ZENworks 2020 Patch Management

Evaluator's Guide
August 2021

Cybersecurity Ventures predicts that global cyber crime damages will reach $10.5 trillion annually by 2025. With cyber theft ranked as the fastest-growing crime in the U.S., even the least-skilled threat actors have become proficient at exploiting unpatched software—the low hanging fruit of cyber crime.

All of this means that software patching must be at the core of every organization's cyber security strategy, providing two essential capabilities: an ***automated, scheduled way to maintain patch currency*** and a process for ***quickly identifying and mitigating known software security vulnerabilities***.

ZENworks 2020 Patch Management is specifically designed to meet today's cyber security challenges. It's ***rules-based policies*** provide an automated, regular cadence of OS and application patching, reducing the effort and resources required to keep devices up-to-date. It's ***Security Dashboard maps Common Vulnerabilities and Exposures (CVE) IDs*** to impacted devices, enabling administrators to quickly deploy the patches required to secure the devices. And it does this for ***Windows, Mac, and Linux devices*** through a single management console.

But don't take our word for it. Use this *Evaluator's Guide* to check out ZENworks 2020 Patch Management yourself. We'll use Windows devices in the evaluation, but if you are interested in patching Mac or Linux we'll provide some guidance at the end of the evaluation as to how to do that as well.

How to Evaluate ZENworks 2020 Patch Management

Review What You'll Need for the Evaluation

Here's a heads up on some of the resources you'll need in order to run through this evaluation. More information about these requirements is provided in the sections that follow.

- ❒ **A Windows/Linux server or VM hypervisor.** The ZENworks software must be installed on a Windows or Linux server (physical or virtual). Or, the ZENworks Virtual Appliance (pre-configured with the ZENworks software) must be run on a supported hypervisor. For more information about supported servers and hypervisors, see "Download the ZENworks Software" on page 2.

  The ZENworks server requires access to the Internet in order to download patches from the ZENworks patch repository and various software vendor sites.

- ❒ **A Windows 10 device.** This can be a desktop or laptop running any Windows 10 version that has not reached its end of service date. Use a device that hasn't been patched in a while so that there are more patches available. If you have multiple Windows 10 devices to use, you'll have more patching options to enhance your evaluation experience.

Set Up a ZENworks System

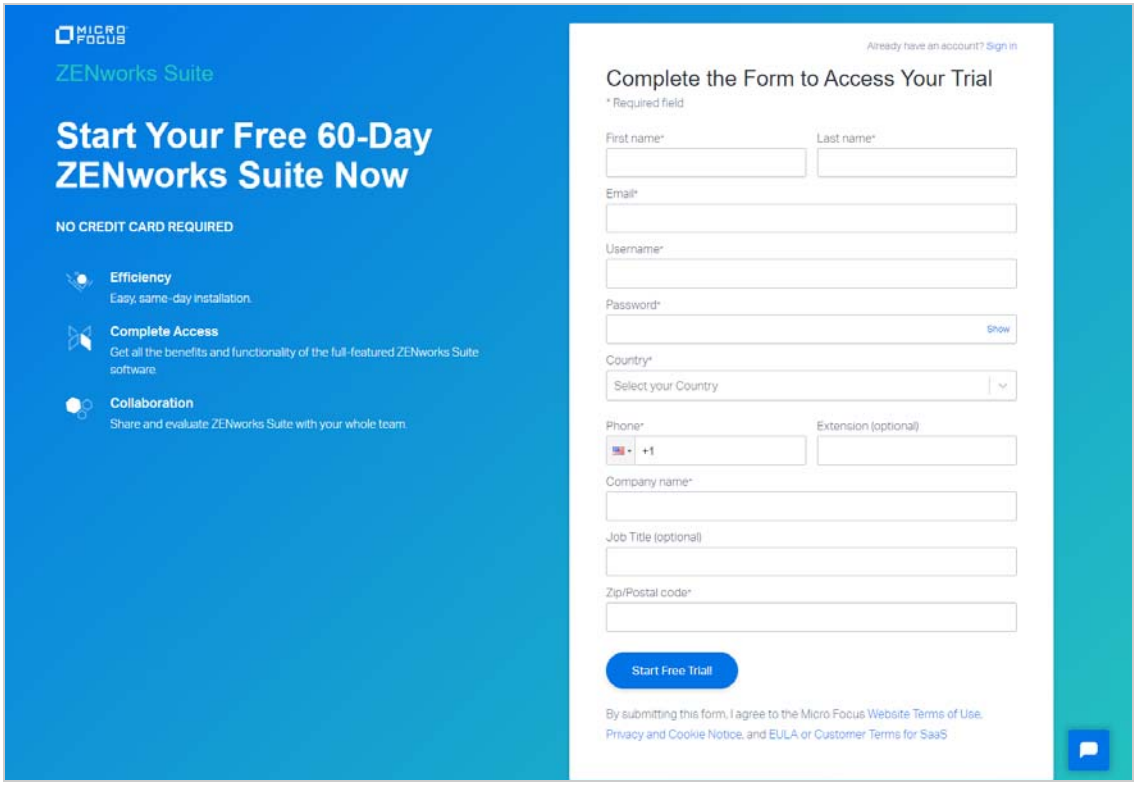
As a Unified Endpoint Management and Protection solution, all ZENworks Suite products (Asset Management, Configuration Management, Endpoint Security, Full Disk Encryption, and Patch Management) use the same ZENworks infrastructure. This means that when you complete the ZENworks installation, not only can you evaluate ZENworks Patch Management but you can also evaluate any of the other products. The products can be licensed as a Suite or individually.

- "Download the ZENworks Software" on page 2
- "Install ZENworks" on page 8
- "Register a Windows 10 Device" on page 9

Download the ZENworks Software

To download the ZENworks software, you need a Micro Focus account. If you don't already have an account, no worries, we'll help you easily create one through our free trial website. Not only does your Micro Focus account let you access the ZENworks software to evaluate, it also gives you access to trials for other Micro Focus products and membership in the Micro Focus product communities.

1. Go to the ZENworks 2020 Suite Trial Registration page (https://www.microfocus.com/products/zenworks/free-trial).



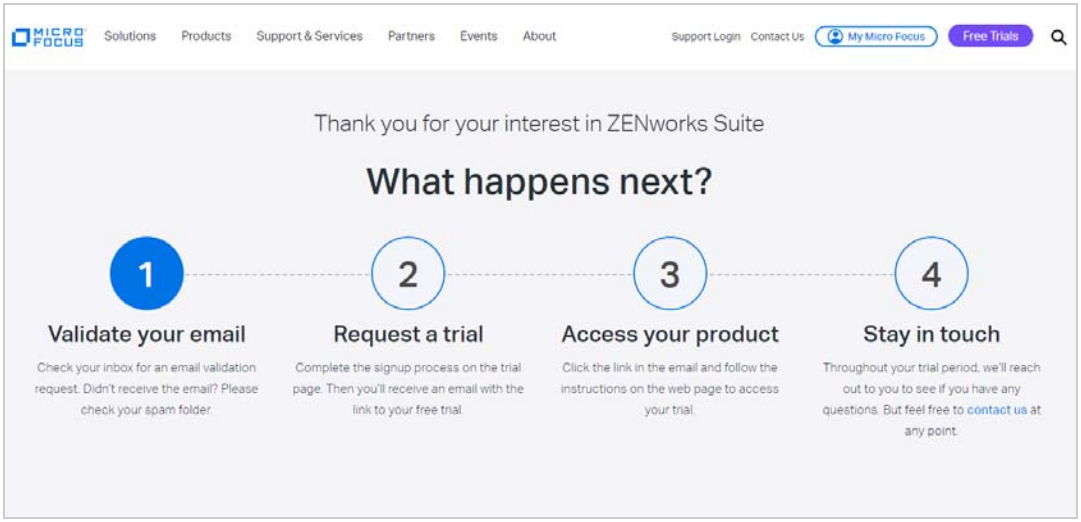
2 If you already have a Micro Focus account, click the **Sign In** link in the top right corner of the form and sign in to your account. Then continue with Step 3 below.

or

If you don't have a Micro Focus account:

2a Fill in the form to provide information for your account, then click **Start Free Trial**.

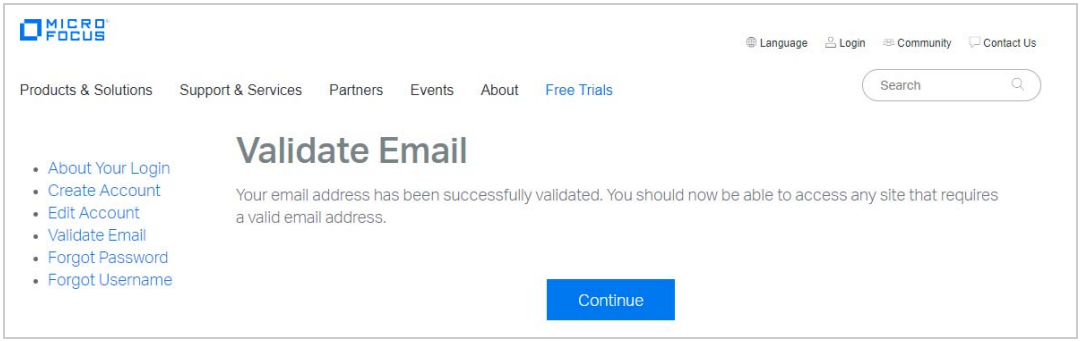
Your account is created and the following page is displayed.



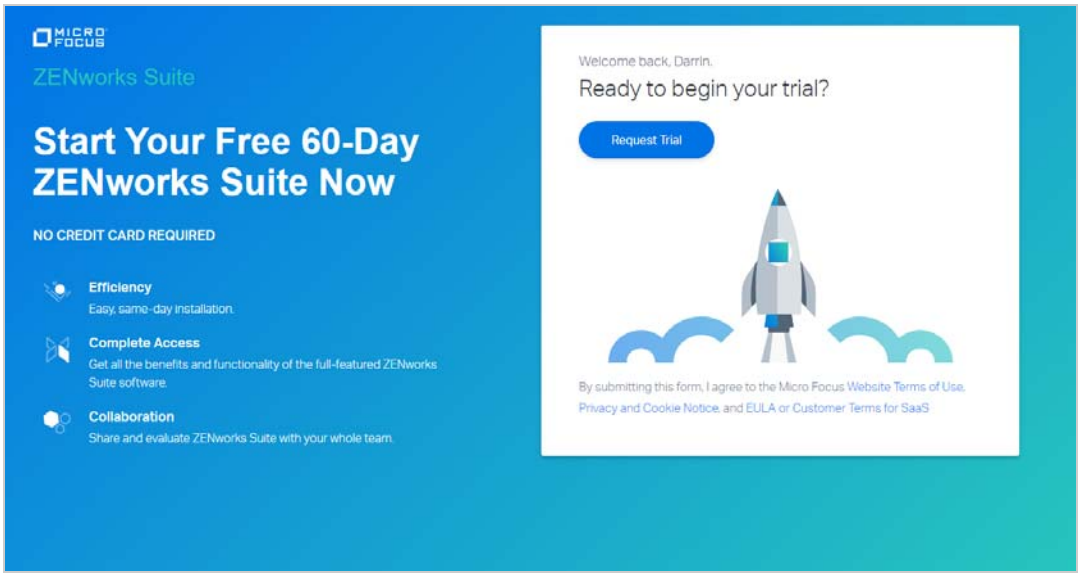
2b In your email account, open the Micro Focus Account email and click the **Validate Email** link.

2c Sign in with your Micro Focus account username and password.

After successful login, your email is validated and your Micro Focus account is activated.



2d Click **Continue** to return to the ZENworks Suite trial page.

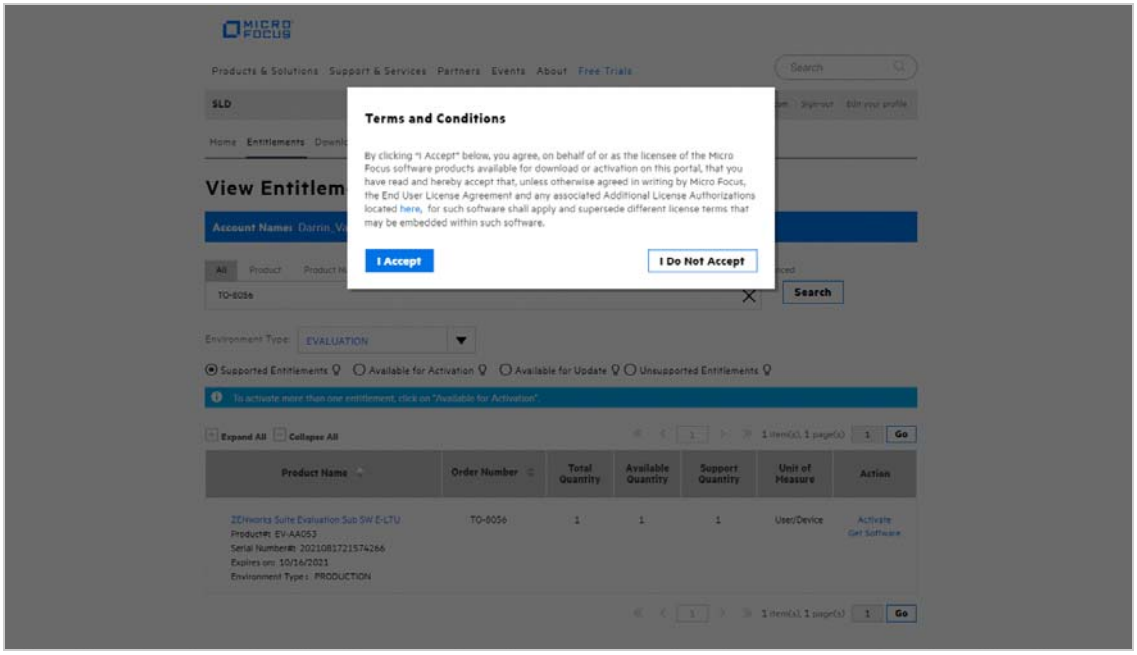


3 Click the **Request Trial** link.

4 In your email account, open the MFI Trials and Eval email and click the **Sign in** link.

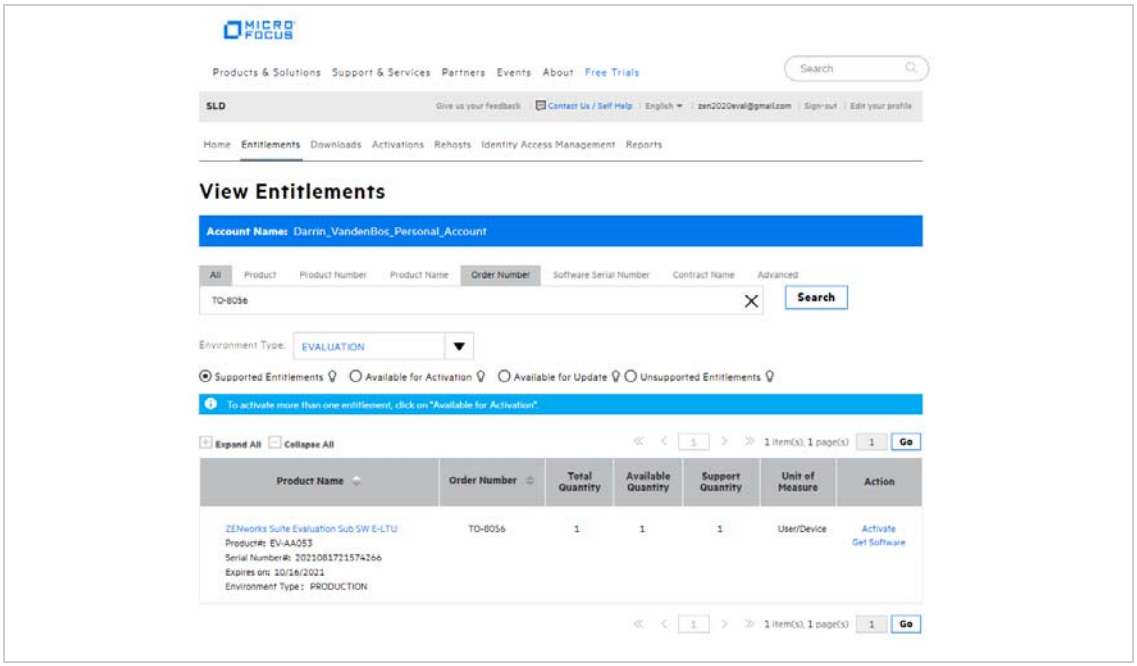
5 If prompted, sign in with your Micro Focus account username and password.

Your Micro Focus Software and License Distribution (SLD) portal is displayed.



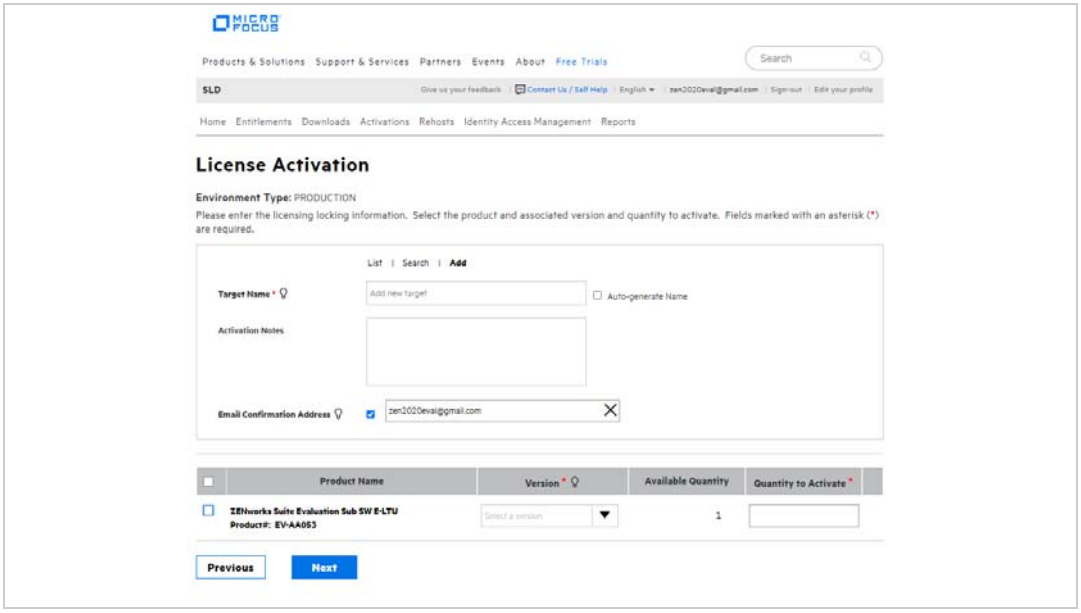
6 Click **I Accept** to agree to the terms and conditions for Micro Focus software products.

7 Click **OK** to dismiss the *How to access your License Entitlements and Software Downloads* dialog.



8 Activate the product:

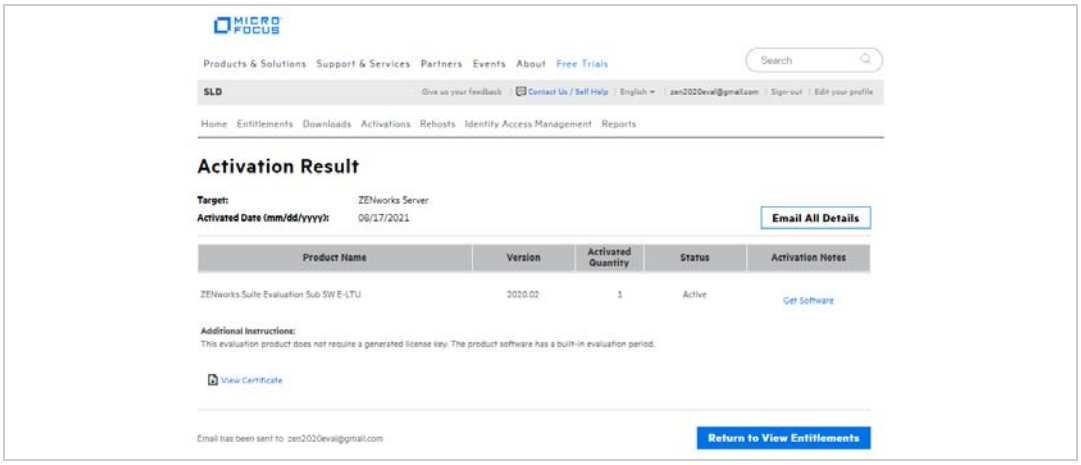
8a In the product list, click the **Activate** link for the *ZENworks Suite Evaluation Sub SW-E-LTU* entry to display the License Activation page.



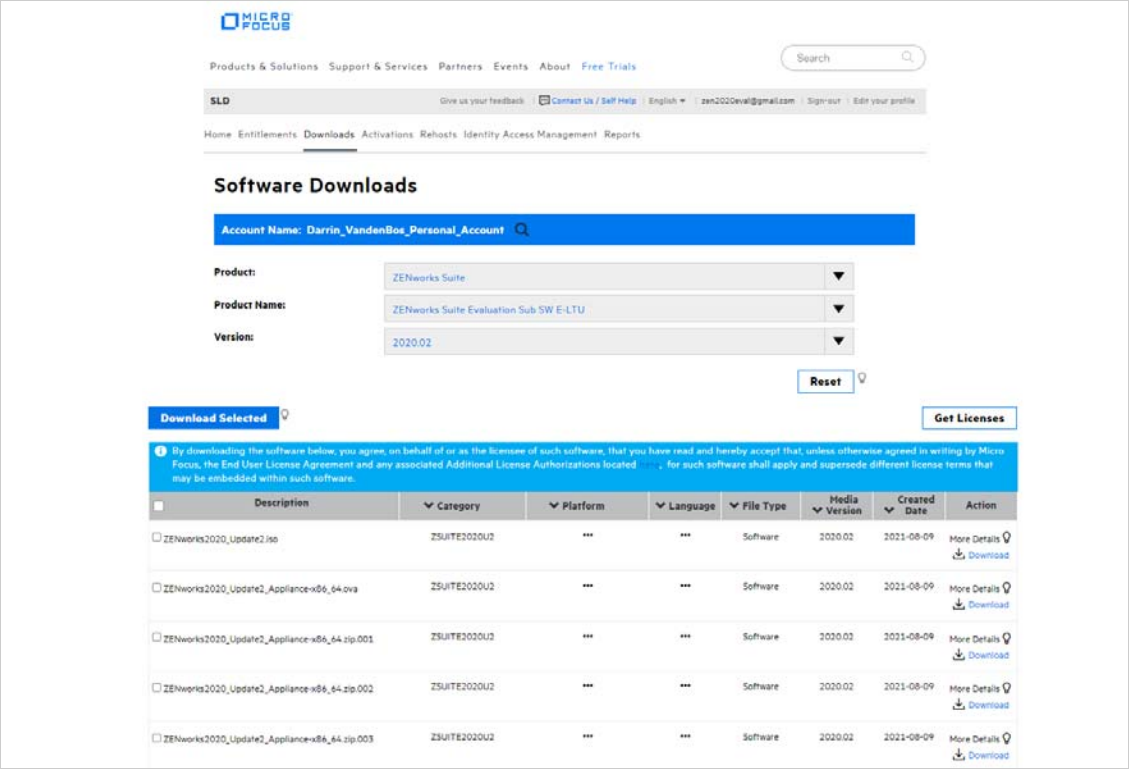
8b In the Target Name field, enter `ZENworks Server`.

8c In the list, select **ZENworks Suite Evaluation Sub SW E-LTU**, select **2020.02** for the version, enter 1 as the quantity to activate, then click **Next**.

8d Click **Submit** to confirm the activation details and display the Activate Results page.



9 Click **Get Software** to display the Software Downloads page.



You'll quickly notice that there are a bunch of different download files. The files you need depend on whether you want to use the ZENworks Virtual Appliance or perform a traditional install.

Virtual Appliance: ZENworks is available as a virtual appliance that can be deployed to a supported virtual infrastructure. The appliance is built on a customized SUSE Linux Enterprise Server (64-bit) and comes pre-installed with ZENworks.

We strongly recommend that you use the appliance for the evaluation. Why? Because the appliance is convenient, easy to use, and doesn't require you to supply an operating system license.

The appliance is supported on the following hypervisors.

Hypervisor	File to Download
VMware ESXi 6.x VMware Workstation 6.5 and newer (use in non-production environments only)	ZENworks2020_Update2_Appliance-x86_64.ova
Microsoft Hyper-V Server Windows 2012 | 2012 R2 | 2016 | 2019	ZENworks2020_Update2_Appliance-x86_64.vhd.zip ZENworks2020_Update2_Appliance-x86_64.vhdx.zip
XEN on SLES 12.x |15.x	ZENworks2020_Update2_Appliance-x86_64.xen.tar.gz
Citrix XenServer 7.x and Citrix Hypervisor 8.x	ZENworks2020_Update2_Appliance-x86_64.xva.tar.gz

Traditional Install: You can install the software on a server listed below.

Operating System	File to Download
Windows 2012 Server x86_64 Windows 2012 Server R2 x86_64 Windows 2016 Server x86_64 Windows 2019 Server x86_64	ZENworks_2020_Update2.iso
SLES 12 SP4 | SP5 x86_64 SLES 15 | SP1 | SP2 x86_64	ZENworks_2020_Update2.iso

10 Click the **Download** link for the files you want to download.

Install ZENworks

After you've downloaded the ZENworks software, you are ready to install the ZENworks Primary Server and establish a management zone. The Primary Server manages the devices that register in the zone. For example, patches are downloaded by the Primary Server and distributed to the managed devices.

Refer to the appropriate section for installation instructions:

- Deploy the ZENworks Virtual Appliance (page 8)
- Install the ZENworks Software (page 8)

Deploy the ZENworks Virtual Appliance

1. Make sure the host machine has at least 16 GB RAM and 130 GB free disk space, and has a static IP address or a permanently leased dynamic (DHCP) IP address.
2. Import the ZENworks Virtual Appliance into your hypervisor to create a new virtual machine.
3. After the virtual machine has been created, add a second hard disk of size 40 GB. The first disk (90 MB) is used for the Appliance while the second disk (40 GB) will be used to store the ZENworks data.
4. Power on the new virtual machine.
5. Follow the prompts to configure the virtual machine and then the ZENworks Server and zone.

   For this evaluation, we recommend the following:

   - Create a new ZENworks Management Zone.
   - Use the embedded PostgreSQL database. Even if you use Oracle or MSSQL database in your environment, using the embedded PostgreSQL database is more convenient and quicker.
   - Use the internal Certificate Authority. Even if you use an external CA in your environment, using the internal CA is more convenient and quicker.

If you need more details, refer to the *ZENworks Appliance Deployment and Administration Reference (https://www.novell.com/documentation/zenworks-2020-update-2/zen_ca_appliance)*.

Install the ZENworks Software

1. Make sure the target server has at least 16 GB RAM and 80 GB free disk space, and has a static IP address or a permanently leased dynamic (DHCP) IP address.
2. Log in to the server as a user with administrative rights.

3 Mount the ZENworks ISO and run the installation program:

- **Windows:** Run `setup.exe`.
- **Linux:** Run `setup.sh`.

4 Complete the installation wizard.

For this evaluation, we recommend the following:

- Create a new ZENworks Management Zone.
- Use the embedded PostgreSQL database. Even if you use Oracle or MSSQL database in your environment, using the embedded PostgreSQL database is more convenient and quicker.
- Use the internal Certificate Authority. Even if you use an external CA in your environment, using the internal CA is more convenient and quicker.

If you need more details, refer to the *ZENworks 2020 Server Installation Guide (https://www.novell.com/documentation/zenworks-2020-update-2/zen_installation)*.

Register a Windows 10 Device

A device must register with the ZENworks management zone in order for it to be managed. To register a Windows device, you install the ZENworks Agent on the device. The agent then contacts the ZENworks Primary Server and completes the registration process.

- "Create an Authorization Key" on page 9
- "Register a Device" on page 12

Create an Authorization Key

When you install the ZENworks Agent on a device, it has the information required to connect back to your ZENworks Primary Server and register in your zone. To secure your ZENworks system against access by rogue devices, ZENworks allows only authorized devices to register. One way to authorize a device is to issue an authorization key that must be entered during installation and registration of the ZENworks Agent on the device. This is the method we'll have you use, which means you first need to create an authorization key.

