

ZENworks 2020 Update 1 Patch Management Reference

June 2020

Legal Notice

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

Copyright 2008 - 2021 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors (Micro Focus) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contents

About This Guide	7
1 Patch Management Overview	9
Features of Patch Management	9
Supported Environments and Patch Content	10
Product Overview	11
Patch Management Process and Workflow	12
2 CVE and Patch Management	15
What is a CVE?	15
Using CVEs with ZENworks Patch Management	15
Additional Information About CVEs	16
3 Configure Patch Management	17
Licensing Patch Management	17
Viewing and Configuring the Subscription Service	20
Subscription Service Settings	21
Configuring the HTTP Proxy Detail	22
Configuring Patch Subscription Credentials	22
Configuring Subscription Service Content Download	23
Cleaning up Patch Content	26
Register for or Migrate to RHSM	30
Configuring Email Notification	31
Configuring Patch Dashboard and Trending	31
Configuring the Schedule for Vulnerability Detections	31
Setting Vulnerability Detection at the Folder Level	35
Initiating a Patch Scan	35
Scan using updated patch scan signature (DAU) file	35
Scan using device's current patch scan signature (DAU) file	35
No scan; retrieve existing scan results only	35
Configuring Patch Policy Settings	36
Schedule Enforcement	36
Patch Policy Reboot Behavior	38
Configure Patch Policy Settings at the Folder Level	39
Configuring Patch Policy Pre-Install Behavior	39
Schedule Distribution	39
Pre-Install Notification Options	41
Configure Patch Policy Pre-Install Behavior at the Folder Level	41
4 Assess Vulnerabilities	43
Security Pages	43
Employing the Security and Patch Dashboard	43
Viewing Patch Policies	50

Viewing Zone Patches	50
Viewing Patch Status	51
Viewing Patches for a Device	52
Accessing Patch Management Reports	55
Generating Patch Audit Reports	56
5 Distribute and Apply Patches	57
Creating and Publishing Patch Policies	57
Patch Policy - Best Practices	57
Create a Patch Policy	59
Editing Patch Policies	63
Assign a Patch Policy to Devices	64
Test a Policy Before Deploying to a Live Environment	64
Publish a Patch Policy	65
Deploying Patches Manually	66
Create a Deployment Schedule	66
Confirm Devices	67
License Agreement	68
Remediation Schedule	69
Deployment Order and Behavior	72
Remediation Options	73
Advanced Remediation Options	73
Pre Install Notification Options	75
Distribution Schedule	76
Notification and Reboot Options	79
Choose Deployment Name	81
Deployment Summary	81
6 Best Practices	83
Testing Patches	84
Deploying Patches in a Controlled Way	84
Monitoring Patch Implementation	84
7 Manage Patches	87
Configure the Patch Display	87
View Patch Details	88
Zone-Level Patches	88
Device Patches	94
Create a Custom Patch	102
Delete a Patch	103
Execute Action Menu Options	104
Release Quarantined Patches	105
Quarantine Folder	105
Patch Details Page	106
Patch Information	106
Relationships	108
Devices	109
Patch Requirements	110
Applicability Requirements	110
Patched Requirements	110

A Troubleshooting	111
Patch Management Issues	111
Configuration Issues	120
Error Codes	120
B System Variables	131
Patch Management System Variables	131

About This Guide

This *ZENworks Patch Management Reference* includes information to help you successfully license, configure, navigate, and employ a ZENworks Patch Management system.

Audience

This guide is intended for ZENworks administrators.

Feedback

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

Additional Documentation

ZENworks is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. See [ZENworks Documentation](#).

1 Patch Management Overview

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

Features of Patch Management

Patch Management has the world's largest repository of automated patches, including patches for all major operating systems and various third-party applications. By preconfiguring Patch Management to detect patch vulnerabilities and then creating policies to patch those vulnerabilities, Patch Management can quickly cache patches from the patch repository and deploy them to managed devices.

Patch Management creates a Patch Fingerprint Profile that includes all missing patches for each machine, ensuring the continued compliance of each end point. Each end point is then continually monitored to make sure it stays patched. In addition, because many organizations need to demonstrate patch compliance, Patch Management provides standard reports that document changes and demonstrate progress toward internal and external audit and compliance requirements.

The following table describes the important features of Patch Management:

Table 1-1 Patch Management Features

Feature	Description
Patented multi-platform patch management	Enables security of all operating systems and applications within heterogeneous networks, including Windows (32-bit and 64-bit) and Linux distributions. US Pat #6999660.
World's largest automated patch repository	Provides the largest repository of tested patches to support all major operating systems and applications used in the enterprise.
Policy-based administration	Ensures that all systems meet regulatory compliance by using patch policies to deploy patches on devices that need them.
Extensive pre-testing	Reduces the amount of development and testing required prior to patch deployment.

Feature	Description
Agent-based architecture	Protects laptop and mobile devices that are often disconnected from the network, and reduces network bandwidth usage.
Automatic notifications	Distributes e-mail alerts directly to administrators for proactive security and administrative management.
Patch fingerprint accuracy	Ensures the highest level of accuracy in the detection of security patches.
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.

Supported Environments and Patch Content

Platforms that Patch Management supports for installing and operating Patch Management are congruent with system requirements for the ZENworks suite.

Refer to the system components below to see their supported Patch Management platforms:

- ◆ [Primary Servers](#)
- ◆ [Satellite Servers](#)
- ◆ [Managed Devices](#)

For a complete list of requirements for the ZENworks system, see the [ZENworks 2020 Update 2 System Requirements](#).

NOTE: SUSE Linux Enterprise distributions require [rpm-python](#) installation as a prerequisite to run the patch scan process. This package is typically installed by default on the ZENworks-supported distributions. If rpm-python is not installed, you must manually install it for the patch scan engine to return an accurate patch status.

Supported patch content: The Patch Management Content Development Team continuously evaluates vendor patch solutions for emerging threats to provide the latest patch content support for operating systems and applications used by ZENworks Patch Management customers.

Due to the evolving nature of patch content support, the ZENworks Patch Management team issues a *Content Quarterly* report with updated information about vendors, products, and product versions that are supported with patch content via the Micro Focus Global Subscription Service (GSS). To access the latest Content Quarterly, see the [ZENworks-Patch-Management-Content-Report.pdf](#).

For relevant Cool Solution articles about Microsoft updates, reference the links below:

- ◆ [ZENworks Patch Management support for Windows 7 and 8.1 updates \(https://www.novell.com/communities/coolsolutions/zenworks-patch-management-support-windows-7-8-1-updates\)](https://www.novell.com/communities/coolsolutions/zenworks-patch-management-support-windows-7-8-1-updates)

- ♦ [Update to ZENworks Patch Management support for Windows 7 and 8.1 updates \(https://www.novell.com/communities/cool solutions/update-zenworks-patch-management-support-windows-7-8-1-updates\)](https://www.novell.com/communities/cool solutions/update-zenworks-patch-management-support-windows-7-8-1-updates)
- ♦ [ZENworks Patch Management Support for Windows 10 Updates \(https://www.novell.com/communities/cool solutions/zenworks-patch-management-support-windows-10-updates\)](https://www.novell.com/communities/cool solutions/zenworks-patch-management-support-windows-10-updates)
- ♦ [Patching Microsoft Office 365 \(https://www.novell.com/communities/cool solutions/patching-microsoft-office-365/\)](https://www.novell.com/communities/cool solutions/patching-microsoft-office-365/)

Product Overview

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

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

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

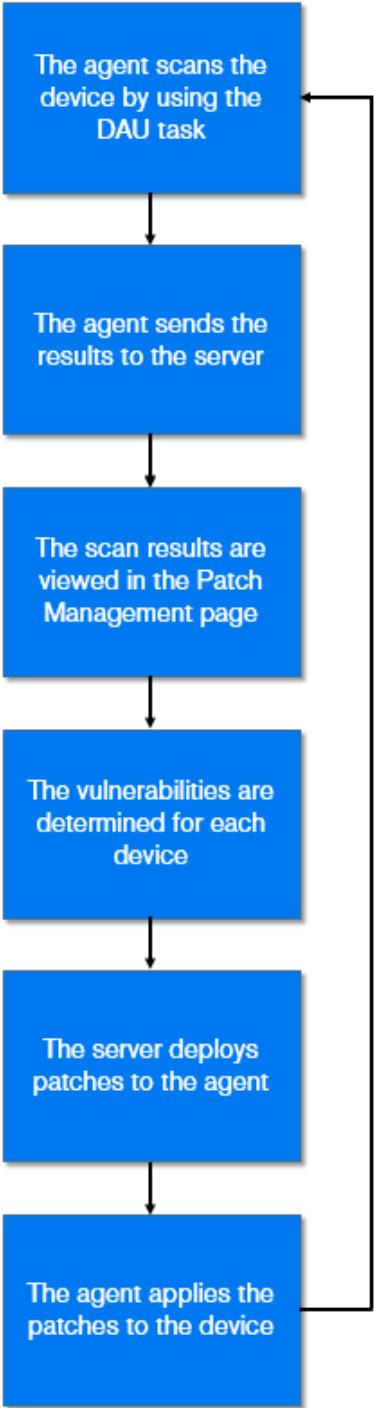
When a new patch is released into the ZENworks Patch Subscription Network, it is downloaded automatically to the ZENworks Server and an e-mail is sent to the administrator. When the administrator logs in to the ZENworks Control Center, the list of devices and the new patches that require deployment can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

NOTE: ZENworks Patch Management provides software updating and patching services for Windows operating systems and applications, eliminating the need to run the Microsoft Windows Update service. If necessary, however, you can continue to run Windows Update service on the same device as ZENworks Patch Management. Regardless of which solution performs the patch installation, ZENworks Patch Management detects and reports the installation status and source, allowing you to easily monitor the patch compliance of your devices in ZENworks Control Center.

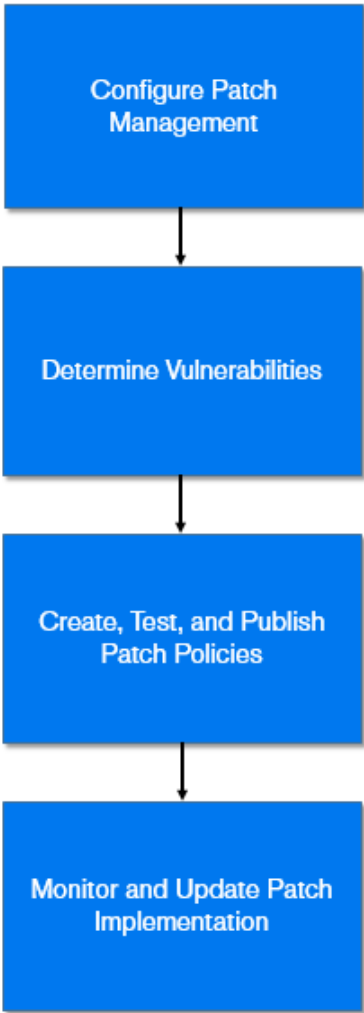
Patch Management Process and Workflow

The following process maps demonstrate how patch information is communicated between the ZENworks Server and the ZENworks Agent and the general workflow administrators use to implement patch policy across the management zone:

System Process



Administrator Workflow



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

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

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

After completion of the patch detection cycle, patches will either be distributed via patch policies or the ZENworks administrator will deploy the desired patches to each applicable device on the network.

2 CVE and Patch Management

Using the Patch Management feature you can view the patches that are published and identify if the devices in your zone are vulnerable or not. However, information about the vulnerabilities being addressed by the patch is not easily available. You have to either know the CVE Identifier or you have to check the patch details to identify the vulnerability being addressed by the patch. ZENworks now provides an enhanced security view into the vulnerabilities on the devices by introducing the ability to map Common Vulnerabilities and Exposures (CVE) to the related patches in ZENworks 2020.

What is a CVE?

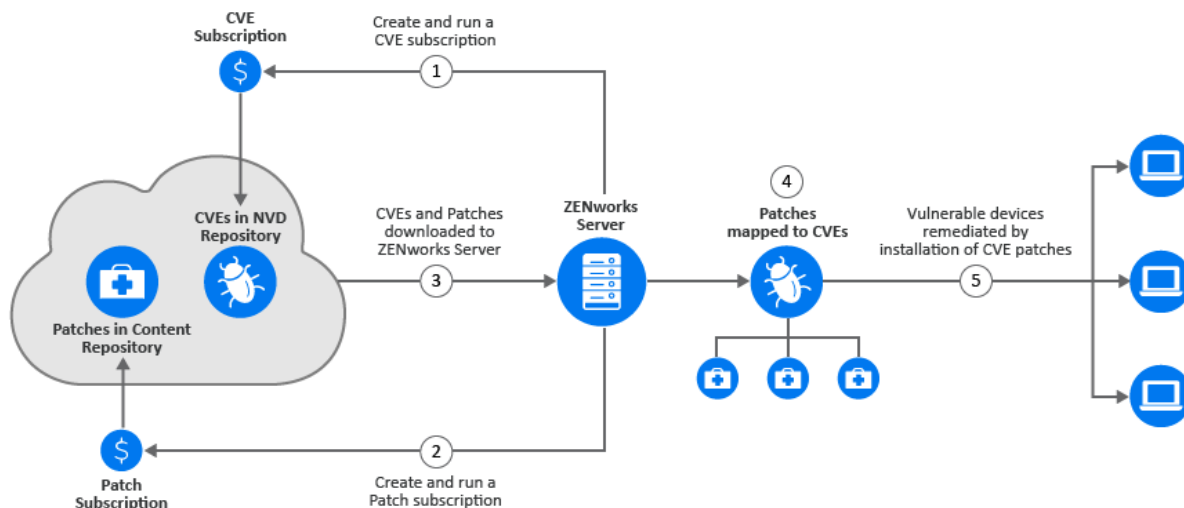
CVE is a list of entries for publicly known cyber security vulnerabilities and exposures. Potential security vulnerabilities are discovered and assigned a CVE ID and description by a CVE Numbering Authority (CNA). The CVE entry is added to the CVE list on cve.mitre.org. The U.S. National Vulnerabilities Database (NVD) imports new CVE entries and adds severity scores and fix information.

ZENworks now provides you with a better security view through CVEs. You can track vulnerabilities through the use of CVEs and then remediate the vulnerabilities through the application of the associated patches to the devices. In order to use CVEs you need to first create a CVE subscription and to view the patches associated with the CVEs you need to create a Patch subscription as well.

Using CVEs with ZENworks Patch Management

With Patch Management, after the patches are downloaded to the ZENworks server and a patch scan is performed, you can identify the vulnerable devices in your zone. However, you cannot easily identify the vulnerability addressed by the patch. To identify the vulnerability addressed by the patch you need to view the Patch Details window or you need to know the CVE ID based on which you can perform a search. However, now, as part of the Security feature, ZENworks provides you with a new security view that simplifies the setting up and tracking of security in your zone. You can quickly grasp the security posture of your devices with the vulnerability based view and approach to

remediation. You can identify patches based on the CVE information and then remediate the vulnerable devices by applying the relevant patch policy or remediation bundle. The process by which ZENworks identifies these vulnerabilities is as follows:



- 1 Create and run a CVE subscription to import data from the NVD repository.
- 2 Create and run a Patch subscription to import data from the Patch Content repository.
After the CVE and Patch subscriptions are run, CVEs and Patches are imported to the configured ZENworks Server.
- 3 ZENworks maps the patches to the CVEs, based on the CVE ID associated with the patch signature.
When a patch scan is performed on devices as part of the device refresh, the vulnerable devices are identified. Users can also configure the patch scan schedule or they can manually run the initiate patch scan quick task based on their requirement.
- 4 The applicable patches are then deployed on the vulnerable devices, either through patch policies or through remediation bundles.

After all the CVE's patches are installed on the device, the device is no longer vulnerable.

Additional Information About CVEs

For additional information about CVEs see the [CVE Reference](#).

3 Configure Patch Management

Before using ZENworks Patch Management, you need to activate the [license subscription](#) and configure the following settings:

- ◆ [Subscription Service Settings](#)
- ◆ [Subscription Service Content Download](#)
- ◆ [Email Notification](#)
- ◆ [Dashboard and Trending](#)
- ◆ [Vulnerability Detection Schedule](#)
- ◆ [Patch Policy Settings](#)
- ◆ [Patch Policy Pre-Install Behavior](#)

Licensing Patch Management

Access the Patch Management License page to view and verify the patch management subscription for the ZENworks Primary Server. You can also activate or renew your paid subscription if 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 Patch Management Subscription Service.

- 1 Click **Configuration** in the navigation menu to display the Configuration page:
- 2 If necessary, expand the **Licenses** section:
- 3 Click **ZENworks 2020 Patch Management**.

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

Patch Management offers the following licenses:

Table 3-1 Patch Management Licenses

License Type	Description
<i>Trial</i>	Denotes trial access to all features of Patch Management for 60 days.
<i>Extended Trial</i>	Denotes continued access to some Patch Management features after the initial 60-day trial, up to 12 months since ZENworks service is installed.
<i>Valid</i>	Denotes a valid subscription license.

License Type	Description
<i>Trial Expired</i>	Denotes that the initial 60-day trial period or the extended trial period has ended, depending on the license in use earlier.
<i>License Expired</i>	Denotes expiry of the current Patch Management license.
Company Name	Name of the company that Patch Management Service is registered to.
Email Address	E-mail address that you can use for receiving alerts and for future communications.
Account ID	Key created by the ZENworks Server, which is passed to the Patch Management Subscription Service and used to validate the update request.
Total Non-Expired Licenses	Total number of active licenses. Each registered device requires one license.
Description	The description of the license or the name of the license.
Vendor	The source where the license was purchased.

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

- ◆ **Trial:** All Patch Management capabilities are free to use for 60-days. The 60-day evaluation period starts when you starts the Patch subscription service and not from when you install the product.
- ◆ **Extended Trial:** On any installation (new or old), you can request a 90-day evaluation key by filling out a [form](#). The 90-day time period starts when the evaluation key is specified. During this license period, only Windows devices have Patch Management support. You can only download new patches released by Microsoft and run Vulnerability Detection for those patches. Patches that were cached previously will have their content cleared so you cannot deploy them. Other features disabled are patch caching, remediation, and generation of reports. In addition, a message appears, asking you to purchase a Patch Management license.
- ◆ **Valid:** All Patch Management functions are available.
- ◆ **Trial Expired:** After the trial ends, the Server will not download any new patches. All Patch Management functionalities are disabled and you will receive a message asking you to purchase a Patch Management license.

If ZENworks Configuration Management is not enabled, the Patch subscription is stopped, and no new patch signatures or patch content is downloaded. Scanning and remediation using the existing patches will not be stopped, but nothing new will be added.

If ZENworks Configuration Management is enabled, ZENwork Patch Management continues to download Windows patch signatures so that scans of Windows devices take place and results are reported. However, the patch content cannot be downloaded, so no remediation can occur. This takes place for 1 year.

- ◆ **License Expired:** After the license expires, the Server will not download any new patches. However, you can continue to use all Patch Management features on the patches downloaded prior to license expiration.

NOTE: During the evaluation period (keyed or key-less), ZENworks Patch Management is available for all platforms (Windows, Linux, Mac). Devices can be scanned, results reported, and devices patched.

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

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

- 1 Enter a valid subscription serial number for Patch Management.
- 2 Revalidate the subscription serial number.

The license record is now valid, and displays serial number, status, expiration date, purchased for the License Record.

To validate the serial number and obtain the authorization to download patches, the Primary Server on which patch subscription is being downloaded must have port 443 (HTTPS) access to <https://novell.patchlink.com/update>, for ZENworks 2017 Update 3 and later, use <https://download.novell.com/patchlink> for license verification.

The Patch Management content distribution network is a global cache infrastructure with many servers. Downloading patches from this network requires port 80 (HTTP) access to https://novell.cdn.heatsoftware.com/novell/<release_version>.xml. The `release_version` is ZEN2020, ZEN2020U1 or ZEN2020U2. For security reasons, it is also recommended that SSL access to the Internet should be allowed. The **SSL** option is enabled by default and downloads the lists of patches from a secure and trusted site.

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

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

Table 3-2 Patch Management License Items

Item	Definition
Activate product	Activates the patch management service. The Patch Management page is restored in the main panel and the Patch Management section is restored in the Configuration panel.
Deactivate product	Deactivates the patch management service. The Patch Management page is removed from the main panel and the Patch Management section is removed from the Configuration page.
Product Subscription Serial Number	Patch Management license number (serial number).
Company Name	Name of the company that Patch Management Service is registered to.
Email Address	E-mail address that you can use for receiving alerts and for future communications.

Item	Definition
Account ID	Key created by the ZENworks Server, which is passed to the Patch Management Subscription Service and used to validate the update request.
Total Non-Expired Licenses	Total number of active licenses. Each registered device requires one license.
Description	The description of the license or the name of the license.
Status	Status of license verification. When verification begins, the status reads Initializing Verification . When replication ends, the status reads Completed .
Vendor	The source where the license was purchased.
Expiration	The date the licenses expire. Typically, licenses expire one calendar year from the date of purchase.
Purchased	The total number of licenses purchased with the product.

After you enter the serial number, you can verify the license by clicking the **Action** drop-down list on the Patch Management License page and selecting **Verify License**.

To start the license verification process, click **Apply**. Automatic verification of the license happens every day with the replication process.

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

NOTE: You can check the license verification status under **Security > Patch Dashboard > Patch Subscription**. 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.

Viewing and Configuring the Subscription Service

To configure the Subscription Service, in the navigation menu click **Configuration > Security > Patch Subscription Service Settings**.

Subscription Service Settings

The following table describes each status item featured in Subscription Service Settings and how to start the service:

Subscription Service Setting	Definition
Start Subscription Service	<p>Select a server from the drop-down list, and click Start to start the subscription service.</p> <ul style="list-style-type: none">After the subscription service starts running, the Start button reads Service Running.If there are multiple ZENworks Servers in your management zone, you can select any one of them to be the Patch Management Server. <p>The Patch Management Server selected will download new patches and updates daily, so it should have good connectivity to the Internet.</p> <p>NOTE: Selecting the Patch Management Server can be done only once per zone in this release.</p>
Last Subscription Poll	The date and time of the last successful update.
Subscription Replication Status	The latest status of the process of patch subscription replication.
Subscription Communication Interval (Every Day at)	The time at which the ZENworks Server will communicate with the ZENworks Patch Subscription Network to retrieve new patches and updates.
Update Now	Enables you to manually run the replication process without waiting for the time set in the Subscription Communication Interval.
Reset ZENworks Patch Management Settings	Enables you to set all Patch Management settings, including deployments and patch policies, back to the default state.
Reset Subscription Service	Clears the assigned server and resets the download time to the default 00:00. If a new patch server is selected when the Subscription Service runs, the signature files will be downloaded to the server. This might slightly increase download time from the previous patch server. If previously downloaded patch bundles were replicated to the new server, they are not downloaded again.

Reference the mapping below for descriptions of the execution options:

Button	Action
OK	Save configuration changes and return to the Configuration page.
Apply	Save changes made to Subscription Service Settings.
Reset	Reset the replication status and initiate a complete replication with the ZENworks Patch Subscription Network.
Cancel	Cancel unsaved configuration changes.

Configuring the HTTP Proxy Detail

An HTTP proxy server allows a device to connect indirectly to an HTTP server. When a proxy server is configured, the ZENworks Agent communicates with a ZENworks Primary Server through the configured proxy server. A proxy responds either from the ZENworks Server or from its cache. It reduces bandwidth and improves response time by caching and reusing frequently requested web pages.

To configure HTTP Proxy Server Details:

- 1 Select **Configuration** in the navigation menu, and go to **Configuration > Security > Patch Subscription Service Settings**.
- 2 Refer to the descriptions below to configure HTTP Proxy Server Details.

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

NOTE: If HTTP server credentials are required, they will need to be added to the [Credential Vault](#) before they can be configured in the HTTP Server Details.

- 3 Click **Apply** or **OK** to save changes.


Configuring Patch Subscription Credentials

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

Credentials are required for SUSE 11 and Red Hat distributions using the RHN subscription model. They are not required for SLE 12 and newer distributions or Red Hat distributions using RHSM. Although credentials are not required for these newer distributions and RHSM, these managed devices do need to be registered with SUSE or Red Hat, as applicable, and have access to their external networks to be able to download patch content.

IMPORTANT: All Red Hat clients need to migrate to the RHSM subscription model before July 31, 2017. RHN will no longer be supported after this date. Since RHSM uses certificate-based authentication through native vendor installations and registration, subscription credentials will no longer be required for Red Hat clients after migration.

To configure Patch Subscription Credentials for Linux distributions:

- 1 Select **Configuration** in the ZENworks navigation menu, and go to **Configuration > Security > Subscription Service Settings**.
- 2 Next to the subscription credentials field you want to specify, click **Browse**  to open a browse window to the Credentials Folder.
- 3 Click the arrow next to the **Credentials** option to display the list of available credentials for that subscription provider.

Operating System	Description
Red Hat Network Credentials	Credentials that authenticate with the Red Hat network. (For RHEL 5 & 6 using RHN)
SUSE Network Credentials	Credentials that authenticate with SUSE Customer Center for SUSE 11.

