



# Tenable Patch Management Express User Guide

Last Revised: December 20, 2024

# Table of Contents

- Getting Started with Tenable Patch Management .....6
- Prerequisites .....6
- Supported Browsers .....6
- Logging .....6
- Customer Support.....7
- Tenable Patch Management Admin Portal .....7
  - Log in to the Admin Portal .....7
  - Resolve Mozilla Firefox Active Directory Login Issue .....7
- Licensing Tenable Patch Management.....8
  - Add a License Key .....9
  - Add a Licensed Product to a Collection Group .....9
- Tenable Patch Management Express Dashboard ..... 10
  - Access the Dashboard..... 10
- Tenable Patch Management Setup Wizard ..... 11
  - Welcome to Tenable Patch Management Express ..... 11
  - Detection Integrations ..... 12
    - Integrate a Partner Product ..... 12
  - Use Copy From..... 14
  - Select a Remediation Schedule ..... 15
  - Enable Vulnerability Detection..... 16
  - Enable Patch Pre-staging.....17
  - Configure Deployment Notifications.....17
  - Configure Deployment Approval ..... 19
  - Configure Test Deployment .....22
  - Configure Test Approval.....25
  - Complete Tenable Patch Management Express Setup ..... 27
- Integrate Tenable Vulnerability Management .....29
  - Add Tenable Access Settings to Tenable Patch Management .....29
    - Configure Tenable Vulnerability Management Settings .....30
    - Configure Tenable Security Center Settings..... 31
  - Create Tenable Access and Secret Key ..... 31
  - Administrators and Roles .....34

Access Security Settings.....	34
View Administrators.....	35
Create a New Administrator.....	35
Create a Microsoft Teams Webhook URL .....	36
View Roles .....	37
Create a New Role .....	37
Best Practices for Patch Express .....	41
Menu Objects for Tenable Patch Management.....	42
Patching Analytics Dashboards .....	43
Using Search in Tenable Patch Management .....	43
Patching Analytics Overview.....	43
Products View.....	44
Patches View .....	47
Devices View .....	49
Flex Controls .....	52
Blocklisting.....	52
Blocklist Settings.....	52
Blocklisted Patches.....	53
Cycle Operations.....	57
Patching Cycles .....	57
Deployment Cycles.....	60
Rollout Cycles .....	62
Patching Exceptions .....	63
Using Patching Exceptions.....	63
Create a Patching Exception .....	63
Set Override Details for Patch Exception.....	64
Set Last Allowed Patch Versions.....	66
Add Target Business Units for Patch Exceptions.....	67
Global Pause .....	68
Stop All Patching Activity Immediately.....	69
Resume All Paused Patching Activity Immediately.....	70
Pause Patching for Specific Objects .....	72
Pause Deployment of a Specific Software Product .....	73
Pause Deployment of a Specific Patch .....	77
Pause Specific Cycles .....	80

Pause Deployment to a Business Unit .....	90
Rollbacks Overview .....	91
Rollback.....	92
Rollback to Version .....	110
Approval Requests.....	129
Approve or Reject a Patch Request.....	129
Auto Remediation .....	131
Access Auto Remediation and Deployment Settings .....	131
Using Auto Remediation Settings .....	132
Enable Auto Remediation .....	133
Vulnerability Detection Source Settings.....	135
Production Deployment Settings for Auto Remediation.....	135
Test Deployment Settings for Auto Remediation.....	135
Verify that Auto Remediation Works as Expected.....	136
Patching Preferences .....	137
Using Patching Preferences .....	137
Access Patching Preferences.....	137
Create a New Patching Preference .....	138
Add a Target Business Unit.....	138
Select a Server Maintenance Window .....	140
Select Server User Interaction Settings .....	141
Business Units.....	142
Understanding Business Units.....	142
Parent and Child Business Units .....	143
Managing Inheritance Settings .....	144
Enable Inheritance .....	144
Disable Inheritance .....	145
Organizing the Business Unit Hierarchy .....	145
Best Practices when Changing Priorities.....	146
Change the Order of the Hierarchy .....	146
Creating a Business Unit .....	147
Open and Save a Business Unit Template .....	147
Add Evaluation Schedules to a Business Unit .....	149
Configure Business Unit Scopes .....	150
Verify Business Unit Members .....	157

Create a Lab Business Unit .....	157
Create a Custom Lab Business Unit .....	158
Open and Save a Business Unit Template .....	159
Verify Business Unit Members .....	161
Create a Lab Business Unit .....	161
Test Deployment Settings for Auto Remediation .....	162
Create a Custom Lab Business Unit .....	162
Maintenance Windows .....	163
Open and Save a Maintenance Window Template .....	163
Add Dynamic Detection Workflow (Optional) .....	163
Apply to All Urgencies.....	164
Set Maintenance Windows by Urgency.....	164
Create a Maintenance Window.....	164
Set the All Urgencies Override Duration .....	165
Save and Deploy the Maintenance Window .....	165
User Interaction Settings .....	166
Understanding User Interaction Settings .....	166
Create User Interaction Settings .....	166
Open and Save a User Interaction Template .....	166
Edit or Create Urgency Settings.....	167
Set Deployment Notification Settings .....	168
Create System Reboot Notification Settings .....	168
Save and Deploy User Interaction Settings .....	170
Customized Products.....	172
Manage Settings for Customized Products.....	172
Open and Save a Customized Product Template .....	172
Add a Deployment Wave to a Customized Product Template.....	172
Add a Target Product .....	173
Configure Software Install Settings .....	174
Navigating the Tenable Patch Management Dashboard .....	176
Date Settings, Export, and Refresh .....	176
Set Dates for Status Views .....	176
Export Widget Data .....	177
Refresh the Status View .....	179
Tenable Patch Management Menus.....	179

Integration Menu .....	179
Platform Features Menu .....	180
Tenable Patch Management Dashboard and Performance Widgets.....	180
Patching Metrics .....	181
Patching Status .....	181
Overall Compliance.....	181
Risk Score.....	182
Patching Metadata .....	182
Patching System Health .....	183
Patching Activity.....	183
Top 5 Non-Compliant Products.....	184
Top 5 Missing Patches .....	184
Appendices .....	185
Software Products Library.....	185
Metadata Catalog .....	185
Endpoint Scans.....	185
Request a Scan .....	185

# Getting Started with Tenable Patch Management

Tenable Patch Management Express automates even the most complex enterprise patching processes, allowing IT and security teams to precisely mirror their patching strategies and tailor processes for specific device groups.

Tenable Patch Management is powered by Adaptiva. This collaboration brings advanced patch management to customers, ensuring you benefit from the combined expertise of both companies. Tenable Patch Management is a robust and versatile product that focuses on risk-driven patch prioritization. is committed to providing the best tools for our customers to achieve their security outcomes. This partnership exemplifies that dedication.

## Prerequisites

Before using Tenable Patch Management Express, you must set up your environment. See the *Tenable Patch Management Installation Guide* for details.

The Server and Client software installations support all patching products. After you add license keys, you are ready to access the power of Tenable Patch Management in your environment.

## Supported Browsers

Tenable Patch Management supports the following browsers:


- Google Chrome
- Microsoft Edge and Chromium Edge
- Mozilla Firefox
- Safari
- Most other commonly used browsers

### **Important**

Do not use Microsoft Internet Explorer.

\* If you receive an Admin Portal login error when using Mozilla Firefox, see [Resolve Mozilla Firefox Active Directory Login Issue](#).

## Logging

You may access logs and log management for the Tenable Server through the  on the Admin Portal or from the Tenable Server in Program Files/Tenable/PatchServer/Logs.

Access Tenable Client logs from the Tenable Client in Program Files/Tenable/ClientServer/Logs.

# Customer Support

Whenever you need information beyond what this documentation provides, enter a support ticket and request help from Tenable Customer Support.

## Tenable Patch Management Admin Portal

Tenable Patch Management uses an admin portal and a dashboard for configuration.

You will use the portal to set up your environment, create policies, add administrators, and more. Settings, such as groups, security, and administrators are global.

### Log in to the Admin Portal

During installation, the administrator creates a SuperAdmin account using either a native Tenable Patch Management login or a Windows Active Directory account (recommended).

1. Enter the **Fully Qualified Domain Name (FQDN)** for the Tenable Server followed by the **port (optional)** into the browser address bar:

`https://<FQDN>:[port]`

If necessary, confirm the port with the administrator who defined the port during software installation. If the server is already using port 80, for example, the web site might use port 9678.

2. Press **Enter**. The OneSite Admin Portal login dialog opens.
3. Log in using one of the following methods:
  - a. Click **Login with Active Directory** (recommended).
  - b. Enter the **Login ID** (email address) and password provided by your administrator, and then click **Login with Tenable**.

After successfully logging in, the OneSite Admin Portal dashboard appears.

If you have issues logging in with Active Directory using Mozilla Firefox, see [Resolve Mozilla Firefox Active Directory Login Issue](#).

## Resolve Mozilla Firefox Active Directory Login Issue

To access the Admin Portal using Active Directory, Mozilla Firefox requires adding the Tenable Server as a trusted URI to enable SSPI/Kerberos authentication. If you receive the following message when using Mozilla Firefox to log into the Admin Portal using Active Directory, use the steps provided to below resolve the issue:

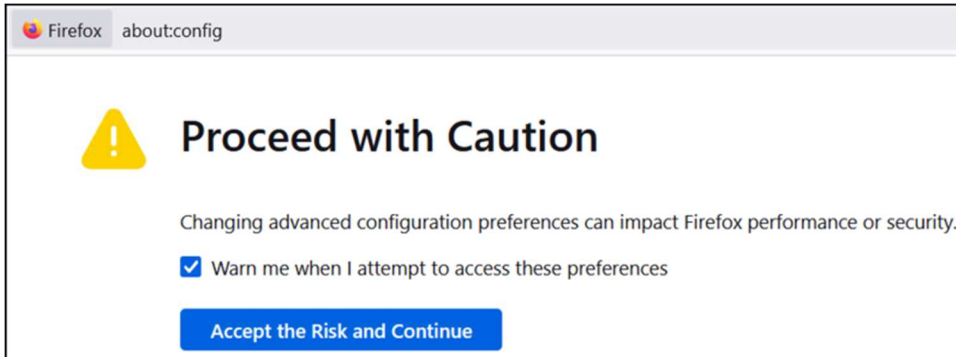
### **Authentication is possible but has failed or not yet been provided.**

1. Open a new browser tab and enter the following command:

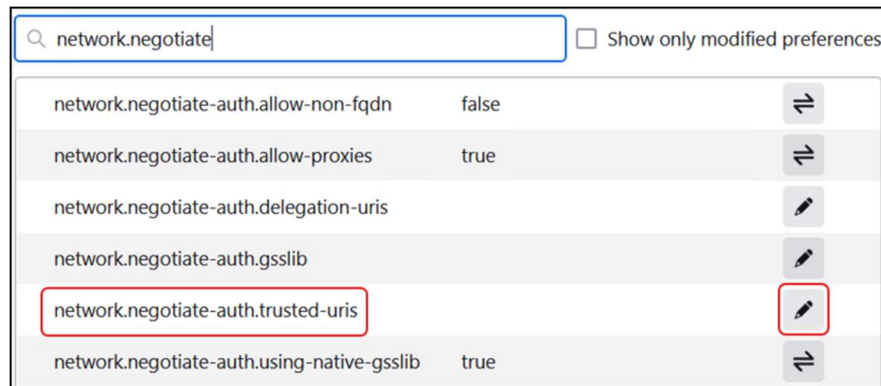


about:config

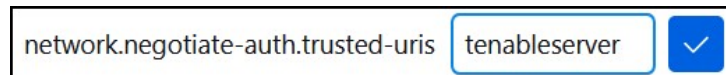
2. Select **Accept the Risk and Continue** if prompted to do so. Use care when modifying the Firefox configuration preferences.



3. Add the Tenable Server fully Qualified Domain Name (FQDN) as a trusted device:
  - a. Enter `network.negotiate-auth.trusted-uris` on the search line.



- b. Select  to edit the `network.negotiate-auth.trusted-uris` setting, and then enter the **Fully Qualified Domain Name (FQDN)** for the server that hosts the Tenable Server. The example uses `https://tenableserver` as the FQDN.



- c. Select the checkbox to save, and then return to the Admin Portal tab.
4. Select **Log in with Active Directory**.

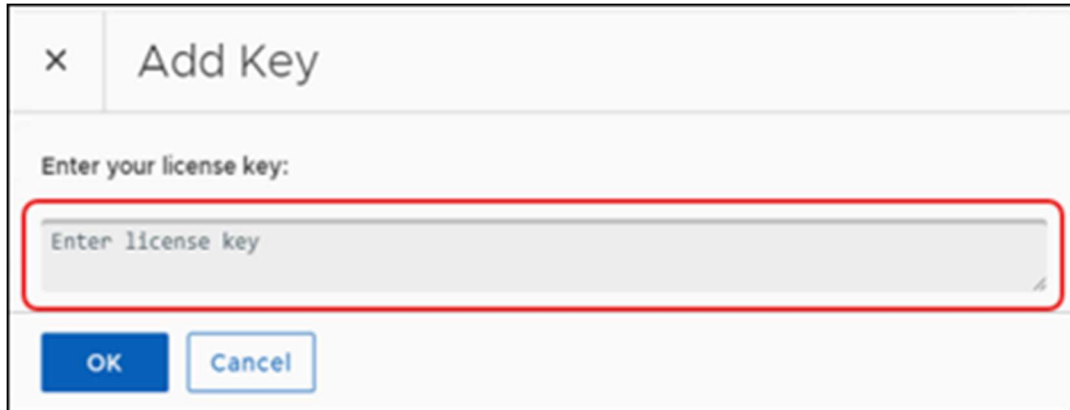
## Licensing Tenable Patch Management

Tenable Patch Management requires a license for each active client. The license key contains the licensed company name and client count. The Tenable server periodically counts all active, healthy, reporting clients as licensed clients.

Enter your license key using the Tenable Patch Management Admin Portal. If you are starting the portal for the first time or your key has expired, the software prompts you for a license key at login.

## Add a License Key

1. Click **Manage Licenses** at the upper-right of the Admin Portal dashboard.
2. Click **Add Key**, and enter your license key.



3. Click **OK** to return to the **Product Licensing** workspace.
4. Wait for the licensing process to complete. For any user-generated changes, OneSite sends a status update when it has enabled the installed solution.

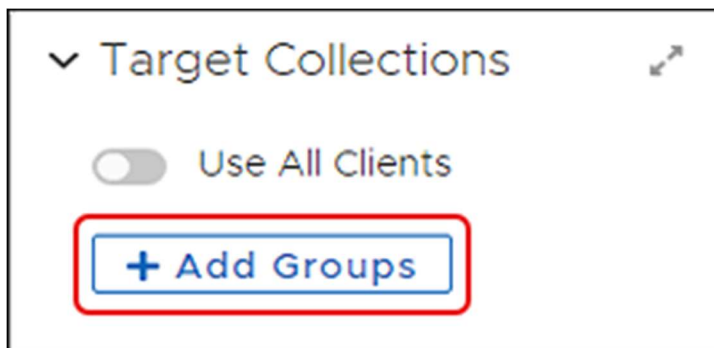
## Add a Licensed Product to a Collection Group

After entering a license key, select a Collection group for the licensed product.

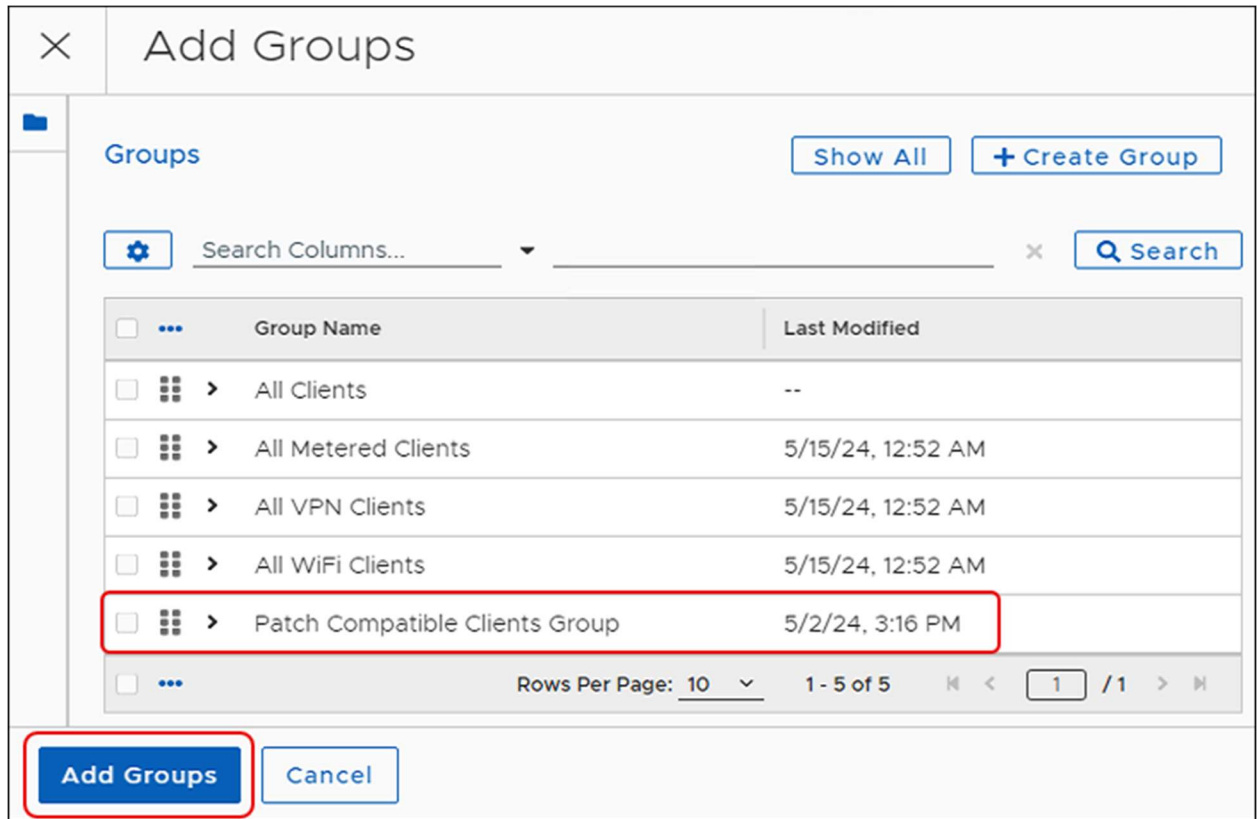
### Caution

Do not select **All Tenable Clients**. Depending on the installed version of Tenable Patch Management Express, doing so can corrupt the patch environment.

1. Select the product name in the **Product Licensing** list.
2. Select **+ Add Groups** in the **Target Collections** section.



This opens the **Add Groups** dialog.



3. Select a **Group Name** from the **Add Groups** table. Tenable recommends choosing **Patch Compatible Clients Group**.
4. Select **Add Groups** on the lower-left corner to return to the **Product Licensing** workspace.

## Tenable Patch Management Express Dashboard

Use the dashboard, available from the admin portal, to manage your patching strategies, review patching status, and more.

### Access the Dashboard

Open the dashboard from the [admin portal](#) using one of the following methods:

- Click **Tenable Patch Management Express** near the top of the page.
- Click **Go to Tenable Patch Management Express** under **Licensed Products**.

This opens the Tenable Patch Management Express Dashboard.

# Tenable Patch Management Setup Wizard

The Tenable Patch Management setup wizard provides step-by-step guidance for your first introduction to Patch Express. The wizard walks you through automatic deployment of patch remediation for each patch vulnerability level (Critical, High, Medium, and Low). You may use Patch Express on its own, or use Patch Express with an integrated partner product.

<b>Welcome</b>	Use the guided setup to configure Tenable Patch Management Express to meet the needs of your organization. See <a href="#">Welcome to Tenable Patch Management Express</a> .
<b>Enablement</b>	Enable automatic deployment of patch remediation for the specified vulnerability level.. See <a href="#">Use Copy From</a> .
<b>Remediation Schedule</b>	Schedule automatic remediation of the specified patch vulnerability level . See <a href="#">Select a Remediation Schedule</a> .
<b>Detection Integrations</b>	Enable detection integrations for the specified patch vulnerability level. See <a href="#">urn:resource:component:12036</a> .
<b>Patch Pre-staging</b>	Enable content pre-staging to download all patches to applicable and licensed devices prior to deployment. See <a href="#">Enable Patch Pre-staging</a> .
<b>Deployment Notifications</b>	Notify administrators about the specified patch deployment. See <a href="#">Configure Deployment Notifications</a> .
<b>Approval</b>	Setup approval before deploying the specified patch vulnerability level patches. See <a href="#">Configure Deployment Approval</a> .
<b>Test Deployment</b>	Deploy the specified patch vulnerability level patches to a test group before production deployment. See <a href="#">Configure Test Deployment</a> .
<b>Test Approval</b>	Setup approval before deploying the specified patch vulnerability level patches to test devices. See <a href="#">Configure Test Approval</a> .
<b>Complete</b>	Complete the Tenable Patch Management Express Setup process and save the settings to the server. See <a href="#">Complete Tenable Patch Management Express Setup</a> .

## Welcome to Tenable Patch Management Express

After you have completed installation, the Guided Setup wizard starts automatically. You may choose to walk through it immediately to start and configure auto-remediation, or cancel the wizard and come back to it later

Select **Begin** to get started. Your first step is [Integrations](#).

## Detection Integrations

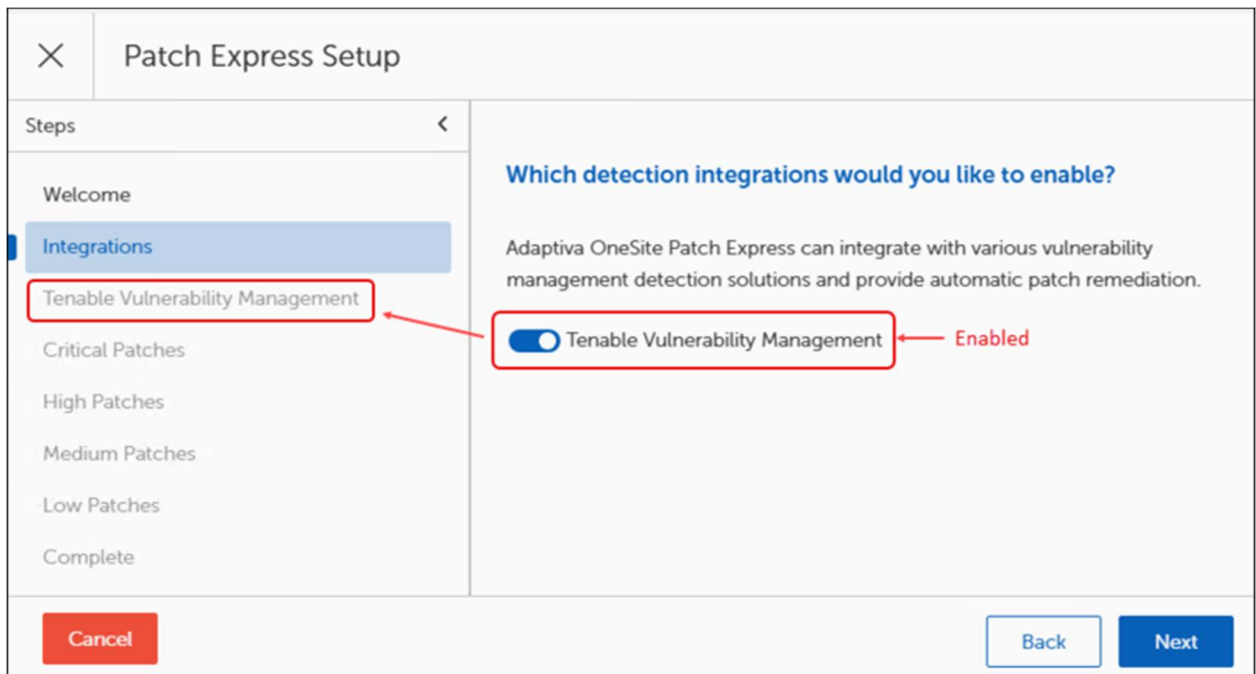
Detection integration means that Tenable Patch Management has detected a licensed partner product and wants to know whether to integrate it.

To integrate a partner product, you must have a valid license. This is in addition to the base license for. Without a valid license, the integration pane has no options for integration. If you don't have a license for your partner product, contact Tenable Customer Support.

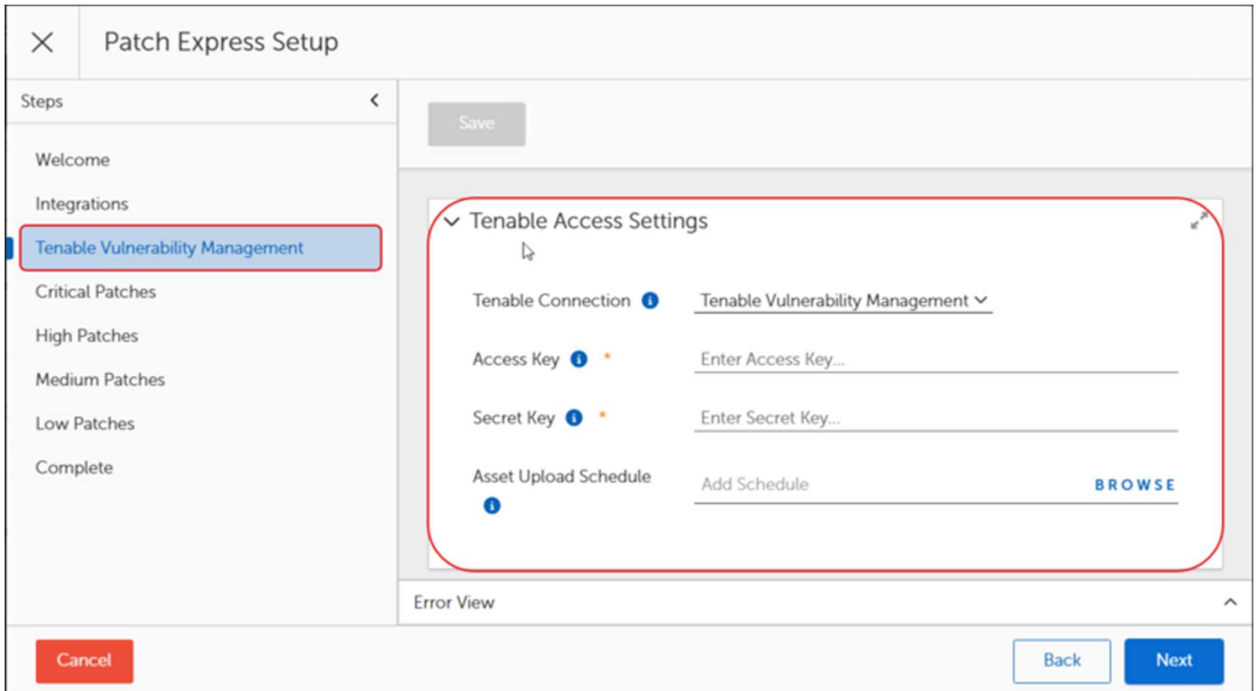
## Integrate a Partner Product

1. Select **Begin** on the **Welcome** screen of the Setup Wizard. This opens the Integrations pane.
  - a. If you have licensed a partner product, you will see it listed here. Continue to the next step.
  - b. If you do not use a partner product, skip to [Enablement](#).
2. Select the **[Partner Product]** toggle to enable or disable (default) integration of your partner product.

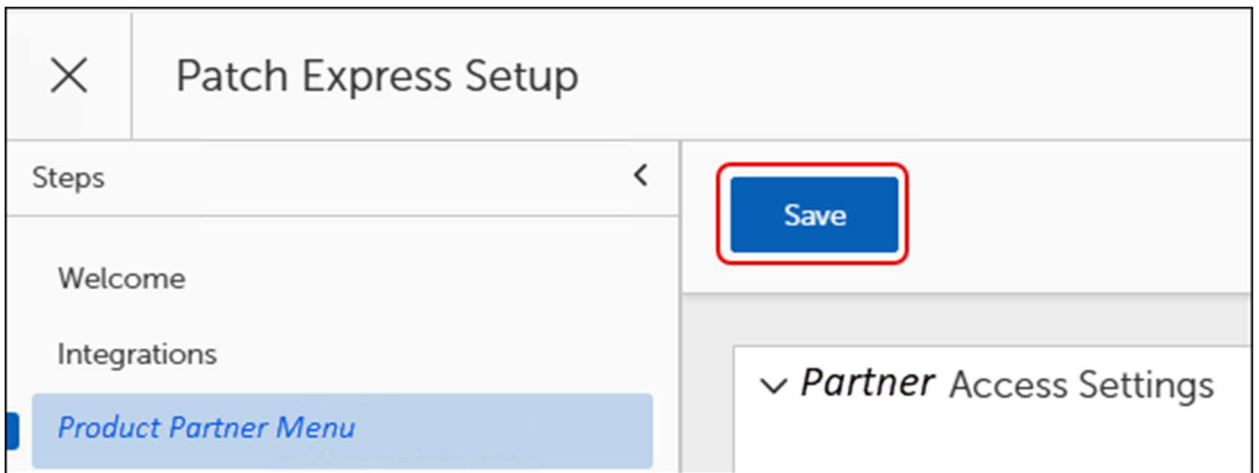
With the product enabled, the Steps of the left navigation menu include a new item related to product integration.



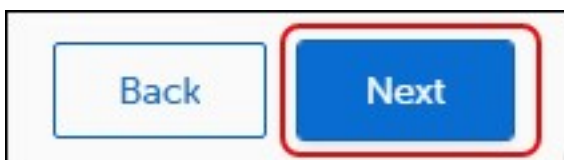
3. Select **Next** to enter the partner product integration details. If you do not have these details, see [Integrate Tenable Vulnerability Management](#) to create or find them.



4. Select **Save** above the partner access settings to save the integration details.



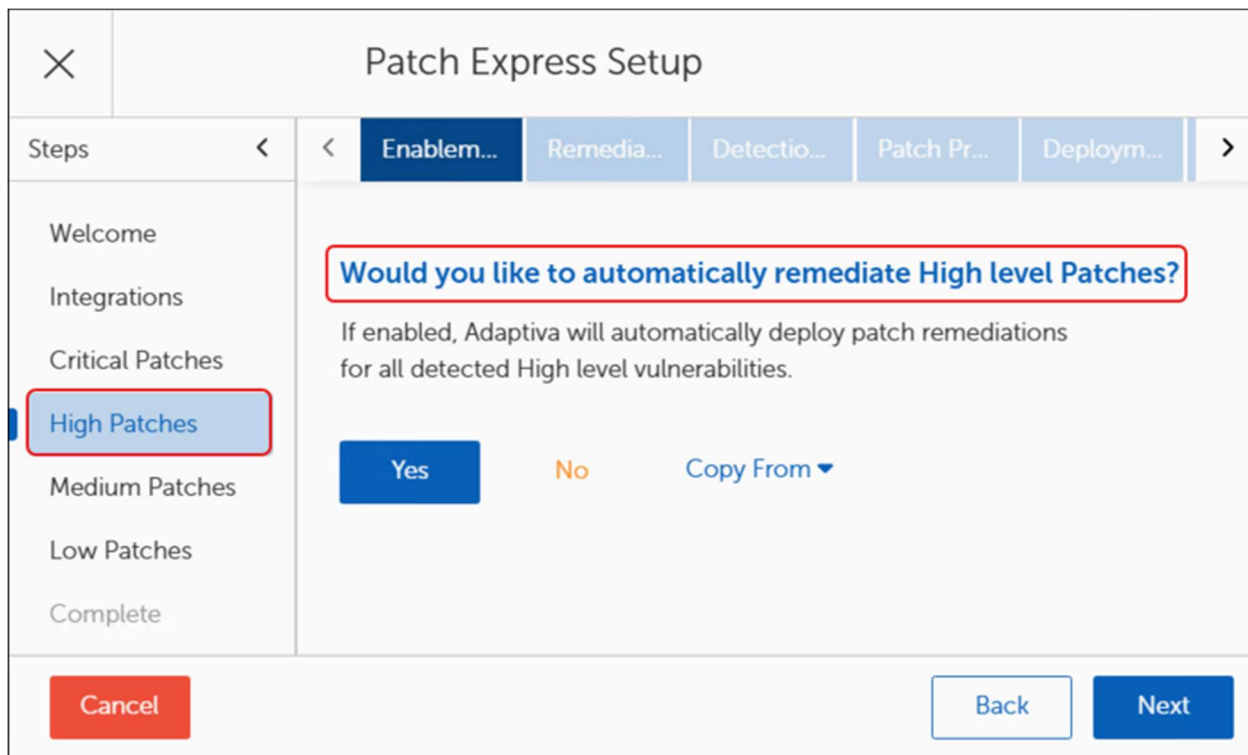
5. Select **Next** on the bottom right corner of the **Patch Express Setup Wizard** to enable auto remediation.



## Use Copy From

When you have completed at least one configuration for a remediation level, you can easily create new levels using the same details, and then customize only those details that might be different, such as Business Unit or approval roles. To copy a patch vulnerability level, complete the following steps on the [Enablement](#) tab:

1. Use one of the following methods to select the Patch severity level that you want to configure or change:



The screenshot shows the 'Patch Express Setup' wizard. The 'Enablement...' step is active. The main content area displays the question: 'Would you like to automatically remediate High level Patches?'. Below the question, it states: 'If enabled, Adaptiva will automatically deploy patch remediations for all detected High level vulnerabilities.' There are three buttons: 'Yes' (blue), 'No' (orange), and 'Copy From' (blue with a dropdown arrow). The 'High Patches' option is selected in the left navigation pane. At the bottom, there are 'Cancel', 'Back', and 'Next' buttons.

- c. If enabled, click the patch severity level from the Steps menu on the left navigation pane of the Patch Express Setup. The example uses High Patches
- d. Otherwise, click **No** to cycle to through the remaining patch severity levels.

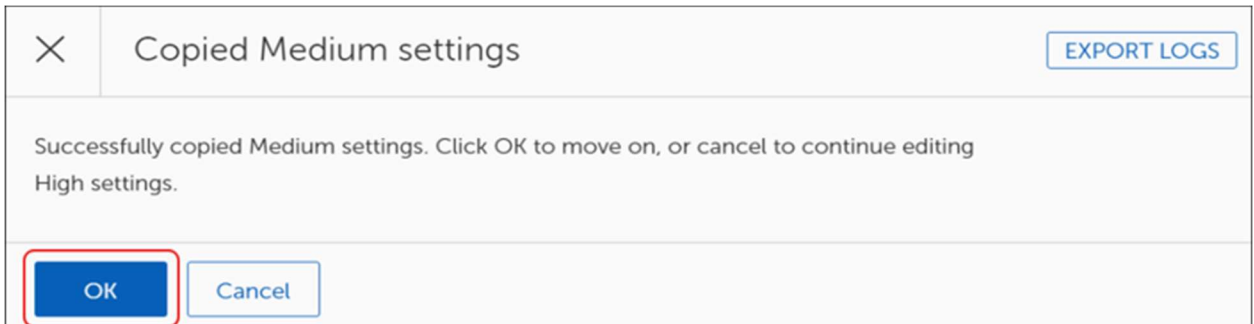
### Tip

Selecting No to cycle through each patch severity level in the wizard without configuring them enables each selection in the Steps menu for easier navigation between levels.

2. Select **Copy From**, and then select a **patch severity level** to copy. The example begins with High level patch remediation, so the available levels available to select are as follows:
  - e. **Copy Auto Remediation Level Low**
  - f. **Copy Auto Remediation Level Medium**

g. **Copy Auto Remediation Level Critical**

3. Select **OK** to return to the **Enablement** tab. The remediation level you started with now uses the same settings as the level you copied.



4. To make any changes to the applied settings, click **OK**, and then select the patch severity level you started with, in this case High Patches.
  - d. Select **Yes** to begin cycling through the applied settings.
  - e. Verify that the applied settings used the correct Remediation, Detection, Patch Pre-staging, Production Deployment and Approvals, and Test Deployment and Approvals.
  - f. Make any modifications necessary to reflect the needs of your environment for the selected patch severity level.
5. Select **Complete** on the left navigation menu, and then click **Finish** to save your changes.
6. Repeat this procedure or cycle through the [Enablement](#) process to configure other severity level patch deployments.

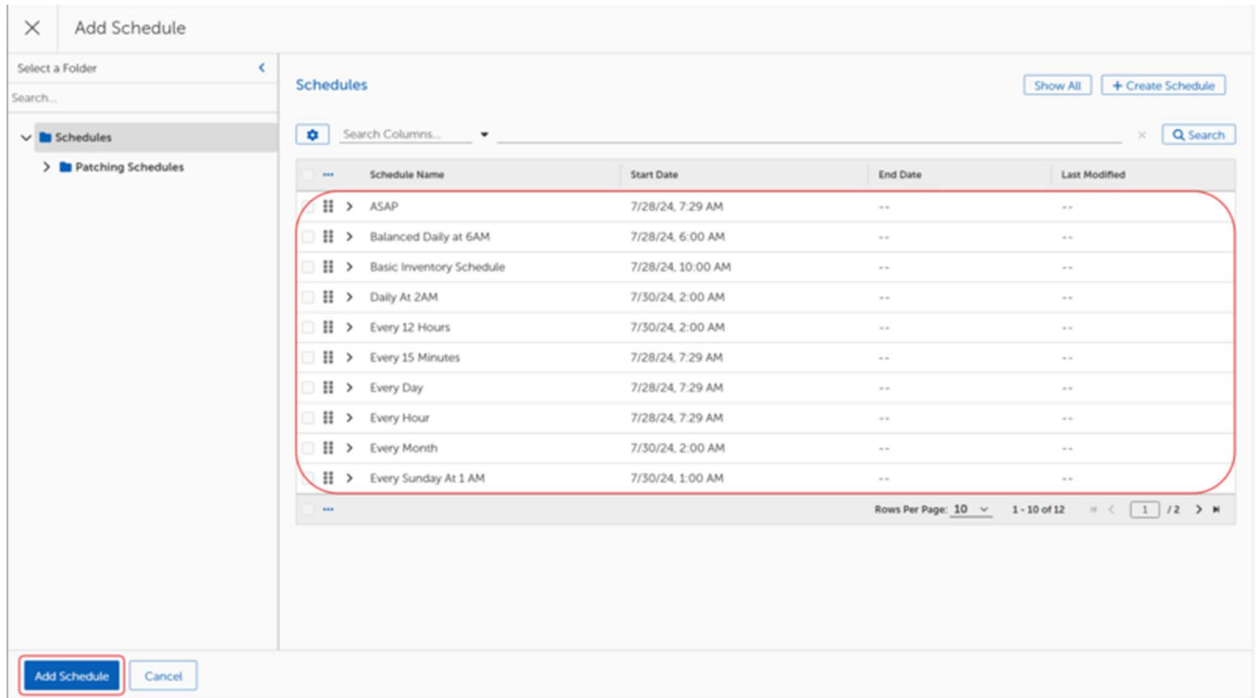
## Select a Remediation Schedule

1. Select **Browse** to open the **Add Schedules** dialog.

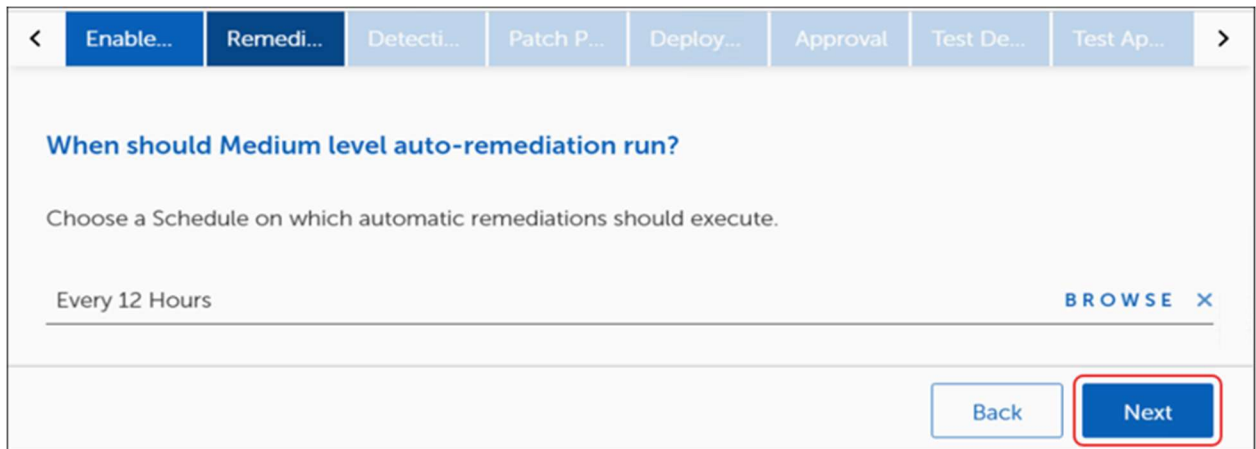


2. Select a **Schedule** to add, and then select **Add Schedules** on the bottom-left corner to return to the **Remediation Schedule** step. You may add only one schedule to a remediation at a time.





3. Select **Next** to go to the **Detection Integrations** step.



## Enable Vulnerability Detection

Choose whether to use Tenable, a partner product, or both to detect vulnerabilities for patches.