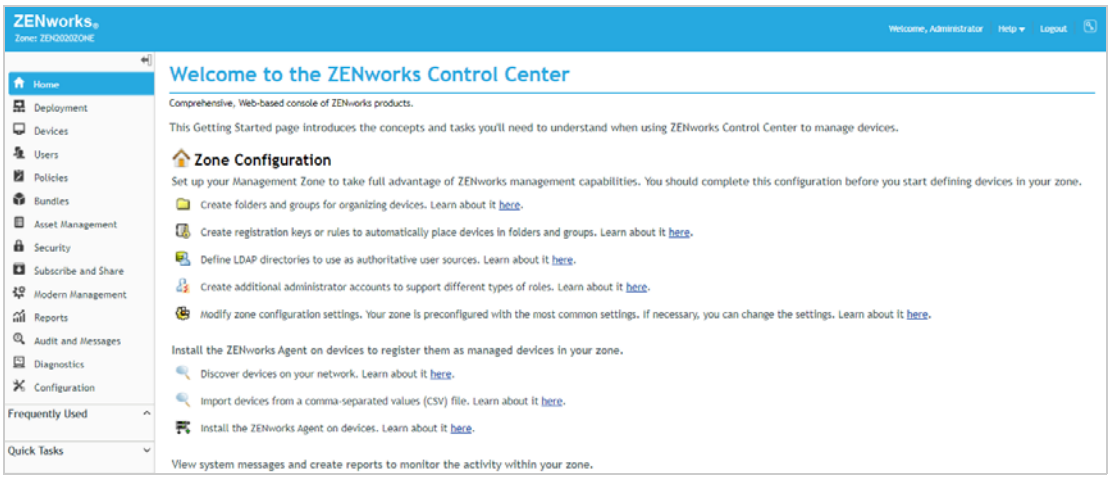
1 Log in to ZENworks Control Center:

1a In a web browser, enter the following URL:

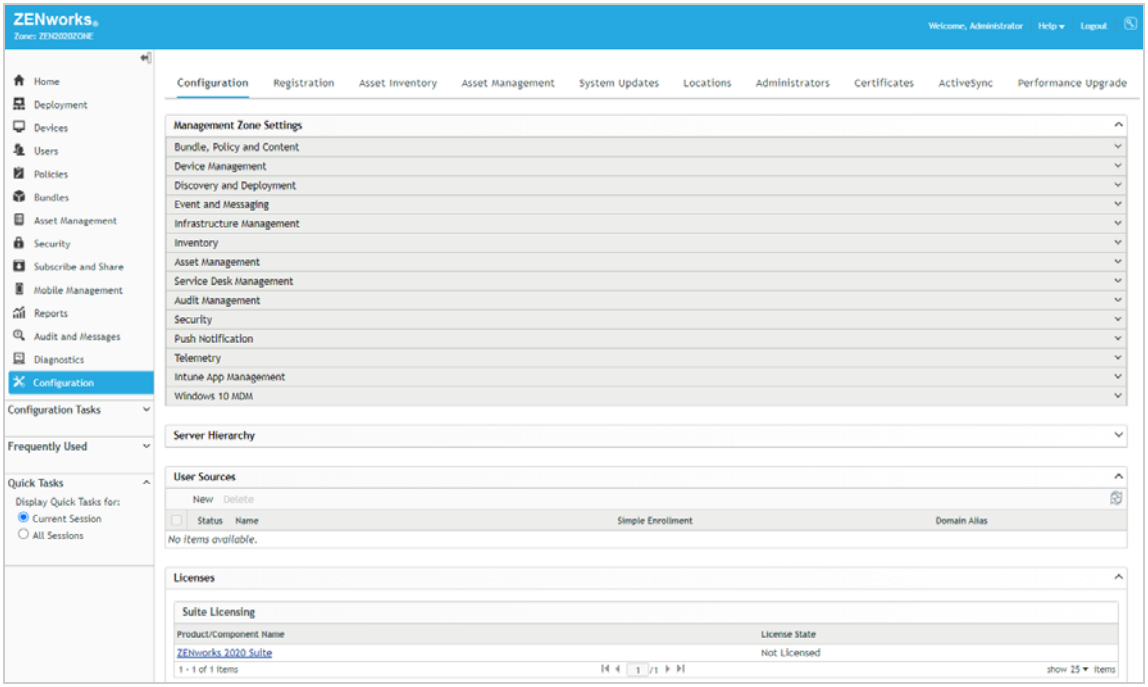
`https://ZENworks_Server_Address`

Replace `ZENworks_Server_Address` with the IP address or DNS name of the ZENworks Primary Server.

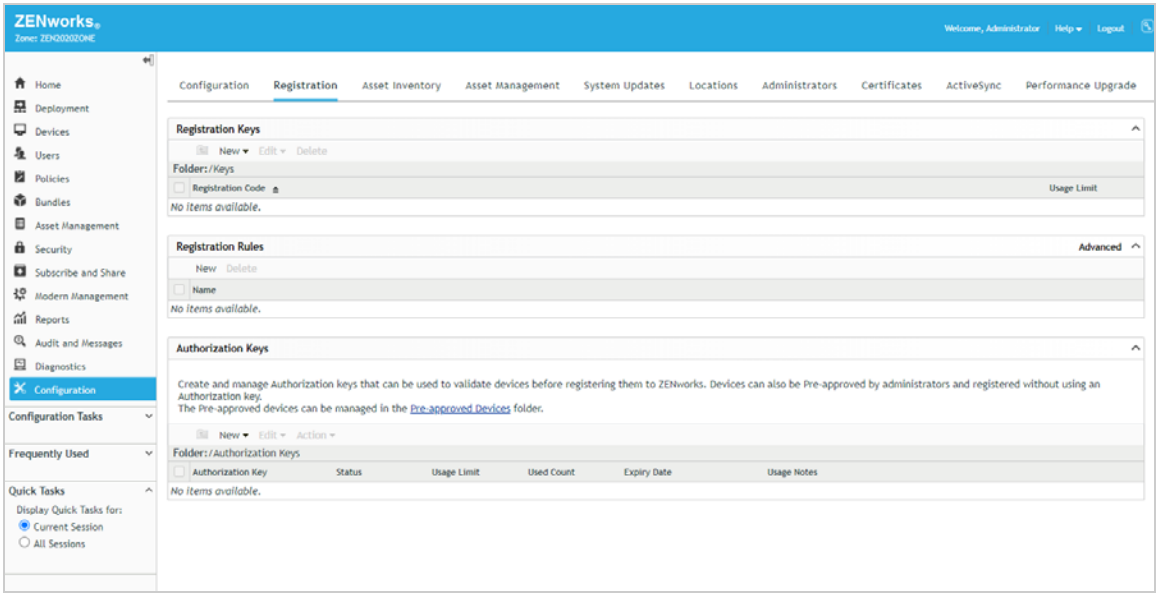
1b Specify *Administrator* as the username, specify the password you defined during installation, then click **Login** to display the Welcome page.



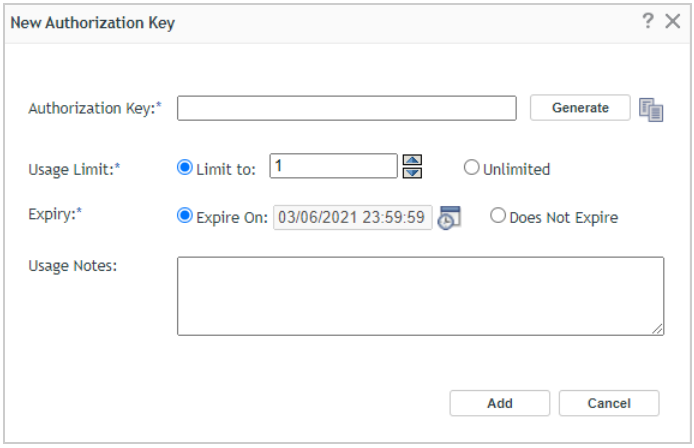
2 Click **Configuration** (in the left navigation pane).



3 Click the **Registration** tab (top of page).



4 In the Authorization Keys panel, click **Configure > Authorization Key** to display the New Authorization Key dialog box.



5 Configure the settings as follows, then click Add to create the key.

- **Authorization Key:** Enter an 8 - 10 character key of your choice, or click **Generate** to automatically generate one. You'll need to remember the key. Write it down if necessary.
- **Usage Limit:** Select the limit for the number of times this key can be used, or select **Unlimited** to remove the usage limit for this evaluation. Security best practices dictate that you not allow unlimited uses in a production environment.
- **Expiry:** Select an expiration date for the key, or select **Does Not Expire** for this evaluation. As with the usage limit, security best practice in a production environment would be to use an expiration date.

6 Click **Add** to create the key and add it to the list.

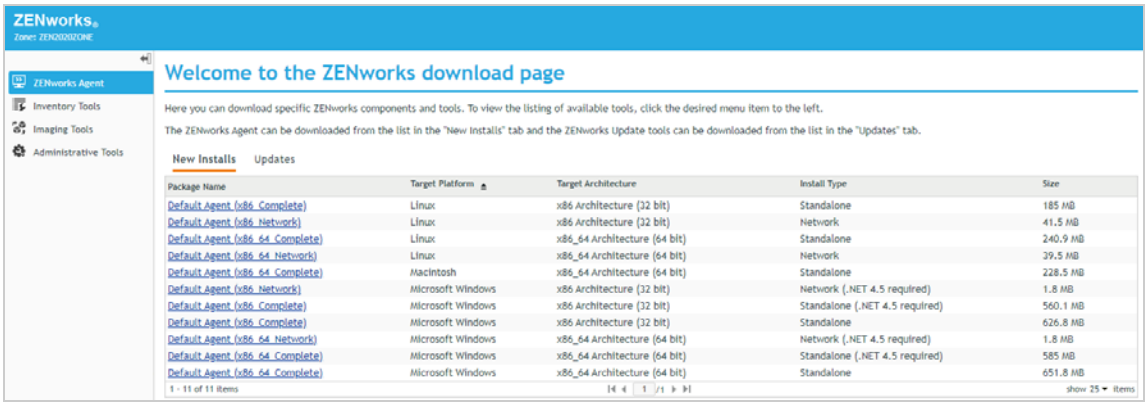
Register a Device

There are several ways you can distribute the ZENworks Agent to the device, including using discovery and deployment tasks in ZENworks Control Center to push the agent to devices, but we'll just have you manually download the agent from your ZENworks Primary Server and start the installation.

1 On the Windows 10 device that you want to register, enter the following URL.:

`https://ZENworks_Server_Address/zenworks-setup`

The ZENworks Agent download list is displayed.



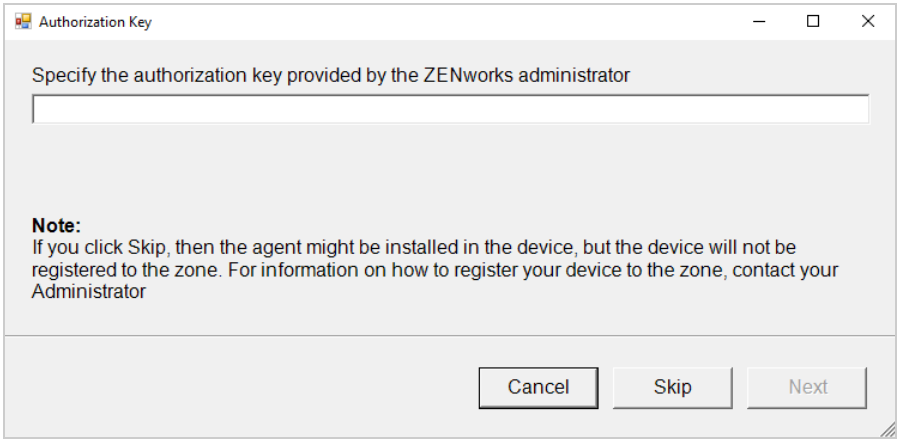
2 In the list, click the installation package you want to download to the device, then follow the prompts to download it.

You want the Microsoft Windows package that is the **Standalone** install type. If you know that the target device has .NET 4.5 or newer installed, you can use the **Standalone (.NET 4.5 required)** install type instead.

- **32 bit:** *Default Agent (x86_Complete)* Microsoft Windows x86 Architecture (32 bit) Standalone package
- **64 bit:** *Default Agent (x86_64_Complete)* Microsoft Windows x86_64 Architecture (64 bit) Standalone package

3 After the ZENworks Agent download completes, double-click the agent to install it on the device.

4 When prompted, enter the authorization key you created, then click **Next** to continue the installation.

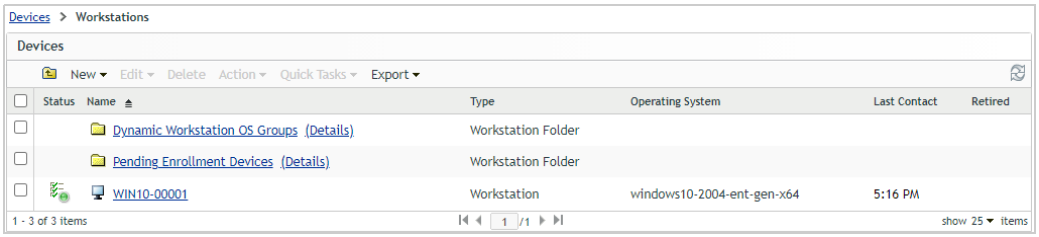


The installation can take a few minutes. You can track the progress through the ZENworks icon located in the notification area.

5 When installation is complete, reboot the device as prompted.

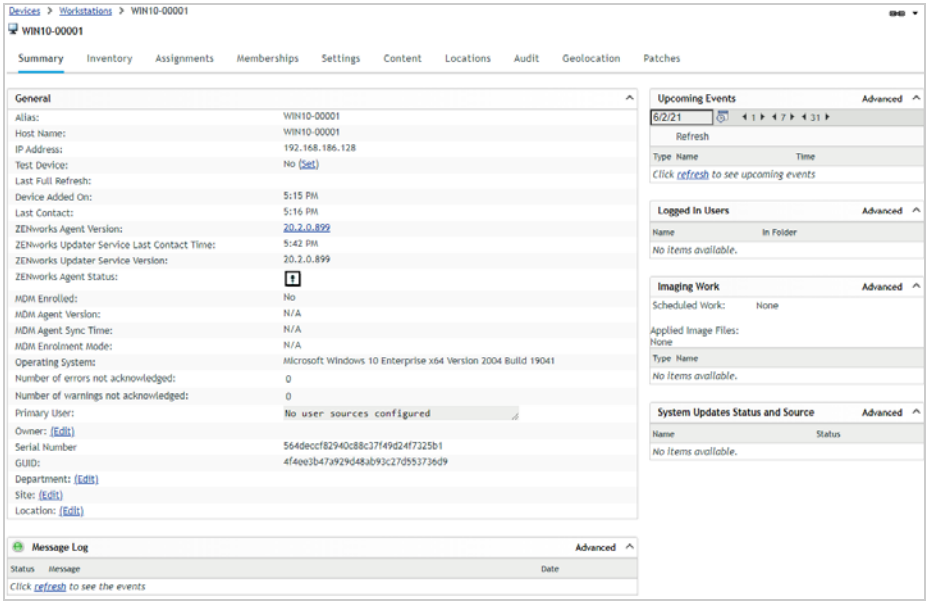
6 In ZENworks Control Center, go to the **Devices** > **Workstations** list to confirm that the device is enrolled in the zone.

The Windows device is listed after the predefined device folders. In this example, we enrolled a Windows device named *WIN10-00001*.



7 (Optional) In the list, click the Windows device to display its Summary page.

The Summary page provides details about the device.



You now have a device that you can use for the rest of this evaluation. One device is sufficient, but you can register additional Windows devices (for example, other Windows 10 versions) if you'd like to see patching across multiple devices. If you installed the ZENworks Primary Server to a Windows server, you can also patch that Windows server.

Start the Patch Services

ZENworks Patch Management subscribes to two external services:

- **U.S. National Vulnerability Database:** This database contains the Common Vulnerabilities and Exposures (CVE) data needed to monitor your ZENworks-managed devices for known software security vulnerabilities.

- **ZENworks Patch Repository:** This content download network (CDN) contains the operating system and application patches available for your managed devices.

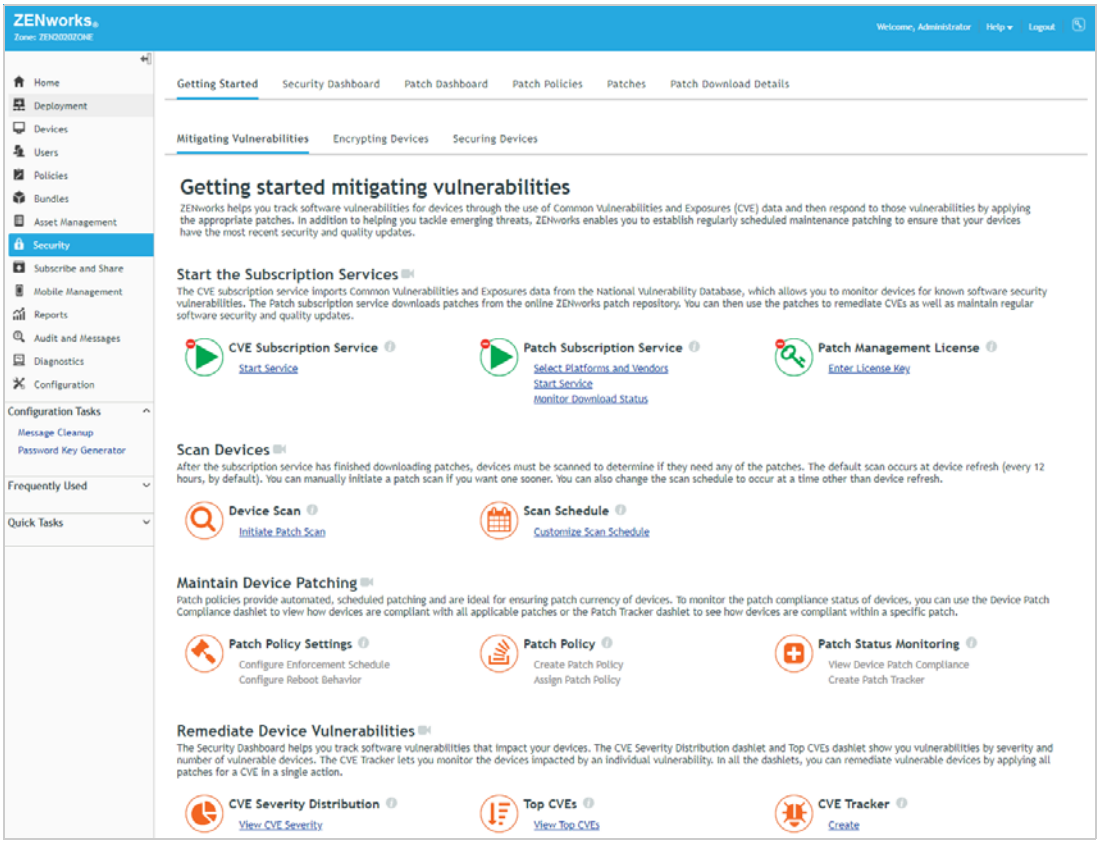
You must start both subscription services to populate your ZENworks system with the required CVE data and patches.

- “Start the CVE Subscription Service” on page 14
- “Start the Patch Subscription Service” on page 18

Start the CVE Subscription Service

1 In ZENworks Control Center, click **Security** > **Getting Started** to display the Getting Started Mitigating Vulnerabilities page.

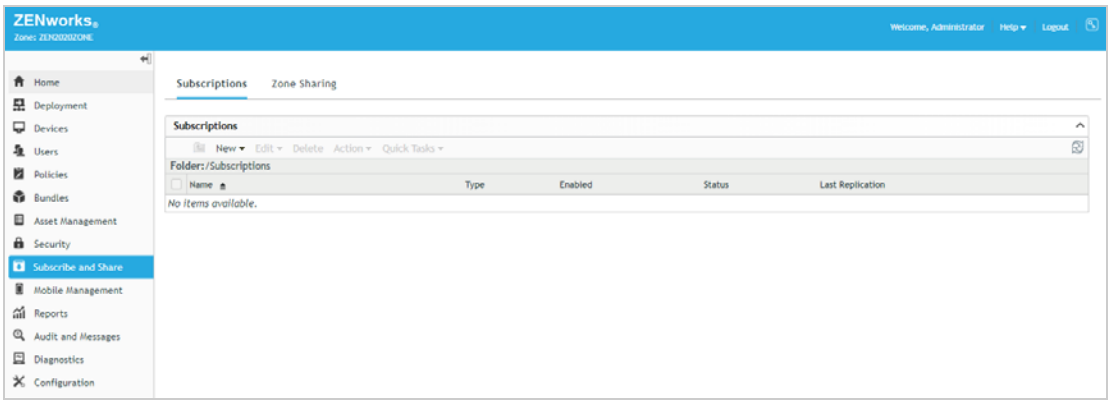
This Getting Started page helps you configure ZENworks Patch Management and use it to patch devices. We’ll use it as the starting point for the various tasks you’ll do as part of this evaluation.



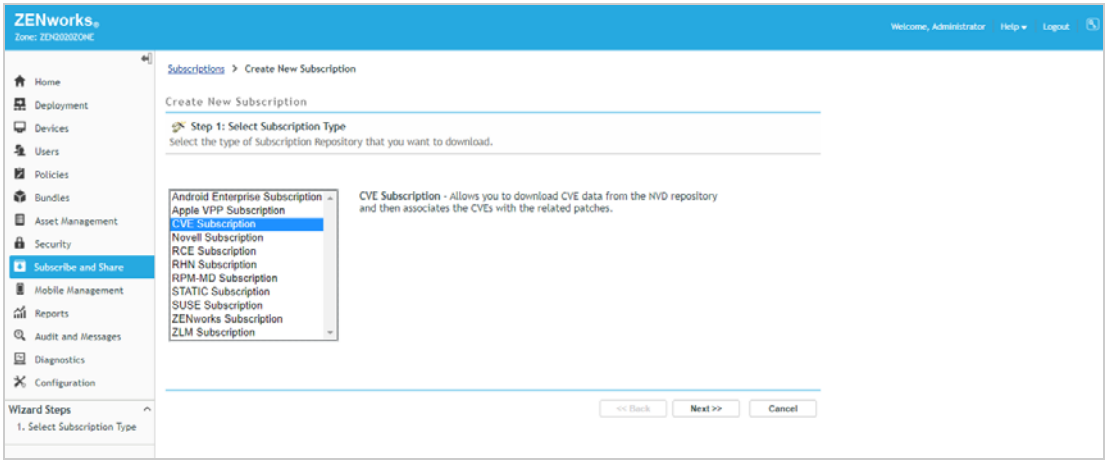
2 Under CVE Subscription Service, click **Start Service** to display the Subscriptions list.

You'll use this list to create the CVE subscription and start the service.

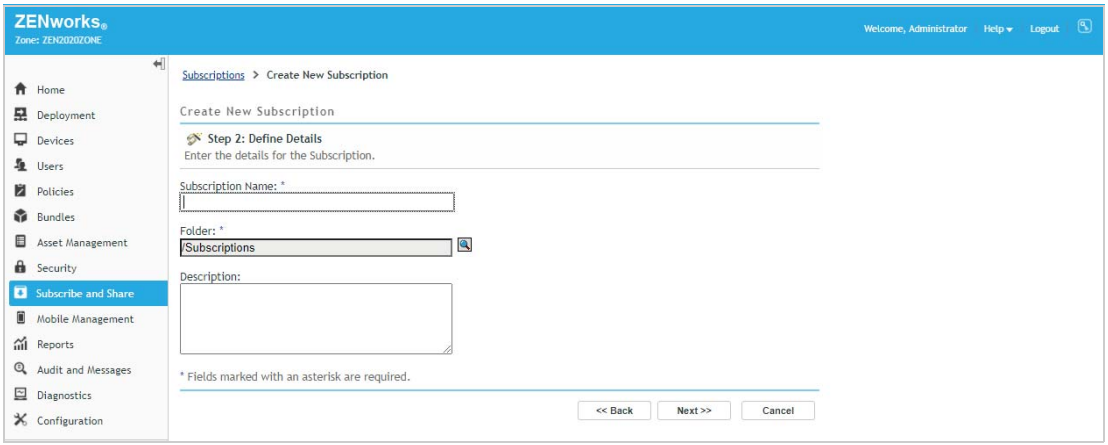
NAVIGATION TIP: You can go directly to the Subscriptions page through **Subscribe and Share** > **Subscriptions**.



3 In the Subscriptions list, click **New** > **Subscription** to display the Select Subscription Type page.

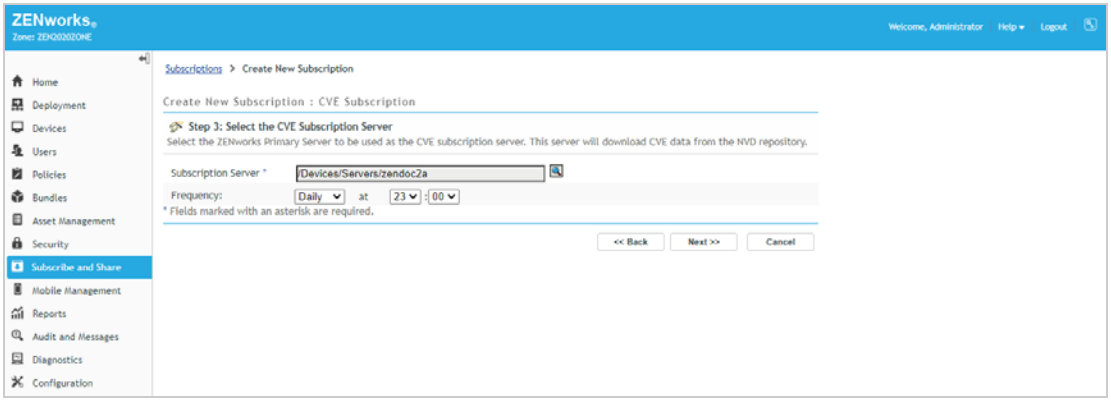


4 Select **CVE Subscription**, then click **Next** to display the Define Details page.

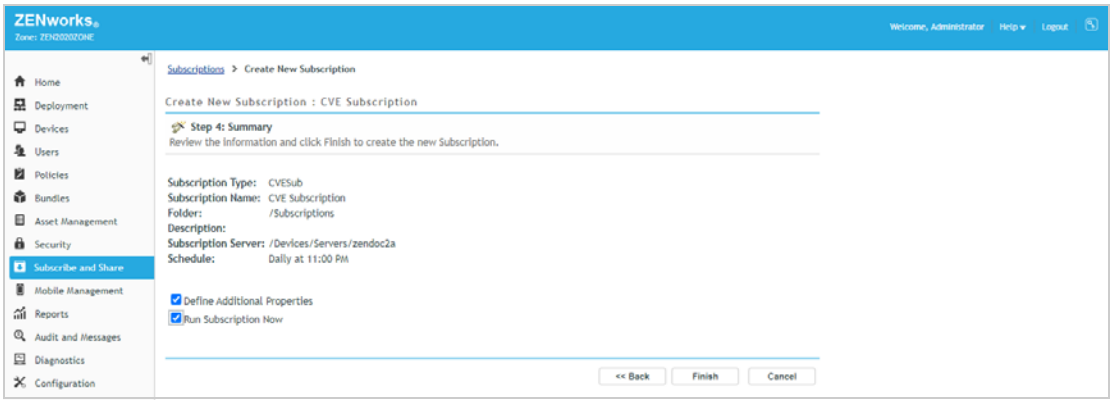


5 Enter CVE `Subscription` for the Subscription Name, then click **Next** to display the Select the CVE Subscription Server page.

You only have one ZENworks Primary Server so it is automatically selected to run the CVE subscription service at the default time of 11:00 PM each day.

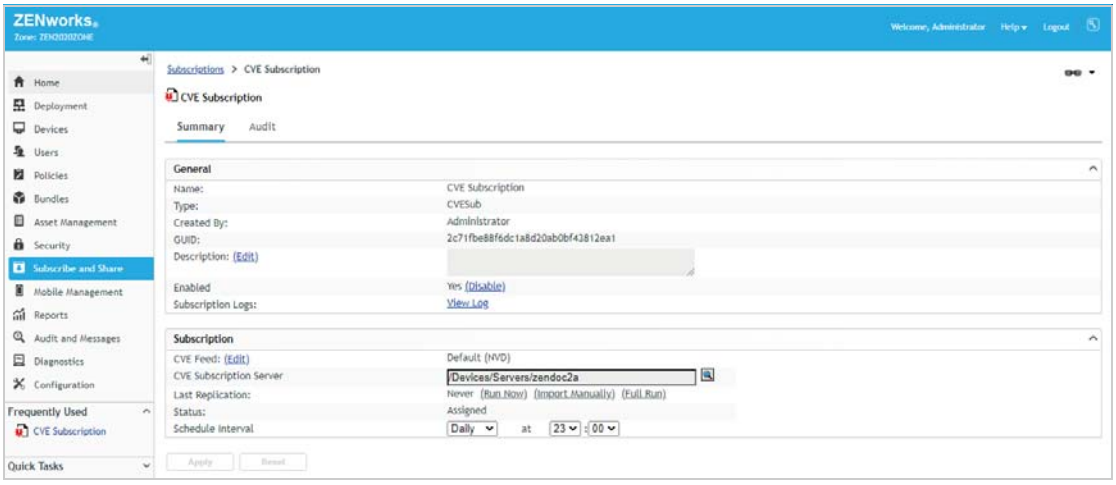


6 Keep the subscription server and frequency defaults, then click **Next** to display the Summary page.



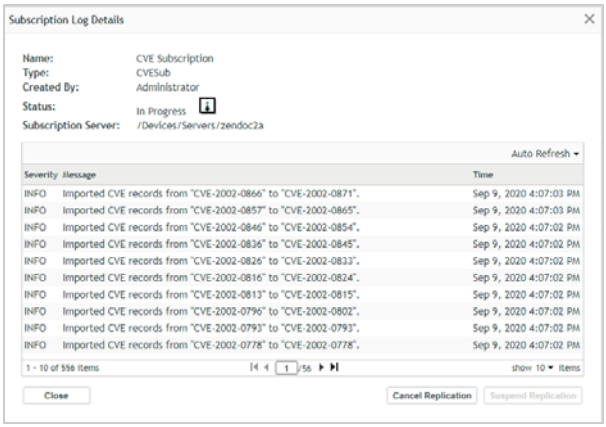
7 Select the **Define Additional Properties** option and the **Run Subscription Now** option, then click **Finish**.