- 4 Select the desired credential, and then click **OK** to confirm credential selection.

NOTE: Red Hat and SUSE credentials will already need to be added to the [Credential Vault](#) before they will be available in Subscription Service Settings. Credentials are not required for SLE 12 and RHEL 7 or Red Hat distributions using RHSM, since those distributions use certificate-based authentication through their native vendor installations and registration.

Adding a Credential

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

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

To add credentials to the Credential Vault:

- 1 Select **Configuration** in the ZENworks navigation menu, and scroll down to the bottom of the **Configuration** page until you see the Credential Vault.
- 2 In the Credential Vault panel, click **New > Credential** to display the Add Credential dialog box.
- 3 Fill in the fields that match your subscription login, and click **OK** to add the new credential.
If you need help, click the **Help** button.

Configuring Subscription Service Content Download

In the Subscription Service Content Download page you configure the subscription download options for the ZENworks Primary Server. These options include choosing platforms, languages, vendors, and other download options. You can select the languages that are used within your

network to ensure that you only download the patches that are most applicable for your organization. The next time replication occurs, only those patches specific to the languages are downloaded, which saves time and disk space on your ZENworks Primary Server.

NOTE: Micro Focus does not recommend selecting all languages because each language can represent hundreds of patches. Downloading unnecessary languages can result in thousands of unused patch definitions within your ZENworks Primary Server database.

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

To configure content download for the Subscription Service, Select **Configuration** in the ZENworks navigation menu, and go to **Configuration > Security > Subscription Service Content Download**.

Refer to the descriptions below to understand and configure the Subscription Service Content Download settings according to your organization's needs:

Item	Description
Select the platforms to download	Enables you to select the operating system platform for which you want to download patches. For example, if you select the Windows check box, only Windows patches are downloaded.
RPM Dependency	This option is only enabled when the LINUX platform is selected. Selecting this check box will download all the root level dependencies that will be necessary to resolve any vulnerabilities. NOTE: This option is not applicable for SLES 12 and later versions.
Red Hat Linux Subscription Management	Enables you to retain the current default subscription type (RHN Classic) for Red Hat systems or to migrate to the preferred subscription type by choosing RHSM , which is a much more efficient method of getting security content from Red Hat. For information on RHSM registration or migration, see Register for or Migrate to RHSM . NOTE: RHSM is currently required for RHEL 7 clients. Effective July 31, 2017 it will be required for all RHEL clients.
Choose your Windows language options	Enables you to select the language of patches you want to download. For example, if you select the French check box, only French language patches are downloaded.
Mix Multiple Languages	Enables you to combine all languages into each Patch Detection Assignment (not recommended).
SSL	Enables you to turn secured downloading on or off.

Item	Description
Cache patch bundles to satellite servers	Enables you to cache patch bundles to the servers or workstations that are managed by primary servers.
Cache patch bundles to primary servers	Enables you to cache patch bundles to primary servers only.
Download location for patch content	<p>ZPM directory: Downloads patch signatures to</p> <ul style="list-style-type: none"> ◆ <i>Windows:</i> installpath\zenworks\zpm ◆ <i>Linux:</i> /var/opt/novell/zenworks/zpm <p>Bundle content directory: Temporarily downloads patch content to</p> <ul style="list-style-type: none"> ◆ <i>Windows:</i> installpath\zenworks\work\content-repo\tmp\zpm ◆ <i>Linux:</i> /var/opt/novell/zenworks/content-repo/tmp/zpm <p>When all patches in a bundle are fully downloaded, the patches are imported to</p> <ul style="list-style-type: none"> ◆ <i>Windows:</i> \installpath\zenworks\work\content-repo\content ◆ <i>Linux:</i> /var/opt/Novell/zenworks/content-repo/content <p>NOTE: Actual content of cached patches is downloaded to the Bundle content directory irrespective of the directory selected in the content download configuration.</p>
Enable not applicable patches	Enables patches that are not applicable to your enterprise. This option may slow performance if enabled.
Enable PD caching	Enables local cache for faster Patch Detection results, which eliminates the decryption and decompression of Vulnerability Detections. Only use this feature if you trust end users to stay out of the ZENworks Agent directory. Ideally, workstations users should not have access to the ZENworks agent directory.
Select vendors to use in the system	<p>Enables you to select the vendors to use in the system. You can choose All or the Selected option. The latter enables the check boxes for selecting individual vendors.</p> <p>NOTE: This list of vendors will not be populated until the initial subscription update has completed.</p>
Patch Policy uses only applicable patches	Configures the system to only have applicable patches available for selection when building patch policies.

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

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

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

Cleaning up Patch Content

Using the CVE and Patch Cleanup page, you can delete disabled patch content and data, as well as you can delay the disabling of superseded patches and patches that are no longer required by ZENworks.

To configure patch cleanup settings, click [Configuration](#) in the ZENworks navigation menu, and go to [Configuration > Security > CVE and Patch Cleanup](#).

Refer to the descriptions below to understand and configure the cleanup settings according to your organization's needs:

Item	Description
Disabled Patch Cleanup	<p data-bbox="870 254 1442 369">Specify the time period after which to delete data and content for a disabled patch. This setting deletes the patch listing and any cached bundles for a patch that meets the following conditions:</p> <ul data-bbox="894 401 1422 579" style="list-style-type: none"><li data-bbox="894 401 1159 422">◆ The patch is disabled.<li data-bbox="894 443 1422 495">◆ The patch does not have any dependencies to deployed bundles.<li data-bbox="894 516 1406 579">◆ The patch has been disabled longer than the time duration selected from the drop-down. <p data-bbox="870 600 1398 663">IMPORTANT: Applicable bundles are not deleted until the next subscription update.</p> <p data-bbox="870 684 1442 873">To see if a patch has dependencies to a deployed bundle from a patch policy or remediation, reference the services-messages log, which shows the patches that cannot be automatically or manually deleted because of dependencies. The location of the log is provided below:</p> <ul data-bbox="894 905 1433 1062" style="list-style-type: none"><li data-bbox="894 905 1433 957">◆ Linux: <code>/var/opt/novell/log/zenworks/services-messages.log</code><li data-bbox="894 978 1382 1062">◆ Windows: <code>%ZENWORKS_HOME%\logs\services-messages.log</code> <p data-bbox="870 1094 1333 1115">This setting provides the following options:</p> <ul data-bbox="894 1146 1442 1354" style="list-style-type: none"><li data-bbox="894 1146 1390 1241">◆ Delete disabled patch content after: Specify when the disabled patch content should be deleted. The default value is 6 months.<li data-bbox="894 1262 1442 1354">◆ Delete disabled patch data after: Specify when the disabled patch data should be deleted from ZENworks. The default value is 5 years.

Item	Description
Superseded Patches Disablement	<p>By default, when a patch is superseded by a newer patch, it is disabled and can no longer be applied to devices. In general, this is the desired behavior because best practice dictates that you keep devices updated with the most recent patches in order to minimize security risks. However, you might have situations where you need a superseded patch to remain enabled. The following settings let you change when superseded patches become disabled:</p> <ul style="list-style-type: none"> ◆ Delay disabling of superseded patches xx days: <p>Use this setting to keep superseded patches enabled in your system for up to 90 days. This allows you to continue to deploy the patches to devices either through patch remediations or policies.</p> <p>NOTE</p> <ul style="list-style-type: none"> ◆ You can configure a value other than 30, 60 or 90 days by configuring the <code>PATCH_DELAY_SUPERSEDED_DISABLE</code> system variable. For more information about this system variable, see “PATCH_DELAY_SUPERSEDED_DISABLE” on page 132 ◆ Do not disable superseded patches that are included in a policy: By default, a superseded patch is not removed from a policy and replaced by the superseding patch until the policy is rebuilt and republished. This behavior can result in a period of time where the policy does not apply the superseded patch (because it is disabled) or the new superseding patch (because it is not in the policy). <p>You can use this setting to ensure that patches that are included in a policy are never disabled as long as they are in the policy. Patches that are included in the policy via a rule remain enabled until they are removed when the policy is rebuilt. Patches that are included via the Members list remain enabled until they are manually removed from the list and the policy is rebuilt.</p> <p>Also, if a user enables a superseded patch that is within a policy, but there are no applicable devices, then, on the next subscription update, the patch will get disabled, even though this option is selected.</p> <p>NOTE: Both settings apply only to patches that are superseded after the setting is enabled.</p>

Item	Description
Patches Disablement	<p>This setting disables patch content within the system based on the criteria you select. These options are useful for filtering out obsolete content and enhancing performance. All options are selected by default.</p> <p>More clarifications are provided below for those settings that are often misunderstood:</p> <ul style="list-style-type: none"> ◆ <i>Disable legacy patches that were updated with a newly issued duplicate patch</i> <p>Legacy patches are patches replaced by the vendor with a newly issued patch, generally in a shorter time frame than a superseded patch. They are not superseded patches.</p> ◆ <i>Disable obsolete security patches</i> <p>Obsolete patches are patches discontinued by the vendor, but not replaced. They are not superseded patches.</p> ◆ <i>Detect only the current supported Service Packs</i> <p>This setting enhances the timeliness of deploying the latest service pack patches to managed devices, as opposed to scanning for non-applicable patches in the DAU.</p> ◆ <i>Disable older patches by age</i> <p>This setting enables you to delete patches based when they were released by the OS Vendor or a Third-party Vendor.</p> ◆ <i>Disable patches for specific cultures</i> <p>This setting enables you to disable patches that are specific to cultures such as United Kingdom (English) and South African (English).</p> ◆ <i>Disable Windows Embedded patches</i> <p>This setting enables you to disable Windows Embedded patches.</p>

Register for or Migrate to RHSM

The Red Hat Subscription Management service (RHSM) is the latest model provided by Red Hat to register for Red Hat subscriptions. RHSM is compatible with ZENworks Patch Management. It provides a much more efficient method for Red Hat patch distribution. All Red Hat client subscriptions will be required to use RHSM by July 31, 2017.

To use RHSM, a new subscriber will have to first register with Red Hat or an existing subscriber will have to migrate from the Classic service to RHSM. The ZENworks procedures for both options are provided below:

- ◆ **New subscription.** To configure RHSM as a new subscriber:
 1. In the ZENworks Control Center, go to **Configuration > Security > Subscription Service Content Download**.
 2. Select **RHSM** under the **Red Hat Linux Subscription Management** configuration.
 3. Scroll to the bottom of the configuration page and click **Apply** to save the changes.
 4. Register the RHEL 5, 6, or 7 agent for RHSM:
 - a. On the Red Hat device, go to **Applications > System Tools**, and select **Red Hat Subscription Manager**.
 - b. Click **Register**, in the Subscription Manager, followed by **Next**.
 - c. In the System Registration page, click **Register**.
 - d. In the Subscription Attachment page, click **Attach**.
 5. Wait for the next DAU task to execute per the schedule, or click **Update Now** in the **Subscription Service Settings** page (**Configuration > Security > Patch Subscription Service Settings**).
- ◆ **RHSM migration.** To migrate to RHSM from the RHN Classic mode:
 1. In the ZENworks Control Center, go to **Configuration > Security > Subscription Service Content Download**.
 2. Select **RHSM** under the **Red Hat Linux Subscription Management** configuration.
 3. Scroll to the bottom of the configuration page and click **Apply** to save the changes.
 4. Log in to your Red Hat account at <https://access.redhat.com/articles/1161543>, and follow the instructions to migrate to RHSM.
 5. Wait for the next DAU task to execute per the schedule, or click **Update Now** in the **Subscription Service Settings** page (**Configuration > Patch Management > Subscription Service Settings**).

Configuring Email Notification

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

To configure Email Notification:

- 1 Select **Configuration** in the ZENworks navigation menu, and go to **Configuration > Security > Email Notification**.
- 2 Type the desired email addresses in the **From**, **To**, and **CC** fields.
- 3 Click **OK** to save changes and return to the **Configuration** page.

Configuring Patch Dashboard and Trending

The Patch Compliance Criteria in the Security Dashboard page enables you to define the compliance percentage for Critical and Recommended patch impacts. In order for a device to register as compliant for each impact type, the device must be patched to that percentage, respectively.

The criteria that you define here is displayed in the Device Patch Compliance dashlet in the Dashboard. To view the dashlet, go to Security > Patch Dashboard.

The Device Malware Status Threshold enables you to specify after how many days of receiving the last malware status from the device can ZENworks display the device malware status as Unknown in the Device Malware Status dashlet. To view the dashlet, go to Security > Security Dashboard.

For information about the Patch Management Dashboard, see [Employing the Security and Patch Dashboard](#).

Configuring the Schedule for Vulnerability Detections

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

To configure the Vulnerability Detection Schedule, select **Configuration** in the ZENworks navigation menu, and go to **Configuration > Security > Vulnerability Detection Schedule**.

NOTE: If you want to make changes to the schedule of a DAU Bundle, you should configure it within the Vulnerability Detection Schedule page. If the DAU bundle schedule is modified within any other page of ZCC, such as the Device's Assignments or the Bundle's Relationship page, under Assignment Details, it will be overridden during the next subscription update by the value configured in the Vulnerability Detection Schedule page.

Refer to the descriptions below to understand which configuration options to choose for running Vulnerability Detection:

Item	Description
Distribute vulnerability definition before scan	Lets you deploy bundle content immediately.
Distribute vulnerability definition content on a schedule	Lets you specify a schedule when Vulnerability Detection bundles will be distributed to devices.
Check for vulnerabilities on device refresh	Lets you initiate Vulnerability Detection action when the Agents on the managed devices are refreshed.
Check for vulnerabilities on a schedule	Lets you specify a schedule when the Vulnerability Detection will run.

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

- ◆ **Date Specific:** Select **Date Specific** to schedule the deployment to your selected devices according to the selected date.

Set the following options in the Date Specific page:

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

- ◆ **Start immediately at Start Time:** Deactivates the **End Time** panel and starts the action at the start time specified. In this option, you must set the start time in the **Start Time** panel:

Start Time: :

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

End Time: :

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

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

- ◆ **Recurring:** Select **Recurring** to start the deployment on the selected day at a selected time, repeat the deployment every day/week/month, and if defined, end on a specific date.

Set the following options in the Recurring page:

- ◆ **When a Device is Refreshed:** This option enables you to schedule a recurring deployment whenever the device is refreshed. In this option, you can choose to delay the next deployment until after a specific time.

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

Delay execution after refresh: Days Hours Minutes

NOTE: The device is refreshed based on the settings in **Configuration > Device Management** menu > **Device Refresh and Removal Schedule** (Manual Refresh or Timed Refresh). Alternatively, you can refresh the device by selecting a device in the **Devices** page and clicking the **Refresh Device** option in the **Quick Tasks** menu.

- ◆ **Days of the Week:** This option enables you to schedule the deployment on selected days of the week.

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

If you click the **More Options** link, additional deployment options appear:

- ◆ Selecting the **Use Coordinated Universal Time** check box enables you to schedule the deployment of all devices at the same time, regardless of time zone differences. Coordinated Universal Time (UTC), also known as World Time, Z Time, or Zulu Time, is a standardized measurement of time that is not dependent upon the local time zone. Deselecting UTC schedules the distribution at local time.
- ◆ Selecting the **Start at a random time between Start Time and End Times** check box activates the **End Time** panel in addition to the **Start Time** panel. You can specify the end time and the start time so that the deployment occurs at any random time between the start and end times.
- ◆ The **Restrict schedule execution to the following date range** option enables you to schedule a recurring deployment at the selected time, repeat the deployment on the days specified, and, if defined, end at the specific time. This option also enables you to restrict the deployment to the period between the start date and the end date. To set this option, select the **Restrict schedule execution to the following date range** check box, and click the **Calendar** icon to open the calendar and pick a start date or end date.
- ◆ **Monthly:** This option enables you to specify the monthly deployment options.

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

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


To select an additional day of the month, click the **Plus** icon and use the drop-down arrows in the second row. To remove a particular day from the list, click the **Minus** icon.

If you click the **More Options** link, additional deployment options appear.

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

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

⊙ **Fixed Interval**

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

[Hide Options](#)

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

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

If you click the **More Options** link, additional deployment options appear.

Setting Vulnerability Detection at the Folder Level

The Vulnerability Detection schedule can also be set at the folder level which enables you to set the deployment options for Vulnerability Detection for the Server or Workstation estate. By configuring Patch Management settings at the folder level you will override the System settings (configured in the Configuration page), however, you can return to the System settings at any time by using the Revert option.

To configure the Vulnerability Detection Schedule at the folder level:

- 1 Click **Devices** in the ZENworks navigation menu.
- 2 Click the **Details** link on the folder you would like to configure settings for.
- 3 Go to **Settings > Security > Vulnerability Detection Schedule**.
- 4 At the top of the page there is an option to **Override the System** settings, select this to begin making changes.

NOTE: This option can be used to revert back to System settings if you need to change back.

- 5 Select your desired schedule for the Vulnerability Detection, as described in [Configuring the Schedule for Vulnerability Detections](#).

Initiating a Patch Scan

Use this quick task to update the primary server with required patches for one or more selected devices without waiting for a scheduled scan so that patches can be identified for caching and installation. The actions and results for the different Patch Scan options are explained in more detail below:

Scan using updated patch scan signature (DAU) file

This default option retrieves the latest information from the patch repository to scan selected devices. If there are patches available in the patch repository that the selected devices require and do not have, the scan will upload that information to the server.

Scan using device's current patch scan signature (DAU) file

This option scans the selected devices using the patch signature file currently available on each device and uploads the results of required patches to the server. The uploaded results might not be the latest from the patch repository for applicable devices.

No scan; retrieve existing scan results only

This option uploads or refreshes the results of the last patch scan that occurred for each selected device. The uploaded results might not include all patches from the current patch signature file on each device and/or the latest patch signatures from the patch repository.

Configuring Patch Policy Settings

Patch Policy Settings are used to define enforcement times and reboot behaviors for each patch policy.

NOTE: If you want to make changes to the schedule of a Patch Policy, you should configure it within the Patch Policy Settings page. If the schedule is configured within any other page of ZCC, such as Device's Assignments or the Bundle's Relationship page, under Assignment Details, it will not override the schedule that was previously defined in the Patch Policy Settings page. Instead, it will be run multiple times, based on the schedule configured within each page.

- ◆ **Schedule Enforcement:** When configuring **Schedule Enforcement**, you can leave the default setting to manually apply patches on the agent device using the “zac pap” command in the Command Line Utility (zac), or you can define a schedule when patches will automatically be applied.
- ◆ **Patch Policy Reboot Behavior:** When configuring **Patch Policy Reboot Behavior**, you can leave the system defaults in place (no reboots or prompts), or you can define how users are prompted and interact with device reboots when patches are applied.

Schedule Enforcement

You can schedule dates and times that your Patch Policies are pushed out. This feature is useful for distributing and enforcing Patch Policies during off hours, thus decreasing network traffic and strain. The idea is that a policy can be scheduled to be released at different times or outside of working hours. Using this configuration will affect all policies that are set up and will set the schedule for the deployment.

NOTE: Before you can schedule Patch Policy enforcement, a patch policy must be created. Click **Security** in the navigation menu, and select the **Patch Policies** page. Make sure a patch policy exists. If you have to create a new one, make sure the system has time to download the patches.

- ◆ **Default (Manually apply patches on the agent using “zac pap”):** This configuration is the system default and requires manually implementing patch policies using the zac Command Line Utility.
- ◆ **Schedule patch policy application time:** This configuration enables setting a schedule to automatically apply patches, which includes the option to limit the duration time of patch installation based on a specific date or a recurring schedule.
 - ◆ **Restrict Duration:** If you check the **Restrict Duration** check box, you can limit how long patches are applied by entering a time increment based on the number of hours, minutes, or a combination of both.
 - ◆ **Date Specific:** If you choose the **Date Specific** schedule type, you can schedule patch deployment using the following criteria:
 - ◆ **Start Date(s):** Enables you to pick the date when you need to start the deployment.
 - ◆ **Run event every year:** Ensures that the deployment starts on a selected date at selected time and repeats every year. If defined, ends on a specific date.

- ♦ **Process immediately if device unable to execute on schedule:** Ensures that the deployment starts immediately if the device was unable to execute on the selected schedule.
- ♦ **Select When Schedule Execution Should Start:** There are two options to enable you to select the start time of the schedule execution namely:
 - ♦ **Start Immediately at Start Time:** Deactivates the **End Time** panel and starts the deployment at the start time specified. In this option, you must set the start time in the **Start Time** panel.
 - ♦ **Start at a random time between Start Time and End Times:** Activates the **End Time** panel next to the **Start Time** panel. You can specify the end time and the start time so that the deployment occurs at any random time between them.

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

- ♦ **Recurring:** If you choose the **Recurring** schedule type, you can schedule patch deployment using the following criteria:

- ♦ **When a device is refreshed:** Enables you to schedule a recurring deployment whenever the device is refreshed. In this option, you can choose to delay the next deployment until after a specific time.

To set the delay, select the **Delay execution after refresh** check box, and specify the days, hours, and minutes of the time by which you require delaying the deployment.

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

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

NOTE: The device is refreshed based on the settings in **Configuration > Device Management** menu > **Device Refresh and Removal Schedule** (Manual Refresh or Timed Refresh). Alternatively, you can refresh the device by selecting a device in the **Devices** page and clicking the **Refresh Device** option in the **Quick Tasks** menu.

- ♦ **Days of the week:** Enables you to schedule the deployment on selected days of the week. To set the day of deployment, select **Days of the week**, select the day of the week, and set the start time for the deployment.
- ♦ **Monthly:** You can schedule the deployment on a specific day of the month, the last day of the month, or a specific day every week or month.
- ♦ **Fixed Interval:** Enables you to schedule a recurring deployment that runs on a regular basis. You can choose the number of months, weeks, days, hours, and minutes of the interval and the start date for the deployment schedule.

Patch Policy Reboot Behavior

Some patches require their host to be rebooted after installation. You can leave the default of no reboots or prompts and handle these actions another way, or you can choose to notify users when a reboot is required and also give them some flexibility for when the reboot takes place.

Refer to the reboot options described below to better understand how to configure them:

- ♦ **Default Disabled (no reboots or prompts):** The default option is typically used when zone administrators have other processes in place that handle reboots on a routine basis.
- ♦ **Enabled:** Select this option to allow reboots when patching and to enable the Notify Users check box.
- ♦ **Notify Users:** Select the check box to enable reboot notification and its configuration options.
 - ♦ **Description text:** Edit the text of the notification prompt when Notify Users is selected.
 - ♦ **Options:** Define how the user is notified of and interacts with the reboot. There are three options:
 - ♦ **Suppress reboot:** Select **Yes** to prevent the reboot.

NOTE: Selecting **Yes** also prevents the notification prompt. However, the following system variable can be used to enable the prompt while still repressing the reboot:

PATCH_ALWAYS_SHOW_REBOOT_PROMPT

For more information about this variable and setting system variables in general, see [Patch Management System Variables](#).

- ♦ **Allow User to cancel:** Select **Yes** to enable a cancel option in the reboot notification prompt.
- ♦ **Allow User to snooze:** Select **Yes** to enable a snooze option in the patch policy reboot notification prompt, which delays the reboot.
 - ♦ **Snooze interval:** The duration the reboot is delayed when the user clicks Snooze.
 - ♦ **Reboot within:** The deadline when the user can no longer delay the reboot.
 - ♦ **Show tray notification:** If you select this option, a notification for a pending reboot is displayed in the system tray. Notification options include the following:
 - ♦ **Tray notification duration:** Enter a value in hours, minutes or seconds for how long the system tray notification is displayed before being hidden.
 - ♦ **Tray notification text:** Edit the text you want to appear in the notification prompt.

IMPORTANT: If you delete an old patch policy from an end point and then publish a new policy to replace it, the end point may list a Device-Assigned Bundle Status of Not Installed for an indefinite period of time. If you encounter this end point status, reboot the end point to complete publication of the patch policy.

Configure Patch Policy Settings at the Folder Level

Patch Policy Settings can also be set at the folder level which enables you to set patch enforcement and reboot behavior for the Server or Workstation estate. By configuring Patch Management settings at the folder level you will override the System settings (configured in the Configuration page), however, you can return to the System settings at any time by using the Revert option.

To configure the Patch Policy Settings at the folder level:

- 1 Click **Devices** in the ZENworks navigation menu.
- 2 Click the **Details** link on the folder you would like to configure settings for.
- 3 Go to **Settings > Security > Patch Policy Settings**.
- 4 At the top of the page there is an option to **Override** the system settings, select this to begin making changes.

NOTE: This option can be used to revert back to System settings if you need to change back.

- 5 Configure [Schedule Enforcement](#) and [Patch Policy Reboot Behavior](#) sections for the folder.

Configuring Patch Policy Pre-Install Behavior

In Patch Policy Pre-Install Behavior you define when patches are distributed to the agents and how end users are notified of the patch installations.

- ♦ **Schedule Distribution:** When configuring [Schedule Distribution](#), you can leave the default setting, which distributes patches according to the configuration in Patch Policy Settings, or you can define a schedule for patch distribution.
- ♦ **Pre-Install Notification Options:** When configuring [Pre-Install Notification Options](#), you can leave the system defaults in place, or you can override the system settings and define how end point users are prompted and interact with patch installations.

