Novell ZENworks® 10 Patch Management

10.0.3

www.novell.com

REFERENCE

May 16, 2008

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/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

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/) 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

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

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide

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

Audience

This guide is intended for ZENworks administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to the Novell Documentation Feedback site (http://www.novell.com/documentation/feedback.html) and enter your comments there.

Additional Documentation

ZENworks 10 Configuration Management is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. See the ZENworks 10 Configuration Management documentation Web site (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 Services Overview

1

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

In this chapter

1.1 Product Overview

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

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

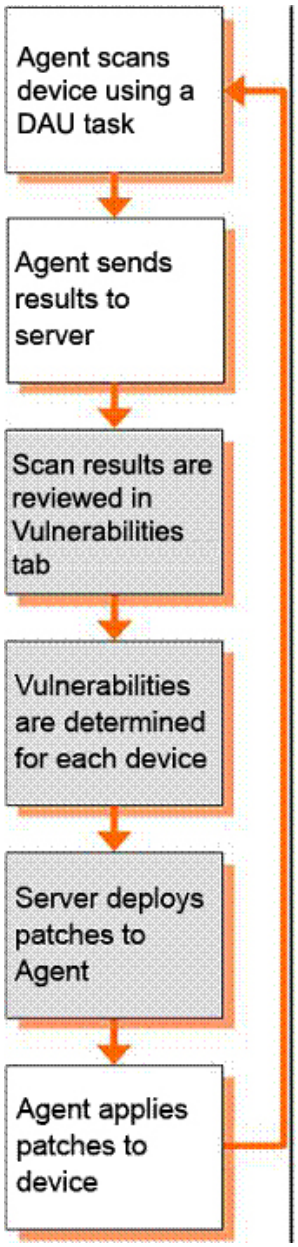
The ZENworks Server has a management tool known as ZENworks Control Center, which is a centralized web-interface that allows you to monitor and maintain patch compliance throughout the whole enterprise. ZENworks Server can deploy a ZENworks Adaptive Agent on every client system in the target network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

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

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

1.1.1 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 a Discover Applicable Updates (DAU) scan of all ZENworks managed 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 scan are posted to the Vulnerabilities tab of the ZENworks Control Center, 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 Services

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

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

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

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

Table 1-1 *ZENworks Patch Management Services Features*

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

Feature	Description
Automatic notifications	Distributes e-mail alerts directly to administrator(s) for proactive security and administrative management (2008 feature)
Patch fingerprint accuracy	Ensures the highest level of accuracy in the detection of security vulnerabilities
Multi-patch deployments	Delivers multiple patches to multiple computers in one distribution to increase IT productivity
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 Services

2

Review the following section:

- Section 2.1, “Using the ZENworks Patch Management Services Home Page,” on page 13

2.1 Using the ZENworks Patch Management Services Home Page

Review the following section:

- Section 2.1.1, “Viewing and Configuring Subscription Information,” on page 13

2.1.1 Viewing and Configuring Subscription Information

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

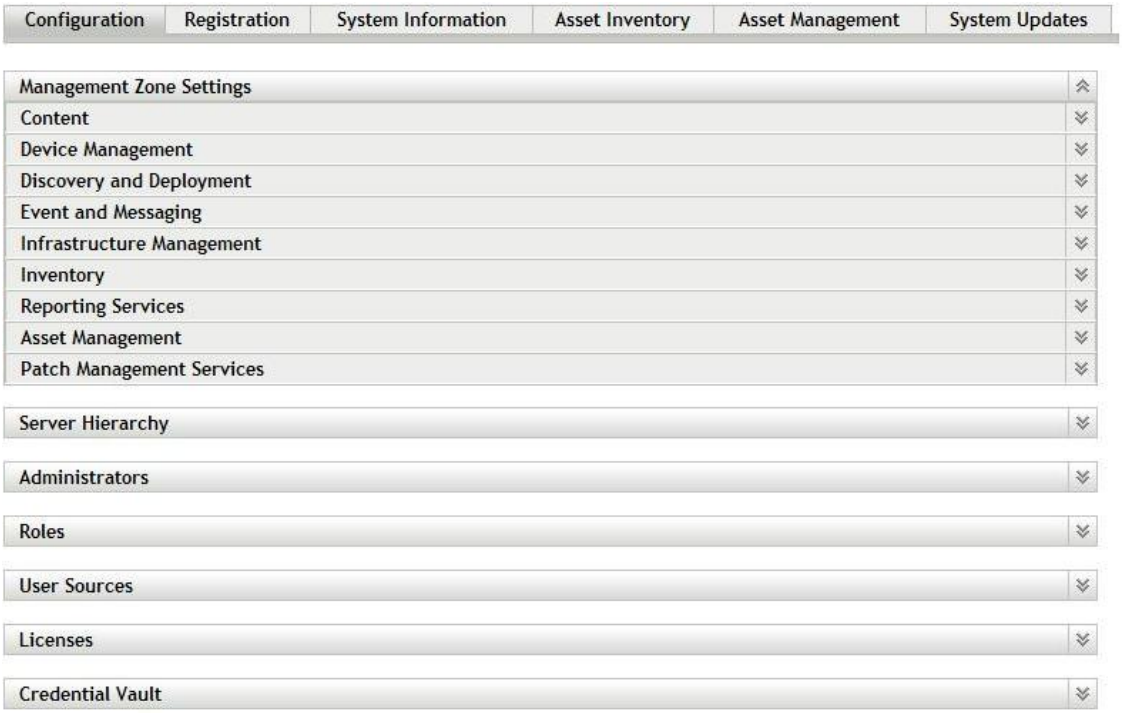
- “Viewing Subscription Service Information” on page 13
- “Activating/Viewing the Subscription Serial Number” on page 17
- “Configuring HTTP Proxy Details” on page 20
- “Configuring Subscription Download Details” on page 22

Viewing Subscription Service Information

To view the current subscription service information:

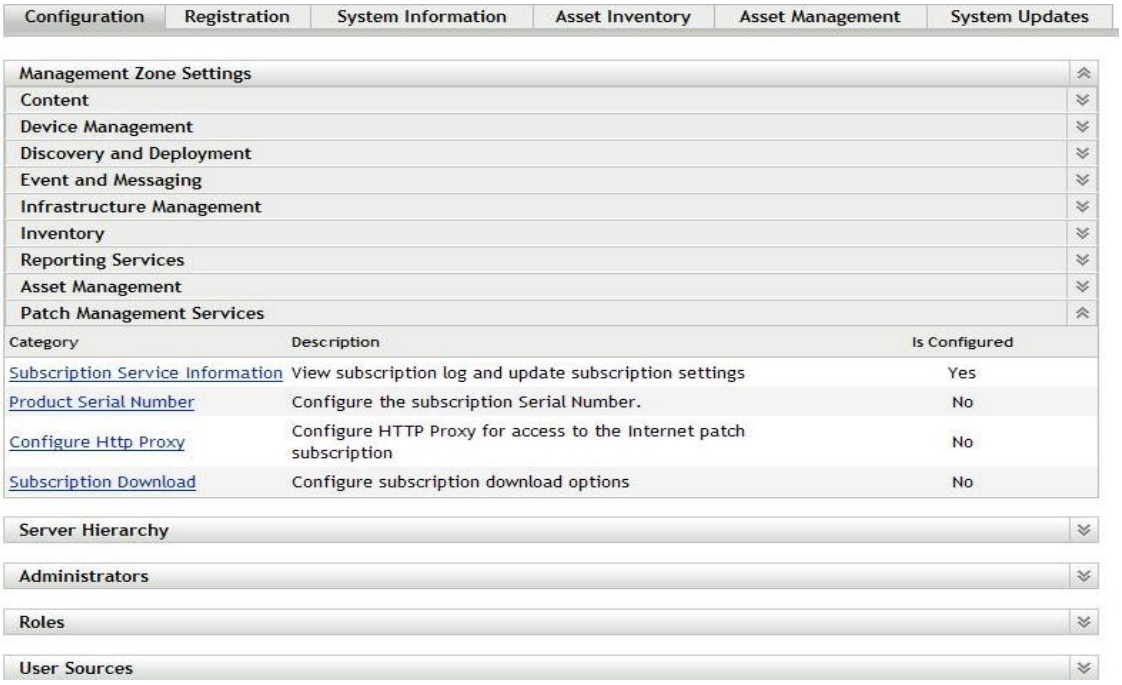
1. Click the *Configuration* tab in the left panel. The *Configuration* page appears as shown in the following figure.

Figure 2-1 *Configuration Page*



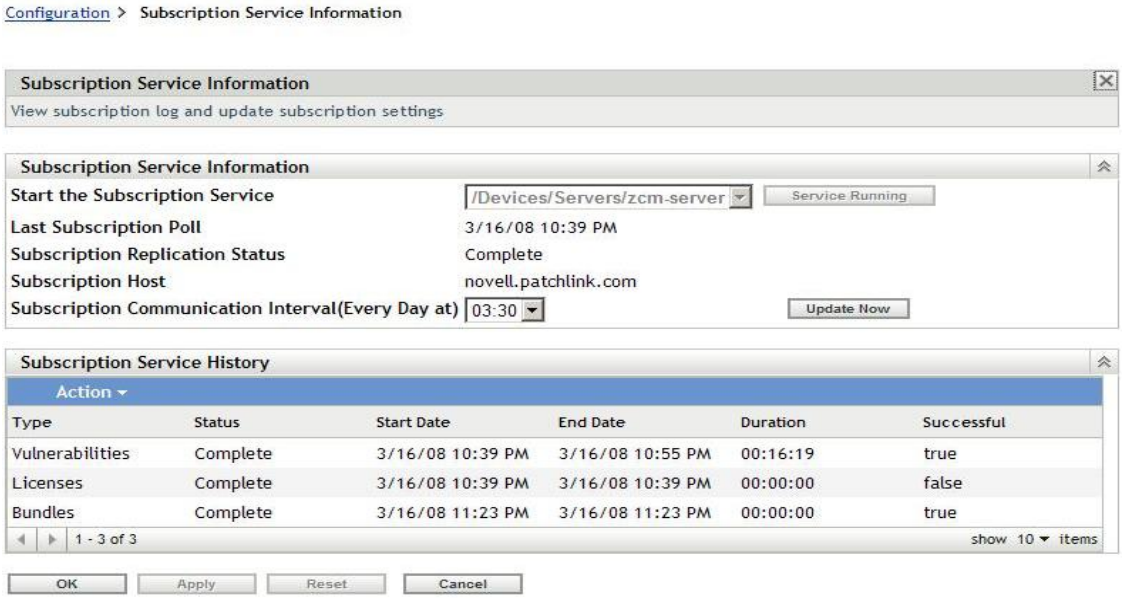
2. Click *Patch Management Services*. Four hyperlinks—*Subscription Service Information*, *Product Serial Number*, *Configure HTTPProxy*, and *Subscription Download*—are displayed as shown in the following figure.