The CVE subscription service is started and the details for the subscription are displayed. You can use this page to monitor the subscription as it imports CVE data from the National Vulnerability Database.



8 In the General box, click **View Log** to display the log details.

The CVE records are imported by year. The initial import can take a while, but when the subscription runs each day thereafter, it only imports changes and requires much less time.



9 When the data import is finished, close the dialog box.

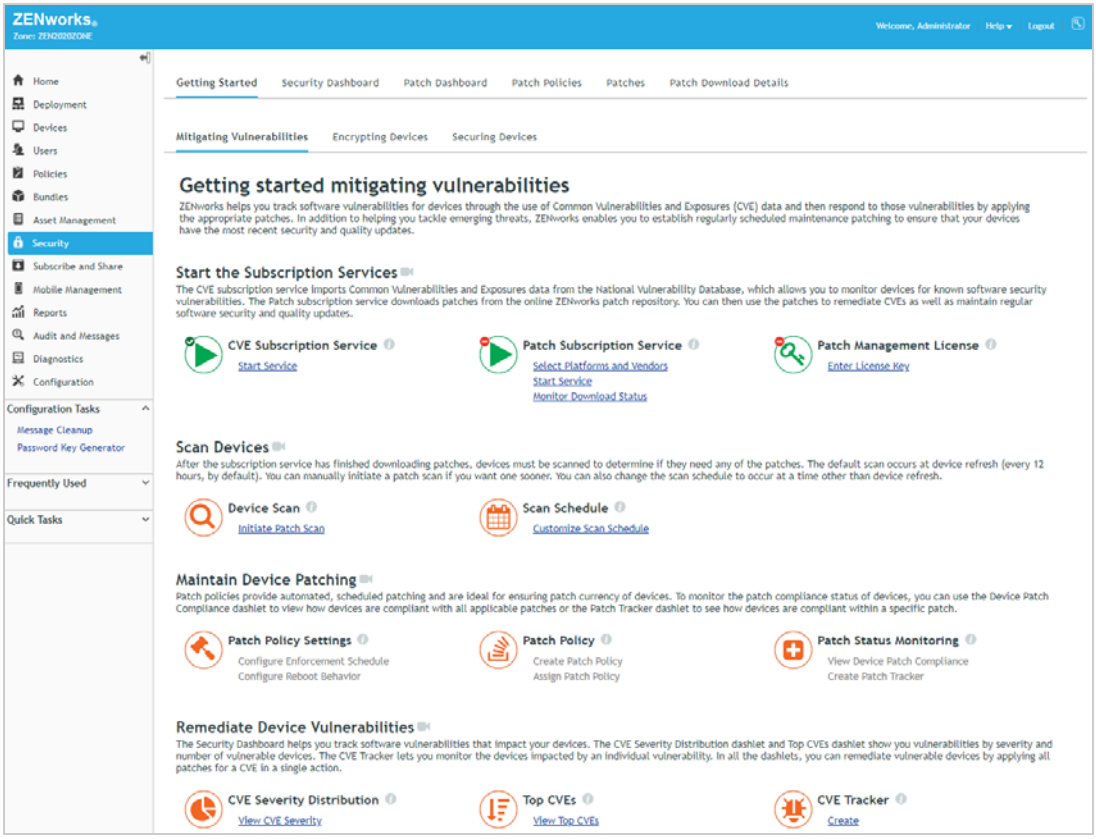
Start the Patch Subscription Service

The Patch subscription service runs on the ZENworks Primary Server. It connects daily to the online patch repository to discover and download patches for the devices in your zone.

As part of the subscription process, the service also associates the CVEs in your system with the patches that remediate them. For this reason, you should run the Patch Subscription service each day after the CVE subscription service. The default configuration runs the services in this order.

1 In ZENworks Control Center, click **Security** > **Getting Started** to display the Getting Started Mitigating Vulnerabilities page.

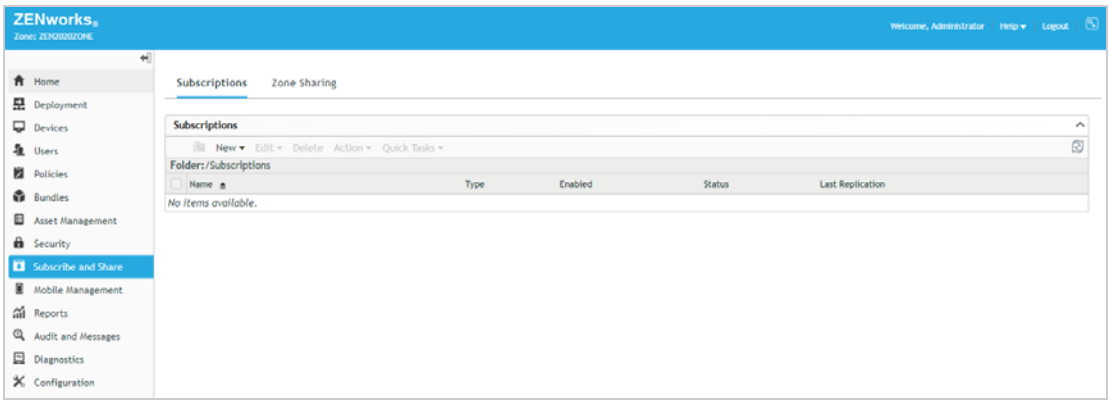
Notice that the CVE Subscription Service icon now has a green check mark to show that you've started that service.



2 Under Patch Subscription Service, click **Select Platforms and Vendors** to display the Subscription Service Content Download page.

This page lets you configure settings related to the patch content downloaded by the subscription service.

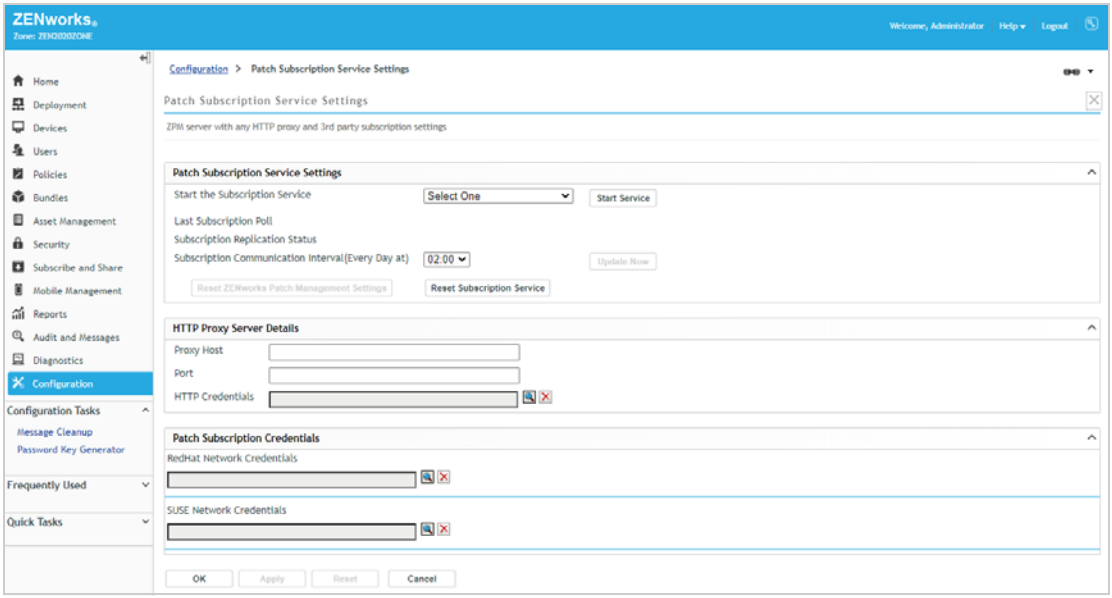
NAVIGATION TIP: You can go directly to the Subscription Service Content Download page through **Configuration** > **Management Zone Settings** > **Security** > **Subscription Service Content Download**.



All of the default settings are appropriate for this evaluation, with the exception of the platform setting. Since you will only be applying patches to Windows devices, you don't need to download the Linux and Mac patches.

3 Under the *Select the platforms to download* option, deselect **Linux** and **Mac**, then scroll to the bottom of the page and click **OK** to save the settings and return to the Getting Started.

4 Under Patch Subscription Service, click **Start Service** to display the Patch Subscription Service Settings page.

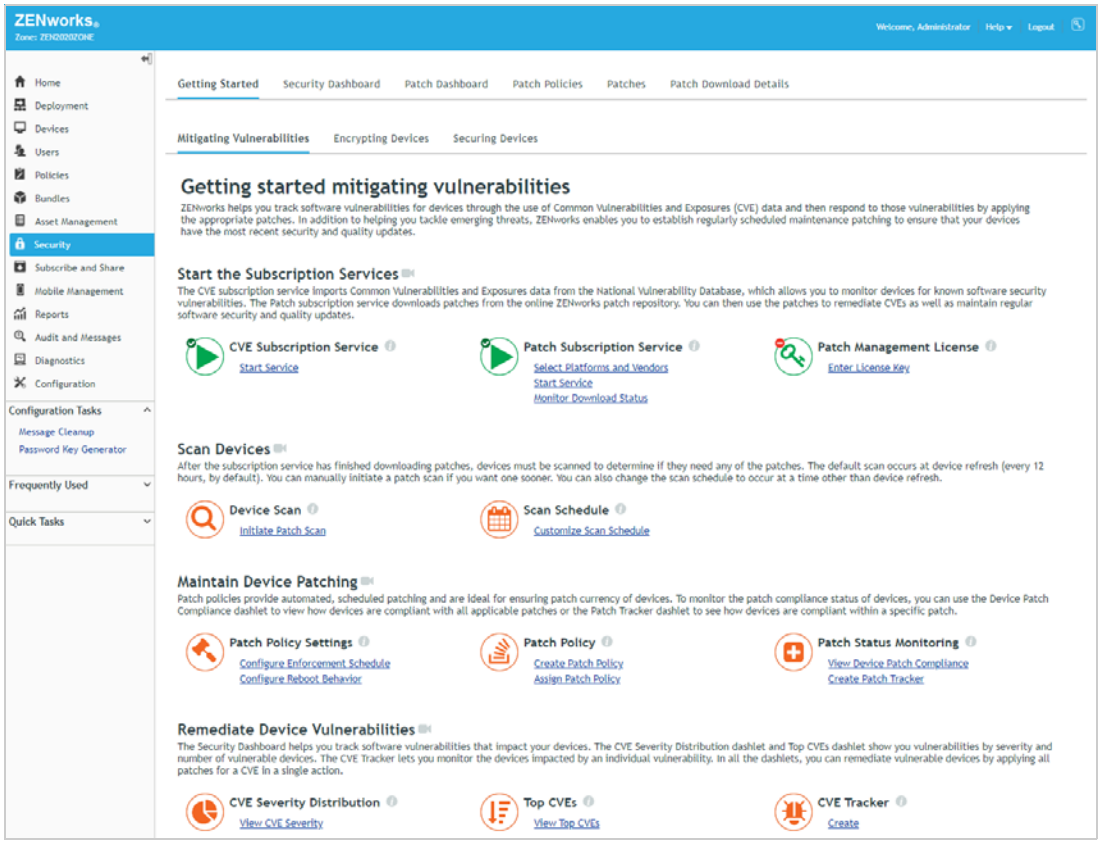


5 In the Start the Subscription Service list, select your ZENworks Primary Server, then click **Start Service**.

6 By default, the subscription service runs daily at 2:00 AM. However, we want to run it immediately in order to download available patches from the patch repository for your Windows devices. To do so, click **Update Now**, then click **OK** to dismiss the notification message.

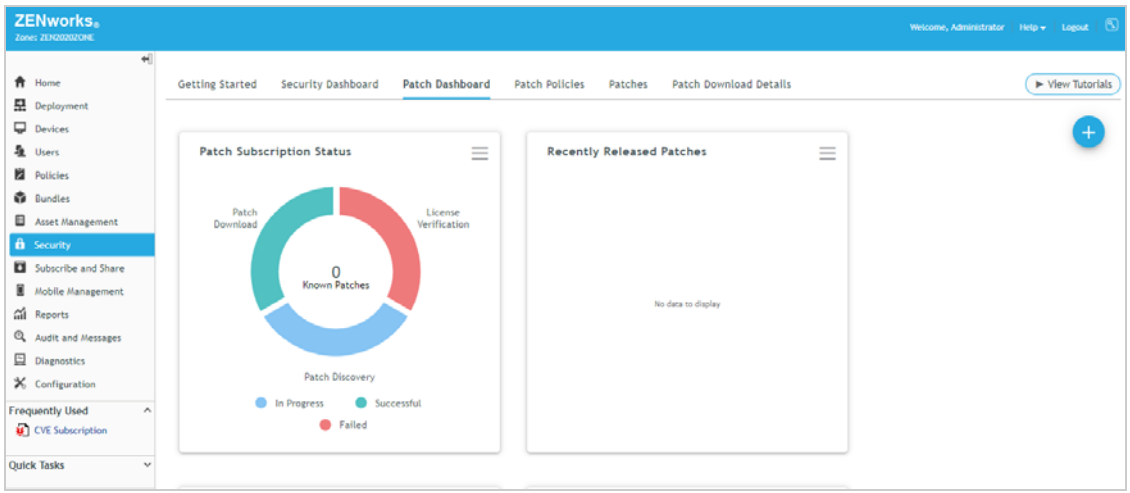
7 At the bottom of the page, click **OK** to save the settings and return to the Getting Started.

Notice that the Patch Subscription Server icon now has a green check mark to show that you've started the service.



8 Under Patch Subscription Service, click **Monitor Download Status** to display the Patch Dashboard.

The Patch Dashboard includes a Patch Subscription Status dashlet that you can use to monitor the progress of the patch download process.

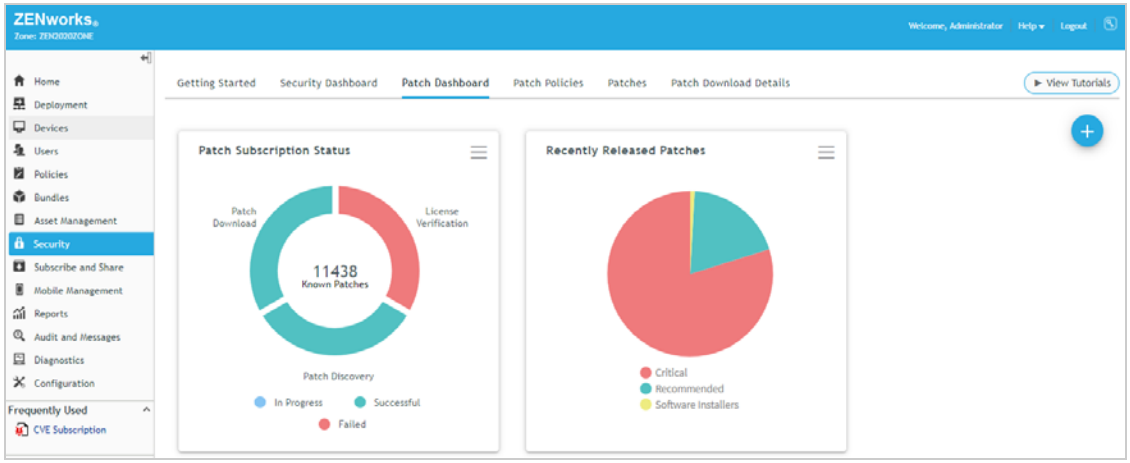


The dashlet shows three stages:

- **License Verification:** Determines if you have a valid Patch Subscription license. Normally this chart segment would be green (for Successful) but since you are using the built-in evaluation there is no license key to check and it shows as failed. You can ignore this, it does not affect the evaluation.
- **Patch Discovery:** Imports the signature files for patches that are applicable to devices in your zone. A patch signature file contains the metadata used when analyzing a device to determine if it requires the patch. As part of the Patch Discovery process, the subscription service bundles patch signature files into a DAU file (or *Discover Applicable Updates* file). The DAU file is then distributed to devices to be used during the patch scan.
- **Patch Download:** Downloads the content for patches. By default, only the content for patches included in Patch policies is automatically downloaded. You must manually download the content for any other patches (outside of Patch policies) you want to distribute. This ensures that your ZENworks Primary Server only needs to store the content for patches that you actually want to distribute.

The initial download can take several hours to complete. You can click the dashlet to see more details about each stage, including the current duration of the stage.

Once the process is complete, both the Patch Discovery and the Patch Download stages show green (Successful). In addition, the Recently Released Patches dashlet now shows the patches released in the last 30 days, organized by impact. If for some reason the dashlet is not showing data, simply click it to expand the dashlet and the data should populate.



Identify Device Vulnerabilities

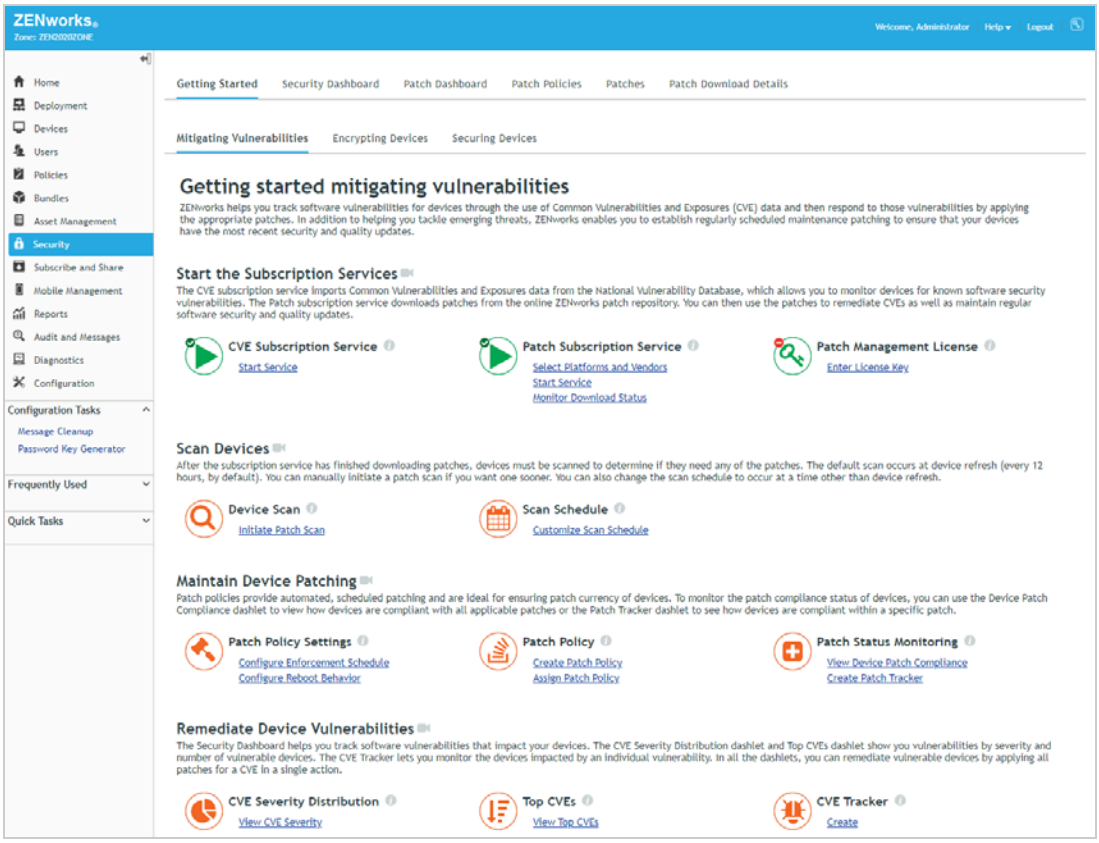
Now that the subscription services are running and have populated your ZENworks zone with CVE and patch data, you are ready to perform a patch scan on your Windows 10 device to identify its missing patches and security vulnerabilities.

- "Initiate a Scan" on page 22
- "Assess Vulnerability Status" on page 27

Initiate a Scan

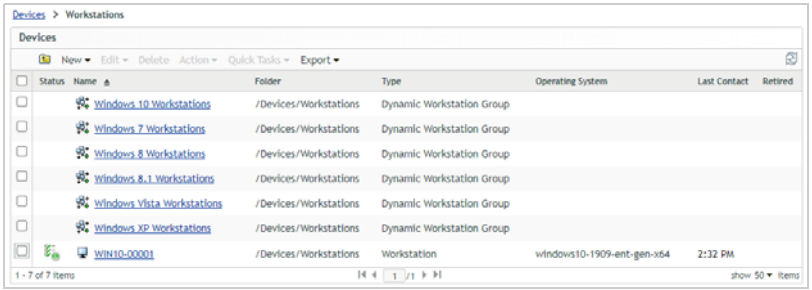
By default, a patch scan runs any time a device's ZENworks Agent performs a refresh, which is scheduled for every 12 hours. We don't want to wait for the scheduled refresh, so well have you manually initiate a patch scan.

1 In ZENworks Control Center, click **Security** > **Getting Started** to display the Getting Started Mitigating Vulnerabilities page.

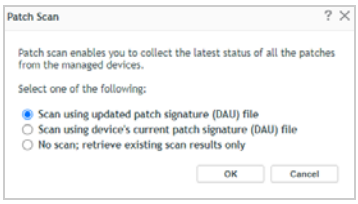


2 Under Device Scan, click **Initiate Patch Scan** to display the Workstations folder in the Devices list.

NAVIGATION TIP: You can go directly to the Workstations list through **Devices** > **Workstations**.

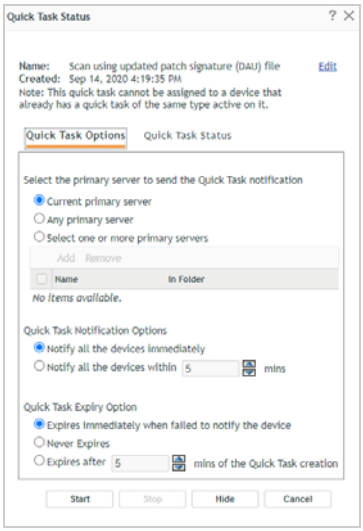


3 Locate your Windows 10 device in the list, select the check box in front of it, then click the **Quick Tasks** menu > **Initiate Patch Scan** to display the Patch Scan dialog.



4 Keep the default selection (**Scan using updated patch signature (DAU) file**) so that the recently created DAU file will be distributed to the device before the scan, then click **OK** to display the Quick Task Status dialog.

Initiating the patch scan is done via a Quick Task. A Quick Task is an task sent from ZENworks Control Center to a device. This dialog lets you configure options for the Quick Task and view the status of the Quick Task.

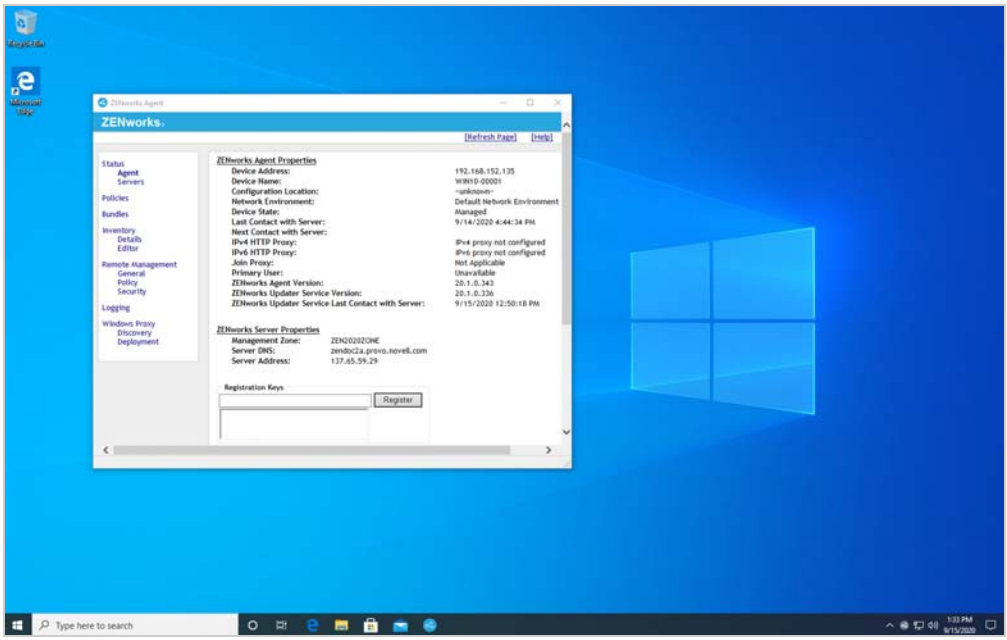


5 Click **Start** to send the Quick Task using the default options.

The task is assigned. When the scan is done, the task status changes to completed. However, it can take some time (10 -15 minutes) to run a scan the first time because the scan engine must be downloaded and then a full scan is performed. So, let's go take a look at what is happening on the device during the scan.

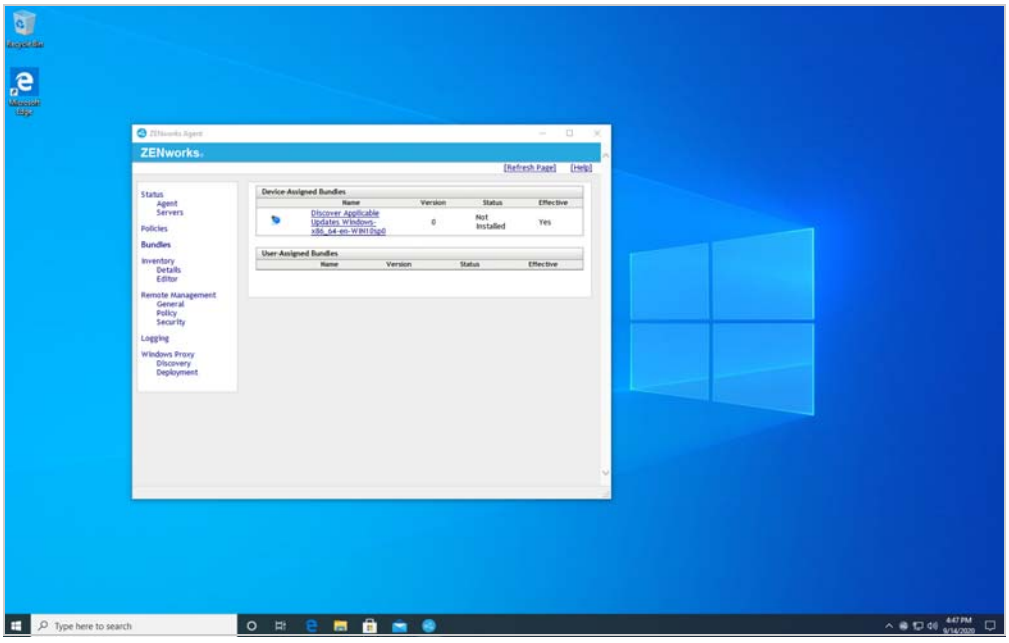
6 At the Windows 10 device:

6a Right-click the ZENworks icon in the Notification tray, then click **Technician Application** to display the ZENworks Agent window.



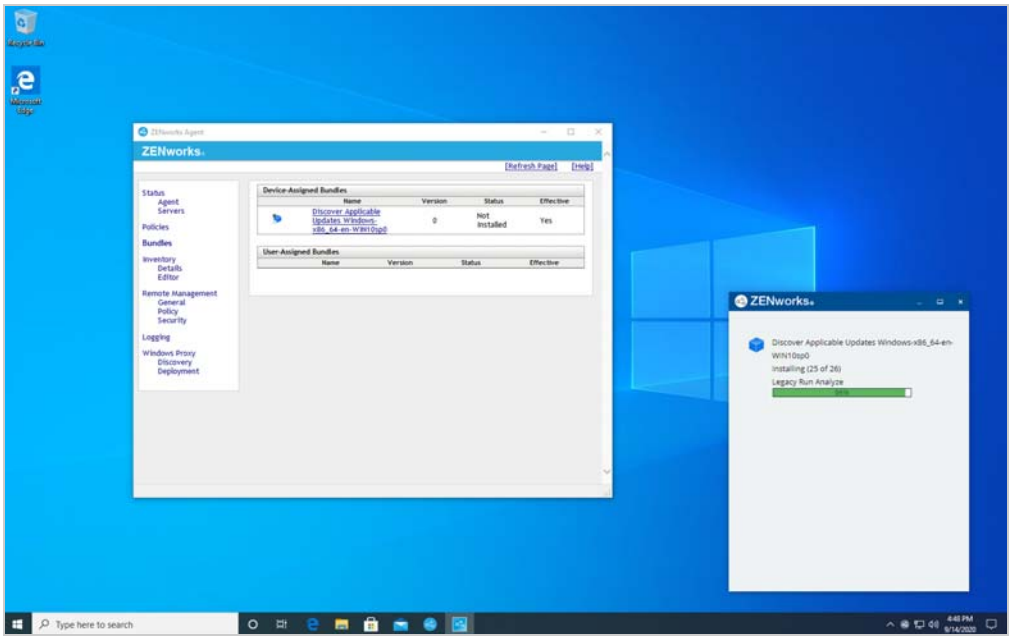
6b In the left-navigation, click **Bundles**.