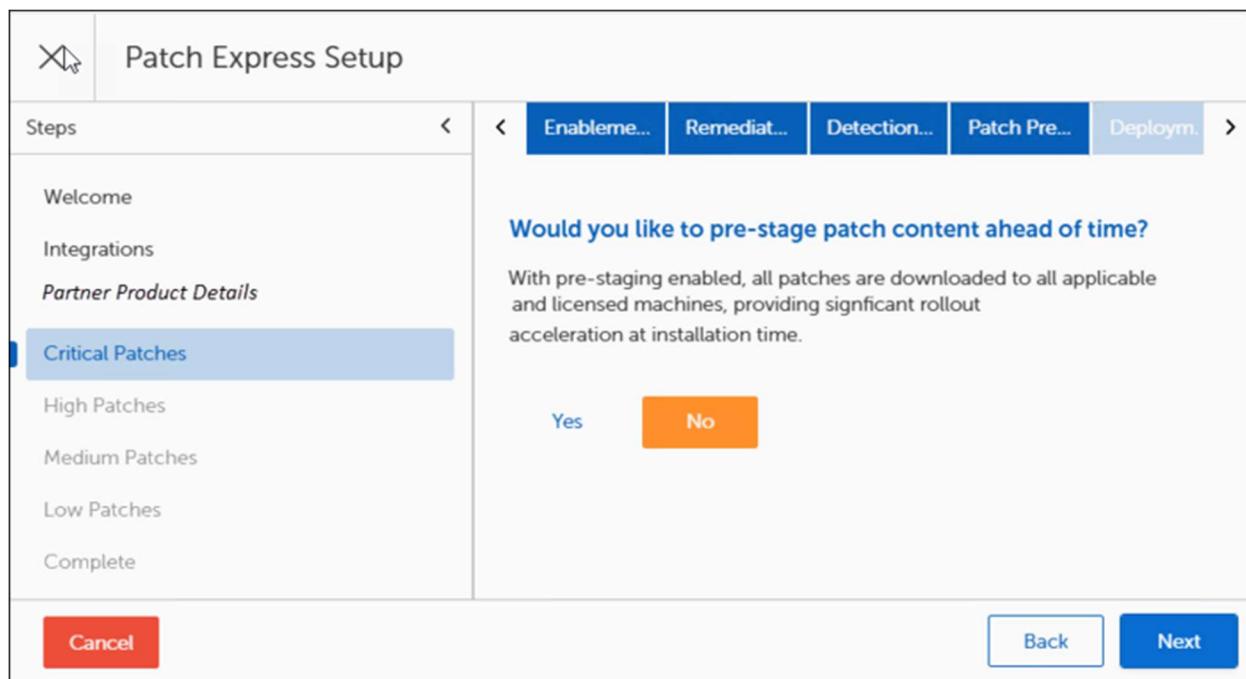
1. Select the **Tenable** or **Product Partner** toggle to enable or disable one or more of the available Detection Integrations. You must enable at least one.
2. Select **Next** to [prestige patch content](#).

## Enable Patch Pre-staging

When you pre-stage patches, Tenable Patch Management downloads the matching severity level patches to all licensed devices prior to deployment. This accelerates rollout time during deployment.

Choose whether to pre-stage patches:

- Select **Yes** to enable patch pre-staging. This takes you to [Configure Deployment Notifications](#).
- Select **No** to skip patch pre-staging. This takes you to [patch approvals](#) (no deployment notification required).
- There is no need to click Next from this tab. If you do click Next, it takes you to the Deployment Notifications tab.



The screenshot shows the 'Patch Express Setup' wizard. The 'Steps' sidebar on the left includes: Welcome, Integrations, Partner Product Details, **Critical Patches** (selected), High Patches, Medium Patches, Low Patches, and Complete. The main content area is titled 'Patch Pre...' and asks: 'Would you like to pre-stage patch content ahead of time?'. Below the question, it states: 'With pre-staging enabled, all patches are downloaded to all applicable and licensed machines, providing significant rollout acceleration at installation time.' There are two buttons: 'Yes' (blue) and 'No' (orange). At the bottom, there are 'Cancel' (red), 'Back' (white), and 'Next' (blue) buttons.

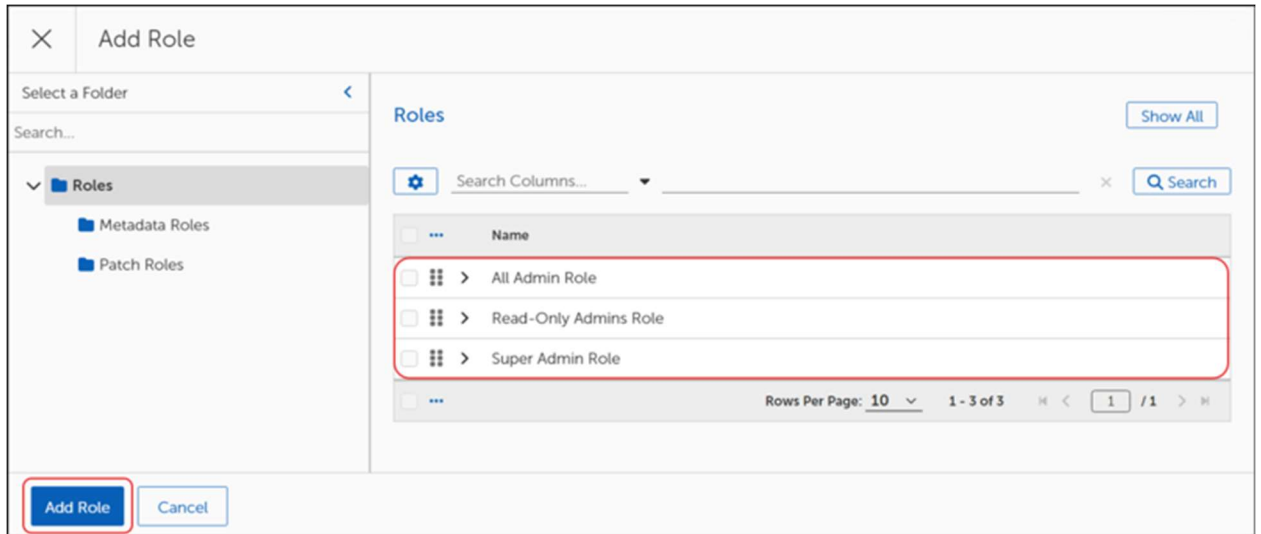
## Configure Deployment Notifications

Choose whether to notify administrators of the vulnerability level patch installation and select the type of administrators to notify based on Roles.

1. Decide whether to notify administrators about the patch deployment:
  - a. Select **Yes** to choose the Roles to notify, and then continue with the next step.
  - b. Select **No** to skip notifications. This takes you to [Approvals](#).

- c. Select Next on the bottom right corner to skip notifications. This takes you to [Approvals](#).

2. Select **Browse** to open the **Add Role** dialog.
3. Select a **Role** to add. You may select only one.

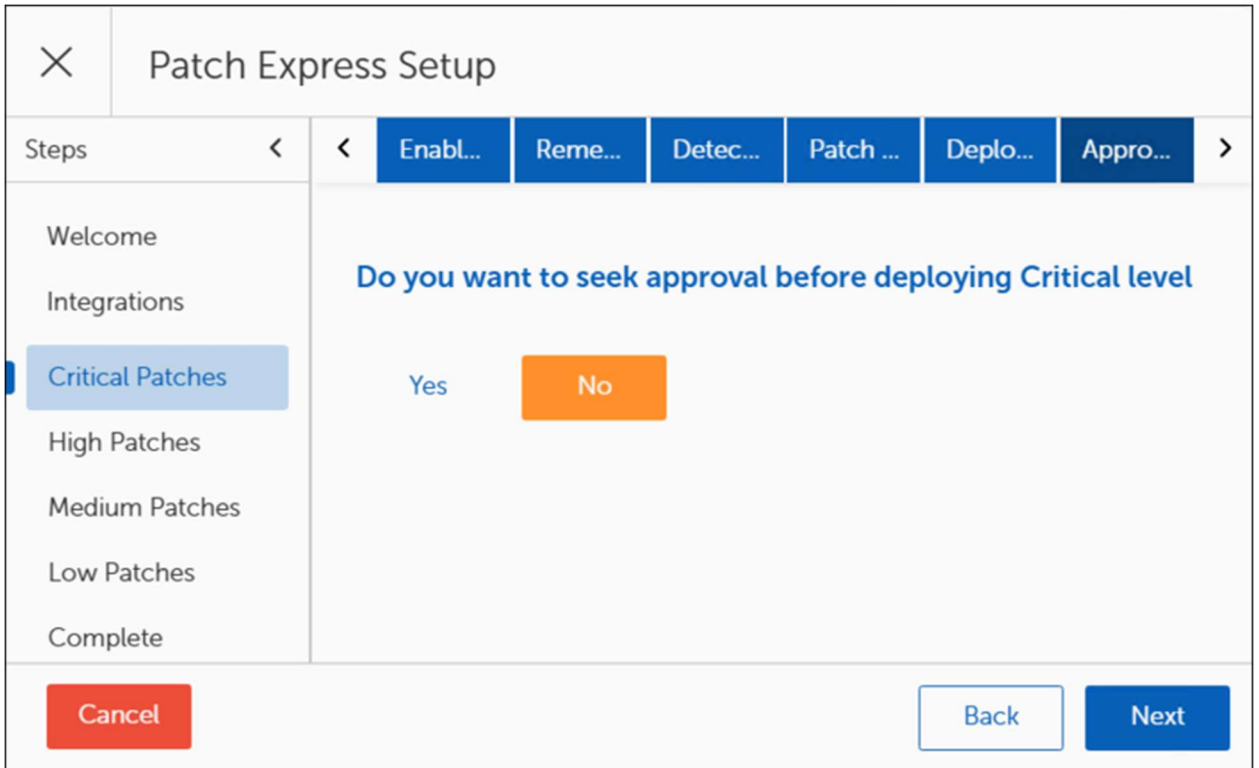


4. Select **Add Role** to save your selection. This takes you directly to the [Approval](#) tab.

## Configure Deployment Approval

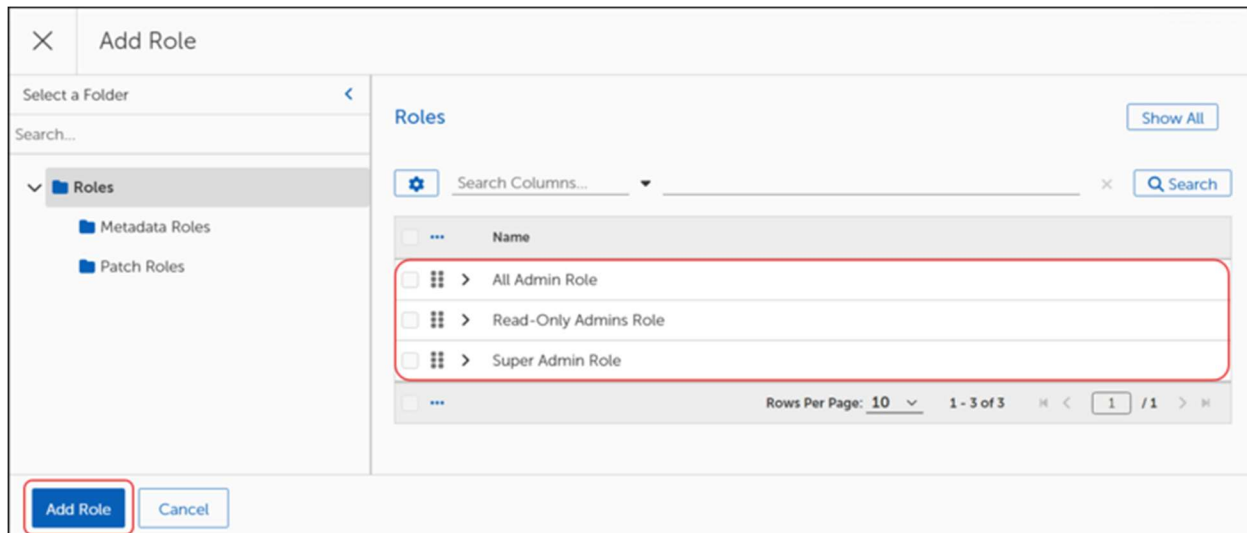
Choose whether to ask administrators to approve of the patch severity level installation and select the type of administrators to approve of the installation based on Roles.

1. Decide whether to request administrator approval of the patch deployment:
  - a. Select **Yes** to choose the Roles to approve of the deployment, and then continue with the next step.
  - b. Select **No** to skip approvals. This takes you to [Configure Test Deployment](#).
  - c. Select Next on the bottom right corner to skip notifications and approvals and go directly to [deploying to a test group](#).



2. Select **Browse** to add an administrator role for approvals:

a. Select a **Role** to add. You may select only one.



b. Select **Add Role** to save your selection. This takes you back to the Approval tab and displays two additional configuration options: Approval Timeout (required) and Load Leveling (optional).

< **Enab...** **Rem...** **Dete...** **Patc...** **Depl...** **Appr...** Test ... Test ... >

### Approval Timeout

Set an amount of time to wait for automatic production deployment approval. If a non-0 value is specified, production deployment will be automatically approved after this duration, even if no approval has been received.

0 Days 0 Hours 0 Minutes

### Do you want to enable load leveling on Medium level patch deployments?

Optionally specify time over which production patch installation is load leveled across all the target machines. If not specified, patches will be deployed immediately on all machines.

3. Set the number of **Days**, **Hours**, or **Minutes** to wait for approval to occur:

< **Enablen...** **Remedia...** **Detectio...** **Patch Pr...** **Deploym...** **Approval** **Test Depl...** **Test Appr...** >

### Approval Timeout

Amount of time to wait for test deployment approval before moving on to production.

0 Days 0 Hours 0 Minutes

- a. A non-zero value means deployment begins after the wait time passes, even if no one has approved.
  - b. If you use a zero value, the deployment waits indefinitely for approval.
4. (Optional) Enable and set a time frame for Load Leveling:

< Enablem... Remedia... Detectio... Patch Pr... Deploym... Approval >

**Do you want to enable load leveling on Critical level patch deployments?**

Optionally specify time over which production patch installation is load leveled across all specified, patches will be deployed immediately on all machines.

**Yes** No

Load Leveling Window

0 Days 0 Hours 0 Minutes

Back Next

- a. Select **Yes** to enable load leveling for the specified level patch deployments. When enabled, load leveling for the production patch installation occurs across all target devices.
- b. Set the number of **Days, Hours, or Minutes** for load leveling to occur prior to initiating production patch deployment.  
  
If you don't specify a load leveling time, production patch installation deployment to all devices occurs immediately.
- c. Select **Next** to set up deployment to a test environment prior to production

## Configure Test Deployment

Choose whether to deploy the vulnerability patch installation to a test group prior to production deployment (recommended).

< Enablem... Remedia... Detectio... Patch Pr... Deploym... Approval Test Depl... Test >

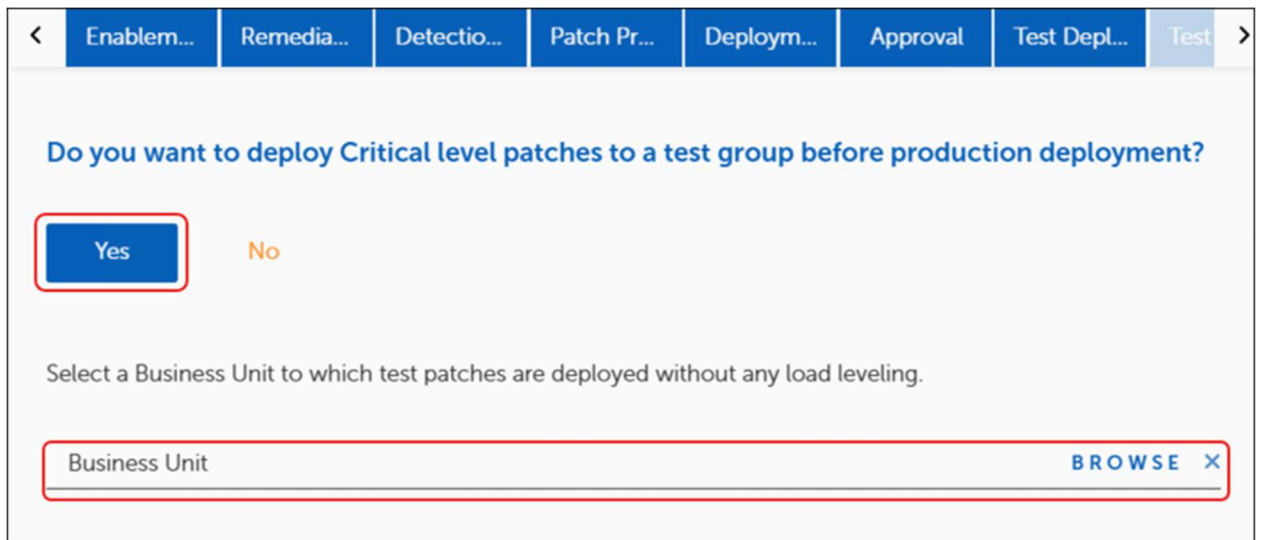
**Do you want to deploy Critical level patches to a test group before production deployment?**

Yes **No**

Back Next

1. Decide whether to deploy the patch installation to a test group (recommended):
  - a. Select **Yes** to configure test group installation, and then continue with the next step.
  - b. Select **No** to skip setting up a test environment and have all vulnerability patch installations deploy to the production environment.

This takes you back to the [Enablement](#) tab where you can configure remediation for a different vulnerability level.
  - c. Select Next on the bottom right corner to skip setting up a test environment and go directly to test approvals.
2. Select **Browse** to show the available Business Units.



3. Select the **Business Unit** to use as the test environment, and then click **Add Business Unit** on the bottom left corner of the dialog:
  - d. Patches deployed to a test environment do not use load leveling.
  - e. If Patch Pre-staging is enabled, the patch is pre-staged to all target machines, and then the machines assigned to the business unit that you specified for the test deployment.



× Add Business Unit

⚙ Search Columns... × 🔍 Search

<input type="checkbox"/> ...	Name
<input type="checkbox"/> >	All Clients Business Unit
<input type="checkbox"/> >	Architecture
<input type="checkbox"/> >	Architecture - 32-bit Systems
<input type="checkbox"/> >	Architecture - 64-bit Systems
<input type="checkbox"/> >	Office Type
<input type="checkbox"/> >	Office Type - Default
<input type="checkbox"/> >	Office Type - VPN
<input type="checkbox"/> >	Office Type - Wi-Fi
<input type="checkbox"/> >	OneSiteCloud License Business Unit

Add Business Unit Cancel

4. Choose whether to create preferences or test duration:

< Enablem... Remedia... Detectio... Patch Pr... Deploy... Approval Test Depl... Test Appr...

### Do you want to set patching preferences for this Business Unit?

Patching Preferences allow you to control maintenance windows, user interaction settings, and reboots.

+ Create Preferences

#### Test Deployment Duration

Optional: specify the amount of time for which patch deployment will wait after initiating test patch deployment, before initiating production patch deployment. If set to 0, production patch deployment will be initiated without any wait.

0 Days 0 Hours 0 Minutes

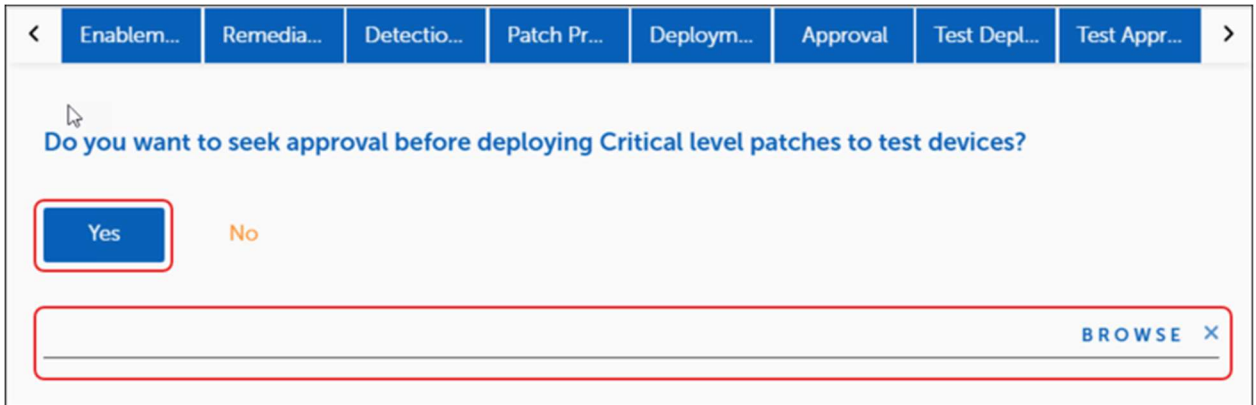
Back Next

- a. To create preferences, click **+ Create Preferences** to control maintenance windows, user interaction settings, and reboots for the selected test environment. See [Patching Preferences](#) for configuration guidance.
  - b. To create a test duration (Optional), set the number of **Days, Hours, or Minutes** to specify how long the test patch deployment process will run before initiating production patch deployment.
5. Select **Next** to set test approval requirements.

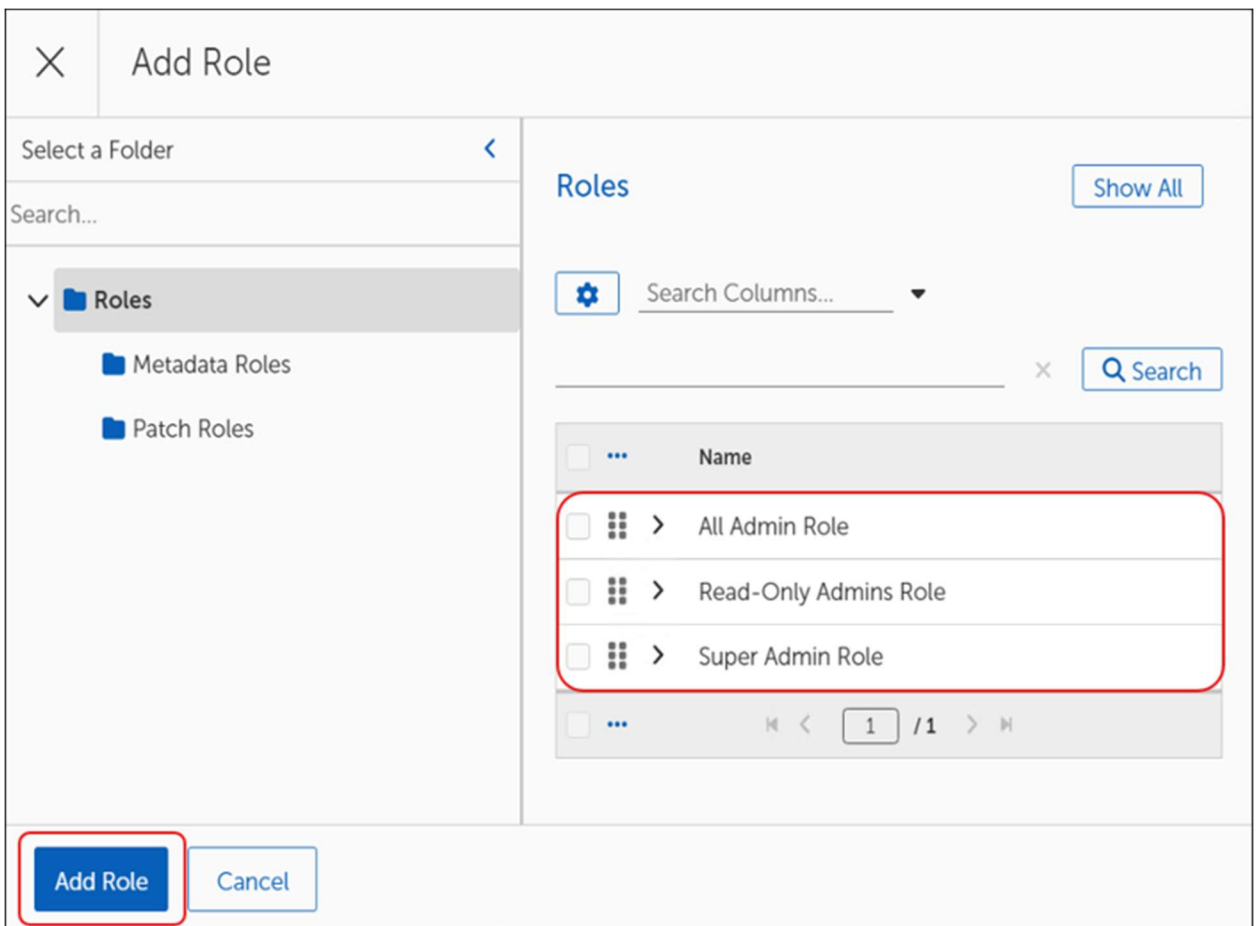
## Configure Test Approval

Decide whether to ask administrators to approve of deploying the patch installation to a test environment and select the type of administrators to approve based on Roles.

1. Decide whether to request administrator approval of the patch deployment:
  - a. Select **Yes** to choose the Roles to approve of the deployment, and then continue with the next step.
  - b. Select **No** to skip approvals. This takes you to back to Enablement where you can configure remediation settings for another vulnerability level.
  - c. Select Next on the bottom right corner to go directly to back to Enablement where you can configure remediation settings for another vulnerability level.



2. Select **Browse** to open the **Add Role** dialog.
3. Select a **Role** to add, and then click **Add Role**. to return to the Test Deployment tab.



4. Set the number of **Days**, **Hours**, or **Minutes** to wait for approval to occur:

< Enablem... Remedia... Detectio... Patch Pr... Deploym... Approval Test Depl... Test Appr... >

### Approval Timeout

Amount of time to wait for test deployment approval before moving on to production.

0 Days 0 Hours 0 Minutes

Back Next

- a. A non-zero value means deployment begins after the wait time passes, even if no one has approved.
  - b. If you use a zero value, the deployment waits indefinitely for approval.
5. Select **Next** on the bottom right corner of the dialog to return to the [Enablement](#) tab:
- a. Repeat all steps for the next vulnerability level configure remediation for other vulnerability levels.
  - b. To skip other vulnerability levels and finish the Express Setup, click **Next**.

## Complete Tenable Patch Management Express Setup

Select **Finish** on the lower-right corner of the **Patch Express Setup** dialog. The patch remediation automatically begins on the specified schedules when you complete the Tenable Patch Management Express Setup wizard.

× Patch Express Setup

Steps <

- Welcome
- Integrations
- Critical Patches
- High Patches
- Medium Patches
- Low Patches
- Complete**

**That's it. Ready to start patching?**

**Automatic patch remediation will begin on the specified schedules upon confirmation.**

Click "Finish" to save these settings to the server.

**Cancel** Back **Finish**

# Integrate Tenable Vulnerability Management

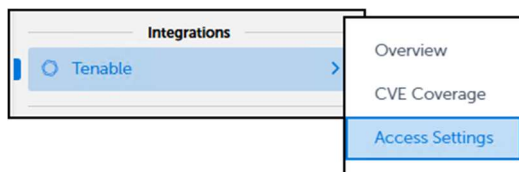
With this integration, a configuration automatically patches vulnerabilities identified by Tenable Security Center® and Tenable Vulnerability Management products. This integration bridges the gap between identifying vulnerabilities and immediately patching them, increasing the speed of securing multiple devices and eliminating security threats.

To access Tenable Vulnerability Management from Tenable Patch Management, you must have a license from Tenable.

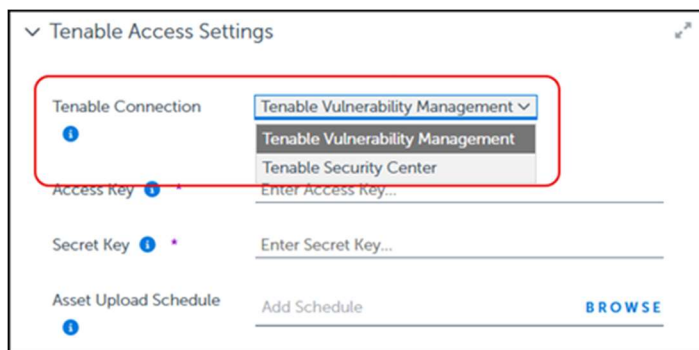
## Add Tenable Access Settings to Tenable Patch Management

To integrate Tenable Vulnerability Management (cloud) or Tenable Security Center (server) details with Tenable Patch Management, complete the following steps:

1. Create Tenable Access keys. If you do not have a Tenable Access Key or Secret Key, see [Create Tenable Access and Secret Key](#).
2. Log on to the [Tenable Patch Management Admin Portal](#) and open the [Tenable Patch Management Dashboard](#).
3. Select **Tenable Vulnerability Management** in the left navigation menu of the dashboard, and then select **Access Settings**.

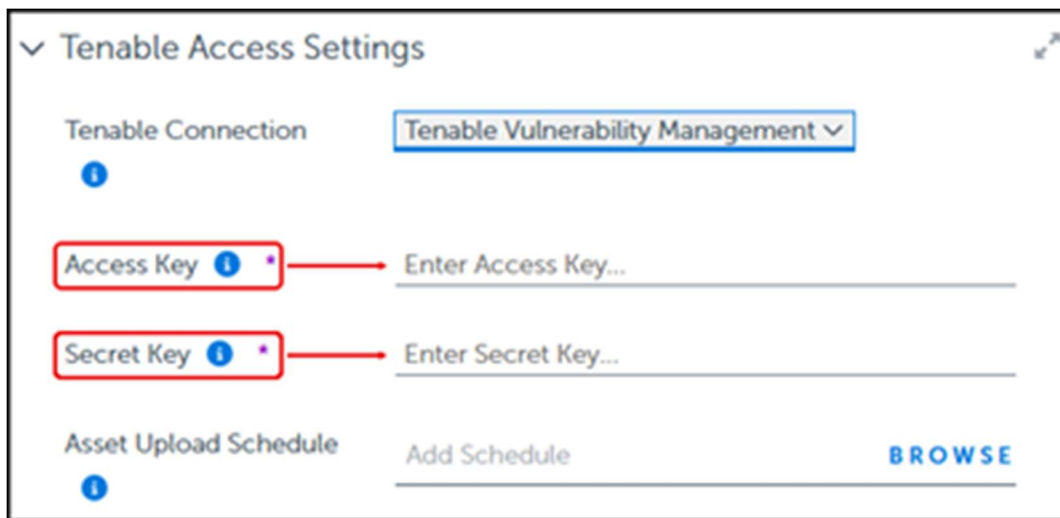


5. Select the Tenable Connection you want to create:
  - a. Select Tenable Vulnerability Management, and then see [Configure Tenable Vulnerability Management Settings](#).
  - b. Select Tenable Security Center, and then see [Configure Tenable Security Center Settings](#).



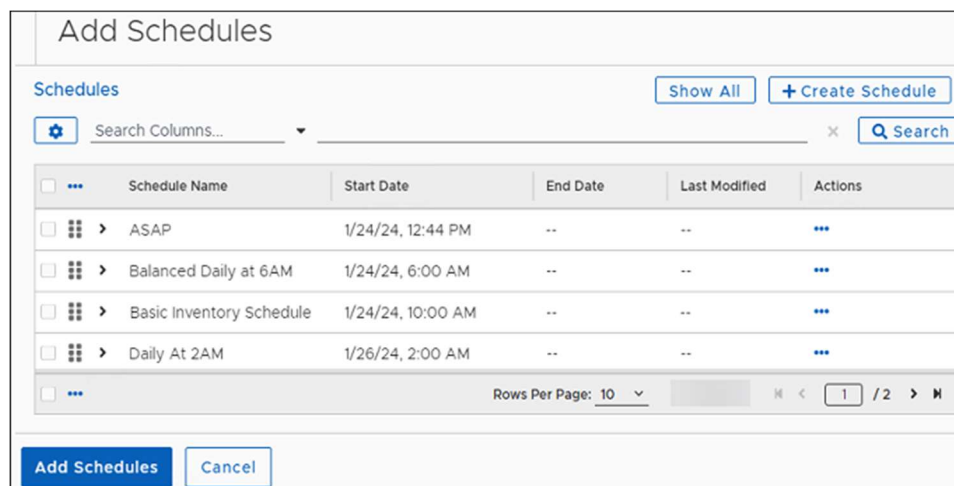
## Configure Tenable Vulnerability Management Settings

6. Enter the **Access Key** and the **Secret Key** for Tenable Vulnerability Management.



The screenshot shows the 'Tenable Access Settings' configuration page. At the top, there is a dropdown menu for 'Tenable Connection' set to 'Tenable Vulnerability Management'. Below this, there are two input fields: 'Access Key' and 'Secret Key', both with red boxes around them and red arrows pointing to their respective input areas. The 'Access Key' field is labeled 'Enter Access Key...' and the 'Secret Key' field is labeled 'Enter Secret Key...'. At the bottom, there is an 'Asset Upload Schedule' section with an 'Add Schedule' button and a 'BROWSE' button.

7. Add an **Asset Upload Schedule**:
  - a. Select **Browse** to select the scheduled time for Tenable Patch Management to upload the Tenable assets.
  - b. Select a **Schedule Name**, and then click Add Schedules on the bottom left of the dialog. to return to the Tenable Access Settings workspace.



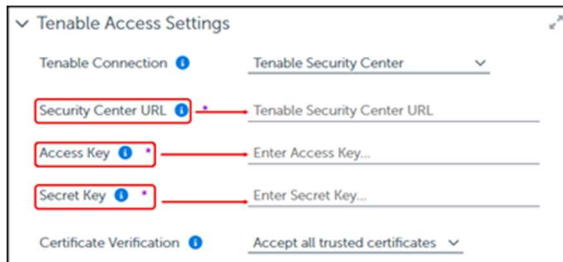
The screenshot shows the 'Add Schedules' dialog box. It features a table with columns for 'Schedule Name', 'Start Date', 'End Date', 'Last Modified', and 'Actions'. The table contains four rows of schedules: 'ASAP', 'Balanced Daily at 6AM', 'Basic Inventory Schedule', and 'Daily At 2AM'. At the bottom of the dialog, there are 'Add Schedules' and 'Cancel' buttons.

...	Schedule Name	Start Date	End Date	Last Modified	Actions
<input type="checkbox"/>	ASAP	1/24/24, 12:44 PM	--	--	...
<input type="checkbox"/>	Balanced Daily at 6AM	1/24/24, 6:00 AM	--	--	...
<input type="checkbox"/>	Basic Inventory Schedule	1/24/24, 10:00 AM	--	--	...
<input type="checkbox"/>	Daily At 2AM	1/26/24, 2:00 AM	--	--	...

8. Select Save on the upper-left corner of the dialog:
  - a. Check the **Error View** and resolve any errors.
  - b. Select **Save** again if you make any changes.
9. Select **Business Units**, and then select **Business Units** to verify your access to **Tenable ACR Business Units**.

## Configure Tenable Security Center Settings

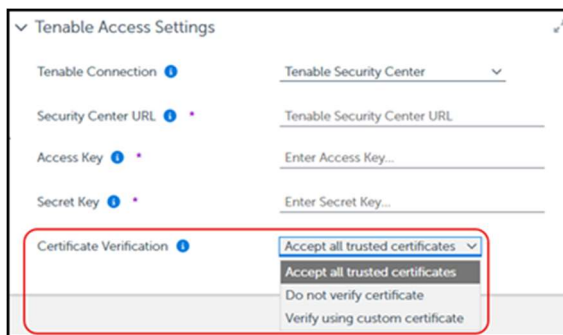
10. Enter the Security Center URL, and then add the Access Key and Secret Key for Tenable Security Center.



The screenshot shows the 'Tenable Access Settings' dialog box. It has a title bar with a dropdown arrow and a close button. Below the title bar, there are several settings:

- Tenable Connection:** A dropdown menu currently set to 'Tenable Security Center'.
- Security Center URL:** A text input field with a red box around it and a red arrow pointing to the label 'Tenable Security Center URL'.
- Access Key:** A text input field with a red box around it and a red arrow pointing to the label 'Enter Access Key...'.
- Secret Key:** A text input field with a red box around it and a red arrow pointing to the label 'Enter Secret Key...'.
- Certificate Verification:** A dropdown menu currently set to 'Accept all trusted certificates'.

11. Select a Certificate Verification to use for Tenable Security Center APIs:
  - a. Accept all trusted certificates:
  - b. Do not verify certificate:
  - c. Verify using custom certificate:



The screenshot shows the 'Tenable Access Settings' dialog box with the 'Certificate Verification' dropdown menu open. The dropdown menu has three options:

- Accept all trusted certificates (highlighted with a blue bar)
- Do not verify certificate
- Verify using custom certificate

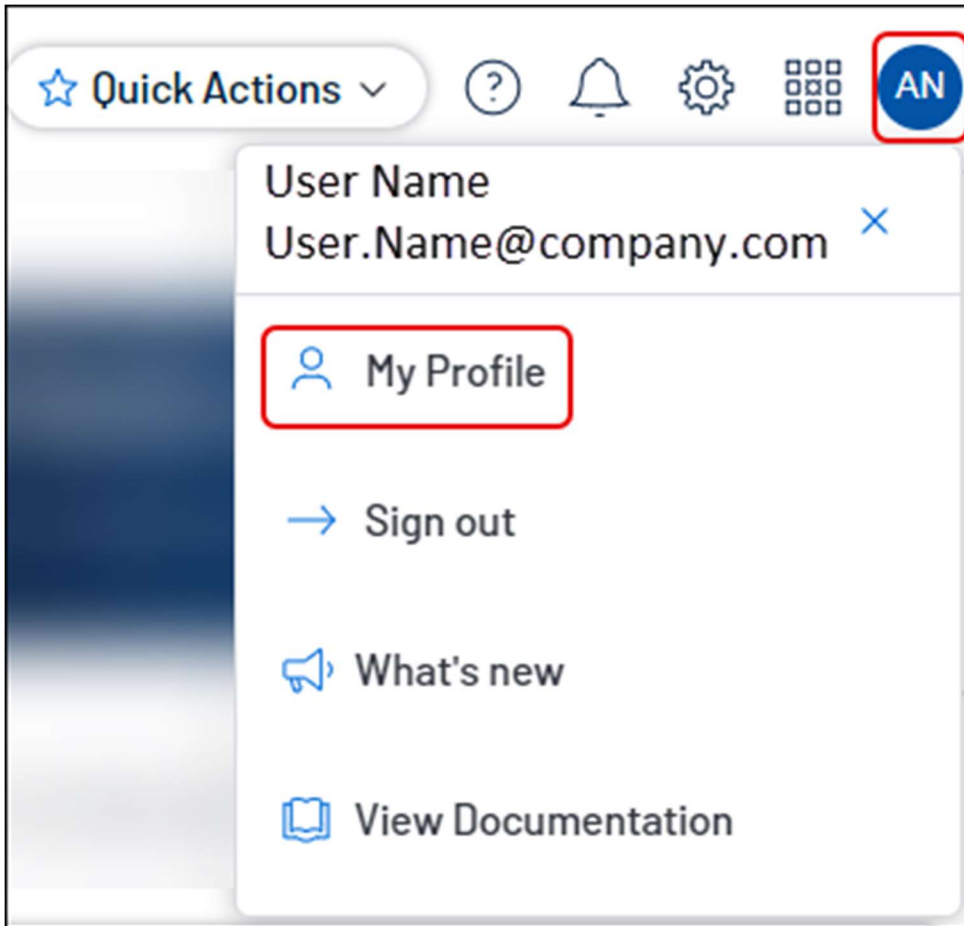
12. Select Save on the upper-left corner of the dialog:
  - a. Check the **Error View** and resolve any errors.
  - b. Select **Save** again if you make any changes.
13. Select **Business Units**, and then select **Business Units** to verify your access to **Tenable ACR Business Units**.

## Create Tenable Access and Secret Key

Create Tenable API Keys to access and integrate client settings with Tenable.

1. Log in to your **Tenable** account, and then click the user icon on the upper right.





2. Select **My Profile**, and then click **API Keys**.

The screenshot shows the Tenable 'My Account' interface. At the top left is the Tenable logo and 'My Account' text. On the top right are icons for settings, a grid, and a user profile labeled 'AN'. Below the header, there's a 'MY ACCOUNT' section with a blurred area and a book icon. A vertical navigation menu on the left includes 'UPDATE ACCOUNT', 'GROUPS', 'PERMISSIONS', and 'API KEYS', with 'API KEYS' highlighted by a red box. The main content area is titled 'API Keys' and contains a warning: 'API Keys are u with requests' and 'NOTICE: API k retrieved later'. A 'Generate' button is located at the bottom right. A dropdown menu is open, showing the user's name 'User Name' and email 'User.Name@company.com', along with options: 'My Profile', 'Sign out', 'What's new', and 'View Documentation'.

3. Select Generate and review the warning:

The dialog box is titled 'Generate API Keys' and contains the following text: 'WARNING: This will replace any existing keys and unauthorize all applications currently utilizing them. Are you sure you want to continue?'. At the bottom, there are two buttons: 'Continue' and 'Cancel'.

4. Select Continue when you are ready to proceed. This generates the API Keys.

● UPDATE ACCOUNT **API Keys**

● GROUPS API Keys are used to authenticate with the Tenable Vulnerability Management R with requests using the "X-APIKeys" HTTP header. For more details, see the [API](#)

● PERMISSIONS **NOTICE:** API Keys are only presented upon initial generation. Please store them retrieved later and will need to be regenerated if lost.

● API KEYS

**Custom API Keys**

ACCESS KEY:  
9ba2dd2b687b12ff34a36a85336973791c3eaf73aec67a6e87454cc1f7a00dec

SECRET KEY:  
a3db5dbd983231251002a16111c2dc5527e78660ddaf0dce2ade1bedf890a3ad

### Important

Save the **Custom API Keys** so you can access them as needed. The system cannot recover these keys for you.


5. See [Add Tenable Access Settings to Tenable Patch Management](#) to complete the integration.

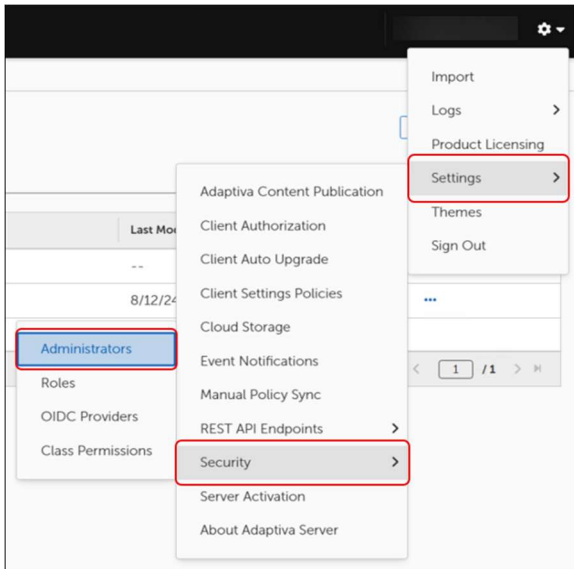
## Administrators and Roles

View, create, or modify Administrators and Roles. Changes made here effect all licensed OneSite products.

After integrating Tenable with Tenable Patch Management, you can view your list of Tenable users and assigned roles for your integrated hosts. To make any changes to Administrators or Roles, you must use the Tenable product.

## Access Security Settings

1. Select  on the upper right of the [OneSite Admin Portal](#) dashboard.
2. Select **Settings > Security > Administrator** to open the **Settings** page with the **Administrators** tab selected. To open to a different tab, select a different item from the final menu.



3. Select **Show All** to view existing administrators.

## View Administrators

1. Select an **Administrators** folder from the Administrators tab of [Security Settings](#).
2. Select **Show All** to list all Administrators in the selected folder.