Schedule Distribution

The Schedule Distribution page allows you to define whether users receive notification when patches are downloaded and installed, and to customize the installation settings.

- ♦ **Default (Distribution and enforcement will apply on enforcement schedule):** Use this option to stay with the [Schedule Enforcement](#) settings defined in [Patch Policy Settings](#).
- ♦ **On Device Shutdown:** Use this option to deploy patches on device during shutdown or reboot.
- ♦ **Schedule patch policy application time:** Select this option to override the default options and choose new ones. This option enables setting a schedule that can limit the duration time of patch installation based on a specific date or a recurring schedule.
 - ♦ **Restrict Duration:** If you check the [Restrict Duration](#) check box, you can limit how long patches are applied by entering a time increment based on the number of hours, minutes, or a combination of both.
 - ♦ **Date Specific:** If you choose the [Date Specific](#) schedule type, you can schedule patch deployment using the following criteria:
 - ♦ **Start Date(s):** Enables you to pick the date when you need to start the deployment.

- ◆ **Run event every year:** Ensures that the deployment starts on a selected date at selected time and repeats every year. If defined, ends on a specific date.
- ◆ **Process immediately if device unable to execute on schedule:** Ensures that the deployment starts immediately if the device was unable to execute on the selected schedule.
- ◆ **Select When Schedule Execution Should Start:** There are two options to enable you to select the start time of the schedule execution, namely:
 - ◆ **Start Immediately at Start Time:** Deactivates the **End Time** panel and starts the deployment at the start time specified. In this option, you must set the start time in the **Start Time** panel.
 - ◆ **Start at a random time between Start Time and End Times:** Activates the **End Time** panel next to the **Start Time** panel. You can specify the end time and the start time so that the deployment occurs at any random time between them.

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

- ◆ **Recurring:** If you choose the **Recurring** schedule type, you can schedule patch deployment using the following criteria:

- ◆ **When a device is refreshed:** Enables you to schedule a recurring deployment whenever the device is refreshed. In this option, you can choose to delay the next deployment until after a specific time.

To set the delay, select the **Delay execution after refresh** check box, and specify the days, hours, and minutes of the time by which you require delaying the deployment.

By default, the patch bundle install frequency is set to **Install once per device**. For a recurring deployment, change it to **Install always**, after completing the patch policy. For more information, see “[Install Action Set Options](#)” in the *ZENworks Software Distribution Reference*.

NOTE: The device is refreshed based on the settings in **Configuration > Device Management** menu > **Device Refresh and Removal Schedule** (*Manual Refresh* or *Timed Refresh*). Alternatively, you can refresh the device by selecting a device in the **Devices** page and clicking the **Refresh Device** option in the **Quick Tasks** menu.

- ◆ **Days of the week:** Enables you to schedule the deployment on selected days of the week. To set the day of deployment, select **Days of the week**, select the day of the week, and set the start time for the deployment.
- ◆ **Monthly:** You can schedule the deployment on a specific day of the month, the last day of the month, or a specific day every week or month.
- ◆ **Fixed Interval:** Enables you to schedule a recurring deployment that runs on a regular basis. You can choose the number of months, weeks, days, hours, and minutes of the interval and the start date for the deployment schedule.

To save any changes made in **Patch Policy Pre-Install Behavior** options, click **Apply**.

Pre-Install Notification Options

The Pre Install Notification Options page allows you to define whether users receive notification when patches are downloaded and installed, and to customize the installation settings.

- ◆ **Use values assigned to system variables or defaults:** Select this option to use the default pre-install notification options defined within the Pre-Install Notification settings.
 - ◆ **Override Settings:** Select this option to override the default options and choose new ones. Selecting this option makes the remaining options available.
 - ◆ **Notify Users of Patch Install:** Select this option to notify the user prior to the installation of the patch.
 - ◆ **Description text:** The text of the notification message. You can edit this field only if you override the default settings.
 - ◆ **Options:** When you define installation options, you can specify whether to use the values in the default settings (the **Use values assigned to system variables or defaults** check box) or the custom settings. There are three options:
 - ◆ **Allow User to cancel:** Allows the user to cancel the patch installation.
 - ◆ **Allow User to snooze:** Allows the user to delay the installation.
 - ◆ **Snooze interval:** The duration the install is delayed when the user snoozes.
 - ◆ **Install within:** The deadline that the user can no longer snooze the installation.
-
- NOTE:** Even if you snooze the installation, the popup window will continue to appear every few seconds until you proceed with or cancel the installation.
-
- ◆ **Show tray notification:** On selecting this option, a notification for a pending installation is displayed in the system tray. If you select this option, define the following:
 - ◆ **Tray notification duration:** Enter a value in hours, minutes or seconds for how long the system tray notification is displayed before being hidden.
 - ◆ **Tray notification text:** Type the text you want to appear in the notification.

To save any changes made in **Patch Policy Pre-Install Behavior** options, click **Apply**.

Configure Patch Policy Pre-Install Behavior at the Folder Level

Patch Policy Pre-Install Behavior can also be set at the folder level, which enables you schedule patch distribution and set pre-install notification options for the Server or Workstation estate. By configuring Patch Management settings at the folder lever you will override the System settings (configured in the Configuration page), however, you can return to the System settings at any time by using the Revert option.

To configure the Patch Policy Pre-Install Behavior at the folder level:

- 1 Click **Devices** in the ZENworks navigation menu.
- 2 Click the **Details** link on the folder you would like to configure settings for.
- 3 Go to **Settings > Security > Patch Policy Pre-Install Behavior**.
- 4 At the top of the page there is an option to **Override** the system settings, select this to begin making changes.

NOTE: This option can be used to revert back to System settings if you need to change back.

- 5 Configure [Schedule Distribution](#) and [Pre-Install Notification Options](#) sections for the folder.

4 Assess Vulnerabilities

After configuring vulnerability detection, licensing, and other settings, you can assess device vulnerabilities via the Security pages, Device patches, and the ZENworks Reporting console. You can also take steps to manage patch compliance from the Dashboard, Patch Policies, and Patches pages.

Security Pages

The Security pages are where the majority of patch-related activities are performed, to include monitoring all patches across all systems registered to the ZENworks Server. From here you can assess patch compliance, view recently released patches, check patch subscription status, check the last time each device was scanned for patch compliance, search for patches, create custom patches, create and manage patch policies, and more.

Employing the Security and Patch Dashboard

The Patch Dashboard has four default dashlets that provide a comprehensive snapshot of key indicators, so you can quickly assess the overall health and compliance of patches on devices in your zone. You can also initiate action directly from respective dashlets, when expanded, to remediate, download, or disable selected patches, to discover patches, to reconfigure the zone vulnerability detection schedule, and to view patch and device details.

The Security Dashboard has four dashlets that enable you to quickly assess the vulnerability status of your zone. Using these dashlets you can track patches and CVEs, identify the top CVEs in the zone and the CVE severity distribution details. Using these dashlets you can deploy remediations, and perform patch scans.

Custom dashlets: You can create custom dashlets from any of the default dashlets or from other custom dashlets using the **Save As** feature. This will save the filter settings on a custom dashlet until you change and save different settings. Unlike the filters on the default dashlets, the filters you set on custom dashlets are persisted beyond the current Dashboard page session.

System settings: Dashlets that can be filtered by Platform reflect patches from the platform types selected in the Subscription Service Content Download configuration. For example, if the Linux platform is the only platform type selected for “platforms to download,” then typically only patches from that platform will be shown or can be filtered in the dashlet.

One exception to the above statement is custom dashlets. Any applicable patches already downloaded before a change was made in the “platforms to download” would still be shown in applicable ‘custom’ dashlets if the excluded platform type was previously saved to show in the dashlet.

Patch dashlet descriptions: A brief description for each default dashlet is provided below. Click a dashlet link for more detailed information about that dashlet.

- ◆ **Patch Subscription Status:** Displays the number of known patches in the zone, their status, and the last start and end times of subscription activities for licenses, patch discovery, and patch download. Mouse over different sections of the chart to see end times for Patch Download, License Verification, and Patch Discovery, or expand the dashlet for more options.
- ◆ **Recently Released Patches:** Displays the number of recently released patches by patch impact type. Mouse over different sections of the chart to see the number of patches for each impact type, or expand the dashlet for more options.
- ◆ **Device Patch Compliance:** Displays compliance status for devices in the zone. Mouse over different sections of the chart to see how many devices are compliant, or expand the dashlet for more options.

NOTE: Patch compliance is measured by Critical and Recommended patch impacts, based on the percentage defined in the Dashboard and Trending configuration. Disabled patches for these impact types are not part of the compliance data.

- ◆ **Device Last Patch Scan:** Displays the number of devices scanned for patches by time range. Mouse over the chart to see the scan information, or expand the dashlet for more options.

Security dashlet descriptions: A brief description for each default dashlet is provided below. Click a dashlet link for more detailed information about that dashlet.

- ◆ **Patch Tracker Dashlet:** This dashlet is a unique dashlet when compared to other dashlets in ZENworks as it does not display any data by default. To view the data, the dashlet should first be configured. When you mouse over the dashlet, it displays the number of vulnerable devices against the total number of impacted devices for the selected patches. In the Vulnerability Trend section of the dashlet, you can view the vulnerability trend of the selected patches, for a specific time period.
- ◆ **CVE Severity Distribution:** Displays all the CVEs that are applicable to devices in the zone, grouped based on their severity. When you mouse over the dashlet you get to see the number of CVEs for each type of severity.
- ◆ **Top CVEs :** Displays the list of top CVEs in the zone based on the date on which they were released. However, you can use the filters to display the top CVEs based on the number of vulnerable devices or based on the severity. Mouse over different sections of the chart to see the number of vulnerable devices against the total number of impacted devices, for a particular CVE.
- ◆ **CVE Tracker:** The CVE Tracker dashlet also does not display any data by default. To view data, the dashlet should first be configured. When you mouse over this dashlet, it displays the number of vulnerable devices against the total number of applicable devices. In the Vulnerability Trend section of the dashlet, you can view the vulnerability trend of the selected CVEs, for a specific time period.

For general information about using the ZENworks Dashboard, see [Using the ZENworks Dashboard - An Overview](#).

Patch Subscription Status

All patching through ZENworks Patch Management begins with retrieving applicable patches into your system via the patch subscription service. The subscription service performs three tasks: it verifies that your license is valid, it discovers new patches that are applicable to devices in your system, and it downloads the patch content as it is needed.

Viewing the Subscription Status is your first indication that your patch process is running smoothly. Use this dashlet to quickly determine the status and end times of these three processes: License Verification, Patch Discovery, and Patch Download. If any of the processes have failed, you have your first indication of where to troubleshoot:

- ♦ *License Verification:* Check the Patch Management License page to verify that your license has not expired.
- ♦ *Patch Discovery:* Click the **Discover Patches** link in the Subscription Status dashlet to scan for new patches in the patch content repository. If new patches are detected, the patch signatures will be downloaded to your devices, so they can be detected in the next DAU scan.
- ♦ *Patch Download:* Check your network environment to ensure patch content is not restricted due to closed ports or other firewall issues. For more information, see [Patch Management Issues](#).

Recently Released Patches

By default, the Recently Released Patches dashlet displays all applicable patches discovered on devices in your Management Zone that were released in the last 30 days. Viewing the information in the default configuration might initially help you determine how to best configure the dashlet for your organization's needs by asking questions such as:

- ♦ What platform types do I need to patch?
- ♦ What patch impact types do I want to include?
- ♦ Do I want to see applicable patches from all vendors or just selected vendors in my dashboard?

From the expanded Recently Released Patches dashlet, you can configure the dashlet to only display those patches that you require to accurately assess your patch environment going forward. You can also create custom dashlets by saving the Recently Released Patches dashlet with another name.

Modify the data display: To filter the data that the dashlet displays, expand and modify any of the sections in the dashlet filter panel for Release Period, Platform, Impact, and Vendors, and then apply your changes.

Execute actions from the Patches panel: The Patches panel displays the patches that meet the criteria you define in the dashlet filter panel. You can also filter the list by searching for any portion of a patch name string via the [Search Patches](#) feature.

For information about other actions and options you have in the Patches panel, see the following:

- ♦ **Remediate patches:** If you see a patch that you need that will not be picked up by your patch policy, you can start remediation of the patch directly from the Patches panel. To start remediating patches, select one or more patches in the list, and click **Remediate**.

Step 1 in the remediation process opens. For information about using the Remediation wizard, see [Deploying Patches Manually](#).

- ♦ **Disable patches:** To disable one or more patches, select them in the Patches panel and click **Disable**.

NOTE: There is no confirmation of this action. Once you click **Disable**, the action is executed.

To enable a disabled patch, go to the **Security > Patches** page, locate and select the patch, and click **Enable** from the Action menu.

- ♦ **Download patches:** To download one or more patches, select them in the Patches panel, and click **Download**. A green status icon indicates that the patch or patches are downloaded.
- ♦ **View patch information:** To view vendor details about a patch, click the patch name in the Patches panel. The Patch information page provides useful details about the patch and a link to the vendor site.
- ♦ **View patched or not patched devices:** To see which devices are applicable to which patches, click the applicable number link in the Patched or Not Patched column. This will list the devices that already have or need that patch, respectively. The list of devices will also include a link to the Summary page for each device in the list.
- ♦ **Sort the Patches list:** To sort the list alphanumerically by column criteria, click a column header. Clicking the column a second time will invert the order of the sort.

Device Patch Compliance

When expanded, the Device Patch Compliance dashlet provides a quick snapshot of how many devices are compliant and how many are not, both by the number of devices in the chart and by percentages in the Devices panel. You can modify the threshold that you want for patch compliance in the Dashboard and Trending configuration. For more information on this setting, see [Configuring Patch Dashboard and Trending](#).

Modify the data display: To filter the data that the dashlet displays, expand and modify any of the sections in the dashlet filter panel for Status, Impact, Device Type, and Platform, and then apply your changes.

Viewing options in the Devices panel: The Devices panel displays compliance status for each device in your zone by percentage, based on the criteria you define in the dashlet filter panel and compliance criteria in the Dashboard and Trending Configuration. You can also filter the list by searching for any portion of a device name via the **Search Devices** feature.

To see specifically which patches are compliant for each device, click a percentage link in either the Critical Patches or Recommended Patches column for a device in the list, and the Patches page will open for that device.

Device Last Patch Scan

Checking the data in the Device Patch Last Scan dashlet can help you determine the health of your current patch environment. When expanded, you can compare the latest scan with information from other patch dashlets and even go directly to the Vulnerability Detection Schedule to modify scan times, if there is a need.

Modify the data display: To filter the data that the dashlet displays, expand and modify any of the sections in the dashlet filter panel for Time Ranges, Platform, and Device Type, and then apply your changes.

Viewing options in the Devices panel: The Devices panel displays the last scan date and the next scheduled scan time for each device. You can also filter the list by searching for any portion of a device name via the [Search Devices](#) feature.

For information about other actions and options you have in the Devices panel, see the following:

- ♦ **View detailed device information:** To see specific information about a device in the Devices panel, click the device name. This will open the Summary page for that device.
- ♦ **Modify the scan schedule:** To go directly to the Vulnerability and Detection Schedule in the Patch Management configuration, click the link in the **Scan Schedule Defined At** column for any of the devices in the Devices panel. From here, you can modify the zone schedule that checks for device vulnerability.
- ♦ **Sort the Devices list:** To sort the list alphanumerically by column criteria, click a column header. Clicking the column a second time will invert the order of the sort.

Patch Tracker Dashlet

The Patch Tracker dashlet enables you to track a single or multiple patches available in the Management Zone. By drilling into the dashlet, you view the current patching status of the devices and also view the patching trend over a defined date range.

You can customize the dashlet to best fit your needs, and create multiple custom dashlets if necessary.

By default, the Patch Tracker dashlet does not display any information, to view information in the Patch Tracker, you need to first configure the dashlet. By configuring the Patch Tracker dashlet, you can track a single patch or multiple, associated, patches.

For the specified patches you can view the current patching status of the devices. The dashlet displays the number of devices that are patched against the total number of applicable devices. After identifying the vulnerable devices, you can use the Deploy Remediation quick task to apply the patches on the devices. With the Patch Tracker dashlet you can view the updated status as devices are patched. In the Unpatched Device Trend section of the dashlet, you can view the patching trend of the selected patches, for a specific time period.

Accessing the Dashlet: In ZCC, click [Security](#) > [Patch Tracker](#).

Configuring the Patch Tracker Dashlet

1. In the Patch Tracker Dashlet, click Configuration, and then click **Add/Remove**.
2. In Select Patches, select the required patches, and then click **OK**.
3. Specify a name for the dashlet and change the tracker icon, if required.
4. Vertica is required to retrieve the trending data. Hence, the Trend Chart fields are enabled only when Vertica is configured

In the Trend Chart section, based on your requirements, using the following option, you can assess the patch trending status in your Management Zone:

- a. **Date Grouping:** You can group the trend data based on Day, Week, Month, Quarter or Year. The chart will not be display any data until the end of the first period of the date grouping.

Example: If you choose Year, then you will not see any Trend Chart data for a year. Hence, while creating a new tracker, ensure that you set the Date Grouping to Day so that you see the data immediately. You can modify the filter at a later time, if you want.

- b. **Date Range:** After selecting the Date Grouping filter, this option enables you to select the date range for the selected date grouping.

NOTE: Vertica is required to retrieve the trending data. The Trend Chart fields will be enabled only when Vertica is configured. For more information, see [Vertica Database Reference](#).




5. Click Apply.
6. To save the dashlet, click the hamburger menu, and then select Save As.

After configuring the Patch Tracker dashlet, following information is displayed:

Patch Status: The Patch Status section provides current known status about the number of patched and unpatched devices that are grouped by platforms. Hover over each of the graph elements to know the number of patched and unpatched devices.

The number displayed in the Patch Status section represents the number of unpatched devices in the zone. The Patch Status graph is grouped based on platforms. This also displays the number of devices that are not patched in the Management Zone.

The Patch Status also displays an arrow that indicates the current unpatched device trend in the Management Zone. The following table describes the various scenarios and the associated status arrow:

- ◆  The green arrow pointing downwards represents the number of unpatched devices at the current point in time is less than the number of devices at the start of the date grouping period (Day, Week, Month, Quarter, or Year).
- ◆  The red arrow pointing upwards represents the number of unpatched devices at the current point in time is more than the number of devices at the start of the date grouping period (Day, Week, Month, Quarter, or Year).
- ◆  The two-sided arrow represents the number of unpatched devices at the current point in time is same as the number of devices at the start of the date grouping period (Day, Week, Month, Quarter, or Year).

Unpatched Device Trend: The trend chart displays the current and historical data of selected patches based on the selected date grouping and date range. By analyzing this section, you can check the patch trend in your zone and also take necessary actions, such as Deploy Remediation, to make your zone more secure. The trend data is displayed based on the server time.

NOTE: If a new device is added to the zone, then the trend data for the newly added device will be displayed only after the data is retrieved from Vertica. By default, the data from Vertica will be retrieved after 12 PM (Server Time).

For example, if the Date Grouping is Day and the Date Range is 1 Month, then the Unpatched Device Trend chart displays the trend for the last 30 days with each day represented as a point in the chart.

NOTE: The Unpatched Device Trend chart is displayed only when Vertica is configured and enabled. For more information, see the Vertica Database Reference in the [documentation site](#).

Filtering the Dashlet Based on requirements, you can narrow-down the data displayed in the dashlet by using the Filter tab. Following are the available filter options:

- ♦ **Device Folders:** In this filter, you can select the required device folders. Select **Include Subfolders** to include folders within the selected folders.
- ♦ **Device Groups:** In this filter, you can select the required device groups.
- ♦ **Device Type:** In this filter, you can select the required type of device. The available options are Servers, Workstations and Mobile Devices.
- ♦ **Platform:** In this filter, you can select the required platform. The available options are Windows, Linux and Mac.
- ♦ **Vulnerability Status:** In this filter, you can select the vulnerability status of the device. The available options are Vulnerable or Not Vulnerable.

Execute actions from the Device Details panel

The Device Details panel displays the devices that meet the criteria that you defined in the dashlet filter panel. You can also filter the list by searching for a device name or a portion of the name in the search panel.

Following are the information displayed in the Device Details panel:

Field	Description
Device	Displays name of the device.
Status	Displays the vulnerability status of the device.
Last Vulnerability Scan	Displays the date and time at which the Vulnerability Scan was performed on the device.
Operating System	Displays operating system on which the device is operating.
Device Folder	Displays the folder path in which the device is located.
Remaining Vulnerabilities	Displays the number of vulnerabilities that should be applied on the device to make the device less vulnerable.

For information about other actions and options you have in the Device Details panel, see the following table:

Table 4-1 Device Details Panel

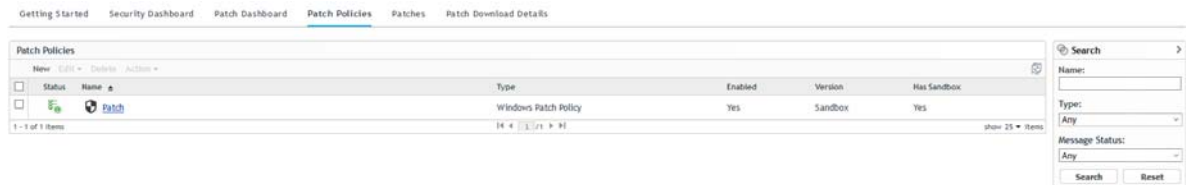
Task	Description
Deploy Remediation	Deploys all patches required to remediate the vulnerability on the selected devices. Any required patches that have not already been downloaded (cached) to your zone will be automatically downloaded. For more information, see Deploying Patches Manually .
Scan Now	This action initiates a patch scan on the selected devices in order to ensure that you have the latest vulnerability status for the devices.
Search	The Search operates on the Device, Operating System, and Device Folder fields to allow you to filter the list based on the data in those fields.

NOTE: For information about the other Security dashlets, see the [Determine Vulnerabilities and Deploy Remediations](#) section in the [CVE Reference](#).

Viewing Patch Policies

You view, create, modify, and delete patch policies from the Patch Policies page. For detailed information about creating and managing patch policies, see [Creating and Publishing Patch Policies](#).

To view patch policies, navigate to [Security > Patch Policies](#).

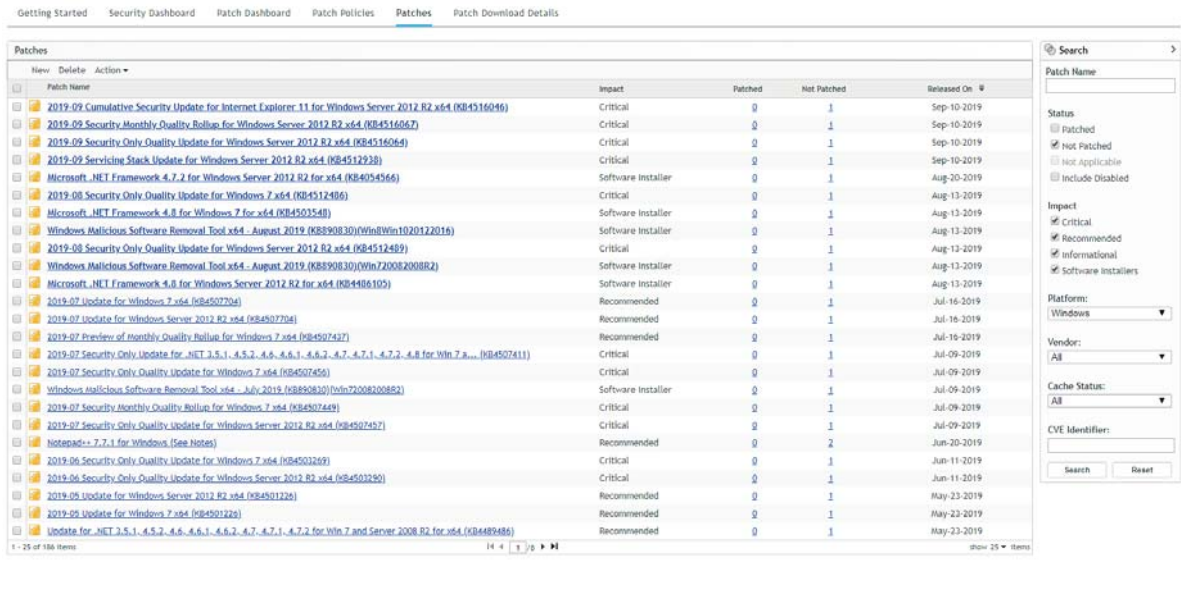


Viewing Zone Patches

To view the patches that are discovered in the zone from the DAU tasks, click [Security](#) in the navigation menu, and select the [Patches](#) page.

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

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



Viewing Patch Status

The [Patch Download Details](#) page displays the download status for patches and bundles in table form, and also displays the details of patch caching and queuing status.

To view the Status page, navigate to **Security > Patch Download Details**.