The Bundles list shows the DAU file that has been assigned and distributed to the Windows 10 device. If it is not yet visible, the Quick Task has not started on the device yet. Wait a few minutes and then click **Refresh Page** (upper-right corner) to refresh the list.

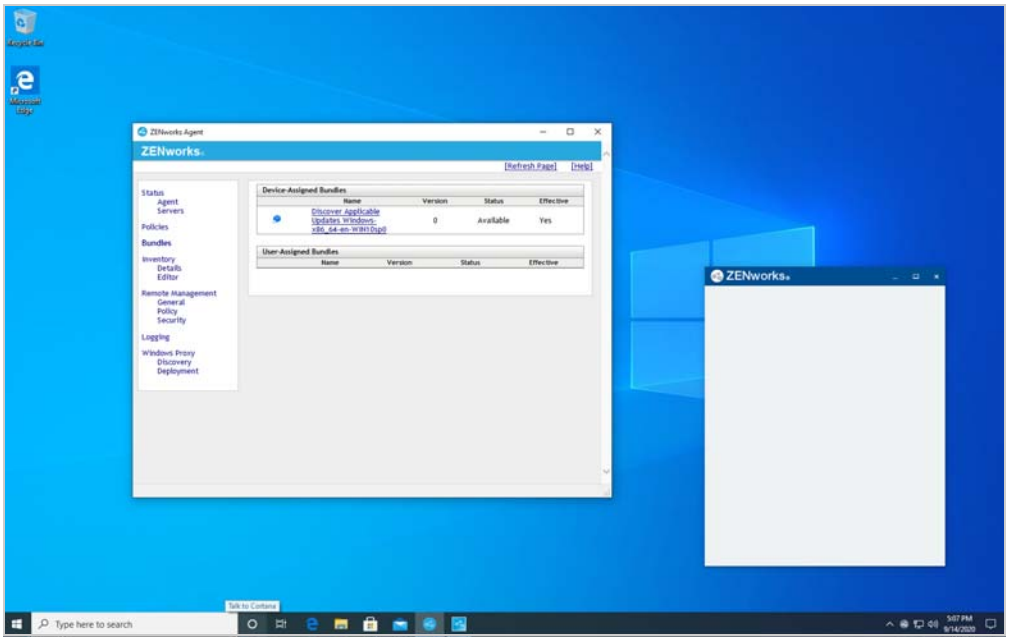


6c Right-click the ZENworks icon in the Notification tray, then click **View Progress**.

The View Progress dialog shows the progress of the installation of the DAU file.



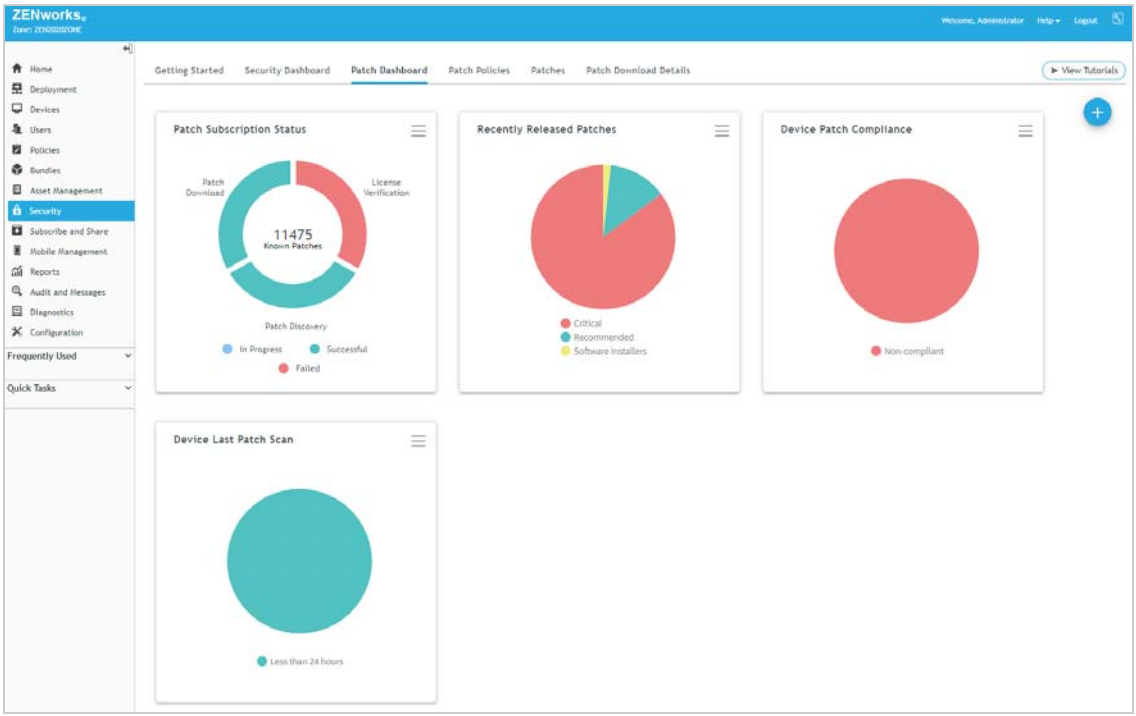
Once the scan completes, the View Progress dialog is cleared and the status of the DAU bundle changes from Not Installed to Available.



7 In ZENworks Control Center, the Quick Task Status shows that the scan is done. Click **Hide** to close the Quick Task Status dialog.

8 After a device is scanned, the ZENworks Agent reports the scan results to the ZENworks Primary Server. Use the Device Last Patch Scan dashlet to verify that the scan results have been reported:

8a Click **Security** > **Patch Dashboard** tab to display the Device Last Patch Scan dashlet.



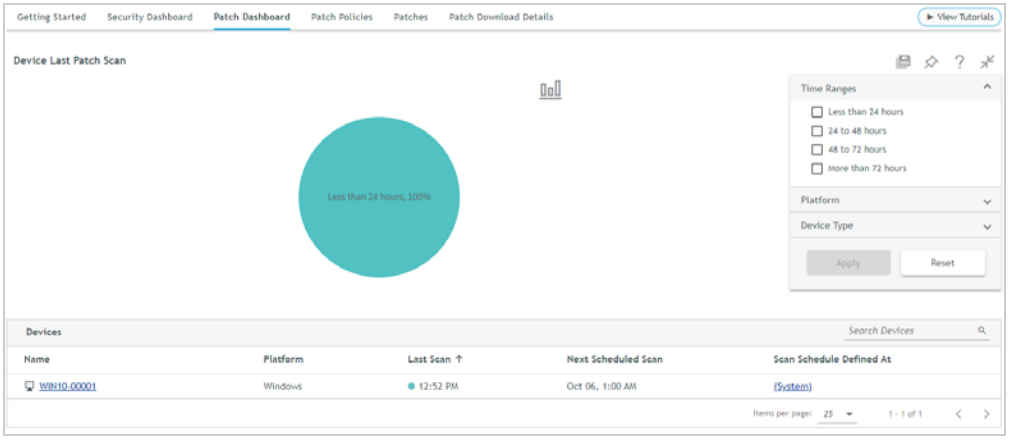
This dashlet is a pie chart that shows how long it has been since devices last performed a patch scan. Typically, the chart includes four segments: *Less than 24 hours*, *24 to 48 hours*, *48 to 72 hours*, and *More than 72 hours*. We're having you use the dashlet to verify that the Windows 10 device has

reported its patch scan, but when your zone includes multiple devices the dashlet also helps you quickly identify devices that haven't scanned within the last 72 hours so you can investigate potential problems.

With only a single Windows 10 device registered and scanned, the chart shows only the one time segment in which the Windows 10 device scan falls. If the Windows 10 device has not reported its scan results yet, the pie chart and grid will not display any data.

8b Click the Device Last Patch Scan dashlet to see the last scan time details.

The Windows 10 device is shown in the Devices list along with its last patch scan time, which should be after you initiated the scan. The last patch scan time is updated at the same time the scan results are uploaded to the server.



8c Click the Collapse icon above the dashlet filter to collapse the dashlet and return to the Patch Dashboard.

Assess Vulnerability Status

With the scan results reported, you're ready to see what patches the device is missing and what security vulnerabilities exist because of the missing patches.

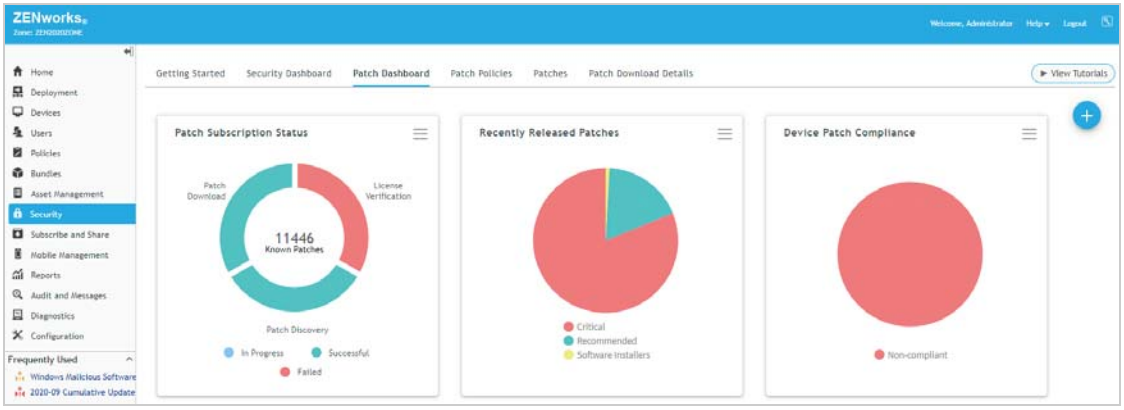
- "View the Patch Status of the Windows 10 Device" on page 28
- "View Patch Status for Individual Patches" on page 30
- "View Security Vulnerabilities" on page 32

View the Patch Status of the Windows 10 Device

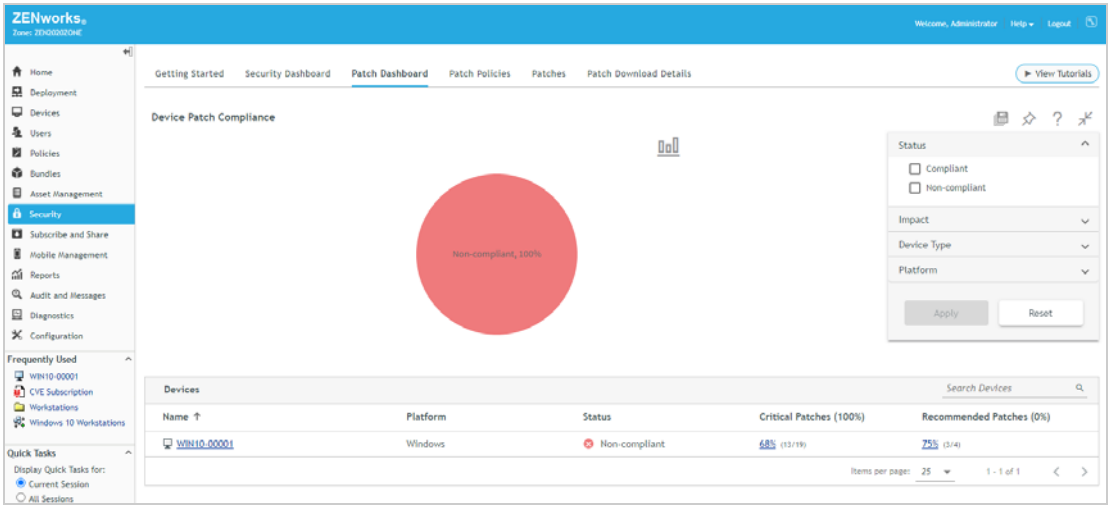
The Device Patch Compliance dashlet is an effective way to see the patch status of your Windows 10 device. The dashlet provides a quick visual of the number of devices that are patch compliant in your zone. A compliant device is one that has all required Critical (security) and Recommended (non-security) patches installed. A non-compliant device is one that is missing at least one required patched. The dashlet lets you drill into each device to see more details and perform patching operations as needed.

1 In ZENworks Control Center, click **Security** > **Patch Dashboard** tab to display the Device Patch Compliance dashlet.

The dashlet is a pie chart with a red segment that represents non-compliant devices and a green segment that represents compliant devices. With only a single Windows 10 device registered and scanned, the chart shows one segment. In the screenshot below, that segment is red because the registered Windows 10 device is not compliant.



2 Click the Device Patch Compliance dashlet to see the patch compliance details.

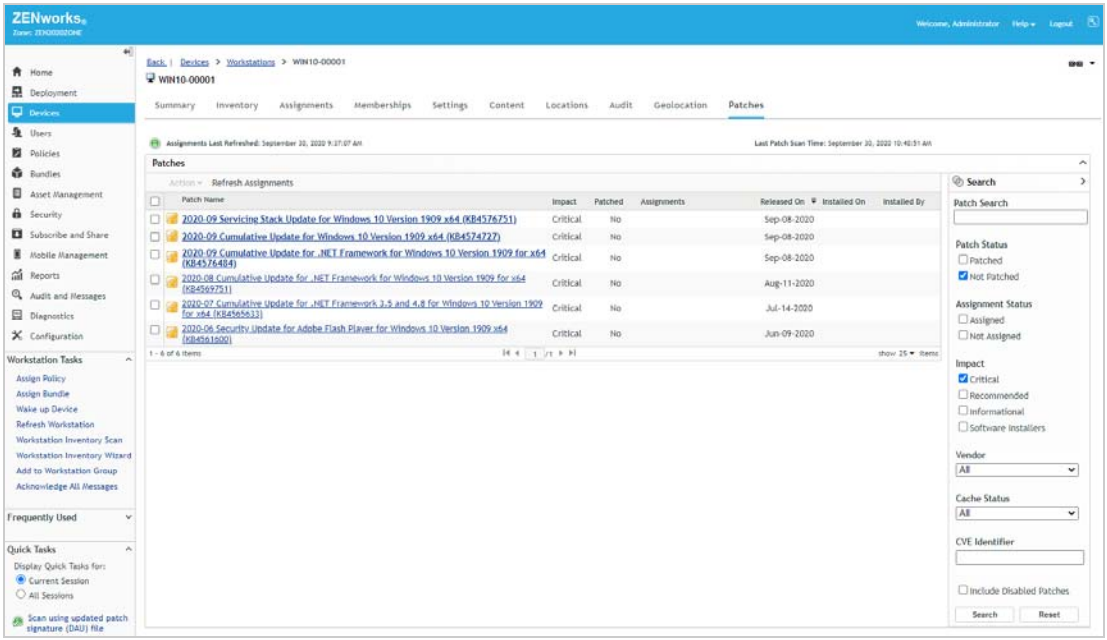


In the example above, the Windows 10 device is listed with a status of *Non-compliant*. By default, compliance requires 100% of all applicable Critical (security) patches to be installed and the device has only 64% (13/19) installed. The default compliance does not require any Recommended patches to be installed, which means that the default compliance is determined strictly from Critical patches.

NOTE: You can change the compliance percentage for both Critical and Recommended patches by using the Dashboard and Trending settings (**Configuration** > **Management Zone Settings** > **Security**).

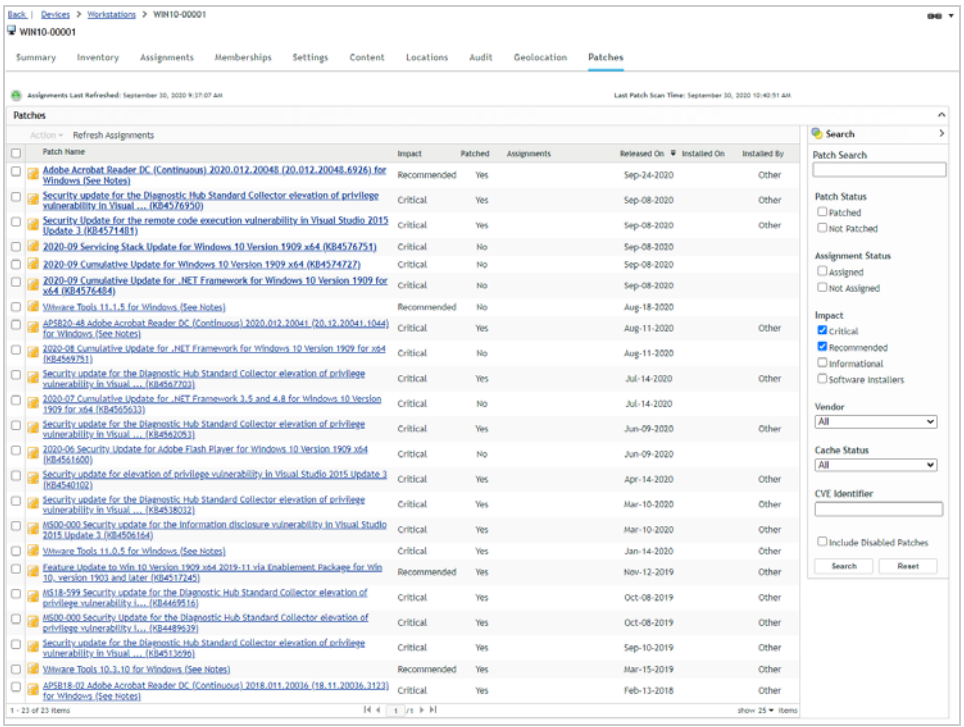
3 Click the **Critical Patches** link (the 64% in the above screenshot) to drill down to the device's Patches page.

The Patches list is filtered to show only the Critical patches that are not installed on the device. At this point, you could use the Actions menu to apply the Critical patches to the device. But don't do any patching right now. We'll have you do that in a little while.



4 In the Search box, deselect **Not Patched** (under Patch Status), select **Critical** and **Recommended** (under Impact), then click **Search**.

The list now displays all Critical and Recommended patches that apply to the device regardless of whether they are installed or not installed.



Notice that ZENworks Patch Management detects installed patches regardless of the installation source. For example, if the device has patches already installed by Windows Update, the Installed By column lists *Other*. When you install patches through ZENworks Patch Management, it shows *ZENworks*.

You'll also want to notice the Assignments column. This column shows whether the patch is assigned to the device via a Patch policy or a Remediation deployment. Only patches that are assigned to the device will be installed. Since you haven't yet created any Patch policies or done any Remediation deployments, none of the patches are assigned. Again, we'll take care of that in a few minutes.

5 Click the **Back** link (in the breadcrumb trail at the top of the page) to return to the Device Patch Compliance dashlet.

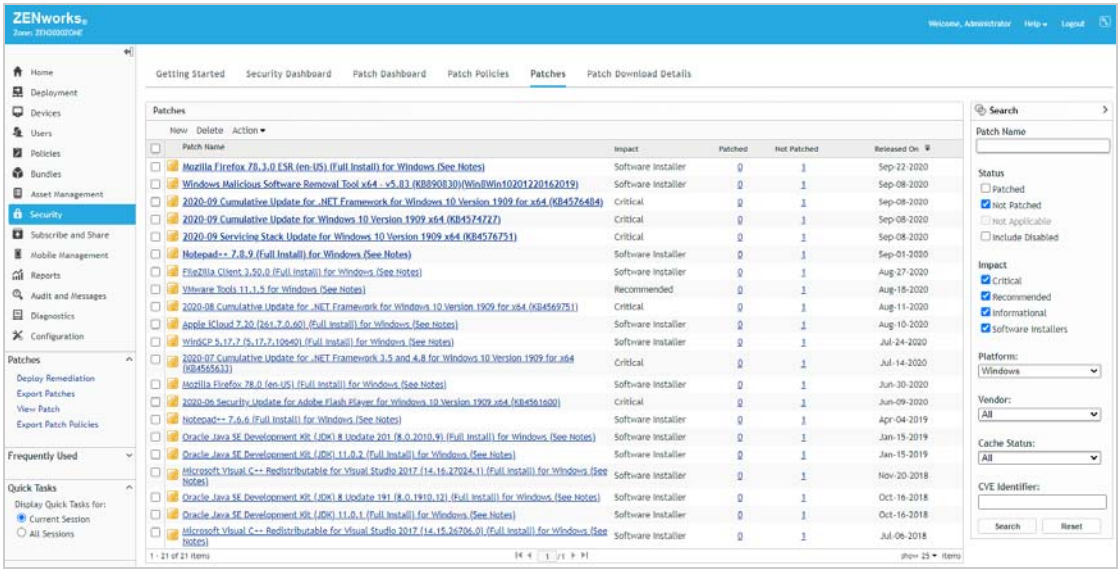
6 Click the Collapse icon above the dashlet filter to collapse the dashlet and return to the Patch Dashboard.

View Patch Status for Individual Patches

While the Device Patch Compliance dashlet lets you assess how well a device is patched, sometimes you need to known the status of a single patch across multiple devices. The zone Patches list lets you view all patches that apply to devices in your zone. For each patch, you can see the number of patched and not patched devices. You can then drill into a patch to see more details and perform patching operations as needed.

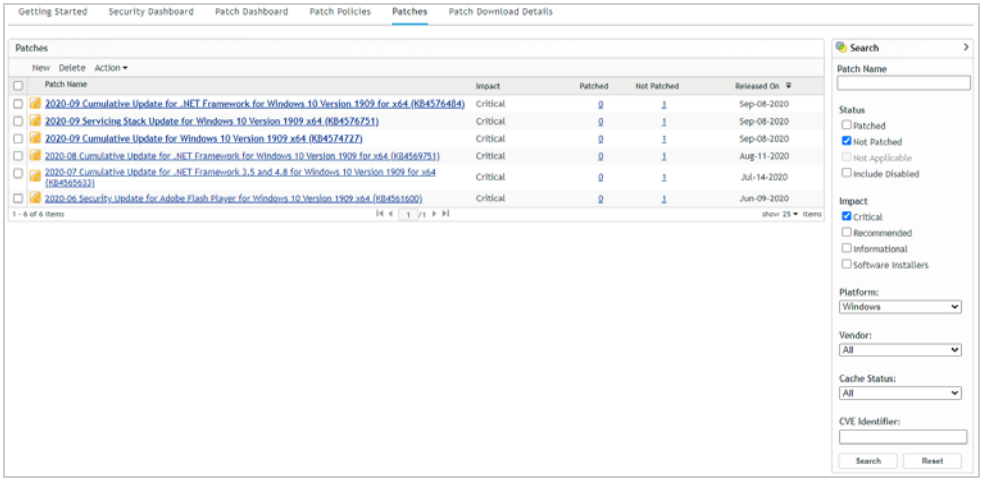
1 In ZENworks Control Center, click **Security** > **Patches** to display the Patches list.

Similar to a device's Patches list, the zone Patches list is filtered to show only the patches that have at least one device on which they are not installed. This is reflected by the device count in the Not Patched column. If you are only using one Windows device for the evaluation, the Not Patched column contains a 1, indicating that the patch is not installed on that one device.



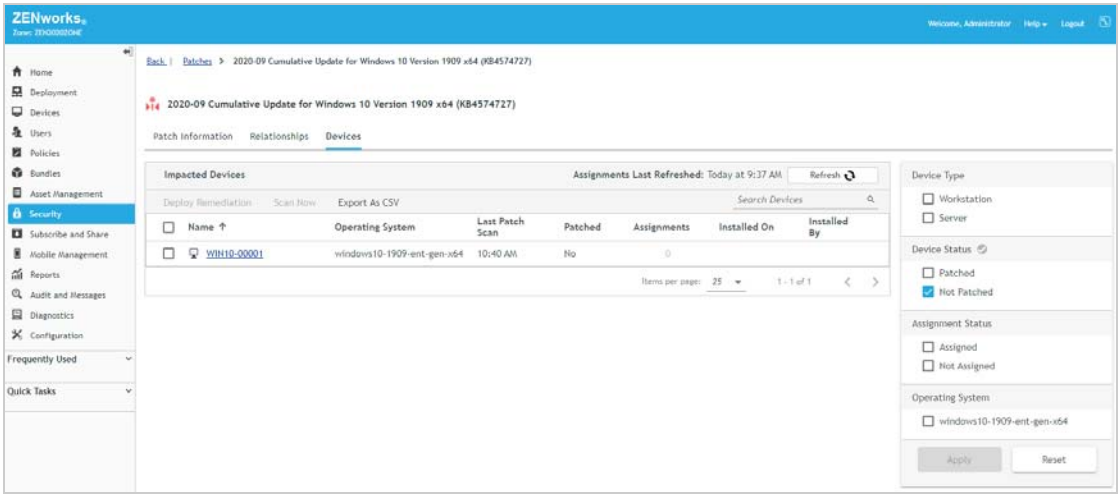
2 In the Search box, deselect **Recommended**, **Informational**, and **Software Installer** (under Impact), then click **Search** to filter the list to show Critical patches only.

At this point, you could use the Actions menu to apply the Critical patches. But don't do any patching right now. We promise that you'll get to that soon, but first there are a few more things we need to show you.



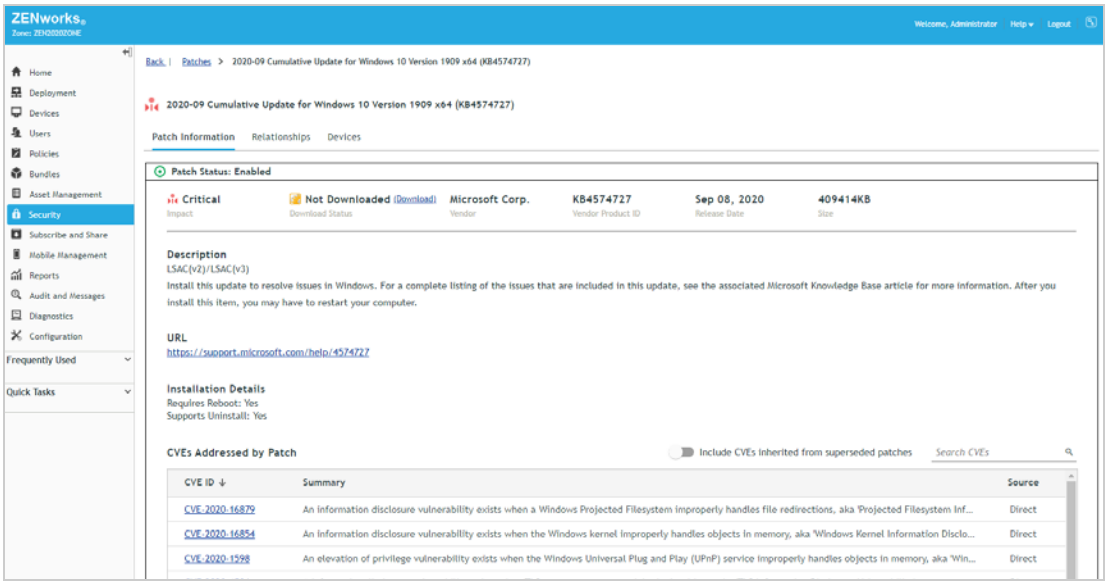
3 Click the Not Patched count (i.e., the 1) for a patch.

The patch's Devices tab is displayed with the list of devices that are not patched. For unpatched device in the list, you can see if the patch is assigned to be installed via a Patch policy or remediation deployment (we'll go over both methods in a little bit). You could also select devices and install the patch either immediately or on a schedule.



4 Click the **Patch Information** tab.

This page provides detailed information about the patch, including the security vulnerabilities (CVEs) addressed by the patch and any older patches that are superseded by the patch.



5 Click the **Back** link (in the breadcrumb trail at the top of the page) to return to the zone Patches list.

View Security Vulnerabilities

So far, we've focused on how you can assess the status of devices from a patch perspective. This perspective can help you monitor and maintain patch currency on devices for both Critical (security) and Recommended (non-security) patches.