Figure 2-2 *Patch Management Services*



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

Figure 2-3 *Subscription Information Page*



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. **NOTE:** Once the subscription service starts running, the *Start* button reads *Service Running*. **NOTE:** If there are multiple ZCM servers in your management zone, you can select any one of them to be the Patch Management Server. However, this must be decided only once per zone in this release.
Last Subscription Poll	The date and time of the last successful update
Subscription Replication Status	Latest status of the process of replication
Subscription Host	The URL of the ZENworks Patch Subscription Network

Status Item	Definition
Subscription Communication Interval (Every Day at)	The frequency of ZENworks Server communication with ZENworks Patch Subscription Network 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 initiate a complete replication with the ZENworks Patch Subscription Network
Update Now	Initiates replication of the ZENworks Server with ZENworks Patch Subscription Network and forces an immediate download of patch subscription
Cancel	Enables you to cancel the last action performed

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

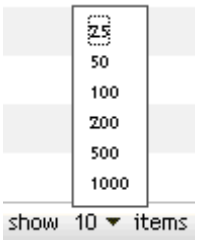
Table 2-3 *ZENworks Subscription Service History Items*

Item	Definition
Type	Subscription type defined for your account namely Vulnerability (Subscription Replication), Bundles (Subscription Replication), and Licenses
Status	Status of replication—when replication begins, the status reads *In Progress*. When replication ends, the status reads *Completed* **NOTE:** If the replication process is interrupted, the status reads *Auto Reset*. This indicates that the replication process has continued from the point where it was interrupted.
Start Date	The date and time at which replication started
End Date	The date and time at which replication ended

Item	Definition
Duration	The length of time for which replication has been going on
Successful	Indicates whether the replication was successful or not—*True* indicates successful replication and *False* indicates incomplete or failed replication

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 the *show items* drop-down and selecting the desired number, as shown in the following figure.

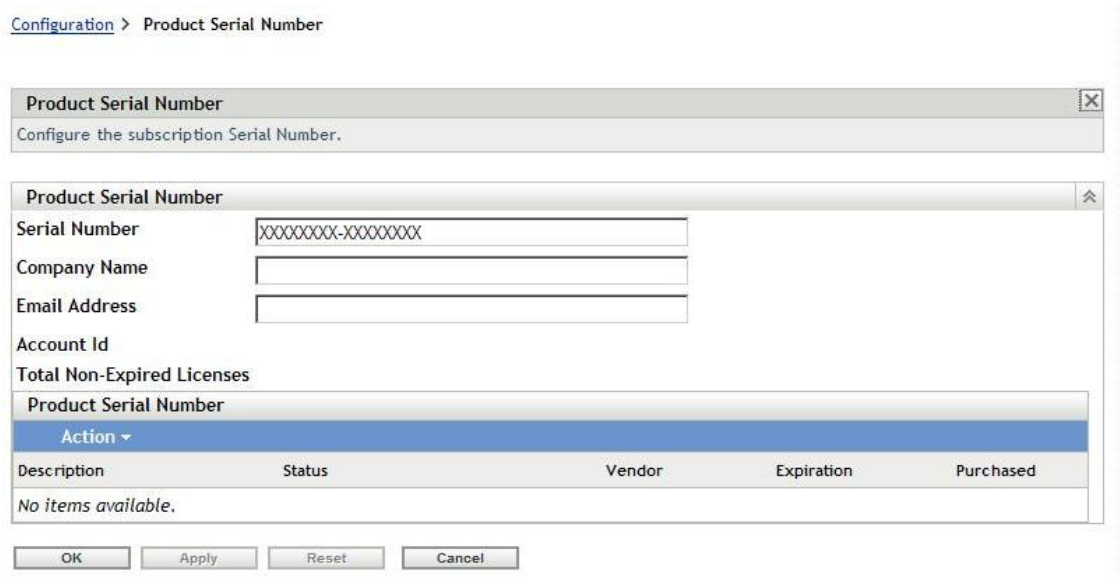


Activating/Viewing the Subscription Serial Number

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*



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

1. Enter the subscription serial number, which is valid only for a 60-day trial. The *Product Serial Number* panel will not display any details since the product is in trial mode.
2. 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 Services along with the company name and email address.
3. Revalidate the subscription serial number. The license record is now valid, and will display 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.lumension.com/update.
- The ZENworks Patch Management Services content distribution network is a global cache infrastructure with many servers. Downloading patches from this network requires port 80 (HTTP) access to the following URL: http://novell.cdn.lumension.com/novell.
- To download patches, you must provide internet access to both novell.lumension.com and novell.cdn.lumension.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 novell.cdn.lumension.com” will

display the local IP address for the content distribution node. Allow access to that specific local address through the firewall.

IMPORTANT: If you are upgrading from a prior version of ZENworks Patch Management Services, you can use your existing patch management subscription serial number once your ZENworks Patch Management 10 server has been uninstalled.

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

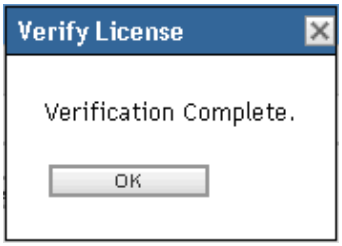
Table 2-4 *ZENworks Subscription Serial Number Items*

Item	Definition
Serial Number	ZENworks Patch Management Services license number (serial number)
Company Name	Name of the company that ZENworks Patch Management Services is registered to
Email Address	Email address, which you can use for receiving alerts and for future communication
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
Total Non-Expired Licenses	Total number of active licenses—each registered device requires one license
Description	The description of the license or the name of the license
Status	Status of license verification—when verification begins, the status reads *Initializing Verification*. When replication ends, the status reads *Completed*
Vendor	The source from where the license was purchased
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

The ZENworks Patch Management Services serial number can be entered only once. Once you have entered the serial number, you can verify the license by clicking the *Action* drop-down on the *Subscription Serial Number* page and selecting *Verify License*. Automatic verification of the license happens everyday with the replication process. The *Verify License* message box appears, as shown in the following figures.

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

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 start the license verification process
Reset	Enables you to reset the data entered in the text fields
Cancel	Enables you to cancel the last action performed

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*

The *Proxy Server Details* page enables you to configure an HTTP proxy for access to internet patch subscription. The HTTP proxy server allows ZENworks Patch Management Services to download subscription service over the internet.

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

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

Item	Description
Proxy Host	The proxy address used to connect to ZENworks Patch Subscription Network
Port	The proxy port used to connect to ZENworks Patch Subscription Network
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

Button	Action
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*

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	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* check box, only 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

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® Server. The page displays the name, description, impact, and statistics of the vulnerabilities.

3.1 About Vulnerabilities

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

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

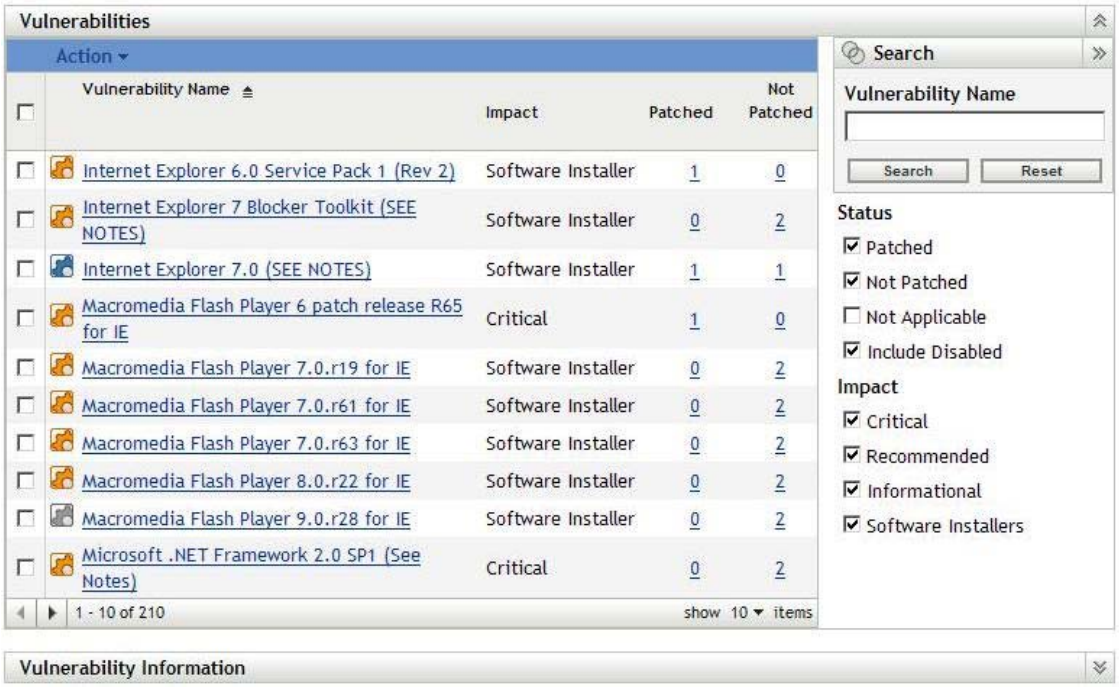
3.1.1 Viewing Vulnerabilities

To view the vulnerabilities in ZENworks Patch Management Services:

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

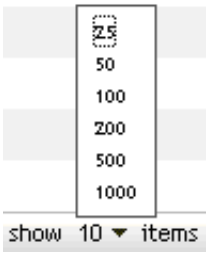
3.2.1 Vulnerabilities

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.



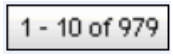
Vulnerability Name

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.

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.



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 Server automatically downloads and saves the vulnerabilities that have critical impact.
- Recommended: Novell has determined that this vulnerability, although not critical or security related, is useful and should be applied to maintain the health of your computers. Therefore, Novell recommends vulnerabilities that fall in 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 Server that meet a specific status. The vulnerability

statistics appear in two columns on the extreme right side of the *Vulnerabilities* page. Each column status is described as follows.

- *Patched*: This column displays a hyperlink indicating the total number of devices to which the corresponding vulnerability has been applied or patched.

  Clicking this hyperlink will display a page that lists the patched devices. You can uninstall the patch using the *Remove* option in the *Action* menu.

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

  Clicking this hyperlink will display a page that lists these devices. You can deploy the patch to these devices using the *Deploy Remediation* option in the *Action* menu.

The vulnerabilities shown on 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*

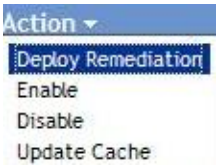
Vulnerability Icon	Significance
	Indicates the vulnerabilities that are disabled. **NOTE:** Disabled vulnerabilities are hidden by default. Use the *Include Disabled* filter in the Search panel to show these items.
	Indicates that only the fingerprint information for the vulnerability has been brought down from the ZENworks Patch Subscription Network. Therefore, this icon represents the vulnerabilities that are not cached.
	Indicates that the fingerprints and remediation bundles necessary to address the vulnerability have been cached into the system. Therefore, this icon represents the vulnerabilities that are cached and ready for deployment.

NOTE: If you choose a vulnerability that does not have cached remediation bundles, the deployment process may fail until the cache download is complete. It is recommended that you download the files from the patch subscription and they must be packaged by ZENworks 10 Configuration Management. Then the icon turns blue. To initiate an immediate download of these packages, select the *Update Cache* option from the *Action* menu.

Action Menu Items

The *Vulnerabilities* section also features an *Action* menu, which enables you to perform one of four actions on the vulnerabilities listed on the page. 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 check box/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 check box for the required vulnerability and select *Disable*. The selected vulnerability is removed from the list.
- *Update Cache*: This option initiates a download process for the bundles associated with the selected vulnerability and caches those bundles on your ZENworks Server.

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

  To use this option:

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

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

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

3.2.2 Vulnerability Information

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

For example, if you select the vulnerability called Internet Explorer 7.0 (SEE NOTES) 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*

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
Impact	The impact of the vulnerability as determined by Novell. See Vulnerability Impacts
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

3.2.3 Searching Vulnerability

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

To search a vulnerability:

1. Enter full or part of the vulnerability name in the *Vulnerability Name* text box.
2. Select the required check box 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*

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

Review the following section:

4.1 Using the Deploy Remediation Wizard

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

You can access the *Deploy Remediation* wizard from the *Devices* or *Vulnerabilities* tab.