The page consists of two data tables, [Patch Download Details](#) and [Cache Status](#). Definitions for each table item are provided below:

Table 4-2 Status Item Definitions

Item Name	Item Status
Signature Download	Indicates whether downloading of the signature has finished or is in progress.
Signature Download Time	Indicates the last time the local server contacted and downloaded the signature from the Patch Subscription server.
Bundle Download	Indicates whether the patch bundle download is finished or is in progress.
Last Patch Download	Indicates the last time the local server contacted and downloaded a patch from the Patch Subscription server.

Item Name	Item Status
Number of Failed Download(s)	Indicates the number of patches that failed to download from the Patch Subscription server.
Number of Patches Queued for Caching	Indicates the number of patches that are queued for download from the Patch Subscription server.
Number of Active Patches	Indicates the number of patches that are available for download from the Patch Subscription server.
Number of New Patches (less than 30 days)	Indicates the number of patches that have been uploaded to the Patch Subscription server in the last 30 days and are available for download.
Latest Patch Released On	Indicates the time when the latest patches were released.

Table 4-3 Cache Status Item Definitions

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

NOTE

By default, the SendChildPatchBundleStatus flag is enabled, i.e. the agent will upload the child patch bundle status to the server even if the registry is not created. Uploading child patch status to the server causes additional overhead on the server to process the status of child patch bundles also overhead on the agent to upload the status of child patch bundles.

If you want SendChildPatchBundleStatus to be disabled, then set the following registry to false:

SOFTWARE\\Novell\\ZCM\\SendChildPatchBundleStatus

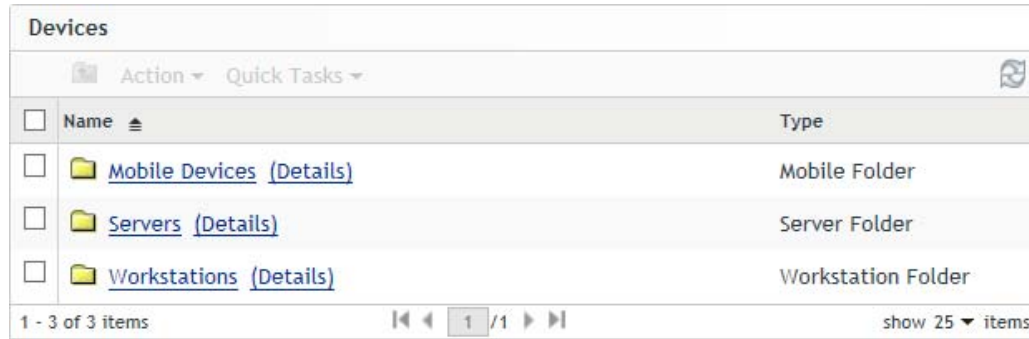
Viewing Patches for a Device

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

To view the patches for a specific server or workstation device:

- 1 Click **Devices** in the navigation menu.

A page displaying the root folders for each type of device appears:



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** or **Workstations** link.

A list of server or workstation groups classified on the basis of their operating systems appears.

Any of the following device icons might appear on the Servers or Workstations page:

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

A specific device, type of device, or device with a given status can also be found using the Search feature on a group page. The following filters are available:

Filter Item	Result
Name	Searches for devices with a particular name.
Type	Searches for devices of a specific type or group.
Operating System	Searches for devices running a particular operating system.
Test Status	Searches for devices based on its ZCM test status.
Message Status	Searches for devices that display a particular message status.
Compliance Status	Searches for devices based on their compliance status, Yes or No .
Device Status	Searches for devices based on the device status.
ERI Status	Searches for devices using disk encryption based on ERI status, Yes or No .

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

If you click a managed device, a page displaying details about the managed device or member is displayed, as shown in the following figure, where the name `az-tp-win2012r2` for the managed device is an example. The network administrator decides the name of the managed device.

Summary Inventory Relationships Settings Content Statistics Locations Audit Patches

General	
Alias:	az-tp-win2012r2
Host Name:	AZ-TP-WIN2012R2
IP Address:	10.000.006.00
Last Full Refresh:	3:52 AM
Last Contact:	7:52 AM
ZENworks Configuration Management Version:	17.0.0.0
ZENworks Asset Management Version:	17.0.0.1002
ZENworks Patch Management Version:	17.0.0.737
ZENworks EndPoint Security Management Version:	17.0.0.1002
ZENworks Full Disk Encryption Version:	17.0.0.1002
ZENworks Agent Version:	17.0.0.1007
ZENworks Updater Service Version:	17.0.0.1002
ZENworks Agent Status:	
Operating System:	Microsoft Windows Server 2012 R2 Standard Edition 6.3.9600 N/A Build 9600
Number of errors not acknowledged:	247
Number of warnings not acknowledged:	2
Primary User:	No user sources configured
Owner:	[Edit]
Serial Number	422ba3ba31d985769156ac
GUID:	0e5a51a5eb53bccf92dfc1e
Department:	[Edit]
Site:	[Edit]
Location:	[Edit]

Upcoming Events	
11/30/16	
Refresh	
Type Name	Time
Click refresh to see upcoming events	

Logged In Users	
Name	In Folder
No items available.	

Imaging Work	
Scheduled Work:	None
Applied Image Files:	None
Type Name	
No items available.	

Assigned System Updates	
Name	Status
No items available.	

- Click the **Patches** page (either from a group or device page) to display the patches associated with the group or device:

Summary Relationships Details Audit **Patches**

Patches

Action ▾	Patch Name	Impact ▲	Patched	Not Patched	Released On
<input type="checkbox"/>	MS16-092 Security Update for Windows Server 2012 R2 (KB3169704)	Critical	0	1	Jul-12-2016
<input type="checkbox"/>	MS16-048 Security Update for Windows Server 2012 R2 (KB3146723)	Critical	0	1	Apr-12-2016
<input type="checkbox"/>	MS16-062 Security Update for Windows Server 2012 R2 (KB3156017)	Critical	0	1	May-10-2016
<input type="checkbox"/>	MS16-075 Security Update for Windows Server 2012 R2 (KB3161561)	Critical	0	1	Jun-14-2016
<input type="checkbox"/>	Security Update for Windows Server 2012 R2 (KB3042058)	Critical	0	1	Oct-13-2015
<input type="checkbox"/>	MS16-142 November, 2016 Security Monthly Quality Rollup for Windows Server 2012 R2 (KB3197874)	Critical	0	1	Nov-08-2016
<input type="checkbox"/>	MS16-076 Security Update for Windows Server 2012 R2 (KB3162343)	Critical	0	1	Jun-14-2016
<input type="checkbox"/>	MS16-014 Security Update for Windows Server 2012 R2 (KB3126593)	Critical	0	1	Feb-09-2016
<input type="checkbox"/>	MS16-047 Security Update for Windows Server 2012 R2 (KB3149090)	Critical	0	1	Apr-12-2016
<input type="checkbox"/>	MS16-074 Security Update for Windows Server 2012 R2 (KB3164035)	Critical	0	1	Jun-14-2016

Search

Patch Name

Status

Patched

Not Patched

Not Applicable

Include Disabled

Impact

Critical

Recommended

Informational

Software Installers

Vendor

Cache Status

CVE Identifier

Accessing Patch Management Reports

Reports are available to customers who install ZENworks Reporting Services (ZRS) inside ZENworks. Login to the ZENworks Reporting console to view the reports. For information on how to deploy or upgrade the ZENworks Appliance, see the [ZENworks Reporting Appliance Deployment and Administration Reference](#).

The following predefined reports are included for Patch Management:

- ♦ **Bundle Deployment Summary:** Displays only the devices on which the patch bundle have been deployed. This report lists deployment name, patch name, assigned device name, and patch device status.
- ♦ **Critical Patch Status Report:** Displays information on critical patches that are assigned to the devices. This report displays the total summary of the patch status and lists patched, not patched, not applicable, error, and total devices.
- ♦ **DAU Status:** Displays a pie chart that shows how many days since the Discover Applicable Updates (DAU) task was run on agents in the management zone (those greater than 7 days and those from 1-3 days).
- ♦ **Device Patch Status by Vendor:** Displays information on device patch status. This report lists agent name, vendor, patched, not patched, not applicable, released on, is patch enabled, and patch impact.
- ♦ **Device Status:** Displays a date-time stamp by device name for the following status indicators: Last Contact Date, Last Full Refresh, Last Inventory Scan, and Last DAU.
- ♦ **Not-Patched Patches by Device:** Displays a table for each device in the management zone that shows patches by the patch name, release date, impact, and vendor.

- ◆ **Overall Patch Percentage:** Displays the total number of devices, Patched and Not Patched, with their respective percentages. The percentages are also reflected in a pie chart.
- ◆ **Patch Analysis:** Displays information on patch assigned as mandatory baseline on a device. This report lists vendor, patch name, released date, criticality, applicable, patched, not patched, and % patched.
- ◆ **Patch Assessment Report:** Displays information on all released patches and their impact. This report lists vendor, released patches, and patch impact.
- ◆ **Patch Bundle Deployment Status:** Displays information on all released patch bundles and their status. This report lists administrator initiated remediation bundle, deployed patch bundle, event type, and event status.
- ◆ **Patch Deployment Summary:** Displays information on all released patch bundles and their status. This report lists admin initiated remediation bundle, deployed patch bundle, event type, and event status.
- ◆ **Patch Detail Report:** Displays detailed information on patches. This report lists patch name, patched status, total devices, and % patched.
- ◆ **Patch Percentage by Folder:** Displays the number of devices patched and not patched in each folder with a percentage of those not patched.
- ◆ **Patch Release Report:** Displays information on released patches. This report lists, patch device status, and device name.
- ◆ **Patch Tuesday Report:** Displays information on Tuesday's released patches. This report lists, patch name, patch status, and total devices.
- ◆ **Top 10 Not Patched Critical Patches:** Displays information on the most critical patches that are not deployed. This report lists patch name and patch impact.

Generating Patch Audit Reports

While not recommended for long term use due to database usage, two audit reports, Device Patch Audit and Patch Audit Summary, will be generated for patch deployments when the **Save patch status history** option is turned on in the Dashboard and Trending configuration. For information on how to deploy or upgrade the ZENworks Appliance, see the [ZENworks Reporting Appliance Deployment and Administration Reference](#).

To configure the setting:

- 1 Go to **Configuration > Security > Dashboard and Trending** link.
- 2 In the Dashboard and Trending section, select the **Save patch status history (Warning: This can cause large database usage)** check box.
- 3 Choose the number of days to store the data in the database in the drop-down menu.
- 4 Click **Apply** at the bottom of the configuration page.

5 Distribute and Apply Patches

There are two ways to distribute and apply patches to devices in the management zone:

- ♦ [Create patch policies](#)
- or
- ♦ [Deploy patches manually](#)

The first option automatically deploys patches based on rules and requirements you define in patch policies. The second option requires you to manually select the patches to deploy and manually configure their distribution. Both options require automated DAU tasks to have a required patch list to draw from.

While using patch policies is the most efficient, preferred, and recommended way to manage patches, Deploy Remediation gives you the flexibility to quickly deploy patches, custom or otherwise, that may not be covered in your patch policies.

Creating and Publishing Patch Policies

Patch policies are designed to make deployment of multiple patches easier across large estates. They can be used as a testing ground for new patches before they are released onto the network, and can also be used to filter content, so that some devices can be selected or omitted as part of the patch remediation.

Patch Policy - Best Practices

In general use, the Patch Policy function is the most effective and labor saving way to deploy patches across large estates. Once set up, it can deliver the patches to the target machines with much less oversight than manual remediation.

While we advocate the automated setup that this function delivers, it is important to remember not to overstretch your systems or the capabilities of the product.

Recommendations:

1. Keep the policies reasonably simple. Try to organize individual patch policies around a common outcome, for example: assuming some of your stock is comprised of Windows 7 machines; setup a policy called Win7 and use this to deliver all Microsoft updates to those targets. Similarly, you could organize policies by vendor or architecture.
2. Devise a naming convention for your policies; this will enable you to track policies more easily, and will also make it simpler to make changes to individual policies.
3. When you are setting up individual policies, try to plan into the policy. For example: in real terms, how often will a policy be deployed? does that specific vendor have regular updates? and what would your expectation be for throughput? It is our general recommendation that you should have a team process to steer your approach to this. This is in line with [NIST](#) recommendations.

4. When you are designing policies, be careful not to apply conflicting statements. There are a lot of different settings built in to ensure that policies can perform some very useful tasks, but be aware that changing Rules, Requirements, Actions, Relationships, and Members may bring your policy into conflict with previously defined settings.
5. Choose a schedule type based on network load, for example: it might be advisable to schedule policy deployments out of hours or at times when you know that your network will be least busy.
6. Use the Patch Policy Enforcement and Distribution settings in ZENworks > Configuration to their full extent, especially around Reboot settings; why reboot if the patch does not require this?
7. Use the Sandbox function to its full extent. We cannot stress how important it is to test patches before deploying them, especially over big networks. It is therefore prudent to set up a test server or a proving ground and deploy to this in the first instance. Once there has been a clean and issue free deployment, then you are ready to release to the wider network.

For more information, see [Test a Policy Before Deploying to a Live Environment](#).

8. Do not overload the policy. Patch Management has a default limit of no more than 1500 bundle actions per policy. This is to keep policies within a manageable parameter. If you believe your patch server has performance issues due to the number of patch bundle actions, you can divide up your patch policies with a more defined set of rules and requirements for each policy, which will reduce the number of actions per policy.

You can also modify the default limit for policy bundle actions with the use of the system variable, `PATCH_POLICY_ACTIONS_LIMIT`. For information about setting the variable, see [Patch Management System Variables](#).

9. Continually monitor patch policies, ensuring that you have the available space and bandwidth to avoid any calamity on your network. If you have large groupings among your assets, it may be necessary to stagger deployments; this way you will not impact the integrity of your network, and normal operating can continue alongside the task of protecting against future problems.
10. If you want to make changes to the schedule of a Patch Policy, ensure that you configure it within the Patch Policy Settings page. If the schedule is configured within any other page of ZCC, such as Device's Assignments or the Bundle's Relationship page, under Assignment Details, it will not override the schedule that was previously defined in the Patch Policy Settings page. Instead, it will be run multiple times, based on the schedule configured within each page.
11. If you delete an old patch policy from an end point and then publish a new policy to replace it, the end point may list a Device-Assigned Bundle Status of **Not Installed** for an indefinite period of time. If you encounter this end point status, reboot the end point to complete publication of the patch policy.
12. Vendors will occasionally supersede Critical patches with Recommended patches. For example, Microsoft sometimes releases a second recommended Windows 10 cumulative update later in the month that supersedes an earlier critical update. The recommended update fixes the same security issues as the superseded critical update, but no new security issues are fixed so Microsoft rates it as Recommended rather than Critical.

If you want to continue to distribute the Critical patch rather than a Recommended patch that supersedes it, you can use the following options:

- ◆ Delay the disabling of superseded patches for XX days: This option causes the superseded patch to remain enabled so that it can continue distributed to devices.
- ◆ Do not disable superseded patches that are included in a policy: This option keeps a superseded patch enabled until it is removed from a Patch policy during the policy's next scheduled rebuild.

For example, assume that you have a Patch policy that installs all Microsoft critical patches. If Microsoft releases a second recommended monthly update that supersedes the critical monthly update, the superseded critical monthly update will no longer be distributed by the policy and the recommended update will not be included in the policy (even if the policy is rebuilt) because it is not critical. To avoid this situation and ensure that devices continue to receive the critical cumulative update, you would need to enable the "Do not disable superseded patches that are included in a policy" option.

A second example would be a Patch policy that installs all patches with "Cumulative Update for Windows 10" in the name. Occasionally, Microsoft releases a preview patch with "Cumulative Update Preview for Windows 10" in the name. The preview patch, which is recommended, supersedes the critical cumulative update so the policy no longer installs the superseded critical update. In this situation, enabling the "Do not disable superseded patches that are currently in a policy" option would also resolve the issue.

The two supersedence options are in the CVE and Patch Cleanup settings in ZENworks Control Center ([Configuration](#) > [Management Zone Settings](#) > [Security](#) > [CVE and Patch Cleanup](#)).

Create a Patch Policy

Before creating a patch policy it is important to plan your deployment, and ensure that you know the devices you would like to reach and the remediations you would like to deliver. It is recommended that you setup a test machine to test the efficacy of the patch before deploying across a global environment. For more information, see [Test a Policy Before Deploying to a Live Environment](#).

To create a new patch policy:

- 1 Click **Security** in the navigation menu, and select the **Patch Policies** page.
- 2 Click **New** in the Patch Policies panel.
- 3 Choose a platform, and click **Next**.
- 4 Name the policy, add any descriptive notes to identify the policy by, and click **Next**.
- 5 Click **Add Filter** and select rules for the policy that will limit the patches cached in the zone to only those you need. The following filters are available:

Filter Item	Result
Age	Select by age of patch: in days, weeks, months etc.
Architecture	Toggle between 32bit and 64bit
CVE Identifier	Insert a relevant CVE code
Impact	Choose Impact of patch 'Critical', 'Recommended', or 'Informational'
	<p>NOTE: Software Installers are not included to avoid unnecessary risk. However, you can always add specific installers to the policy via the Members tab.</p> <p>For more information, see Step 4 in Configure Advanced Parameters.</p>
Patch Name	Filter by Patch Name ie: MSxxx xxx
Release date	Select by Patch Release date
Vendor	Select by Patch Vendor

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

- Once the selection is made, click **Apply**. The box below the selection tool will populate with relevant patches (assuming that you have replicated and have at least one registered agent). Review the Patches in the Included Patches table, and if satisfied to continue, click **Next**.
- Configure the final options for creating the policy in Step 4 of the wizard (see below), and then click **Finish**.

Option	Description
Auto approve patches after successful test enforcements	Automatically applies patches to non-test devices after they are successfully tested in the Sandbox on one or more test devices.
Approve after x days	Delays applying patches to non-test devices this number of days after a successful test in the Sandbox.
Recalculate after x days	Rebuilds the patch policy to include any filter changes after a number of specified days. After the policy is created, this setting can be modified in the policy Summary page by editing Time to recalculate patch policy from rules .
Rebuild policy on creation	Auto-rebuilds the patch policy upon policy creation.
Define additional properties	Opens directly to the policy editing pages after the policy is created. From here you can assign the policy and make other property changes. When this option is not selected, the Patch Policies list displays, and you have to open the policy from the list to define additional properties. See Configure Advanced Parameters .

Before you can test or publish a policy, you need to assign one or more devices to it and then execute the Rebuild function. Any changes to the patch policy after initially testing it, or publishing it, will not be effective until you either manually rebuild the policy or it is auto-rebuilt on the Recalculation interval.

For information on editing a patch policy, assigning the patch policy to devices, testing the patch policy, or publishing the patch policy, see the following:

- ◆ [“Editing Patch Policies” on page 63](#)
- ◆ [Assign a Patch Policy to Devices](#)
- ◆ [Test a Policy Before Deploying to a Live Environment](#)
- ◆ [Publish a Patch Policy](#)

IMPORTANT: If you delete an old patch policy from an end point and then publish a new policy to replace it, the end point may list a Device-Assigned Bundle Status of **Not Installed** for an indefinite period of time. If you encounter this end point status, reboot the end point to complete publication of the patch policy.

Configure Advanced Parameters

To achieve an even more targeted remediation within the Patch Policy function, there are a number of advanced settings available. These settings are accessible when a patch policy is opened from the Patch Policies page or when **Define Additional Properties** is selected during patch creation.

To configure advanced parameters in a patch policy:

- 1 Go to **Security > Patch Policies**.
- 2 Click a patch name in the **Patch Policies** page to display the editing page options. In addition to the Summary and **Relationships** pages, there are five other pages where you can modify patch policy criteria:
 - ◆ Requirements
 - ◆ Rules
 - ◆ Members
 - ◆ Actions
 - ◆ Patches
- 3 Select the **Requirements** page to configure filters from several variables that further define the devices that will get patched as a result of the patch policy.

Click **Add** to choose a single filter option, or click **Add Filter Set** to insert the and/or operator between a set of variables.

Filter Item	Result	Platform
Architecture	Toggle between 32bit and 64bit	All
Bundle Installed	Choose between installed bundles	All
Configuration Location	The location of the server	All

Filter Item	Result	Platform
Configuration Network Environment	Select the network environment	All
Connected	Connected or Not Connected	All
Connection Speed	Choose the speed of the connection	All
Disk Space Free	Select by Disk space available	All
Disk Space Total	Select by Disk space total	All
Disk Space Used	Select by Disk space used	All
Environment Variable Exists	Is there a pre-existing variable	All
Environment Variable Value	The value of the pre-existing variable	All
File Date	Select by File date	All
File Exists	Select by pre-existing File name	All
File Size	Select by File size	All
File Version	Select by File version	Windows
IP Segment	Select by pre-existing File date	All
Linux Distribution	Select the Linux variants to target	Linux
Linux Kernel version	Select the Linux Kernel version to target	Linux
Linux Service Pack	Select the Service pack version to target	Linux
Logged on to Primary Workstation	Select Logged on or not Logged on	Windows
Mac Distribution	Select the Mac OS version	Mac
Memory	Choose the memory	All
Novell Client Installed	Novell client installed - yes or no	Windows
Operating System- Windows	Choose the Windows variant	Windows
Primary User is Logged In	Primary user logged in -yes or no	Windows
Processor Family	Select by Processor	All
Processor Speed	Select by Processor speed	All
Registry Key Exists	Add a Registry Key and choose yes or no	Windows
Registry Key Value	Add a Registry Key value and yes or no	Windows
Registry Key and Value Exists	Add a Registry Key and Value and yes or no	Windows

Filter Item	Result	Platform
Security Location	Select by security location	Windows
Service Exists	Insert a Service name and yes or no	All
Specified Devices	Add specific devices (has search function)	All
Version of Application	Select by Application Version	Mac
Version of RPM	Select by RPM Version	Linux
ZENworks Agent Version	Select by ZENworks Agent version	Windows

4 Select the **Members** page to add a specific patch to the policy.

The patches can be selected by Name, Impact, Date, Vendor, or All and either added or removed. If you are using this feature in conjunction with other settings, it will ensure no duplication of caching, and the selected patch will stay as a member of the policy until it is removed.

5 Select the **Actions** page to specify an administrative action before or after a deployment.

Click the **Add** button on Pre-Enforcement or Post-Enforcement sections to open the selection menu. Each selection has its own set of custom parameters.

End Process	Choose to end a process -i.e. Notepad
File Removal	Choose to remove a file
Install Bundle	Select to install a bundle
Launch Bundle	Select to launch a bundle
Launch Executable	Launch an executable
Run Script	Run a custom script

6 The purpose of the patches page is for the user to have control over the deployment of patches. When a policy is first created, the final step is to rebuild the policy. This is done using the **Rebuild** button on the policy Summary page. After this button is clicked, the list of patches in the Patches page should populate.

After the page is populated with patches, click **Actions** and it will open a small menu. The options available are **Enable**, **Disable**, and **Update Cache**. When you have an action to take, check the box next to the patch you wish to take action with and select the appropriate action. The Patches page also contains information about patch deployment status, including patch impact, patch or not patched devices for a given patch, and the patch release date.

Editing Patch Policies

Using the Edit option you can make a copy of or rename an existing patch policy. You can save time by copying a patch policy when a complex patch configuration can be reused or slightly modified. The selection box must be checked to enable this option. When you copy a patch policy, the published version of the policy is copied.

Assign a Patch Policy to Devices

Once a patch policy is created and configured, you need to assign it to one or more devices. You can also assign it to a workstation group. If you have not already configured one or more devices as Test devices, see [Test a Policy Before Deploying to a Live Environment](#).

To assign a patch policy to one or more devices:

- 1 Go to the Patch Policy Summary page (**Security > Patch Policies**), and click the patch link in the Name column.
- 2 Select the **Relationships** page, and click **Add**.
- 3 Click the down arrow for **Devices** to display the type of devices available.
- 4 Click the down arrow for **Servers** or **Workstations** to display the groups and devices for the selected folder.
- 5 Select the devices that are targeted for patch testing or deployment to move them into the **Selected** panel, and then click **OK**.

IMPORTANT: If you delete an old patch policy from an end point and then publish a new policy to replace it, the end point may list a Device-Assigned Bundle Status of Not Installed for an indefinite period of time. If you encounter this end point status, reboot the end point to complete publication of the patch policy.

The devices assigned to the patch policy will now be listed in the Relationships page. With the assignment complete, you are ready to test and publish the policy.

Test a Policy Before Deploying to a Live Environment

We advise ZENworks Administrators to always dry run their policies on a Test device before releasing to a live environment. Once a policy is released in a live environment, rescinding the changes that have been made can be difficult and time consuming.

Normally you would configure your Test devices before creating a patch policy for them; however, you can run a Rebuild at anytime. The Rebuild command uses the Sandbox to apply patches on all test devices assigned to the policy that is being rebuilt, according to the rules you configure for the policy.

If your test devices are configured as "Test" devices before they are assigned to the patch policy, applicable patches are automatically deployed to the test devices without rebuilding or publishing.

Understanding "Auto approve patches after successful test enforcement"

If the patch policy has **Auto approve patches after successful test enforcement** configured, the policy will automatically enforce on non-Test devices assigned to the policy after successfully applying ALL patches to ALL Test devices in the policy (post Rebuild).