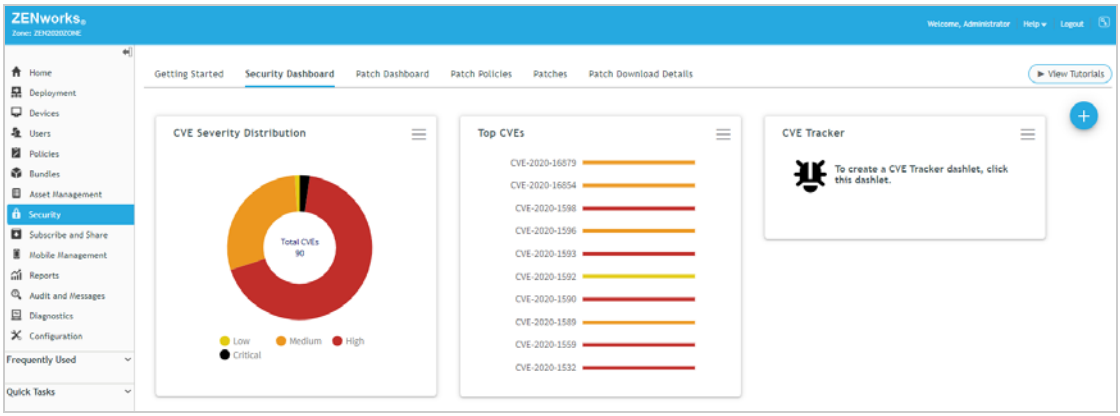
ZENworks Patch Management also lets you assess the status of devices from a security vulnerability perspective. This perspective lets you monitor critical software security exposures, identified by Common Vulnerability and Exposure IDs (or CVE IDs) that you might want to remediate sooner than your next schedule patch maintenance window.

You monitor and remediate security vulnerabilities through the dashlets available on the Security Dashboard.

1 In ZENworks Control Center, click **Security** > **Security Dashboard**.

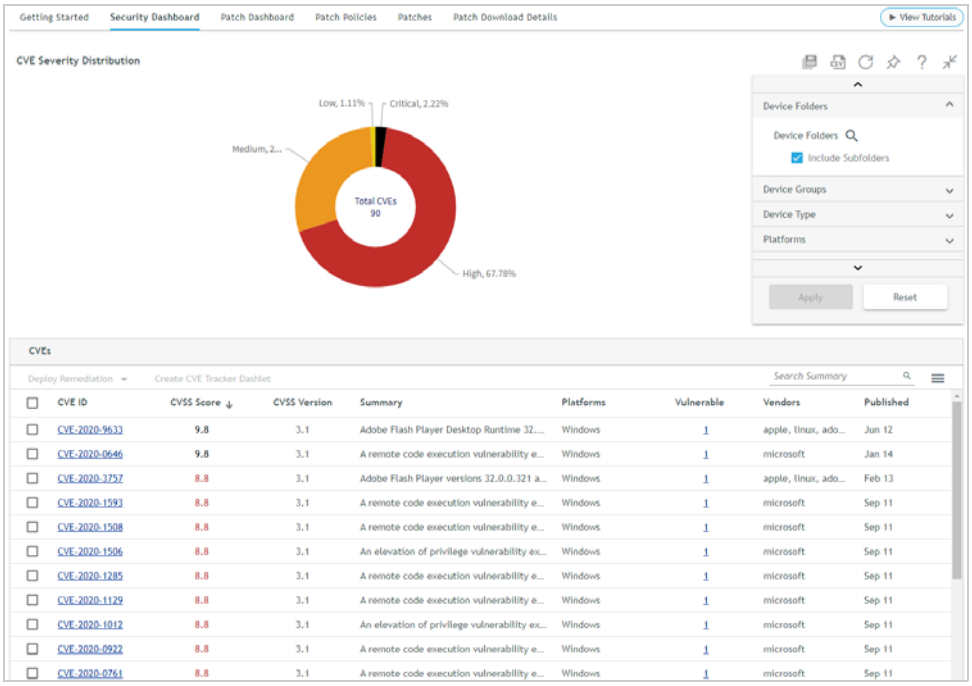
The CVE Severity Distribution dashlet and the Top CVEs dashlet include any CVEs for which you have at least one vulnerable device and for which there is a patch.

NOTE: The Security Dashboard also contains four ZENworks Endpoint Security Antimalware dashlets that are not used during this evaluation. To remove these unconfigured dashlets from the dashboard, click the hamburger menu on the dashlet card, then click Unpin > Security Dashboard. If you are interested in evaluating ZENworks Endpoint Security Antimalware, see the ZENworks Endpoint Security Management Evaluator's Guide.



2 Click the CVE Severity Distribution dashlet to expand it.

The CVE chart organizes CVEs by their severity as determined by the U.S. National Vulnerability Database. In the example below, there are a total of 90 CVEs to which devices are vulnerable. In our case, we have only registered the one Windows 10 device, which means that all 90 vulnerabilities are found on that one device. The CVEs list is sorted by severity score (CVSS) from highest to lowest.

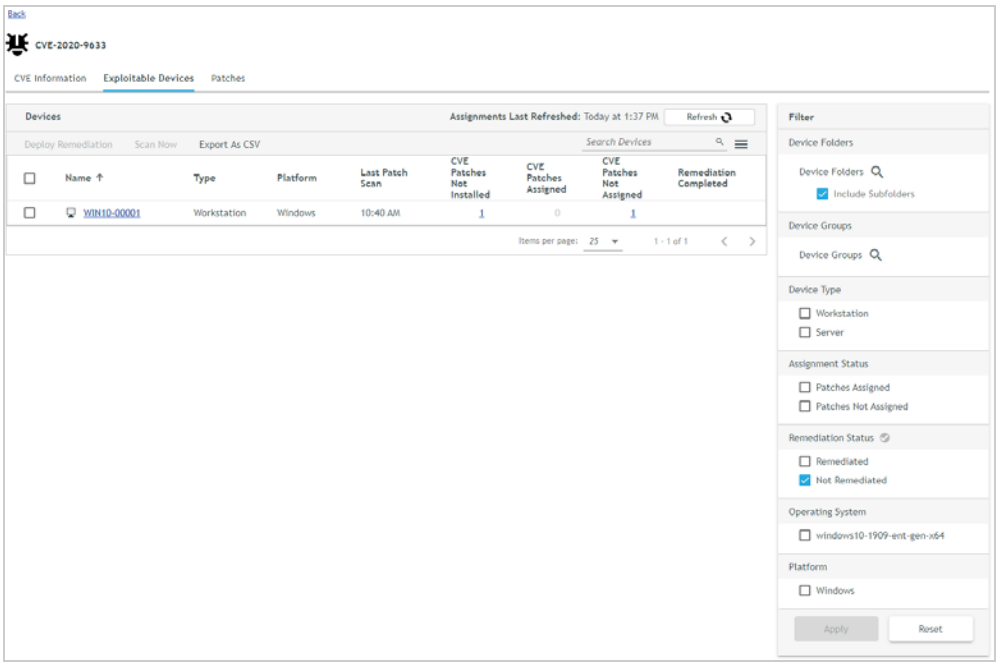


2a Play around with the dashlet chart and filters. Some things to try:

- Click the Critical (black) segment of the chart to list only the CVEs with Critical severity. Click the segment again to deselect it and return the chart to its default state.
- Click the Published column to sort the CVEs by their publish dates.
- In the Filters list, scroll to the Vulnerability Status filter, click the filter to expand it, deselect the **CVEs with Vulnerable Devices** option, then click the **Apply** button to apply the filter. The dashlet now displays all CVEs that are applicable to the Windows 10 device, even the ones to which the device is no longer vulnerable because the needed patches have already been installed. Click **Reset** > **Apply** to return the dashlet to its default state.

2b In the CVEs list, click the Vulnerable number (i.e., 1) for one of the CVEs to display the CVE details.

The CVE's list of exploitable devices is shown. In some cases, a CVE can require multiple patches to fix it, so each device lists the number of CVE patches not installed. It also shows the number of patches assigned to be installed (via a Patch policy or Deployment remediation) and the number of patches not assigned. This assignment status helps you know if your current patching measures are sufficient to remediate the device or if you need to take additional steps.



2c Click the **Patches** tab to display the patches that fix the CVE.

2d Click the **CVE Information** tab to display information provided by the National Vulnerability Database.

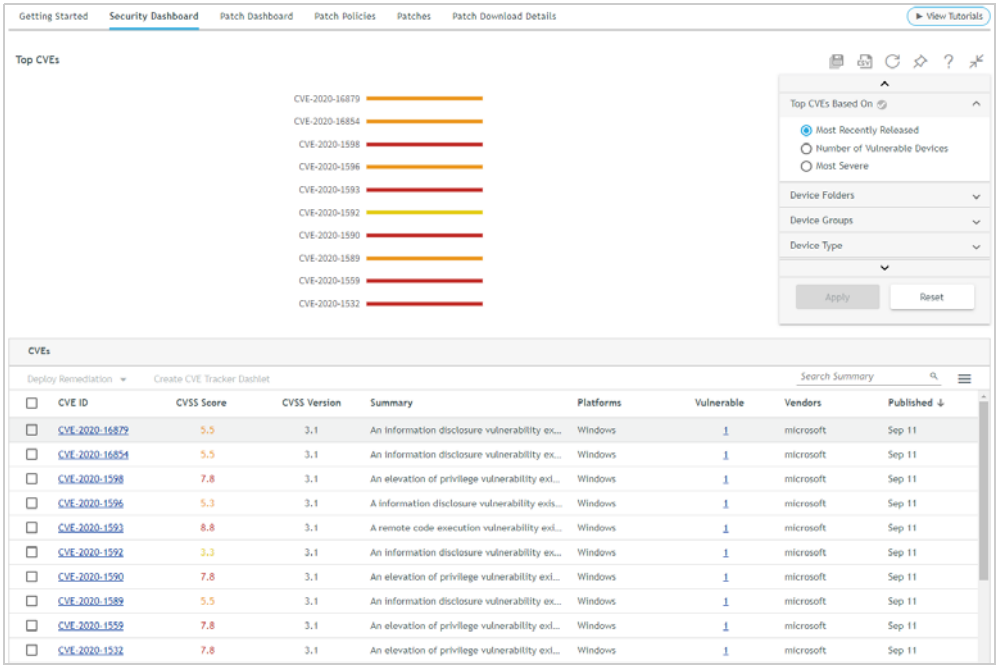
2e Click the **Back** link (in the breadcrumb trail at the top of the page) to return to the CVE Severity Distribution dashlet.

2f Click the Collapse icon above the dashlet filter to collapse the dashlet and return to the Security Dashboard.

3 Click the Top CVEs dashlet to expand it.

The CVE chart organizes the CVEs by most recently published. This view is useful for seeing how new CVEs impact your devices. However, one of the great benefits of the Top CVEs dashlet is that you can customize it to list the top CVEs according to severity score or by number of vulnerable devices. Using those views,

you can see how the most severe CVEs impact your devices and which CVEs have the most vulnerable devices. And you can save each customized dashlet separately so you could actually have three (or more) Top CVE dashlets. One by recently published, one by severity, and one by vulnerable devices.



3a Play around with the dashlet chart and filters. Some things to try:

- Mouse over a CVE bar in the chart to see the number of devices that are vulnerable to the CVE.
- In the Filters list, change the Top CVEs Based On filter to **Most Severe**, then click the **Apply** button to apply the filter. The dashlet now displays CVEs from highest severity score to lowest.
- Click the Save As icon above the dashlet filter, enter `Top CVEs by Severity` for the dashlet name, then click **OK** to save the customized dashlet. The default Top CVEs dashlet remains unchanged and the customized dashlet is saved as a new dashlet.
- In the CVEs list, click the Vulnerable number (i.e., 1) for one of the CVEs. As with the CVE Severity Distribution dashlet, this takes you to the CVE details where you can get more information about the CVE, the vulnerable devices, and the patches that remediate the CVE.

3b Click the Collapse icon above the dashlet filter to collapse the dashlet and return to the Security Dashboard.

If you saved a custom dashlet, you'll notice that both dashlets are now displayed on the dashboard. You can drag and drop dashlets to rearrange them. You can also unpin dashlets from the Security dashboard and re-pin dashlets by clicking the icon.

Deploy Maintenance Patches

Keeping software up-to-date is a key to mitigating both security vulnerabilities and operational issues on devices. This includes regularly updating a device's operating system software and applications.

ZENworks Patch Management reduces the burden of maintenance patching by enabling you to create rules-based policies that automatically select and install the patches that meet the rule criteria. You determine how often a policy is rebuilt to include newly released patches and how often the policy's patches are installed on devices.

In this part of the evaluation, we'll have you create a Patch policy to deploy the current Windows 10 cumulative update. Before you do that, however, we'll have you create a Patch Tracker dashlet that you can use to more easily track the installation status of the cumulative update on devices. And, just in case you need to install a patch that isn't part of a Patch policy, we'll show you how to do a manual deployment as well.

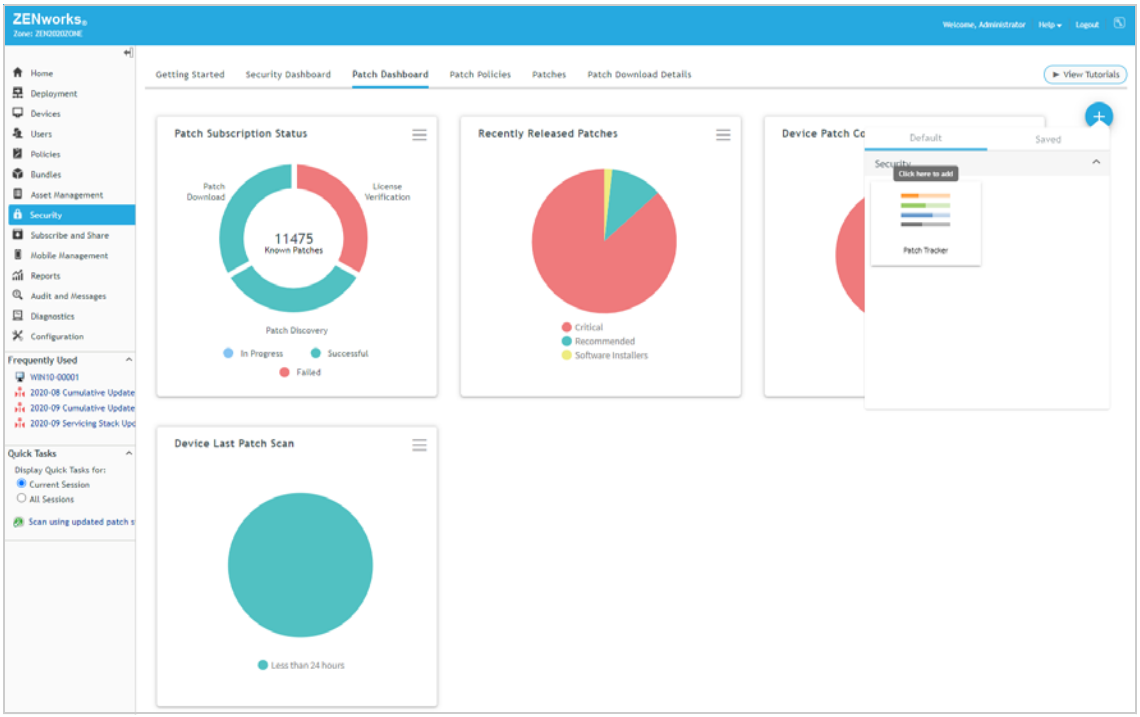
- "Create a Patch Tracker" on page 37
- "Automate Maintenance Patching with Policies" on page 41
- "Manually Deploy Remediations" on page 53

Create a Patch Tracker

To show you how the Patch Tracker dashlet works, we'll have you create a tracker for the current Windows 10 cumulative update. Then, in the next section (Automate Maintenance Patching with Policies), we'll apply the cumulative update and you can see the patch results in the tracker.

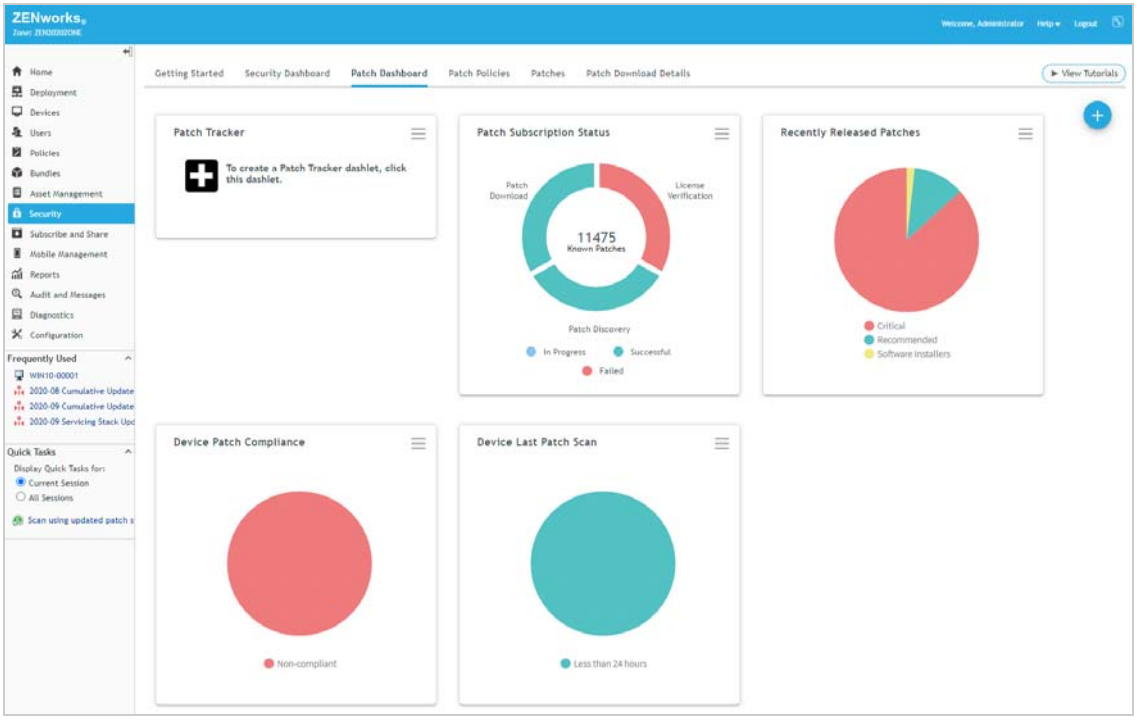
1 In ZENworks Control Center, click **Security** > **Patch Dashboard**.

By default, the Patch Tracker dashlet is not pinned to the Patch Dashboard. You have to add the dashlet from the + icon, shown expanded below.

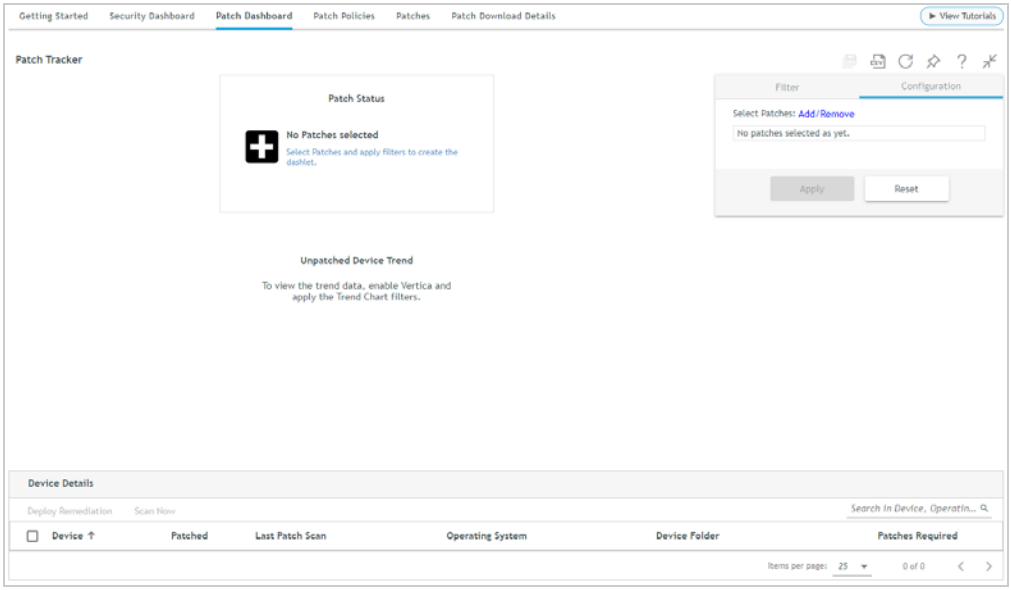


2 Click the icon, then click Patch Tracker to add the dashlet.

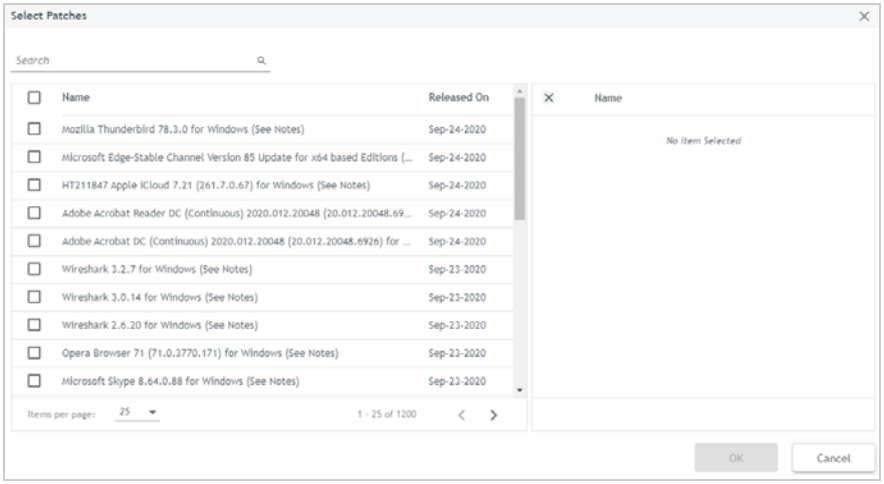
The Patch Tracker dashlet is different than the other dashlets in that it is a *template* dashlet. You have to configure the template dashlet to include the patches you want to track and then save it as a new dashlet.



3 Click the Patch Tracker dashlet to expand it.

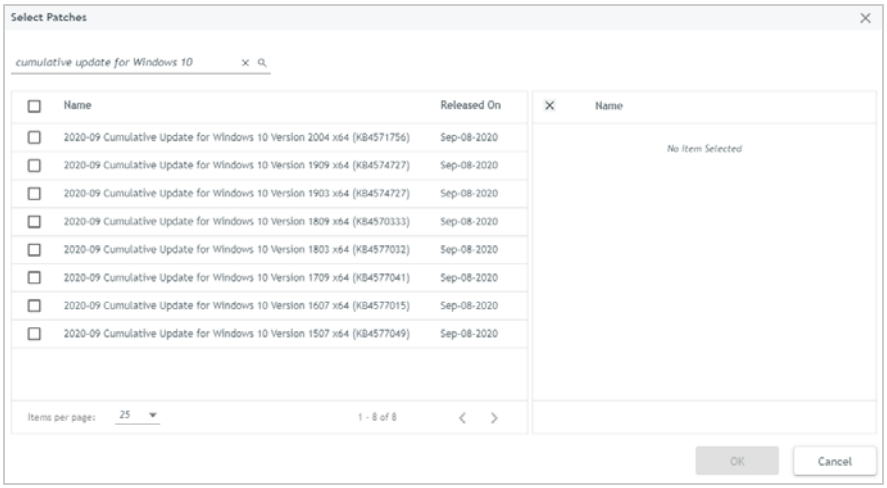


4 In the Configuration pane (right-side), click **Add/Remove** to display the Select Patches dialog.



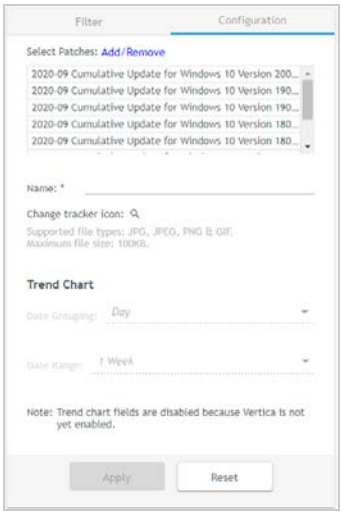
5 In the Search field, enter `cumulative update for Windows 10` to filter the list.

The list shows all of the most recently released Windows 10 cumulative update versions.



6 Select all of the versions, then click **OK** to add them to the tracker.

The Configuration pane lists the selected patches.

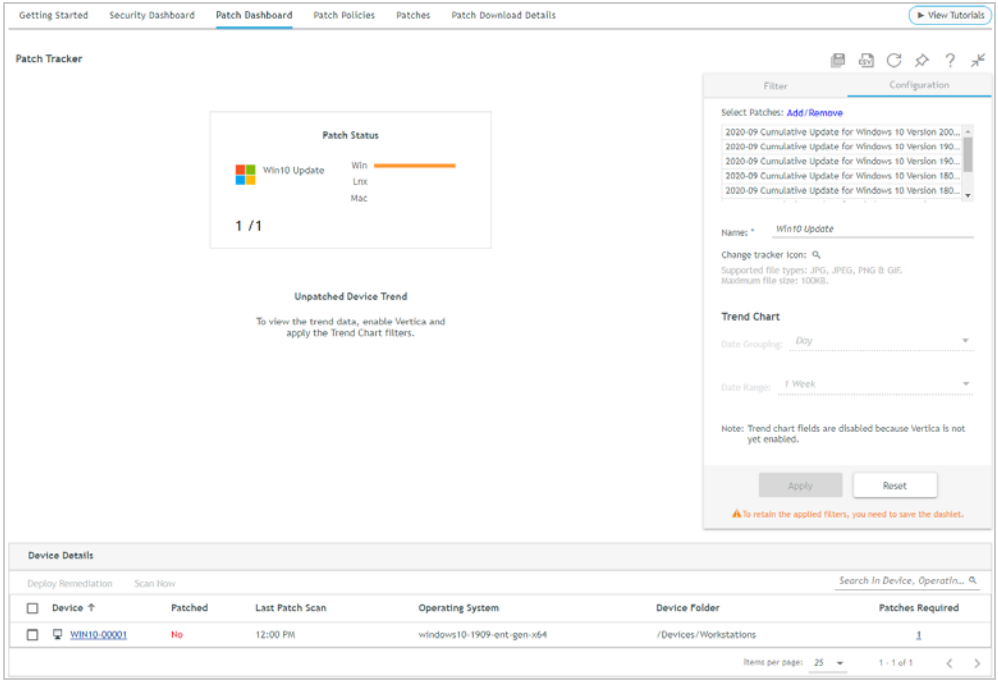


7 In the **Name** field, enter `Win10 Update`.

8 (Optional) In the **Change tracker icon** field, click  to change the default icon  to another icon you'd prefer. You must supply the icon.

9 Click **Apply** to apply the configuration settings.

Any device to which one of the tracker's patches applies is displayed in the Device Details list. In our case, the list shows the single Windows 10 device we registered.



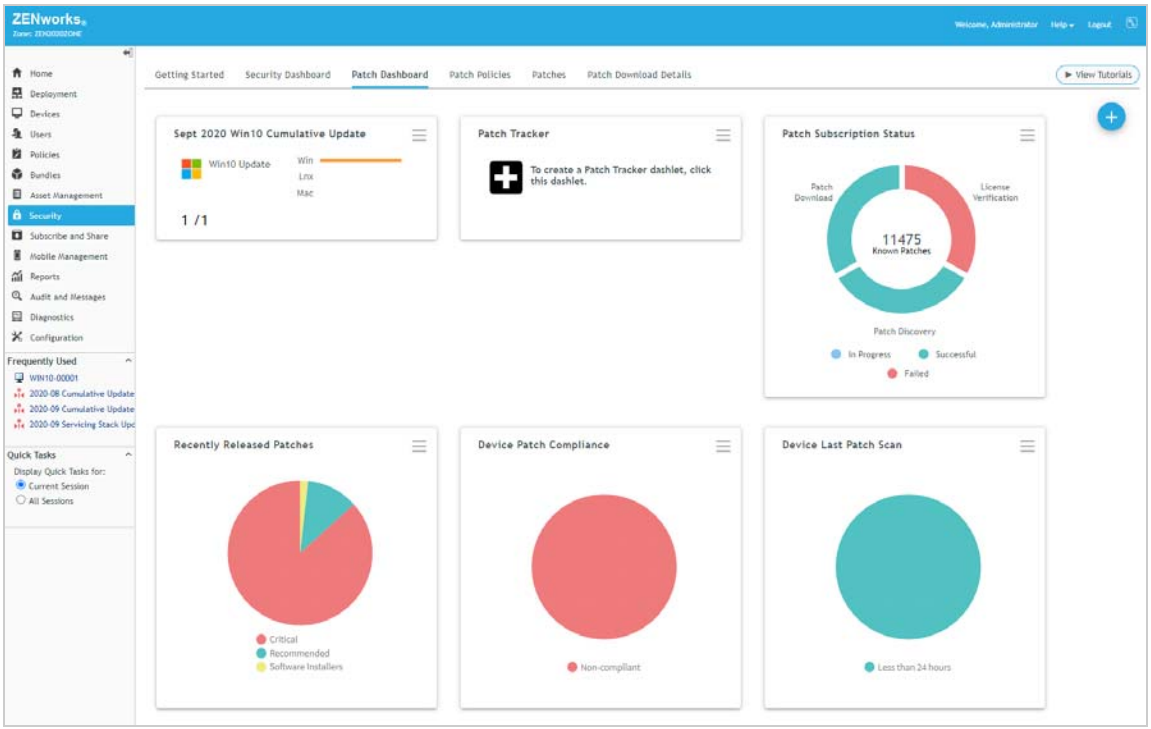
Because we are primarily concerned with unpatched devices, the Patch Status chart shows the number of unpatched devices out of the total applicable devices (1/1). If you mouse over the Windows bar, you will see "1 unpatched devices of 1".

