each other or can be combined to provide extensive drill-down capabilities. Figure 6-6 shows the *Vulnerability Search* section.

To search a vulnerability:

1. Enter full or part of the vulnerability name in the Vulnerability Name textbox.
2. Select the required checkbox under "Status" and "Impact."
3. Click *Search*.

---

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

---

**Figure 6-6** Search Section in Vulnerabilities Page

The screenshot shows a web-based search interface. At the top is a window titled "Search" with a double-right arrow button. Inside this window is a label "Vulnerability Name" above a text input field. Below the input field are two buttons: "Search" and "Reset". Below the "Search" window, there are two sections of filters. The first section is titled "Status" and contains four checkboxes: "Patched", "Not Patched", "Not Applicable", and "Include Disabled". The second section is titled "Impact" and contains four checkboxes: "Critical", "Recommended", "Informational", and "Software Installers". All checkboxes are currently unchecked.

Table 6-2 describes the result of selecting each filter option under *Status*.

**Table 6-2** Status Filters in Search

Status Filter	Result
Patched	Search results will include all the vulnerabilities in the vulnerability list that have been applied or patched to one or more devices.

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

Table 6-3 describes the result of selecting each filter option under Impact.

**Table 6-3** *Impact Filters in Search*

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












## Workstation Device Vulnerabilities

To view the vulnerabilities for a specific workstation device:

1. Click the *Workstation* link on the *Devices* page, as shown in Figure 6-1. A list of workstation groups classified on the basis of their operating systems appears, as shown in Figure 6-7.

**Figure 6-7** *The List of Workstation Groups*

Devices > Workstations

Workstations					
 New ▾  Edit ▾  Delete  Action ▾  Quick Tasks ▾					
<input type="checkbox"/>	Status	Name	Operating System	Type	Last Contact
<input type="checkbox"/>		 <a href="#">System Update Test Group</a>		Workstation Group	
<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="#">patch02</a>	winxp-pro-sp2-x86	Workstation	3/20/07 2:47 AM
1 - 5 of 5					show 25 ▾ items

2. Click the required group (Workstation Group 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 Figure 6-8.

---

**NOTE:** The name "patch02" is by way of an example.

---

Figure 6-8 shows the page displaying details for the workstation device "patch02."






**Figure 6-8** Device Details Page for the Selected Workstation

[Devices](#) > [Workstations](#) > **patch02**

## **patch02**

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

General		⌵
<b>Alias:</b>	patch02	
<b>Host Name:</b>	PATCH02	
<b>IP Address:</b>	192.168.1.140	
<b>Last Full Refresh:</b>	May 18, 2007 11:27:52 AM	
<b>Last Contact:</b>	May 18, 2007 6:53:37 PM	
<b>ZENworks Agent Status:</b>		
<b>Operating System:</b>	Microsoft Windows XP Professional SP2 5.1	
<b>Number of errors not acknowledged:</b>	0	
<b>Number of warnings not acknowledged:</b>	5	
<b>Primary User:</b>	No user sources configured 	
<b>Owner:</b> <a href="#">(Edit)</a>		
<b>GUID:</b>	4f8d7955779852f8ca09050afea49693	
<b>Department:</b> <a href="#">(Edit)</a>		
<b>Site:</b> <a href="#">(Edit)</a>		
<b>Location:</b> <a href="#">(Edit)</a>		

- Click the *Vulnerabilities* tab. The vulnerabilities associated with the workstation device appear as shown in Figure 6-9.

**Figure 6-9** *Vulnerabilities Page for the Selected Workstation Device*

Vulnerabilities			
Action ▾			
<input type="checkbox"/>	Vulnerability Name 	Impact	Patched
<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="#">MS 892313 Updates for Windows Media Player 9 and 10</a>	Recommended	No
<input type="checkbox"/>	 <a href="#">MS 912945 Internet Explorer ActiveX Update</a>	Recommended	No
<input type="checkbox"/>	 <a href="#">MSXML 6.0</a>	Software Installer	No
<input type="checkbox"/>	 <a href="#">MS 910437 Resolves Access Violation Errors for WU and AU</a>	Recommended	No
<input type="checkbox"/>	 <a href="#">MS 913538 Update for Windows Management Instrumentation</a>	Recommended	No
  1 - 10 of 74		show 10 ▾ items	

The page in Figure 6-9 displays vulnerability information associated with the selected workstation device. The features on this page are similar to those in the *Vulnerabilities* page for the selected server device as shown in Figure 6-4. For more information on the features of the Vulnerabilities page, see [Using the Vulnerabilities Page for the Selected Device](#).

# Device Group Vulnerabilities

# 7

*Device Group Vulnerabilities* refers to the vulnerabilities that have been assigned to the members of a group of devices - either the server group or the workstation group - in the network and 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 75](#)
- ♦ [Section 7.2, “Workstation Group Vulnerabilities,” on page 77](#)





## 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 in the left panel. A page displaying the root folders for each type of device appears, as shown in Figure 7-1.

**Figure 7-1** Root Folders of Device Groups





Discovered		Inventoried		Managed	
Devices					
		Action ▾		Quick Tasks ▾ 	
<input type="checkbox"/>	Name ▲			Type	Last Contact
<input type="checkbox"/>	 <a href="#">Servers</a> <a href="#">(Details)</a>			Folder	
<input type="checkbox"/>	 <a href="#">Workstations</a> <a href="#">(Details)</a>			Folder	
 		1 - 2 of 2		show 25 ▾ items	

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 Figure 7-2.