Other considerations for this setting:

- ♦ A patch scan determines and reports when all Test devices assigned to the policy have all applicable patches installed.
- ♦ Having any of your assigned test devices offline for an extended period of time could impact the timing of non-Test devices assigned to the policy from getting patched.

- ◆ Rebuilds (whether manual or automatic from recalculation), that are spaced too close together, could impact the timeliness of patching, because a rebuild restarts the patching of any uninstalled patches on Test devices according to the schedule set in the patch policy.
- ◆ Once all assigned Test devices are successfully patched, the patch policy is published, irrespective of any schedule settings. However, when **Auto approve patches after successful test enforcement** is enabled, you can use the **Auto approve time delay** option in the policy Summary page to delay this action.
- ◆ Patches are not applied to any devices (Test or non-Test) until the ZENworks Agent is refreshed on applicable devices.

To configure one or more devices for Test:

- 1 Beginning in the navigation menu, click **Devices > Workstations**.
- 2 Select the check box for one or more devices. Only workstations or satellite servers can be configured for test, a Primary Server cannot be used for testing while operating as a server.
- 3 Open the **Action** drop-down menu, and select **Set as Test**.

Once you have made the selection, a small yellow arrow appears on the workstation icon . If you mouse over the workstation icon, an info box displays “Test Workstation.”

- 4 If you assigned the test device(s) to the policy before configuring it as a test device, you can now execute the **Rebuild** option from the policy Summary page to test the policy. Otherwise, make the **assignments** before testing the policy.

NOTE: You can also configure devices for testing directly from the device Summary page by clicking the **Set** link on the **Test Device** item. However, you can only configure one device at a time in this manner.

Publish a Patch Policy

If you chose to not **auto approve patches after successful test enforcements** in the patch policy configuration, you will need to publish the policy after executing Rebuild to apply patches to policy-assigned devices that are not set as Test devices.

To publish a patch policy:

- 1 Go to the Patch Policy Summary page, **Security > Patch Policies**, and click the patch link in the Name column.
- 2 Review the policy configuration in the Summary page (if applicable, make changes).
- 3 Click **Rebuild** in the Summary page.

When the policy is first created, its default status is **Sandbox** in the Displayed Version menu at the top of the page. If the policy was previously published, it will have one or more policy versions to choose from here.

- 4 Click **Publish** to update the information in the summary box and to publish the policy.

If you return to your agent device and refresh it, you will see the policy in the ZENworks Agent window.

IMPORTANT: If you delete an old patch policy from an end point and then publish a new policy to replace it, the end point may list a Device-Assigned Bundle Status of Not Installed for an indefinite period of time. If you encounter this end point status, reboot the end point to complete publication of the patch policy.

Deploying Patches Manually

To distribute patches manually, use the Deploy Remediation Wizard, which 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. After completing the wizard, the deployment will be listed in the Bundles page.

You can access the Deploy Remediation Wizard from the Action menu on one of the following pages:

- ◆ Security > Dashboard > Recently Released Patches
- ◆ Security > Patches
- ◆ Devices > [selected device] > Patches

You can also click the **Deploy Remediation** link under Patch Management shortcuts in the navigation menu. These shortcut options appear when the Patch Management > Patches page is open.

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

IMPORTANT: Once you initiate a patch remediation and the patch bundles are created for the remediation, the patch bundles should not be modified. If patch remediation bundles get modified, they may not replicate to Primary servers leaving the intended devices not patched.

Create a Deployment Schedule

To create a deployment schedule for one or more patches on one or more devices:

- 1 Go to **Security > Dashboard** or **Security > Patches**.
- 2 Select one or more patches that you want to deploy.
- 3 Select **Deploy Remediation** from the **Action** menu in the Patches list.

The Deploy Remediation steps vary, depending on the remediation option chosen in Step 5 of the wizard. For information about a specific step, click its applicable link in the table below:

Deploy Remediation Steps		
Auto Reboot	No Reboot	Advanced

Deploy Remediation Steps		
1. Confirm Devices	1. Confirm Devices	1. Confirm Devices
2. License Agreement	2. License Agreement	2. License Agreement
3. Remediation Schedule	3. Remediation Schedule	3. Remediation Schedule
4. Deployment Order and Behavior	4. Deployment Order and Behavior	4. Deployment Order and Behavior
5. Remediation Options	5. Remediation Options	5. Remediation Options
6. Notification and Reboot Options	6. Choose Deployment Name	6. Advanced Remediation Options
7. Choose Deployment Name	7. Deployment Summary	7. Pre Install Notification Options
8. Deployment Summary		8. Distribution Schedule
		9. Notification and Reboot Options
		10. Choose Deployment Name
		11. Deployment Summary

Confirm Devices

The Confirm Devices page allows you to select and confirm the devices for which you need to schedule a deployment.

The page indicates the total number of devices to which the selected patch will be deployed. You can change how many items are listed on the page by using the **show items** drop-down menu.

- 1 Select one of the following options to determine the devices to which the patches are to be deployed.:
 - ♦ **All non-patched devices:** Deploys the patch to those devices that are in a non-patched state. Selecting this option deploys the patch to all the devices that are not patched.
 - ♦ **Select applicable devices:** Deploys the patch to the devices you select from the devices list. You can deploy a patch to a device regardless of its existing patch status, which can be patched or not patched.

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

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

- ◆ **Select devices, folders and groups:** Deploys the patch to specific devices, folders, or groups that are in a non-patched state.

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

1. Click the **Add** menu item on the Confirm Devices page.
2. Click the arrow next to the **Devices** option on the left side of the window to display the available devices, folders, and groups.
3. Click the desired device to add it to the **Selected** panel on the right side of the window.

or

To remove a device from the panel, click the **Delete** button in the **Remove** column for that device.

4. Click **OK** to confirm device selection.

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

- 2 After choosing an option and selecting one or more devices, click **Next** to open the [License Agreement](#) page.

License Agreement

The License Agreement page displays all the third-party licensing information associated with the selected patches.

Select **Accept** for the license agreements you want to accept. To view the license agreement details, click the name of the patch. If the selected patches do not require a license, you can proceed to the next step.

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

Click **Next** to open the [Remediation Schedule](#) page.



Remediation Schedule

In the Remediation Schedule page you configure how a patch is scheduled and deployed for selected devices.

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

- ◆ **Now:** Schedules the deployment to your selected devices immediately after you complete all the steps in the Deployment Remediation Wizard.
- ◆ **Date Specific:** Schedules the deployment to your selected devices according to the selected date.

When you select **Date Specific**, you can choose from the following schedule options:

- ◆ **Start Date:** Enables you to pick the date when you need to start the deployment. To do so, click the plus icon  to open the calendar and pick the date. To remove the selected date, click the minus icon .
- ◆ **Run event every year:** Ensures that the deployment starts on a selected date at a selected time, repeats every year, and if defined, ends on a specific date.
- ◆ **Process immediately if device unable to execute on schedule:** Ensures that the deployment starts immediately if the device could not execute on the selected schedule.
- ◆ **Select when schedule execution should start:** There are two options to enable you to select the start time of the schedule execution using a 24 hour clock, namely:

- ◆ **Start immediately at Start Time:** Deactivates the **End Time** panel and starts the deployment at the start time specified. In this option, you must set the start time in the **Start Time** panel:

Start Time: :

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

End Time: :

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

- ◆ **Recurring:** Starts the deployment on the selected day at a selected time, repeats the deployment every day/week/month, and if defined, ends on a specific date.

By default, the bundle install frequency is set to **Install once per device**. For a recurring deployment, change it to **Install always**, after finishing the Deploy Remediation Wizard. For more information, see “[Install Action Set Options](#)” in the *ZENworks Software Distribution Reference*.

In the Recurring Remediation Schedule, 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 until after a specific time.

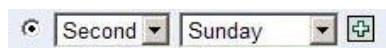
To set the delay, select the **Delay execution after refresh** check box, and specify the days, hours, and minutes of the time to delay the deployment:

NOTE: The device is refreshed based on the settings in the **Device Management** page under the **Configuration** page. Click the **Device Refresh Schedule** link under **Device Management** 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** page and clicking the **Refresh Device** option under the **Quick Tasks** menu.

- ◆ **Days of the Week:** This option enables you to schedule the deployment on selected days of the week:

To set the day of deployment, select the **Days of the week** button, select the required day of the week, and set the start time of deployment. If you click the **More Options** link, additional deployment options appear:

- ◆ Select the **Use Coordinated Universal Time** check box to schedule the deployment of all devices at the same time, regardless of time zone differences. Coordinated Universal Time (UTC), also known as World Time, Z Time, or Zulu Time, is a standardized measurement of time that is not dependent upon the local time zone. Deselecting UTC schedules the distribution at local time.
- ◆ Select the **Start at a random time between Start Time and End Times** check box to activate the **End Time** panel in addition to the **Start Time** panel. You can specify the end time and the start time so that the deployment occurs at any random time between the start and end times.
- ◆ The **Restrict schedule execution to the following date range** option enables you to schedule a recurring deployment at the selected time, repeat the deployment on the days specified, and if defined, end at the specific time. This option also enables you to restrict the deployment to the period between the start date and the end date. To set this option, select the **Restrict schedule execution to the following date range** check box and click the  icon to open the calendar and pick a start date or end date. Click the **Close** button when you have finished selecting the date.
- ◆ **Monthly:** In the **Monthly** deployment option, you can specify the following:
 - ◆ **Days of the month:** Enables you to schedule the deployment on a specific day of the month. You can specify any number between 1 and 31.
 - ◆ **Last day of the month:** Enables you to schedule the deployment on the last day of the month.
 - ◆ **Particular days of the month:** Enables you to schedule the deployment on specific days of every month. The valid options for the day are first, second, third, fourth, and fifth. The valid options for the weekday are Sunday through Saturday. To select one particular day of the month, use the drop-down arrows. An example is shown as follows.



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



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

If you click the **More Options** link, additional deployment options appear as shown below.

Monthly

Day of the month:
 Last day of the month

Start Time: :

[Hide Options](#)


Process immediately if device unable to execute on schedule
 Use Coordinated Universal Time (Current UTC 8:19 AM)
 Start at a random time between Start and End Times
End Time: :
 Restrict schedule execution to the following date range:
Start Date:
End Date:

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

- ◆ **Fixed Interval:** This option enables you to schedule a recurring deployment that runs after a fixed duration on a regular basis. You can choose the number of months, weeks, days, hours, and minutes of the interval and the start date for the deployment schedule.

If you click the **More Options** link, additional deployment options appear:

Fixed Interval

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

[Hide Options](#)

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

End Date:

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

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.

All of the schedule settings above also have the option to configure the Wake-on-LAN setting, which can schedule a deployment to devices that are powered off. For more information, see [Remediation Schedule: Wake On LAN](#).

Remediation Schedule: Wake On LAN

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

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

To change the parameters:

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

Deployment Order and Behavior

The Deployment Order and Behavior page enables you to set the order for each deployment schedule. If you have more than one patch, use the arrow buttons to set the priority for deployment.

The page consists of the following:

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

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

Click [Next](#) to open the [Remediation Options](#) page.

Remediation Options

The Remediation Options page enables you to select the required remediation option for each deployment schedule.

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

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

Table 5-1 The Remediation Options





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



















Click [Next](#) to open the [Advanced Remediation Options](#) page.


Advanced Remediation Options

The Advanced Remediation Options page enables you to set patch flags for each remediation. The icons displayed on the page represent the patch flags that can be set for each package.

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

Icon	Name	Functionality
	Uninstall	Uninstalls the packages.
	Force Shutdown	Forces all applications to close if the package causes a reboot.
	Do Not Back Up	Does not back up files for uninstalling.
	Suppress Reboot	Prevents the computer from rebooting after installation of the package.

Icon	Name	Functionality
	Quiet Mode	Sets the installer to function in quiet mode. Quiet mode suppresses any user interfaces (if a user is logged in) during the remediation.
	Unattended Setup	Installs the packages in the Unattended Setup mode.
	List Hot Fixes	Returns a list of the hot fixes installed on the target computers.
	Force Reboot	Forces the computer to reboot regardless of package requirements.
	Reboot is Required	Indicates that this package requires a reboot prior to completing the installation. Selecting this option reboots the device even if the specific bundle does not require a reboot.
	Chain Packages	Sets the package as chainable (if the package supports chaining). This option cannot be modified in this release; the package is always installed with the “chain” option.
	Suppress Chained Reboot	Suppress the reboot, allowing other chained packages to be sent following this package You should suppress the final reboot for all chained packages, then send a reboot deployment when all packages are finished.
	Repair File Permissions	Repairs file permissions after package installation.
	Download Only	Distributes the package without running the package installation script.
	Suppress Notification	Suppresses any user notifications during installations.
	Debug Mode	Runs the package installation in debug mode.
	Do Not Repair Permissions	Suppresses the repair of filename permissions after the reboot.
	May Reboot	Allows the package to force a reboot if required.
	Multi-User Mode	Performs the installation in Multi-User mode.
	Single-User Mode	Performs the installation in Single-User mode.
	Restart Service	Restarts the service following the deployment.
	Do Not Restart Service	Does not restart the service following the deployment.
	Reconfigure	Performs the system reconfigure task following the deployment.

Icon	Name	Functionality
	Do Not Reconfigure	Does not perform the system reconfigure task following the deployment.

NOTE: Depending on the type of patch you select, the icons displayed above change dynamically, so you might not be able to select some of the options described in the table.

Click **Next** to open the [Pre Install Notification Options](#) page.

Pre Install Notification Options

The Pre Install Notification Options page allows you to define whether users receive any notification when patches are downloaded and installed, and to customize the notification.

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

Refer to the information below to understand how to define Pre Install options:

- ◆ **Use values assigned to system variables or defaults:** Select this option to use the default pre-install notification options defined within **Patch Policy Settings**.
- ◆ **Override Settings:** Select this option to override the default options and choose new ones. Selecting this option makes the remaining options available.
 - ◆ **Notify Users of Patch Install:** Select this option to notify the user prior to the installation of the patch. There are two additional options:
 - ◆ **Prompt before download:** Select this option to notify the user when the patch download process begins.
 - ◆ **Prompt before install:** Select this option to notify the user when the patch installation process begins.
 - ◆ **Description text:** The text of the notification message. You can edit this field only if you override the default settings.
 - ◆ **Options:** When you define installation options, you can specify whether to use the values in the default settings (the **Use values assigned to system variables or defaults** check box) or the custom settings. There are three options:
 - ◆ **Allow User to cancel:** Allows the user to cancel the patch installation.
 - ◆ **Allow User to snooze:** Allows the user to delay the installation.
 - ◆ **Snooze interval:** The duration the install is delayed when the user snoozes.
 - ◆ **Install within:** The deadline that the user can no longer snooze the installation.

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



- ◆ **Show tray notification:** On selecting this option, a notification for a pending installation is displayed in the system tray. If you select this option, define the following:
 - ◆ **Tray notification duration:** Enter a value in hours, minutes or seconds for how long the system tray notification is displayed before being hidden.
 - ◆ **Tray notification text:** Type the text you want to appear in the notification.

Click the **Next** button to proceed to the Notification and Reboot Options Distribution Schedule page.

Distribution Schedule

The Distribution Schedule page of the Deploy Remediation Wizard allows you to determine when a patch will be distributed to and installed on the devices.

To start setting the distribution schedule, you need to select the schedule type. Patch Management offers three types of schedules to determine when the patches are actually distributed to the target device: No Schedule, Date Specific, and Recurring.

- ◆ **No Schedule:** If you select **No Schedule**, the distribution to your selected devices begins immediately after you complete all the steps in the Deploy Remediation Wizard.
- ◆ **Date Specific:** If you select **Date Specific**, the distribution to your selected devices occurs according to the selected date that you set in the wizard's Distribution Schedule page, as follows:
 - ◆ **Start Date:** Enables you to pick the date when you need to start the distribution. To do so, click the plus icon  to open the calendar and pick the date. To remove the selected date, click the minus icon .
 - ◆ **Run event every year:** Ensures that the distribution starts on a selected date at a selected time, repeats every year, and if defined, ends on a specific date.
 - ◆ **Process immediately if device unable to execute on schedule:** Ensures that the distribution starts immediately if the device could not execute on the selected schedule.
 - ◆ **Select when schedule execution should start:** There are two options to enable you to select the start time of the schedule execution namely:
 - ◆ **Start immediately at Start Time:** Deactivates the **End Time** panel and starts the distribution at the start time specified. In this option, you must set the start time in the **Start Time** panel:

Start Time: :

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

End Time: :

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

Selecting the **Use Coordinated Universal Time** check box enables you to schedule the distribution to all devices at the same time, regardless of time zone differences.

Coordinated Universal Time (UTC), also known as World Time, Z Time, or Zulu Time, is a standardized measurement of time that is not dependent upon the local time zone.

Deselecting UTC schedules the distribution at the local time.

- ◆ **Recurring:** If you select **Recurring**, you can start the distribution on the selected day at a selected time, repeat the deployment every day/week/month, and if defined, end on a specific date.

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


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

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

NOTE: The device is refreshed based on the settings in **Configuration > Device Management** menu > **Device Refresh and Removal Schedule** (Manual Refresh or Timed Refresh). Alternatively, you can refresh the device by selecting a device in the **Devices** page and clicking the **Refresh Device** option in the **Quick Tasks** menu.

- ◆ **Days of the week:** This option enables you to schedule the distribution on selected days of the week.

To set the day of distribution, select the **Days of the week** button, select the required day of the week, and set the start time of distribution. If you click the **More Options** link, additional distribution options appear. Click the **Hide Options** link to hide the additional distribution options and show only the default distribution options.

- ◆ Selecting the **Use Coordinated Universal Time** check box enables you to schedule the distribution to all devices at the same time, regardless of time zone differences. Coordinated Universal Time (UTC), also known as World Time, Z Time, or Zulu Time, is a standardized measurement of time that is not dependent upon the local time zone. Deselecting UTC schedules the distribution at local time.
- ◆ Selecting the **Start at a random time between Start Time and End Times** check box activates the **End Time** panel in addition to the **Start Time** panel. You can specify the end time and the start time so that the distribution occurs at any random time between the start and end times.
- ◆ The **Restrict schedule execution to the following date range** option enables you to schedule a recurring distribution at the selected time, repeat the distribution on the days specified, and, if defined, end at the specific time. This option also enables you to restrict the distribution to the period between the start date and the end date. To set this option, select the **Restrict schedule execution to the following date range** check box and click the calendar icon  to open the calendar and pick a start date or end date. Click the **Close** button when you have finished selecting the date.

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

A screenshot of a configuration interface for 'Particular days of the month'. It features a radio button selected next to the text 'Particular days of the month'. Below this, there are two dropdown menus: the first is set to 'Second' and the second is set to 'Sunday'. To the right of these dropdowns is a plus icon (+) for adding more days.

To select an additional day of the month, click the plus icon (+) and use the drop-down arrows in the second row shown as follows:

A screenshot of the configuration interface showing two rows of dropdown menus. The first row has 'Second' and 'Sunday' selected. The second row has 'First' and 'Monday' selected. Each row has a minus icon (-) to its right, and a plus icon (+) is located at the bottom right of the second row.

NOTE: To remove a particular day from the list, click the minus icon (-).

If you click the **More Options** link, additional distribution options appear. Clicking the **Hide Options** link hides the additional distribution options and shows only the default distribution options.

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

- ◆ **Fixed Interval:** This option enables you to schedule a recurring distribution that runs after a fixed duration on a regular basis. You can choose the number of months, weeks, days, hours, and minutes of the interval and the start date for the distribution schedule.

☑ **Fixed Interval**

A screenshot of the 'Fixed Interval' configuration. It shows five input fields for 'Months', 'Weeks', 'Days', 'Hours', and 'Minutes', each containing the number '0'. Below these are two date/time fields: 'Start Date' with the value '10/25/2011' and a calendar icon, and 'Start Time' with the value '1:00' and dropdown arrows for hours and minutes.

[More Options](#)

If you click the **More Options** link, additional distribution options appear as shown in the following figure.

Fixed Interval

0 Months 0 Weeks 0 Days 0 Hours 0 Minutes

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

[Hide Options](#)

Process immediately if device unable to execute on schedule

Use Coordinated Universal Time

Restrict schedule execution to the following date range:

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

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.

Notification and Reboot Options

In the Notification and Reboot Options page you can define whether users receive notification of patch deployments and reboots. You can also customize the notification.

The page provides the following options:

- ◆ **Define Reboot Options:** Allows you to use the default reboot options you've set in options or override them and set them manually for the deployment.
 - ◆ **Use values assigned to system variables or defaults:** Uses reboot options set for deployments.
 - ◆ **Override Settings:** Overrides the default reboot settings and lets you choose from the options below.
- ◆ **Notify Users:** Select this option to notify the user prior to a reboot required for installation of the patch.
- ◆ **Description Text:** The text of the message that appears before patch installation completes and the computer reboots. You can edit this field only if you override the default settings.
- ◆ **Options:** When you define reboot options, you can specify whether to use the values in the default settings (the **Use values assigned to system variables or defaults** check box) or the custom settings. There are four options:
 - ◆ **Suppress Reboot:** If a patch requires a reboot by default, and no reboot is desired, select the **Suppress Reboot** option to stop this action. This will prevent a reboot after installation.
 - ◆ **Allow User to cancel:** On selecting this option, the user is allowed to cancel the reboot option.
 - ◆ **Allow User to snooze:** On selecting this option, the user is allowed to snooze (pause) the reboot for a particular time.
 - ◆ **Snooze interval:** The amount of time before a user is prompted again to reboot after snoozing.
 - ◆ **Reboot within:** The amount of time before a user is forced to reboot for the deployment.

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

A message prompt appears when a reboot is required.



Depending on the notification settings configured, the prompt may include delay and cancellation options.

Click **Next** to define a deployment name.

Variables

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

- ♦ **ConfigManager.SetDefaultConfigValue(PATCH_MANDATORY_NOTIFY_REBOOT_REBOOT_TIMEOUT, "7200");** Time to do prompts before rebooting, in seconds.
- ♦ **ConfigManager.SetDefaultConfigValue(PATCH_MANDATORY_NOTIFY_REBOOT_POPUP_SHOW_TRAY, "true");** Whether to show the popup in the corner.
- ♦ **ConfigManager.SetDefaultConfigValue(PATCH_MANDATORY_NOTIFY_REBOOT_POPUP_DURATION, "20");** How long to display the popup, in seconds.
- ♦ **ConfigManager.SetDefaultConfigValue(PATCH_MANDATORY_NOTIFY_REBOOT_SNOOZE_INTERVAL, "600");** The time to wait before showing popup again. In seconds.
- ♦ **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_REBOOT_REBOOT_TIMEOUT, "7200");** The time to wait before the system notifies a time out, in seconds.
- ♦ **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_REBOOT_POPUP_SHOW_TRAY, "true");** The value indicates whether or not the system will show a popup before reboot.
- ♦ **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_REBOOT_POPUP_DURATION, "20");** This value indicates the length of time for the popup to remain.
- ♦ **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_REBOOT_SNOOZE_INTERVAL, "600");** The value sets the length of time for the snooze interval before reboot prompt, in seconds.

- ◆ **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_INSTALL_REBOOT_TIMEOUT,"7200");**
The value shows the amount of time before the system reboots after an install timeout, in seconds.
- ◆ **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_INSTALL_POPUP_SHOW_TRAY,"true");**
The value determines whether a popup appears to notify of install.
- ◆ **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_INSTALL_POPUP_DURATION,"20");**
This value sets the length of time that the popup will show for on install, in seconds.
- ◆ **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_INSTALL_SNOOZE_INTERVAL,"600");**
The value sets the length of time for the snooze interval after install, in seconds.

The following are no longer used:

- ◆ PATCH_NOTIFY_REBOOT_SNOOZE_TIMETOLIVE
- ◆ PATCH_NOTIFY_REBOOT_DIALOG_TIMEOUT
- ◆ PATCH_NOTIFY_INSTALL_SNOOZE_TIMETOLIVE
- ◆ PATCH_NOTIFY_INSTALL_DIALOG_TIMEOUT
- ◆ PATCH_MANDATORY_NOTIFY_ALLOW_SNOOZE
- ◆ PATCH_MANDATORY_NOTIFY_DIALOG_TIMEOUT
- ◆ PATCH_MANDATORY_NOTIFY_DIALOG_TIMEOUT_ENABLED
- ◆ PATCH_MANDATORY_NOTIFY_SNOOZE_HOURS
- ◆ PATCH_MANDATORY_NOTIFY_SNOOZE_MINUTES
- ◆ PATCH_MANDATORY_NOTIFY_SNOOZE_DAYS

Choose Deployment Name

The Choose Deployment Name of the Deploy Remediation Wizard lets you customize the name of the deployment you have scheduled.

The page provides the following options:

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

Deployment Summary

The Deployment Summary page displays a summary of the configuration made in the previous steps:

- ◆ **Deployment Name:** The name of the deployment as defined on the Choose Deployment Name page.
- ◆ **Delivery Schedule:** The schedule selected for distribution of patches as defined on the Distribution Schedule page.
- ◆ **Deployment Schedule:** The schedule selected for the deployments as defined on the Remediation Schedule page.