You should also note that the dashlet can include a second Unpatched Device Trend chart. This chart displays the number of unpatched devices over a period of time so that you can see how your device patching is progressing. Because storing and displaying trend data can impact the ZENworks database performance, a separate Vertica database is required for trend data. We won't set it up for this evaluation.

10 To save the dashlet, click (above the dashlet filter list), enter *Month\Year* `Win10 Cumulative Update` for the dashlet name, then click **OK**. For example, `Sept 2020 Win10 Cumulative Update`.

11 Click the Collapse icon above the dashlet filter to collapse the dashlet and return to the Patch Dashboard.

The new dashlet is displayed along with the default Patch Tracker dashlet.



Here are a few other tips for using the Patch Tracker dashlet:

- You can keep the default Patch Tracker dashlet pinned to the dashboard, or you can use the menu on the dashlet to unpin it from the Patch dashboard until you need to create another Patch Tracker dashlet.
- As an alternative, you can create Patch Tracker dashlets directly from the zone Patches list and Recently Released Patches dashlet by selecting a patch (or multiple patches) and using the Create Patch Tracker Dashlet option.

Automate Maintenance Patching with Policies

Now that you have a Patch Tracker dashlet to monitor the installation status of the current Windows 10 cumulative update, go ahead and complete the tasks in the following sections to create a Patch policy containing the cumulative update and apply it to your Windows 10 device:

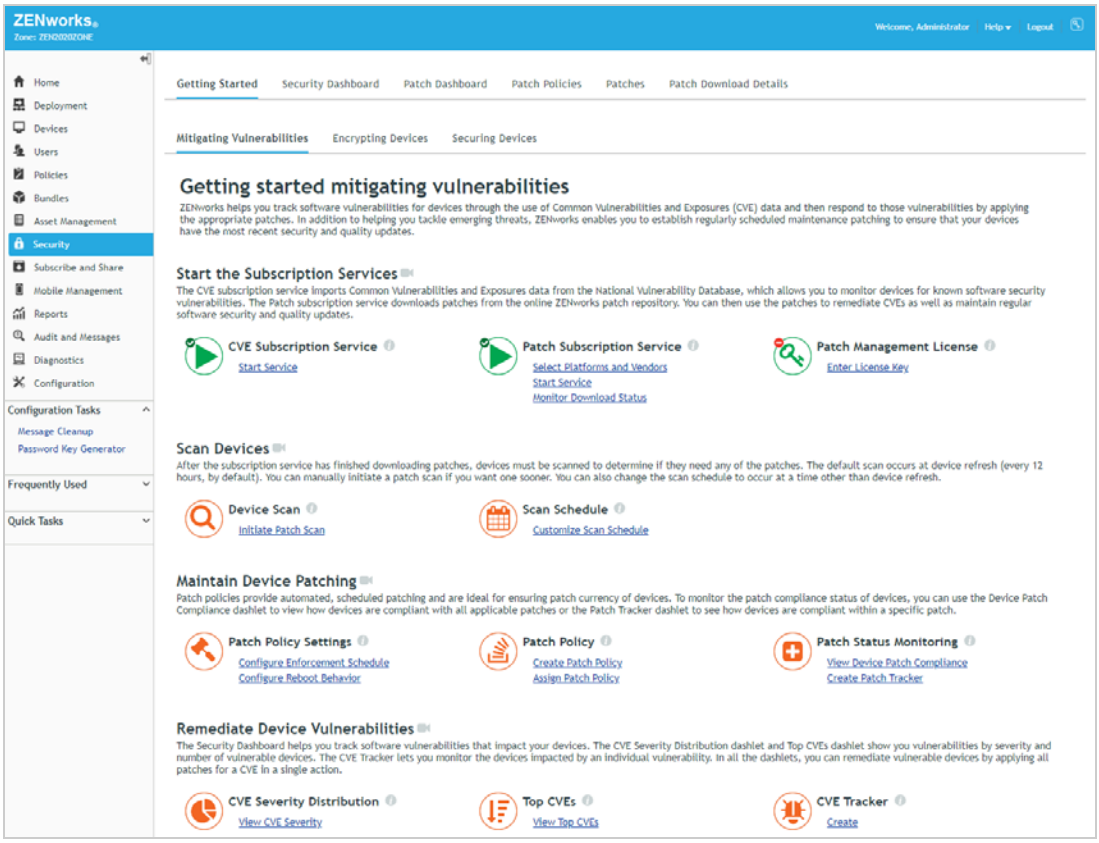
- "Configure Patch Policy Settings" on page 42
- "Create a Patch Policy" on page 44

- “Apply the Patch Policy” on page 49
- “View the Patching Results” on page 51

Configure Patch Policy Settings

Before you create Patch policies, there are a few policy settings that you should be aware of. These setting control when policies are enforced on devices (i.e. the policy’s patches are installed) and how reboots are handled.

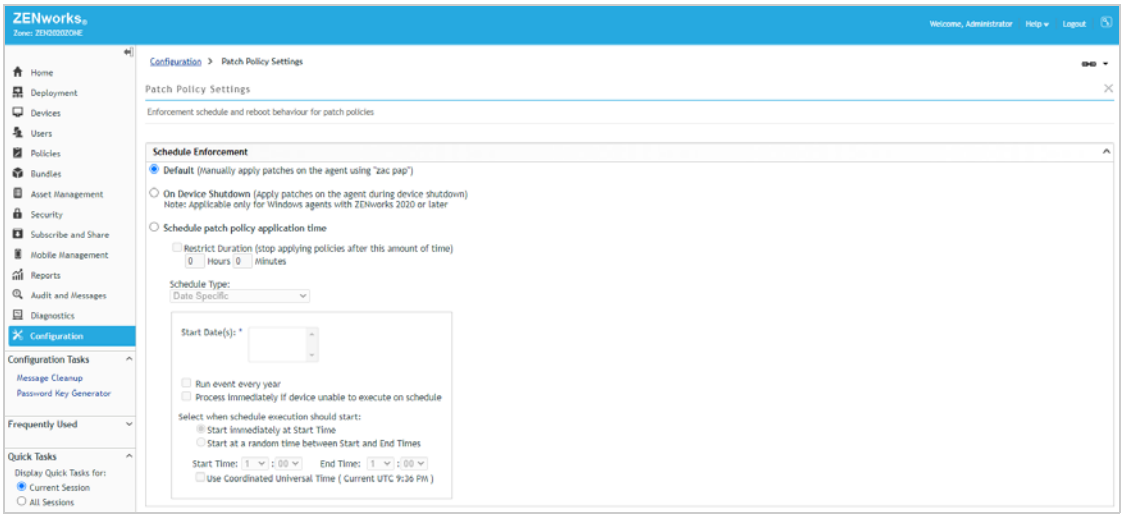
1 In ZENworks Control Center, go to the Security Getting Started (**Security** > **Getting Started** > **Mitigating Vulnerabilities**).



2 Under Patch Policy Settings, click **Configure Reboot Behavior** to display the Patch Policy Settings page.

NAVIGATION TIP: You can go directly to the Patch Policy Settings page through **Configuration** > **Management Zone Settings > Security > patch Policy Settings**.

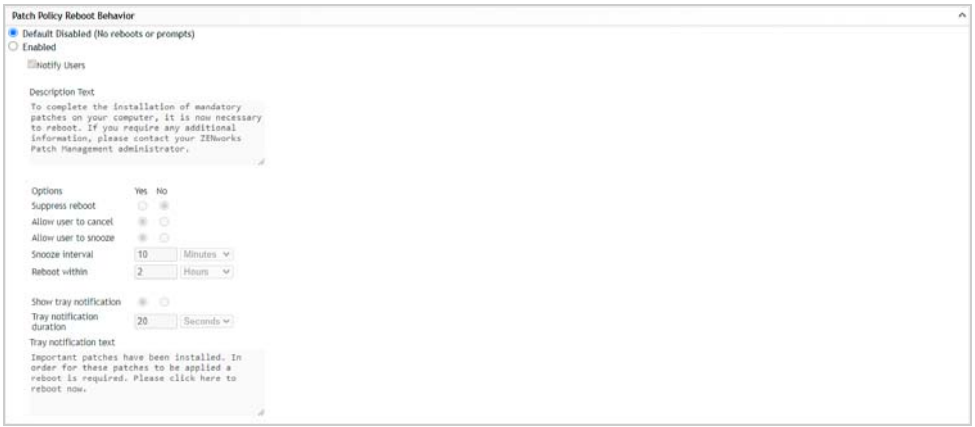
The Patch Policy Settings let you configure the enforcement schedule for policies as well as the device's reboot behavior after policies are applied.



3 Leave the policy enforcement schedule set as is.

By default, Patch policies are only enforced when the *zac pap* command is manually run from the command line of a device. Normally you would want to change this to an automated recurring schedule, but for this evaluation we're going to use the *zac pap* command so there is no need to change the schedule.

4 Scroll down the page to display the Patch Policy Reboot Behavior settings.



By default, no reboot occurs after the patches are applied and no reboot prompt is displayed to the user. Any patch that requires a reboot to finish the installation will not be completely installed until a reboot occurs by some other means. Let's change the setting to prompt the user to reboot.

5 In the Patch Policy Reboot Behavior settings, click **Enabled**.

The Notify Users setting is turned on by default, which results in users being prompted to reboot.

6 Set **Show tray notification** to **No** and leave the rest of the options as is.

This supresses the tray notification and automatically displays the Reboot dialog to the user.

7 Click **OK** to save the changes you made to the Patch policy settings and to return to the Getting Started.

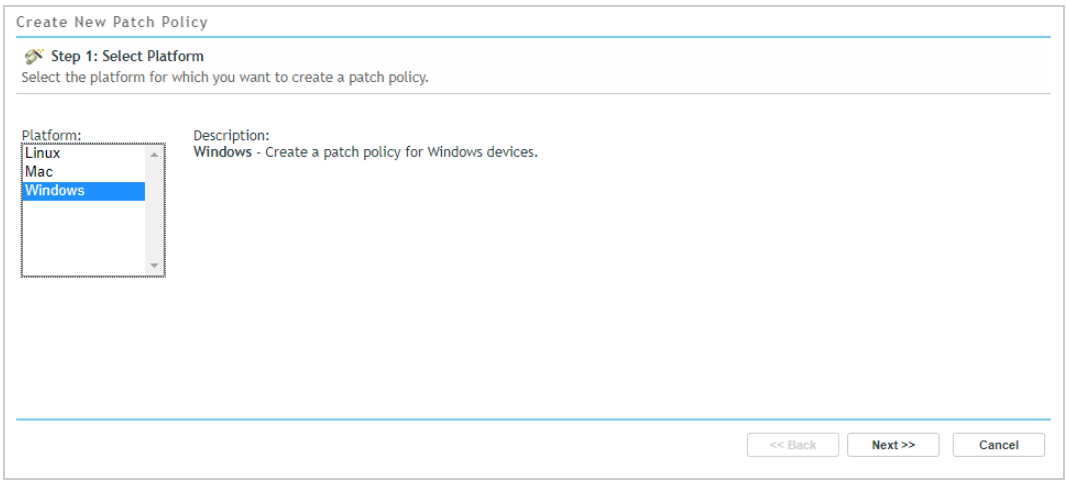
Create a Patch Policy

As mentioned earlier, a Patch policy is a set of rules that defines which patches are included in the policy. When the policy is assigned to a device, ZENworks Patch Management applies any of the policy's patches required by the device.

Patch policy rules allow you to use a variety of criteria for matching patches, including Vendor, Age, Architecture, Impact, and Patch Name. For example, using the Vendor, Impact, and Age criteria, you could create a Patch policy that includes all Microsoft Critical patches that are older than 7 days. Or, you could create a policy that installs all Google Chrome updates.

We're going to create a simple policy that includes the current Windows 10 cumulative update.

1 On the Security Getting Started page under Patch Policy, click **Create Patch Policy** to display the Create New Patch Policy wizard.



2 Select **Windows** to create a Patch policy for Windows devices, then click **Next**.

3 Name the policy *Windows 10 Cumulative Update*, then click **Next**.

4 Define the rules for the policy:

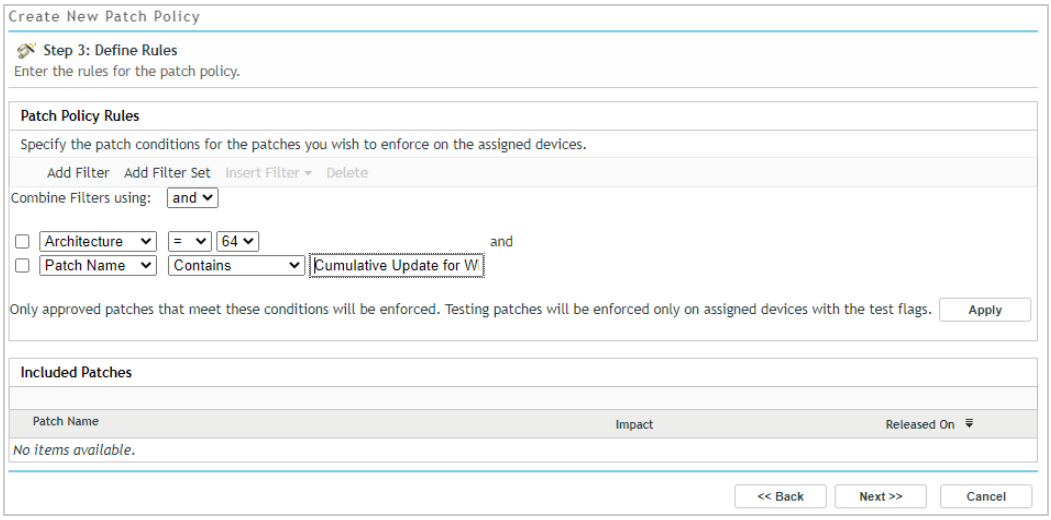
4a In Patch Policy Rules, click **Add Filter**.

4b Select the **Architecture** filter, then select **64** to include only the updates for 64-bit devices.

4c Click **Add Filter** to add a second filter.

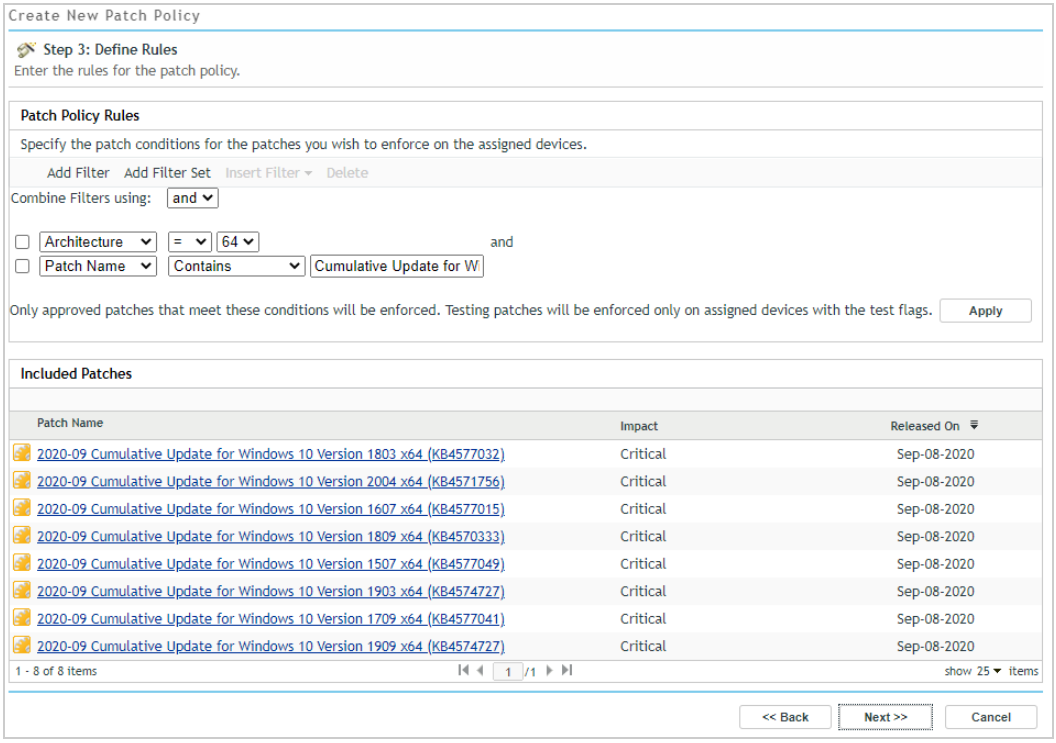
4d Select the **Patch Name** filter and enter *Cumulative Update for Windows 10*.

Your filter should now look like this:



4e Click **Apply**.

The rules are applied to all available patches. Patches that match the rules are displayed in the Included Patches list.



In this case, the policy criteria matches the updates for all currently supported Windows 10 versions. This allows you to assign the policy to all Windows 10 devices and have the correct update applied regardless of the device's version.

4f Click **Next** to display the Summary page.

5 On the Summary page:

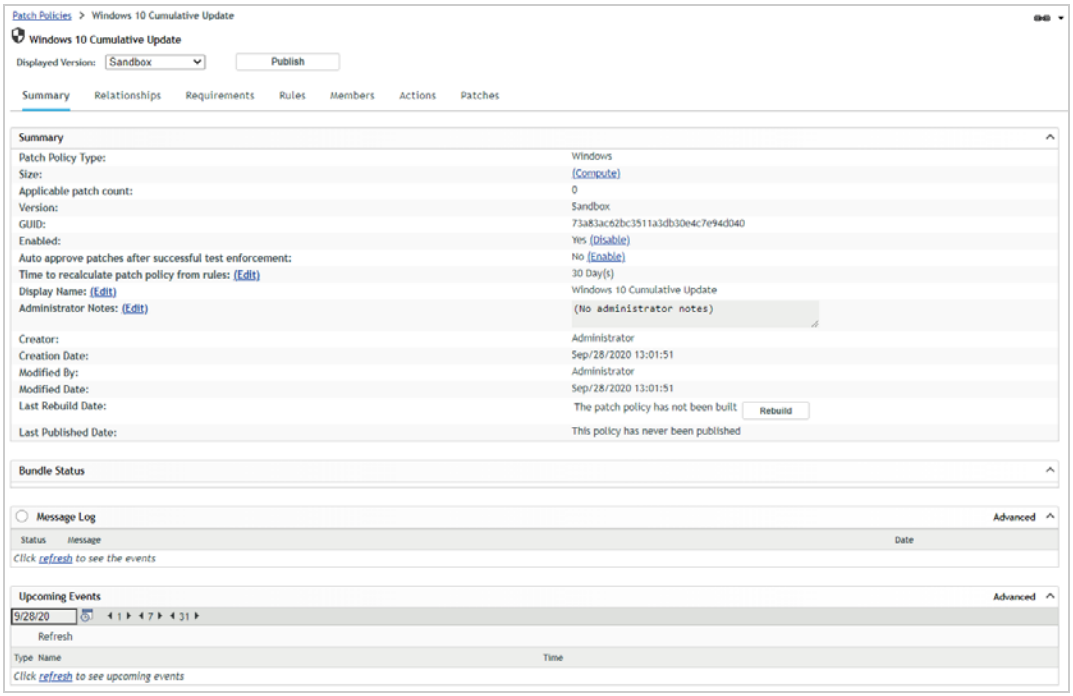
5a Leave the **Recalculate after 30 days** option set to **30 days**.

The Recalculate setting determines how often the policy rules are applied to determine the patch membership (in other words, to add new patches and remove disabled or superseded patches).

5b Enable the **Rebuild policy on creation** option.

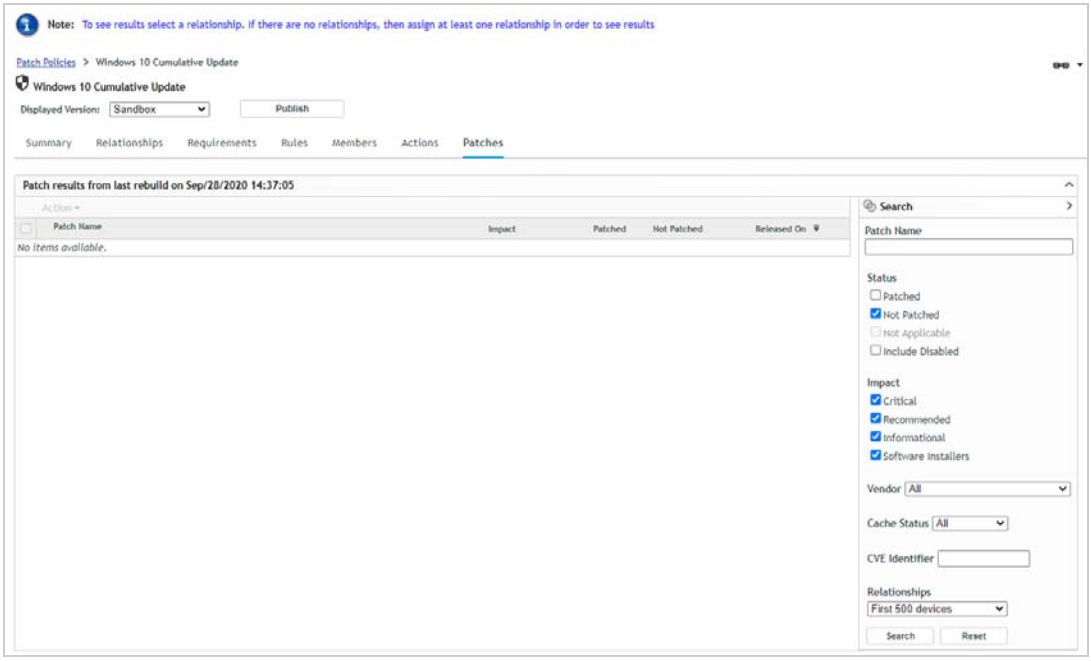
Once you define the policy, the policy has to be built in order to include the patches that match the rules. Selecting this option simply causes the build process to occur as part of the policy creation. If you don't select the option, you can use the Rebuild option in the policy after it is created.

5c Select the **Define Additional Properties** option, and then click **Finish** to create and display the Patch policy.



6 Click the **Patches** tab.

You'll notice that there are no patches listed. That is because the Patches list only shows the policy's patches that apply to assigned devices. At this point, we haven't assigned the policy to any devices, so no patches are listed.

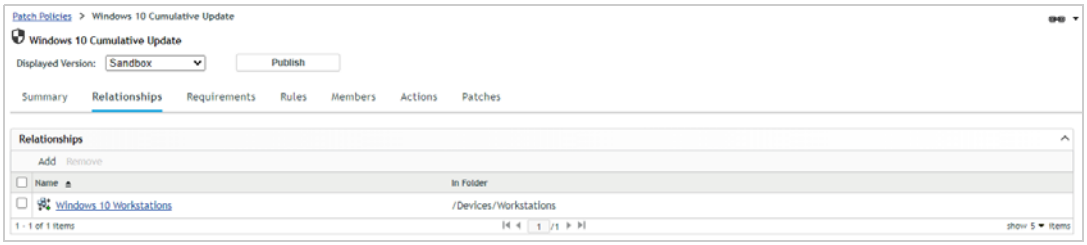


7 Assign the Patch policy:

7a Click the **Relationships** tab.

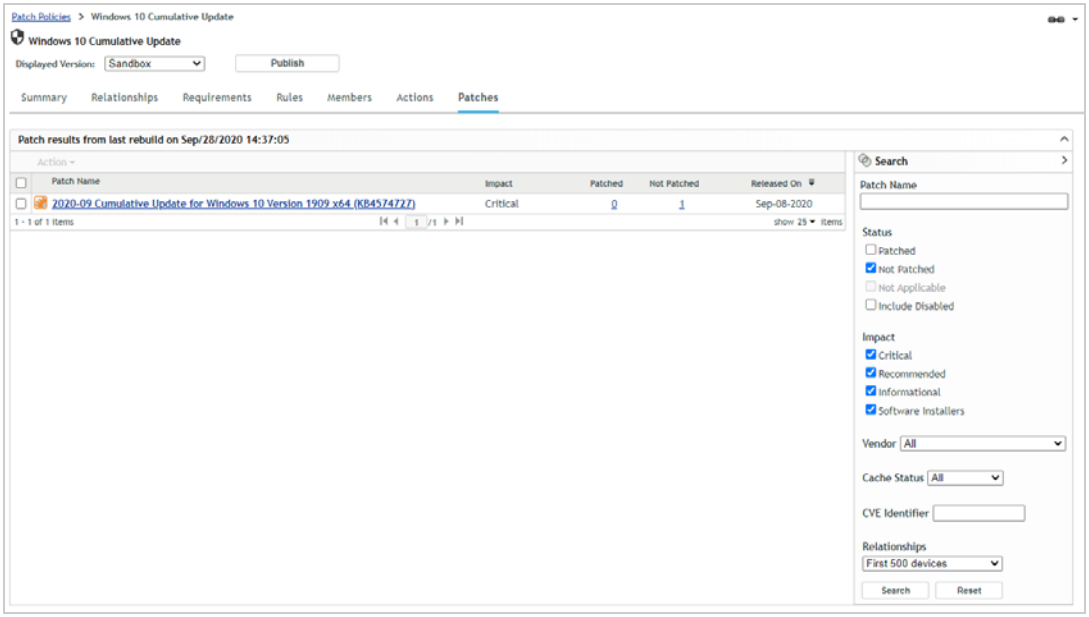
7b Click **Add**, drill down into the Devices folder and then into the Workstations folder, then select the **Windows 10 Workstations** dynamic group and click **OK** to add the group to the Relationships list.

All Windows 10 workstations that you register in the zone are automatically added to the Windows 10 Workstations dynamic group. We could assign the policy directly to the device, but by assigning it to the dynamic group the policy will automatically be assigned to any Windows 10 workstations you register later.



8 Click the **Patches** tab.

The Patches list now displays all of the policy's patches that are applicable to the Windows 10 device. In this case, the list shows the Windows 10 Cumulative Update for the Windows 10 version running on the Windows 10 device.



9 Mouse over the icon in front of the patch to see its current download status.

The initial patch discovery process only downloads the signatures for applicable patches. The actual patch content is not downloaded until the patch is included in a Patch policy and an assigned device needs it. You can also select patches and initiate a manual download of their content. The download icon turns green once the patch content is downloaded, but you don't need to wait for it to download. Go ahead with the next step.

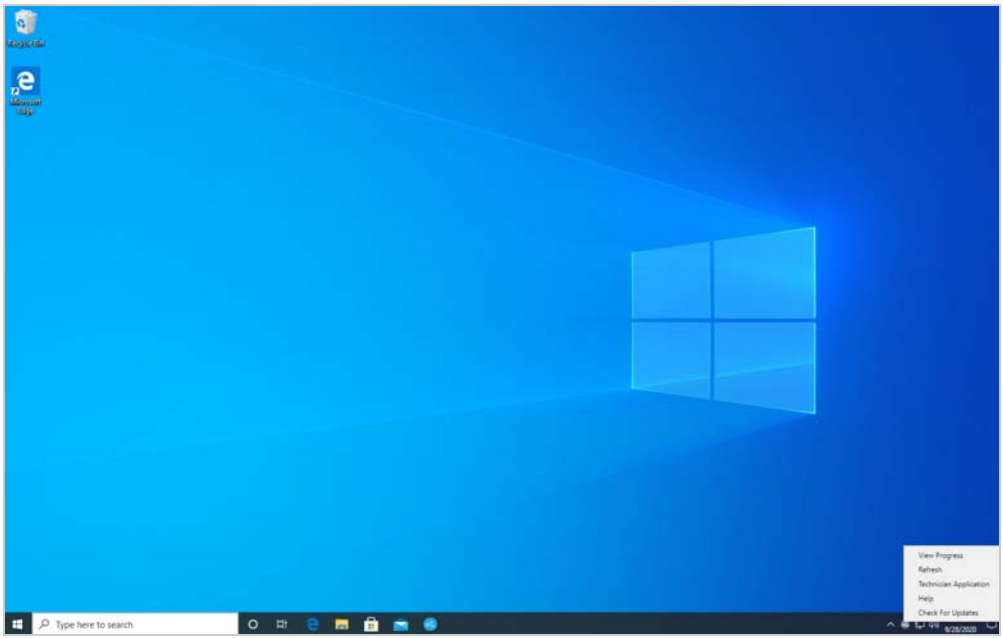
10 Click **Publish** > **Finish** to publish the policy.

Publishing the policy makes it available to the assigned devices.