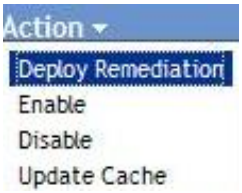
NOTE: Using the *Deploy Remediation* wizard, if you select multiple vulnerabilities, the wizard will automatically select all the applicable devices and packages. If any device is selected, the wizard will automatically select all vulnerabilities that are applicable for that device. If a group is selected,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

NOTE: In 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 on 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.

Figure 4-2 *Confirm Devices Page*

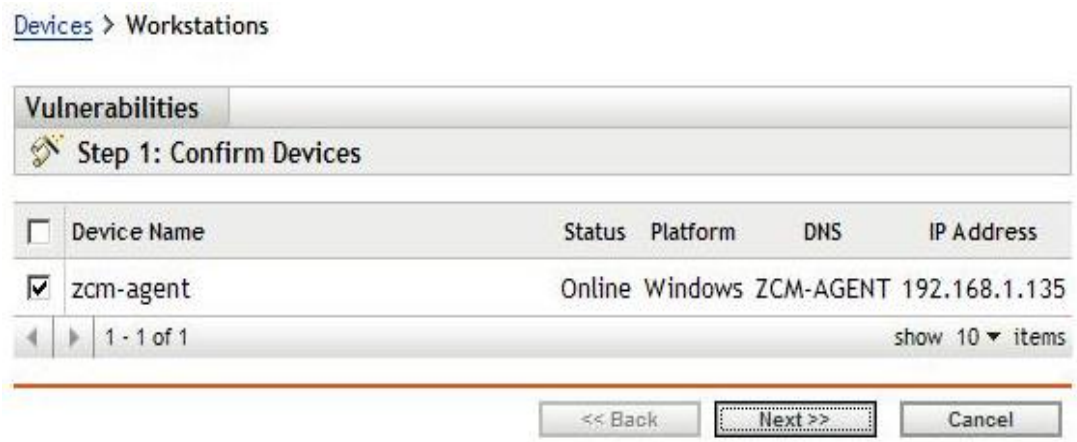


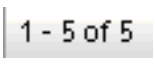
Table 4-1 describes the column headings in the *Confirm Devices* page.

Table 4-1 *Confirm Devices Page Column Headings*

Column Heading	Description
Device Name	The name of the device registered with ZENworks Patch Management Services (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 name 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 on the page. In the following example, the total number of devices is five.

Figure 4-3 *Total Number of Devices*

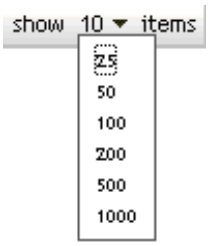


You can sort the devices in ascending and descending alphabetical order. To sort, click the arrow in the column heading *Device Name* as shown in Figure 4-4.

Figure 4-4 *Sorting Devices*

You can choose the total number of items to be displayed on 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 third-party licensing information associated with the selected vulnerabilities. Accepting or declining the license agreement of the vulnerability is the second step in scheduling a deployment for a selected vulnerability.

Figure 4-6 *License Agreement Page*

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.

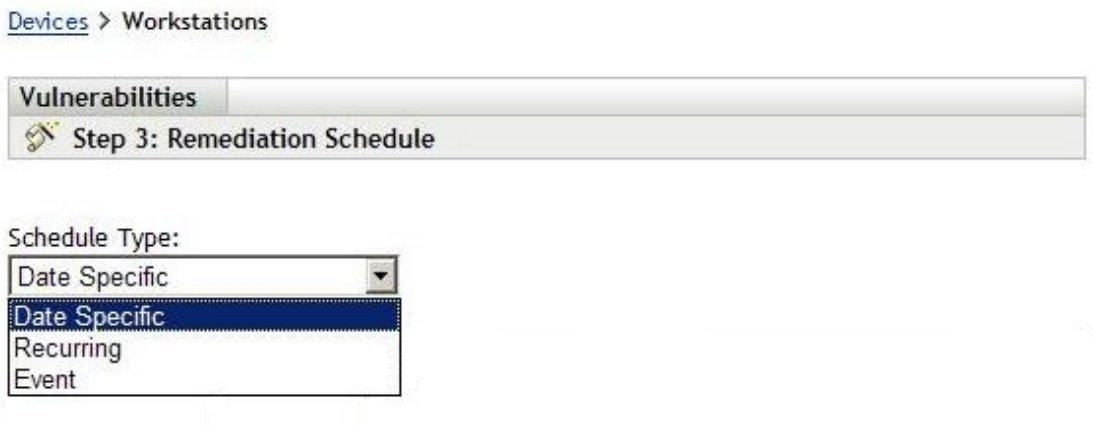
NOTE: If you want to abort the wizard, click the *Cancel* button.

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. See Figure 4-7.

Figure 4-7 *Remediation Schedule Page*



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

- Date Specific: Selecting *Date Specific* will schedule the deployment 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 *Event* will trigger the scheduled deployment when a particular event (chosen from a given list of events) takes place.

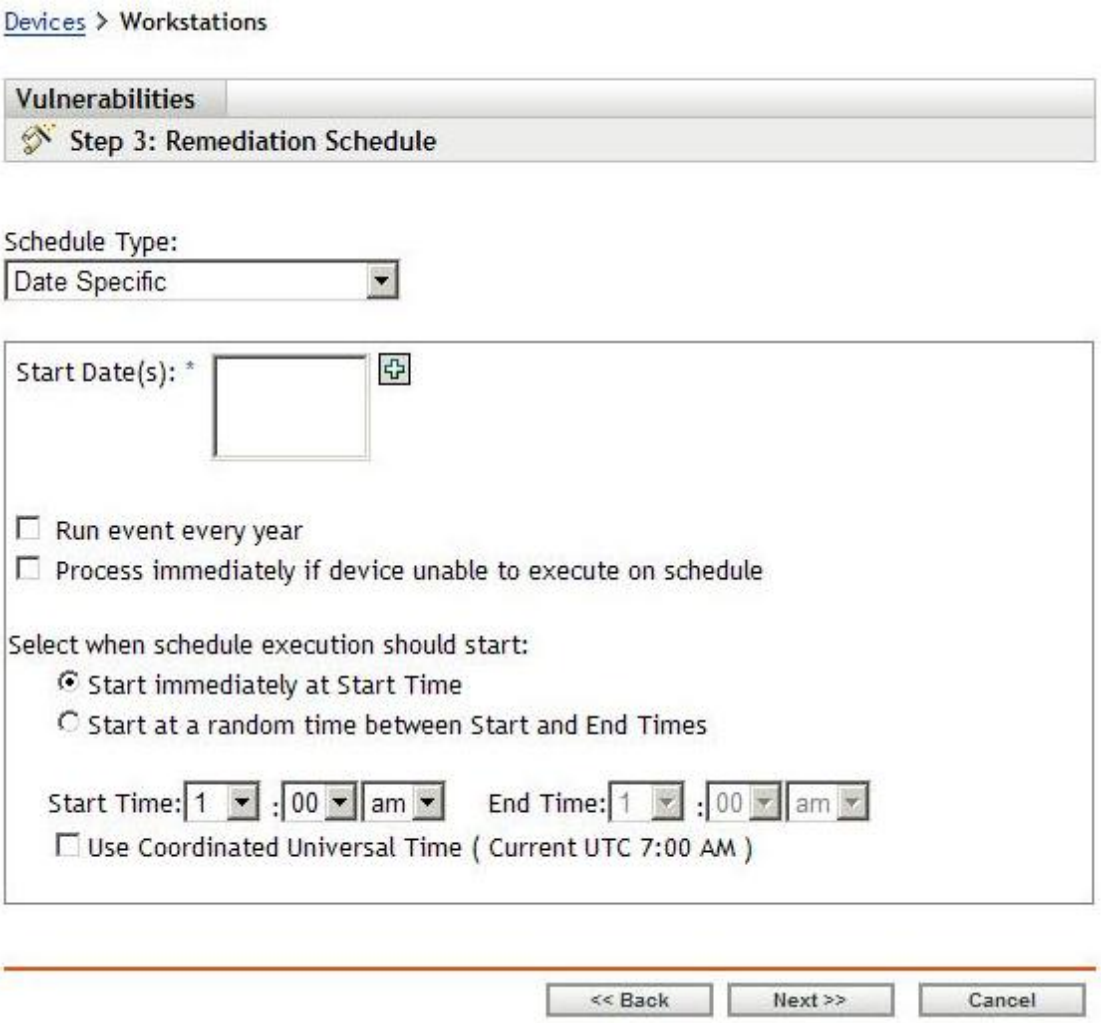
TIP: For an immediate installation of a patch, select the *Recurring* schedule type, and choose the *When a device is refreshed* option. This will force the installation of the patches during the next Device Refresh Schedule (the frequency of communication between the ZENworks Adaptive Agent and the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

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

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*



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*s.
  - *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 at a random time between Start Time and End Times*: 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:

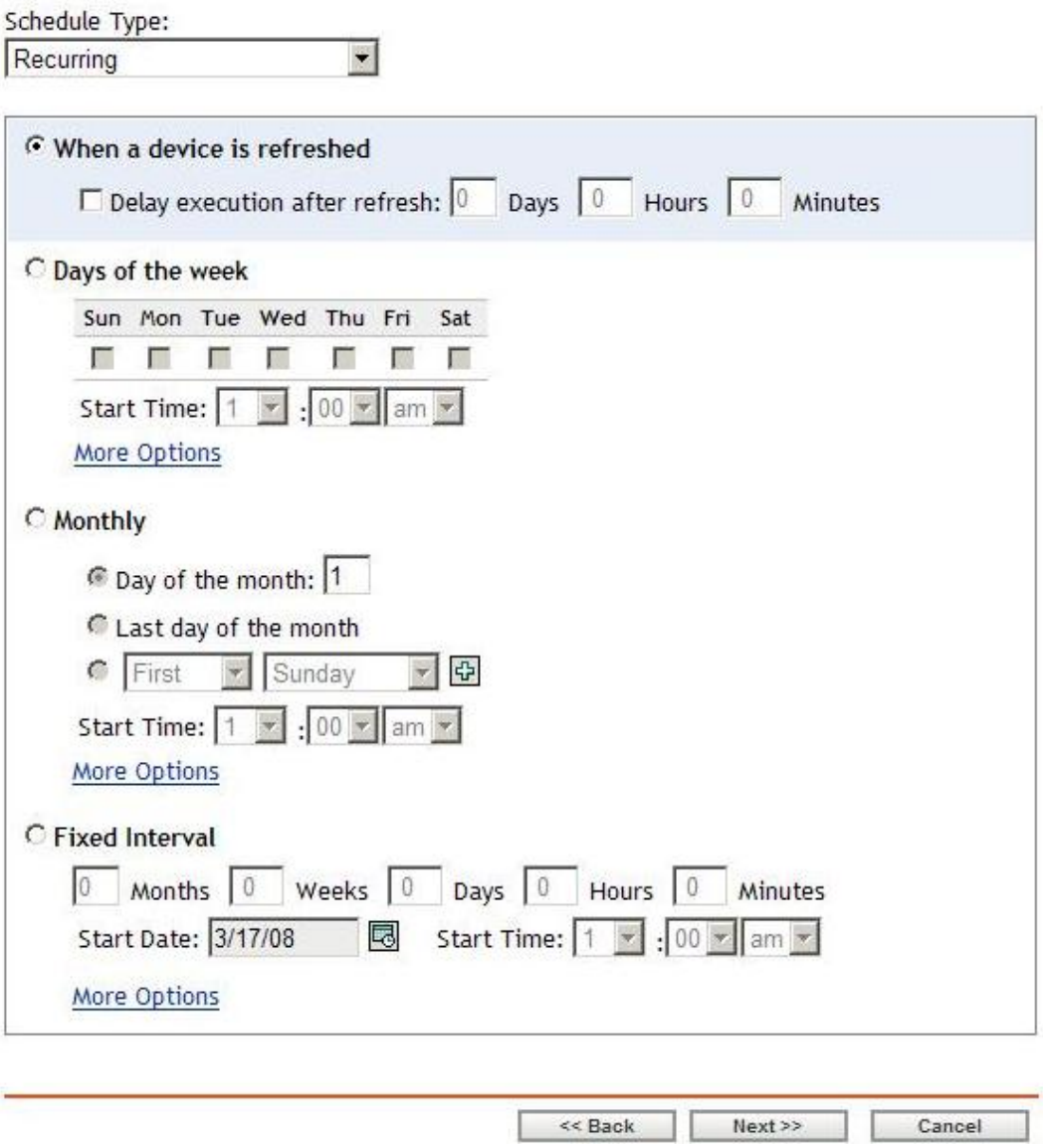
NOTE: In both the time panels, the first drop-down enables you to select the hour, the second drop-down enables you to select the minute, and the third drop-down enables you to select the am and pm period.