To make any changes to Administrators, you must use the Tenable product.

## Create a New Administrator

1. Select an **Administrators** folder from the Administrators tab of [Security Settings](#), and then select **+ NEW** to open the new administrator template.
2. Enter the **Administrator Details**:
  - a. Select the **Admin Type** login from the list. Tenable recommends Windows Active Directory.
  - b. Enter the email address and login details for the new administrator.
3. Enter the **User Details**:
  - a. Add the **Name** and contact details for the new administrator.
  - b. Choose country codes from the drop-down lists for phone numbers.

User Details  
 First Name \*   
 Last Name \*   
 Voice Phone Number   
 After Office Phone Number   
 Text Message Phone Number   
 WhatsApp Phone Number   
 Teams Webhook URL

4. Assign **Direct Roles**:

- a. Select **+ Manage Roles**.

Direct Roles ⓘ  
 Roles

- b. Select one or more roles for the new administrator:

- High level roles include **All Admin Role**, **Read-only Admin Role**, and **Super Admin Role**.
- Patch Express roles include **Patch Express Administrator**.
- To create additional roles, you must use the Tenable product.

- c. Select **Manage Roles** on the bottom-left corner of the dialog to return to the .

5. Select **Save** at the top left to save the new administrator.

- a. Check the **Error View** and resolve any errors.
- b. Select **Save** again if you make any changes.

## Create a Microsoft Teams Webhook URL

When adding a new administrator or modifying administrator details in Tenable Patch Management , add a Teams Webhook URL to post notices to a Teams channel, and then assign that URL in Tenable Patch Management , to your administrators. Administrators can check the Teams channel for patch notifications and take the necessary action.

1. Go to Microsoft.com for instructions on creating a Team and a Channel. The links below go to a third-party website outside of the Tenable domain:

- c. Go to [Microsoft Windows Team and Channel topics](#) to set up a new channel in an existing Team in Microsoft Teams, or create a new Team and add a channel for patch notification purposes.
  - d. Go to [Create an Incoming Webhook](#) to create the Webhook URL.
2. Open the **Admin Portal**, and then navigate to **Settings > Security > Administrators**.
  3. Open an existing administrator or select **+NEW** to create a new Administrator.
  4. Scroll down to **Teams Webhook URL** under **User Details**, and then paste the URL you generated in Step 1b into the associated text box.
  5. Return to [Create a New Administrator](#) to complete any other administrator details.

## View Roles

1. Select a **Roles** folder from the Roles tab of [Access Security Settings](#).

The screenshot shows the 'Roles' tab in the Admin Portal. The left sidebar has a 'Roles' folder selected, with sub-folders 'Metadata Roles' and 'Patch Roles'. The main area displays a table of roles:

Name	Actions
All Admin Role	...
Read-Only Admins Role	...
Super Admin Role	...

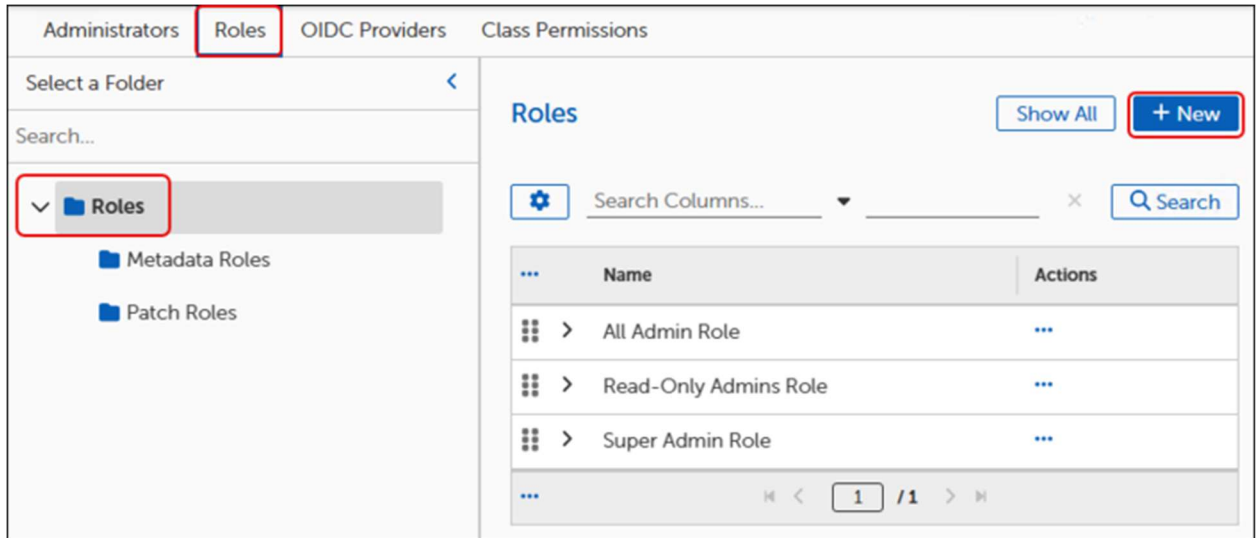
At the top right of the main area, there is a 'Show All' button (highlighted with a red box) and a '+ New' button. Below the table, there is a pagination control showing '1 / 1'.

2. Select **Show All** to list all Roles in the selected folder.

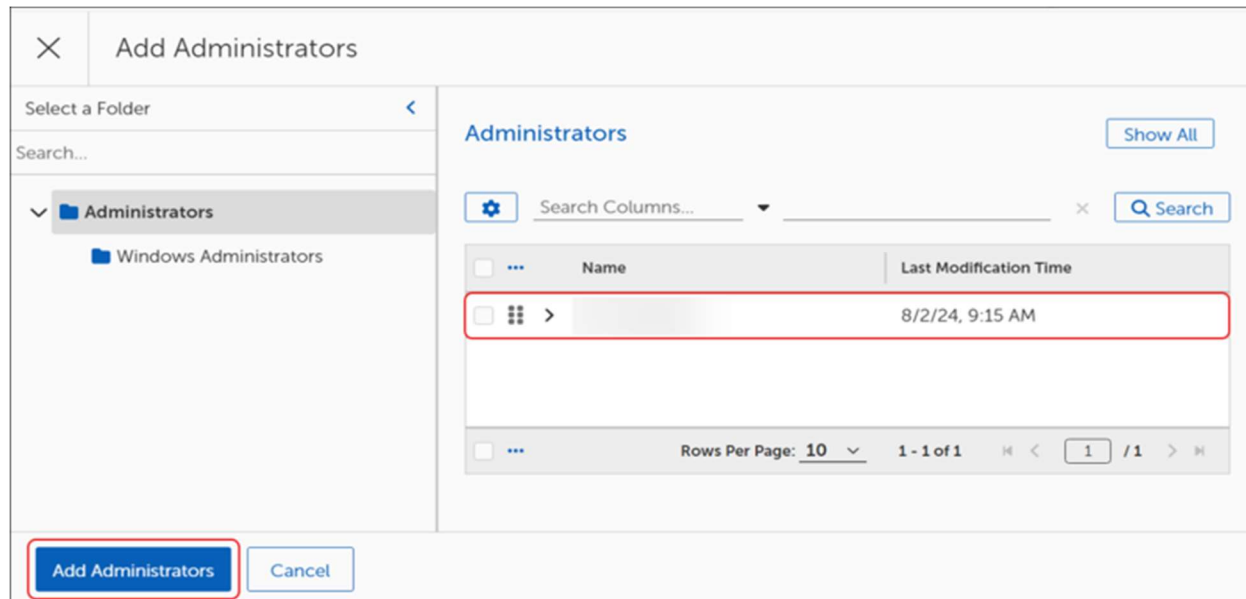
To make any changes to Roles, you must use the Tenable product.

## Create a New Role

1. Select a **Roles** folder from the Roles tab of [Security Settings](#), and then select **+ NEW** to open a new Role template.



2. Enter a **Role Name** and a detailed **Role Description** in the **Role Properties** workspace.
3. Add one or more **Direct Administrators** in the **Role Membership** section:
  - a. Select **Add Administrators** to open the **Add Administrators** dialog.
  - b. Select one or more administrators from the table for the new role.



- c. Select **Add Administrators** to return to the Role template.
4. Add an existing **AD Group** (Active Directory):
  - a. Select **Add AD Group** to open the **Active Directory Group** dialog.

Active Directory Groups

[+ Add AD Group](#)

No data provided

- b. Enter the the **Domain Name** and **Group Name**, and then select **Check Group** to locate. If it exists, the group name appears in the data table.

✕ Active Directory Group

Domain Name

Group Name

[Check Group](#)

No data provided

[Add AD Group](#) [Cancel](#)

- c. Select **Add AD Group** to return to the Role template.



5. Select **Save** at the top left to save the new role:
  - a. Check the **Error View** and resolve any errors.
  - b. Select **Save** again if you make any changes.

# Best Practices for Patch Express

After licensing Tenable Patch Management Express, you can enable Auto Remediation, set a schedule, and begin using Tenable Patch Management immediately. Auto Remediation targets every licensed Tenable Client. The Tenable Server periodically counts all active, healthy, and reporting clients as licensed clients.

Auto Remediation deploys patches without requiring approvals until you configure production or test deployment settings. The deployment configuration used depends on the severity setting of the Auto Remediation template and whether you have configured any approval requirements.

Tenable recommends customizing a few administrative items before you begin.

- Create Administrators and assign roles using the Admin Portal. When Tenable Patch Management Express deploys patches, it uses the assigned roles to send notifications of required approval. See [Administrators and Roles](#).
- Create a Business Unit using the Patch Express dashboard. Use this Business Unit for testing deployments prior to production. See [Business Units](#) for more information.

To further customize Patch Express deployment, you can modify the following settings prior to using Auto Remediation.

- **Patching Preferences:** Specify maintenance window and user interaction settings for a target Business Unit.
- **Maintenance Windows:** Manage maintenance window options.
- **User Interaction Settings:** Manage user interaction settings.
- **Customize Products:** Target a deployment wave for a specific product.
- **Auto Remediation:** Enable Auto Remediation, define deployment settings, and choose whether to deploy to a test group prior to production.

# Menu Objects for Tenable Patch Management

The Tenable Patch Management menu in the left pane of the Tenable Patch Management dashboard lists the objects available for configuring and managing your patching requirements. Any references to [Intent Schema](#) relate specifically to the group of navigation objects between Integrations and Platform in the left navigation menu of the Tenable Patch Management dashboard. For descriptions of each menu item, see [Tenable Patch Management Menus](#).

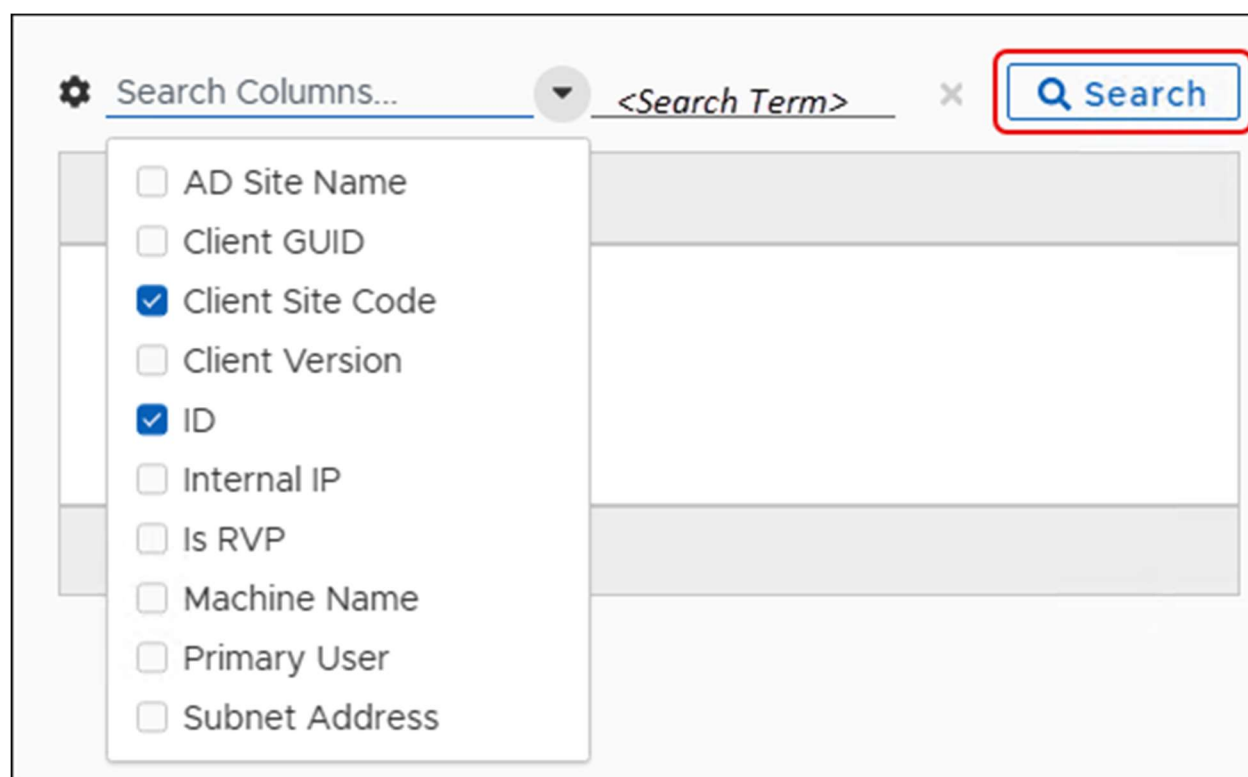
# Patching Analytics Dashboards

Patching Analytics has five separate dashboard views. Each view looks at patching information in the environment from a distinct perspective and shows summary information for related status.

All times in these graphs use the date information provided in the calendar settings (see [Date Range, Export, and Refresh](#)).

## Using Search in Tenable Patch Management

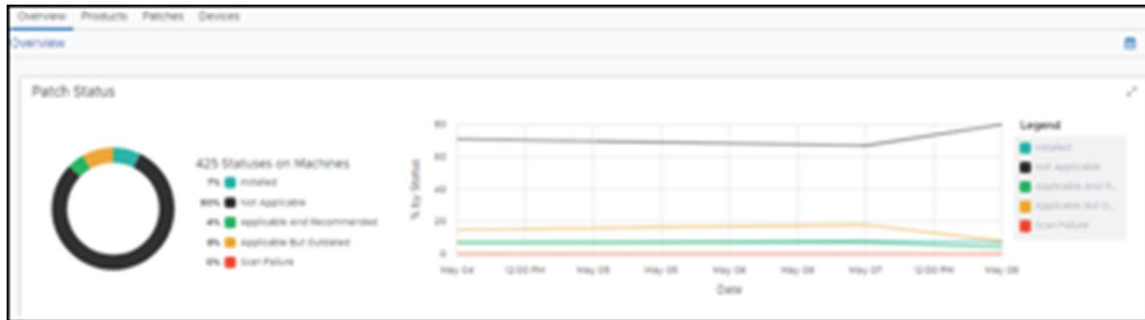
For tables in any dashboard view, the drop-down list next to **Search** allows you choose a column to search within. This provides several options for searching depending on the search term you have selected. Column choices change depending on the menu object.



## Patching Analytics Overview

The **Overview** summarizes the state of all patches in the environment. This view includes Patch Status and Product Status widgets.

**Patch Status** shows the total number of patches required in your environment and the installation/applicability of the aggregate total.



**Product Status** is a table that lists each product that Tenable Patch Management looks for during a scan, the installation/applicability status of each, and the status, compliance, and Risk Score for each.

The right arrow next to a product in the status table drops down a list of additional details for that product.

Product Status

Search Columns...

Product Name	Product Name	Publisher	Patc...	Mach...	Devic...	Comp...	Risk ...	Actions
1Password x64	1Password ...	Aglebits Inc.	18	0	0	100%	0	...

ID: 1000000270

Description: 1Password keeps track of password breaches and other security problems so you can keep your accounts safe. It checks for weak, compromised, or duplicated passwords and lets you know which sites are missing two-factor authentication or using unsecured HTTP.

Percentage Installed On: 0%

Strategies Including this Product: 0

Average Risk Score: 0

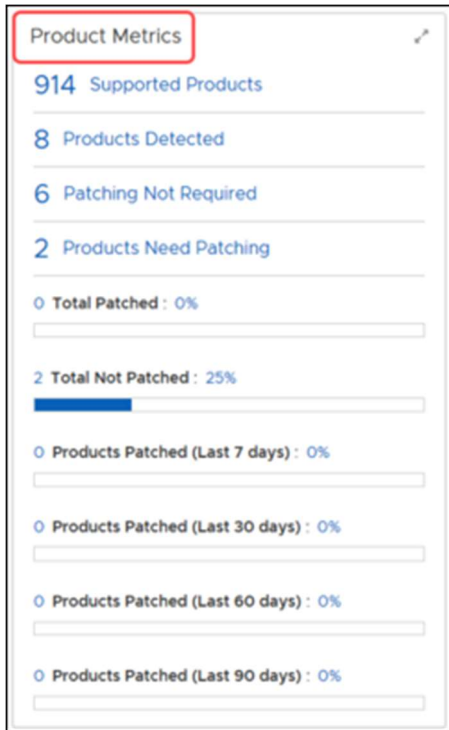
Risk Contribution: 0

Criticality: 50

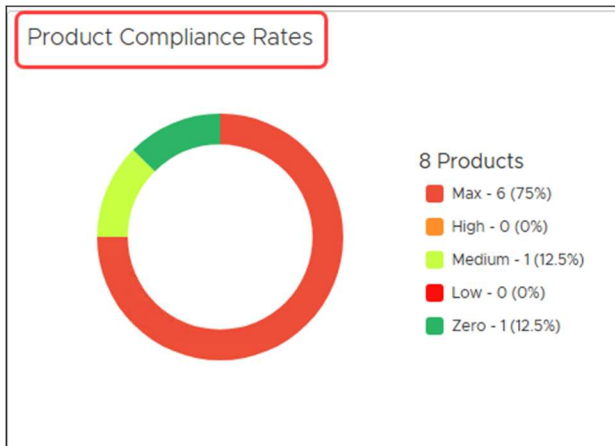
## Products View

The **Products** view summarizes information from the product perspective.

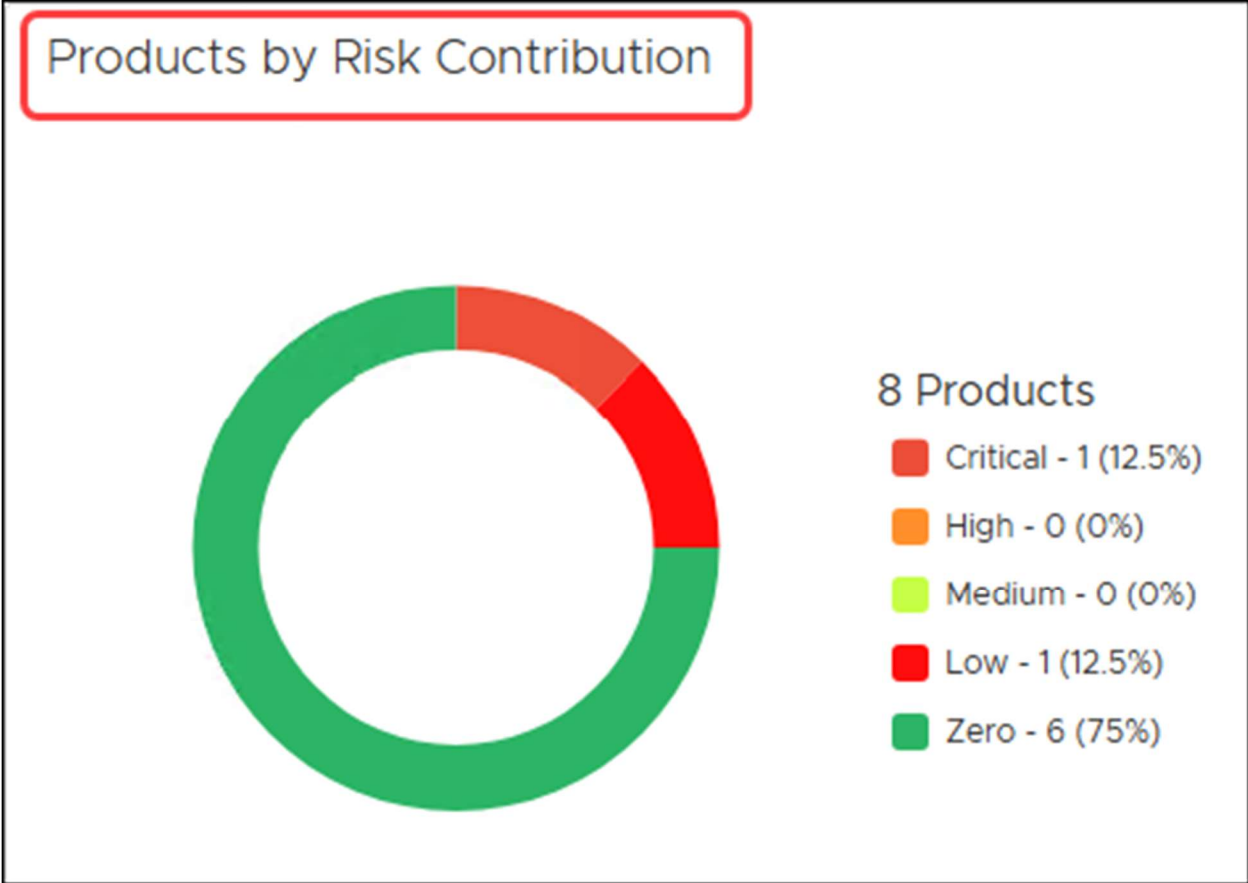
**Product Metrics** tracks supported products, detected products, and patching requirements, and provides a visual indication of product patching over time.



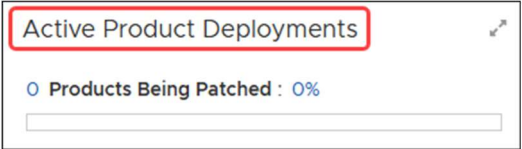
**Product Compliance Rates** show the number of products in the environment and the compliance rates by percentage. It also includes a chart that shows the level of compliance (Compliant, Compliant by Exclusions, and Non-Compliant) over time.



**Risk Contribution** shows the number of products in the environment and the risk rates (Critical, High, Medium, Low, Zero) by percentage. The chart tracks risk levels over time.



**Active Product Deployments** for products provides the number of products undergoing patch and the percentage of completion.



**Product Status** is a table that lists each product that looks for during a scan, the installation/applicability status of each, and the status, compliance, and Risk Score for each.

The right arrow next to a product in the status table drops down a list of additional details for that product.

Product Name	Publisher	Patc...	Mach...	Devic...	Comp...	Risk ...	Actions
IPassword x64	IPassword ...	Aglebits inc.	18	0	0	100%	0
<b>ID</b> 1000000270 <b>Description</b> IPassword keeps track of password breaches and other security problems so you can keep your accounts safe. It checks for weak, compromised, or duplicated passwords and lets you know which sites are missing two-factor authentication or using unsecured HTTP. <b>Percentage Installed On</b> <input type="text" value="0%"/> <b>Strategies Including this Product</b> 0 <b>Average Risk Score</b> 0 <b>Risk Contribution</b> 0 <b>Criticality</b> 50							

## Patches View

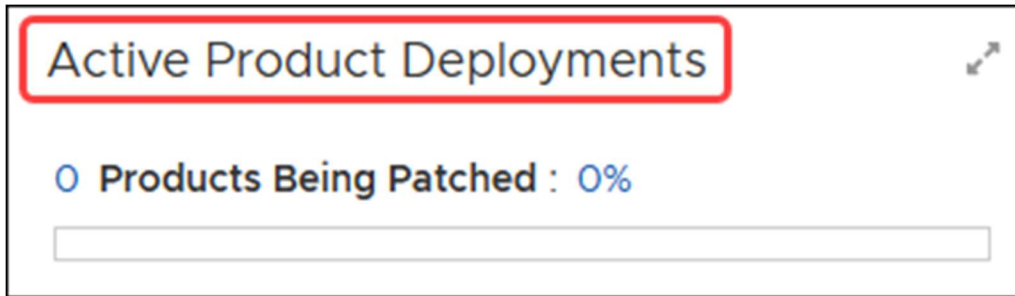
The **Patches** view summarizes information from the patch perspective.

**Patch Metrics** tracks total patches, patches consumed, installed, or not required, and provides a visual indication of patch installation over time.

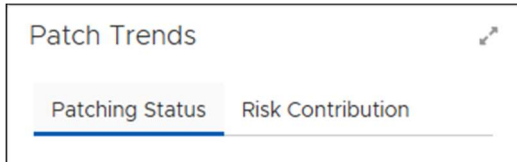
Patch Metrics	
19494	Total Patches
15134	Patches Consumed
17	Patches Installed
15128	Patches Not Required
0	Patches Installed (Last 7 days)
0	Patches Installed (Last 30 days)
0	Patches Installed (Last 60 days)
0	Patches Installed (Last 90 days)
0	Being Patched : 0%
6	Not Patched : 0%

**Active Product Deployments** provides the number of patches undergoing installation and the percentage of completion.

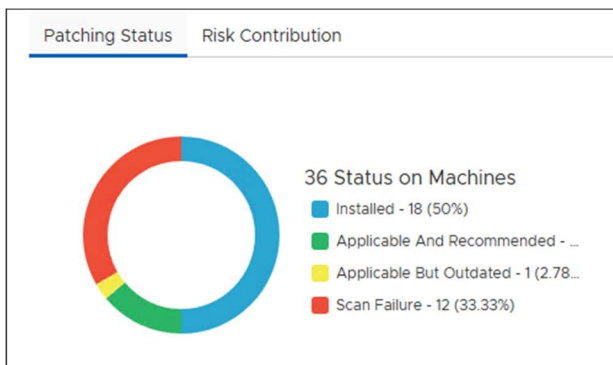




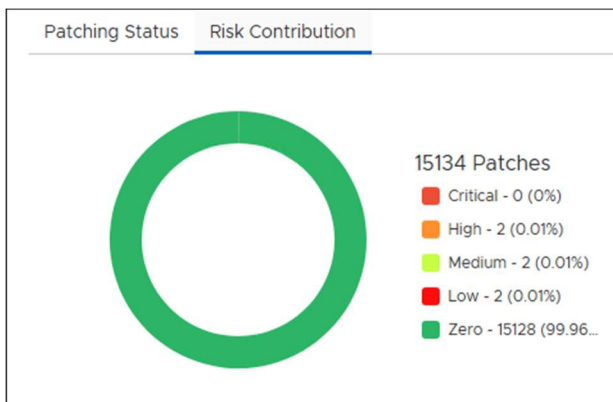
**Patch Trends** includes two tabs, one for Patching Status and one for Risk Contribution.



**Patching Status** shows the status of all patches, the number of machines tracked in the environment, and the number of patches in each status (Installed, Applicable and Recommended, Applicable but Outdated, Scan Failure) by percentage. The chart shows patching status over time.



**Risk Contribution** shows the number of patches in the environment and the risk rates (Critical, High, Medium, Low, Zero) by percentage. The chart tracks risk levels over time.



**Top 10 Most Critical Patches** tracks the risk contribution of the top ten most critical patches in the environment.

Patch Name	Risk Contribution	Actions
2023-11 Cumulative Updt	15%	...

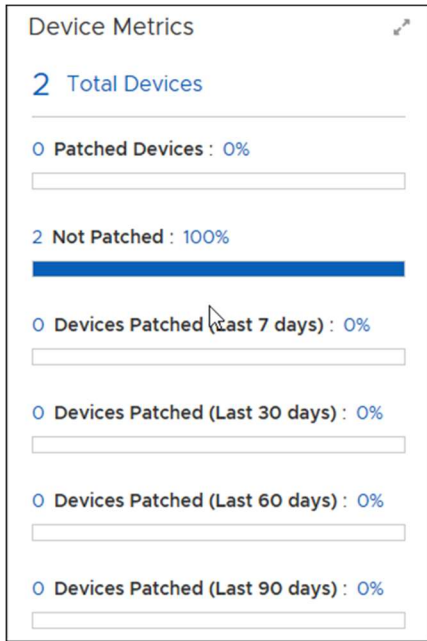
**Patch Status** is a table that lists each patch that Tenable Patch Management looks for during a scan, the installation/applicability status of each, and the status, compliance, and Risk Score for each.

The right arrow next to a product in the status table drops down a list of additional details for that product.

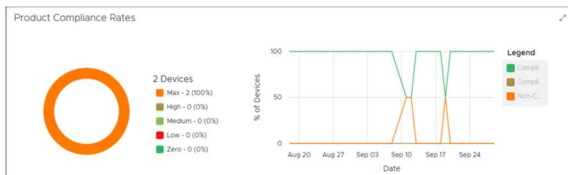
Patch Name	Details																						
.NET 3.5 Feature on Demand for X64	<table border="1"> <tr><td>ID</td><td>1021000947</td></tr> <tr><td>Description</td><td>--</td></tr> <tr><td>Patch Notes</td><td>--</td></tr> <tr><td>Reboot Type</td><td>N/A</td></tr> <tr><td>Product ID</td><td>1000990001</td></tr> <tr><td>Not Applicable</td><td>2</td></tr> <tr><td>Applicable Outdated</td><td>0</td></tr> <tr><td>Scan Failed</td><td>0</td></tr> <tr><td>Average Risk Score</td><td>0</td></tr> <tr><td>Risk Contribution</td><td></td></tr> <tr><td>Standalone Risk Score</td><td>16</td></tr> </table>	ID	1021000947	Description	--	Patch Notes	--	Reboot Type	N/A	Product ID	1000990001	Not Applicable	2	Applicable Outdated	0	Scan Failed	0	Average Risk Score	0	Risk Contribution		Standalone Risk Score	16
ID	1021000947																						
Description	--																						
Patch Notes	--																						
Reboot Type	N/A																						
Product ID	1000990001																						
Not Applicable	2																						
Applicable Outdated	0																						
Scan Failed	0																						
Average Risk Score	0																						
Risk Contribution																							
Standalone Risk Score	16																						

## Devices View

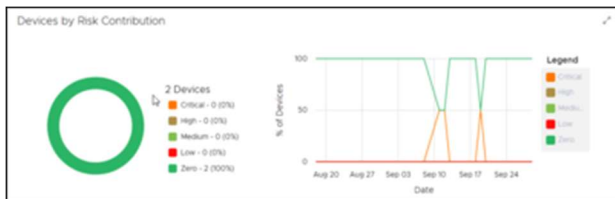
The **Device Metrics** widget shows the total number of devices in the environment, the percentage of patched and unpatched devices, and the percentage of devices patched in the last 7-, 30-, 60-, and 90-days.



The **Product Compliance Rates** for Devices shows the rate of compliance for each device in the environment based on the latest device scan information. The graph displays the percentage of devices that fall into each category of compliance (max, high, medium, low, and zero), and the line graph shows compliance trends over time.



The **Risk Contribution** widget for Devices shows the total number of devices and the percentage that fall into each risk category (critical, high, medium, low, zero). The chart shows risk contribution trends over time.



**Active Product Deployments** for devices provides the number of devices undergoing patch and the percentage of completion.



The **Device Status** table lists the device name of every device in the environment and shows a customizable view of the various details related to each device.

# Flex Controls

Flex Control settings include the functions listed in the table below. These options provide added flexibility when managing your patching environment.

<b>Blocklisting</b>	Provides an extra level of protection for customer devices and patching processes. Prevents the download and installation of potentially damaging content to customer devices. See <a href="#">Blocklisting</a> .
<b>Cycle Operations</b>	Includes access to Patching, Deployment, and Rollout Cycle details. Details include a graphical representation of any cycles in progress and a table that lists details for each cycle in progress. Also includes a graphical representation of previously completed cycles and a table that lists a each completed cycle. Select each completed cycle to review details. See <a href="#">Cycle Operations</a> .
<b>Exceptions</b>	Allows administrators to exclude Business Units from specific updates on certain products or to use settings to maintain all endpoints at a specific version of a product. See <a href="#">Patching Exceptions</a> .
<b>Global Pause</b>	Use Global Pause to pause or resume all patching activities for specified software products and patches. Affects all clients contained in one or more specified Business Units. See <a href="#">Global Pause</a> .
<b>Rollbacks</b>	Create a Rollback object to rollback one or more patches to a system determined or specified version. See <a href="#">Rollbacks</a> .

## Blocklisting

includes an extra level of protection for customer devices and patching processes called Blocklisting. The Tenable metadata team reviews all metadata that vendors provide for their new products and patches to verify relevance and integrity.

When a vendor releases products and patches, the team reviews the content and determines whether the patch has any issues that might cause unexpected behavior. The team blocklists patches and products that have issues and automatically creates an exclusion for the patch on all clients. Blocklisting prevents the download and installation of potentially damaging content to customer devices.

## Blocklist Settings

The Blocklist Settings workspace provides configuration options for Notifications and Communication Providers. The Notification Chains and Communication Providers configured from this workspace identify the process and delivery of communications related to blocklisted patches. See [Managing Blocklist Notification Settings](#).

## Managing Blocklist Notification Settings

Set categories of notification by selecting a Notification Chain to use when Tenable blocklists a patch/release. Select the same or different Notification Chain to notify administrators when you blocklist a patch or a release. You can also select specific communication providers for either category of notification.

### View Blocklist Settings

Blocklist Settings include notification details for blocklisted patches including Notification Chains and Communication Providers. You can use the provided details (Tenable Curated) or create your own (Customer). Update these settings as needed for your notification preferences.

1. Mouse over or click **Flex Controls** on the Home menu, and then select **Blocklisting > Blocklisted Patches**.
2. Select **Settings** to view the Blocklist Settings workspace.

### Select a Notification Chain for Blocklisted Patches

1. Navigate to [Blocklist Settings](#).
2. Select **Browse** next to either **Tenable Curated Chain** or the **Customer Chain** to list the available Notification Chains. If you need to create a new Notification Chain for these purposes, see [Create a Notification Chain](#).
3. Select the **Name** of the Notification Chain you want to use for whichever field you are editing – the **Tenable Curated Chain** or the **Customer Chain**.
4. Select **Add Notification Chain** on the bottom left of the dialog.

### Choose Communication Providers for Notification Chains

1. Navigate to [Blocklist Settings](#).
2. Select **+ Add Communication Providers** for either **Tenable Curated Communication Providers** or **Customer Communication Providers** from the **Blocklist Settings**.
3. Select one or more **Names** from the **Communications Provider** table, and then click **Add Communication Providers** at the bottom left of the dialog.

If you need to add providers to the table, see [Create a New Communication Provider](#).

## Blocklisted Patches

Blocklisted Patches provides a Tenable table and a Customer table. Tenable populates the Tenable table with all patches that Tenable has blocklisted. The Customer table becomes populated when customers add their own blocklisted patches. See [Managing Blocklisted Patches](#).

## Managing Blocklisted Patches

When a vendor issues a deficient or erroneous patch, Tenable blocklists the metadata and notifies customers automatically about the blocklisted patch. Blocklisting prevents inclusion of the patches in Patching Strategies and automatically creates an exclusion for the patch on all clients.

If Tenable determines that the vendor has fixed a blocklisted item, the metadata team can revoke the blocklisting. When the updated metadata arrives at the customer device, OneSite automatically removes the patch from the Blocklist, making it available for deployment.

You may not remove a patch from the Tenable blocklist. Although strongly discouraged by Tenable, you can ignore the Tenable recommendations, suppress the blocklisted status, and move forward with inclusion of the patch in your environment.

Customers may also create their own Blocklist for products they do not want deployed in their environment. Customers are responsible for managing their own blocklisted patches.

### View Blocklisted Patches

1. Mouse over or click **Flex Controls** on the Home menu, and then select **Blocklisting > Blocklisted Patches**.
2. Select **Blocklisted Patches**, and then select **Patches**.
3. Expand the **Blocklisted Patches** folder, and then select either the **Tenable** folder or the **Customer** folder to view blocklisted patches. This example uses the Tenable folder.

This displays the list of Tenable Blocklisted Patches.

4. Select the **Customer** folder to view patches blocklisted by the customer.

### Remove a Tenable Blocklisted Patch

When you enable **Removed from Blocklist** in a Tenable Blocklisted Patch template, you are expressly allowing clients in your environment to install a patch that Tenable has found deficient or erroneous.

#### Caution

Tenable does not recommend removing blocklisted patches.

1. Navigate to the table of Tenable Blocklisted Patches ([View Blocklisted Patches](#)), and then click the **Name** of the blocklisted patch you want to suppress. This opens to General Settings in the template.
2. Select the **Removed from Blocklist** toggle to enable removal of this patch from the blocklist. Defaults to disabled.

#### Caution

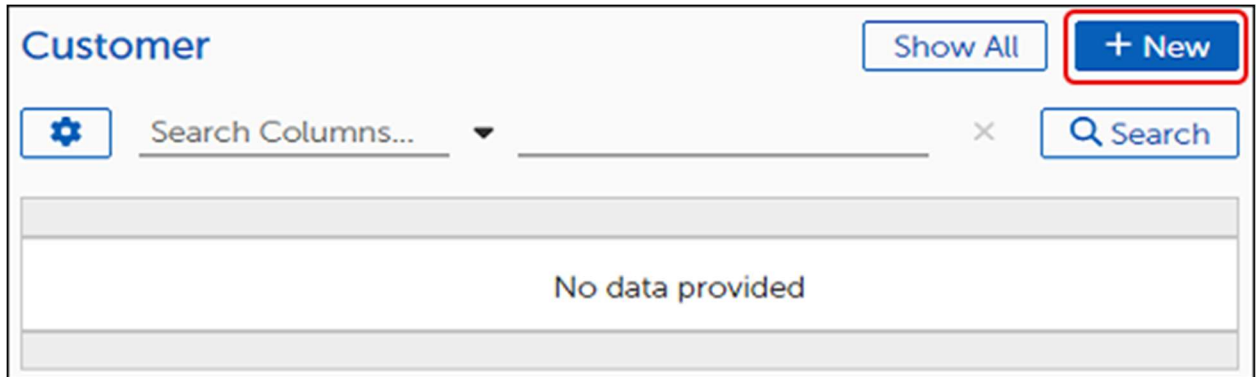
Enabling customer suppression means you expressly choose to ignore this blocklist recommendation from the Tenable metadata team.

3. Select **Save**, and then click **<-- Back** at the upper left to return to the list of blocklisted patches.

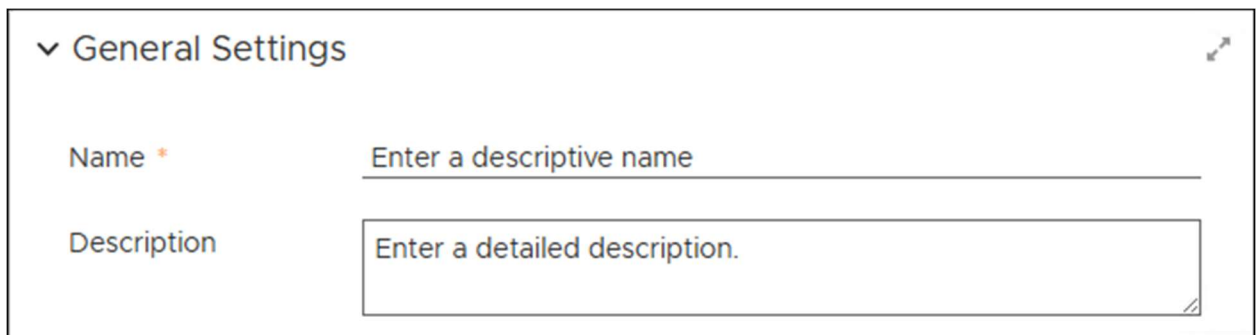
## Add a Patch to Customer Blocklisted Patches

A Customer Blocklist is a customer created list of patch exceptions that applies globally to all customer devices. The red asterisk next to the field name indicates a required field.

1. Navigate to the table of blocklisted patches ([View Blocklisted Patches](#)).
2. Select the **Customer** folder to view the table of patches blocklisted by the customer. Until you add patches, this table is blank.
3. Select **+ New** to add a patch to the blocklist table.



4. Enter a **Name** and **Description** for the patch you intend to blocklist.

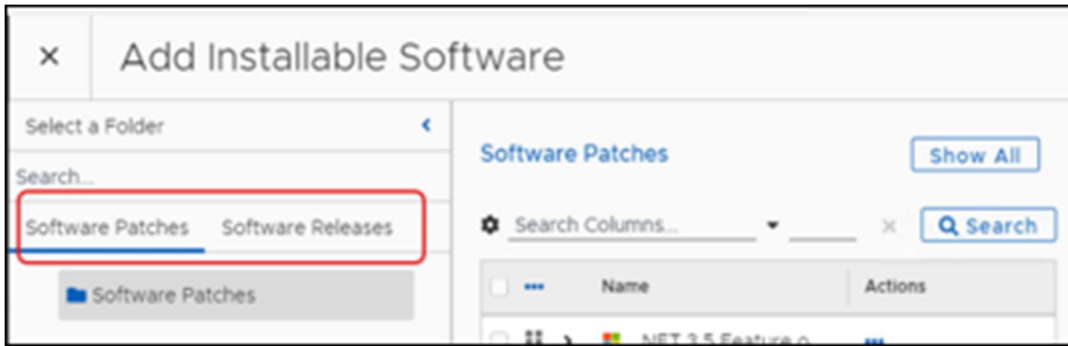
A screenshot of a form titled "General Settings" with a dropdown arrow on the left and a refresh icon on the right. The form contains two input fields. The first is labeled "Name" with a red asterisk indicating it is required, and has a text input field with the placeholder text "Enter a descriptive name". The second is labeled "Description" and has a larger text area with the placeholder text "Enter a detailed description.".

### Configure Blocklist Settings

1. Select **Browse** next to add Installable Software in the Blocklist Settings of an open Blocklisting template ([Add a Patch to Customer Blocklisted Patches](#)).