Apply the Patch Policy

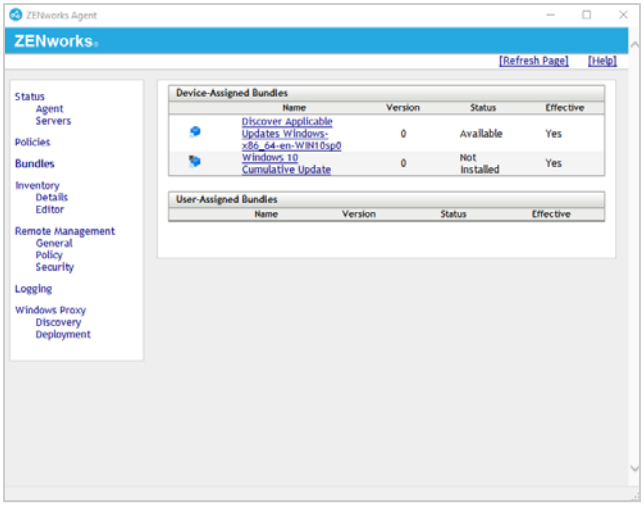
Normally, we would just sit back and wait for the Patch policy to be applied to the Windows 10 device based on the policy enforcement schedule. However, since we didn't set a schedule, we'll manually apply the policy to the device.

1 On the Windows 10 device, right-click the ZENworks icon, then click **Refresh** to download the Patch policy.



2 After the refresh completes, right-click the ZENworks icon again, click **Technician Application** to display the ZENworks Agent dialog box, then click **Bundles**.

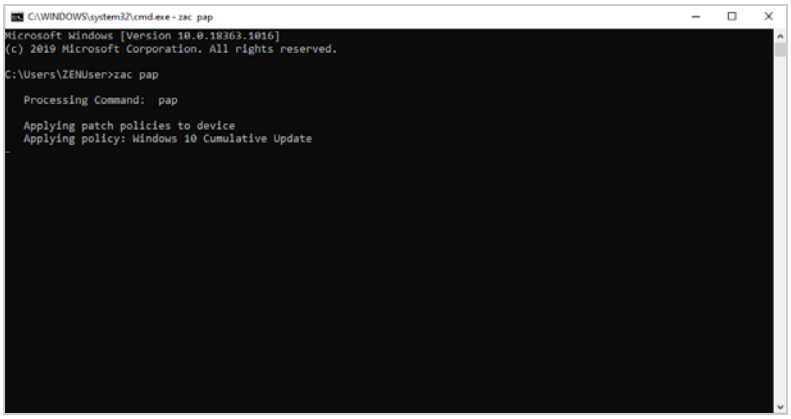
The Patch policy is distributed to the device as a bundle. It is displayed in the Device-Assigned Bundles list. Also, depending on how long it has taken for you to reach this part of the evaluation, your DAU bundle version might be a number other than 0. The DAU is regenerated with a new version during the Patch subscription process each day and then distributed to devices. This ensures that the DAU contains the signatures for any newly released patches that might be applicable to the device.



3 Open a Command Prompt window.

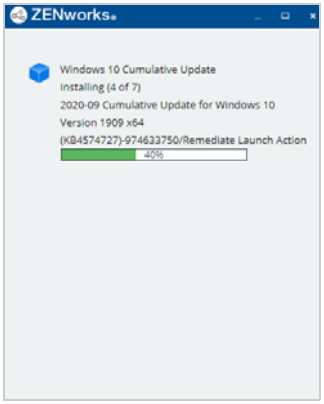
4 Enter `zac pap`.

`zac` is the ZENworks Agent Command line utility. The `pap` command stands for `patch-apply-policy` and causes the ZENworks agent to apply all Patch policies assigned to the device. In this case, it begins applying the Windows 10 Cumulative Update policy.

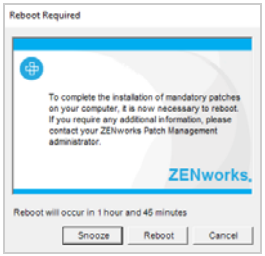


This process of applying the policy includes downloading the policy's patches (which in this case is the appropriate Windows 10 Cumulative Update version), installing the patch, running a new patch scan after installation, and reporting the installation results to the server. Since the cumulative update requires a reboot to complete the installation, that reboot has to occur before the final patch scan and report.

5 Right-click the ZENworks icon, then click **View Progress** to monitor the patch download and installation.



When the device needs to be restarted, you will receiving the following dialog.



6 Click **Reboot**.

7 After the device restarts and completes installation of the Windows 10 cumulative update, log in to Windows.

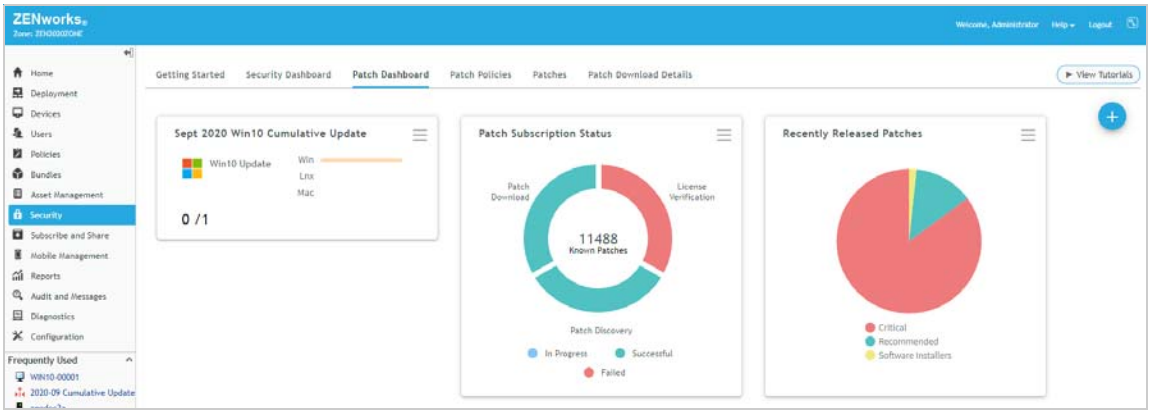
After login, the device is rescanned and the results are reported to the server. This can sometimes take up to 20 minutes.

View the Patching Results

Once the Patch policy is applied and the patch results have been reported to the ZENworks Primary Server, you can view the results in ZENworks Control Center.

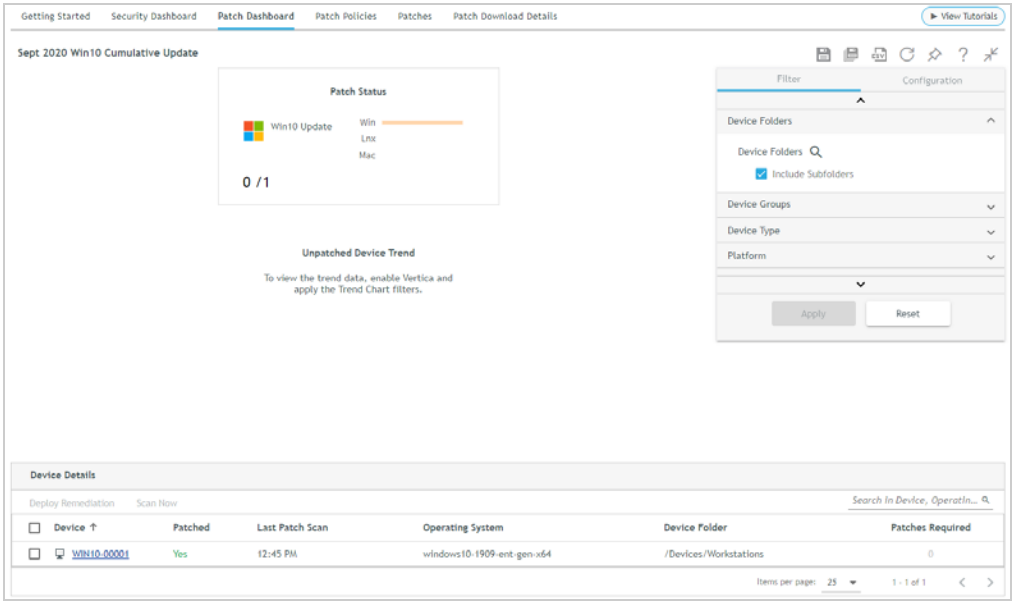
1 In ZENworks Control Center, click **Security** > **Patch Dashboard**.

Notice that the Win10 Cumulative Update tracker dashlet now shows that their are 0 unpatched devices.



2 Click the Win10 Cumulative Update dashlet to expand it.

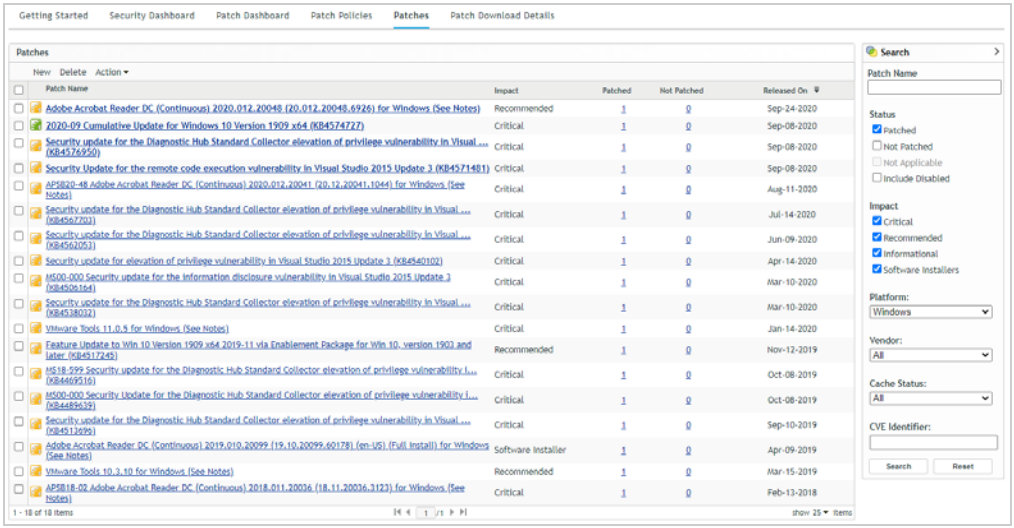
The Windows 10 device is now shown as patched.



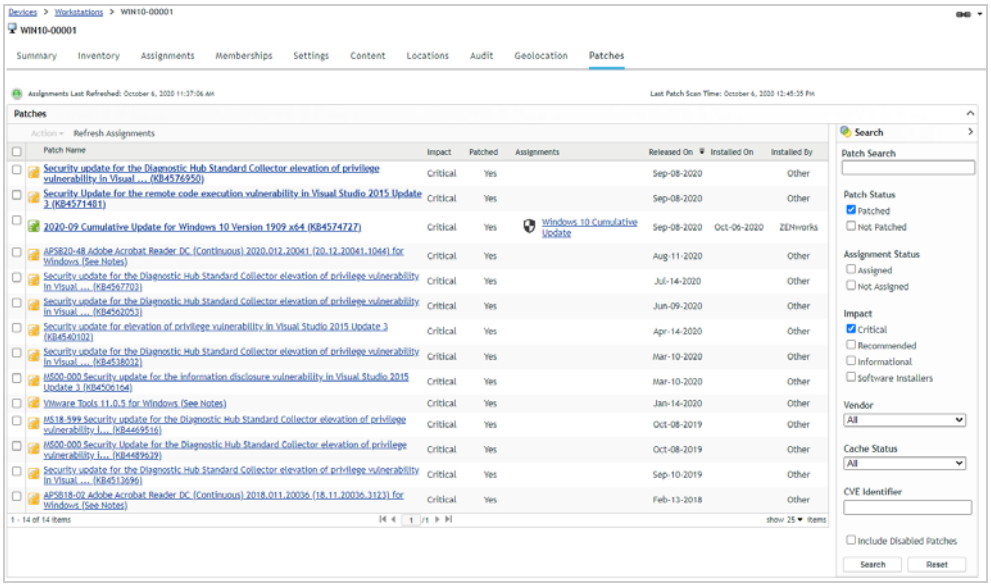
3 Click the **Back** link (in the breadcrumb trail at the top of the page) to return to the Patch Dashboard.

4 (Optional) Check out some of the other ZENworks Control Center locations that show the patch status for the device:

- The zone Patches list (Security > Patches). Make sure the Status filter in the Search box is set to Patched.



- The device Patches list (device > Patches). Make sure the Status filter in the Search box is set to Patched.



Manually Deploy Remediations

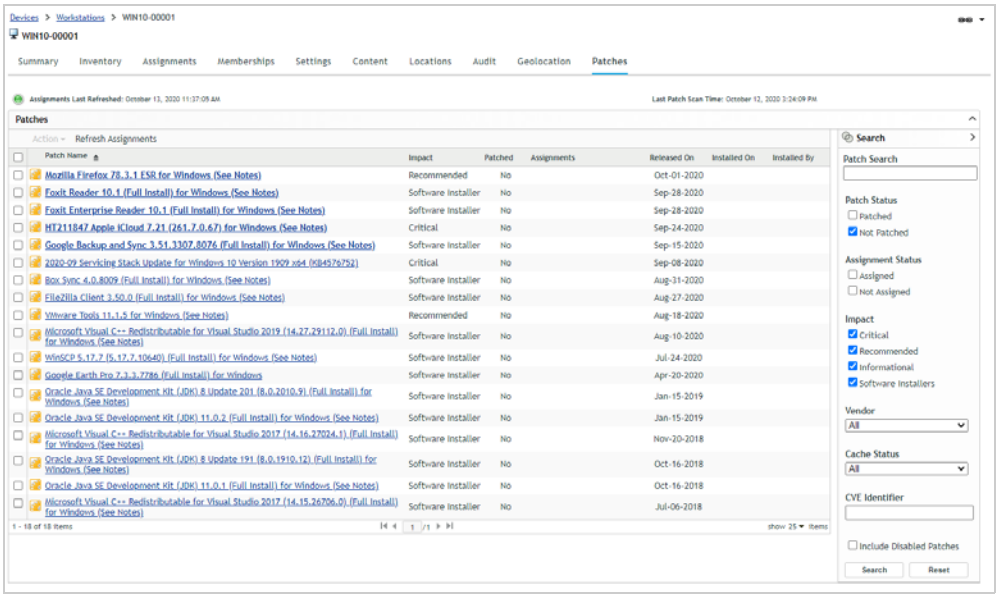
At times you may need to install a patch that is not included in one of your Patch policies or can't wait for the policy schedule to execute. You can easily do this and, in fact, can do it from multiple lists in ZENworks Control Center.

For example, if you need to deploy a patch to a single device, you can do that from the device's Patches list. Likewise, if you need to deploy a patch to a group of devices (such as the Windows 10 Workstations dynamic group), you can do that from the group's Patches list. Or, if you need to deploy a patch to all devices in the zone that need the patch, you can do that from the zone Patches list.

We'll deploy a patch to your Windows 10 device using the device's Patches list.

1 In ZENworks Control Center, open your Windows 10 device's Patches tab.

   The Patches list is filtered to show all patches that have not been installed on the device.



2 Select the check box in front of a patch you want to deploy to the device, then click **Action** > **Update Cache** to download the patch content.

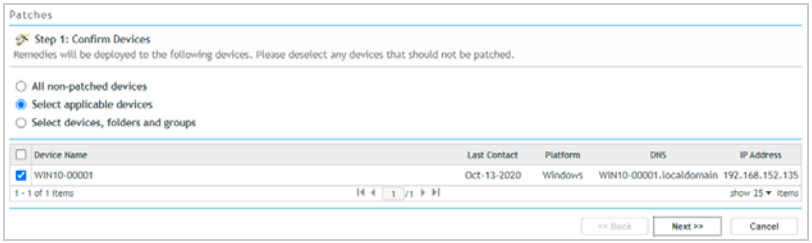
   You can install any of the patches you want. If you select a Software Installer, the full product is installed.

3 After a minute, if the patch is still downloading, click the Patches tab label to refresh the page.

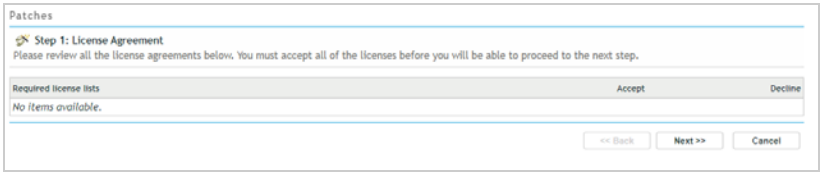
   The patch icon should now be green to indicate the content is downloaded.

4 Select the check box in front of the patch, then click **Action** > **Deploy Remediation** to display the Confirm Devices page of the Remediation Deployment wizard.

   The wizard automatically selects the device.

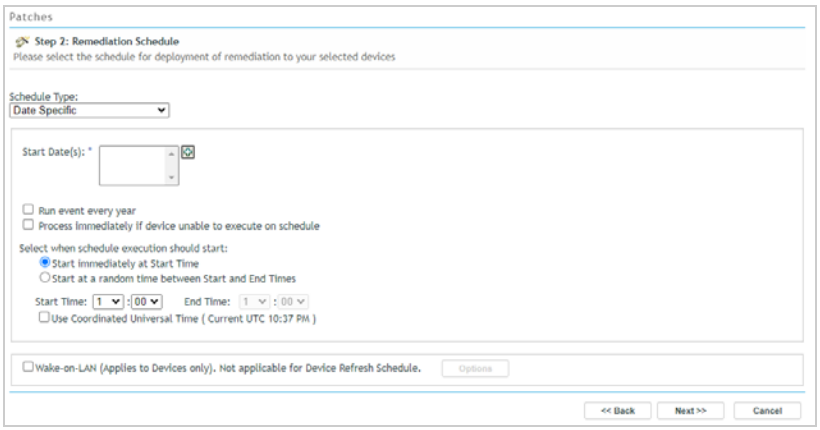


5 Click **Next** to display the License Agreement page.



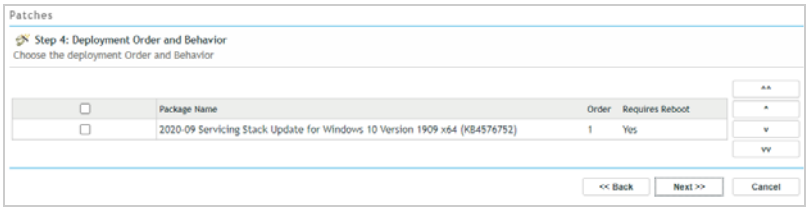
6 Accept any required license agreements, then click **Next** to display the Remediation Schedule page.

The remediation can be deployed immediately or scheduled for a later time. We'll have you deploy it immediately.



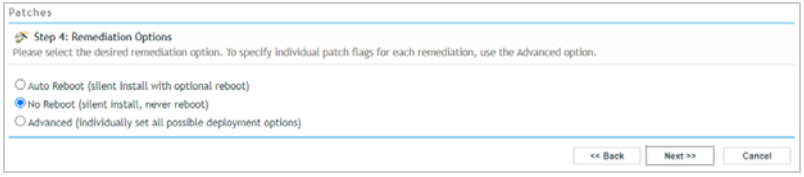
7 In the Schedule Type field, select **Now**, then click **Next** to display the Deployment Order and Behavior page.

In general, you don't need to do anything in this dialog because the order in which multiple patches in a remediation are deployed is resolved on the device. However, in our example below, notice that the patch requires a reboot. This information will help us determine the reboot options coming up in the next dialog.



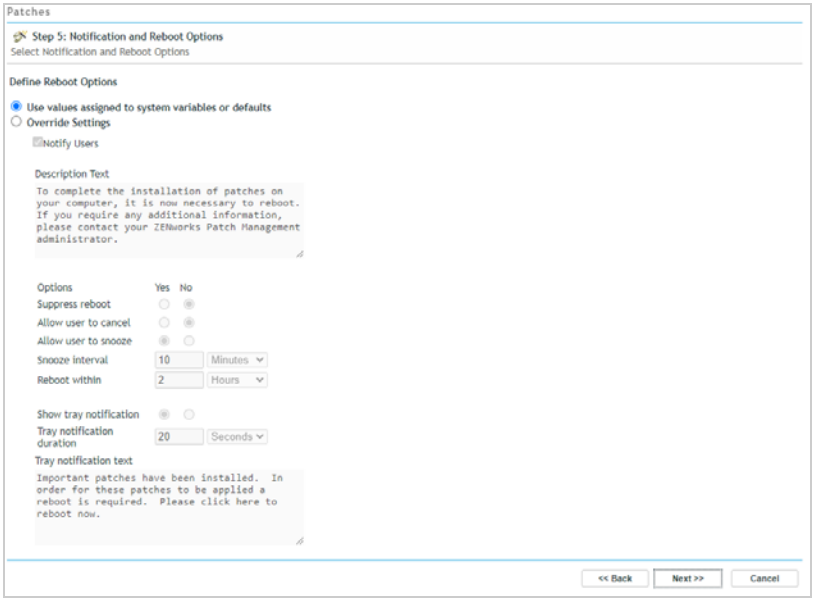
8 Click **Next** to display the Remediation Options page.

The first two Remediation Options determine the reboot behavior. The third option (Advanced) can be used to configure additional deployment options including pre-install notifications. We'll focus on the reboot options right now and skip the Advanced option. You can look at it later as needed.



9 Select **Auto Reboot**, then click **Next**.

With the Auto Reboot option, a reboot occurs only if the patch requires it. The option also lets you determine if you want to notify users before a reboot and configure the options associated with the notification.



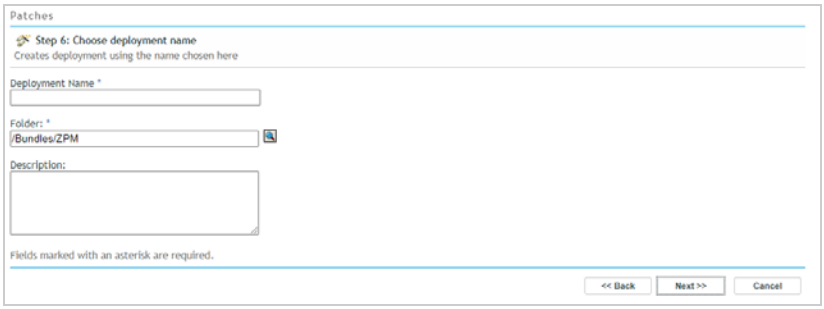
10 Configure the settings so that the user is notified if a reboot is required:

10a Select **Override Settings**.

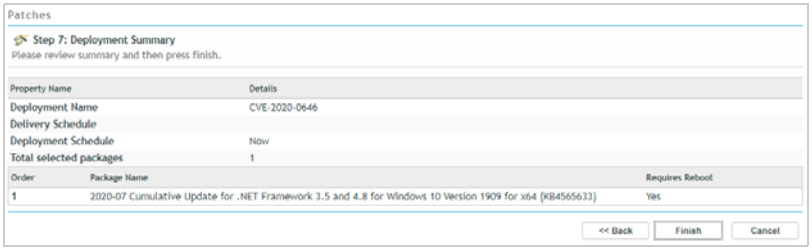
10b Set **Show tray notification** to No.

This suppresses the tray notification and automatically displays the Reboot dialog to the user.

10c Click **Next** to display the Deployment Name page.

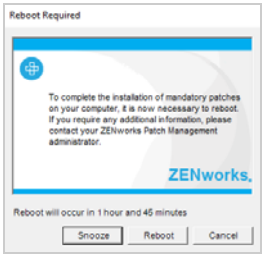


11 Enter a name for the deployment (for example, *Sept 2020 Servicing Stack Update for Windows 10 1909*), then click **Next**.



12 Review the Summary page, then click **Finish** to deploy the remediation to the Windows 10 device.

13 Go to the Windows 10 device and use the ZENworks Agent window (ZENworks icon > **Technician Application**) and View Progress dialog (ZENworks icon > **View Progress**) to monitor the progress of the patch installation. If the patch requires a reboot to complete installation, you are prompted.



14 Click **Reboot**.

The device reboots to complete the patch installation. After login, the device is rescanned and the results are reported to the server. This can sometimes take up to 20 minutes.

15 In ZENworks Control Center, open the device's Patches page.

16 In the Search box, select **Patched** as the status, then click **Search** to filter the list to display only patches that are installed on the device.

You should now see that the patch has been installed by ZENworks.

Remediate Security Vulnerabilities

Many software security vulnerabilities are not critical and can be safely handled by installing the next Windows 10 monthly cumulative update (or similar patch for other platforms or software applications) during your regular patch maintenance cycle.

However, there are times when you might not want to wait for your next patching window to fix a vulnerability. For example, some security vulnerabilities might already be exploited "in the wild" or have publicly disclosed exploitation methods. High-profile examples of these types of threats over the last several years include CurveBall in January 2020, BlueKeep in May 2019, and WannaCry and Petya/NotPetya (EternalBlue) in May/June 2017.

In cases like these, you can use the CVE dashlets on the Security dashboard to help you identify the devices impacted by the security vulnerability, apply the patch (or patches) to remediate the vulnerability, and track the remediation progress across all impacted devices.

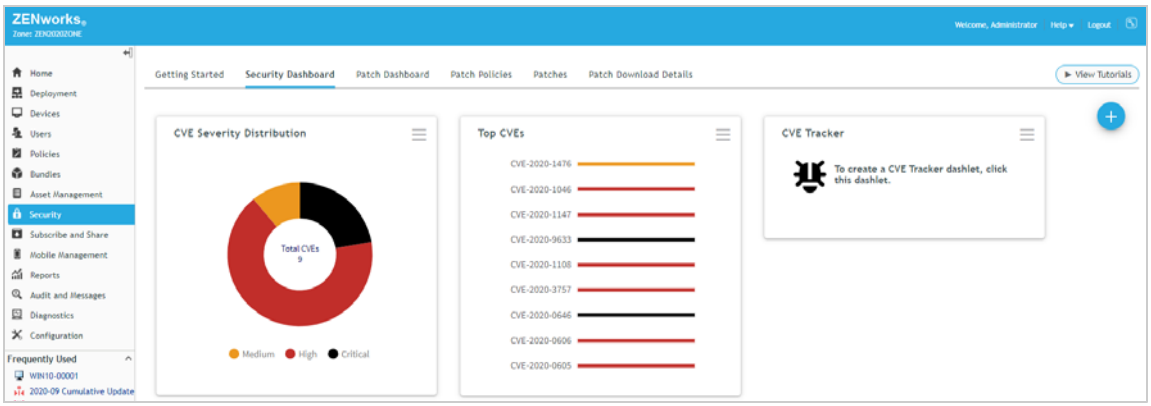
Based on when you are doing this evaluation, there might not be a high-profile vulnerability to address. That's okay, because you can use the CVE dashlets to identify, track, and remediate any CVE, so we'll have you use a couple of different methods to address a few of the highest severity CVEs currently impacting your system.

- "Use the CVE Severity Distribution Dashlet" on page 57
- "Use the CVE Tracker Dashlet" on page 61

Use the CVE Severity Distribution Dashlet

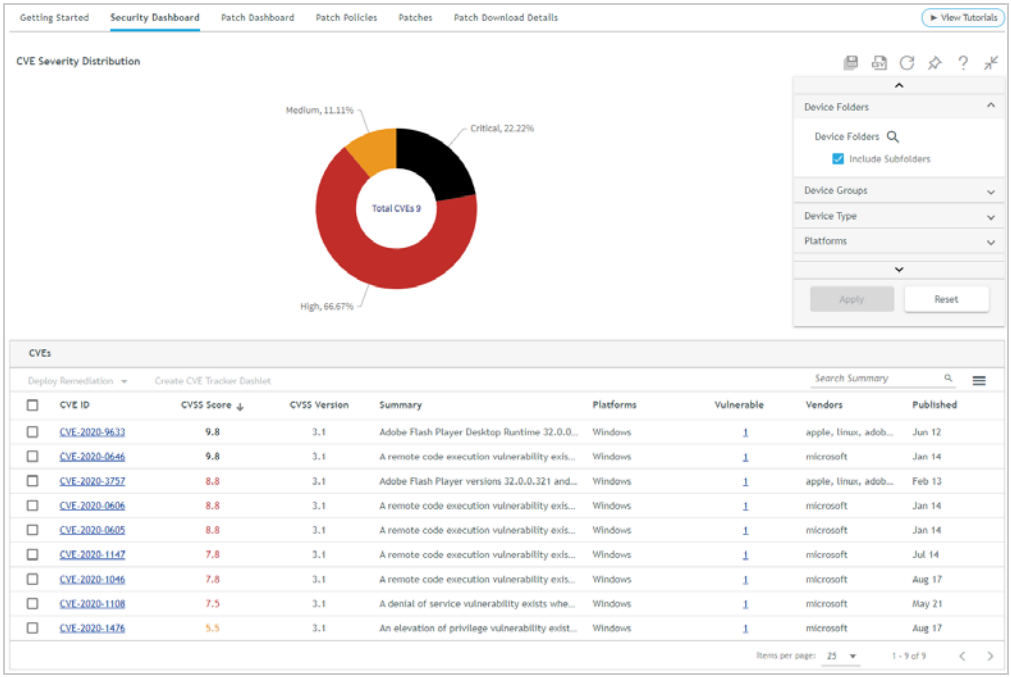
1 In ZENworks Control Center, click **Security** > **Security Dashboard**.