- ♦ **Total Selected Packages:** The total number of patches selected for deployment.
- ♦ **Order:** The order of deployment of the patches as defined on the Deployment Order and Behavior page.
- ♦ **Package Name:** The name of the patch you have selected for deployment.
- ♦ **Reboot:** The reboot setting of the selected patch as defined in the Deployment Order and Behavior page.

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

6 Best Practices

Depending on the state of patch updates, number and type of devices, and other variables in your management zone, you might initially have a significant number of patches being cached on the servers for distribution when you first apply patch policies. Patch policy implementation will incrementally reduce the patch workload over time. The information in this section will help you to make good decisions in both initial deployment of patch policies and managing them in the long term.

Below are a few general recommendations in regards to managing patches using ZENworks Patch Management:

1. Inventory the organization's IT resources to determine which hardware equipment, operating systems, and software applications are used within the organization.
2. Monitor security sources for vulnerability announcements, patch and non-patch remediations, and emerging threats that correspond to the software within the organization's inventory.
3. Prioritize the order in which the organization addresses remediating vulnerabilities.
4. Create patch policies in ZENworks Patch Management that are built on organizational priorities.
5. Conduct testing of patches and non-patch remediations on IT devices that use standardized configurations.
6. Oversee patch policy implementation.
7. Distribute vulnerability and remediation information to local administrators.
8. Perform automated deployment of patches to IT devices using patch policies.
9. Reconfigure automatic update of applications whenever possible and appropriate.
10. Verify vulnerability remediation through network and host vulnerability scanning.
11. Train administrators on how to apply vulnerability remediations using patch policies.

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

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

Testing Patches

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

It is important that your organization determines a strategy for testing patches before release; this will vary from organization to organization, but should be in line with your current security policies. How you decide to test your patches before deployment will depend on your current architecture and policy. In some organizations it may be required to review your policies in order to effectively use this method.

However, it is highly recommended that patches are tested prior to deployment. For information on setting up test devices to implement patch policies, see [Test a Policy Before Deploying to a Live Environment](#).

Deploying Patches in a Controlled Way

You can deploy patches using patch policies or Deploy Remediation. Since the integration of patch policies in ZENworks Patch Management, the manual process of Deploy Remediation, is generally used by exception. See [Distribute and Apply Patches](#).

Patches are released frequently, and it is possible to automate the entire release process by using the deployment settings. While this may suit some smaller companies, in a large organization with multiple platforms and sites, we recommend that administrators design a strategy for deployment. Each patch for each software update will behave differently, which is why it is necessary to control the process. For example, some software will require a reboot after updating, and although ZENworks can manage this process on your behalf, your team should determine the details of this, and be aware of any other software or processes which are running, or patches that are being installed concurrently. The Best Practice recommendation for controlling these processes is to use a phased approach.

Implementing patch management tools in phases allows process and user communication issues to be addressed with a small group before deploying the patch application universally. Most organizations deploy patch management tools first to standardized desktop systems and single-platform server farms of similarly configured servers. Once this has been accomplished, organizations should address the more difficult issue of integrating multi-platform environments, nonstandard desktop systems, legacy computers, and computers with unusual configurations. Manual methods may need to be used for operating systems and applications not supported by automated patching tools, as well as some computers with unusual configurations; examples include embedded systems, industrial control systems, medical devices, and experimental systems. For such computers, there should be a written and implemented procedure for the manual patching process.

Monitoring Patch Implementation

Patch and vulnerability metrics fall into three categories: susceptibility to attack, mitigation response time, and cost, which includes a metric for the business impact of program failures. The emphasis on patch and vulnerability metrics being taken for a system or IT security program should reflect the patch and vulnerability management maturity level. For example, attack susceptibility metrics such as the number of patches, vulnerabilities, and network services per system are generally more useful for a program with a low maturity level than a high maturity level. Organizations should document

what metrics will be taken for each system and the details of each of those metrics. Realistic performance targets for each metric should be communicated to system owners and system security officers. Once these targets have been achieved, more ambitious targets can be set. It is important to carefully raise the bar on patch and vulnerability security to avoid overwhelming system security officers and system administrators.

Organizations should consistently measure the effectiveness of their patch and vulnerability management program and apply corrective actions as necessary.

For information on Patch Management monitoring tools, see the following:

- ◆ [Security Pages](#)
- ◆ [Viewing Zone Patches](#)
- ◆ [Viewing Patches for a Device](#)
- ◆
- ◆ [Accessing Patch Management Reports](#)

7 Manage Patches

In the **Patches** page you can view and take actions on patches that display as a result of the DAU fingerprints that come from devices in the zone. These are manual actions you can do directly from the Patches page, or you can create patch policies in the **Patch Policies** page that do the patch actions automatically based on the schedules you define in patch policies and patch configuration. In ZENworks there is a Patches page to view the zone level patches and a Patches page to view the device level patches.

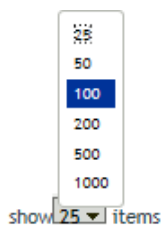
Manual actions in the Patches page include searching for patches, creating new patches from existing bundles, caching patches, and then deploying patches to managed devices. You can also do several house keeping functions to maintain the usefulness of the Patches page, including deleting, disabling, enabling, and even exporting patch entries. You can also refresh assignments using this page.

- [“Configure the Patch Display” on page 87](#)
- [“View Patch Details” on page 88](#)
- [“Create a Custom Patch” on page 102](#)
- [“Delete a Patch” on page 103](#)
- [“Execute Action Menu Options” on page 104](#)
- [“Release Quarantined Patches” on page 105](#)
- [“Patch Details Page” on page 106](#)
- [“Patch Requirements” on page 110](#)

Configure the Patch Display

This section explains features of the **Patches** page and how to use them.

To configure how many items show in the Patches panel, select a different item count in the drop-down menu at the bottom-right corner of the panel.



To sort patches alphanumerically, click on any column header in the table and it will sort based on that column. Clicking a header a second time reverses the order.

View Patch Details

Using the Patches page you can view the details of all patches that are applicable to the zone and you can also view information about all patches that are applicable for a specific device.

- ♦ [“Zone-Level Patches” on page 88](#)
- ♦ [“Device Patches” on page 94](#)

Zone-Level Patches

This page can be accessed by clicking the Security tab in the left navigation menu and then clicking the Patches tab. This page displays a list of all patches that are applicable to the zone and it provides the following information:

- ♦ [“Patch Name” on page 88](#)
- ♦ [“Total Patches Available” on page 89](#)
- ♦ [“Patch Impact” on page 89](#)
- ♦ [“Patched” on page 90](#)
- ♦ [“Not Patched” on page 91](#)
- ♦ [“Patch Release Date” on page 91](#)

Patch Name

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

An example of a patch name is shown as follows. It indicates that Adobe is the vendor, Adobe Flash Player is the application, and 21.0.0.242 is the version information:







 [Adobe Flash Player ActiveX 21.0.0.242 \(Full Install\) for Windows \(See Notes\)](#)

Microsoft Patches:

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

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

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

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

Total Patches Available

The total number of patches that are available for deployment is displayed in the bottom-left corner of the Patches panel. In the following figure, the total number of available patches is 106:

1 - 25 of 106 items

Patch Impact

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

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

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

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

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

Table 7-1 ZENworks and Microsoft Patch Impact Mapping

ZENworks Patch Impacts	Windows	Other
Critical	Critical Security	NA
	Important	
	Moderate	
Recommended	Recommended	NA
	Low	
Informational	NA	NA
	Software Installers	Software Distribution
	Example: Microsoft Windows Malicious Software Removal Tool (Virus Removal)	

Patched

The Patched column displays a link indicating the total number of devices to which the corresponding patch has been applied.

Click a link to display the [Devices](#) that are patched with the selected patch.

The screenshot shows the 'Patches' section of the ZENworks interface. It features a table with the following columns: Patch Name, Impact, Patched, Not Patched, and Released On. The table lists various patches such as 'Microsoft Visual C++ Redistributable for Visual Studio 2017', 'System Management - Enable Protection Against Speculative Store Bypass', 'Oracle Java SE Development Kit', 'Mozilla Firefox 59.0.2', 'Adobe Acrobat Reader DC', 'Opera Browser 49', 'Adobe Flash Player NPAPI', and 'Google Chrome 62.0.3202.94'. Each row includes a 'Patched' column with a link and a count of devices, and a 'Not Patched' column with a count of devices. The 'Released On' column shows the date the patch was released.

Not Patched

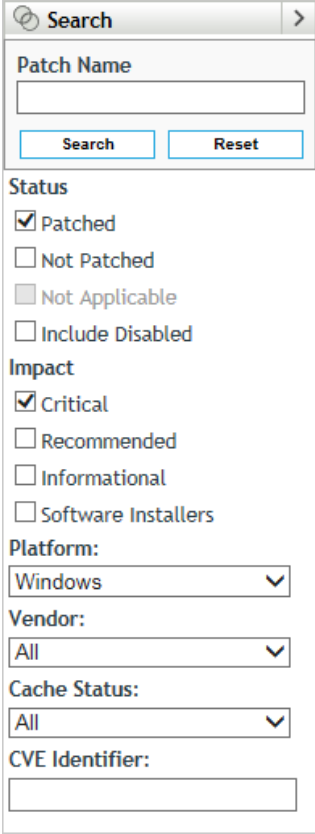
Displays a link indicating the total number of devices to which the corresponding patch has not been applied. Click a link to display the [Devices](#) on which the patch has not been applied as yet. You can deploy the patch to these devices by using the [Deploy Remediation](#) option.

Patch Release Date

The date the patch was released by the vendor is displayed in the right column under [Released On](#). Click the [Released On](#) column to sort patches by their release date. All the patches released in the last 30 days are displayed in bold font.

Search Patches

The [Search](#) panel on the Patches page offers extensive search and data filtering options that allow you to search for specific patches and filter result sets based on the status and impact of the patches. Searching and filtering can be performed independently of each other or can be combined to provide extensive drill-down capabilities.



The screenshot shows a search panel with the following sections:

- Search:** A text box for "Patch Name" with "Search" and "Reset" buttons below it.
- Status:** Checkboxes for "Patched" (checked), "Not Patched", "Not Applicable", and "Include Disabled".
- Impact:** Checkboxes for "Critical" (checked), "Recommended", "Informational", and "Software Installers".
- Platform:** A dropdown menu currently set to "Windows".
- Vendor:** A dropdown menu currently set to "All".
- Cache Status:** A dropdown menu currently set to "All".
- CVE Identifier:** An empty text box.

To search for a patch:

- 1 Type all or part of the patch name in the [Patch Name](#) text box.
- 2 Select applicable filter options; the CVE identifier must be typed.
- 3 Click [Search](#).

To filter from all existing patches:

- 1 Leave the **Patch Name** text box empty.
- 2 Select applicable filter options.
- 3 Click **Search**.

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

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

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

The following table describes the result of selecting each filter option under **Impact** (Impact Filters in Search):

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

The following table describes the remaining filter options on the Search panel:

Filter	Result
Platform	Search results include all the patches relevant to the operating system in the patch list.
Vendor	Search results include all the patches relevant to the vendor in the patch list.
Cache Status	Search results include all the patches relevant to their cache status on the local server.
CVE Identifier	Search results include all the patches that have the common vulnerabilities and exposures ID that you type.
Relationships	Search results include patches for devices assigned to a patch policy, according to the option selected in the filter menu.
NOTE: This filter is only applicable to the Patches page on a selected patch policy.	For more information, see “Understanding the Relationships Filter” on page 93.

Understanding the Relationships Filter

The Search feature on the Patches page for a patch policy differs from the Search feature on the global Patches page by omitting the **Platform** filter and adding the **Relationships** filter. The Relationships filter enables you to limit and define the reporting of patch status according to the devices assigned to the patch policy as described below:

First 500 Devices

This is the default setting. It displays patch status for the first 500 devices assigned under the Relationships tab of a selected patch policy. If the policy is assigned to more than 500 devices, the complete list of devices can be viewed under Patched and Not Patched column values.

Test Devices

This option displays patch status for patches on designated test devices assigned to the selected patch policy.

Specific devices

Specific devices, device folders, or device groups will be listed under the Test devices option. For example, <computer name>, Workstations, Windows 10 Workstations and so forth can be assigned as a relationship to the patch policy.

When you filter on one of these relationship types, patch status will only be displayed for device patches that fall within that device criteria.

IMPORTANT: Due to the complexity of returning Patched and Not Patched results and the variables involved, a hundred percent accuracy for device counts in patch status is uncommon with large organizations. For example, if your organization has more than 500 devices assigned to a patch policy and you open the Patches page on that policy, the aggregate number of devices in the Patched and Not Patched columns is unlikely to reach 500 with the Relationships.

Device Patches

Using the Device Patches Page you can view information related to all patches, patch policies and remediation bundles assigned to the selected device. You can also perform actions for particular patches and refresh the assignments made to the device. The Device Patches page includes the following panels:

- ◆ “Patches” on page 94
- ◆ “Assigned Patch Policies” on page 98
- ◆ “Assigned Remediation Deployments” on page 98

Patches

Figure 7-1

Patch Name	Impact	Patched	Not Patched	Released On
Microsoft Visual C++ Redistributable for Visual Studio 2017 (14.15.26706.0) (Full Install) for Windows (See Notes)	Software Installer	0	1	Jul-06-2018
System Management - Enable Protection Against Speculative Store Bypass (Client) (KB4073119) (Enabled)	Software Installer	0	1	Jun-12-2018
System Management - Enable Protection Against Speculative Store Bypass (Server) (KB4072698) (Enabled)	Software Installer	0	1	Jun-12-2018
System Management - Enable Protection Against Speculative Store Bypass (Server) (KB4072698) (Disabled)	Software Installer	0	1	Jun-12-2018
System Management - Enable Protection Against Speculative Store Bypass (Client) (KB4073119) (Disabled)	Software Installer	1	0	Jun-12-2018
Oracle Java SE Development Kit (JDK) 10.0.1 (Full Install) for Windows (See Notes)	Software Installer	0	1	Apr-17-2018
Oracle Java SE Development Kit (JDK) 8 Update 171 (8.0.1710.11) (Full Install) for Windows (See Notes)	Software Installer	0	1	Apr-17-2018
Mozilla Firefox 59.0.2 (en-US) (Full Install) for Windows (See Notes)	Software Installer	0	1	Mar-26-2018
Adobe Acrobat Reader DC (Continuous) 2018.011.20035 (18.11.20035.2003) (en-US) (Full Install) for Windows (See Notes)	Software Installer	0	1	Feb-23-2018
System Management - Enable Protection Against Spectre Variant 2 Independently (KB4078130) (Disabled)	Software Installer	0	2	Feb-05-2018
System Management - Enable Protection Against Speculative Execution Vulnerabilities (Client) (KB4073119) (Disabled)	Software Installer	0	1	Feb-05-2018
System Management - Enable Protection Against Speculative Execution Vulnerabilities (Client) (KB4073119) (Enabled)	Software Installer	0	1	Feb-05-2018
System Management - Enable Protection Against Spectre Variant 2 Independently (KB4078130) (Enabled)	Software Installer	0	2	Feb-05-2018
System Management - Enable Protection Against Speculative Execution Vulnerabilities (Server) (KB4072698) (Enabled)	Software Installer	0	1	Feb-05-2018
System Management - Enable Protection Against Speculative Execution Vulnerabilities (Server) (KB4072698) (Disabled)	Software Installer	0	1	Feb-05-2018
Opera Browser 49 (49.0.2725.391) (Full Install) for Windows (See Notes)	Software Installer	0	1	Nov-16-2017
Adobe Flash Player NPAPI 32.0.0.187 (Full Install) for Windows (See Notes)	Software Installer	0	1	Nov-14-2017
Adobe Flash Player NPAPI 32.0.0.187 (Full Install) for Windows (See Notes)	Software Installer	0	1	Nov-14-2017
Google Chrome 62.0.3202.94 (Full Install) for Windows (See Notes)	Software Installer	1	0	Nov-13-2017
Oracle Java SE Development Kit (JDK) 9.0.1 (Full Install) for Windows (See Notes)	Software Installer	0	1	Oct-17-2017
Oracle Java SE Development Kit (JDK) 8 Update 151 (8.0.1510.12) (Full Install) for Windows (See Notes)	Software Installer	0	1	Oct-17-2017
Microsoft Silverlight (KB4023207)	Software Installer	0	1	Jun-13-2017

This panel lists all the patches that are applicable to the device and provides the following information for each patch:

- ◆ “Patch Name” on page 95
- ◆ “Patch Impact” on page 95
- ◆ “Patched” on page 97
- ◆ “Assignments” on page 97
- ◆ “Release Date” on page 97
- ◆ “Installed On” on page 97
- ◆ “Installed By” on page 98

Patch Name

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

An example of a patch name is shown as follows. It indicates that Adobe is the vendor, Adobe Flash Player is the application, and 21.0.0.242 is the version information:

 [Adobe Flash Player ActiveX 21.0.0.242 \(Full Install\) for Windows \(See Notes\)](#)

Microsoft Patches:

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

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

When you click the patch name link, the [Patch Details Page](#) is displayed.

Patch Impact

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

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

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

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







Table 7-2 *ZENworks and Microsoft Patch Impact Mapping*

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

Patched

The Patched column indicates if the patch has been applied on the device or not. shows the relationship between a specific patch and the total number of devices (or groups) within ZENworks Server that meet a specific status. The patch statistics appear in two columns on the far right side of the Patches page. Each column status is described as follows:

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

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

Assignments

The name of the patch remediation bundle or policy assignment that includes the signature and is assigned to the device, is displayed in this column. When you click on the Assignment link, the Bundle or Policy Details page is displayed.

Release Date

The date the patch was released by the vendor is displayed in the right column under **Released On**. Click the **Released On** column to sort patches by their release date. All the patches released in the last 30 days are displayed in bold font.

Installed On

The date on which the patch signature was installed on the device, either through a remediation bundle, or through a patch policy. If the patch was not installed by ZENworks, this field will be empty.

Installed By

The name of the user who installed the patch on the device. If the patch was installed by ZENworks, then the value will be ZENworks. Else, if the patch was installed manually, for example, a Windows update, then the value will be Other.

The total number of patches that are available for deployment is displayed in the bottom-left corner of the Patches panel. In the following figure, the total number of available patches is 106:

NOTE: The total number of patches that are available for deployment is displayed in the bottom-left corner of the Patches panel.

Assigned Patch Policies

The Assigned Patch Policies panel displays all the enabled patch policies that are assigned to the device. This panel includes the following information:

- ◆ [“Policy Name” on page 98](#)
- ◆ [“Version” on page 98](#)
- ◆ [“Enforcement Schedule” on page 98](#)
- ◆ [“Source” on page 98](#)

Policy Name

The names of the enabled patch policies that are assigned to the device.

Version

The published version of the patch policy.

Enforcement Schedule

The schedule of when the policy is enforced on the device.

Source

Links to the source of the assignment, either the Device object's Summary page, the Device Group object's Summary page, or the Device Folder's Summary page. When you click the source, the object's Summary page is displayed. If there are multiple sources, they are displayed as an expandable hierarchy.

Assigned Remediation Deployments

This panel displays all the patch bundles that are assigned to the device. This panel includes the following information:

- ◆ [“Deployment Name” on page 99](#)
- ◆ [“Folder” on page 99](#)
- ◆ [“Created On” on page 99](#)

- ♦ [“Enforcement Schedule” on page 99](#)
- ♦ [“Source” on page 99](#)

Deployment Name

The remediation deployment name. When you click this link, the Bundle Summary page is displayed.

Folder

The path to the folder in which the bundle is saved.

Created On

The date on which the bundle assignment was created.

Enforcement Schedule

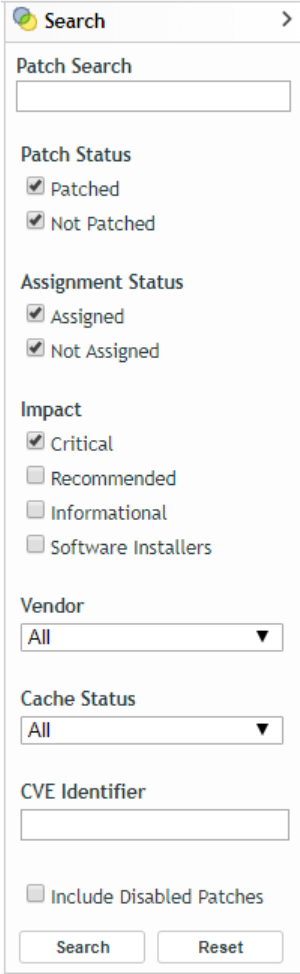
The schedule of when the deployment is enforced on the device. For example, Every Sun, Mon, Tue.

Source

Links to the source of the assignment, either the Device object's Summary page, the Device Group object's Summary page, or the Device Folder's Summary page. When you click the source, the object's Summary page is displayed. If there are multiple sources, they are displayed as an expandable hierarchy.

Search for Patches

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



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

- Patch Search:** A text input field for entering the patch name.
- Patch Status:** Two checked checkboxes: 'Patched' and 'Not Patched'.
- Assignment Status:** Two checked checkboxes: 'Assigned' and 'Not Assigned'.
- Impact:** Four checkboxes: 'Critical' (checked), 'Recommended', 'Informational', and 'Software Installers'.
- Vendor:** A dropdown menu currently set to 'All'.
- Cache Status:** A dropdown menu currently set to 'All'.
- CVE Identifier:** A text input field for entering a CVE ID.
- Include Disabled Patches:** An unchecked checkbox.
- Buttons:** 'Search' and 'Reset' buttons at the bottom.

To search for a patch:

- 1 Type all or part of the patch name in the **Patch Name** text box.
- 2 Select applicable filter options; the CVE identifier must be typed.
- 3 Click **Search**.

To filter from all existing patches:

- 1 Leave the **Patch Name** text box empty.
- 2 Select applicable filter options.
- 3 Click **Search**.

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

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

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

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

Status Filter	Result
Assigned	Search results include all the patches in the patch list that have been assigned to one or more devices.
Not Assigned	Search results include all the patches in the patch list that have not been assigned to any device.

The following table describes the result of selecting each filter option under **Impact** (Impact Filters in Search):

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

The following table describes the remaining filter options on the Search panel:


Filter	Result
Platform	Search results include all the patches relevant to the operating system in the patch list.
Vendor	Search results include all the patches relevant to the vendor in the patch list.
Cache Status	Search results include all the patches relevant to their cache status on the local server.
CVE Identifier	Search results include all the patches that have the common vulnerabilities and exposures ID that you type.
Relationships	Search results include patches for devices assigned to a patch policy, according to the option selected in the filter menu.
NOTE: This filter is only applicable to the Patches page on a selected patch policy.	For more information, see “Understanding the Relationships Filter” on page 93.

Create a Custom Patch


The Patch Wizard assists in selecting existing patch bundles and modifying patch details to create a custom patch. If you are not using an existing bundle, you will need to create a bundle of the patch contents before creating a customized patch. For more information, see [“Creating Bundles”](#) in the *ZENworks Software Distribution Reference*.

When you select the **New** menu item on the Patches page or Recently Released Patches panel, the Patch Wizard appears as shown below:

Patch Wizard

 **Step 1: Patch Wizard**
Select the bundle to be added into the Patch Management system.

Name



To create a customized patch:

- 1 Click the **New** menu item on the Patches page to open Step 1 of the Patch Wizard.
- 2 Click the **Browse** icon and navigate to the desired bundle in the Browse for Folder dialog box.
- 3 After selecting the desired bundle, click **OK** to confirm the bundle selection and then click **Next**.

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

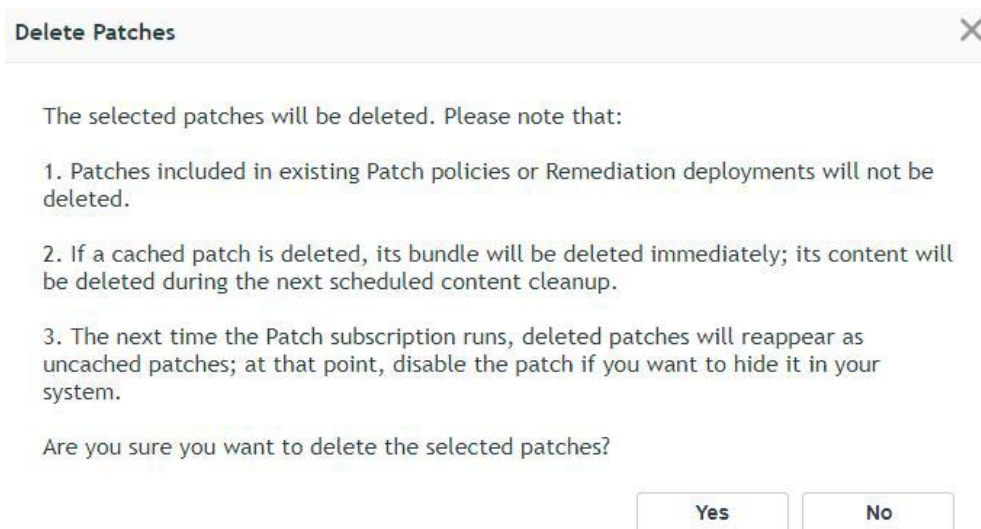
NOTE: After creating a new patch, you cannot immediately deploy it to the applicable devices. A subscription update is required to complete after the custom patch is created in ZENworks Control Center. After the subscription update, a new Discover Applicable Updates (DAU) bundle version is created with the custom patch information. Applicability of the new custom patches to the managed devices will be based on their bundle system requirements evaluation after the DAU bundle is successfully applied and patch scan is completed.