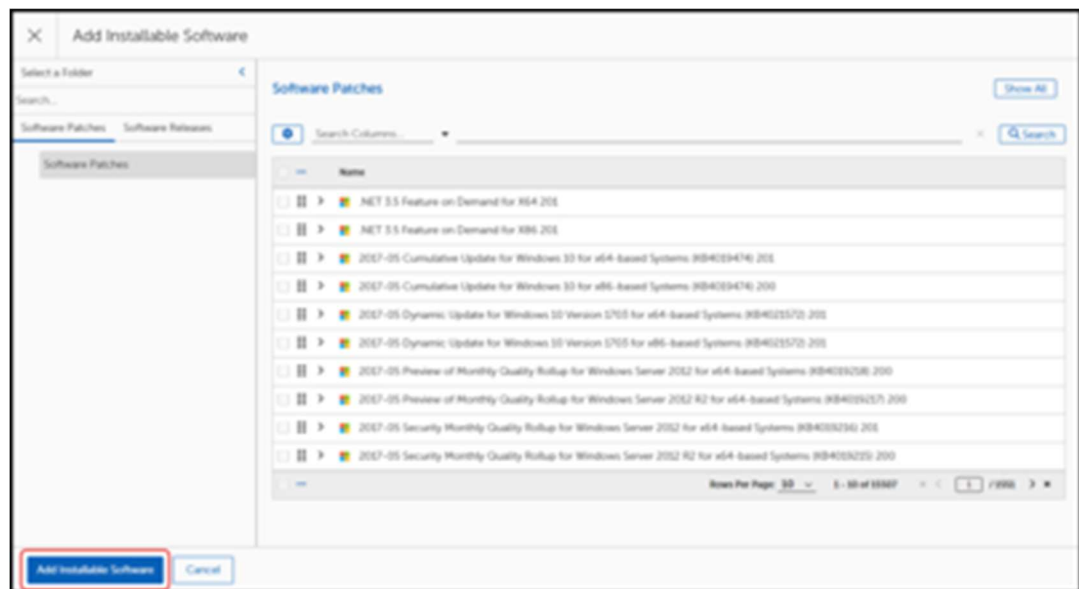
This opens the **Add Installable Software** dialog with a list of all available software or patches.





2.

- a. Select one of the following tabs from the left-side column of the **Add Installable Software** dialog box:
  - Select the Software Patches tab to choose a patch release.
  - Select the Software Releases tab to choose a product release.
- b. Choose one of the methods below to search for a patch or release:



- Use the navigation tools on the bottom right to scroll through the pages to find and select a Software product or release.
  - Enter a product name on the search line, and then click **Search** to find and select a specific product.
3. Select the **Name** of the patch to blocklist, and then click **Add Installable Software** at the bottom left of the dialog.
  4. Enter the following information:
    - a. Name of the person blocklisting this patch

- b. Email of the person blocklisting this patch.
- c. Describe the reason for the blocklisting of this patch.
- d. Enter the vendor URL, if known (optional).

Although you can see the **Tenable Curated** patch toggle on the page, you cannot change this setting because you are creating a customer curated patch.

5. Select **Save** on the upper left:
  - a. Check the **Error View** and resolve any errors.
  - b. Select **Save** again if you make any changes.

## Cycle Operations

Includes access to Patching, Deployment, and Rollout Cycle details. Details include a graphical representation of any cycles in progress and a table that lists details for each cycle in progress. Also includes a graphical representation of previously completed cycles and a table that lists a each completed cycle. Select each completed cycle to review details.

Details available for each cycle type include the following:

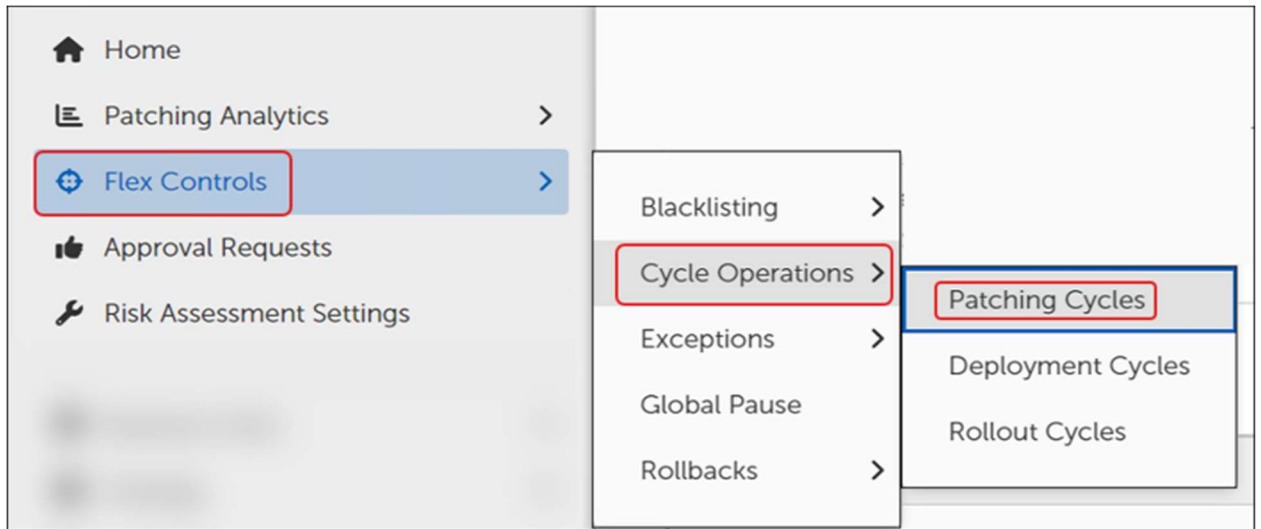
- **Cycle Information:** Provides general information about the Patch Process such as the Current State, the creation date and time, and the Patch Process schedule. This section also contains controls to manually start, stop, or delay a Patch Process.
- **Overall Metrics:** This section contains information about the scope of the running process. This screen shows the number of business units and devices affected by this Patch Process, along with Urgency information.
- **Cycle History:** This section gives a historical perspective of the results of past runs. This view will show the number of devices that previously were successful, failed, aborted, timed out, or errored.
- **Patch Approvals:** One of the key functions of a Patch Process is to execute Approval Chains as defined in the Patching Strategy or Business Unit. This section displays pending Approvals. You cannot grant approvals from this view.
- **Cycle Logs:** Display events relating to the Patch Process. For instance, the Cycle Operation Logs can show the administrator who manually started a Patch Cycle and at what time.

## Patching Cycles

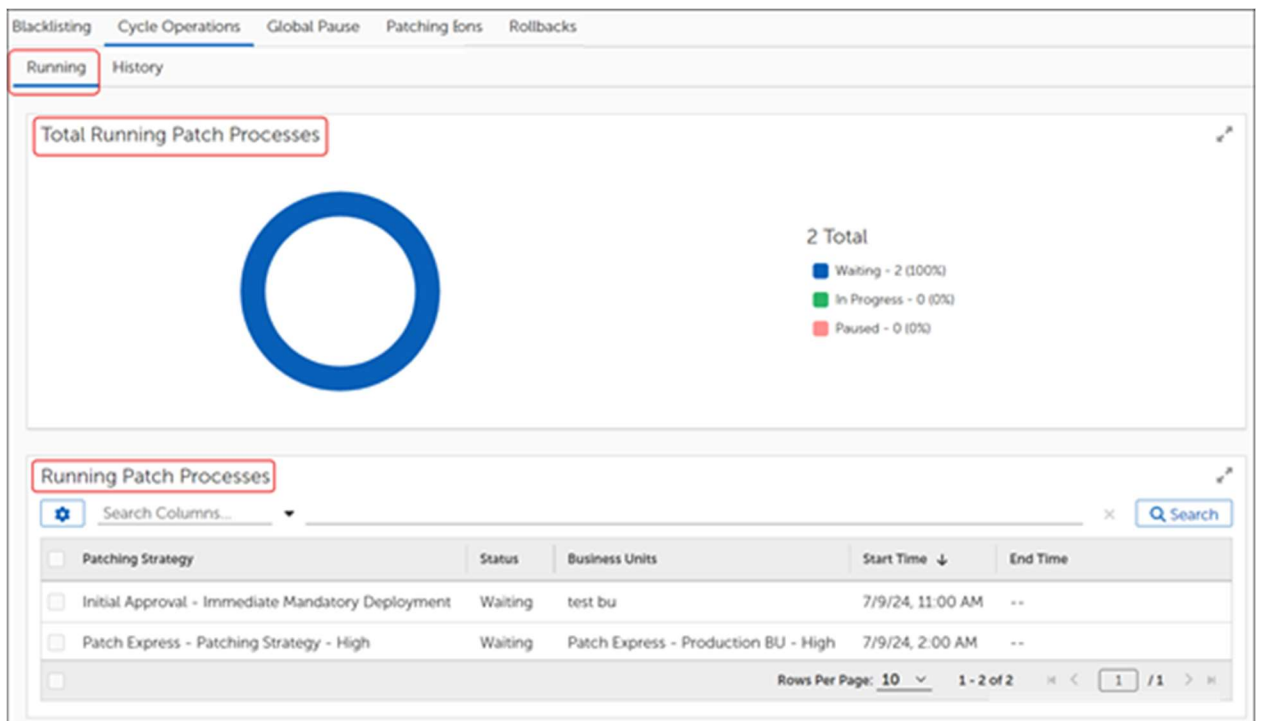
This dashboard shows information about the active Patch Processes in the environment. Patch Processes represent the workflow that models and performs the defined patching routine. As part of the overall Patching Strategy, Patch Deployment Bots use configured criteria to identify patches that apply to endpoints. Once approved, the Bot submits those patches to the Patch Process, which creates a Patch Cycle. The Patch Cycle executes at either a scheduled time or you can start it manually.

View the Running Patch Cycles

1. Mouse over or click **Flex Controls** on the **Home** menu, and then select **Cycle Operations > Patching Cycles**.



This opens to the **Running** tab of the Patching Cycles workspace:



- a. The **Total Running Patch Processes** widget shows an aggregate summary of all patch processes and their corresponding states (Waiting, In Progress, or Paused).
- b. The **Running Patch Processes** table lists the running Patching Strategies by name.

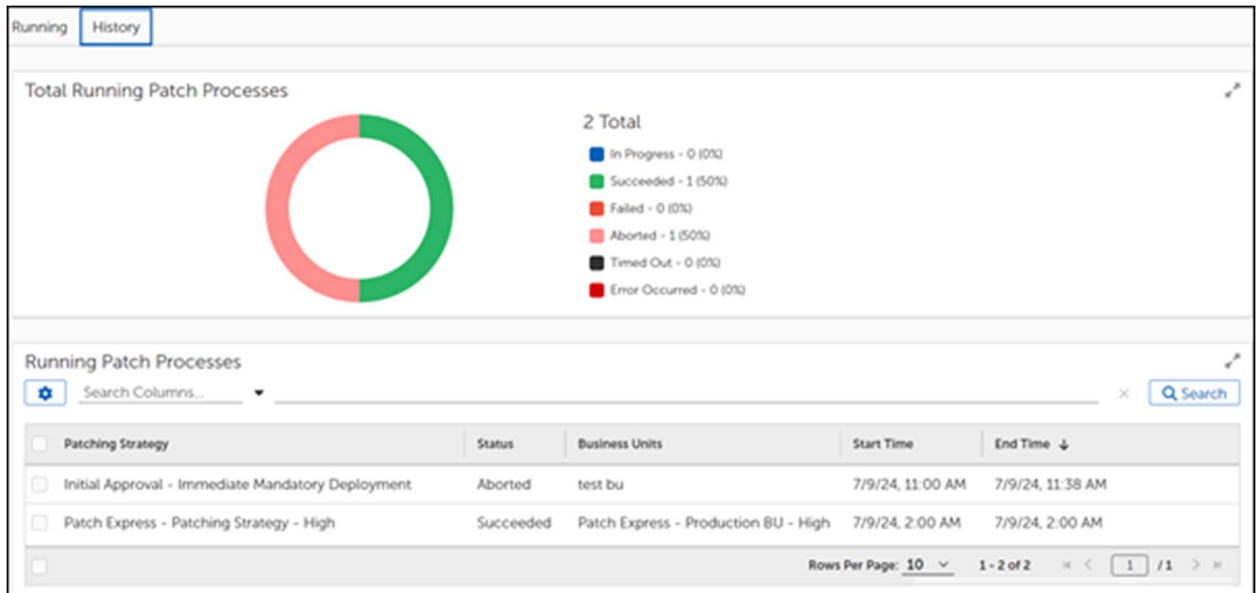
2. Enter a **Patching Strategy** name on the search bar above the **Running Patch Processes** table, and then click **Search**.

Patching Strategy	Status	Business Units	Start Time	End Time
Initial Approval - Immediate Mandatory Deployment	Waiting	test bu	7/9/24, 11:00 AM	--
Patch Express - Patching Strategy - High	Waiting	Patch Express - Production BU - High	7/9/24, 2:00 AM	--

3. Select the **Patching Strategy** name in the **Running Patch Processes** table to see specific details about that process.

### View Patching Cycle History

1. Mouse over or click **Flex Controls** in the **Home** menu, and then select **Cycle Operations > Patching Cycles**.



2. Select **History** on the upper left to change to the **History** tab:
  - a. The **Total Finished Patch Processes** widget on top shows an aggregate summary of all completed patch processes and their corresponding states (In Progress, Succeeded, Failed, Aborted, Timed Out, Error Occurred).
  - b. The **Running Patch Processes** table lists the completed patch processes by Patching Strategy name.
3. Enter a **Patching Strategy** name on the search bar above the **Running Patch Processes** table, and then click **Search**.

Patching Strategy	Status	Business Units	Start Time	End Time
Initial Approval - Immediate Mandatory Deployment	Aborted	test bu	7/9/24, 11:00 AM	7/9/24, 11:38 AM
Patch Express - Patching Strategy - High	Succeeded	Patch Express - Production BU - High	7/9/24, 2:00 AM	7/9/24, 2:00 AM

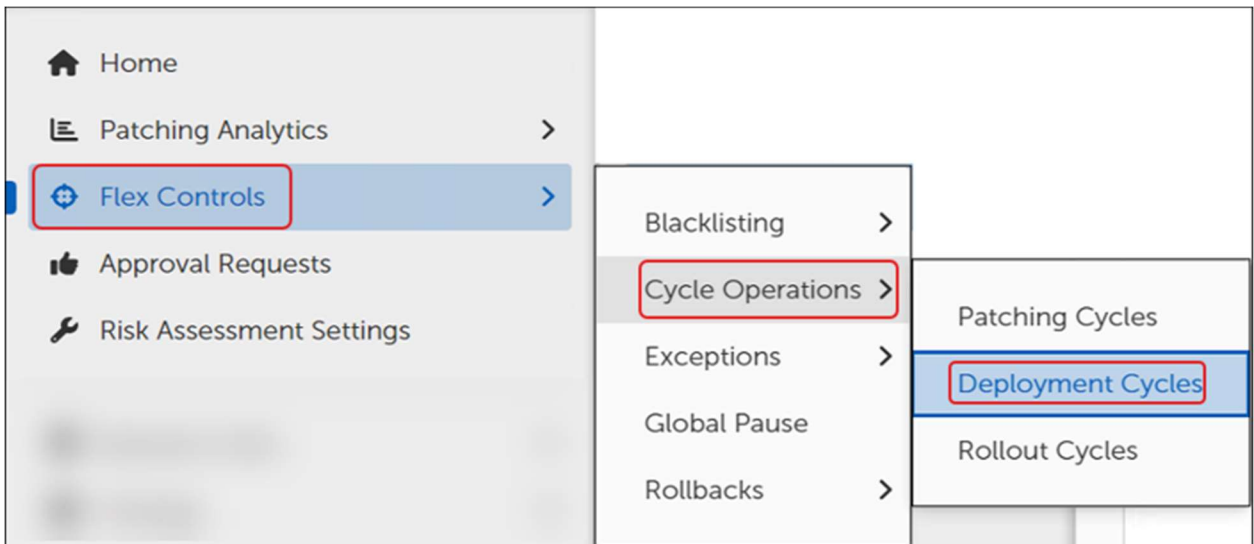
4. Select the **Patching Strategy** name in the **Running Patch Processes** table to see specific details about that process.

## Deployment Cycles

This dashboard shows information about currently running Patch Deployment Channel Processes and the history of completed patch processes. These details show the status of all active Deployment Processes.

View the *Running Deployment Cycles*

1. Mouse over or click **Flex Controls** in the **Home** menu, and then select **Cycle Operations > Deployment Cycles**.



This opens to the **Running** tab of the Deployment Cycles workspace:

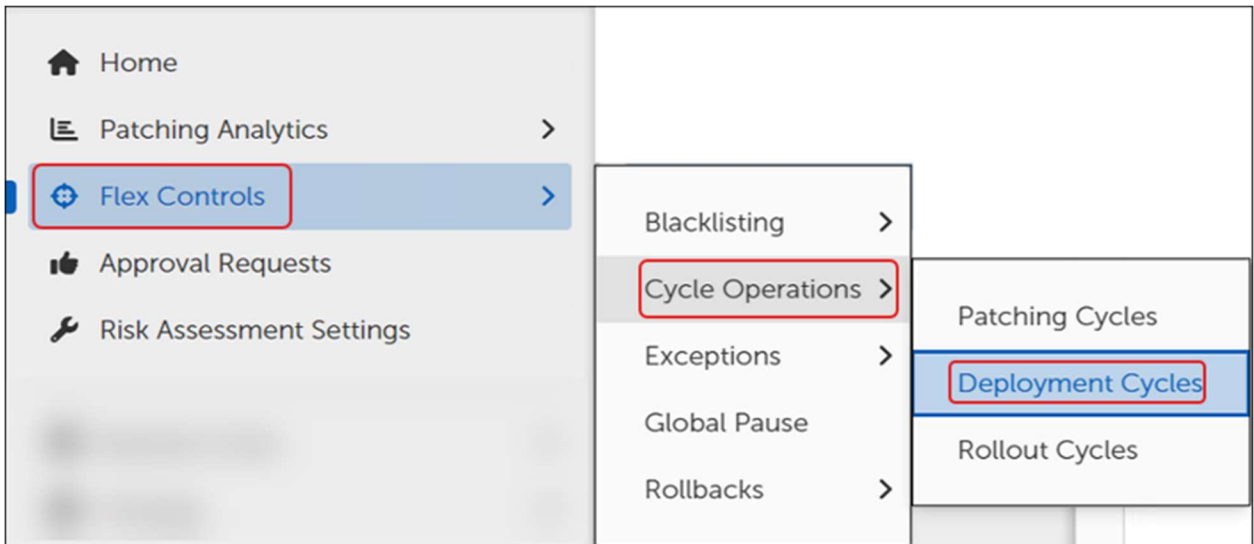
- a. The **Total Running Deployments** widget shows an aggregate summary of all patch processes and their corresponding states (Waiting, In Progress, or Paused).
  - b. The **Running Deployments** widget table lists the running Deployment Strategies by name.
2. Enter a **Deployment Strategy** name on the search bar above the **Running Patch Processes** table, and then click **Search**.

Patching Strategy	Status	Business Units	Start Time ↓	End Time
Initial Approval - Immediate Mandatory Deployment	Waiting	test bu	7/9/24, 11:00 AM	--
Patch Express - Patching Strategy - High	Waiting	Patch Express - Production BU - High	7/9/24, 2:00 AM	--

3. Select the **Deployment Strategy** name in the **Running Patch Processes** table to see specific details about that process.

#### View Deployment Cycle History

1. Mouse over or click **Flex Controls** in the **Home** menu, and then select **Cycle Operations > Deployment Cycles**.



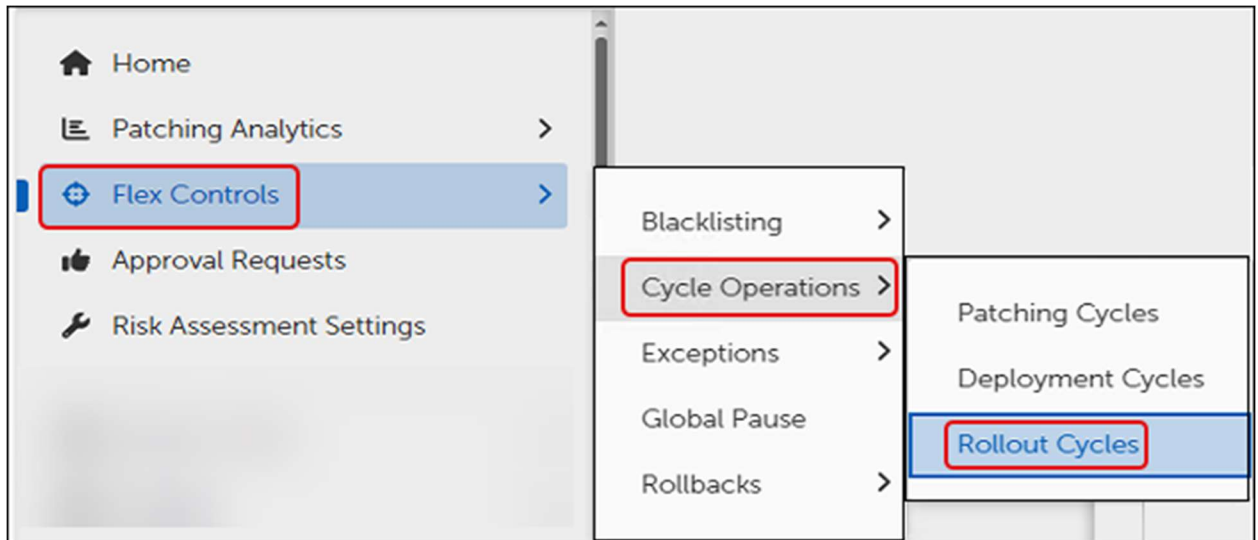
2. Select **History** on the upper left to change to the **History** tab:
  - a. The **Total Running Deployments** widget shows an aggregate summary of all deployment processes and their corresponding states (Waiting, In Progress, or Paused).
  - b. The **Running Deployments** widget table lists the completed Deployment Strategies by name.
3. Enter a **Deployment Strategy** name on the search bar above the **Running Patch Processes** table, and then click **Search**.
4. Select the **Deployment Cycle** name in the **Finished Deployments** table to see specific details about that process.

# Rollout Cycles

Rollout Processes represent the installation of Patches per Business Unit. Each Business Unit involved in the Patch Deployment includes a Rollout Cycle.

## View the Running Rollout Cycles

1. Mouse over or click **Flex Controls** on the **Home** menu, and then select **Cycle Operations > Rollout Cycles**.



This opens to the **Running** tab of the Rollout Cycles workspace:

- a. The **Total Running Rollout Cycles** widget on top shows an aggregate summary of all running Rollout processes and their corresponding states (Waiting, In Progress, Paused).
  - b. The **Running Rollout Cycles** table lists the completed patch processes by Rollout name.
2. Enter a **Rollout Cycle** name on the search bar above the **Running Rollout Processes** table, and then click **Search**.
  3. Select the **Rollout Cycle** name in the **Running Rollout Processes** table to see specific details about that process.

## View Rollout Cycle History

1. Mouse over or click **Flex Controls** on the **Home** menu, and then select **Cycle Operations > Rollout Cycles**.
2. Select **History** on the upper left to change to the **History** tab:
  - a. The **Total Running Deployments** widget shows an aggregate summary of all deployment processes and their corresponding states (Waiting, In Progress, or Paused).

- b. The **Running Deployments** widget table lists the completed Deployment Strategies by name.
3. Enter a **Rollout Cycle** name on the search bar above the **Running Rollout Cycles** table, and then click **Search**.
4. Select the **Rollout Cycle** name in the **Finished Cycles** table to see specific details about that process.

## Patching Exceptions

When Business Units require exemption from specific updates on certain products, or the entire enterprise requires maintenance of a specific version of a product, Patching Exceptions provide a mechanism for creating and implementing these rules.

## Using Patching Exceptions

Tenable Patch Management includes two options: **Desired State Override** and **Last Allowed Version**. In the Patching Exceptions template, you choose the strategy you need, configure the product patches or version, and add Business Units. Configure each option separately to use multiple overrides in one template, and last version in another template.

### Desired State Override Options

- **Mandatory Install:** Allows endpoints to treat the Patch as mandatory.
- **Do Not Install:** Allows endpoints to skip installation of a particular Patch.
- **Rollback:** Forces a specific patch version even if Tenable Patch Management detects higher versions on endpoints.
- **Uninstall:** Removes the Patch/Product from endpoints in the specified Business Unit.

### Last Allowed Version

Specifies a patch level to consider current and ignores all more recent patches or versions. When specified, the Last Allowed Version sets the state for all patches or releases that are a later version than the one specified to do not install.

## Create a Patching Exception

1. Select **Flex Controls** from the Home menu, and then select **Exceptions > Patches**.
2. Select **+ New** on the upper-right corner to open a Patching Exception template.
3. Name and describe the exception:
  - a. Enter a descriptive Name for this exception in the **Name** field.
  - b. Enter a detailed **Description** of the purpose for this exception.
4. Select **Save** on the upper left to save your new template:



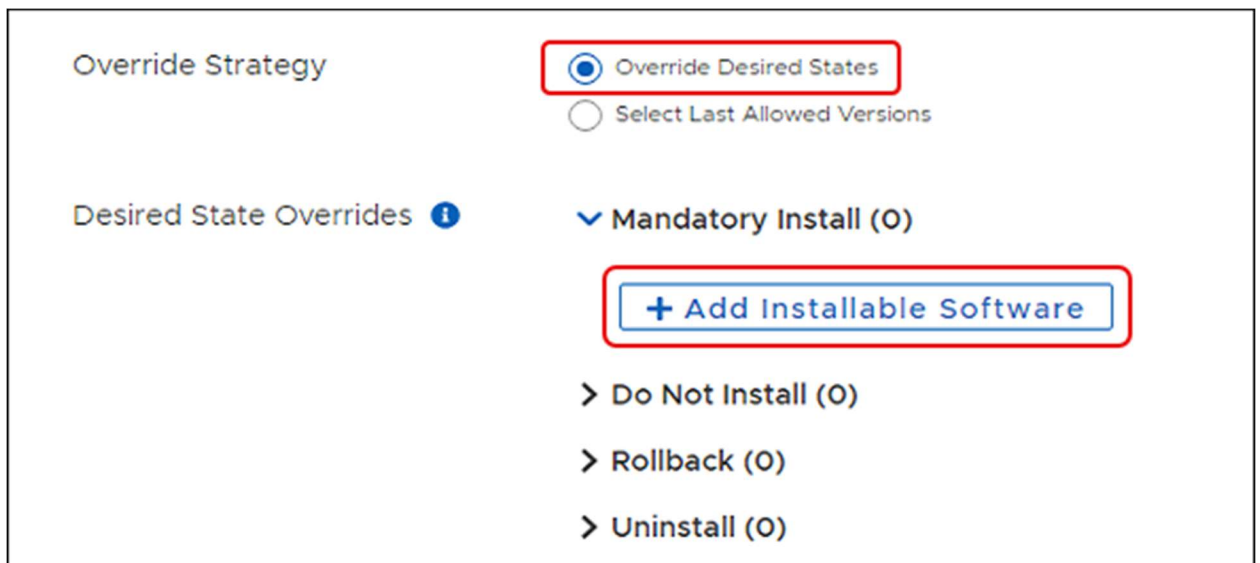
- a. Check the **Error View** and resolve any errors.
  - b. Select **Save** again if you make any changes.
5. Choose an Override Strategy:
- a. If you choose **Override Desired States**, see [Set Override Details for Patch Exception](#).
  - b. If you choose **Select Last Allowed Versions**, see [Set Last Allowed Patch Versions](#).

## Set Override Details for Patch Exception

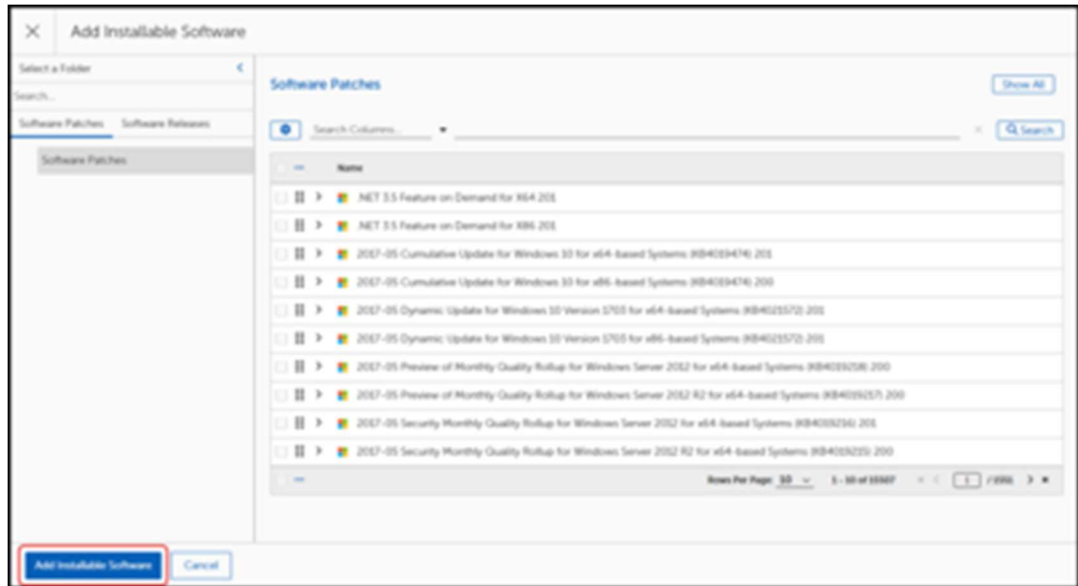
### Important

Choose only one software version per override exception.

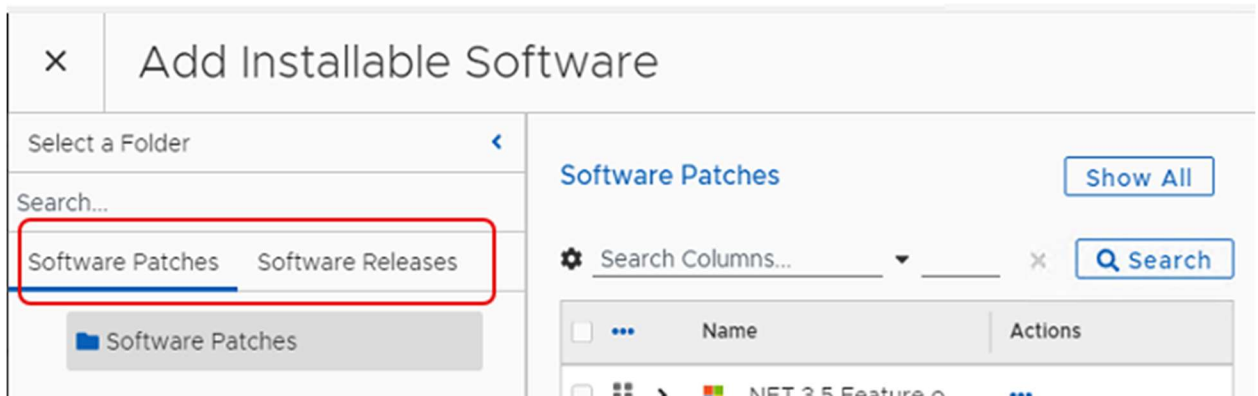
1. Select **Override Desired States** (default) as your **Override Strategy** in an open workspace or dialog.



2. Select the type of **Desired State Override**, such as Mandatory Install, and then click **+Add Installable Software** for that state.
3.
  - a. Select one of the following tabs from the left-side column of the **Add Installable Software** dialog box:
    - Select the Software Patches tab to choose a patch release.
    - Select the Software Releases tab to choose a product release.
  - b. Choose one of the methods below to search for a patch or release:



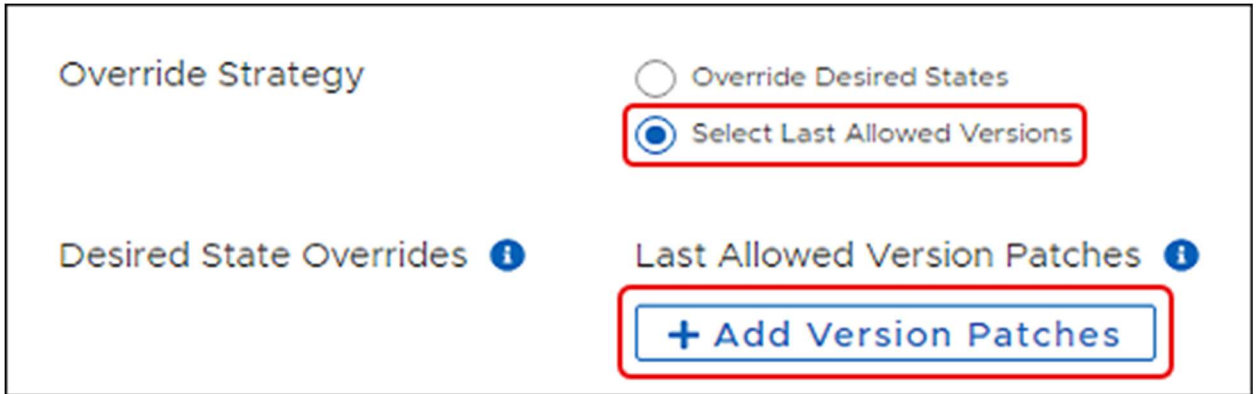
- Use the navigation tools on the bottom right to scroll through the pages to find and select a Software product or release.
  - Enter a product name on the search line, and then click **Search** to find and select a specific product.
4. Select the tab for either **Software Patches** (default) or **Software Releases** to run your search. You may add selections from both tabs to a single override state as long as they are for the same version of software.



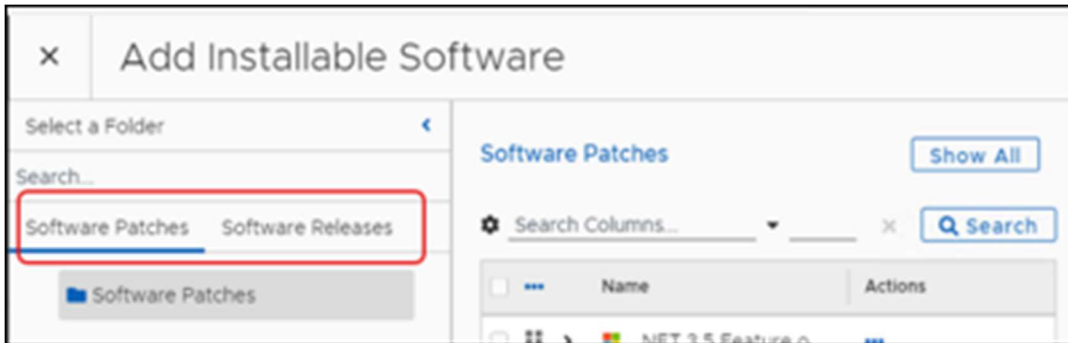
5. Select **Save** on the upper-left corner of the dialog to save your changes:
- Check the **Error View** and resolve any errors.
  - Select **Save** again if you make any changes.
6. Continue to **Add Target Business Units**.

## Set Last Allowed Patch Versions

1. Choose **Select Last Allowed Versions** as your **Override Strategy** in an open [Patching Exception](#) template. Defaults to disabled.



2. Select **+Add Version Patches** to open the **Add Version Patches** dialog.



3. Select the **Search** field, and then enter the release name of the product you want to override:
  - a. Select **Search**.
  - b. Select one or more products for the patch exception. You may add items from both **Software Patches** and **Software Releases** tab.
  - c. Select **Add Version Patches**.
4. Select **Save** on the upper-left corner of the dialog to save your changes:
  - a. Check the **Error View** and resolve any errors.
  - b. Select **Save** again if you make any changes.
5. Continue to **Target Business Units**.

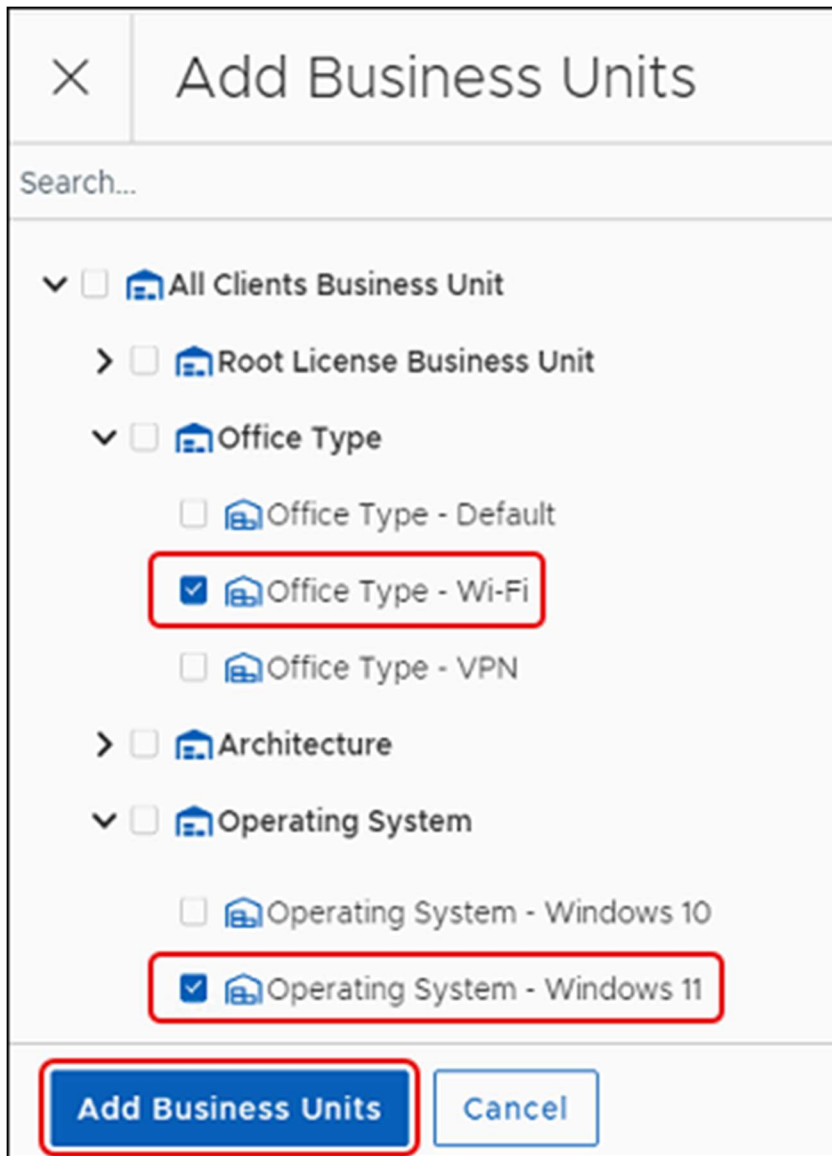
## Add Target Business Units for Patch Exceptions

Use this procedure to select one or more Business Units to which the exception applies. With no Business Units specified, the Patching Exception applies to all endpoints where the specified Patches apply.

1. Select **+ Add Business Units** in an open [Patching Exception](#) template.



2. Select one or more **Business Units** to add to the exception.



3. Select **Add Business Units** at the lower-left corner of the dialog.
4. Select **Save** at the upper left to save your progress:
  - a. Check the **Error View** and resolve any errors.
  - b. Select **Save** again if you make any changes.

## Global Pause

Global Pause settings take effect immediately on the clients you identify either globally or within the selected Business Units. Patch cycles continue to run as configured on the Tenable Server side, and the Tenable Client pauses the deployment of patches identified in the pause settings.

The Global Pause menu item provides access to both a Pause All Patching button and access to configuration details for pausing patch activity for specific products, patches, cycles, or Business Units.

When activated, Pause All Patching immediately stops all patch deployments across all licensed clients. When deactivated (Resume Patching) Tenable Patch Management revokes the Global Pause request and restores normal patching activity to all licensed clients.

In addition, you may create pause configurations for each of the following:

**Paused Products:** Pause patch deployments for specified products either globally or for specific Business Units.

**Paused Patches:** Pause patch deployments for specified patches either globally or for specific Business Units.

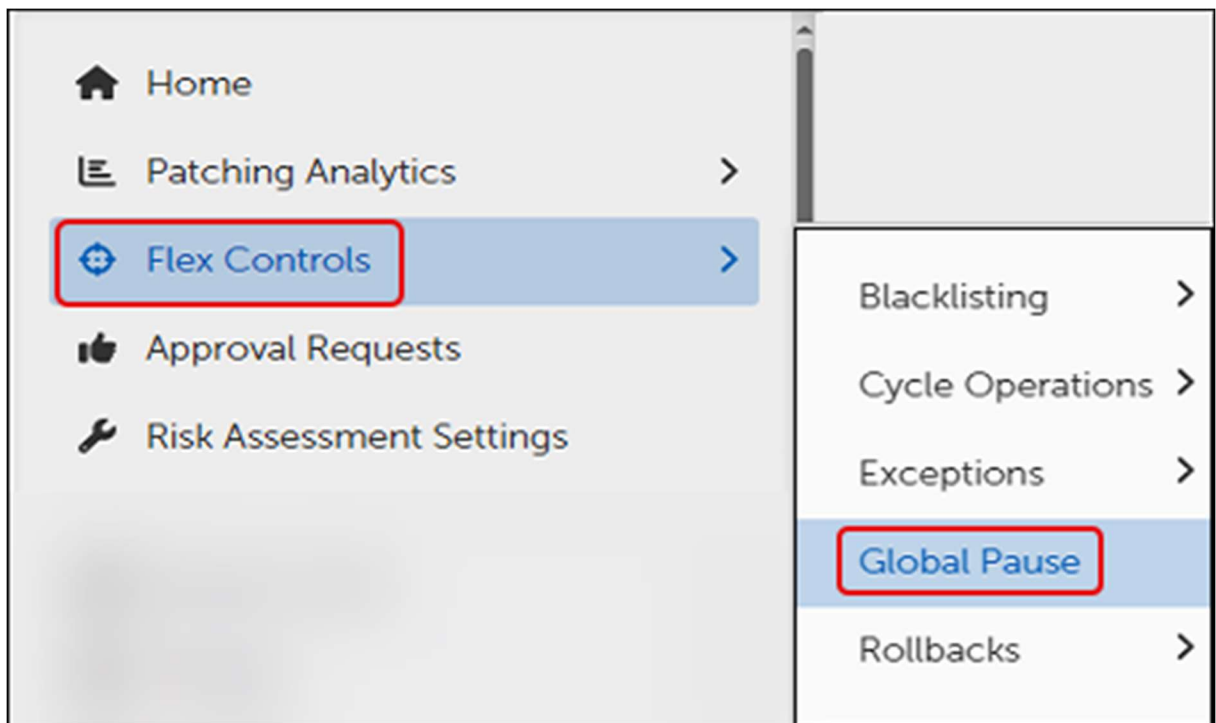
**Paused Cycles:** Pause Patching, Deployment, or Rollout Cycles either for specified Business Units or for the Business Units already targeted by the Cycle.