Since this is our first time looking at the Security Dashboard since we applied the Windows 10 cumulative update in the Automate Maintenance Patching with Policies section, notice that the update remediated many of the security vulnerabilities. In our example, the number of CVEs was reduced from 90 to 9.



2 Click the CVE Severity Distribution dashlet to expand it.

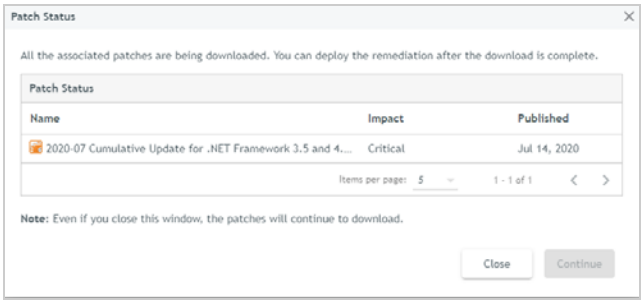
We've chosen to use the CVE Severity Distribution dashlet, but we could also have used the Top CVE dashlet.



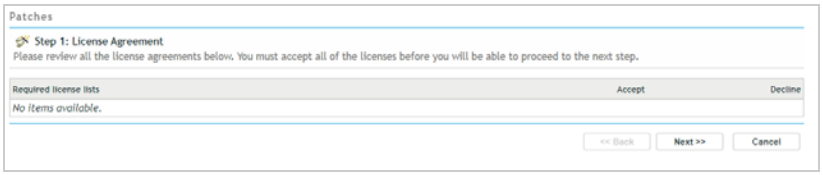
3 Select the check box in front of a CVE, then click **Deploy Remediation** > **Windows Devices** to display the Patch Status dialog.

The Patch Status dialog shows the download status of all patches associated with the CVE that are required to remediate the vulnerable devices. The patches must be downloaded from the online patch repository into your zone before they can be included in the remediation.

NOTE: If all of the CVE patches are already downloaded, the Patch Status dialog is bypassed and the Remediation Deployment wizard (next step) is displayed.

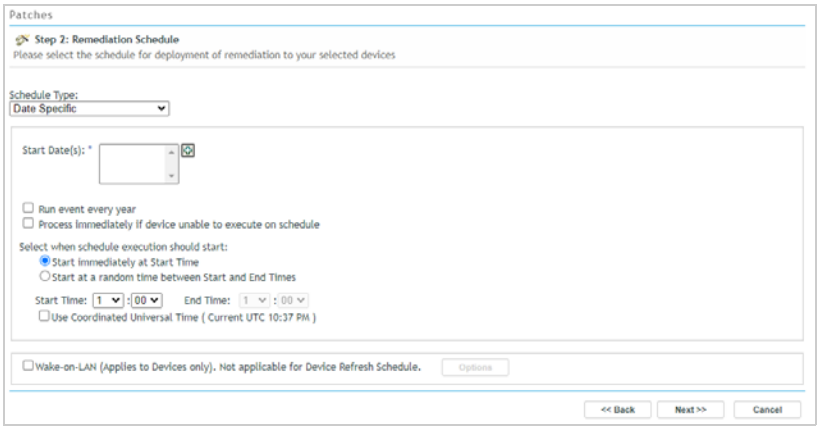


4 When the patch download is complete, click **Continue** to display the License Agreement page of the Remediation Deployment wizard.



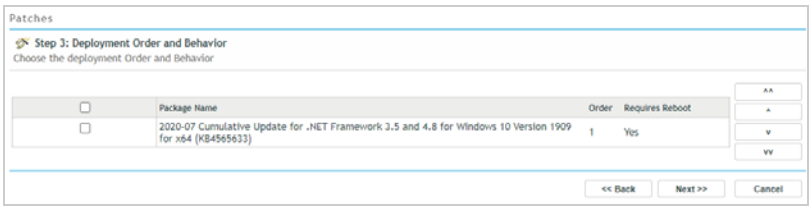
5 Accept any required license agreements, then click **Next** to display the Remediation Schedule page.

The remediation can be deployed immediately or scheduled for a later time. We'll have you deploy it immediately.



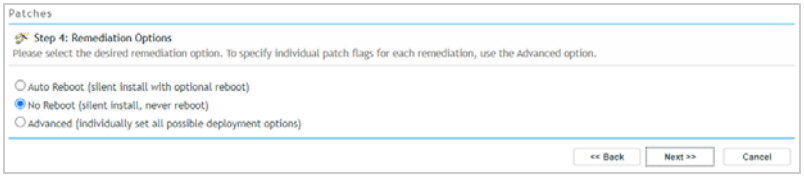
6 In the Schedule Type field, select **Now**, then click **Next** to display the Deployment Order and Behavior page.

In general, you don't need to do anything in this dialog because the order in which multiple patches in a remediation are deployed is resolved on the device. However, in our example below, notice that the patch requires a reboot. This information will help us determine the reboot options coming up in the next dialog.



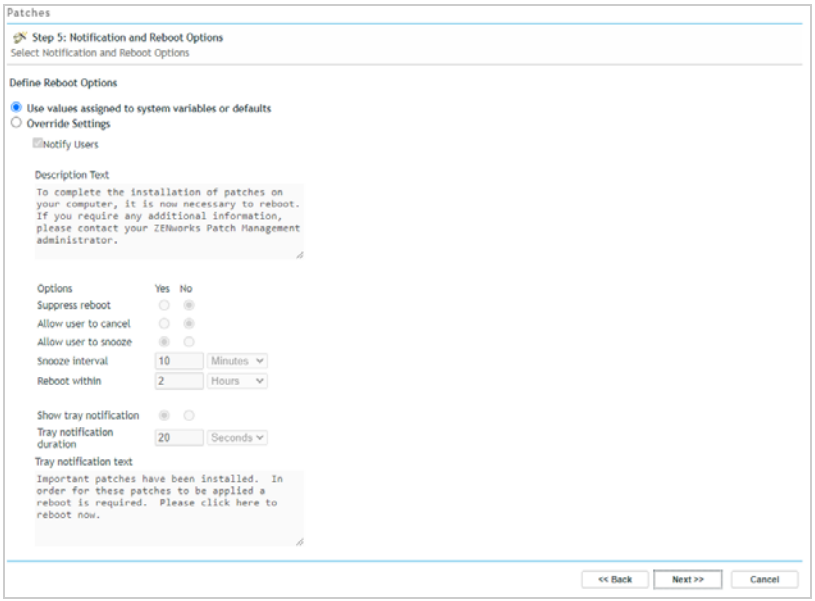
7 Click **Next** to display the Remediation Options page.

The first two Remediation Options determine the reboot behavior. The third option (Advanced) can be used to configure additional deployment options including pre-install notifications. We'll focus on the reboot options right now and skip the Advanced option. You can look at it later as needed.



8 Select **Auto Reboot**, then click **Next**.

With the Auto Reboot option, a reboot occurs only if the patch requires it. The option also lets you determine if you want to notify users before a reboot and configure the options associated with the notification.



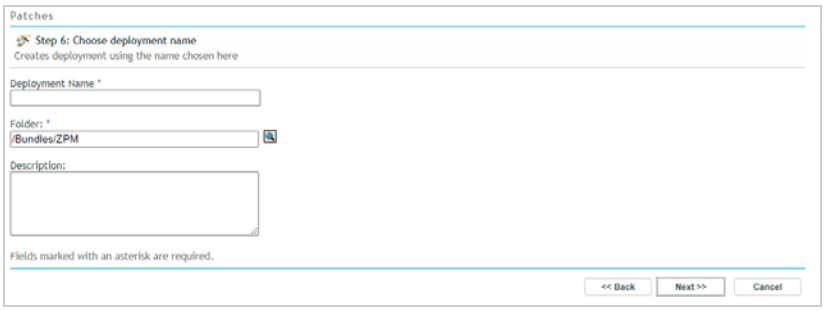
9 Configure the settings so that the user is notified if a reboot is required:

9a Select **Override Settings**.

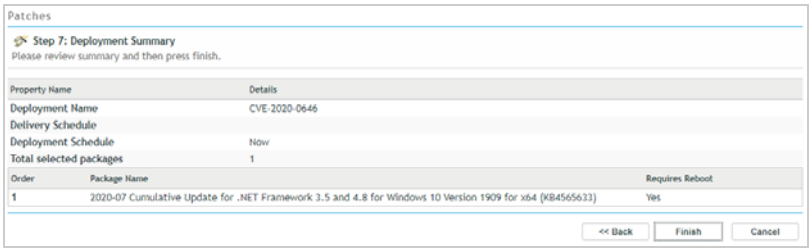
9b Set **Show tray notification** to No.

This suppresses the tray notification and automatically displays the Reboot dialog to the user.

9c Click **Next** to display the Deployment Name page.

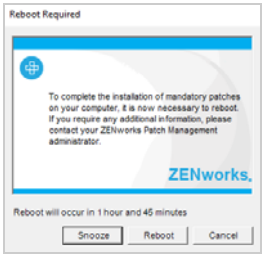


10 Enter a name for the deployment (for example, *CVE-2020-0144 Remediation*), then click **Next**.



11 Review the Summary page, then click **Finish** to deploy the remediation to the Windows 10 device.

12 Go to the Windows 10 device and use the ZENworks Agent window (ZENworks icon > **Technician Application**) and View Progress dialog (ZENworks icon > **View Progress**) to monitor the progress of the patch installation. If the patch requires a reboot to complete installation, you are prompted.



13 Click **Reboot**.

The device reboots to complete the patch installation. After login, the device is rescanned and the results are reported to the server. This can sometimes take up to 20 minutes.

14 In ZENworks Control Center, open the CVE Severity Distribution dashlet.

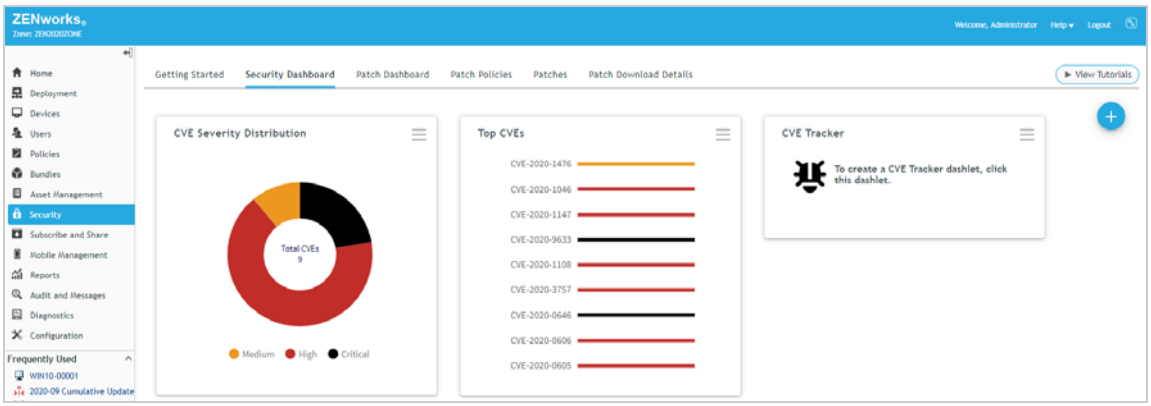
Because the dashlet is configured to only show CVEs with vulnerable devices, the CVE should no longer be displayed in the list unless the Windows 10 device has not yet reported its results. To see the CVE in the list, you can deselect the *CVEs with vulnerable devices* setting in the **Vulnerability Status** filter and apply

the filter. By adding the Not Vulnerable column to the grid you can also see the Windows 10 device counted in that column. To add the column, click the Column Selection icon ☰ in the grid menu, then select the Not Vulnerable column.

Use the CVE Tracker Dashlet

1 In ZENworks Control Center, click **Security** > **Security Dashboard**.

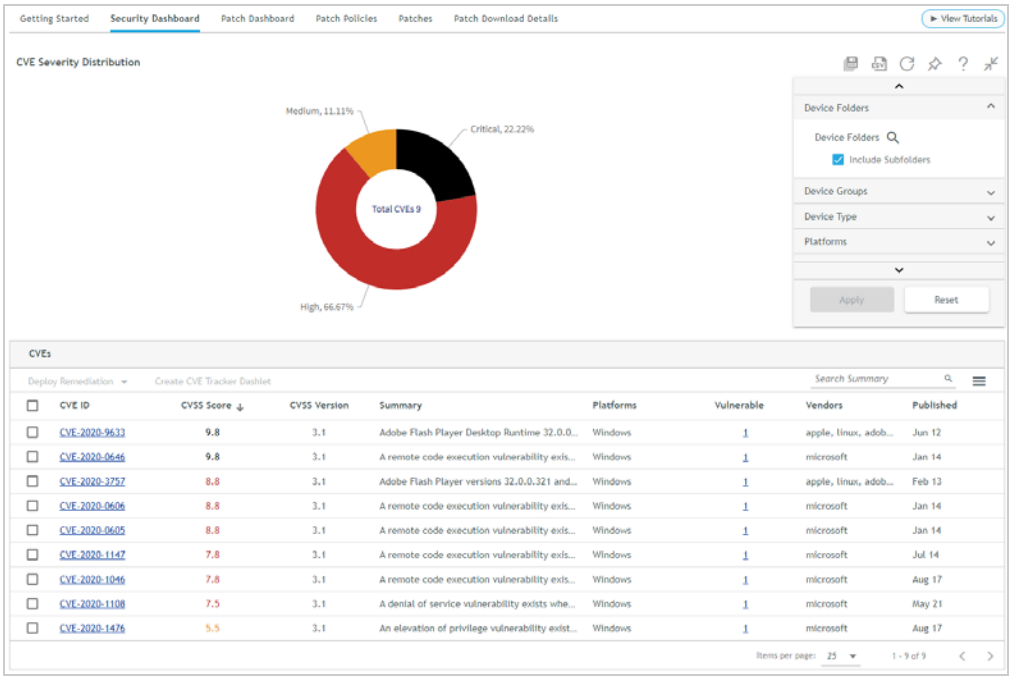
The CVE Tracker dashlet, like the Patch Tracker dashlet, is a template dashlet that you need to configure by identifying the CVE (or CVEs) you want to track. One way to do that is to expand the template dashlet and then add the CVE. Another way to do it is to first identify a security vulnerability using the CVE Severity Distribution dashlet (or Top CVE dashlet) and then use the dashlet's **Create CVE Tracker** option. This is the approach we'll use.



2 Click the CVE Severity Distribution dashlet to expand it.

The CVEs list displays the CVEs with the highest scores first. Notice that the Windows 10 cumulative update that you applied to your Windows 10 device in the Automate Maintenance Patching with Policies section remediated many of the security vulnerabilities. In our example, the number of CVEs was reduced from 90 to 9.

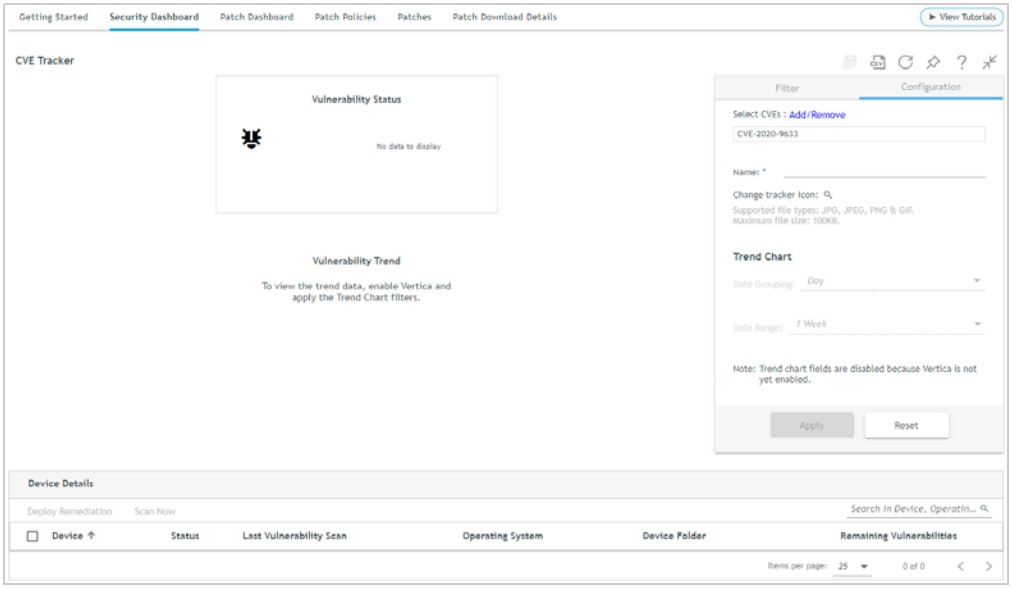
We're going to create and use a CVE Tracker dashlet to remediate a vulnerability. But you could also remediate any of the listed vulnerabilities from this dashlet by simply selecting a CVE and clicking **Deploy Remediation**.



3 Create a CVE Tracker dashlet:

3a Click the check box in front of a CVE to select it, then click **Create CVE Tracker Dashlet**.

The CVE Tracker dashlet opens with the selected CVE auto-populated in the **Select CVEs** field.



3b In the **Name** field, enter the CVE ID (for example, CVE-2020-9633).

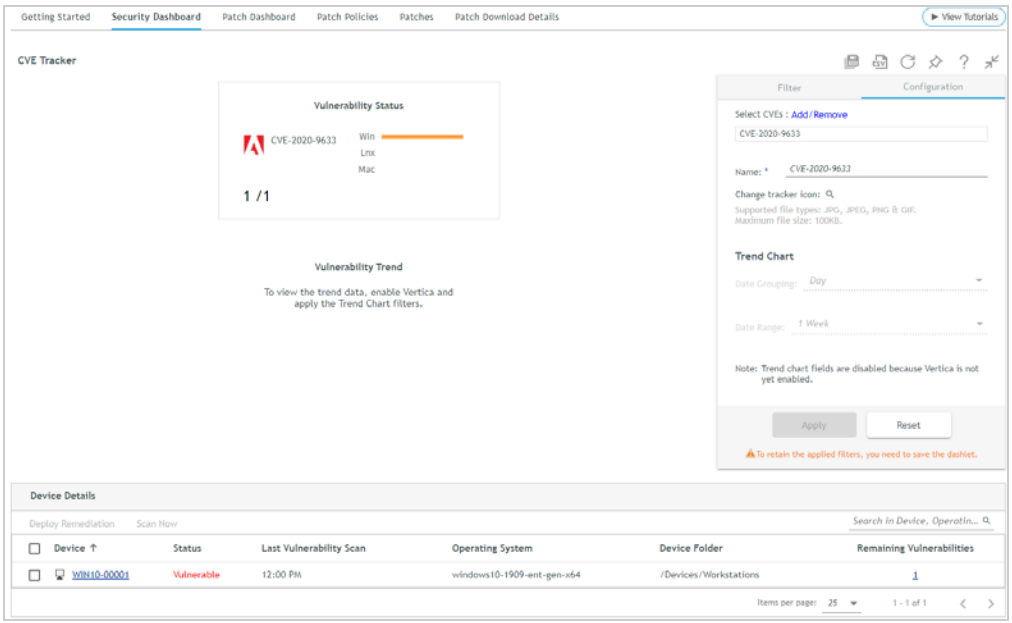
3c (Optional) In the **Change tracker icon** field, click to change the default icon to another icon you'd prefer. You must supply the icon.

3d Click **Apply** to apply the configuration settings.

Any device to which the CVE applies is displayed in the Device Details list. In our case, this is the single Windows 10 device we registered.

Because we are primarily concerned with vulnerable devices, the Vulnerability Status chart shows the number of vulnerable devices out of the total applicable devices (1/1). If you mouse over the Windows bar, you will see "1 vulnerable devices of 1".

You should also note that the dashlet can include a second Vulnerability Trend chart. This chart displays the number of vulnerable devices over a period of time so that you can see how your device patching is remediating the vulnerability. Because storing and displaying trend data can impact the ZENworks database performance, a separate Vertica database is required for trend data. We won't set it up for this evaluation.



3e To save the dashlet, click (above the dashlet filter list, enter a name for the dashlet, then click **OK**.

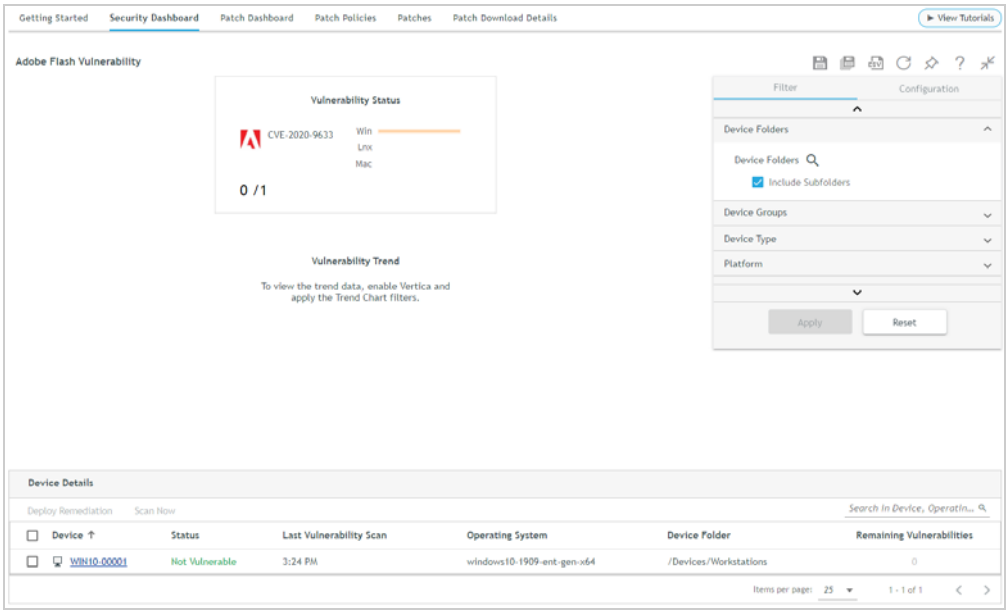
4 Remediate the vulnerability:

4a In the list, select the check box in front of the Windows 10 device, then click **Deploy Remediation**.

4b Follow the prompts to apply the patches required to remediate the CVE on the device. If you need detailed instructions, see "Use the CVE Severity Distribution Dashlet" on page 57.

5 After the results have been reported to the server, view the CVE Tracker dashlet again.

The Windows 10 device now has a status of Not Vulnerable.



Explore Other Areas

ZENworks 2020 Patch Management includes many additional features and capabilities you might want to explore.

- "Staged Rollouts" on page 65
- "Linux Patching" on page 66
- "Mac Patching" on page 66
- "Patch Scan Schedules" on page 66
- "Policy Enforcement Schedules" on page 67
- "Patch Content Distribution Schedules" on page 67
- "Pre-Install User Notifications" on page 67

Staged Rollouts

Best practices for quality assurance dictate a staged rollout of patches to devices in an organization. Patching a smaller number of representative devices allows you to discover and resolve issues while minimizing the potential impact.

ZENworks Patch Management not only supports a staged rollout but can also automate the rollout for you. Each time the patch membership of a Patch policy is recalculated (to include new patches and remove superseded patches), the updated Patch policy is generated as a Sandbox version. The sandboxed policy is deployed to designated test devices and if the installation is successful the policy is published so that it can be applied to non-test devices at their scheduled deployment times. Each step of this process can be automated, from the recalculating the Patch policy to automatically publishing it after successful testing.

For detailed instructions, see Test a Policy Before Deploying in a Live Environment in the *ZENworks Patch Management Reference.*

Linux Patching

You can patch SUSE Linux Enterprise (SLE) devices and Red Hat Enterprise Linux (RHEL) devices. To do so:

1. Install the ZENworks agent on the device to register it in your ZENworks Management Zone. The device must be one of the following operating systems: SLED/SLES 12 SP3 - SP5, SLES 15/15 SP1, RHEL 6.9 - 6.10, RHEL 7.0 - 7.8. For instructions, see Manually Deploying the Agent on Linux in the *ZENworks Discovery, Deployment, and Retirement Reference*.
2. Ensure that the device is registered with SUSE or Red Hat, as applicable, and has access to the SUSE/Red Hat external networks to be able to download patch content.
3. Access the Subscription Service Content Download settings (**ZENworks Control Center** > **Configuration** > **Management Zone Settings** > **Security** > **Subscription Service Content Download**) and enable the **Linux** platform download option. Also make sure that **Red Hat Subscription Management (RHSM)** is selected.
4. Run the Patch subscription service to download Linux patches.
5. Refresh the Linux device to download the patch scan (DAU) file and run the scan.

Mac Patching

You can patch Mac devices, both the operating system and applications. To do so:

1. Install the ZENworks agent on the device to register it in your ZENworks Management Zone. The device must be one of the following operating systems: 10.8.3, 10.9.x - 10.15.x. For instructions, see Manually Deploying the Agent on a Macintosh Device in the *ZENworks Discovery, Deployment, and Retirement Reference*.
2. Access the Subscription Service Content Download settings (**ZENworks Control Center** > **Configuration** > **Management Zone Settings** > **Security** > **Subscription Service Content Download**) and enable the **Mac** platform download option.
3. Run the Patch subscription service to download Mac patches.
4. Refresh the Mac device to download the patch scan (DAU) file and run the scan.

Patch Scan Schedules

By default, patch scans are scheduled to occur whenever the device refreshes its information from the ZENworks Primary Server. This occurs whenever the device operating system starts and every 12 hours (default). You can change the schedule to fit your needs. For example, if you distribute patch policies monthly and are not concerned with daily patch status updates, you could schedule weekly patch scans.

The patch scan schedule is set at the zone level but can be overridden at the device folder to allow you to have different schedules for different devices.

- To change the patch scan schedule for the zone, log into ZENworks Control Center and go to **Configuration** > **Management Zone Settings** > **Security** > **Vulnerability Detection Schedule.**
- To change the patch scan schedule for a device folder, log into ZENworks Control Center, go to **Devices** > locate the device folder > click **Details** next to the folder > click the **Settings** tab > go to **Security** > **Vulnerability Detection Schedule.**

Policy Enforcement Schedules

By default, Patch policies are enforced when the *zac pap* command is manually run from the command line of a device. You can schedule when policies are enforced so that patches are applied automatically when you want. Schedule options include applying patches when the device shuts down, when the ZENworks agent does a device refresh, or on a recurring day (weekly, monthly, or interval).

The Patch policy enforcement schedule is set at the zone level but can be overridden at the device folder and individual device levels to allow you to have different schedules for different devices.

- To change the Patch policy enforcement schedule for the zone, log into ZENworks Control Center and go to **Configuration** > **Management Zone Settings** > **Security** > **Patch Policy Settings.**
- To change the Patch policy enforcement schedule for a device folder, log into ZENworks Control Center, go to **Devices** > locate the device folder > click **Details** next to the folder > click the **Settings** tab > go to **Security** > **Patch Policy Settings.**
- To change the Patch policy enforcement schedule for a device, log into ZENworks Control Center, go to **Devices** > locate and click the device to open its properties > click the **Settings** tab > go to **Security** > **Patch Policy Settings.**

Patch Content Distribution Schedules

By default, patches are downloaded to a device when Patch policies are enforced. If desired, you can schedule distribution of the patch content to devices before the enforcement date. This is useful in situations such as short patching windows. Schedule options include distributing patches when the device shuts down, when the ZENworks agent does a device refresh, or on a recurring day (weekly, monthly, or interval).

The patch distribution schedule is set at the zone level but can be overridden at the device folder and individual device levels to allow you to have different schedules for different devices.

- To change the Patch policy enforcement schedule for the zone, log into ZENworks Control Center and go to **Configuration** > **Management Zone Settings** > **Security** > **Patch Policy Pre-Install Behavior.**
- To change the Patch policy enforcement schedule for a device folder, log into ZENworks Control Center, go to **Devices** > locate the device folder > click **Details** next to the folder > click the **Settings** tab > go to **Security** > **Patch Policy Pre-Install Behavior.**
- To change the Patch policy enforcement schedule for a device, log into ZENworks Control Center, go to **Devices** > locate and click the device to open its properties > click the **Settings** tab > go to **Security** > **Patch Policy Pre-Install Behavior.**

Pre-Install User Notifications

By default, ZENworks Patch Management is configured for silent installation of patches. If desired, you can prompt users before patches are installed during policy enforcement. Options include allowing users to cancel or delay installation.

The pre-install notification options are set at the zone level but can be overridden at the device folder and individual device levels to allow you to have different notification settings for different devices.

- To change the pre-install notification settings for the zone, log into ZENworks Control Center and go to **Configuration** > **Management Zone Settings** > **Security** > **Patch Policy Pre-Install Behavior.**

- To change the pre-install notification settings for a device folder, log into ZENworks Control Center, go to **Devices** > locate the device folder > click **Details** next to the folder > click the **Settings** tab > go to **Security** > **Patch Policy Pre-Install Behavior.**
- To change the pre-install notification settings for a device, log into ZENworks Control Center, go to **Devices** > locate and click the device to open its properties > click the **Settings** tab > go to **Security** > **Patch Policy Pre-Install Behavior.**

Legal Notice