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



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.

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.

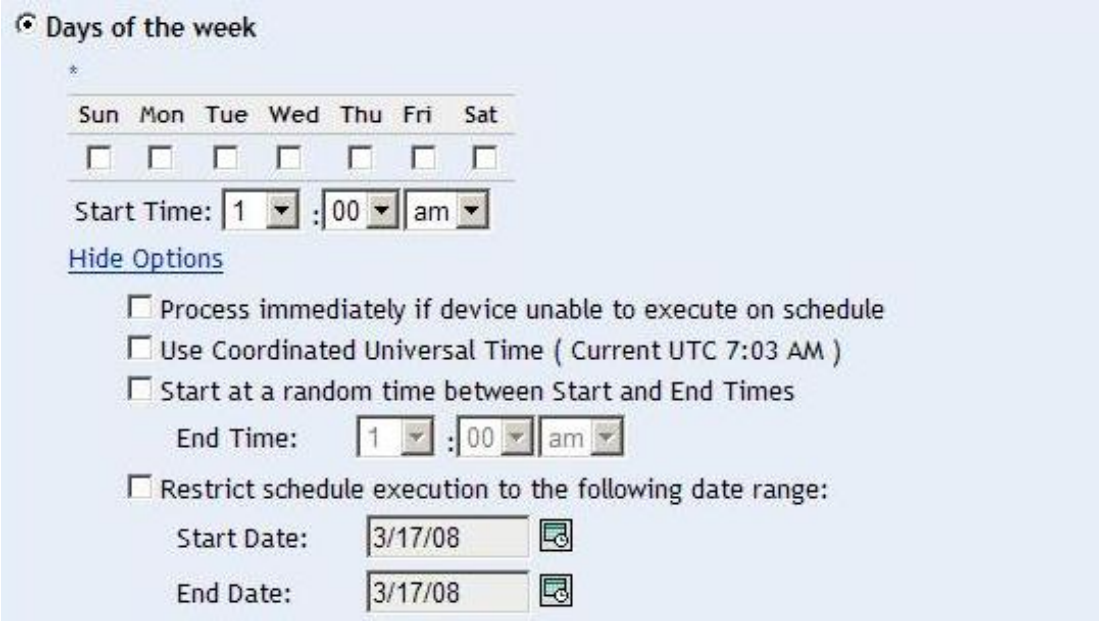
- *Days of the week*: This option enables you to schedule the deployment on selected days of the week. See Figure 4-10.

Figure 4-10 *Weekly Deployment Options - Default*

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*



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 Times* 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.

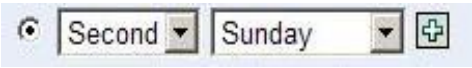
NOTE: The option *Restrict schedule execution to the following date range* enables you to schedule a recurring deployment at the selected time and repeat the deployment on the day(s) specified and if defined, end on the specific time. This option also enables you to restrict the deployment to the period 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.

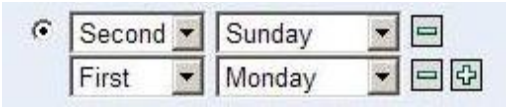
Figure 4-12 *Monthly Deployment Options – Default*

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.



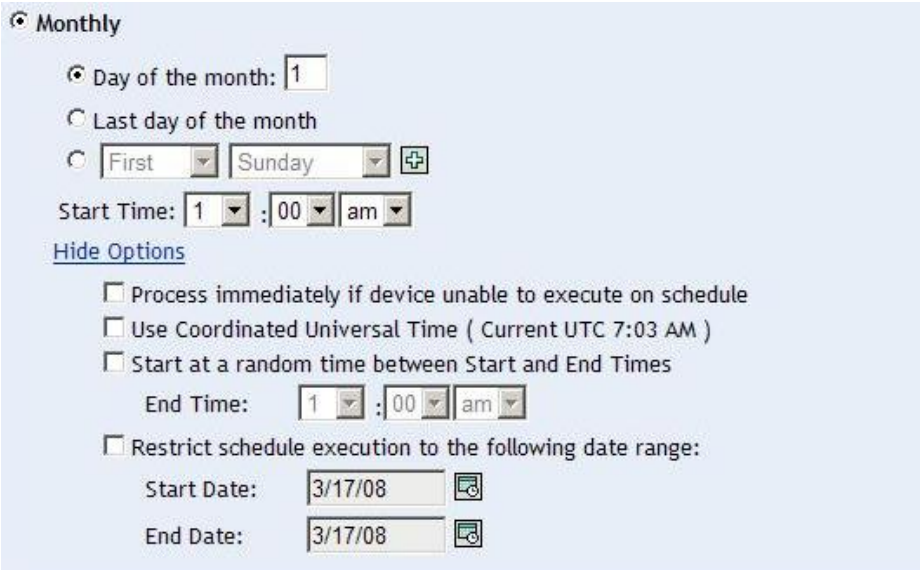
To select an additional day of the month, click the symbol  and use the drop-down arrows in the second row shown as follows.



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*



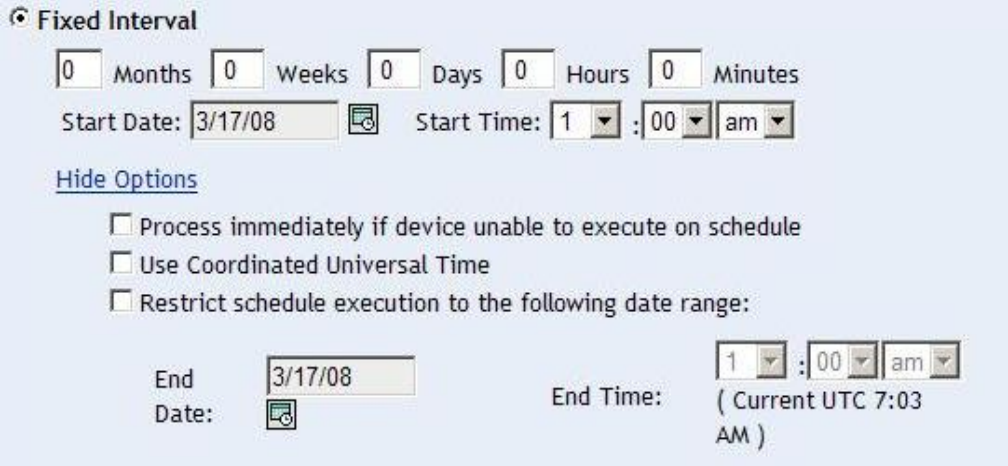
NOTE: The option *Restrict schedule execution to the following date range* enables you to schedule a recurring deployment at the selected time and repeat the deployment on the day(s) specified, and if defined, end on the specific time. This option also enables you to restrict the deployment to the period 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 Interval Deployment Options - Default*

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.

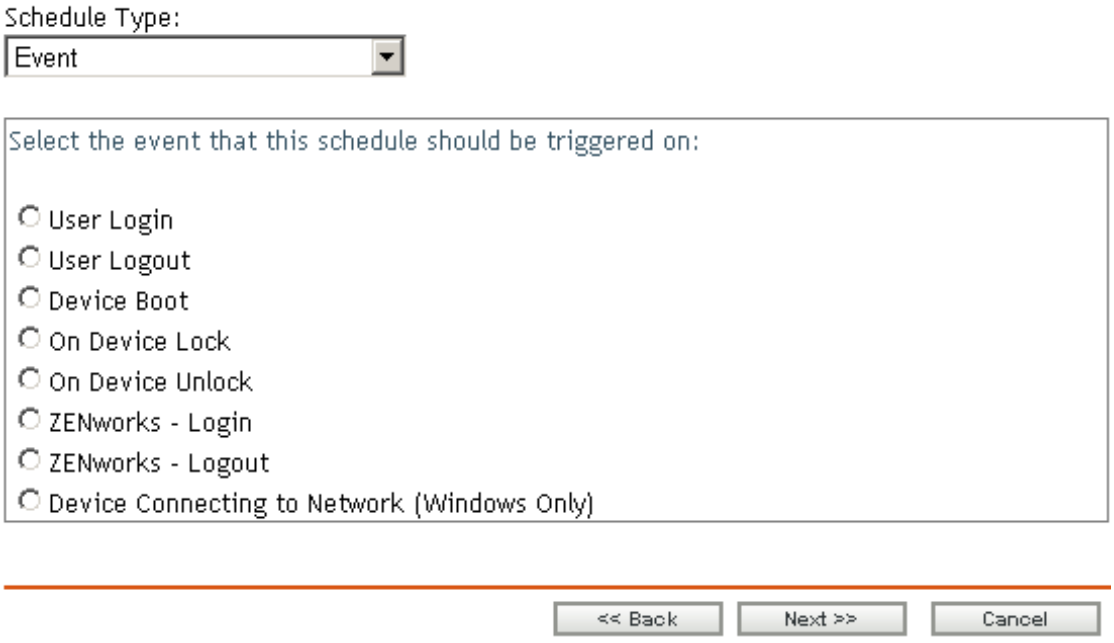
Figure 4-15 *Fixed Interval Deployment Options - All*



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*



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 the ZENworks user source account. This option is not applicable if no user sources are configured.
ZENworks – Logout	Deployment remediation occurs whenever the user logs out of the ZENworks user source account. This option is not applicable if no user sources are configured.
Device Connecting to Network (Windows Only)	Deployment remediation occurs whenever the device tries to connect to any machine (Windows Only) in the network.

7. 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.

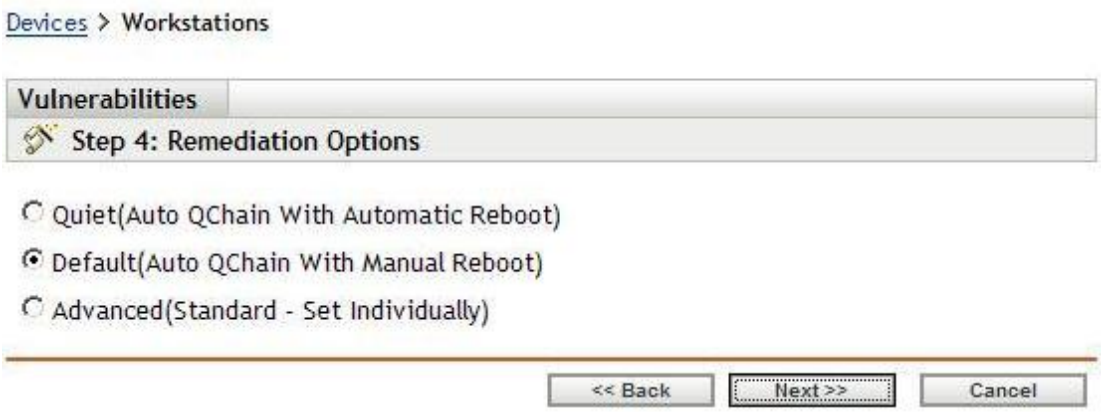
NOTE: To return to the previous page, click the *Back* button. To abort the *Deployment Remediation* wizard, click the *Cancel* button.