**Paused Business Units:** Pause all patches for specified Business Units.

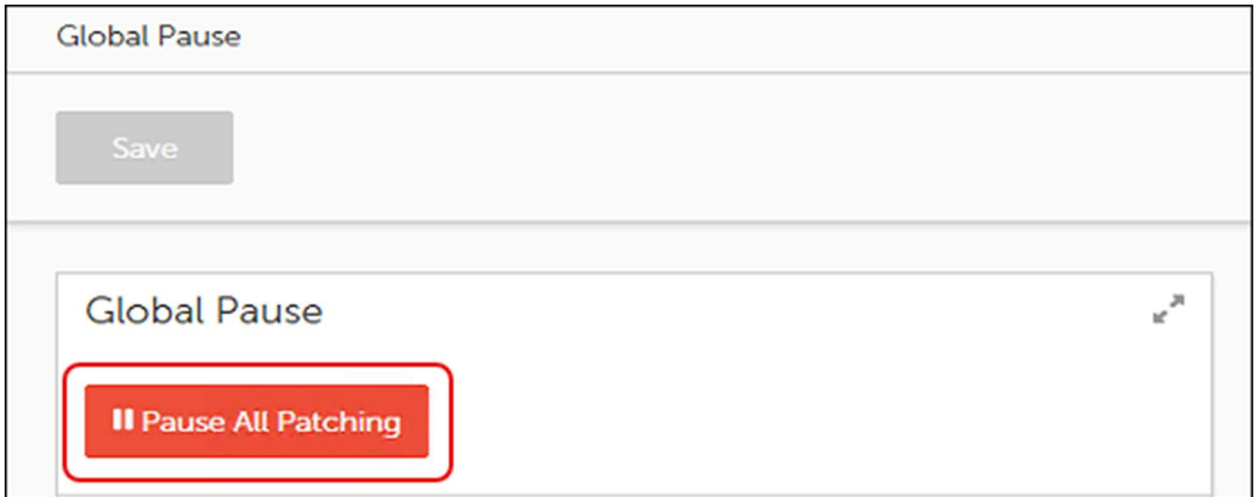
## Stop All Patching Activity Immediately

To stop all patching activity on all licensed clients in the estate, use the following steps to activate Global Pause.

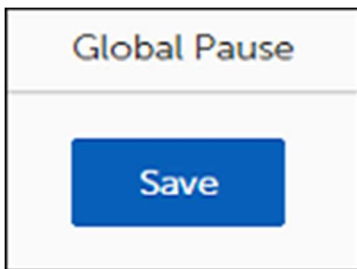
1. Select **Flex Controls** on the Home menu, and then select **Global Pause**.



This opens the **Global Pause** dialog:



2. Select **Pause All Patching**.

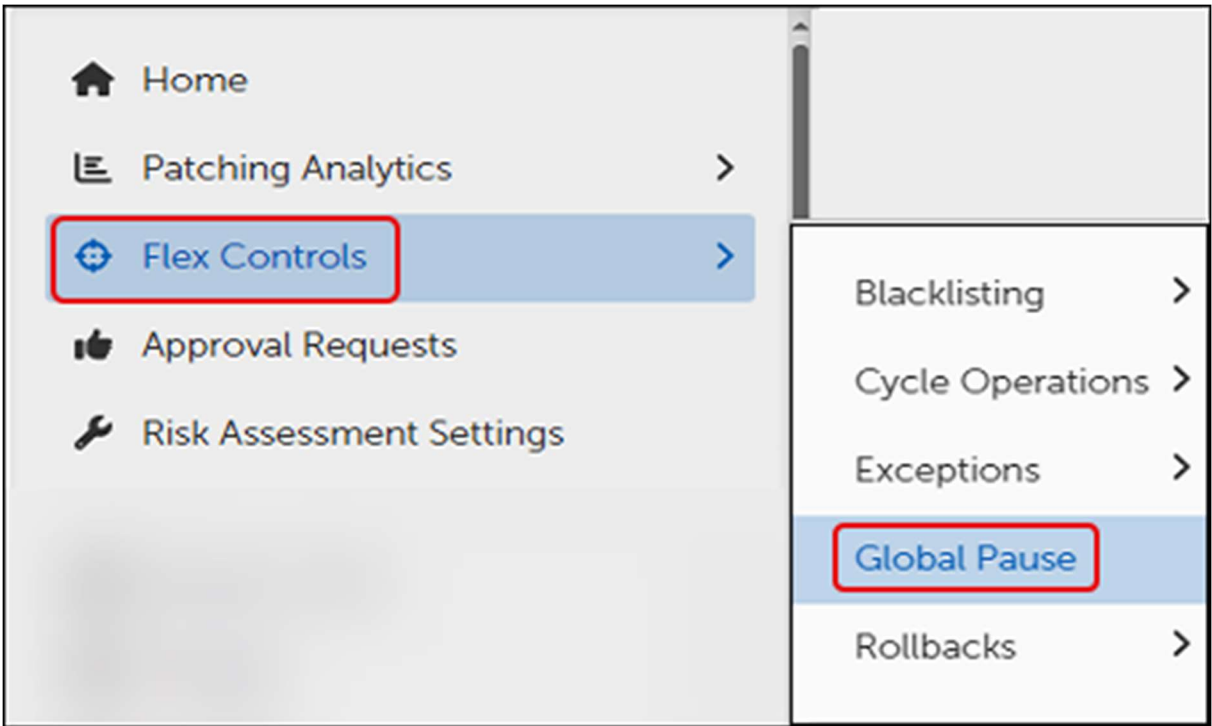


3. Select **Save** to activate Global Pause. This immediately stops all patch deployments across all licensed clients:
  - a. All patch deployments in progress that have not reached an irreversible state are paused immediately.
  - b. All newly initiated patch deployments are paused automatically.

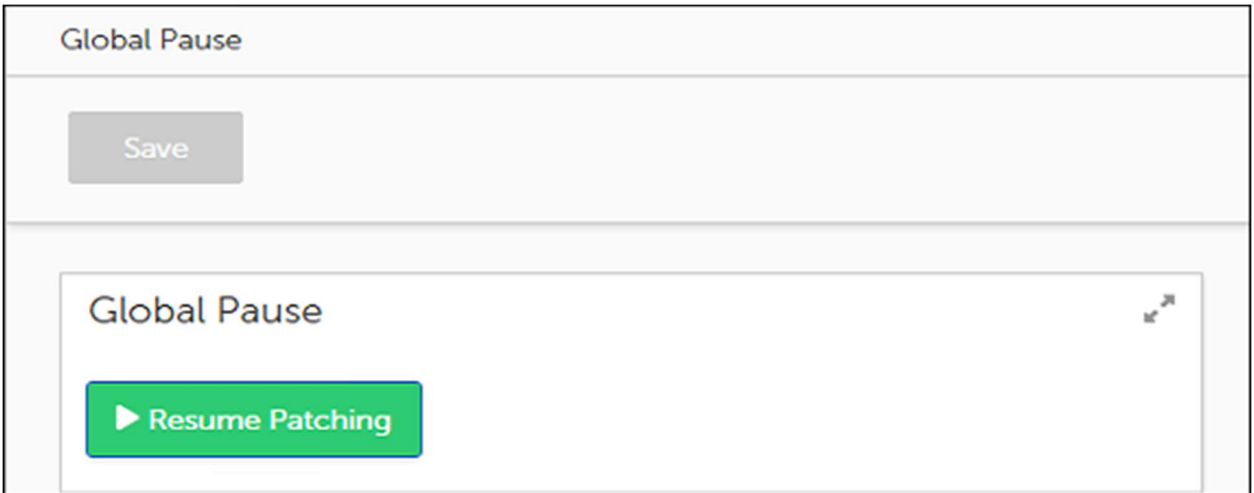
## Resume All Paused Patching Activity Immediately

To resume all paused patching activity on all licensed clients, use the following steps to revoke a Global Pause.

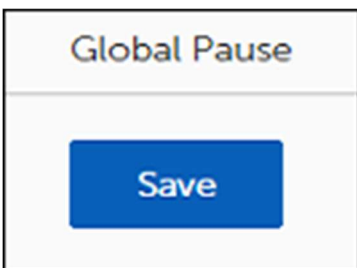
1. Select **Flex Controls** on the Home menu, and then select **Global Pause**.



This opens the **Global Pause** dialog:



2. Select **Resume Patching**.



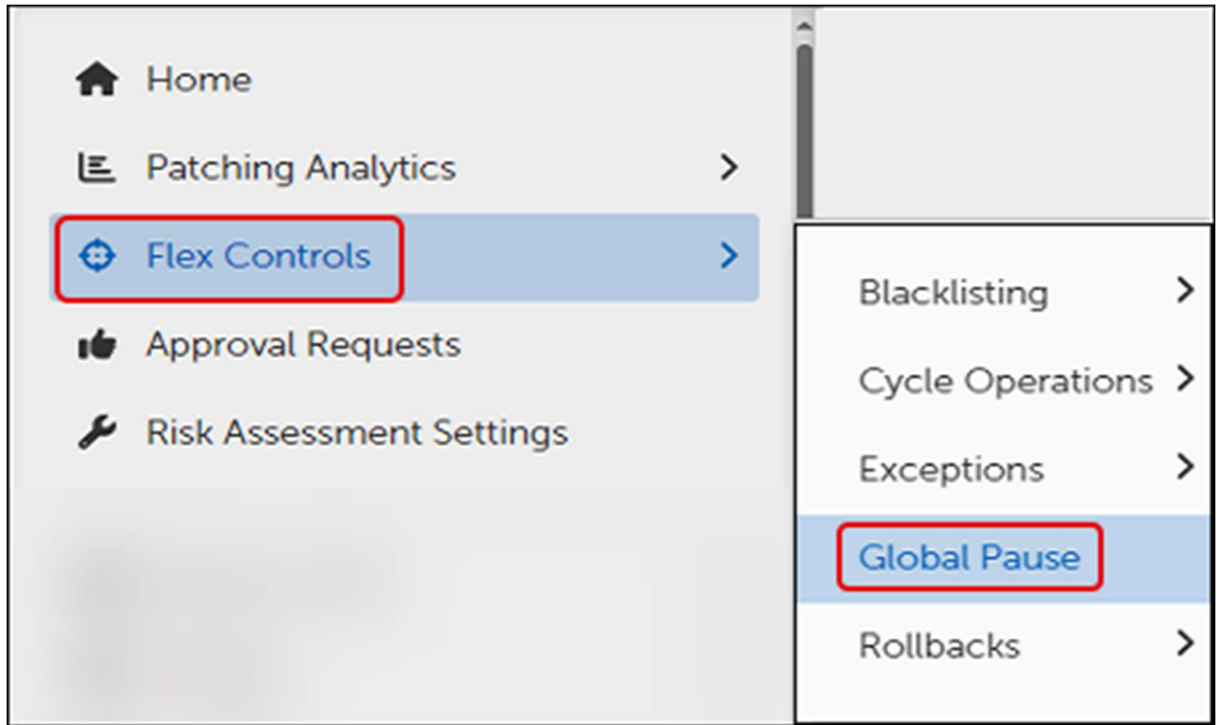


3. Select **Save** to revoke the Global Pause. This immediately revokes the Global Pause and allows patching activity to occur as configured.

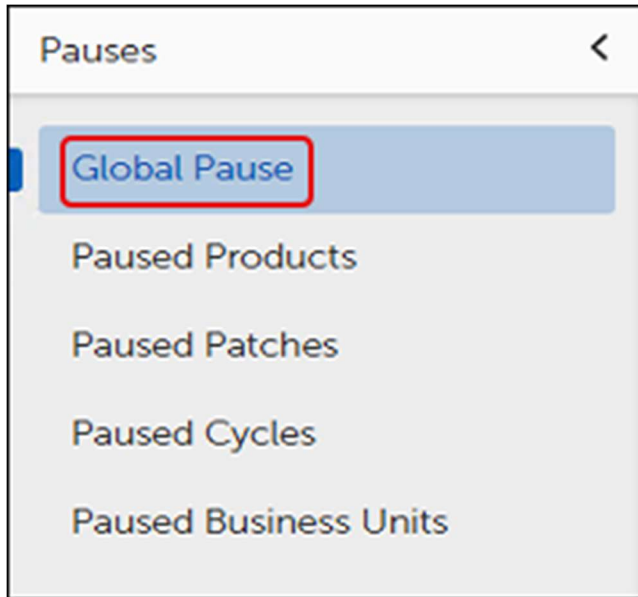
## Pause Patching for Specific Objects

To stop patching activity for specific objects, such as Products, Patches, Cycles, and Business units, use the following steps to access the Pause menu items:

1. Select **Flex Controls** on the Home menu, and then select **Global Pause**.



This opens the Pauses menu:



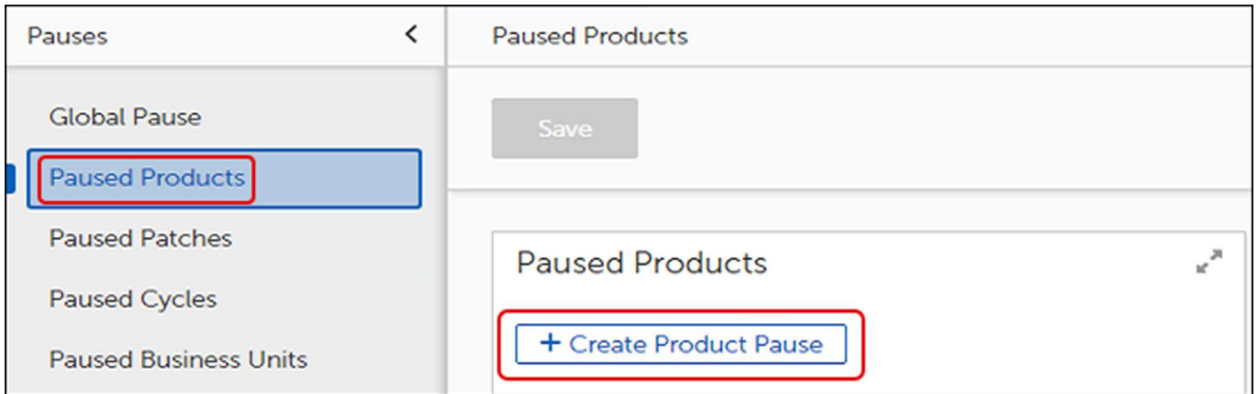
2. Select the pause you want to configure. You can configure multiple types of pauses, but you must configure them separately.
  - a. **Global Pause:** Pause all patching activity immediately ([Stop All Patching Activity Immediately](#)).
  - b. **Paused Products:** Pause patch deployments for one or more products ([Pause Deployment of a Specific Software Product](#)).
  - c. **Pause Patches:** Pause deployment of a software patch or release for one or more products ([Paused Patches](#)).
  - d. **Paused Cycles:** Specify a [Patching](#), [Deployment](#), or [Rollout](#) cycle to pause for one or more products.
  - e. **Pause Business Units:** Pause patch deployments for one or more [Business Units](#).

## Pause Deployment of a Specific Software Product

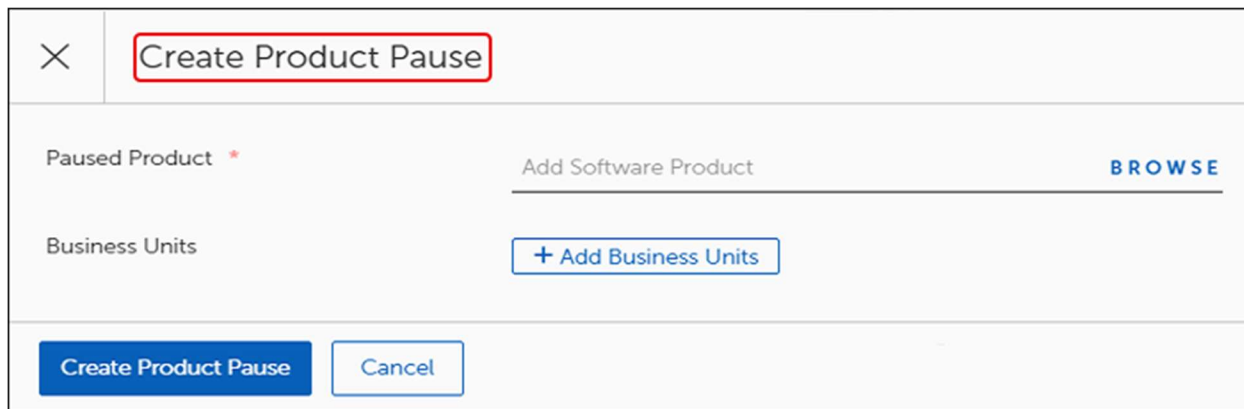
To stop patching activity for specific software products or patches, complete the following steps:

1. Navigate to the Pauses menu (see [Pause Patching for Specific Objects](#)), and then select **Paused Products**.

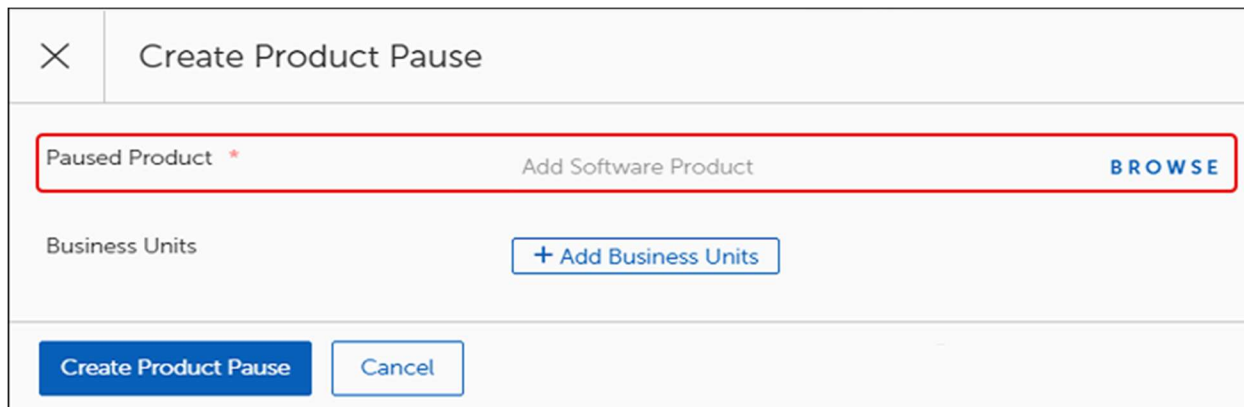
This opens the Paused Products dialog:



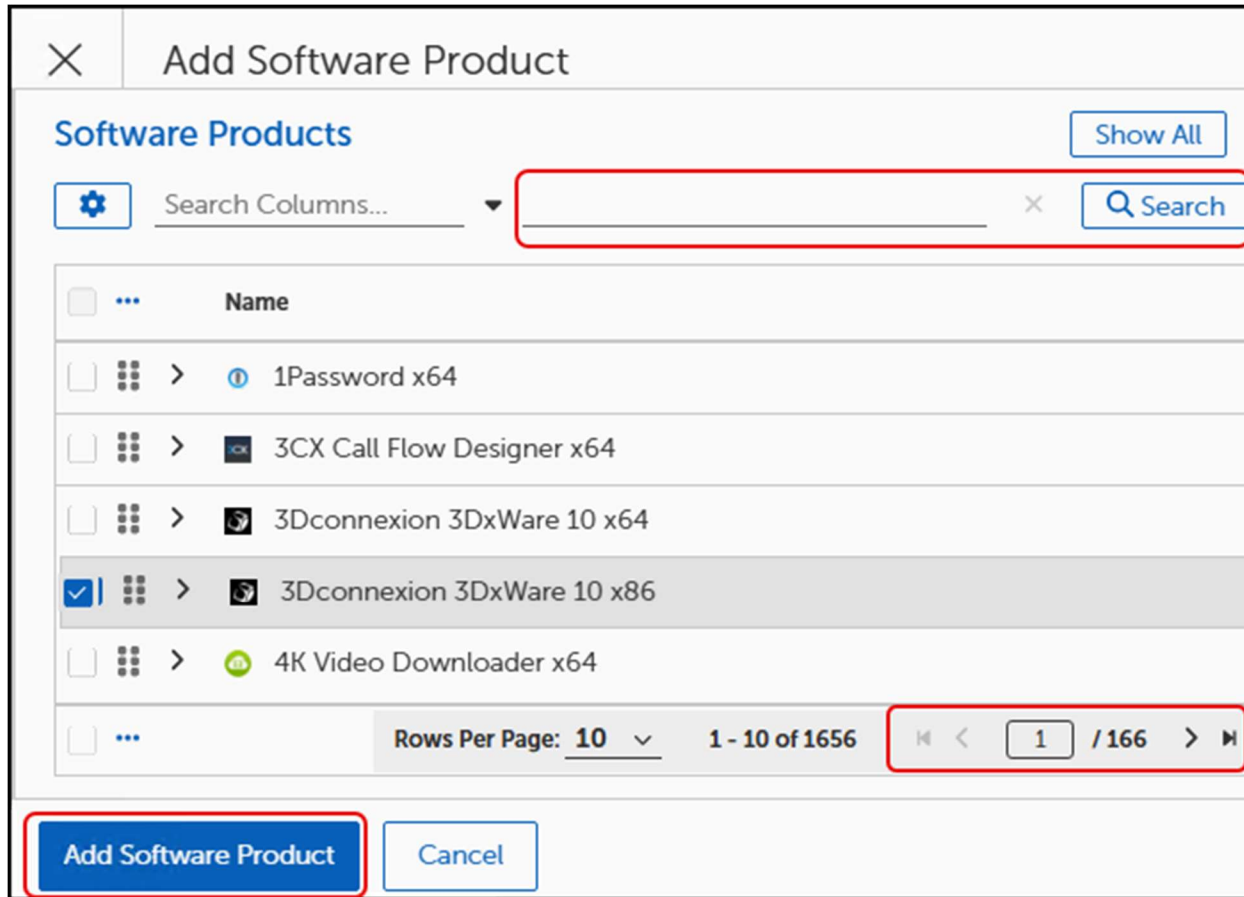
- a. Select **+Create Product Pause** to open the **Create Product Pause** dialog:



- b. Select **Browse** to find the software product to pause.



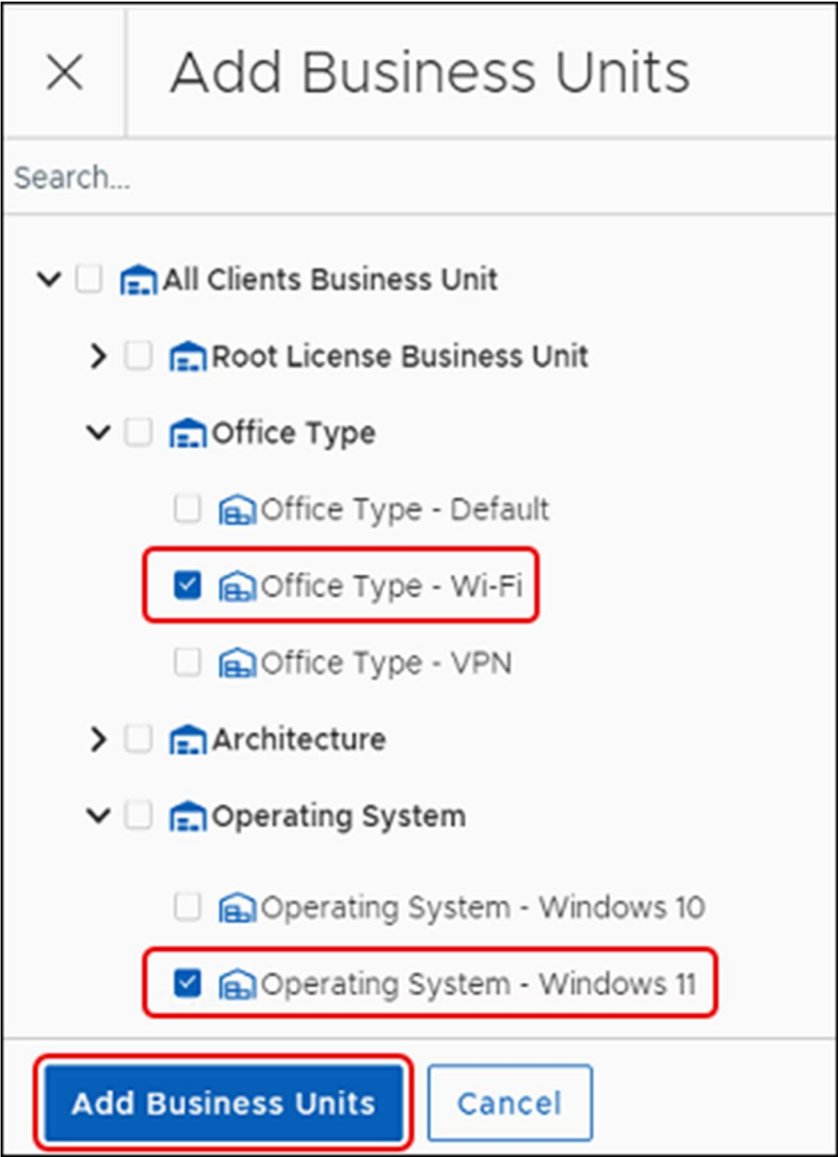
- c. Select the software product you want to pause using either of the following methods:



- Use the navigation tools on the bottom right to scroll through the pages and select one or more **Software Products** from the table.
  - Enter a product name on the search line, and then click **Search** to find a specific product
2. Select **Add Software Product** to return to the **Create Product Pause** dialog, and then choose one of the following methods to proceed:
    - a. To create a **Global Pause** for the selected products, click **Create Product Pause**. This pauses the deployment of the selected software product on all devices in the estate.
    - b. To specify a pause for specific devices, continue with the next step to **Add Business Units**.
  3. Add or remove **Business Units**:
    - a. To remove existing Business Units, select the **ellipsis (...)** under **Actions**, and then select **Remove Row**.
    - b. To add Business Units, complete the following steps:
      - i. Select **+ Add Business Units** in the open workspace or dialog.



This opens the **Add Business Units** workspace. The following example shows possible choices.



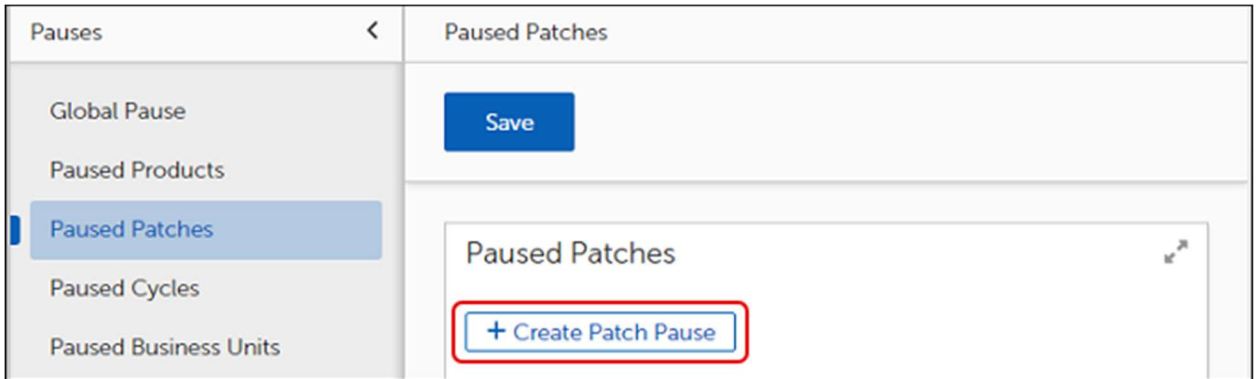
- ii. Select one or more **Business Units** to add, and then click **Add Business Units**.
- 4. Select **Create Product Pause** and then click **Save** to create a global pause for the selected products.

# Pause Deployment of a Specific Patch

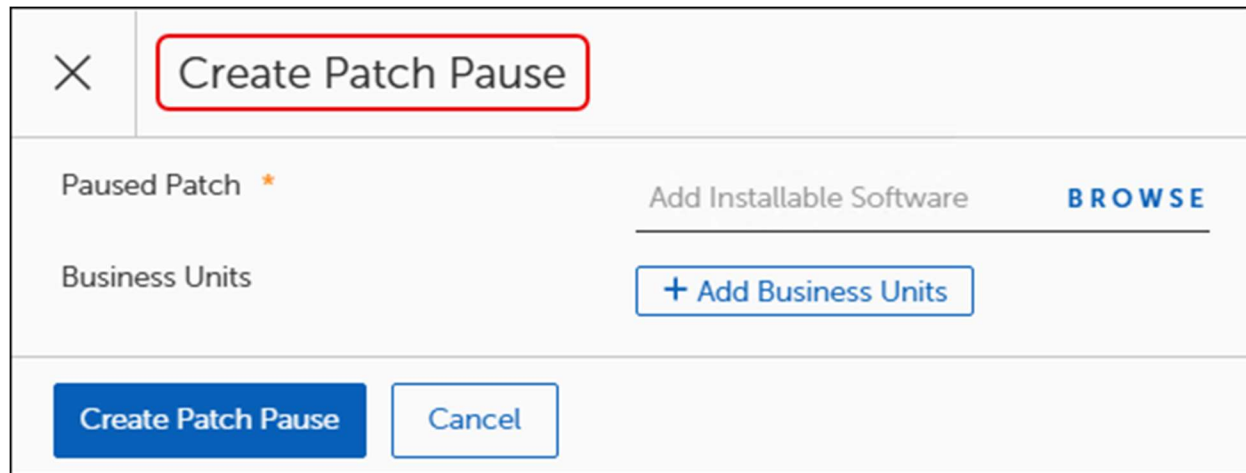
To stop patching activity for a specific patch, complete the following steps:

1. Navigate to the Pause menu (see [Pause Patching for Specific Objects](#)), and then select **Paused Patches**.

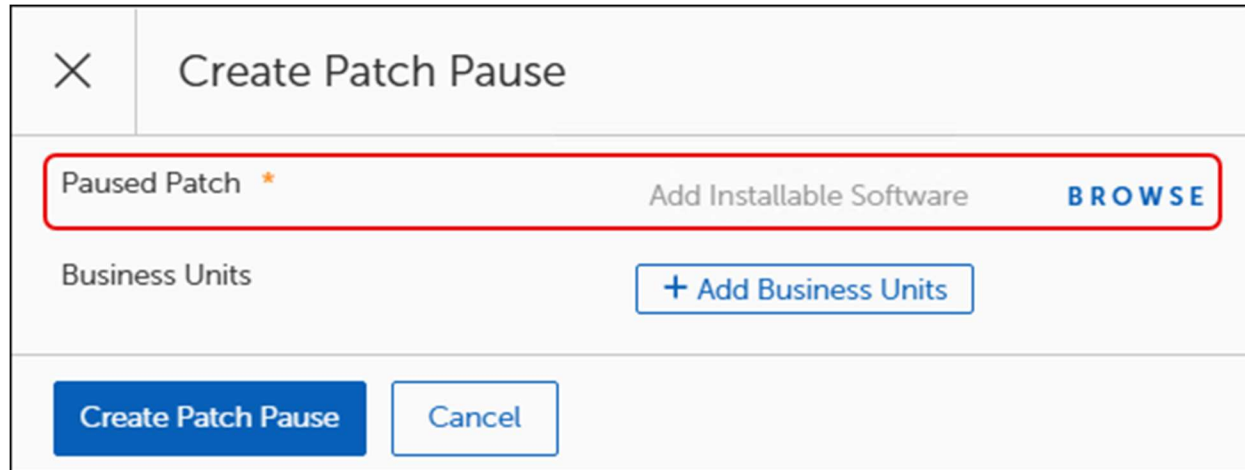
This opens the Paused Patches dialog:



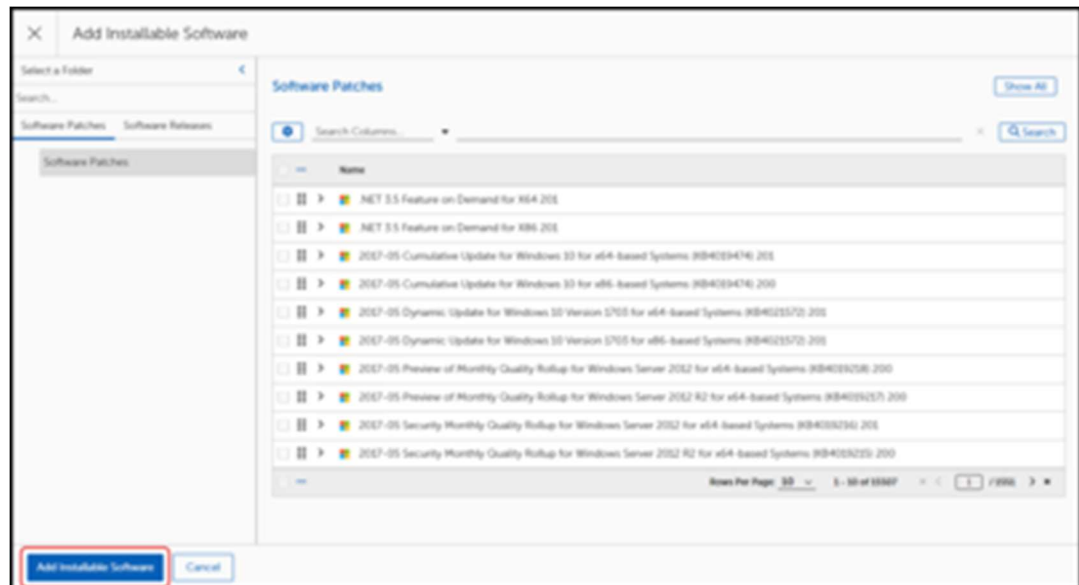
- a. Select **+Create Patch Pause** to open the **Create Product Pause** dialog, and then select Browse to find the Software patch you want to pause:



- b. Select **Browse** to find the Software Patch to pause:

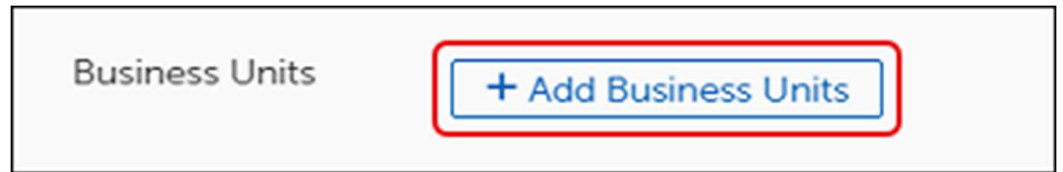


- c. Select the patch you want to pause:

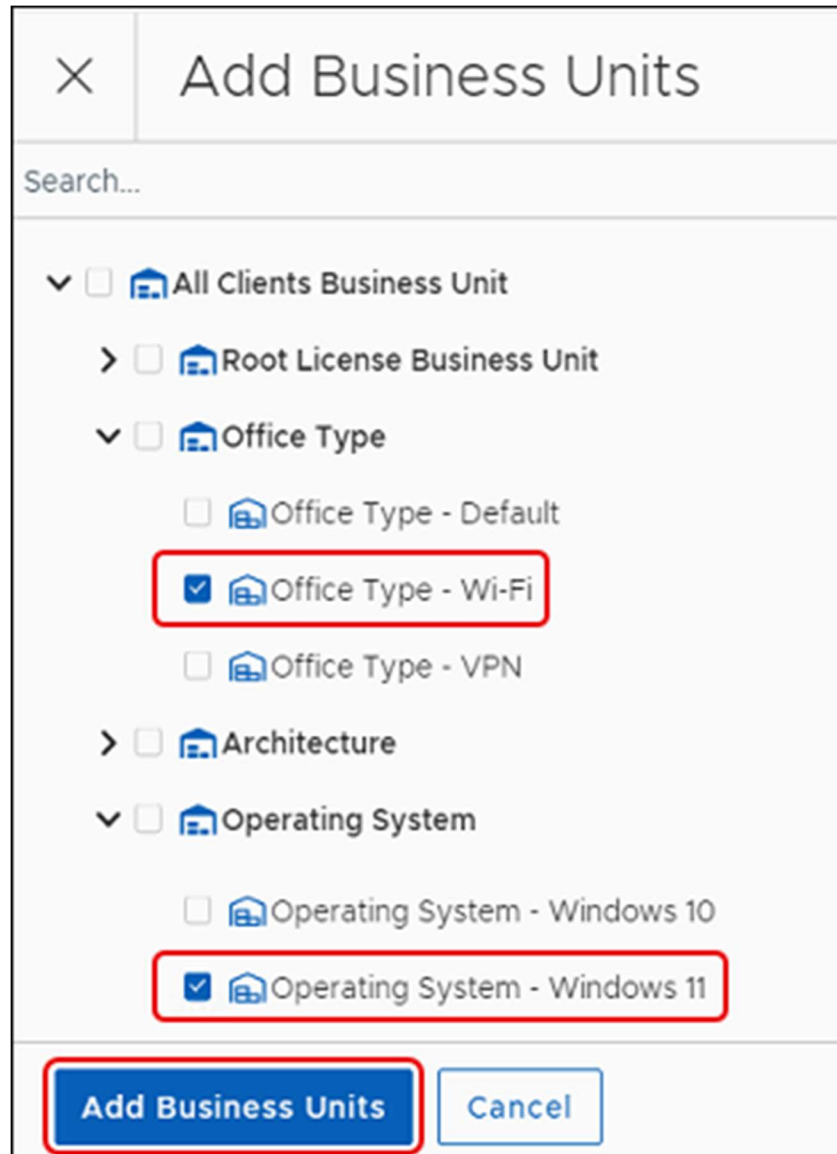


2. Select **Add Installable Software Product** to return to the **Create Patch Pause** dialog, and then choose one of the following methods to proceed:
  - a. To create a **Global Pause** for the selected products, click **Create Patch Pause**. This pauses the deployment of the selected software patch on all devices in the estate.
  - b. To specify a pause for specific devices, continue with the next step to **Add Business Units**.
3. Add or remove **Business Units**:
  - a. To remove existing Business Units, select the **ellipsis (...)** under **Actions**, and then select **Remove Row**.
  - b. To add Business Units, complete the following steps:

- i. Select **+ Add Business Units** in the open workspace or dialog.



This opens the **Add Business Units** workspace. The following example shows possible choices.



- ii. Select one or more **Business Units** to add, and then click **Add Business Units**.



4. Select **Create Patch Pause** and then click **Save** to create a global pause for the selected patch.

## Pause Specific Cycles

Tenable Patch Management allows you to create Patching Cycles, Deployment Cycles, and Rollout Cycles to customize patching in your estate. Global Pause provides a way to pause these cycles when necessary. You may create a pause for one cycle at a time.

- [Paused Cycles - Patching](#)
- [Paused Cycles - Deployment](#)
- [Paused Cycles - Rollout](#)

### Important

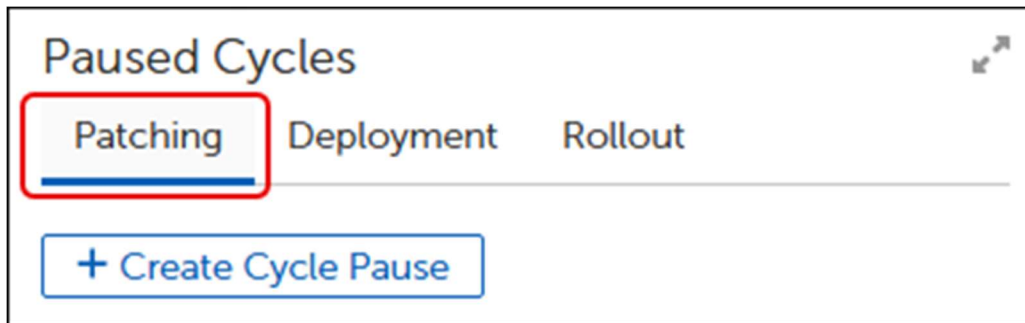
Pausing a cycle that is currently in a WAITING state (has not run yet), prevents that cycle from running until you remove the pause. This is the only server-side behavior related to pausing.

### Pause a Patching Cycle

To stop patching activity for a specific patching cycle, complete the following steps:

1. Navigate to the Pauses menu (see [Pause Patching for Specific Objects](#)), and then select **Paused Cycles**.

This opens the **Paused Cycles** dialog to the **Patching** tab:



2. Select **+Create Cycle Pause** to open the **Create Cycle Pause** dialog, and then click **Browse**.

✕
Create Cycle Pause

Cycle \* Browse

---

Business Units + Add Business Units

Create Cycle Pause
Cancel

3. Search for and select the patching cycle you want to pause using one of the methods described below:

**Important**

Cycles do not appear unless you have created them previously. If you do not have a cycle to stop, do not complete this section.