Delete a Patch

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

To delete a patch:

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



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

When you select Yes:

- ◆ The patches included in the existing Patch policies or Remediation deployments will not be deleted.
- ◆ If a cached patch is deleted, its bundle will be deleted immediately. However, its content will be deleted only during the next scheduled content cleanup.
- ◆ The next time the Patch subscription is run, the deleted patches will reappear as uncached patches. At that point, disable the patch if you want to hide it in your system. To cache the patches the user will have to either manually cache them or include them in a Patch policy.

IMPORTANT: If any of the patches you are deleting are deployed, those patches and their associated bundles are not deleted. In this case, when you click **Yes** to the Delete Patches message, another prompt will open, informing you of the dependencies to deployed bundles and their bundle identification numbers. These bundles can be from patch policies and/or patch remediations.

Any indicated dependencies must be resolved before the patches associated to them can be deleted. The services-messages log shows the patches that cannot be automatically or manually deleted because of dependencies. The location of the log is provided below:

- ♦ Linux: `/var/opt/novell/log/zenworks/services-messages.log`
 - ♦ Windows: `%ZENWORKS_HOME%\logs\services-messages.log`
-

Execute Action Menu Options

From the **Action** menu you can perform one of five actions to patches that are selected in the Patches page. Descriptions of these actions are provided below:

- ♦ **Deploy Remediation:** To use this option, select the check boxes for the patches you want to deploy and select **Deploy Remediation** from the **Action** menu options to open the Deploy Remediation Wizard. For more information, see [Deploying Patches Manually](#).
- ♦ **Enable:** After selecting one or more disabled patches, click this option to enable them. Disabled patches will only display in the Patches page if the **Include Disabled** check box is selected when a search is executed.
- ♦ **Disable:** After selecting one or more patches, click this option to disable them. The selected patch is removed from the list and will only be displayed when the **Include Disabled** check box is selected during a completed search.



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

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

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

To use this option:

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

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

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

To use this option, select the patches you want to export and click **Export** in the **Action** drop-down menu.

The result and follow-on steps after clicking **Export** will vary depending on your browser and browser settings. The file may download immediately to your local download folder, or the browser may present you with an option to open or to save the file.

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

Release Quarantined Patches

The patch quarantine feature is designed to prevent too many installation attempts on operating systems by bad patches or patches that require a reboot. A patch could fail multiple times because of environment issues on a device or because the patch needs to be fixed by the vendor.

If a patch becomes quarantined because of an environment issue that you can resolve, you can use the **Release Quarantined Patches** quick task on a device to remove a patch's quarantined state and then enable ZENworks to attempt to install it one more time, either through a patch policy or a remediation deployment. When the quick task executes it will release all quarantined patches on the device.

To run the Release Quarantined Patches quick task:

- 1 Select the device or server that requires the patch in the Devices list.
- 2 Choose **Release Quarantined Patches** in the Quick Tasks drop-down menu.
- 3 Define your desired options in the Quick Tasks Options dialog box, and click **Start**.

NOTE: Once an attempt is made to install a patch that is released from quarantine, it will return to quarantine if the installation fails.

The details of quarantined patches are available in the zmd-messages.log file. The quarantined patches will be logged as shown below:

[Patch]... "Patch is in quarantine <patch name>

Quarantine Folder

The quarantine folder stores files with a security verification failure. Any collection processor moves the file to quarantine if the following criteria are met:

- ♦ Security is enabled but receives a file without a header
- ♦ Verification of header fails.
- ♦ Mismatch in the GUID that is present in the header and the file contents.

Path to quarantine Folder is <collectionDir>/quarantine/<folderOfProcessor>

Example: For Windows MDM the path is <collectionDir>/quarantine/windowsmdm

The files in the quarantine folder are retained always in case any analysis needs to be done.

Path to quarantine folder are as follows:

- ♦ Windows: %ZENWORKS_HOME%\work\collection
- ♦ Linux: /var/opt/microfocus/zenworks/collection/

Patch Details Page

When you select a particular patch, all information related to the selected patch is displayed. The Patch details are displayed in three tabs, they include the following:

- ◆ [“Patch Information” on page 106](#)
- ◆ [“Relationships” on page 108](#)
- ◆ [“Devices” on page 109](#)

Patch Information

The Patch Information tab is displayed by default when you click the Patch name link in the Security Dashlets page, Patches page (patches applicable for the entire zone) or the Patches page (patches applicable for a particular device). This page displays the following information:

Patch Status

Indicates if the patch is enabled or disabled. If the patch is disabled, the reason for the patch being disabled, along with the date on which it was disabled, is displayed. The reasons for disabling a patch include:






- ◆ Superseded on: The patch was superseded by another patch.
- ◆ By user on: The patch was disabled by the user.
- ◆ Withdrawn on: The patch was withdrawn by the vendor.
- ◆ By vendor on: The patch was disabled by the vendor.
- ◆ By Legacy filter on: The patch was disabled based on the Legacy filter.
- ◆ By Age filter on: The patch was disabled based on the Age filter.
- ◆ By Obsolete filter on: The patch was disabled based on the Obsolete filter.
- ◆ By Culture filter on: The patch was disabled based on the Culture filter.
- ◆ By Windows Embedded filter on: The patch was disabled based on the Windows Embedded platform filter.
- ◆ By WEPOS filter on: The patch was disabled based on the WEPOS filter.
- ◆ No relevant languages: The patch was disabled as there were no relevant languages associated with it.

Impact

Indicates the impact level of the patch. The impact levels include Critical, Recommended, Software Installers and Informational. For more information, see [“Patch Impact” on page 89](#).

Download Status

Indicates the status of the patch download. Based on the Patch Subscription server configuration, the patches are downloaded from the patch repository to a particular server, The status of the download is indicated in this column. The values include:

- ◆  Downloaded: Indicates that the fingerprints and remediation patch bundles that are necessary to address the patch have been cached in the system. This icon represents the patches that are cached and ready for deployment.
- ◆  Not Downloaded: Indicates that only the fingerprint information for the patch has been brought down from the ZENworks Patch Subscription Network. This icon represents the patches that are not cached. You can manually download the patch by clicking the Download link that is displayed against the status.
- ◆  Download Pending: Indicates that a download process for the bundles associated with the selected patch is pending.
- ◆  In Progress: Indicates that a download process for the bundles associated with the selected patch has started. This process caches those bundles on your ZENworks Server.
- ◆  Failed: Indicates that an error has occurred while trying to download the bundle associated with the selected patch.

Vendor

Indicates the name of the vendor who has published the patch.

Vendor Product ID

Indicates the Product ID of the vendor who has published the patch.

Release Date

Indicates the date on which the patch was published for public access.

Size

Indicates the size of the patch file.

Description

Displays a description of the patch as provided by the Vendor. The description of the patch includes detailed information concerning the defect or issue resolved by this patch, deployment notes, and the prerequisites for deployment. To view the entire information, click the Show More link that is displayed against the Description.

URL

The URL to the Vendor's website which provides detailed information about the patch. As a best practice, it is recommended that you visit the URL to identify if there are any patches that are required to be applied before applying the selected patch. Especially for Microsoft patches.

Installation Details

Indicates if the system needs to be rebooted after the patch is installed and also indicates if the patch can be uninstalled when required.

CVEs Addressed by Patch

Lists the Common Vulnerabilities and Exposures (CVEs) that are addressed by the patch. The CVE details include the CVE ID and a summary of the CVE. Clicking the CVE ID will display the CVE details page. For information on the CVE page, see the [CVE Information Page](#) in the *CVE Reference*.

When you enable the Include CVEs inherited from superseded patches filter, CVEs, that are directly associated with the patch and CVEs that are inherited through the superseded patches are displayed. However, if you disable this filter, only CVEs that are directly associated with the patch are displayed. By default, this filter is disabled. When you click a CVE, the page is displayed.

NOTE: For Custom Patches, you can click the [Add/Remove](#) link to add or delete CVEs addressed by the patch.

Supersedence Details

This section of the page provides information about the patches that supersede the selected patch and information about the patches that have been superseded by this patch:

- ◆ **Superseded By:** Lists the patches that supersede the selected patch. Clicking a patch link will display the Patch Information page for the selected patch.
- ◆ **Supersedes:** Lists the patches that are superseded by the selected patch. Clicking a patch link will display the Patch Information page for the selected patch.

Relationships

This page provides information about the patch policies and the remediation bundles that have been created for the selected patch. This page includes the following details:

Patch Policies

This panel lists all the policies associated with the selected patch and provides the following information:

- ◆ **Policy Name:** The name of the patch policy. When you click the link, the Summary page of the Patch Policy is displayed.
- ◆ **Bundle Folder:** The Bundle folder that contains the policy's bundle. When you click this link the Bundles folder page is displayed.

- ◆ Enabled: Indicates if the patch policy is enabled or not.
- ◆ Version: Displays the published version of the patch policy.
- ◆ Has Sandbox: Indicates if the patch policy has a sandbox version or not.

Remediation Deployments

This panel lists all the remediation deployments associated with the selected patch and provides the following information:

- ◆ Deployment Name: The name of the remediation deployment associated with the patch. When you click this link the Deployment bundle's Summary page is displayed.
- ◆ Bundle Folder: The location of the bundle folder for the patch remediation deployment. When you click the link, the bundle folder that contains the deployment bundle is displayed.
- ◆ Enabled: Indicates if the remediation deployment is enabled or not.
- ◆ Version: Displays the published version of the remediation deployment bundle.
- ◆ Has Sandbox: Indicates if the remediation deployment bundle has a sandbox version or not.

Patch Bundles

This panel lists all the patch bundles associated with the selected patch and provides the following information:

- ◆ Bundle Name: The name of the patch bundle that is associated with the patch.
- ◆ Bundle Folder: The location of the bundle folder that includes the patch. When you click the link, the bundle folder is displayed.
- ◆ Enabled: Indicates if the patch bundle is enabled or not.
- ◆ Version: Displays the published version of the patch bundle.
- ◆ Has Sandbox: Indicates if the patch bundle has a sandbox version or not.

Devices

This tab provides information about the various devices that are impacted by the selected Patch. This tab displays the following information:

- ◆ Name: The name of the device that is impacted by the selected patch. When you click this link, the device summary page is displayed.
- ◆ Operating System: Displays the operating system of the selected device.
- ◆ Last Patch Scan: Displays the date on which the last patch scan was performed on the device.
- ◆ Patched: Indicates if the patch has been applied on the device or not.
- ◆ Assignments: Lists the number of assignments for the patch that have been made to the device. When you click the count, the details of the assignments are displayed.
- ◆ Installed On: Displays the date on which the patch was installed on the device.
- ◆ Installed By: Indicates if the patch was installed on the device by ZENworks or it was installed manually (through other sources).

Patch Requirements

This page enables you to edit the Applicability Requirements and the Patched Requirements that are defined for a Custom Patch while creating the patch using the Custom Patch wizard. Administrators need to have Patch Configure, Bundle View and Bundle Author rights to successfully view and change the Applicability Requirements and the Patched Requirements. This page includes the following panes:

- ♦ [“Applicability Requirements” on page 110](#)
- ♦ [“Patched Requirements” on page 110](#)

Applicability Requirements

This pane provides information about the filters that are defined as Applicability Requirements for a Custom Patch. If no requirements were specified during the creation of the custom patch, you can define them using this page. The patch bundle is considered applicable to devices based on the selected filters. You can add, edit or delete filters in this section. When you make any edits to the Applicability Requirements, the bundle version is incremented.

Patched Requirements

This pane provides information about the filters that were defined as Patched Requirements for a Custom Patch. Devices are considered patched based on the selected filters. You can add, edit or delete filters in this section.

A Troubleshooting

This troubleshooting appendix is intended to help you resolve issues when managing Patch Management. It contains error codes and issues you might encounter, as well as many of the actions you can take to resolve these issues.

Many issues can be avoided by following the guidance in the [Patch Policy - Best Practices](#) section in this reference. If you have not already evaluated your Patch Policy configuration with this guidance, we recommend that you do so.

For information about system variables that you can use in Patch Management to enable or disable patch related features, see [Appendix B, "System Variables," on page 129](#).

In many cases patch issues that occur are not related to the Patch Management software or configuration, but can be a problem with a patch itself or an environment issue. Before referring to the content in this appendix, you may want to review the actions below to see if they can help resolve your issue:

- ◆ Read event logs to see if there is any indication of native hardware, software, or environment issues that need to be resolved.

The *WSH* types will show the actions taken by ZPM to apply the patch. *Msixexec* or other errors may also be seen.

- ◆ Determine if the target device meets patch requirements, such as operating system, Bit-level, and so forth.
- ◆ Execute a search for error codes to determine if the issue is vendor or Patch Management related.
- ◆ Apply the patch using the vendor's patching mechanism.

For example, if it is a Microsoft Windows update, use Windows Update to apply the patch. If it fails repeatedly AND fails on multiple machines, the patch is probably bad and needs to be fixed by the vendor. You should contact the vendor directly to report the issue.

Patch Management Issues

This section contains detailed explanations of the error messages you might receive or problems you might encounter when using ZENworks Patch Management. You can also reference these online references:

- ◆ [Knowledgebase](#)
- ◆ [Technical Support Handbook](#)
- ◆ [Cool Solutions](#)

NOTE: If you cannot resolve an issue related to Patch Management using this troubleshooting section or the online resources above, please contact [Technical Support](#).

Review the issues below to see if any them are applicable to your patch environment and take the prescribed action where needed.

- ♦ “Patches are unavailable because of connectivity or firewall issues” on page 112
- ♦ “No patches are shown in the Patches page” on page 116
- ♦ “Patch remediation bundles are not replicating to Primary servers” on page 116
- ♦ “Patches do not seem to be deployed on the target device” on page 116
- ♦ “The Cancel button disappears in the Reboot Required dialog box” on page 116
- ♦ “Superseded patches are shown as NOT APPLICABLE” on page 116
- ♦ “Patch deployment might not start when scheduled” on page 117
- ♦ ““Failed but set to continue” error shows in progress bar” on page 117
- ♦ “Patch Policy assignment: Bundle stays in ‘Pending’ state forever” on page 117
- ♦ “Patch Policy assignment: Error Message should be displayed for (failed) assignment to older agents” on page 118
- ♦ “Linux - Custom Patches: Bundles fail to launch” on page 118
- ♦ “Airgap Server: User receives trial license email after adding the license info to system variables” on page 118
- ♦ “Blank PowerShell window is displayed after deploying patch policies during device shutdown” on page 118
- ♦ “Unable to uninstall patches” on page 119
- ♦ “The patch policy might not rebuild and fails to create a sandbox or published version” on page 119

Patches are unavailable because of connectivity or firewall issues

Source: ZENworks; Patch Management.

Explanation: Ensure that your server environment can access patch providers and hosts and that applicable clients are properly configured for Office 365 updates.

The Novell and Partner URLs for Lumension and Akamai, listed below, must be allowed access in the Firewall policies to enable the Patch Subscription process to download patch content for other vendors such as Microsoft and Adobe.

Action: Follow the steps below:

- 1 Open outbound access to the following websites from the ZENworks Patch Management Server:
 - ♦ Novell
 - ♦ <https://nu.novell.com>
 - ♦ download.novell.com
 - ♦ Lumension
 - ♦ novell.patchlink.com

- ◆ cache.patchlinksecure.net
- ◆ novell.cdn.heatsoftware.com
- ◆ Windows Content
 - ◆ go.microsoft.com
 - ◆ www.download.windowsupdate.com
 - ◆ go.microsoft.com -- CAB file used for Native Scan.
 - ◆ download.windowsupdate.com
 - ◆ download.microsoft.com
 - ◆ wsus.ds.download.windowsupdate.com
- ◆ Adobe Content
 - ◆ ardownload.adobe.com
 - ◆ ardownload2.adobe.com
 - ◆ armdl.adobe.com
 - ◆ download.adobe.com
 - ◆ swupdl.adobe.com
 - ◆ www.adobe.com
- ◆ Oracle Linux
 - ◆ linux-update.oracle.com
- ◆ HP-UX
 - ◆ itrc.hp.com
 - ◆ [ftp.itrc.hp.com](ftp://itrc.hp.com)
- ◆ Red Hat
 - ◆ www.redhat.com
 - ◆ rhn.redhat.com
- ◆ Oracle Solaris
 - ◆ <https://getupdates.oracle.com>
- ◆ SUSE 9
 - ◆ <https://you.novell.com>
- ◆ SUSE 12
 - ◆ <https://scc.suse.com>
- ◆ Apple
 - ◆ <http://updates-http.cdn-apple.com>
 - ◆ secure-appldnld.apple.com
- ◆ National Vulnerability Database
 - ◆ <https://nvd.nist.gov>
- ◆ Dropbox
 - ◆ clientupdates.dropboxstatic.com

- ◆ Lumension
 - ◆ `cache.lumension.com`
- ◆ Skype
 - ◆ `download.skype.com`
- ◆ Mozilla Firefox
 - ◆ `http://ftp.mozilla.org`
- ◆ SourceForge
 - ◆ `http://downloads.sourceforge.net`
- ◆ UVNC
 - ◆ `http://support1.uvnc.com`
- ◆ VideoLAN
 - ◆ `http://download.videolan.org`

NOTE: While adding hosts on the ZENworks server, either use the `nslookup` or `ping` command to get the IP address or secondary DNS names for each URL.

Patch content is downloaded using the SSL-based (TCP port 80) connection. The network should not block the download of binaries or exe files from these remote URLs as they are provided by partners.

- 2 If you have ZENworks Agent clients in the zone that use Microsoft Office 365, configure those clients to receive Office 365 updates natively.
For information about how Patch Management works with Office 365, see the Cool Solutions article [Patching Microsoft Office 365](#).
- 3 Test your connectivity to the new hosting provider from your ZENworks Primary Server that the Patch Management feature is currently running on:
 - ◆ Ping test:
Log in to the server console, and launch a command prompt or shell window:

```
ping novell.cdn.heatsoftware.com
```


If your server is able to connect to the cloud hosting network without a problem, you see a response similar to the one shown below:

```

PING ddnkgb0d00fm8.cloudfront.net (13.35.90.100)
56(84) bytes of data.
64 bytes from server-13-35-90-
100.lax3.r.cloudfront.net (13.35.90.100): icmp_seq=1
ttl=236 time=30.6 ms
64 bytes from server-13-35-90-
100.lax3.r.cloudfront.net (13.35.90.100): icmp_seq=2
ttl=236 time=30.5 ms
64 bytes from server-13-35-90-
100.lax3.r.cloudfront.net (13.35.90.100): icmp_seq=3
ttl=236 time=40.8 ms
64 bytes from server-13-35-90-
100.lax3.r.cloudfront.net (13.35.90.100): icmp_seq=4
ttl=236 time=30.1 ms
64 bytes from server-13-35-90-
100.lax3.r.cloudfront.net (13.35.90.100): icmp_seq=5
ttl=236 time=30.5 ms

```

The ping command shows you the address of the nearest server to your current location.

NOTE: The Ping test is a simple way to establish that a server has a route available to reach the server, it is not used by Patch Management in normal operations.

Ping (ICMP) may be blocked by your corporate firewall, or the server may need to pass through a proxy to reach the hosting provider: In these circumstances the Ping test will fail, so other tests will be needed.

◆ **Browser test:**

Using a Web browser, type in the following URL:

```
http://novell.cdn.heatsoftware.com/novell/pulsar.xml
```

The browser should display formatted output from the website, as shown in the figure below:

```

- <sub>
  - <os name="Windows">
    - <arch name="x86">
      - <lang name="English">
        <lst> windows/x86/en/applications.lst </lst>
        <lst> windows/x86/en/software.lst </lst>
        <lst ver="XP" spack="3"> windows/x86/en/xpsp3.lst </lst>
        <lst ver="XP" spack="2" legacy="Y"> windows/x86/en/xpsp2.lst </lst>
        <lst ver="XP" spack="1" legacy="Y"> windows/x86/en/xpsp1.lst </lst>
        <lst ver="2000" spack="4"> windows/x86/en/2ksp4.lst </lst>
        <lst ver="2000" spack="3" legacy="Y"> windows/x86/en/2ksp3.lst </lst>
        <lst ver="2003" spack="2"> windows/x86/en/2k3sp2.lst </lst>
        <lst ver="2003" spack="1" legacy="Y"> windows/x86/en/2k3sp1.lst </lst>
        <lst ver="2003" spack="0" legacy="Y"> windows/x86/en/2k3sp0.lst </lst>
        <lst ver="VISTA" spack="0" legacy="Y"> windows/x86/en/vistasp0.lst </lst>
        <lst ver="VISTA" spack="1"> windows/x86/en/vistasp1.lst </lst>
      </lang>
    </arch>
  </os>
</sub>

```

If your browser cannot access the XML file, you experience a browser timeout and receive some kind of error message. If the ping test succeeds and the browser test fails, this indicates that the firewall administrator has limited access to the cloud network or the HTTP (TCP port 80) is blocked.

NOTE: If the ZPM server needs to use a proxy to get to the outside world, ensure that the browser is configured for the same proxy or the test is not valid.

No patches are shown in the Patches page

Source: ZENworks; Patch Management.

Possible Cause: The server has just been installed.

Action: You need to start the patch subscription download, and then wait twenty minutes or more for patches to be downloaded automatically from novell.patchlink.com.

Patch remediation bundles are not replicating to Primary servers

Source: ZENworks; Patch Management.

Possible Cause: The patch remediation bundle(s) was modified.

Action: Patch remediation bundles from patch policies or deployment remediations should not be modified.

Patches do not seem to be deployed on the target device

Source: ZENworks; Patch Management.

Possible Cause: The ZENworks administrator has not deployed the patches into the applicable devices in the ZENworks server, or the patches have been deployed in the server but the device refresh schedule has not been triggered in the ZENworks Agent.

Actions: Check to see if the **Device Refresh Schedule** option is set as **Manual Refresh** or **Timed Refresh** on the Configuration page, and wait for the specified interval.

The Cancel button disappears in the Reboot Required dialog box

Source: ZENworks; Patch Management.

Explanation: When two or more patches are deployed, if the **Allow User to Cancel** option is set as No on the Pre Install Notification Options page and the Notification and Reboot Options page of the server, the **Cancel** button disappears in the Reboot Required dialog box for all patches of the agent.

Action: None necessary.

Superseded patches are shown as NOT APPLICABLE

Source: ZENworks; Patch Management.

Explanation: In earlier releases of Patch Management, a patch showed its status as PATCHED or NOT PATCHED, regardless of whether the patch was new or outdated. This often caused many more patches to show as NOT PATCHED than were actually necessary for deployment to a given target device. This issue has been addressed in many of the new advanced content patches provided with ZENworks 2017:

- ♦ When a patch is superseded, it is automatically disabled.
- ♦ If the patch is re-enabled and detected, in most cases the patch shows as NOT APPLICABLE because it has been replaced by a superseded patch. However, if the device has not installed the superseding patch then the re-enabled patch will show as properly scanned (either patched, not patched or not applicable depending on the device patch state of the original patch).

Although this is inconsistent with the behavior of earlier versions of Patch Management, this change is an improvement because only the patches that currently need to be installed are reported or analyzed on each device.

Action: None necessary.

Patch deployment might not start when scheduled

Source: ZENworks; Patch Management.

Possible Cause: If the deployment schedule type includes both the **Recurring** and **Process Immediately If the Device Is Unable to Execute** options, when the device becomes active, the deployment of the patch does not start on the first of its scheduled recurring dates. However, the patch is deployed when the next recurring date occurs.

Action: Instead of selecting a recurring schedule, select a date-specific schedule so that the patch is applied when the device becomes active.

“Failed but set to continue” error shows in progress bar

Source: ZENworks; Patch Management

Explanation: After an 11.2.4 server and agents are set up and some deployments are made, and then following an upgrade from 11.2.4 to 11.3, this error will be shown in the progress bar. The patches ARE installed, but the system can not ‘see’ this. patchReportResult does not action on older agents.

Possible Cause: Mismatch, new actions from the newer architecture are not recognized in older versions. Functionality is NOT affected.

Action: Disable the action in both the deployment and remediation bundles, and immediately refresh the agents to avoid the error.

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

Source: ZENworks; Patch Management.

Possible Cause: There are issues between bundles and older agents

Action: Bundle Assignment having State as "Not Effective" has a reason associated like "System requirement failed", "Unsociable Type", "Blocked", "Wrong Platform" etc. Similarly we have to define a new State like "Not Effective because Older Agent" and then update the existing logic to set that State while filtering the assignments.

Adding / defining new State for Bundle Assignment has more impact as other components on server might be using the value of Effective State for other computations.