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*



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

Table 4-3 *Functionalities of the Remediation Options*

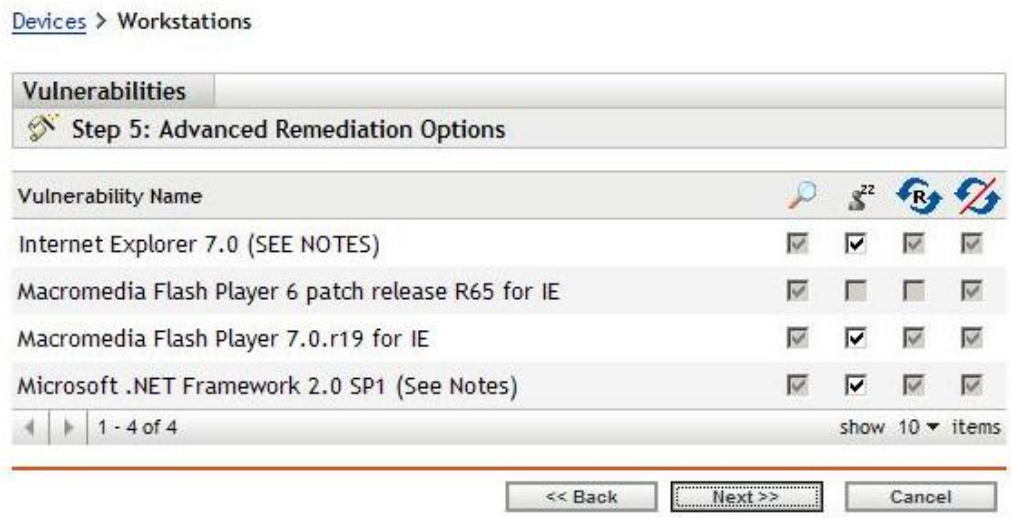
Remediation Options	Functionality
Quiet (Auto QChain With Automatic Reboot)	Automatically sets all possible vulnerabilities to deploy with QChain enabled. All necessary reboots are performed automatically.
Default (Auto QChain With Manual Reboot)	Automatically sets all possible vulnerabilities to deploy 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)	Allows the administrator to set the patch deployment flags as desired, using the default QChain and reboot settings defined for each vulnerability.

8. 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 on the page represent the patch flags that can be set for each package.

Figure 4-18 *Advanced Remediation Options Page*



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

Icon	Behavior Functionality
 (Uninstall)	Uninstalls the packages instead of an installation
 (Force Shutdown)	Forces all applications to close if the package causes a reboot
 (Do Not Backup)	Will not backup files for uninstall
 (Suppress Reboot)	Prevents the computer from rebooting after installation of the package **NOTE:** This option cannot be modified in this release—the patch will always be installed with “suppress reboot,” and ZENworks Adaptive Agent will perform the actual reboot when required.

Icon	Behavior Functionality
 (Quiet 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
 (Unattended Setup)	Installs the packages in the unattended setup mode
 (List Hot Fixes)	Returns a listing of the hot fixes installed on the target computers
 (Force Reboot)	Forces the computer to reboot regardless of package requirements
 (Reboot is Required)	Indicates that this package requires a reboot prior to completing the installation **NOTE:** Selecting this option does not necessarily reboot the device. A reboot will happen only if the specific bundle deployed to the devices requires a reboot.
 (Chain Packages)	Sets the package as chainable (provided the package supports chaining) **NOTE:** This option cannot be modified in this release—the package will always be installed with the “chain” option.
 (Suppress Chained Reboot)	Suppress the reboot, allowing other chained packages to be sent following this package **TIP:** It is recommended that you suppress the final reboot for all chained packages, then send a reboot deployment when all packages are finished
 (Repair File Permissions)	Repairs file permissions after package installation
 (Download Only)	Distributes the package without running the package installation script

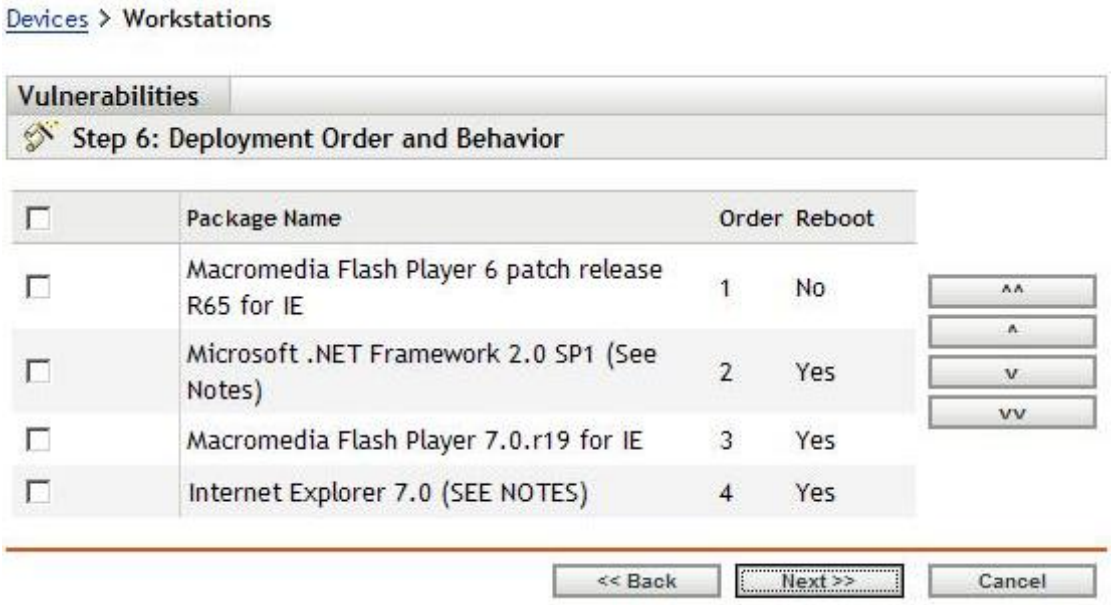
Icon	Behavior Functionality
 (Suppress Notification)	Suppresses any user notifications during installations
 (Debug Mode)	Runs the package installation in debug mode
 (Do Not Repair Permissions)	Suppresses the repair of file name permissions after the reboot
 (May Reboot)	Allows the package to force reboot if required
 (Multi-User Mode)	Performs the installation in ‘Multi-User’ mode
 (Single-User Mode)	Performs the installation in ‘Single-User’ mode
 (Restart Service)	Restarts the service following the deployment
 (Do Not Restart Service)	Does not restart the service following the deployment
 (Reconfigure)	Performs the system reconfigure task following the deployment
 (Do Not Reconfigure)	Does not perform the system reconfigure task following the deployment

9. 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*



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

Button	Action
v	Moves the vulnerability down by one place
vv	Moves the vulnerability to the bottom of the listing

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

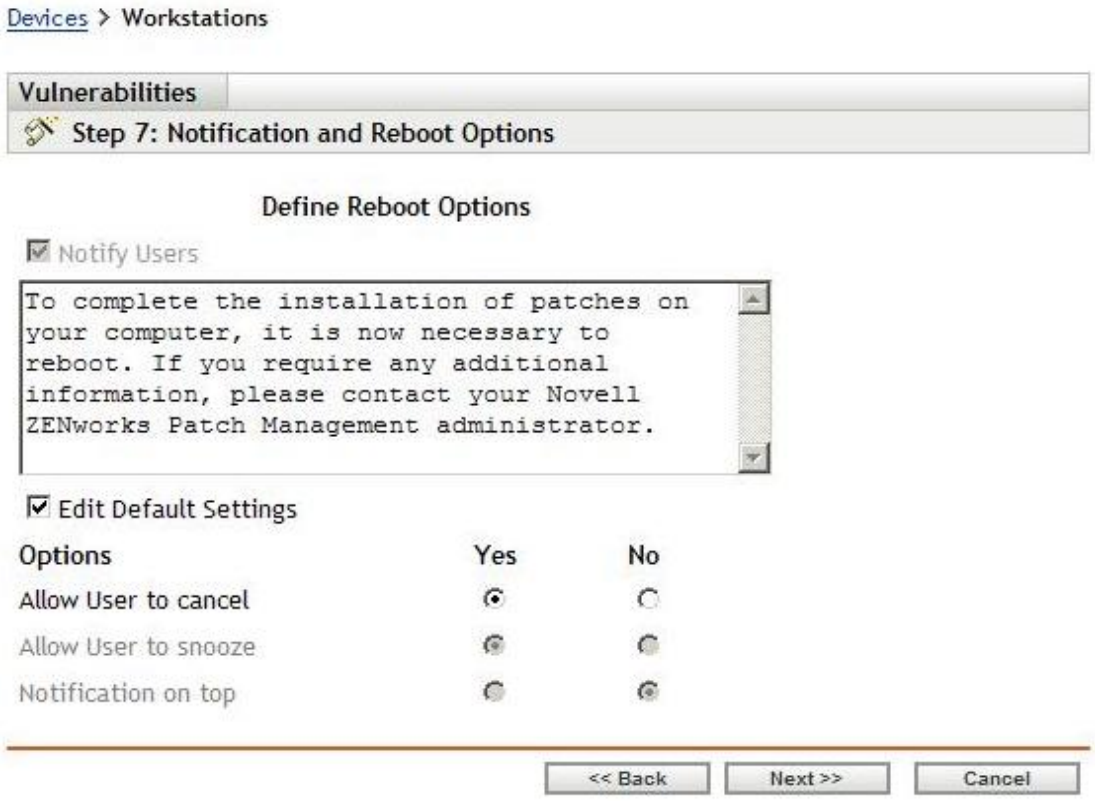
NOTE: Chained vulnerabilities can be moved only after removing their chained status.

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*



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.

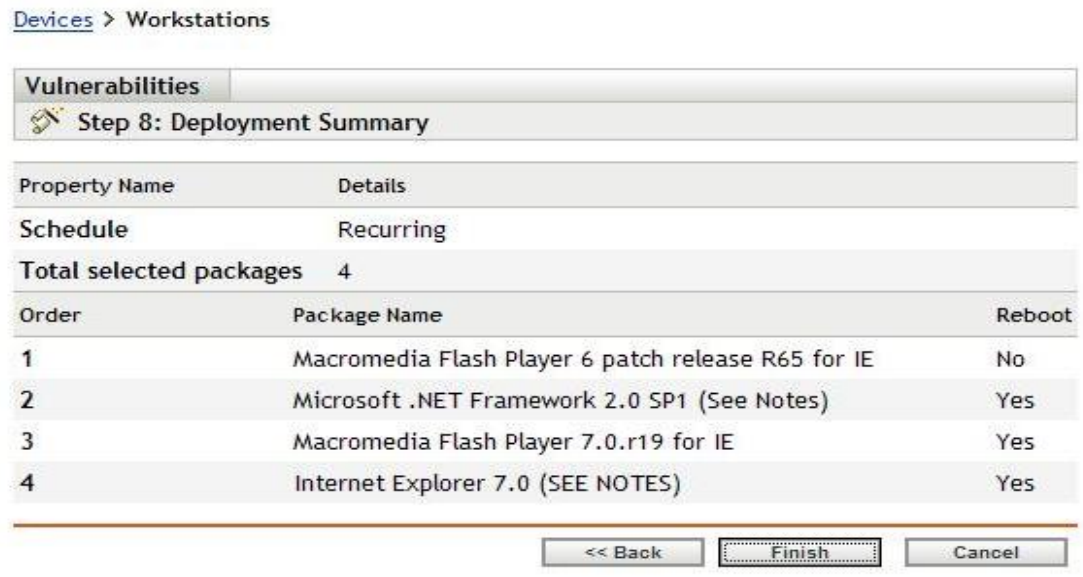
---

11. 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*



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.
- Order: This is the deployment order selected for deployment of the vulnerabilities as defined under the *Deployment Order and Behavior* page.
- 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.