✕
Select a Patching Cycle

⚙️

Search Columns...
▾

✕

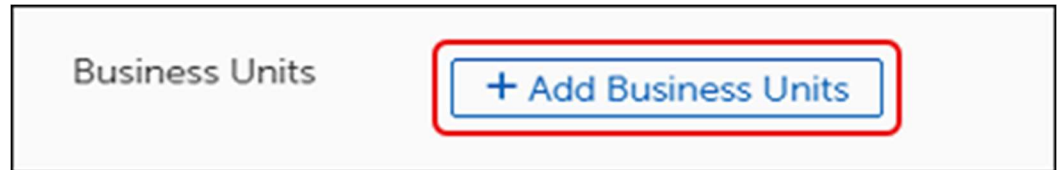
🔍 Search

No data provided

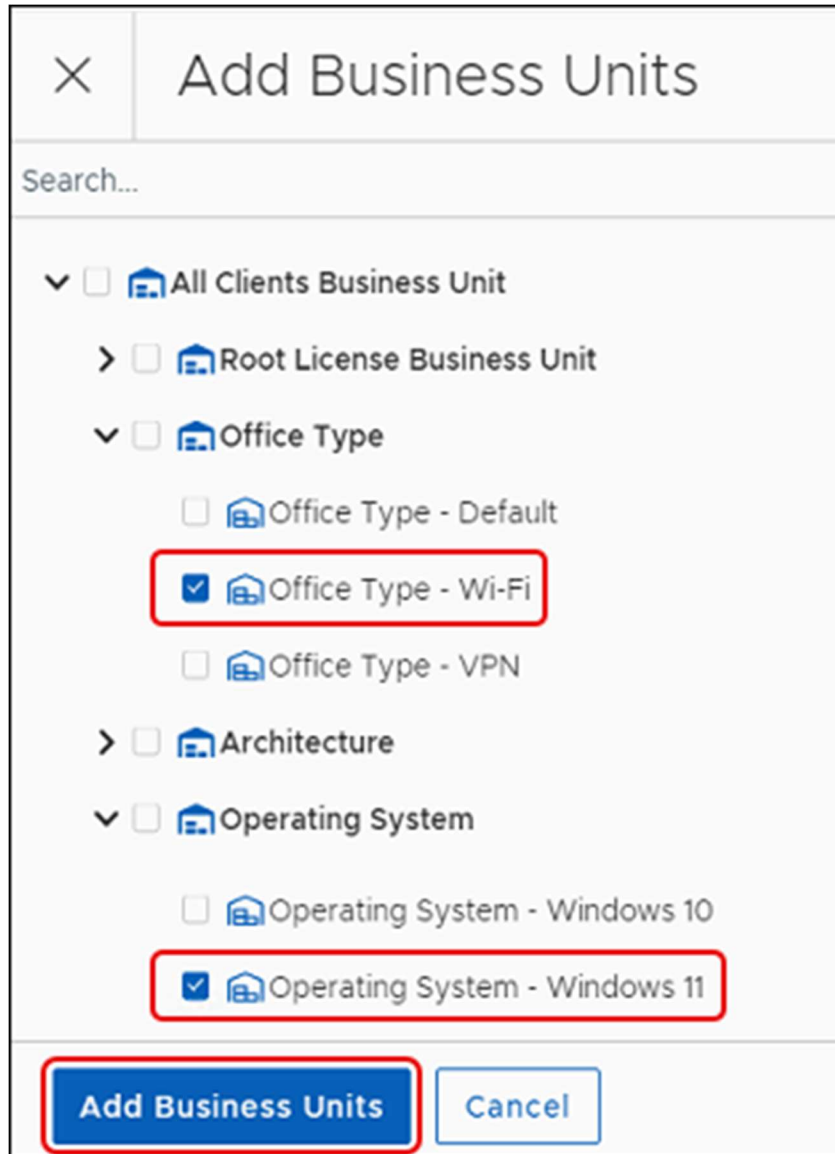
OK

Cancel

- a. Use the navigation tools on the bottom right to scroll through the pages to find and select a Patching Cycle from the table.
  - b. Enter a cycle name on the search line, and then click **Search** to find and select a specific cycle.
4. Select **OK**, and then choose one of the following options to proceed:
- a. To create a **Global Pause** for the selected cycle, skip to **Step 6**. This pauses the deployment of the selected cycle on all devices in the estate.
  - b. To specify a pause for specific devices, continue with the next step to **Add Business Units**.
5. Add or remove **Business Units**:
- a. To remove existing Business Units, select the **ellipsis (...)** under **Actions**, and then select **Remove Row**.
  - b. To add Business Units, complete the following steps:
    - i. Select **+ Add Business Units** in the open workspace or dialog.



This opens the **Add Business Units** workspace. The following example shows possible choices.



- ii. Select one or more **Business Units** to add, and then click **Add Business Units**.

6. Select **Create Cycle Pause** and then click **Save** to create a pause for the selected cycle.

#### *Pause a Deployment Cycle*

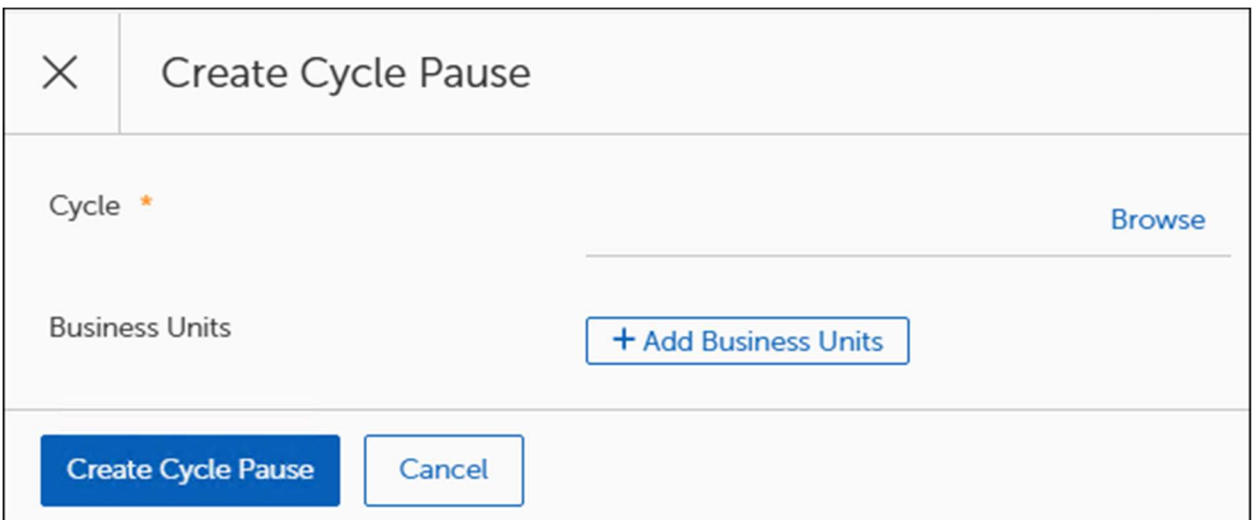
To stop all patching activity for a specific deployment cycle, complete the following steps:

1. Navigate to the Pauses menu (see [Pause Patching for Specific Objects](#)), and then select **Paused Cycles**.

This opens the **Paused Cycles** dialog to the **Deployment** tab:



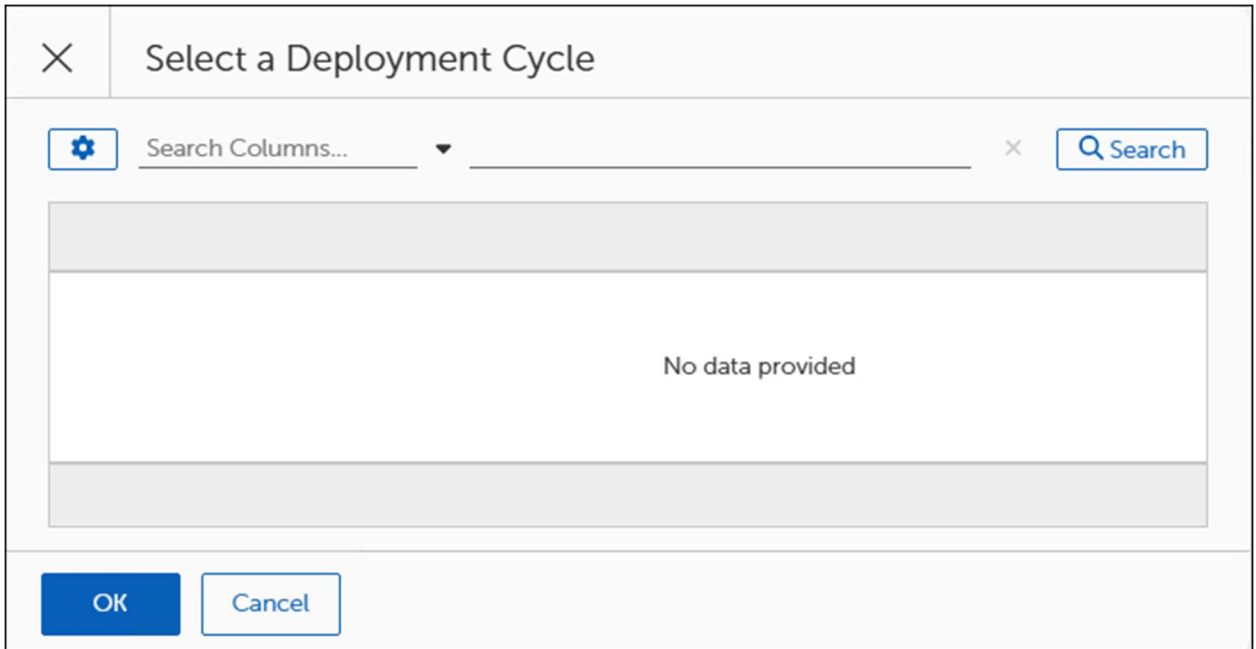
2. Select **+Create Cycle Pause**. This opens the **Create Cycle Pause** dialog:



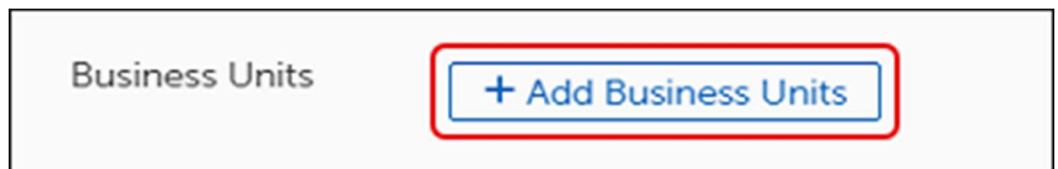
3. Select **Browse** to open the Select a Deployment Cycle dialog, and then use one of the methods below to find and select a cycle.

**Important**

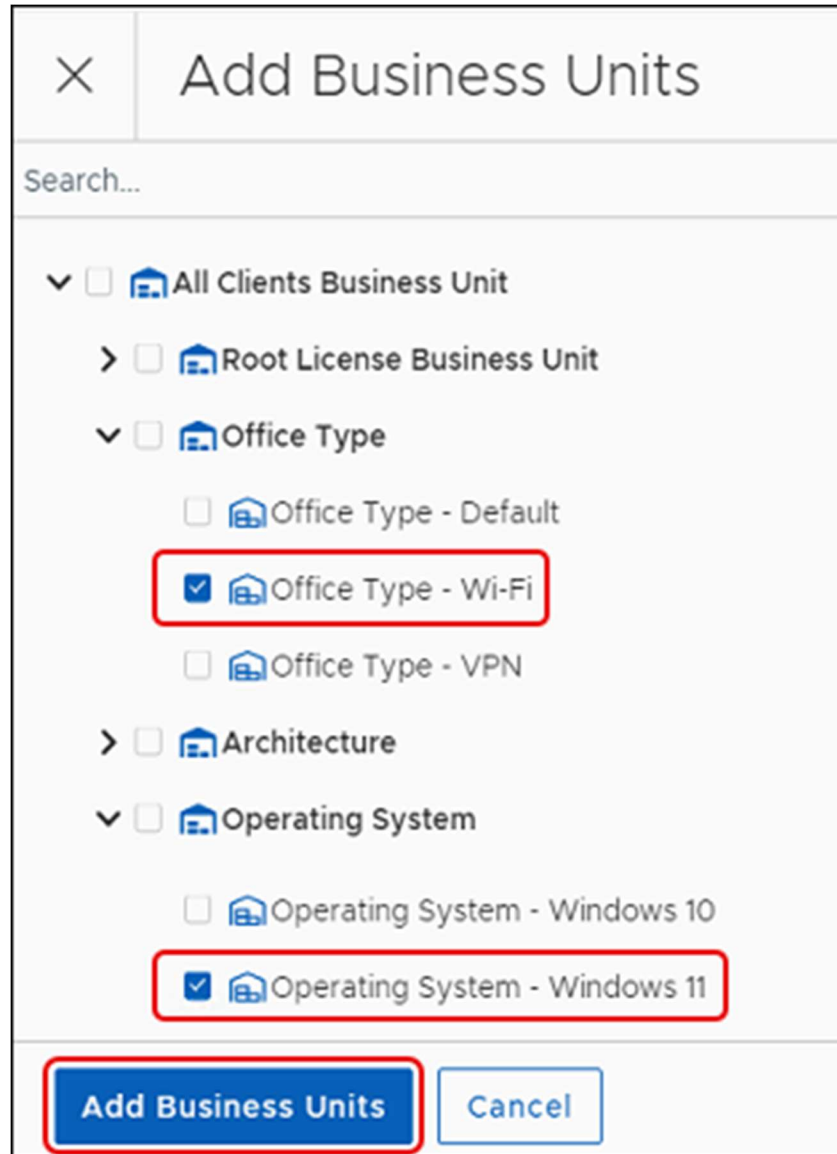
Cycles do not appear unless you have created them previously. If you do not have a cycle to pause, choose a different pause method.



- a. Use the navigation tools on the bottom right to scroll through the pages to find and select a cycle from the table.
  - b. Enter a cycle name on the search line, and then click **Search** to find and select a specific cycle
4. Select **OK** to save your entry, and then choose one of the following options to proceed:
  - a. To create a **Global Pause** for the selected cycle, skip to **Step 6**. This pauses the deployment of the selected software product on all devices in the estate.
  - b. To specify a pause for specific devices, continue with the next step to **Add Business Units**.
5. Add or remove **Business Units**:
  - a. To remove existing Business Units, select the **ellipsis (...)** under **Actions**, and then select **Remove Row**.
  - b. To add Business Units, complete the following steps:
    - i. Select **+ Add Business Units** in the open workspace or dialog.



This opens the **Add Business Units** workspace. The following example shows possible choices.



- ii. Select one or more **Business Units** to add, and then click **Add Business Units**.

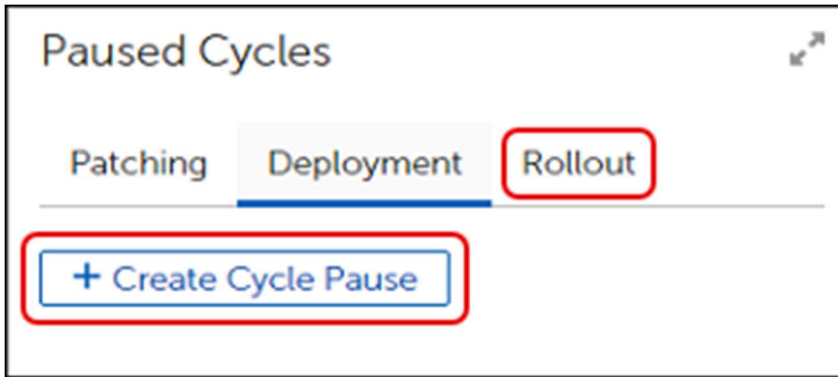
- 6. Select **Create Cycle Pause** and then click **Save** to create a pause for the selected cycle.

*Pause a Rollout Cycle*

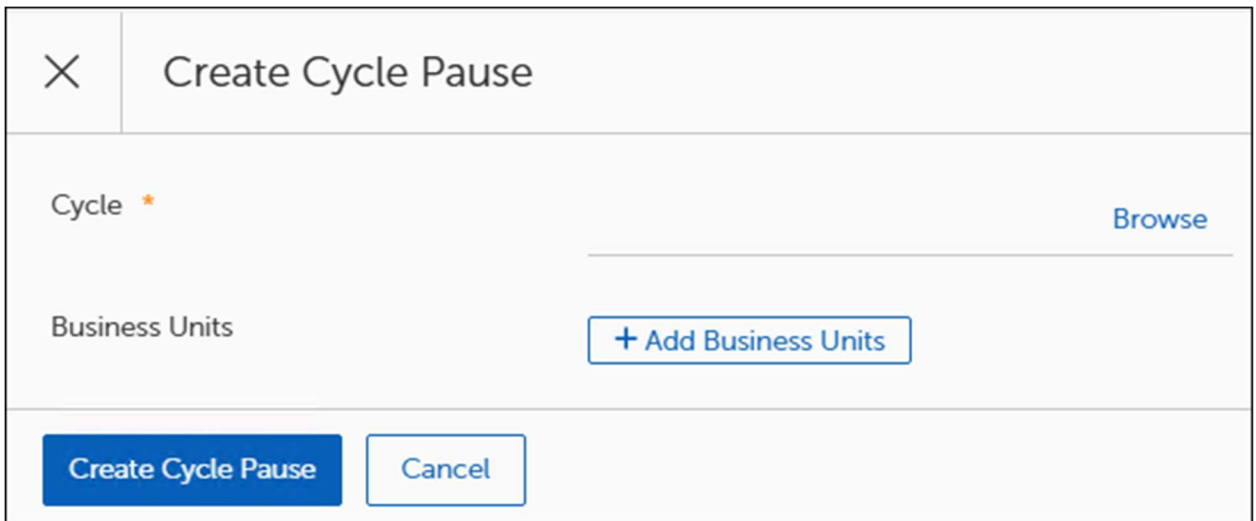
To stop all patching activity for a specific rollout cycle, complete the following steps:

- 1. Navigate to the Pauses menu (see [Pause Patching for Specific Objects](#)), and then select **Paused Cycles**.

This opens the **Paused Cycles** dialog to the **Rollout** tab:



2. Select **+Create Cycle Pause**. This opens the **Create Cycle Pause** dialog:

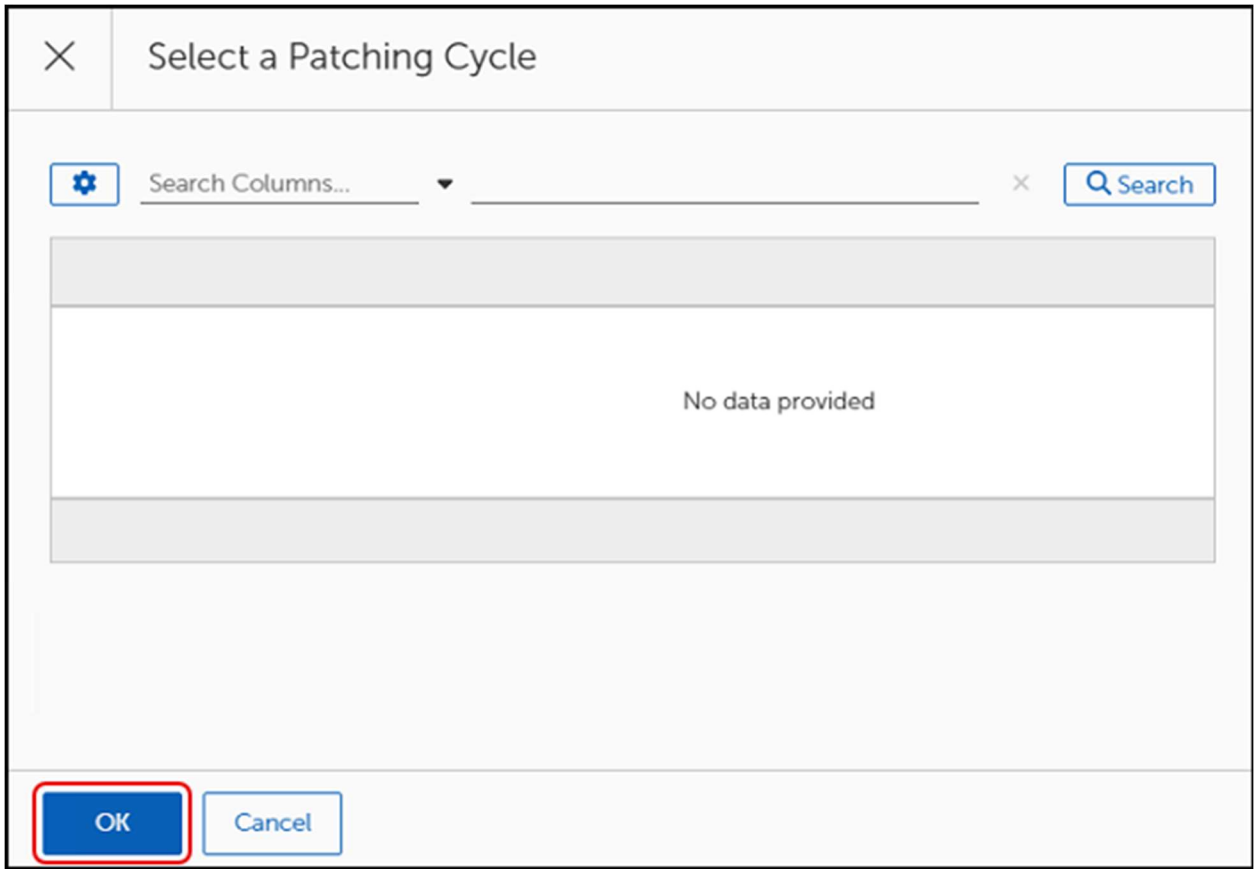


3. Select **Browse** to select the rollout cycle you want to pause. This opens the **Select a Rollout Cycle** dialog.

**Important**

Cycles do not appear unless you have created them previously. If you do not have a cycle to stop, do not complete this section.

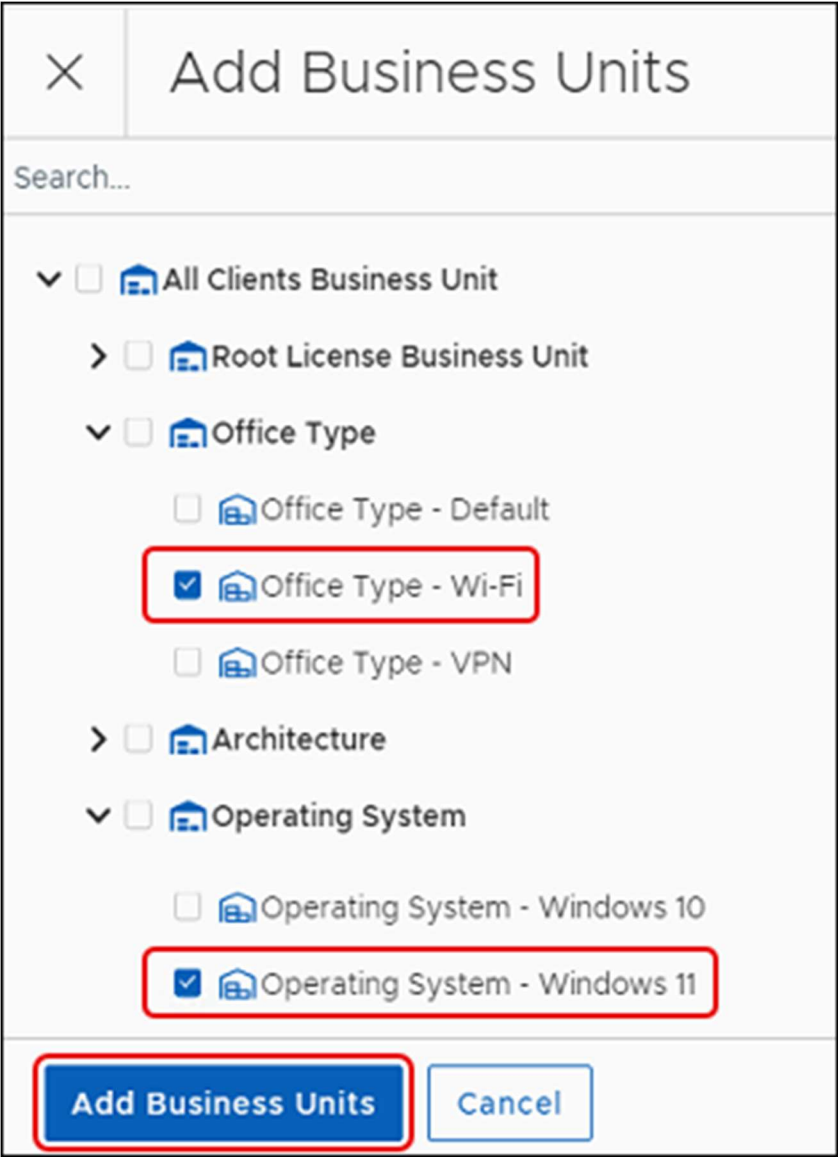




- a. Use the navigation tools on the bottom right to scroll through the pages to find and select a **Rollout Cycle** from the table.
- b. Enter a cycle name on the search line, and then click **Search** to find and select a specific cycle.
4. Select **OK**, and then choose one of the following options to proceed:
  - a. To create a **Global Pause** for the selected cycle, skip to **Step 6**. This pauses the deployment of the selected software product on all devices in the estate.
  - b. To specify a pause for specific devices, continue with the next step to **Add Business Units**.
5. Add or remove **Business Units**:
  - a. To remove existing Business Units, select the **ellipsis (...)** under **Actions**, and then select **Remove Row**.
  - b. To add Business Units, complete the following steps:
    - i. Select **+ Add Business Units** in the open workspace or dialog.



This opens the **Add Business Units** workspace. The following example shows possible choices.



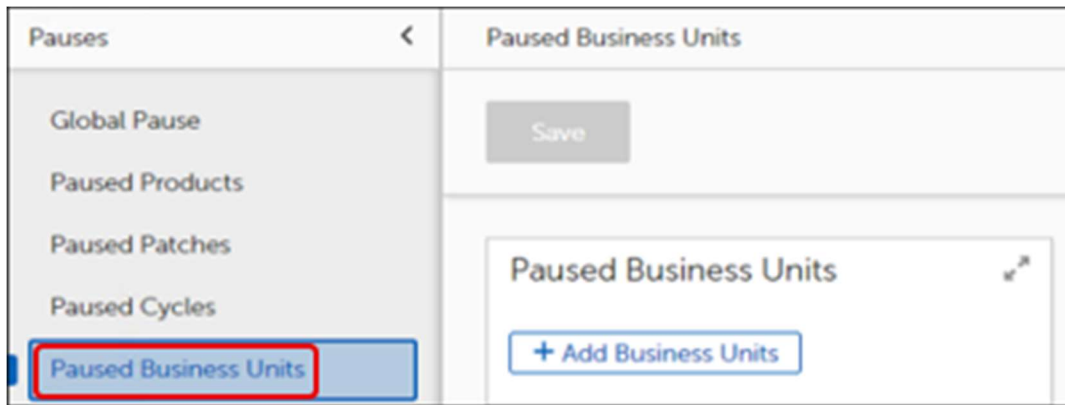
- ii. Select one or more **Business Units** to add, and then click **Add Business Units**.
- 6. Select **Create Cycle Pause** and then click **Save** to create a pause for the selected rollout cycle.

# Pause Deployment to a Business Unit

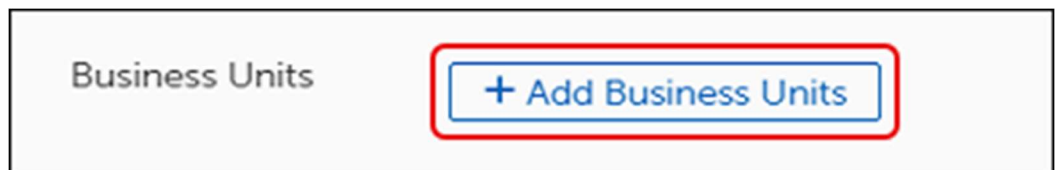
To stop patching deployment for specific business units, complete the following steps:

1. Navigate to the Pauses menu (see [Pause Patching for Specific Objects](#)), and then select **Paused Business Units**.

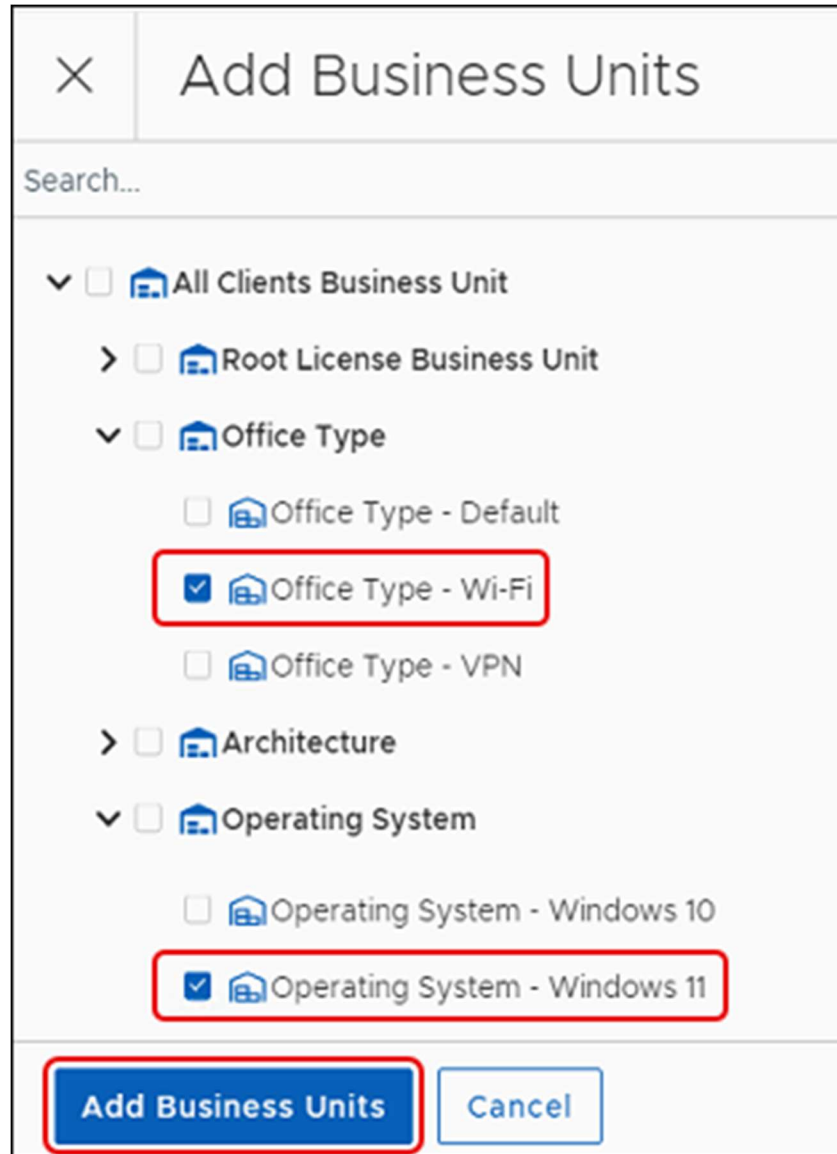
This opens the Paused Business Units dialog:



2. Add or remove **Business Units**:
  - a. To remove existing Business Units, select the **ellipsis (...)** under **Actions**, and then select **Remove Row**.
  - b. To add Business Units, complete the following steps:
    - i. Select **+ Add Business Units** in the open workspace or dialog.



This opens the **Add Business Units** workspace. The following example shows possible choices.



ii. Select one or more **Business Units** to add, and then click **Add Business Units**.

3. Select **Save** to create a global pause for the selected business unit or business units.

## Rollbacks Overview

The Rollbacks feature of Tenable Patch Management allows you to rollback one or more patches or releases to a previous version (Rollback), or you may rollback one or more patches or releases to an earlier, non-sequential version (Rollback to Version).

In either case, you may configure Rollback activities across your entire estate or limit a rollback to one or more Business Units.

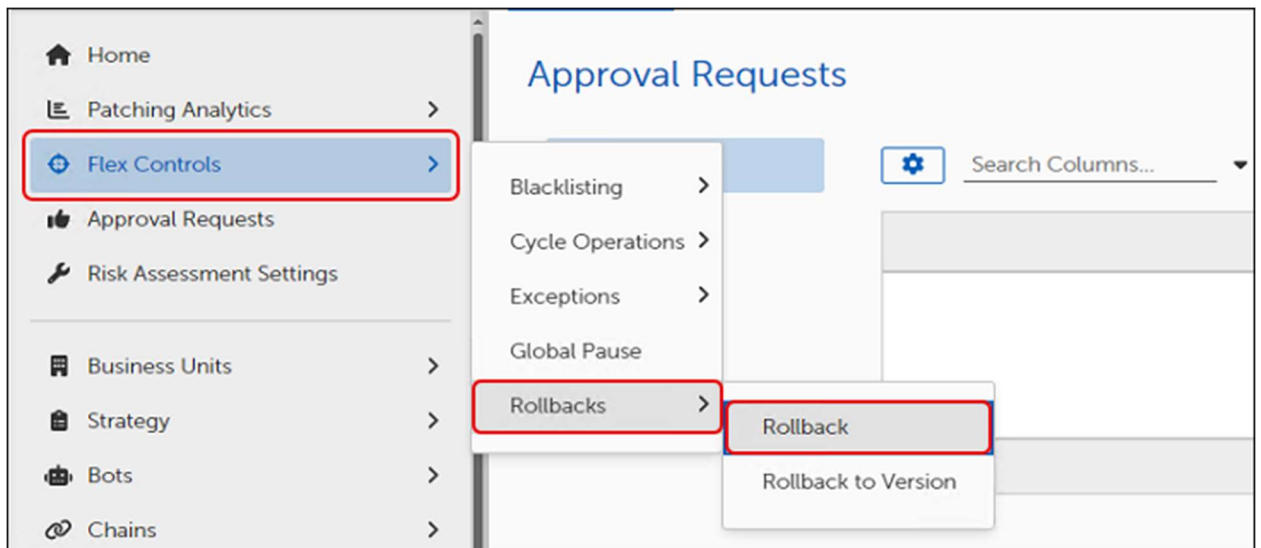
# Rollback

Use the Rollback template to rollback a patch or release to the previous version. To rollback to a specific, earlier version, see [Rollback to Version](#).

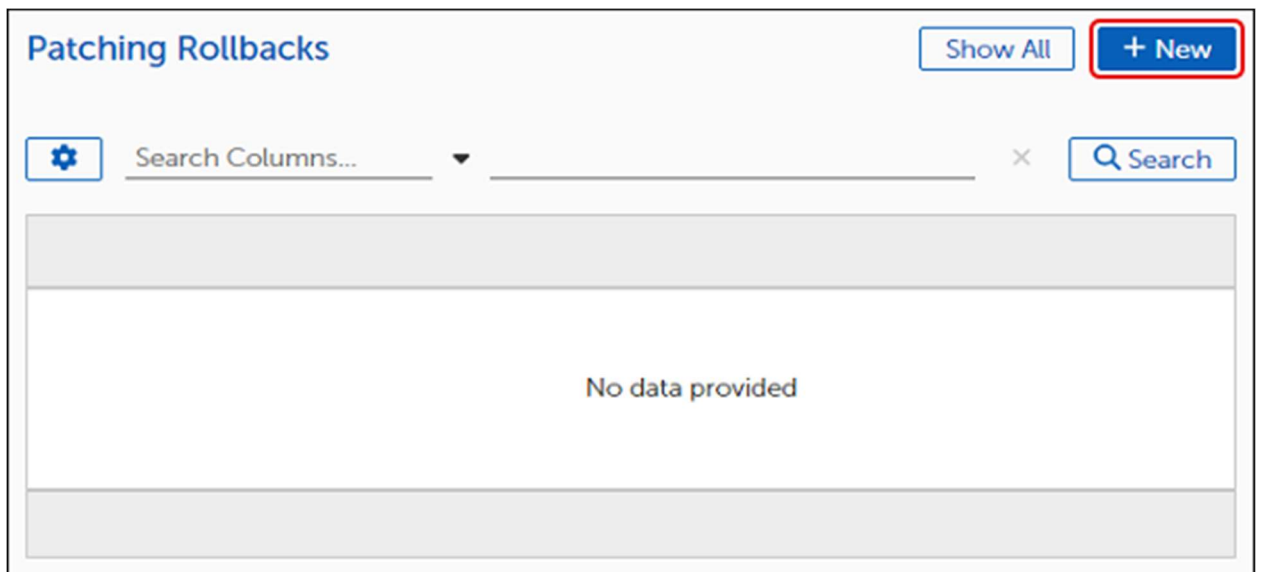
## Create a Rollback

Use the Rollback template to configure a patch or release rollback to the previous version:

1. Select **Flex Controls** on the left navigation menu of the [Tenable Patch Management Dashboard](#), and then select **Rollbacks > Rollback**.



This opens the Patching Rollbacks table. Until you create a rollback, the table is empty.



2. Select **+New** to open the Rollback template, and then enter a **Name** and a detailed **Description** of the rollback.

**Note**

A red asterisk next to a field name indicates a required field.

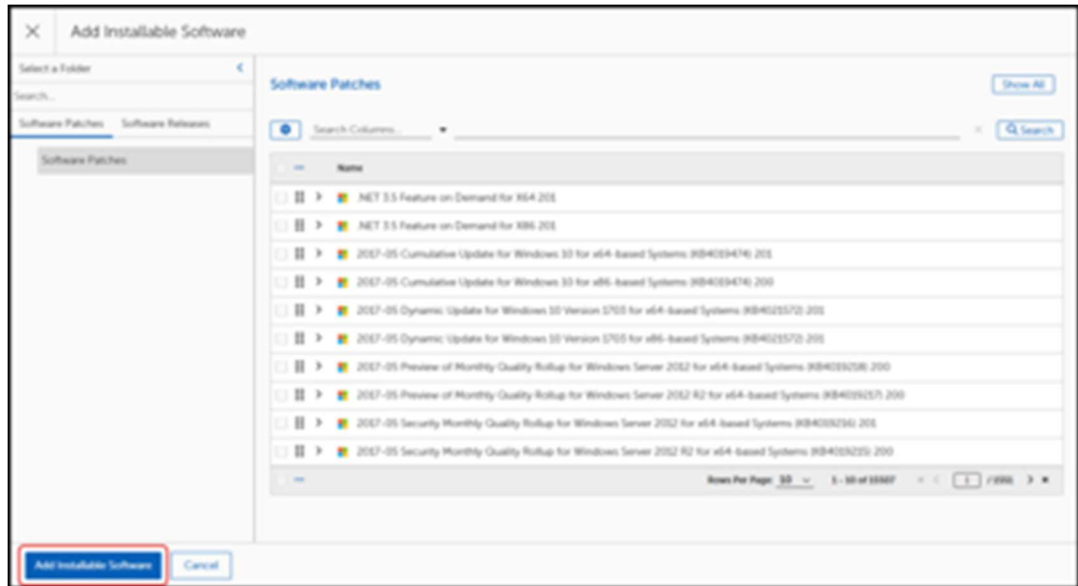
The screenshot shows a form titled "General Settings" with a close button in the top right corner. It contains the following fields and controls:

- Name \***: A text input field with the label "Name" above it.
- Description**: A large text area with the label "Description" above it.
- Patch *i* \***: A label with an information icon and a red asterisk. Below it is the text "Add Installable Software" and a blue button labeled "BROWSE".
- Target Business Units *i* \***: A label with an information icon and a red asterisk. Below it is a blue button labeled "+ Add Business Units".

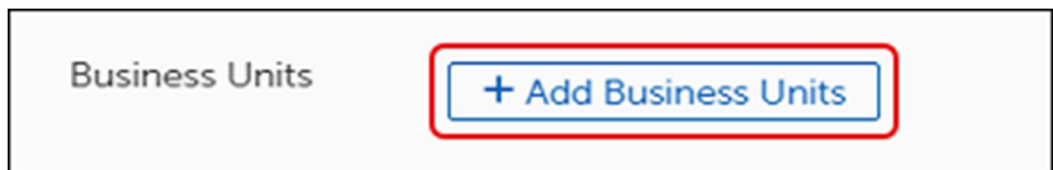
3. Locate the patch or release you want to roll back:

This close-up shows the "Patch *i* \*" label, the "Add Installable Software" text, and a blue button labeled "BROWSE" which is highlighted with a red rectangular border.

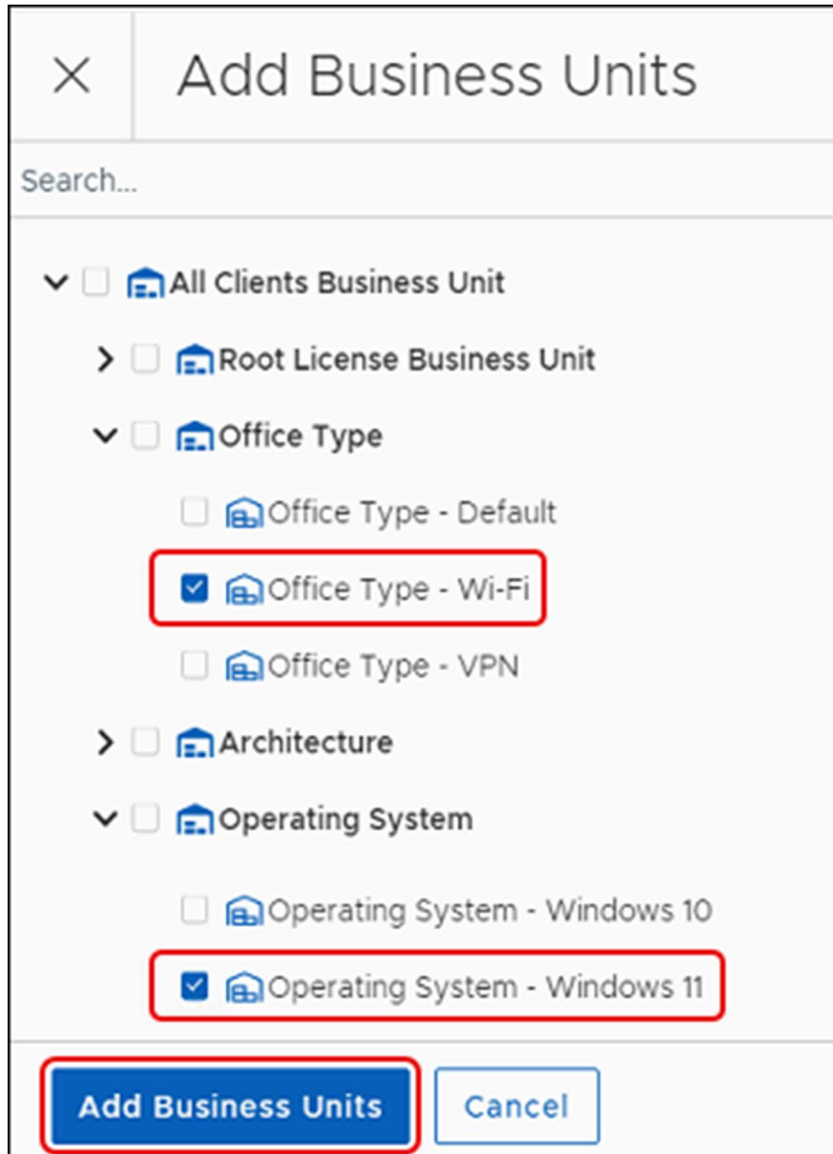
4. Select a Software patch or release :
  - a. Select one of the following tabs from the left-side column of the **Add Installable Software** dialog box:
    - Select the Software Patches tab to choose a patch release.
    - Select the Software Releases tab to choose a product release.
  - b. Choose one of the methods below to search for a patch or release:



- Use the navigation tools on the bottom right to scroll through the pages to find and select a Software product or release.
  - Enter a product name on the search line, and then click **Search** to find and select a specific product.
5. Add one or more Business Units to specify the devices to rollback.
- a. Select **+ Add Business Units** in the open workspace or dialog.



This opens the **Add Business Units** workspace. The following example shows possible choices.



- b. Select one or more **Business Units** to add, and then click **Add Business Units**.
6. Select **Save** to save the Rollback configuration. This returns you to the **Patching Rollbacks** table, which lists your new rollback.