Patch Policy assignment: Error Message should be displayed for (failed) assignment to older agents

Source: ZENworks; Patch Management.

Possible Cause: "Patch bundles assigned through patch policies do not flow down to older version agents than 11.3" message should be displayed on assignment of patch to older version agents.

Action: Assignment can be done from the device side as well as from the object (patch policy/bundle) side. So, various checks are required here i.e. whether the device is an older agent and whether the object type is patch policy. Also, since multiple objects can be assigned to multiple devices (including folders and groups), the checks need to be iterative which further increases the complexity.

Linux - Custom Patches: Bundles fail to launch

Source: ZENworks; Patch Management.

Possible Cause: RPM Application Bundle and Custom RPM Bundle fails on both SUSE as well as Red Hat when it is assigned to the device with Launch Schedule On Device Refresh.

Action: Work around for the custom patch: Add 1-2 minutes of delay execution after refresh for "Remediation Schedule" to resolve it.

Airgap Server: User receives trial license email after adding the license info to system variables

Source: ZENworks; Patch Management.

Explanation: After setting up an Airgap server, you receive trial license emails from the server although you've added your license to the Airgap server system variables.

Possible Cause: The Airgap server requires the Patch Management license file from the connected server.

Action: Contact Micro Focus Support.

Blank PowerShell window is displayed after deploying patch policies during device shutdown

Source: ZENworks; Patch Management.

Explanation: After assigning the Patch Policies on Shutdown schedule to a Windows 1903 device, during the device shutdown, a blank PowerShell window is displayed. Though the patches have installed correctly on the device, the Powershell window does not display any messages.

Action: None. Ignore the blank PowerShell window.

Unable to uninstall patches

Source: ZENworks; Patch Management.

Explanation: Patches that support uninstall cannot be removed from a device by clicking the Patched count within the Patches page in ZCC.

Action: In the Devices page of the patch object, select the device on which you want to uninstall the patch and then click **Deploy Remediation**. In the wizard, select the **Advanced** option and configure the deployment with the uninstall action. For more information on the uninstall action see [“Advanced Remediation Options” on page 73](#).

The patch policy might not rebuild and fails to create a sandbox or published version

Source: ZENworks 2020

Explanation: While creating a patch policy, the policy might not rebuild. Hence, it fails to create a sandbox or published version, and in the services-messages.log, the following message is displayed:

```
ERROR: duplicate key value violates unique constraint  
"zpatchpolicysignaturemap_pkey"
```

Possible Cause: This error might be displayed due to the newly added sequences in the database.

Action: Perform the following steps to correct the sequences in the database:

1. Download the latest version of the Database Migration tool.
2. Unzip the Database Migration tool, and then copy the db-migration-utility.jar file to the following location:
 - ♦ **On Linux:** /opt/novell/zenworks/java/lib/
 - ♦ **On Windows:** %ZENworks_HOME%\lib\java\common
3. After copying the file, run the following configure action:
novell-zenworks-configure -c FixSequencesConfigureAction

Configuration Issues

- ♦ [“Deploying patches with Auto Reboot causes the device to shut down” on page 120](#)

Deploying patches with Auto Reboot causes the device to shut down

Source: ZENworks 2017; Patch Management.

Possible Cause: Trying to deploy patches with auto-reboot might shut down the machine instead of rebooting. It might also fail to report patch results to the ZENworks Server.

Action: Perform reboots with a Quick Task rather than using the Auto Reboot option.

Error Codes

- ♦ [“ERROR CODE: ERROR = 40” on page 121](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_MORE_THAN_MAXAPPLICABLE_SIGS = 45” on page 121](#)
- ♦ [“ERROR CODE: PPX_ERROR_ARCHIVE_EXTRACT = 2” on page 122](#)
- ♦ [“ERROR CODE: PPX_ERROR_PACKAGE_ARCHIVE_INITIALIZE = 8” on page 122](#)
- ♦ [“ERROR CODE: PPX_ERROR_EXTRACT_FILE = 20” on page 122](#)
- ♦ [“ERROR CODE: PPX_ERROR_PACKAGE_REIMPORT = 40” on page 122](#)
- ♦ [“ERROR CODE: PPX_ERROR_EXPIRED_LICENSE_KEY = 27” on page 122](#)
- ♦ [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1” on page 122](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 3” on page 122](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 4” on page 122](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_MANY_APPLICABLE_SIGNATURES = 5” on page 123](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 6” on page 123](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 7” on page 123](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 9” on page 123](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 10” on page 123](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 11” on page 123](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 12” on page 123](#)
- ♦ [“ERROR CODE: PPX_ERROR_SIGNATURE_PREREQ_CACHE_EXHAUSTED = 13” on page 123](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 14” on page 123](#)
- ♦ [“ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 15” on page 124](#)
- ♦ [“ERROR CODE: PPX_ERROR_FINGERPRINT_EXPRESSION_SYNTAX = 16” on page 124](#)
- ♦ [“ERROR CODE: PPX_ERROR_FINGERPRINT_FILEROOT_UNSUPPORTED = 17” on page 124](#)
- ♦ [“ERROR CODE: PPX_ERROR_FINGERPRINT_TYPE_UNSUPPORTED = 18” on page 124](#)
- ♦ [“ERROR CODE: PPX_ERROR_SCRIPT_BAD_FILEHANDLE = 19” on page 124](#)
- ♦ [“ERROR CODE: PPX_ERROR_WMI_FINGERPRINT_UNSUPPORTED = 22” on page 124](#)
- ♦ [“ERROR CODE: PPX_ERROR_JAVASCRIPT_UNSUPPORTED = 23” on page 124](#)

- ◆ “ERROR CODE: PPX_ERROR_MISSING_PREREQ_SIGNATURE = 25” on page 124
- ◆ “ERROR CODE: PPX_ERROR_INVALID_PREREQ_LANGUAGE = 26” on page 124
- ◆ “ERROR CODE: PPX_ERROR_INVALID_ROOT_HKEY = 21” on page 124
- ◆ “ERROR CODE: PPX_ERROR_FINGERPRINT_INVALID_SYSINFO = 31” on page 125
- ◆ “ERROR CODE: PPX_ERROR_FINGERPRINT_EXPRESSION_MISSING_VARIABLE = 32” on page 125
- ◆ “ERROR CODE: PPX_ERROR_FINGERPRINT_FILESCAN_UNSUPPORTED = 34” on page 125
- ◆ “ERROR CODE: PPX_ERROR_FINGERPRINT_WMI_ERROR = 35” on page 125
- ◆ “ERROR CODE: PPX_ERROR_RELEVANCE_SCRIPT_SYNTAX = 36” on page 125
- ◆ “ERROR CODE: PPX_ERROR_ENTITLED_FILE_INVALID = 41” on page 125
- ◆ “ERROR CODE: PPX_ERROR_ENTITLED_FILE_MISSING = 28” on page 125
- ◆ “ERROR CODE: PPX_ERROR_ENTITLED_FILE_BAD_CHECKSUM = 29” on page 125
- ◆ “ERROR CODE: PPX_ERROR_ENTITLED_FILE_WRONG_SIZE = 30” on page 126
- ◆ “ERROR CODE: PPX_ERROR_OUT_OF_MEMORY = 24” on page 126
- ◆ “ERROR CODE: PPX_ERROR_PACKAGE_MKDIR_FAILURE = 33” on page 126
- ◆ “ERROR CODE: PPX_ERROR_UNKNOWN” on page 126
- ◆ “ERROR CODE: 41” on page 126
- ◆ “ERROR CODE: 142” on page 126
- ◆ “ERROR CODE: 143” on page 127
- ◆ “ERROR CODE: 144” on page 127
- ◆ “ERROR CODE: 145” on page 127
- ◆ “ERROR MESSAGE: “There is an issue with checksum metadata at CDN”” on page 127
- ◆ “ERROR : zman prb "<baseline_patch_name>" - java.lang.NullPointerException when trying to get the DefaultHibernateSessionManager” on page 127
- ◆ “OTHER ERROR CODES” on page 128

ERROR CODE: ERROR = 40

Source: ZENworks 2017; Patch Management.

Possible Cause: The patch file cached to the ZCM Server is corrupt.

Action: Try re-caching the patch to the ZCM Server.

ERROR CODE: PPX_ERROR_PATCH_MORE_THAN_MAXAPPLICABLE SIGS = 45

Source: ZENworks 2017; Patch Management.

Possible Cause: The patch file contains more than the maximum applicable signatures.

Action: Notify Micro Focus Support of the error. We will fix the problem with the patch and notify you when it is fixed.

ERROR CODE: PPX_ERROR_ARCHIVE_EXTRACT = 2

Source: ZENworks 2017; Patch Management.

Possible Cause: Extraction of the .cab file or its contents fails.

Action: Follow the steps below:

- 1 Make sure that CABARC runs on the end point where the error message appears.
- 2 Check the available disk space on the end point.
- 3 Re-cache the patch to the ZCM Server.
- 4 If the issue persists, contact Micro Focus Support.

ERROR CODE: PPX_ERROR_PACKAGE_ARCHIVE_INITIALIZE = 8

Source: See [“ERROR CODE: PPX_ERROR_ARCHIVE_EXTRACT = 2” on page 122.](#)

ERROR CODE: PPX_ERROR_EXTRACT_FILE = 20

Source: See [“ERROR CODE: PPX_ERROR_ARCHIVE_EXTRACT = 2” on page 122.](#)

ERROR CODE: PPX_ERROR_PACKAGE_REIMPORT = 40

Source: See [“ERROR CODE: PPX_ERROR_ARCHIVE_EXTRACT = 2” on page 122.](#)

ERROR CODE: PPX_ERROR_EXPIRED_LICENSE_KEY = 27

Source: ZENworks 2017; Patch Management.

Possible Cause: The .plk license file you are using is outdated or has expired. This error code might also appear if the license file is erased or did not get decrypted properly.

Action: Ensure that you have the latest System Update installed.

ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1

Source: ZENworks 2017; Patch Management.

Possible Cause: You might encounter any of these error codes if a patch has bad metadata.

Action: Contact Technical Support.

ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 3

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1” on page 122.](#)

ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 4

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1” on page 122.](#)

ERROR CODE: PPX_ERROR_PATCH_MANY_APPLICABLE_SIGNATURES = 5

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 122.

ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 6

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 122.

ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 7

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 122.

ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 9

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 122.

ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 10

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 122.

ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 11

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 122.

ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 12

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 122.

ERROR CODE: PPX_ERROR_SIGNATURE_PREREQ_CACHE_EXHAUSTED = 13

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 122.

ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 14

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 122.

ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 15

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 122.

ERROR CODE: PPX_ERROR_FINGERPRINT_EXPRESSION_SYNTAX = 16

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 122.

ERROR CODE: PPX_ERROR_FINGERPRINT_FILEROOT_UNSUPPORTED = 17

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 122.

ERROR CODE: PPX_ERROR_FINGERPRINT_TYPE_UNSUPPORTED = 18

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 122.

ERROR CODE: PPX_ERROR_SCRIPT_BAD_FILEHANDLE = 19

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 122.

ERROR CODE: PPX_ERROR_WMI_FINGERPRINT_UNSUPPORTED = 22

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 122.

ERROR CODE: PPX_ERROR_JAVASCRIPT_UNSUPPORTED = 23

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 122.

ERROR CODE: PPX_ERROR_MISSING_PREREQ_SIGNATURE = 25

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 122.

ERROR CODE: PPX_ERROR_INVALID_PREREQ_LANGUAGE = 26

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 122.

ERROR CODE: PPX_ERROR_INVALID_ROOT_HKEY = 21

Source: See [“ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1”](#) on page 122.

ERROR CODE: PPX_ERROR_FINGERPRINT_INVALID_SYSINFO = 31

Source: See “[ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1](#)” on [page 122](#).

ERROR CODE:

PPX_ERROR_FINGERPRINT_EXPRESSION_MISSING_VARIABLE = 32

Source: See “[ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1](#)” on [page 122](#).

ERROR CODE: PPX_ERROR_FINGERPRINT_FILESCAN_UNSUPPORTED = 34

Source: See “[ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1](#)” on [page 122](#).

ERROR CODE: PPX_ERROR_FINGERPRINT_WMI_ERROR = 35

Source: See “[ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1](#)” on [page 122](#).

ERROR CODE: PPX_ERROR_RELEVANCE_SCRIPT_SYNTAX = 36

Source: See “[ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1](#)” on [page 122](#).

ERROR CODE: PPX_ERROR_ENTITLED_FILE_INVALID = 41

Source: ZENworks 2017; Patch Management.

Possible Cause: These error codes indicate possible problems in bundle distribution. The ZCM server might not be able to access a third-party website where bundles are located.

Action: Follow the steps below:

- 1 Check your Internet connection and firewall settings.
- 2 Check that the ZCM Server can access a third-party website such as the [Microsoft Download Center \(http://www.microsoft.com/downloads/en/default.aspx\)](http://www.microsoft.com/downloads/en/default.aspx).
- 3 Download patches from the third-party website.
- 4 Re-cache the downloaded patches.

ERROR CODE: PPX_ERROR_ENTITLED_FILE_MISSING = 28

Source: See “[ERROR CODE: PPX_ERROR_ENTITLED_FILE_INVALID = 41](#)” on [page 125](#).

ERROR CODE: PPX_ERROR_ENTITLED_FILE_BAD_CHECKSUM = 29

Source: See “[ERROR CODE: PPX_ERROR_ENTITLED_FILE_INVALID = 41](#)” on [page 125](#).

ERROR CODE: PPX_ERROR_ENTITLED_FILE_WRONG_SIZE = 30

Source: See [“ERROR CODE: PPX_ERROR_ENTITLED_FILE_INVALID = 41”](#) on page 125.

ERROR CODE: PPX_ERROR_OUT_OF_MEMORY = 24

Source: ZENworks 2017; Patch Management.

Possible Cause: This error arises when there is a deficiency in system resources, such as insufficient disk space, low available memory, and so on.

Action: Check the available disk space and memory, then verify that it is sufficient to meet the ZCM Server and Agent requirements.

ERROR CODE: PPX_ERROR_PACKAGE_MKDIR_FAILURE = 33

Source: ZENworks 2017; Patch Management.

Possible Cause: The user has insufficient permissions to carry out the specified action.

Action: Check whether you have appropriate system rights or permissions.

ERROR CODE: PPX_ERROR_UNKNOWN

Source: ZENworks 2017; Patch Management.

Possible Cause: This error is a general exception. If logging is enabled, the error is recorded in the `.log` file.

Action: Follow the steps below:

- 1 Open a support ticket with Lumension.
- 2 Contact Micro Focus Support.

ERROR CODE: 41

Source: ZENworks 2017; Patch Management.

Possible Cause: This error code implies that ZENworks Patch Management was unable to perform patch remediation. This error occurs when deployment of a different version of the same patch is in progress.

Action: Wait for the previous deployment to complete, then deploy the patch again.

ERROR CODE: 142

Source: ZENworks 2017; Patch Management.

Possible Cause: The selected patch requires certain prerequisites before the patch can be deployed. This error can also occur when package files for a patch are unavailable.

Action: Contact Micro Focus Support and report the patch name. This is most likely a bad patch.

ERROR CODE: 143

Source: ZENworks 2017; Patch Management.

Possible Cause: This error is a general exception. If logging is enabled, the error is recorded in the `.log` file.

Action: Follow the steps below:

- 1 Redeploy the patch.
- 2 If the error persists, file an incident report with Micro Focus.

ERROR CODE: 144

Source: ZENworks 2017; Patch Management.

Possible Cause: This error code appears if there are errors in the patch deployment script. If logging is enabled, the error is recorded in the `.log` file.

Action: File an incident report with Micro Focus.

ERROR CODE: 145

Source: ZENworks 2017; Patch Management.

Possible Cause: The script failed to open the registry. This issue is most probably associated with timing.

Action: Deploy the patch again.

ERROR MESSAGE: "There is an issue with checksum metadata at CDN"

Source: ZENworks 2017; Patch Management.

Possible Cause: There is a problem with not having access to the VEGA content path.

Action: Check the following URL's and see if you can download them:

<http://cache.patchlinksecure.net/PatchComponents/OSPXSet.xml>

<http://cache.lumension.com/patchcomponents/1f12ad89-5711-41ce-ae84-9df6487153f3/win8x64.ospx>

ERROR : zman prb "<baseline_patch_name>" - java.lang.NullPointerException when trying to get the DefaultHibernateSessionManager

Source: ZENworks 2017; Patch Management.

Possible Cause: zman prb "<baseline_patch_name>" is throwing a `java.lang.NullPointerException`. This is being caused by code returning a null `DefaultHibernateSessionManager`.

The following error will be seen:.

Code:

```
com.novell.zenworks.zman.commands.PatchHandler.patchRemoveBaseline()Line: 123 DirectServiceStoreImpl dssi = (DirectServiceStoreImpl) store;Line: 124 DefaultHibernateSessionManager dsm =(DefaultHibernateSessionManager) ((HibernateAbstractSession)dssi.getSession()).getSessionManager();Line: 125 session = dsm.openSession();Stack Trace:java.lang.NullPointerException (java.lang.StackTraceElement[])[com.novell.zenworks.zman.commands.PatchHandler.patchRemoveBaseline(PatchHandler.java:125),sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method),sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:57),sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43),java.lang.reflect.Method.invoke(Method.java:606),com.novell.zenworks.zman.CommandRunner.execute(CommandRunner.java:94),com.novell.zenworks.zman.ZMan.executeRunner(ZMan.java:328),com.novell.zenworks.zman.ZMan.runCommand(ZMan.java:531),com.novell.zenworks.zman.ZMan.main(ZMan.java:465),com.novell.zenworks.zman.ZManExecutor.execute(ZManExecutor.java:101),com.novell.zenworks.zman.ZManExecutor.main(ZManExecutor.java:41),sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method),sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:57),sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43),java.lang.reflect.Method.invoke(Method.java:606),com.novell.zenworks.zman.ZManLoader.loadZMan(ZManLoader.java:59),com.novell.zenworks.zman.ZManLoader.main(ZManLoader.java:143)]
```

Action: Increase memory size as follows:

```
modify "JVM_STARTUP_OPTIONS=-Xms64m -Xmx128m" to "JVM_STARTUP_OPTIONS=-Xms64m -Xmx1024m" in the zman-config.properties file. The error disappears and indicates the baseline clears successfully.
```

Then,

1. Assign a baseline in a group.
2. Refresh the agent to receive the baseline.
3. Remove the baseline on the server.
4. Refresh agent again and notice the baseline should remain.
5. Modify memory in the file "zman-config.properties file."
6. Refresh the agent again.

OTHER ERROR CODES

Source: ZENworks 2017; Patch Management.

Action: Contact Micro Focus Support.

B System Variables

Within ZENworks Control Center, you can enter system variables to enable or disable certain Patch Management behaviors.

Patch Management System Variables

See below for a list of variables and how to enter them. You can enter these variables by selecting [Configuration > Configuration](#) page > [Device Management > System Variables](#).

NOTE: All system variables are case-sensitive.

AIRGAP_COLLECTOR_ALWAYS_DOWNLOAD

Set to `true` to force to download all bundles and expected patches on the Airgap connection server.

(For troubleshooting only)

CONNECTION_TIMEOUT

Enables the adjustment of URL connection timeout duration when downloading patch files (signatures, packages & payloads). Using this system variable can be beneficial when operating in a slow or intermittent network environment.

Default Value: 180 seconds

Valid Range: 0 (infinite) to 3600 seconds (1 hour)

PATCH_AIRGAP_COLLECTOR

Set to `true` to enable Airgap function on the connection server.

PATCH_AIRGAP_LICENSE

Set valid license for the Airgap disconnection server.

PATCH_AIRGAP_SERVER

Set to `true` to enable Airgap function on the disconnection server.

PATCH_ALWAYS_SHOW_REBOOT_PROMPT

Set to `true` to display the patch reboot prompt to users when the Patch Policy Reboot Behavior option for **Suppress reboot** is set to **Yes**.

No prompt is displayed on **Suppress reboot** if this variable is set to `false`, which is the default behavior.

PATCH_CONVERT_BASELINES_TO_POLICIES

Set to `false` to skip the process of converting mandatory baselines to patch policies.

PATCH_DAU_SYSTEM_CONTENT

If that is set to `true` then DAU bundles are created with content type of Patch System.

NOTE: If this is not set prior to existing DAU bundles being created, it is necessary to delete the existing DAU bundles and then re-download the subscription update.

Default Value: `false`

Valid Values: `true`, `false`

PATCH_DELAY_REBOOT_ANALYZE

Delays the initial patch scan, which is run during device startup, by the specified number of minutes, when a reboot-required patch is installed and the system is rebooted

Valid Range: From 1 to 60 minutes. If the specified value is above 60, then the Analyze process will be delayed by 60 minutes.

Value: Integer value in minutes (from 1 to 60).

PATCH_DELAY_SUPERSEDED_DISABLE

Delays the disabling of superseded patches by the specified number of days. The value configured using this system variable will override the 30, 60 or 90 day value configured in ZENworks Control Center.

Default Value: 120 days

PATCH_DEPLOY_USER_SYSTEM

Set `true` or `false` to specify the Windows executable's security level.

`true`: The option **Run as secure system user (Don't allow system to interact with desktop)** will be selected.

`false`: The option **Run as dynamic administrator** will be selected.

PATCH_NEW_AGENT_SET_CONFIGURED_DAU_SCHEDULE

Set to `true` to have the DAU Schedule for new devices the same as configured in ZCC when they get registered to the zone, provided the respective DAU bundle is already available in the zone

PATCH_NOTIFY_INSTALL_ALLOWCANCEL

Set to `true` to allow the user to cancel the patch installation.

PATCH_NOTIFY_INSTALL_POPUP_DURATION

Set value to define how long the system tray notification is displayed before being hidden.

PATCH_NOTIFY_INSTALL_POPUP_SHOW_TRAY

Set to `true` to enable a notification for a pending installation is displayed in the system tray.

PATCH_NOTIFY_INSTALL_MESSAGE

Set value for the text of the notification message.

PATCH_NOTIFY_INSTALL_MESSAGE_POPUP

Set value for text that appears in the notification.

PATCH_NOTIFY_INSTALL_NOTIFYUSER

Set to `true` to notify the user prior to the installation of the patch.

PATCH_NOTIFY_INSTALL_REBOOT_TIMEOUT

Set the value of the countdown for install notification.

PATCH_NOTIFY_INSTALL_SNOOZE

Set to `true` to allow the user to delay the installation.

PATCH_NOTIFY_INSTALL_SNOOZE_INTERVAL

Set the value for the duration the install is delayed when the user snoozes.

PATCH_NOTIFY_REBOOT_ALLOWCANCEL

Set to `true` to enable a cancel option in the reboot notification prompt.

PATCH_NOTIFY_REBOOT_MESSAGE

Set value for the text of the message that appears before patch installation completes and the computer reboots.

PATCH_NOTIFY_REBOOT_MESSAGE_POPUP

Set value for text that appears in the notification.

PATCH_NOTIFY_REBOOT_NOTIFYUSER

Set to `true` to enable reboot notification and its configuration options.

PATCH_NOTIFY_REBOOT_POPUP_DURATION

Enter a value in hours, minutes or seconds for how long the system tray notification is displayed before being hidden.

PATCH_NOTIFY_REBOOT_POPUP_SHOW_TRAY

Set to `true` to enable a notification for a pending reboot which is displayed in the system tray.

PATCH_NOTIFY_REBOOT_REBOOT_TIMEOUT

Set the value of the countdown for reboot notification.

PATCH_NOTIFY_REBOOT_SNOOZE

Set to `true` to enable a snooze option in the deployment reboot notification prompt, which delays the reboot.

PATCH_NOTIFY_REBOOT_SNOOZE_INTERVAL

Set the value for the duration the reboot is delayed when the user clicks **Snooze**.

PATCH_NOTIFY_REBOOT_SUPPRESSREBOOT

Set to `true` to enable an option in the reboot notification prompts to prevent the reboot.

PATCH_POLICY_ACTIONS_LIMIT

Enables adjustments of the maximum number of patch policy actions. Thus, using this system variable allows users finer control of patch policy child bundle actions.

Default Value: 1500 actions

Valid Range: 100 to 99999 actions

PATCH_SCAN_ALWAYS

Set to `true` to ensure that the patch detection scan runs on all devices as scheduled, even when patch discovery for new content does not indicate the need for a scan. When the variable is not set, the default behavior is the same as `true`.

Default Value: `true`

Valid Values: true, false

PATCH_SHOW_BLANK_POLICY

This variable, when set to true, opens the Patches page in a policy that is blank.

Default Value: false

Valid Values: true, false

PATCH_TREND_DATA_DAYS

This variable controls the number of days that patch Dashboard and Trending data, which was configured in an earlier version of ZENworks, is stored in the database. Set the value to *x* days of storing data or set it to 0 to disable storing the data.

NOTE: Patch Dashboard and Trending provided patch compliance and trending data on the Patch dashboard in ZENworks 2017 Update 2 and earlier versions. This variable is only applicable to ZENworks Patch Management environments that have updated to ZENworks Patch Management 2017 Update 4 from an earlier version. It is not applicable for new installations from Update 4 and later. For information about accessing this data, contact [Technical Support](#).