12. 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 Services mandatory baselines:

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.

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

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

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

NOTE: Some patches such as MDAC and IE require both reboot 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:

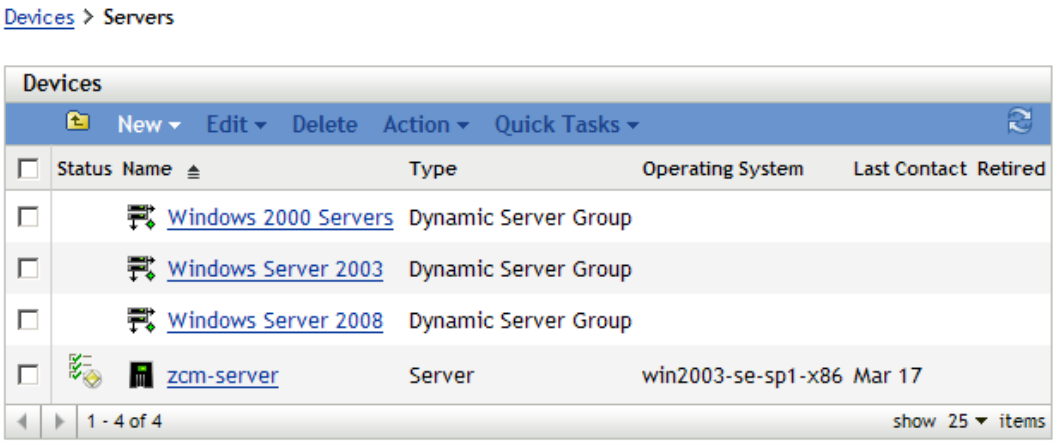
1. Click the *Devices* tab in the left panel. A page displaying the root folders for each type of device appears, as shown in Figure 5-1.

Figure 5-1 *Root Folders of Device Groups*

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.

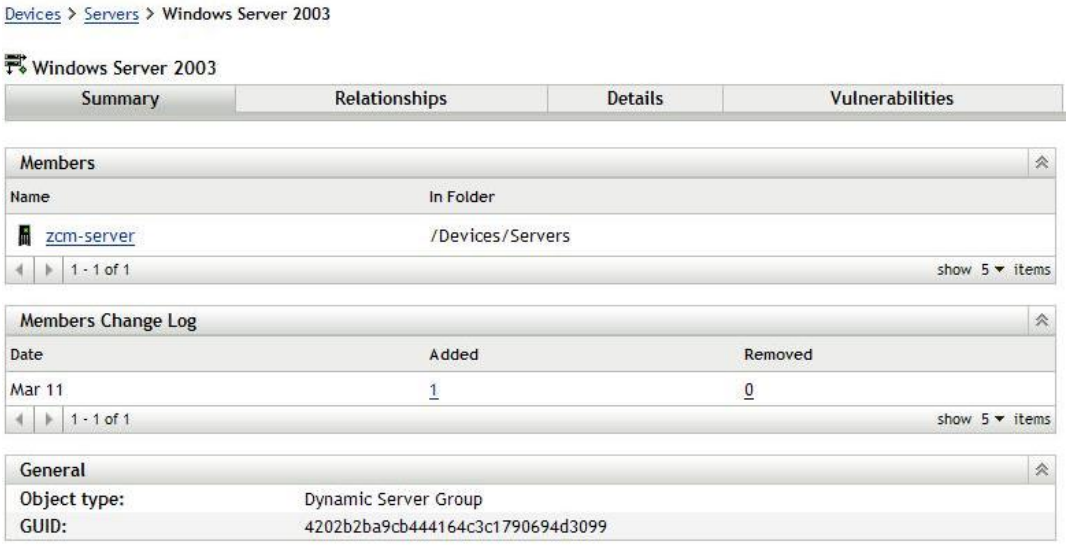
2. Click the *Server* or *Workstation* link. A list of server or workstation groups classified on the basis of their operating systems appears. Figure 5-2 shows a list of server groups, by way of an example.

Figure 5-2 *List of Server Groups*



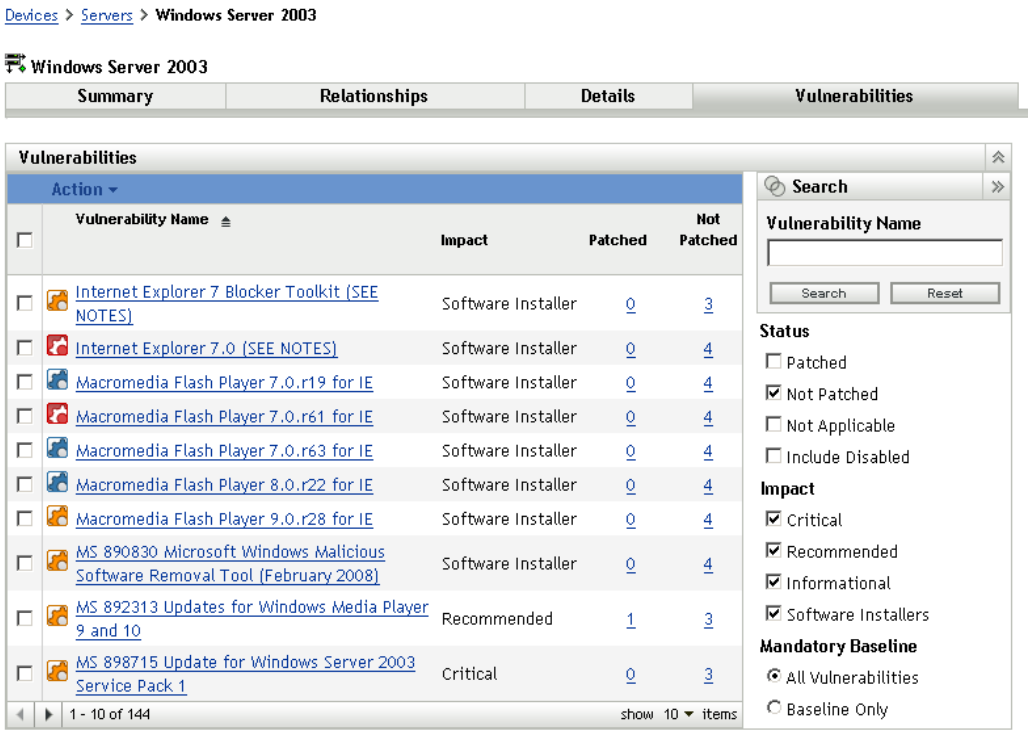
3. On the *Servers* or *Workstation* page (in this case, it is the *Servers* page), select any group. A page displaying the general details of the group and the members in the group appears. Figure 5-3 shows such a page that appears when a Dynamic Server Group called 'Windows Server 2003' is selected.

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*



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 on 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 on the *Mandatory Baseline* page to view the baseline vulnerabilities.

The *Search* panel on 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.

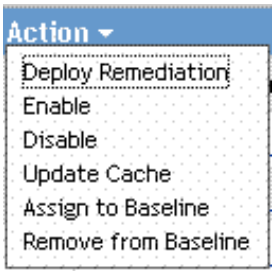
Figure 5-5 *Mandatory Baseline Search*

5.2 Working with Mandatory Baselines

The *Action* menu on the *Device Group Vulnerabilities* page enables you to perform various actions concerning the mandatory baseline vulnerabilities. The *Action* menu options also assist you in

managing and deploying vulnerabilities in a consistent and uniform manner across groups. 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 *Assign to Baseline*, *Remove from Baseline*, and *Update Cache* options, see the following three sections:

- Section 5.2.1, “Assigning or Managing a Mandatory Baseline,” on page 57
- Section 5.2.2, “Removing a Mandatory Baseline,” on page 58
- Section 5.2.3, “Using Update Cache,” on page 58

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 *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 Server automatically schedules a daily Discover Applicable Updates task for all devices in that group.
2. Every few hours, depending on the results of the DAU task, the ZENworks Server determines the devices that are applicable and out of compliance (based upon the vulnerabilities added to the baseline).
3. Necessary bundles, as defined in the baseline, are deployed as soon as possible for each device.

4. Once patches have been deployed, it may be necessary to reboot those devices for them to be detected as patched.

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

5.2.2 Removing a Mandatory Baseline

To remove patches from a mandatory baseline, repeat steps 1 to 4 in the *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 download process for the bundles associated with a selected vulnerability and caches those bundles on your ZENworks Server.

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

To update caching of vulnerability data:

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

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

Using Devices

6

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

6.1 About Devices

Review the following section:

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:

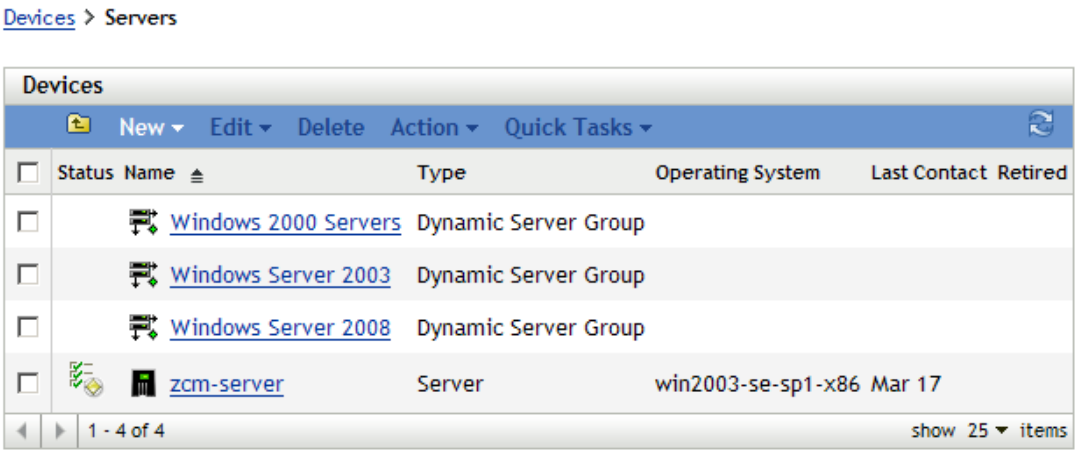
1. Click the *Device* tab on the left panel. A page displaying the root folders for each type of device appears as shown in Figure 6-1.

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.