*Edit a Rollback Template*

1. Select a **Rollback** template from the **Patching Rollbacks** table of an open [Patching Rollbacks](#) template.



**Patching Rollbacks** Show All + New

Search Columns... × Q Search

<input type="checkbox"/> ...	Name	Patch	Actions
<input checked="" type="checkbox"/> ... >	Windows	.NET 3.5 Feature on Demand for X64	...
<input type="checkbox"/> ... >	Windows Rollback	.NET 3.5 Feature on Demand for X86	...
<input type="checkbox"/> ... >	Windows Update	2017-05 Security Monthly Quality Rollup for Windows Server 2012 for ..	...
<input type="checkbox"/> ...	Rows Per Page: <u>10</u> 1 - 3 of 3		1 / 1

This opens the template.

**Note**

A red asterisk next to a field name indicates a required field.

General Settings

Name \* Windows

Description

Patch ⓘ \* .NET 3.5 Feature on Demand for X64 201 BROWSE ×

Target Business Units ⓘ \* + Add Business Units

<input type="checkbox"/> ...	Name	Actions
<input type="checkbox"/> ... >	Operating System	...

2. Modify the Rollback settings:
  - a. Select **Browse** to choose a different patch or release to roll back.
  - b. Select **+Add Business Units** to add or remove target devices.
3. Select **Save** on the upper-left corner of the template to save the new settings.

*Copy a Rollback*

1. Select a **Rollback** template from the **Patching Rollbacks** table of an open [Patching Rollbacks](#) template.

Patching Rollbacks Show All + New

Search Columns... × Q Search

<input type="checkbox"/> ...	Name	Patch	Actions
<input checked="" type="checkbox"/> ...	> Windows	.NET 3.5 Feature on Demand for X64	...
<input type="checkbox"/> ...	> Windows Rollback	.NET 3.5 Feature on Demand for X86	...
<input type="checkbox"/> ...	> Windows Update	2017-05 Security Monthly Quality Rollup for Windows Server 2012 for ..	...
<input type="checkbox"/> ...	Rows Per Page: <u>10</u> 1 - 3 of 3		1 / 1

This opens the template.

### Note

A red asterisk next to a field name indicates a required field.

General Settings

Name \*

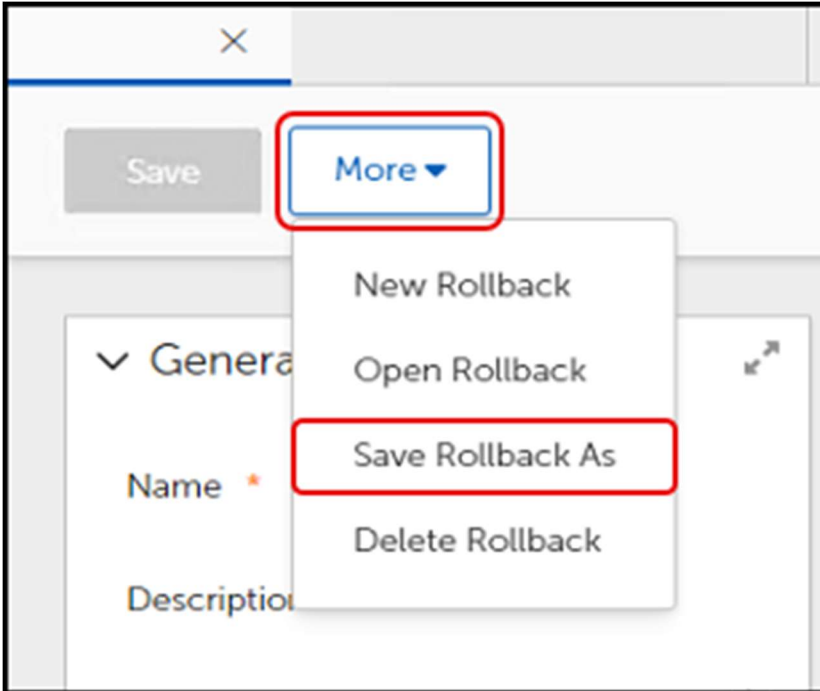
Description

Patch ⓘ \*  BROWSE ×

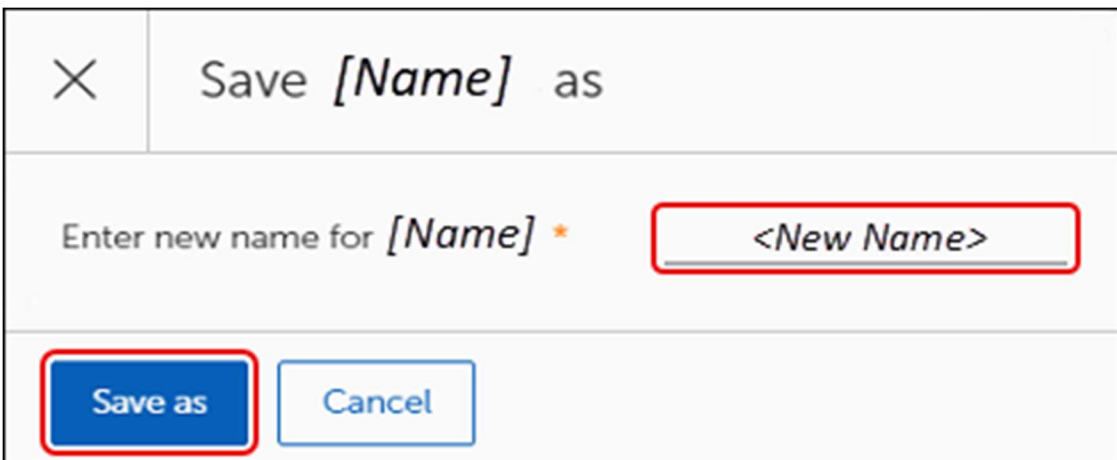
Target Business Units ⓘ \* + Add Business Units

<input type="checkbox"/> ...	Name	Actions
<input type="checkbox"/> ...	> Operating System	...

2. Select **More**, and then select **Save Rollback As**.



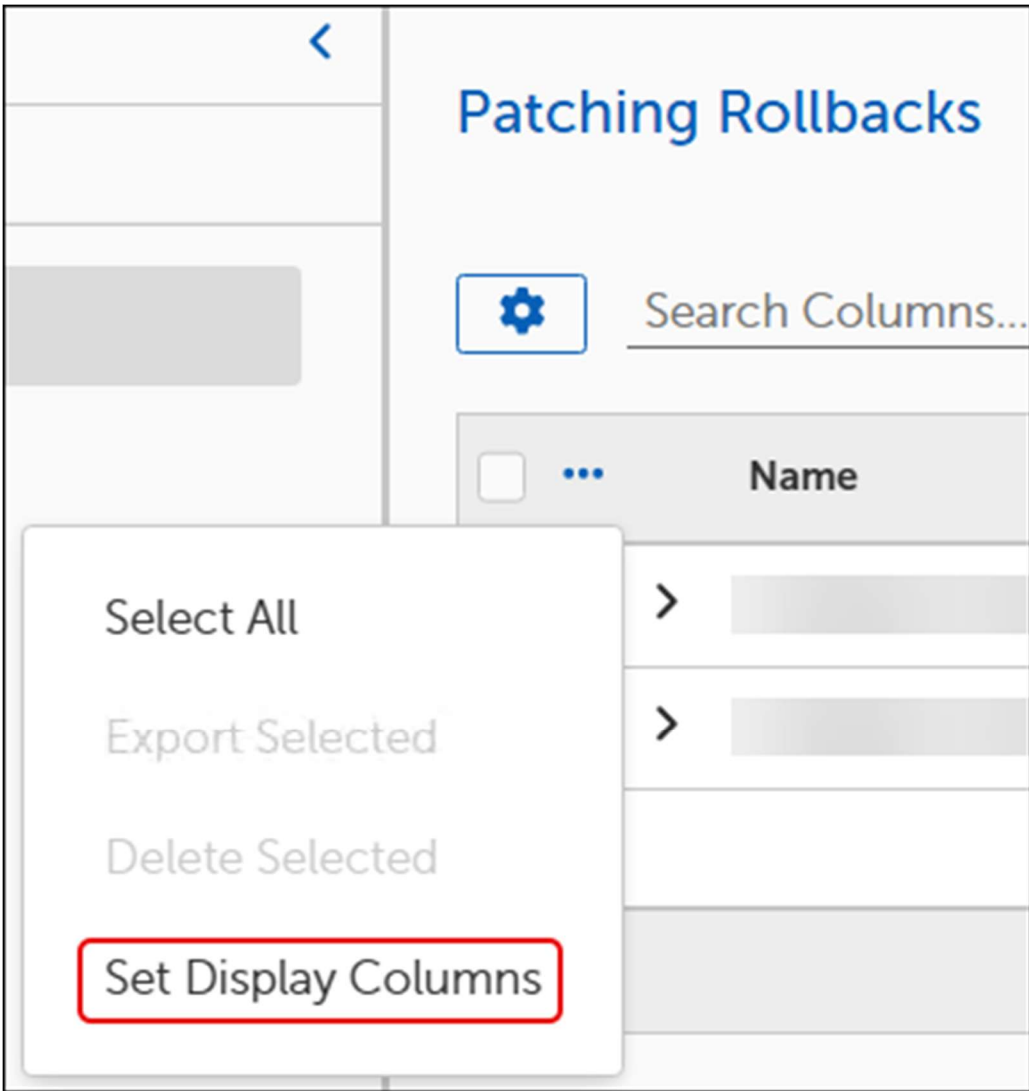
3. Enter a new **Name** for the template, and then click **Save as**.



4. Revise the **Description** to reflect any changes needed for the copy, and then click **Save**.
5. Select **Back to Rollbacks** on the upper-left corner of the template to return to the **Rollbacks** table and view your changes.

#### *Customize Patching Rollback Table Settings*

1. Open the **Patching Rollbacks** table (Flex Controls > Rollbacks > Rollback).
2. Select the **ellipsis (...)** next to Name in the **Patching Rollbacks** table, and then click **Set Display Columns**.



This opens the Set Table Columns dialog.

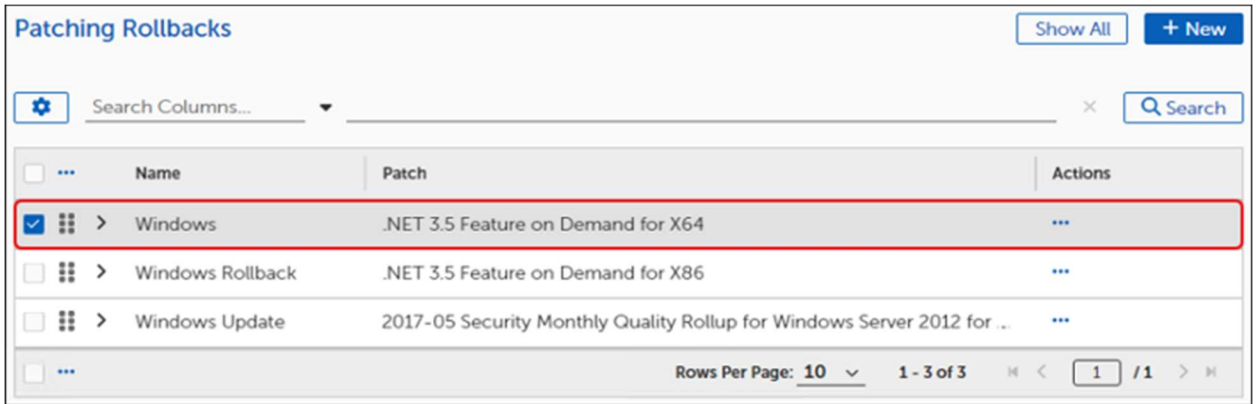
× Set Table Columns

- Select All
- Built In
- Created By
- Creation Time
- Description
- Enabled
- Last Modification Time
- Modified By
- Name
- Object ID
- Parent Folder ID
- Patch
- Read Only
- Version

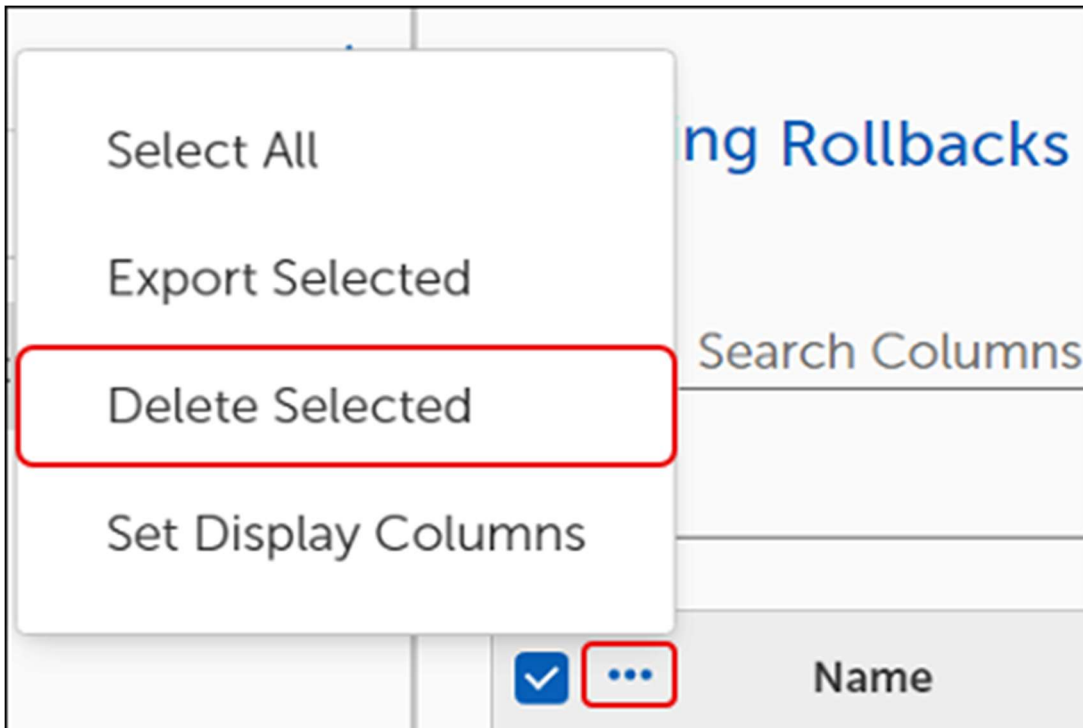
3. Select the **column names** you want the **Patching Rollbacks** table to display, and then click **OK**.

*Delete a Rollback*

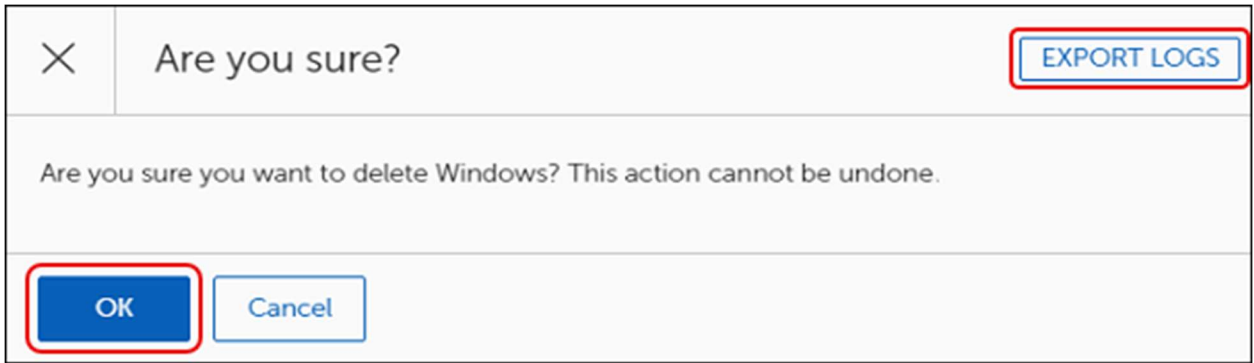
1. Select a **Rollback** template from the **Patching Rollbacks** table of an open [Patching Rollbacks](#) template.



2. Select the **Ellipsis (...)** next to **Name**, and then select **Delete Selected**.



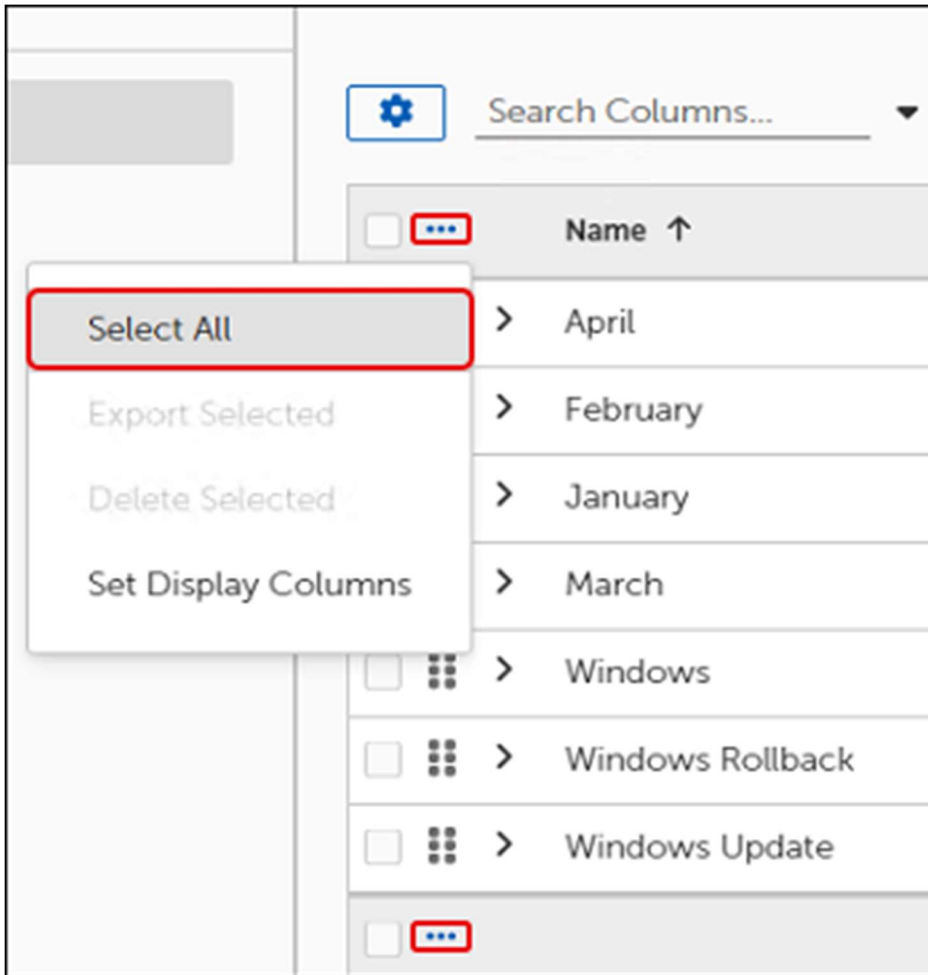
3. Review the Are you sure? dialog:



- a. Select **Export Logs** on the top-right corner of the **Are you sure?** dialog to export trace logs. The trace logs download to your device as a file with a **.log** extension.
  - b. Select **OK** to delete the Rollback.
4. Select **Back to Rollbacks** on the upper-left corner of the template to return to the **Rollbacks** table and view your changes.

*Select All Rollbacks*

1. Open the **Patching Rollbacks** table (Flex Controls > Rollbacks > Rollback).
2. Select the **ellipsis (...)** next to Name, and then click **Select All**.

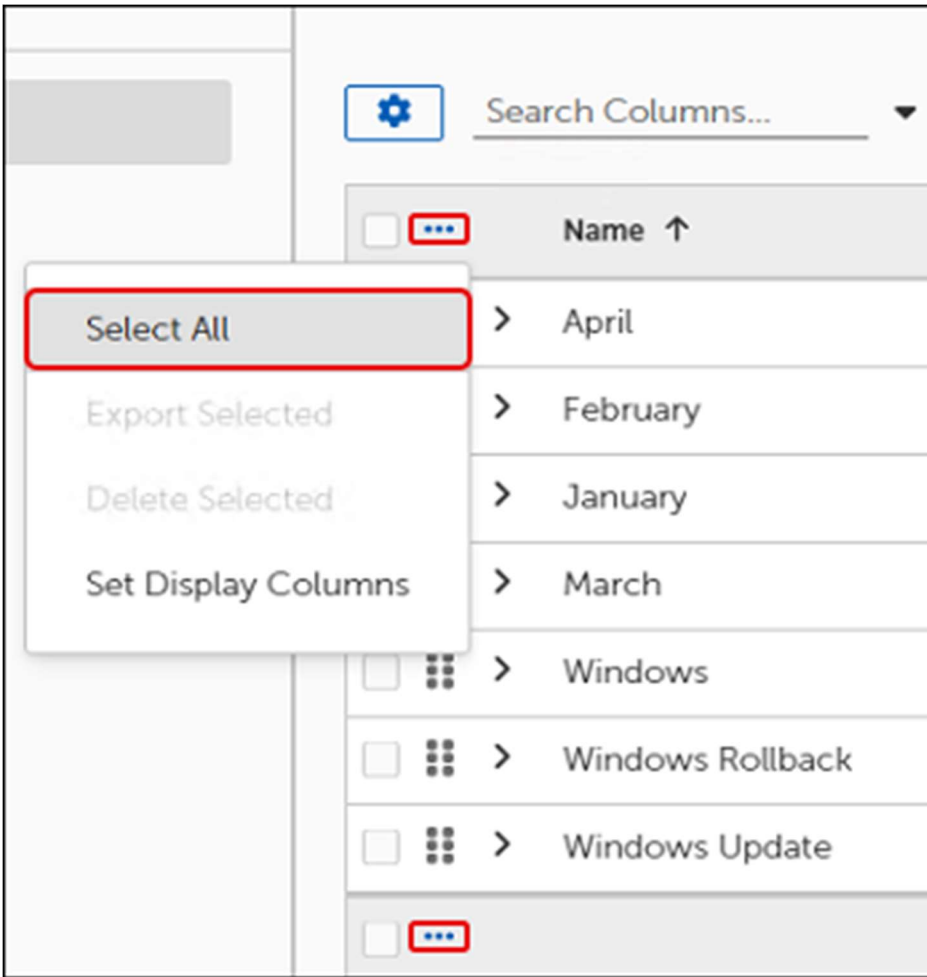


3. Select the ellipsis (...) again, and then choose what you want to do with the selected Rollbacks:
  - a. To export the selected Rollbacks, see [Select All Rollback to Version Objects](#).
  - b. To delete the Selected templates, see [Bulk Delete Rollbacks](#).
  - c. To customize the display columns of the Patching Rollbacks table, see [Customize Patching Rollback Table Settings](#).

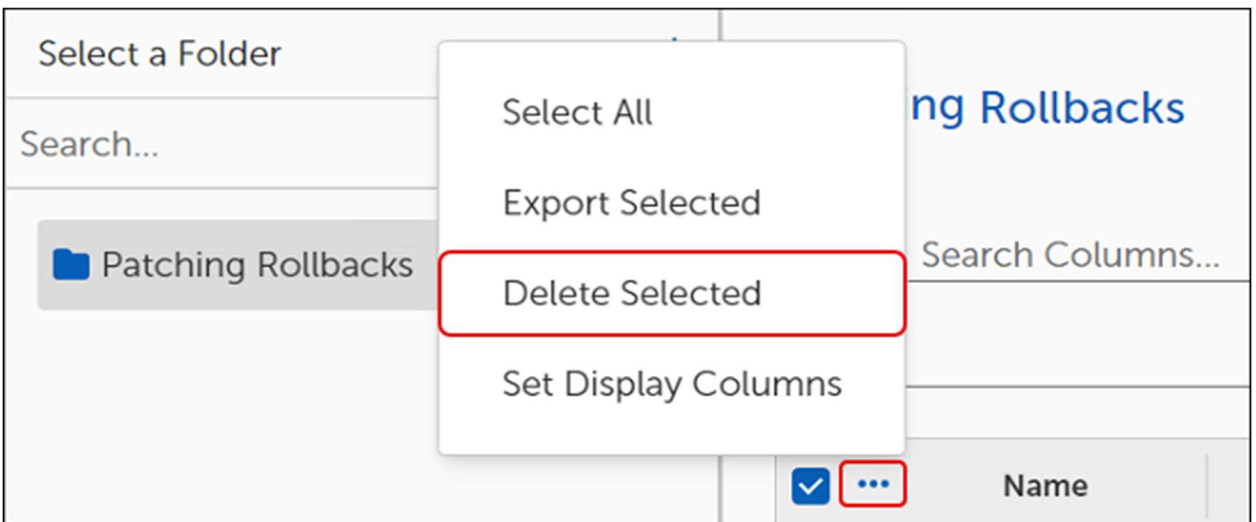
#### *Bulk Delete Rollbacks*

1. Open the **Patching Rollbacks** table (**Flex Controls > Rollbacks > Rollback**).
2. Select the **ellipsis (...)** next to Name, and then click **Select All**.

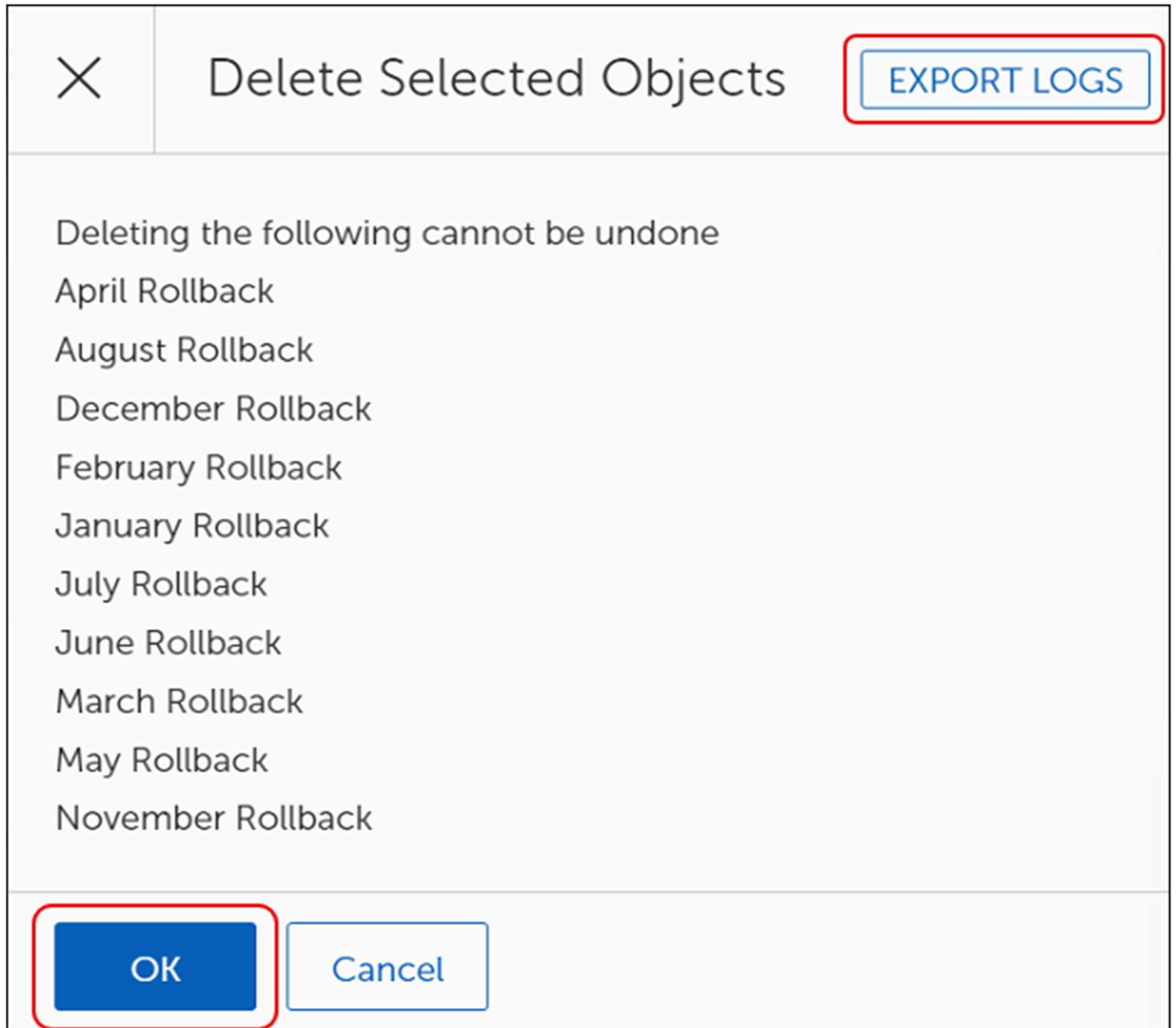




3. Select the **ellipsis (...)** next to **Name**, and then select **Delete Selected**.



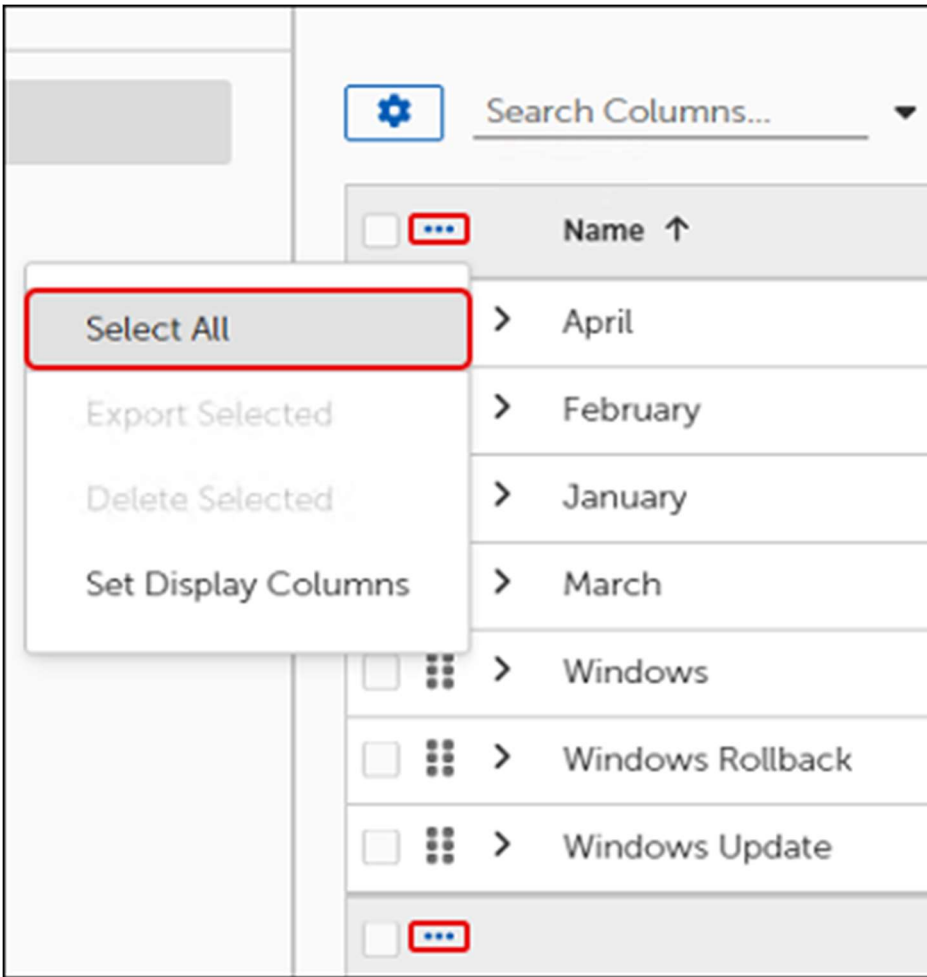
This opens the **Delete Selected Objects** dialog:



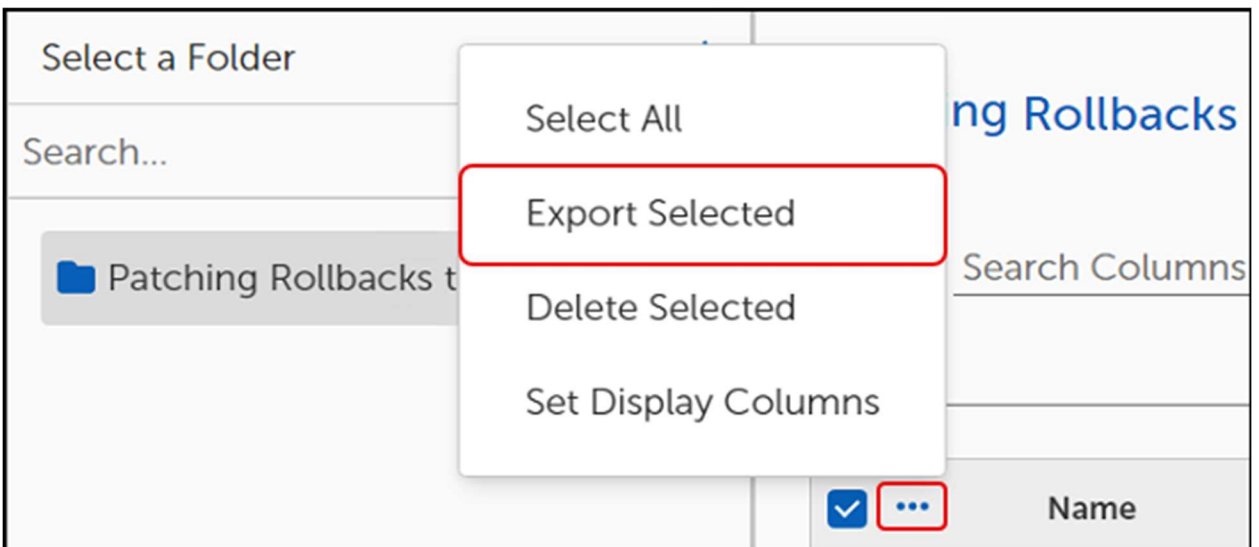
4. (Optional) Select **Export Logs** on the top-right corner of the **Delete Selected Objects** dialog to export trace logs. The trace logs download to your device as a file with a `.log` extension.
5. Select **OK** to delete the Rollbacks. This returns you to the **Patching Rollbacks to** table where the deleted Rollbacks no longer appear.

#### *Export Rollbacks*

1. Open the **Patching Rollbacks** table (Flex Controls > Rollbacks > Rollback).
2. Select a single **Patching Rollback** from the table, or click the **ellipsis (...)** next to Name, and then click **Select All** to export all Rollbacks



3. Select the **ellipsis (...)** next to Name again, and then click **Export Selected**.



This opens the **Object Export Settings**:

### Object Export Settings

Exporting Organization

Description

Export as JSON

Automatically Import Objects Into the Specified Folder

4. Continue to [Configure the Object Export Settings](#).

#### Configure Object Export Settings

1. Complete the steps in [Export Rollback](#) to open the **Object Export Settings** template.

▼ Object Export Settings ↕

Exporting Organization Exporting Organization Name

Description Description

Export as JSON

Automatically Import

Objects Into the Specified Folder

2. Enter an **Exporting Organization Name** and a **Description** of the settings you intend to create.
3. Toggle the **Export as JSON** switch to enable or disable (default) whether to export the settings as a JSON file.
4. Toggle the **Automatically Import ...** switch to enable or disable whether to select a specific folder to save the import.
5. Select **Export** on the bottom left corner of the Object Export Settings to export the selected objects.

**Important**

Tenable no longer supports the **Export to Linked Servers** functionality. Do not make any changes to the default settings.

*Show Rollback References*

To view the folder location of a Rollback to Version template, complete the following steps:

1. Open the **Patching Rollbacks** table (Flex Controls > Rollbacks > Rollback).
2. Select the **ellipses (...)** in the **Actions** column of the Patching Rollbacks table, and then select **Show References**.

Patching Rollbacks Show All + New

Search Columns... Search

<input type="checkbox"/>	Name	Patch	Actions
<input type="checkbox"/>	> April Rollback	.NET 3.5 F...	...
<input type="checkbox"/>	> August Rollback		Show References Export
<input type="checkbox"/>	> December Rollback		
<input type="checkbox"/>	> February Rollback	.NET 3.5 F...	...

This opens the **[Rollback Name] Object References** dialog.

✕ December Rollback Object References

- Root
  - Folder
    - Patching Rollbacks

OK

3. Select the **caret** next to a **Folder** icon to expand the folder and view the contents, if needed.
4. Select **OK** to return to the **Patching Rollbacks** table.

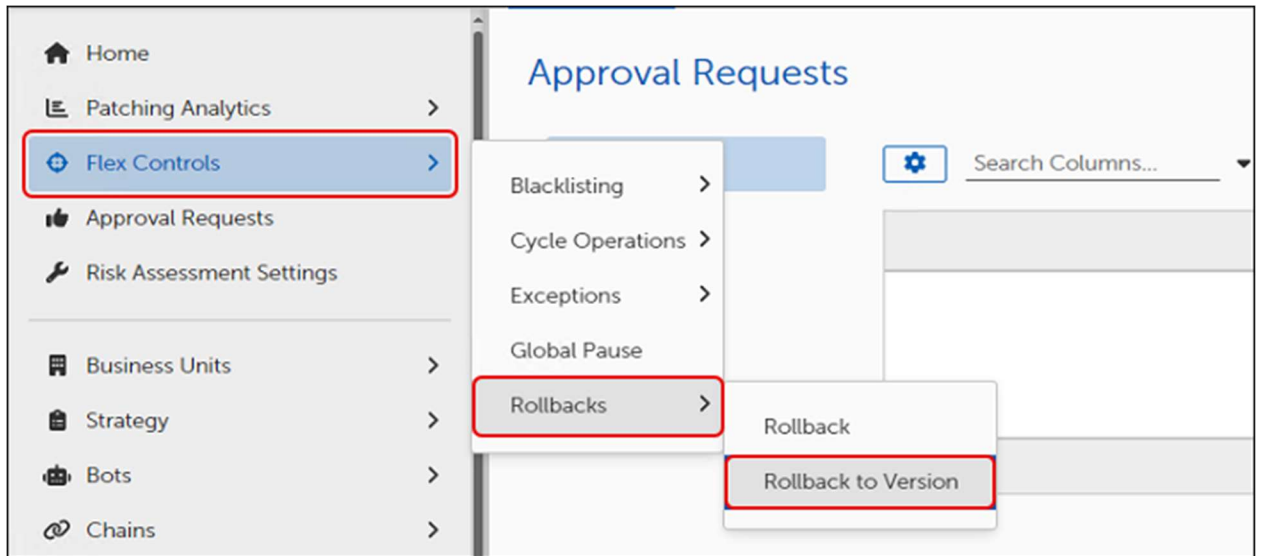
# Rollback to Version

Use the Rollback to Version template to rollback a patch or release to a specific release or version. To rollback to the previous version, see [Rollback](#).

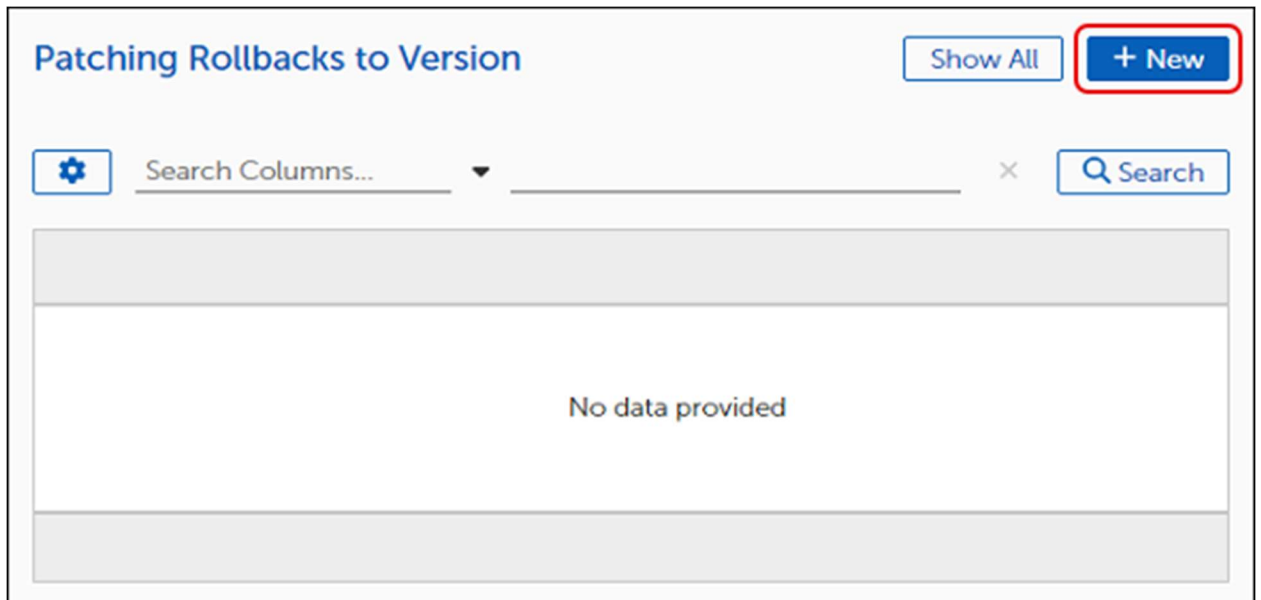
## Create a Rollback to Version

To rollback a patch to a previous patch or release version, complete the following steps:

1. Select **Flex Controls** on the left navigation menu of the [Tenable Patch Management Dashboard](#), and then select **Rollbacks > Rollback to Version**.



This opens the **Patching Rollbacks to Version** table. Until you create a rollback, the table is empty..



2. Select **+New** to open the Rollback template, and then enter a **Name** and a detailed **Description** of the rollback.

**Note**

A red asterisk next to a field name indicates a required field.