**Figure 7-2** List of Server Groups


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

Servers				
New Edit Delete Action Quick Tasks				
<input type="checkbox"/>	Status	Name	Operating System	Type
<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="#">zenbeta3</a>	win2003-ee-sp1-x86	Server
1 - 3 of 3				show 25 items

3. Click the required group (Server Group or Dynamic Server Group). A page displaying the general details of the group and the members in the group appears. Figure 7-3 below shows such a page that appears when the Dynamic Server type group 'Windows Server 2003' is selected.

**Figure 7-3** General Details and Members of the Selected Server Group

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

Windows Server 2003	
Summary	Vulnerabilities
<b>General</b>	
Object type:	Dynamic Server Group
GUID:	c03d4208159f971e205f01eb5ff67c54
Description: <a href="#">(Edit)</a>	Windows Server 2003 Group
<b>Members</b>	
Name	In Folder
 <a href="#">zenbeta3</a>	/Devices/Servers
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 Server 2003*, the Vulnerabilities tab displays all the vulnerabilities applicable to the member devices within the group 'Windows Server 2003', as shown in Figure 7-4.

**Figure 7-4** Device Group Vulnerabilities Page for the Selected Server Group

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

Windows Server 2003

Summary Relationships Details **Vulnerabilities**

Vulnerabilities				
Action ▾				
<input type="checkbox"/>	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 912945 Internet Explorer ActiveX Update</a>	Critical	0	1
<input type="checkbox"/>	<a href="#">MSXML 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 server group, see the section [Mandatory Baseline](#).

## 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 in the left panel. A page displaying the root folders for each type of device appears, as shown in Figure 7-1.
2. Click the Workstation link. A list of workstation groups classified on the basis of their operating systems appears, as shown in Figure 7-5.

**Figure 7-5** List of Workstation Groups

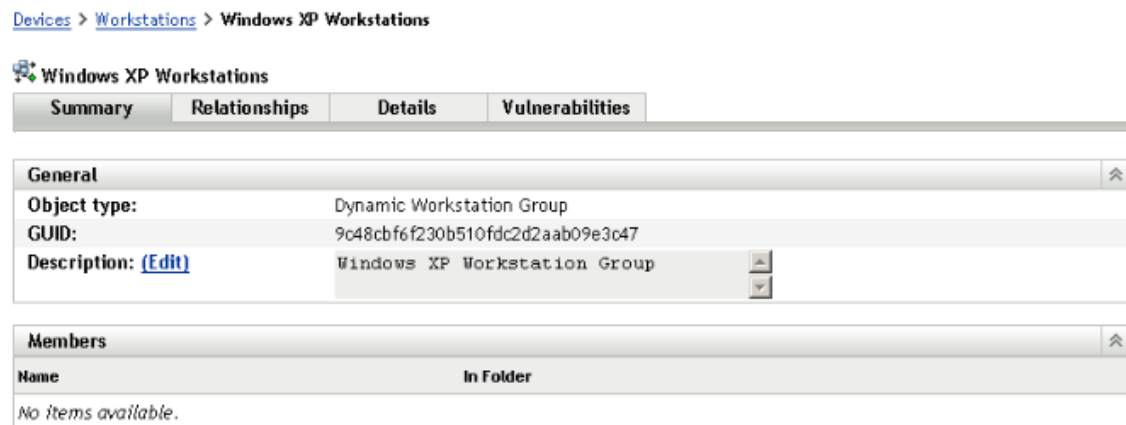
[Devices](#) > **Workstations**

Workstations			
New ▾  Edit ▾  Delete  Action ▾  Quick Tasks ▾			
<input type="checkbox"/>	Status	Name ▲	Operating System Type Last Contact
<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

1 - 3 of 3 show 25 items

3. Click the required group (Workstation Group or Dynamic Workstation Group). A page displaying the general details of the group and the members in the group appears. The following Figure 7-6 shows such a page that appears when the Dynamic Workstation Group called *Windows XP Workstations* is selected.

**Figure 7-6** General Details and Members of Selected Workstations Group



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 Figure 7-7.

**Figure 7-7** Device Group Vulnerabilities Page for the Selected Workstations Group

Summary Relationships Details Vulnerabilities				
Vulnerabilities				
Action ▾				
<input type="checkbox"/>	Vulnerability Name ▲	Impact	Patched	Not Patched
<input type="checkbox"/>	Macromedia Flash Player 7.0.r19 for IE	Critical	0	1
<input type="checkbox"/>	Macromedia Flash Player 7.0.r61 for IE	Critical	0	1
<input type="checkbox"/>	Macromedia Flash Player 7.0.r63 for IE	Critical	0	1
<input type="checkbox"/>	Macromedia Flash Player 8.0.r22 for IE	Critical	0	1
<input type="checkbox"/>	Macromedia Flash Player 9.0.r28 for IE	Critical	0	1
<input type="checkbox"/>	MS 890830 Microsoft Windows Malicious Software Removal Tool (March 13 2007)	Critical	0	1
<input type="checkbox"/>	MS 892313 Updates for Windows Media Player 9 and 10	Critical	0	1
<input type="checkbox"/>	MS 912945 Internet Explorer ActiveX Update	Critical	0	1
<input type="checkbox"/>	MSXML 6.0	Critical	0	1
<input type="checkbox"/>	MS 913538 Update for Windows Management Instrumentation	Critical	0	1
<div> <span>1 - 10 of 66</span> <span>show 10 items</span> </div>				

For information on the features of the Device Group Vulnerabilities page for the selected workstation group, see [Mandatory Baseline](#).