Figure 6-2 *The List of Server Groups*

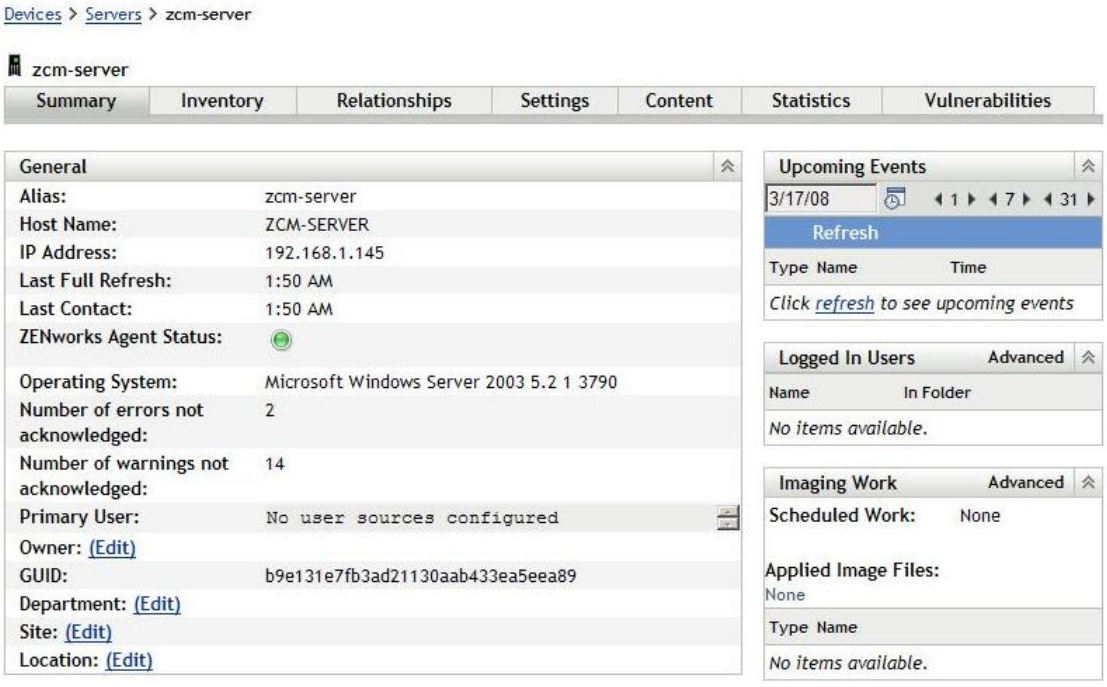


3. Click the required group (Server or Dynamic Server Group) to view details of the group and the members of the group. Alternatively, you can click the managed device. A page displaying details about the managed device or member appears. See Figure 6-3.

   NOTE: The name "zcm-server" for the managed device is by way of an example. The network administrator will decide the name of the managed device.

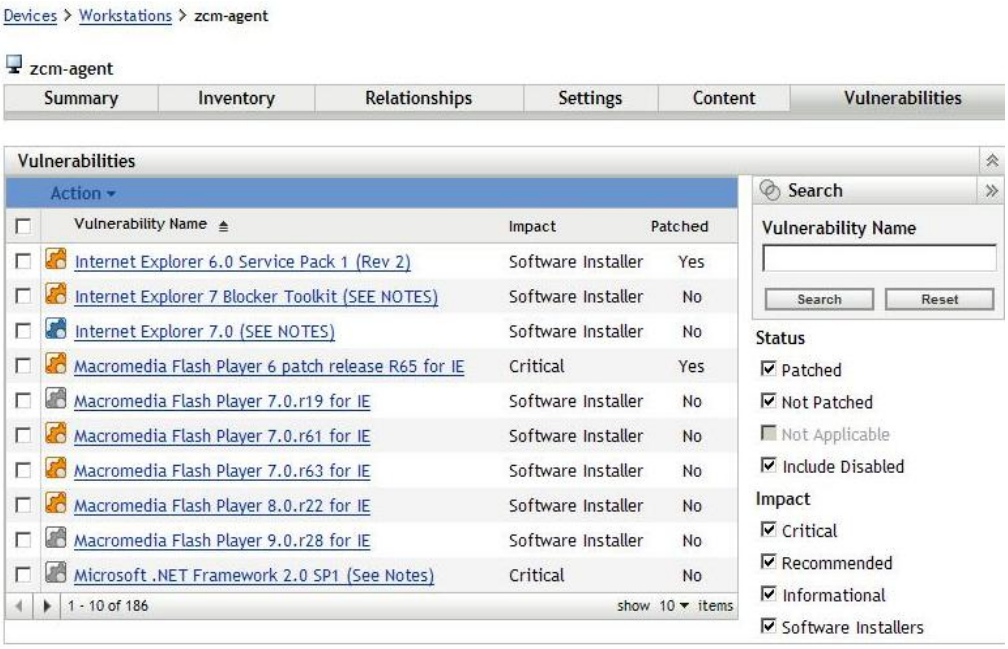
   Figure 6-3 shows the page displaying details for the managed device named "zcm-server."

Figure 6-3 *Device Details Page for a Managed Device*



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

Figure 6-4 *Vulnerabilities Associated with a Managed Device*



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

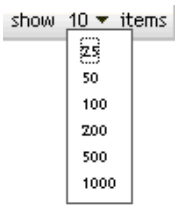
Vulnerabilities

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.



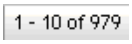
Vulnerability Name

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.

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.



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 into this category. ZENworks Server automatically downloads and saves the vulnerabilities that have critical impact.
- Recommended: Novell has determined that this vulnerability, although not critical or security related, is useful and should be applied to maintain the health of your computers. Therefore, Novell recommends vulnerabilities that fall in 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.

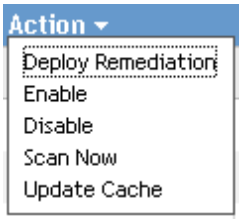
Vulnerability Statistics

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 check box 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 check box 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 (DAU) task for immediate execution. The DAU runs on a predefined interval schedule. A manual scan schedules the task for immediate execution.
- *Update Cache*: This option initiates a download process for the bundles associated with the selected vulnerability and caches those bundles on your ZENworks Server.

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

To use this option:

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

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

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 Macromedia Flash Player 7.0.r19 for IE from the list of vulnerabilities, the *Vulnerability Information* section displays the result of a vulnerability analysis for the selected vulnerability, as shown in Figure 6-5.

Figure 6-5 *Vulnerability Information for Selected Vulnerability*

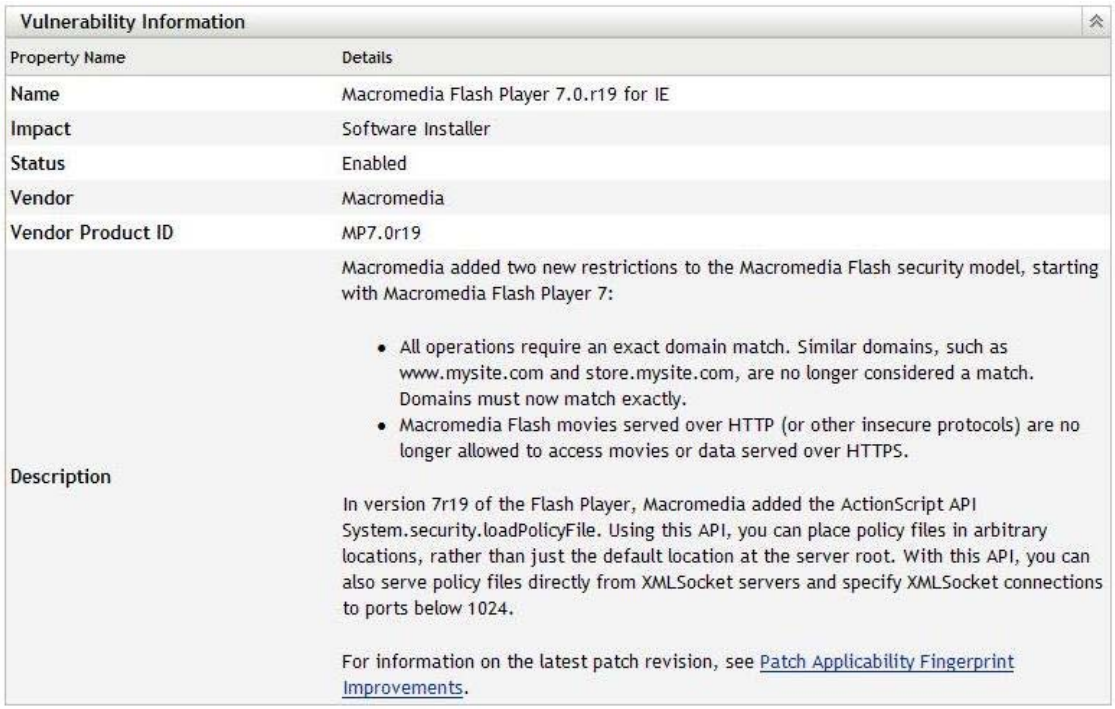


Table 6-1 below defines each property name in the *Vulnerability Information* section.

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 Vulnerability Impacts
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

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

Searching Vulnerabilities

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

To search a vulnerability:

1. Enter full or part of the vulnerability name in the *Vulnerability Name* text box.
2. Select the required check box 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 following table 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.
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*

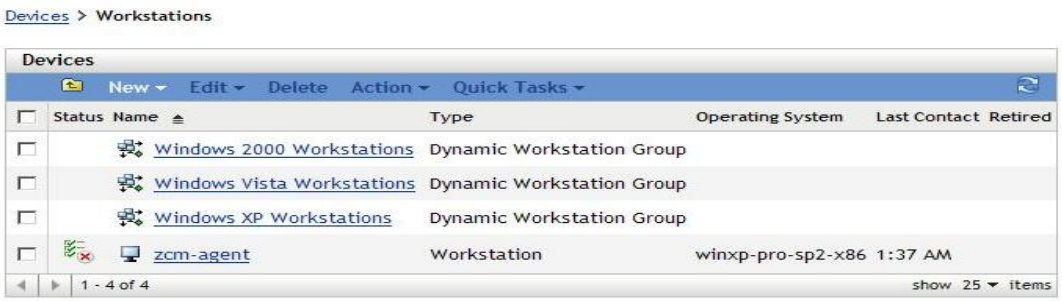
Impact Filter	Result
Critical	Search results will include all the vulnerabilities in the vulnerability list that are classified as Critical by Novell.
Recommended	Search results will include all the vulnerabilities in the vulnerability list that are classified as Recommended by Novell.
Informational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

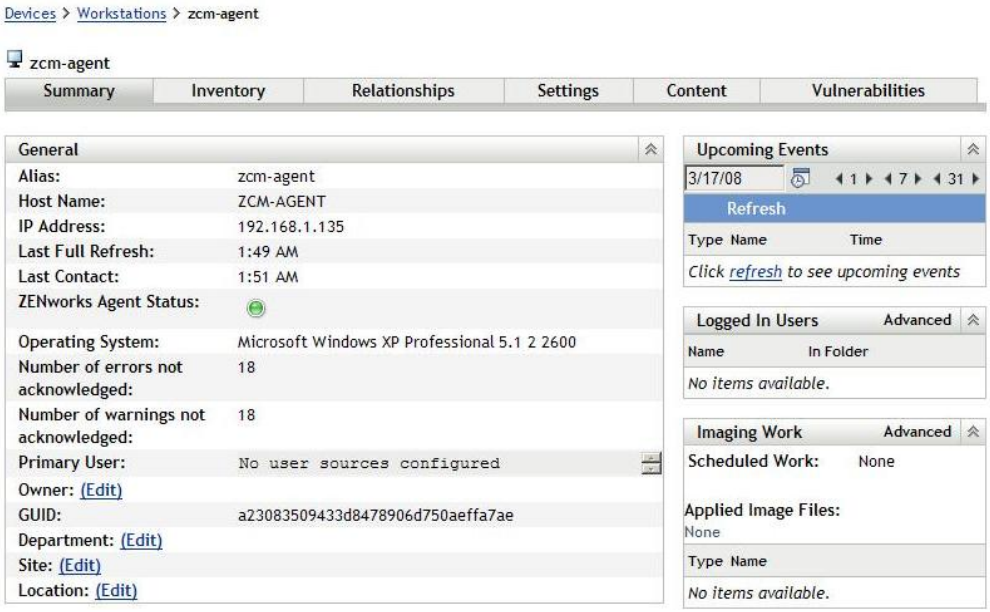


2. Click the required group (Workstation or Dynamic Workstation Group) to view details of the group and the members of the group.
3. Click the required member or workstation device. A page displaying details of the member appears. See Figure 6-8.

   NOTE: The name "zcm-agent" is by way of an example.

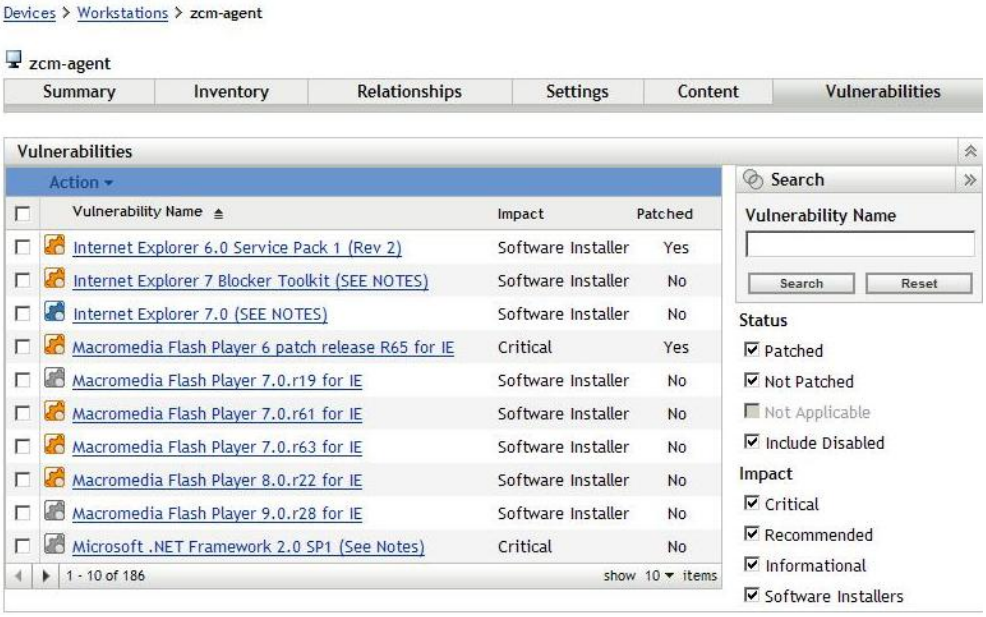
   Figure 6-8 shows the page displaying details for the workstation device “zcm-agent.”

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



4. 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*



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 servers group or the workstations 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.

7.1 Server Group Vulnerabilities

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

To view the vulnerabilities for a specific group of servers:

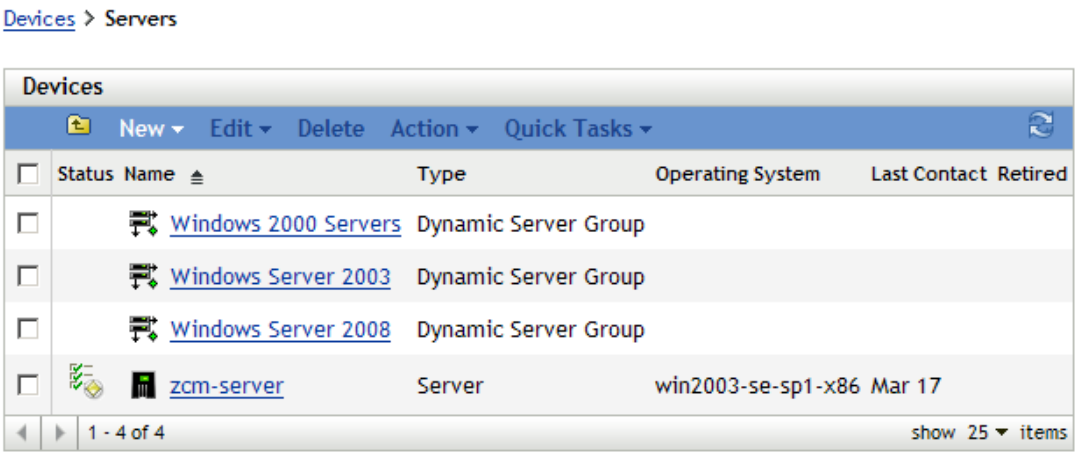
1. Click the *Devices* tab on the left panel. A page displaying the root folders for each type of device appears, as shown in Figure 7-1.

Figure 7-1 *Root Folders of Device Groups*

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.

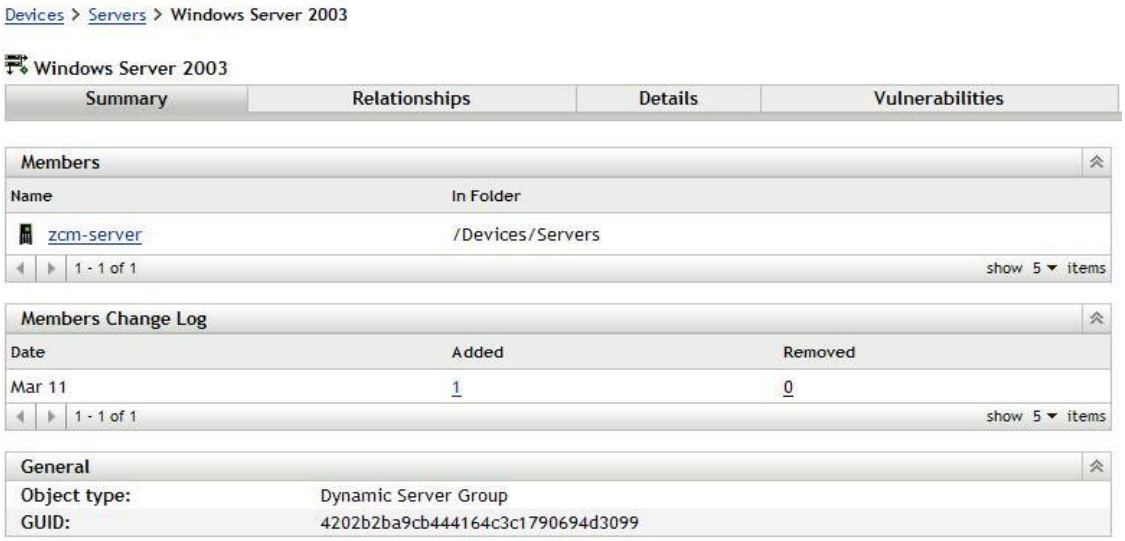
2. Click the *Servers* link. A list of server groups classified on the basis of their operating systems appears, as shown in Figure 7-2.

Figure 7-2 *List of Server Groups*



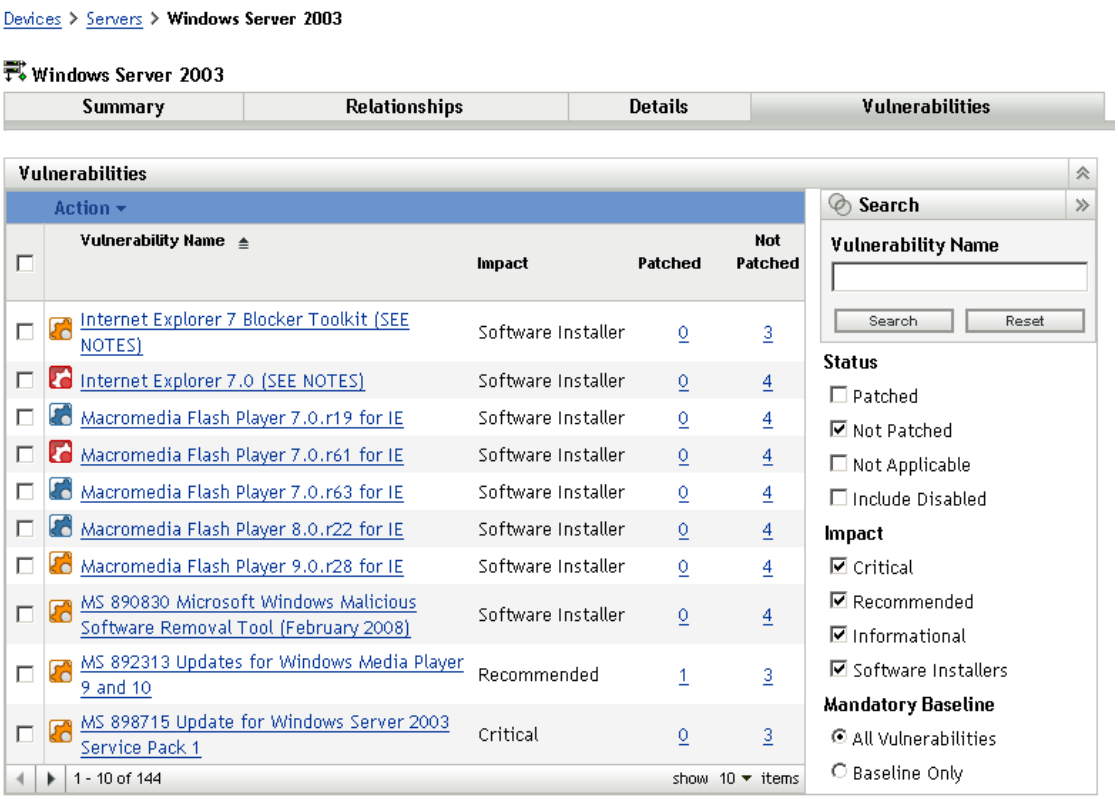
3. Click the required group (Server or Dynamic Server Group). A page displaying the general details of the group and the members in the group appears. Figure 7-3 below shows such a page that appears when the Dynamic Server Group type Windows Server 2003 is selected.

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



For information on the features of the *Device Group Vulnerabilities* page for the selected server group, see the section Mandatory Baseline.

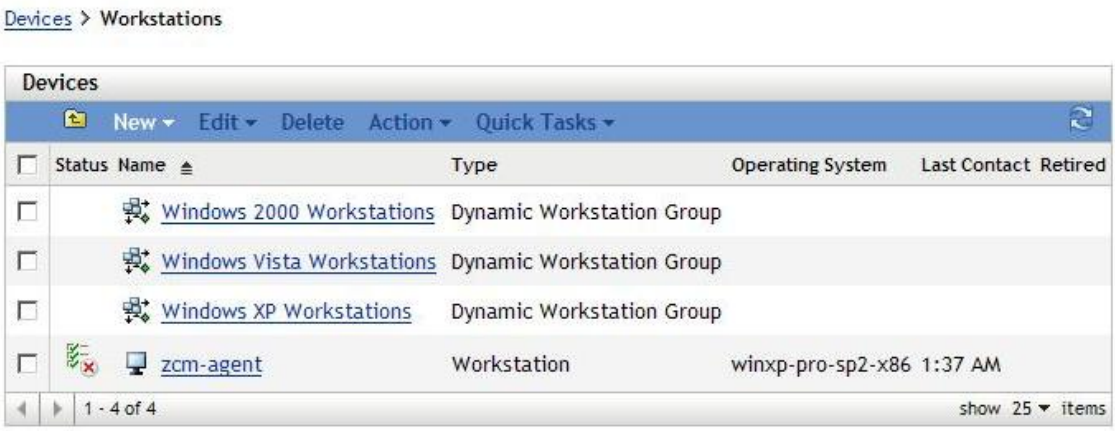
7.2 Workstation Group Vulnerabilities

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 on the left panel. A page displaying the root folders for each type of device appears, as shown in Figure 7-1.
2. Click the *Workstations* 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*



3. Click the required group (Workstation or Dynamic Workstation Group). A page displaying the general details of the group and the members in the group appears. The following Figure 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*

For information on the features of the *Device Group Vulnerabilities* page for the selected workstations group, see Mandatory Baseline.