General Settings

Name \*

Description

Patch ⓘ \*  **BROWSE**

Rollback ⓘ \*  **BROWSE**

Target Business Units ⓘ \*

3. Enter a **Name** and a detailed **Description** of your Rollback to Version.
4. [Add the patch or release to roll back from.](#)

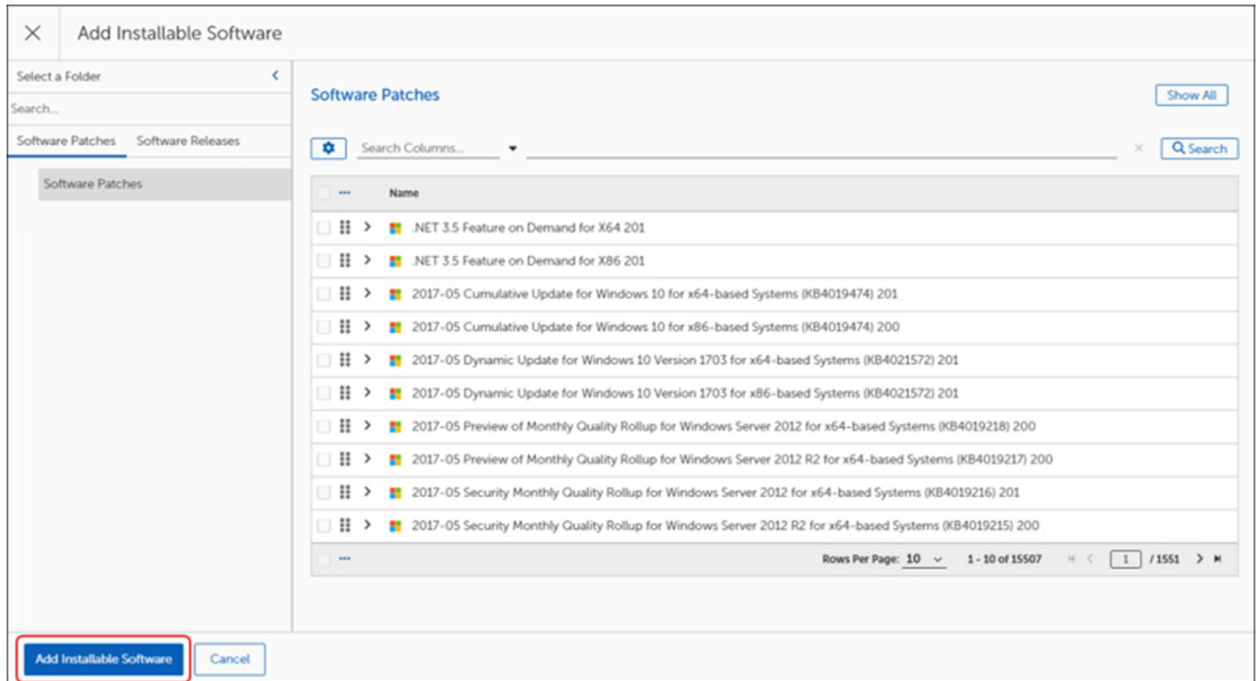
Choose the Software Patch or Release Version to Roll Back From

1. Select **Browse** next to **Add Installable Software** in an open [Rollback to Version](#) template.

Patch ⓘ \*  **BROWSE**

2. Choose the **Software Patch** or **Software Release** from the **Add Installable Software** table to roll back from. You can select only one Patch or Release to roll back from.

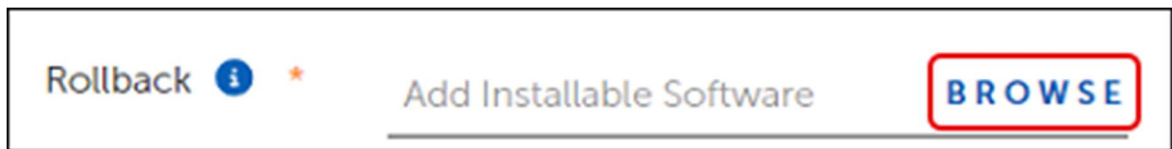




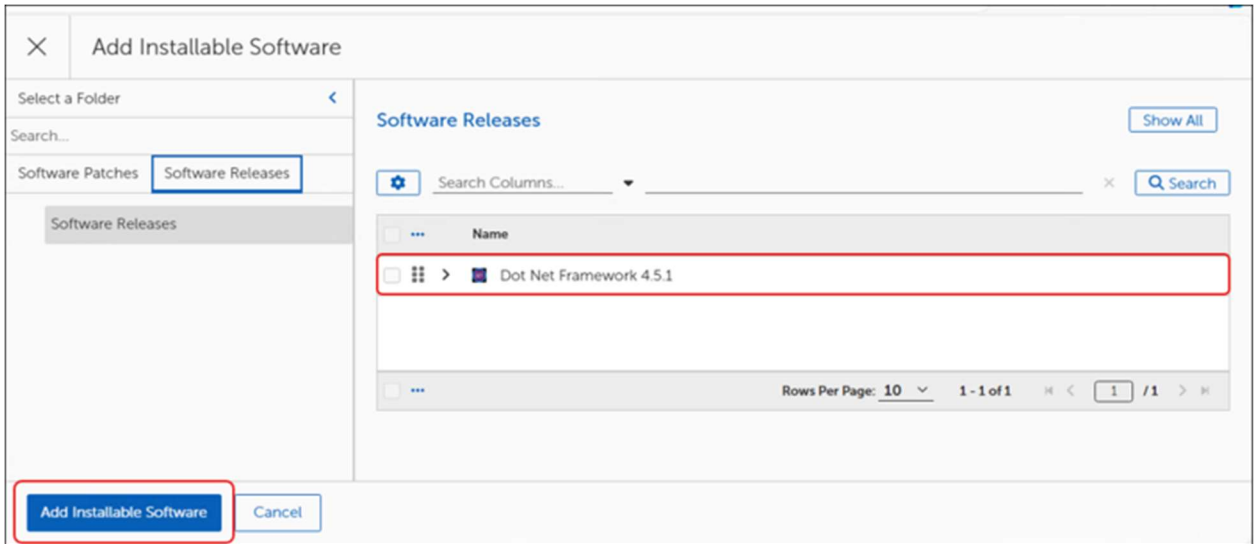
3. Select **Add Installable Software** to return to the Rollback to Version template.
4. Choose the software patch or release version to roll back to.

Choose the Software Patch or Release Version to Roll Back To

1. Select **Browse** next to **Rollback** in an open [Rollback to Version](#) template.



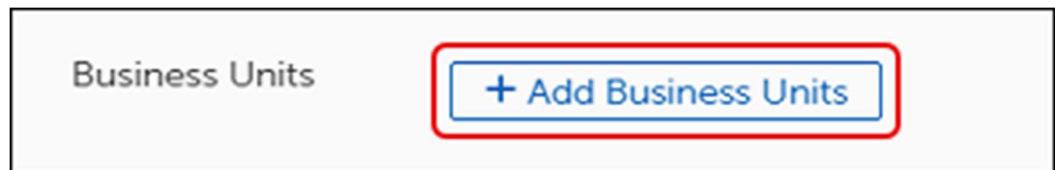
2. Select a **Patch** or **Release** version from the **Add Installable Software** table to roll back to. The only visible versions are those that match the item you selected for Patch. You can select only one Patch or Release to roll back to.



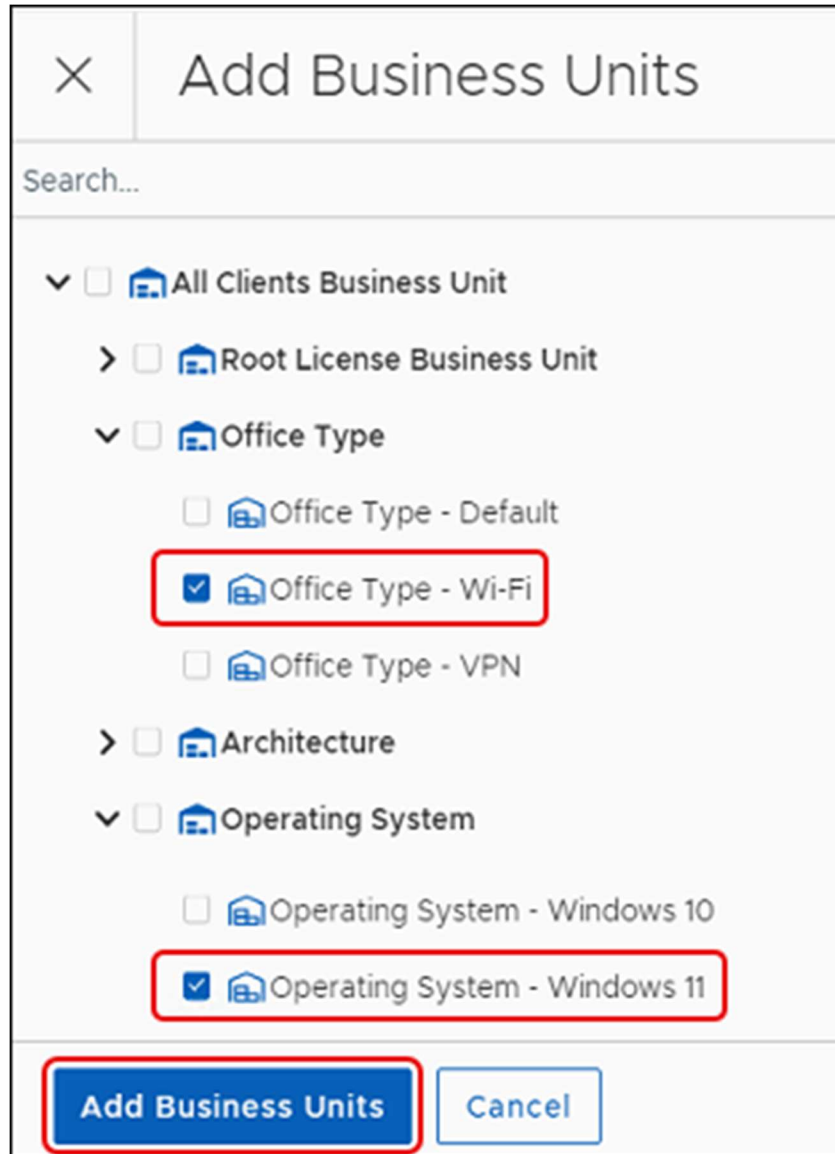
3. Select **Add Installable Software**.
4. Add target Business Units for the Rollback to Version.

Add Business Units for a Rollback to Version

1. Add one or more **Business Units** using the following steps:
  - a. Select **+ Add Business Units** in the open workspace or dialog.



This opens the **Add Business Units** workspace. The following example shows possible choices.



- b. Select one or more **Business Units** to add, and then click **Add Business Units**.
2. Select **Save** to rollback a patch to a prior version.

#### *Edit a Rollback to Version Template*

1. Select a **Rollback to Version** template from the **Patching Rollbacks to Version** table of an open [Patching Rollbacks](#) template.

Patching Rollbacks to Version Show All [+ New](#)

Search Columns... Search

<input type="checkbox"/>	Name	Patch	Actions
<input checked="" type="checkbox"/>	> Windows	.NET 3.5 Feature on Demand for X64	...
<input type="checkbox"/>	> Windows Rollback	.NET 3.5 Feature on Demand for X86	...
<input type="checkbox"/>	> Windows Update	2017-05 Security Monthly Quality Rollup for Windows Server 2012 for ..	...

Rows Per Page: 10 1 - 3 of 3 1 / 1

This opens the template.

General Settings

Name \*

Description

Patch i \*  BROWSE

Rollback i \*  BROWSE

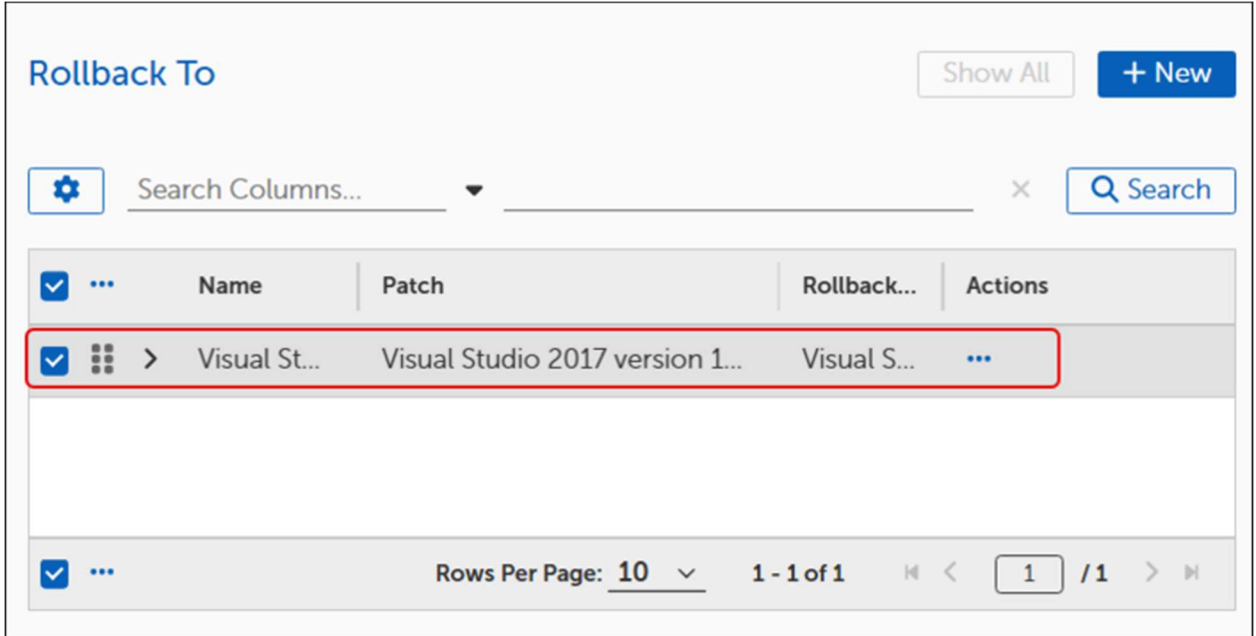
Target Business Units i \*

2. Modify the Rollback settings:
  - a. Select **Browse** for Patch to choose a patch or release to roll back from.
  - b. Select **Browse** for Rollback to choose the version of the patch or release to roll back to.
  - c. Select **+Add Business Units** to add or remove target devices.

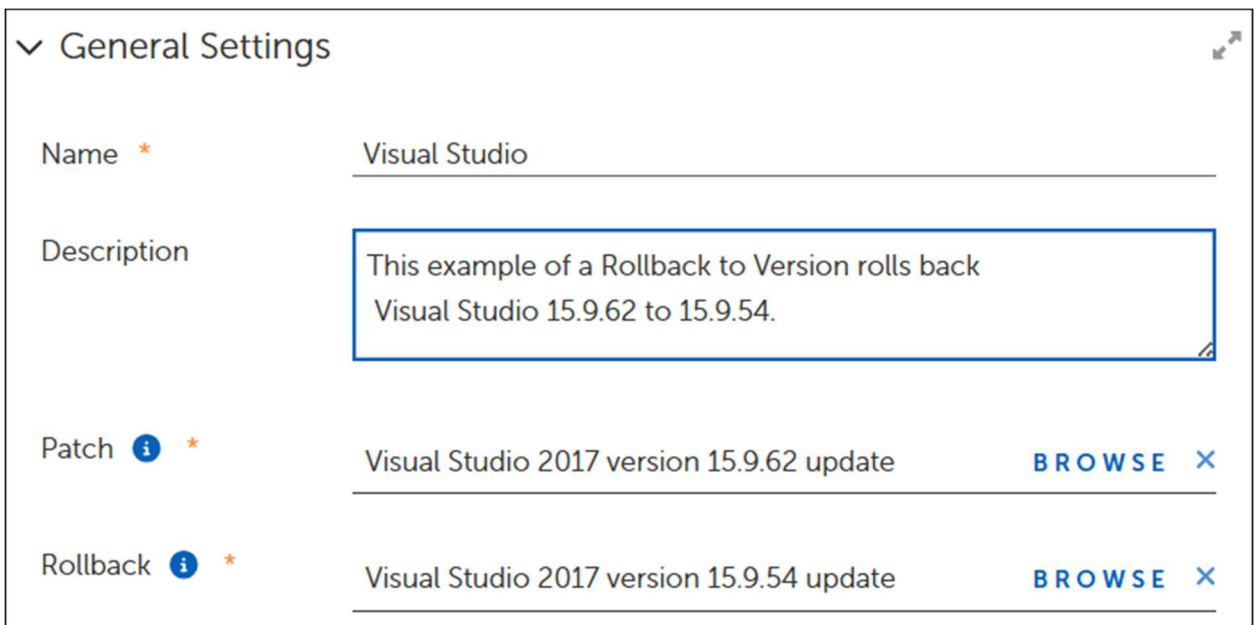
3. Select **Save** top-left corner of template to save the changes.

*Copy a Rollback to Version Template*

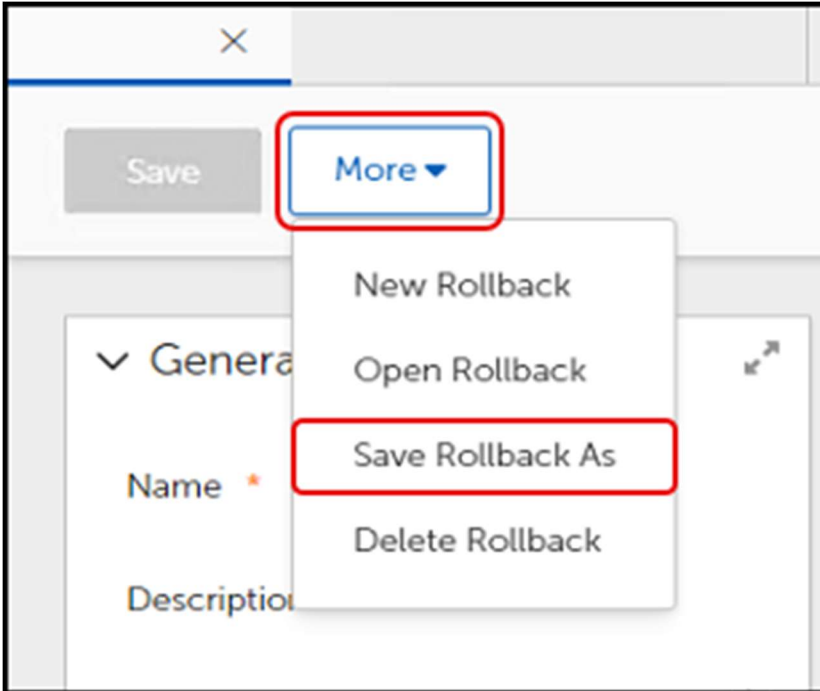
1. Select a **Rollback** template from the **Patching Rollbacks to Version** table of an open [Patching Rollbacks](#) template.



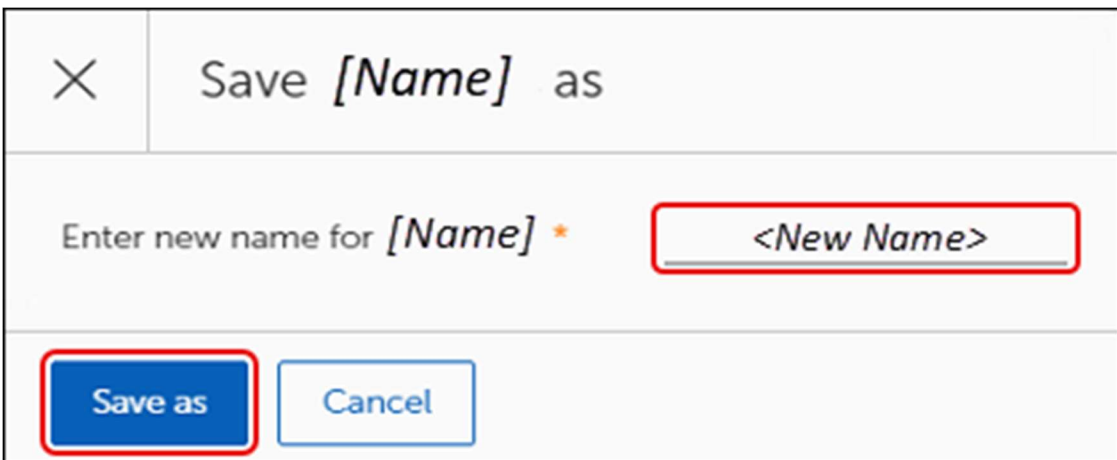
This opens the template.



2. Select **More**, and then select **Save Rollback As**.



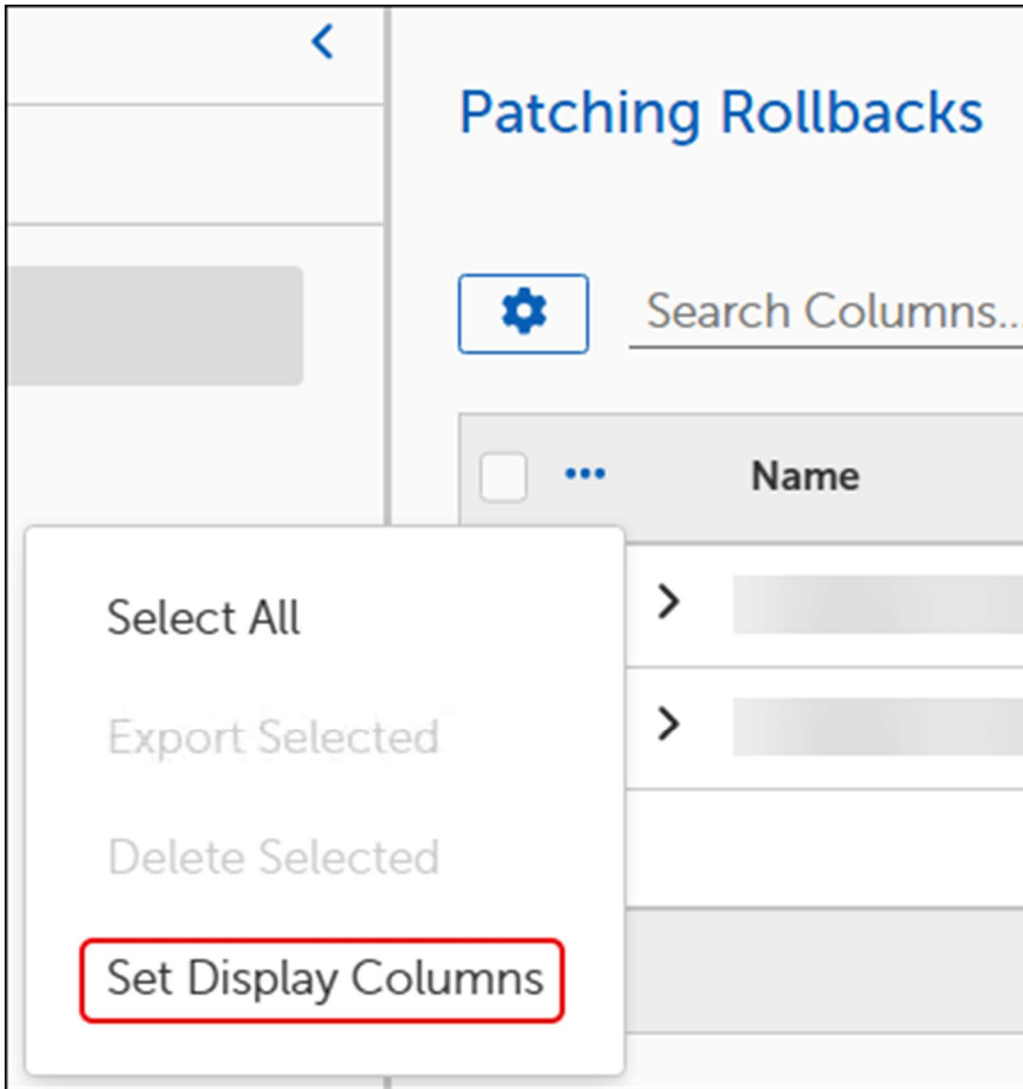
3. Enter a new **Name** for the template, and then click **Save as**.



4. Revise the **Description** to reflect any changes needed for the copy, and then click **Save**.
5. Select **Back to Rollbacks** on the upper-left corner of the template to return to the **Rollbacks** table and view your changes.

#### Customize Patching Rollback Table Settings

1. Open the **Patching Rollbacks** table (Flex Controls > Rollbacks > Rollback).
2. Select the **ellipsis (...)** next to Name in the **Patching Rollbacks** table, and then click **Set Display Columns**.



This opens the Set Table Columns dialog.

✕ Set Table Columns

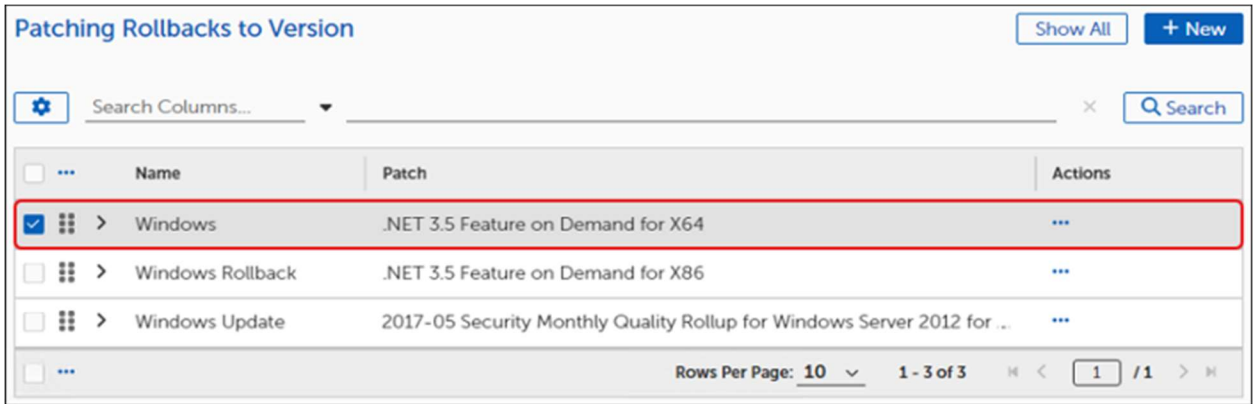
- Select All
- Built In
- Created By
- Creation Time
- Description
- Enabled
- Last Modification Time
- Modified By
- Name
- Object ID
- Parent Folder ID
- Patch
- Read Only
- Version



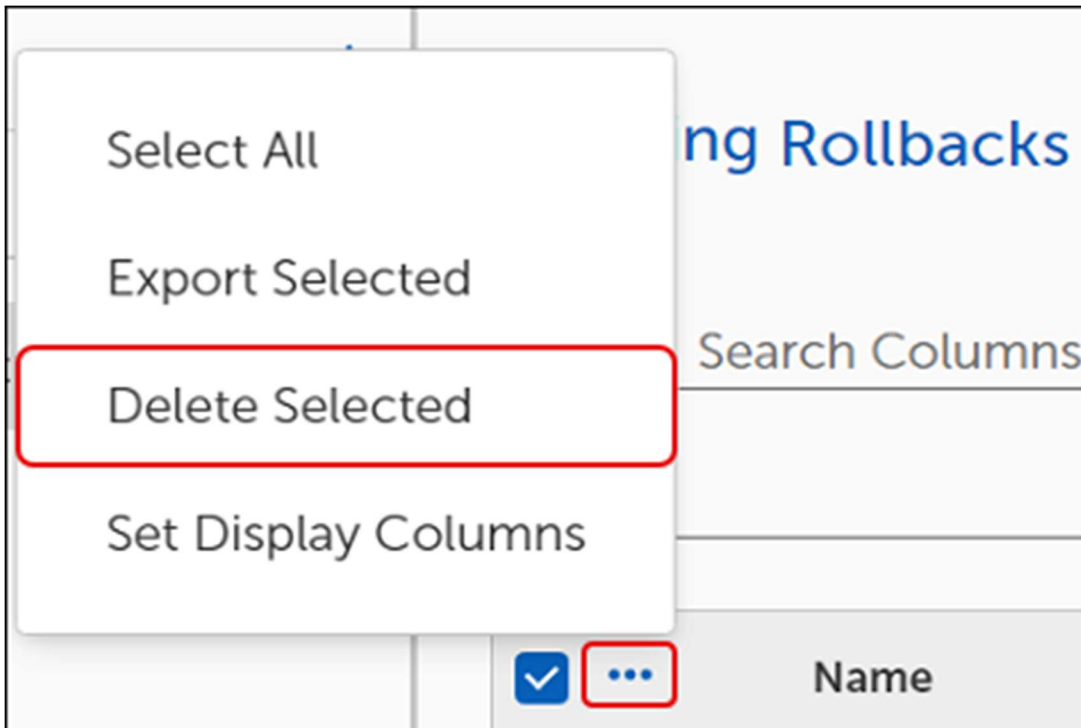
3. Select the **column names** you want the **Patching Rollbacks** table to display, and then click **OK**.

*Delete a Rollback to Version*

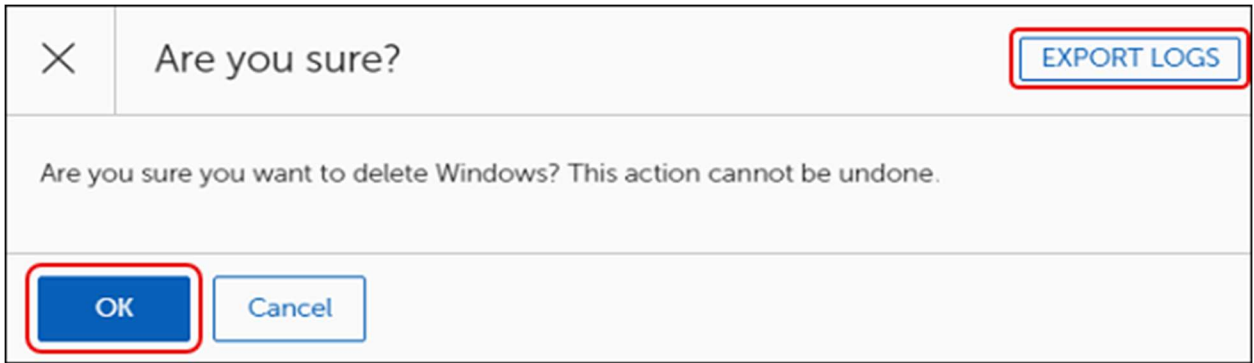
1. Select a **Rollback to Version** template from the **Patching Rollbacks to Version** table of an open [Patching Rollbacks](#) template.



2. Select the **Ellipsis (...)** next to **Name**, and then select **Delete Selected**.



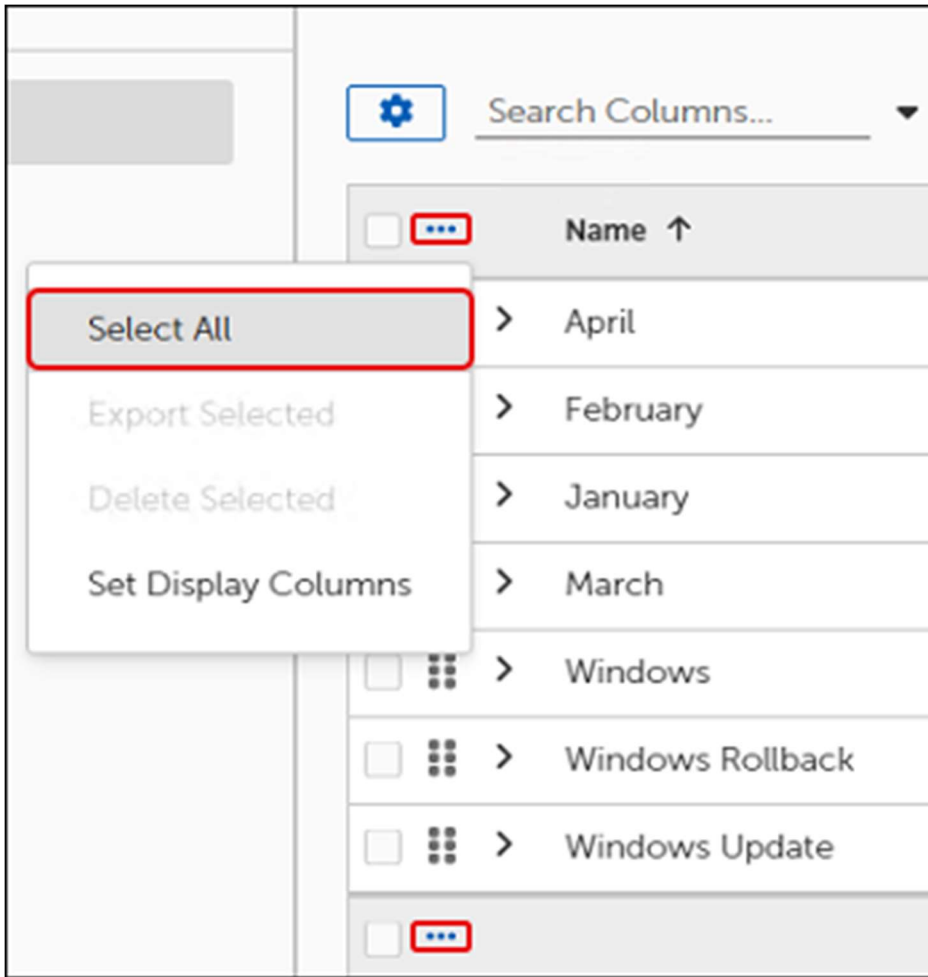
3. Review the Are you sure? dialog:



- a. Select **Export Logs** on the top-right corner of the **Are you sure?** dialog to export trace logs. The trace logs download to your device as a file with a `.log` extension.
  - b. Select **OK** to delete the Rollback.
4. Select **Back to Rollbacks** on the upper-left corner of the template to return to the **Rollbacks** table and view your changes.

*Select All Rollback to Version Objects*

1. Open the **Patching Rollbacks** table (Flex Controls > Rollbacks > Rollback to Version).
2. Select the **ellipsis (...)** next to Name, and then click **Select All**.

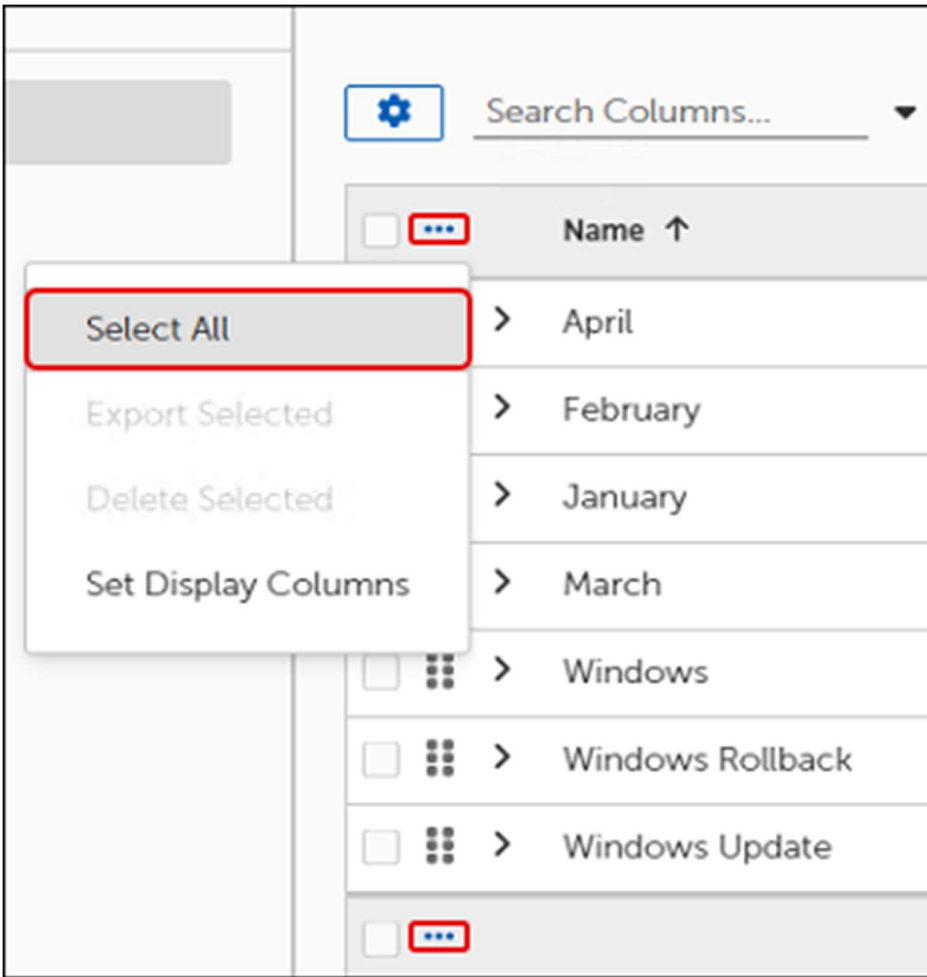


3. Select the ellipsis (...) again, and then choose what you want to do with the selected Rollbacks:
  - a. To export the selected Rollbacks, see [Select All Rollback to Version Objects](#).
  - b. To delete the Selected templates, see [Bulk Delete Rollbacks](#).
  - c. To customize the display columns of the Patching Rollbacks table, see [Customize Patching Rollback Table Settings](#).

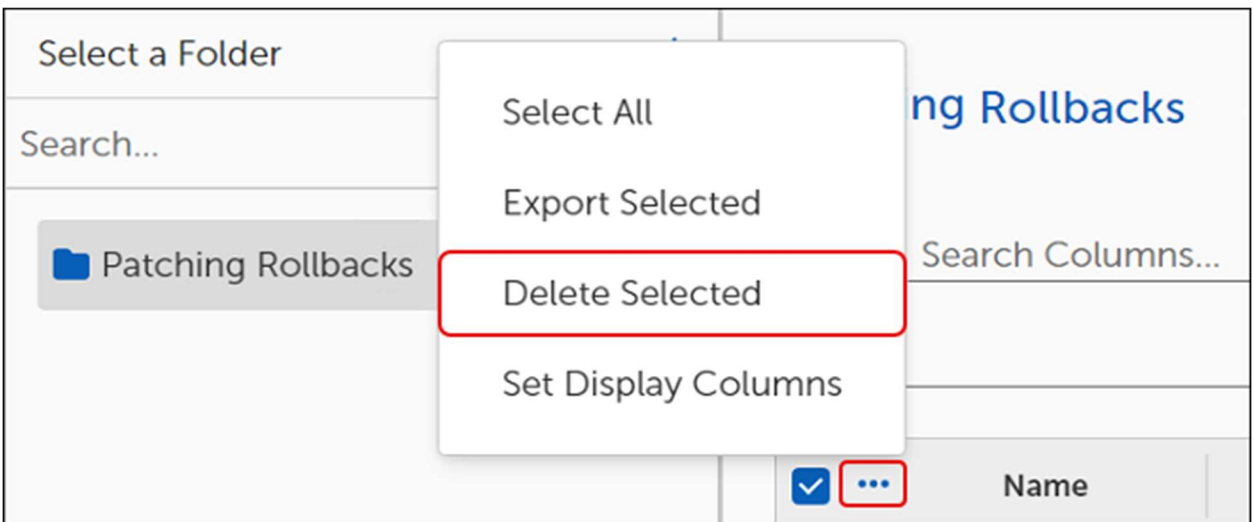
#### *Bulk Delete Rollback to Version*

Use the following task to delete all Rollback to Version templates.

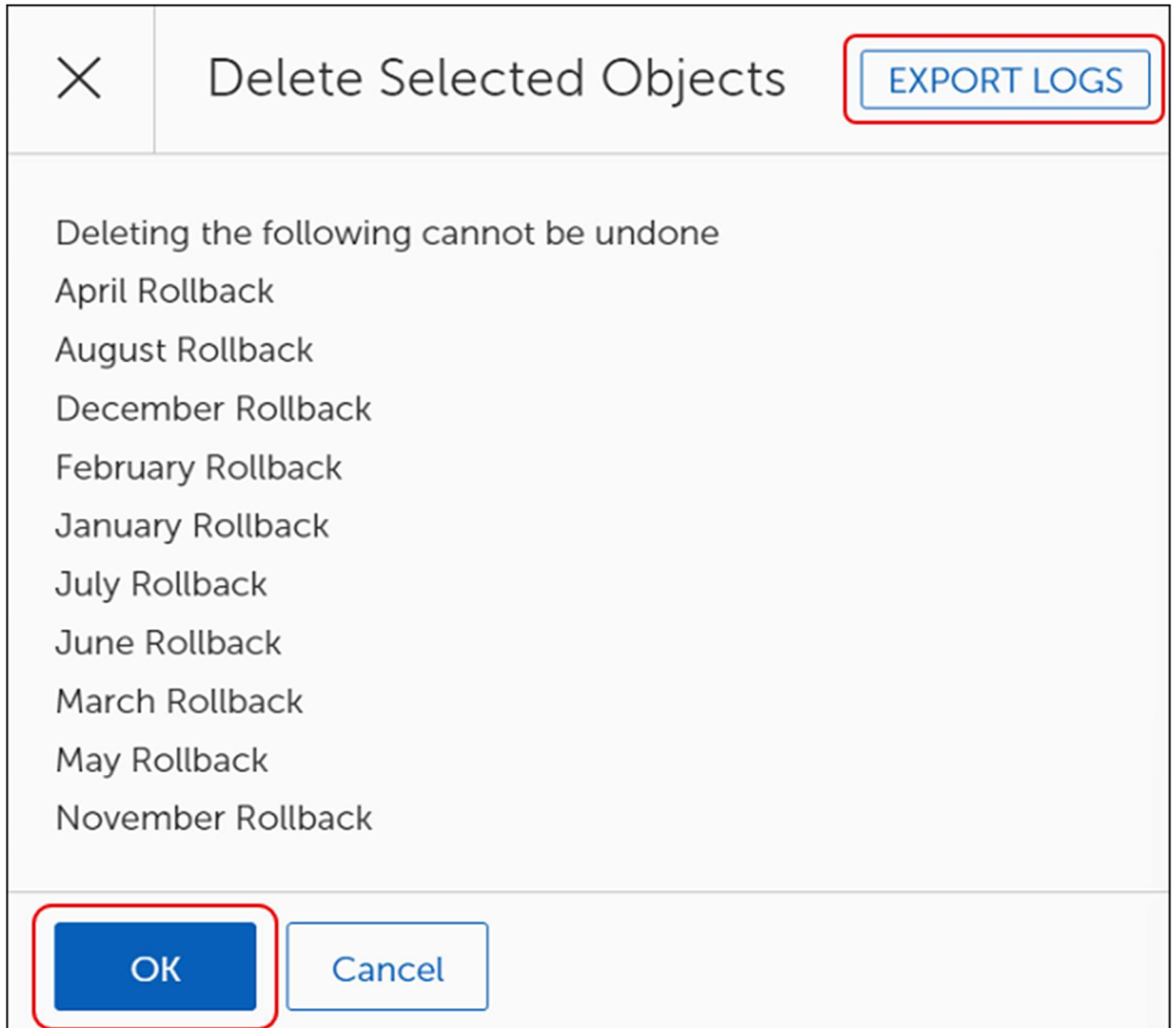
1. Open the **Patching Rollbacks** table (**Flex Controls > Rollbacks > Rollback to Version**).
2. Select the **ellipsis (...)** next to Name, and then click **Select All**.



3. Select the **ellipsis (...)** next to **Name**, and then select **Delete Selected**.



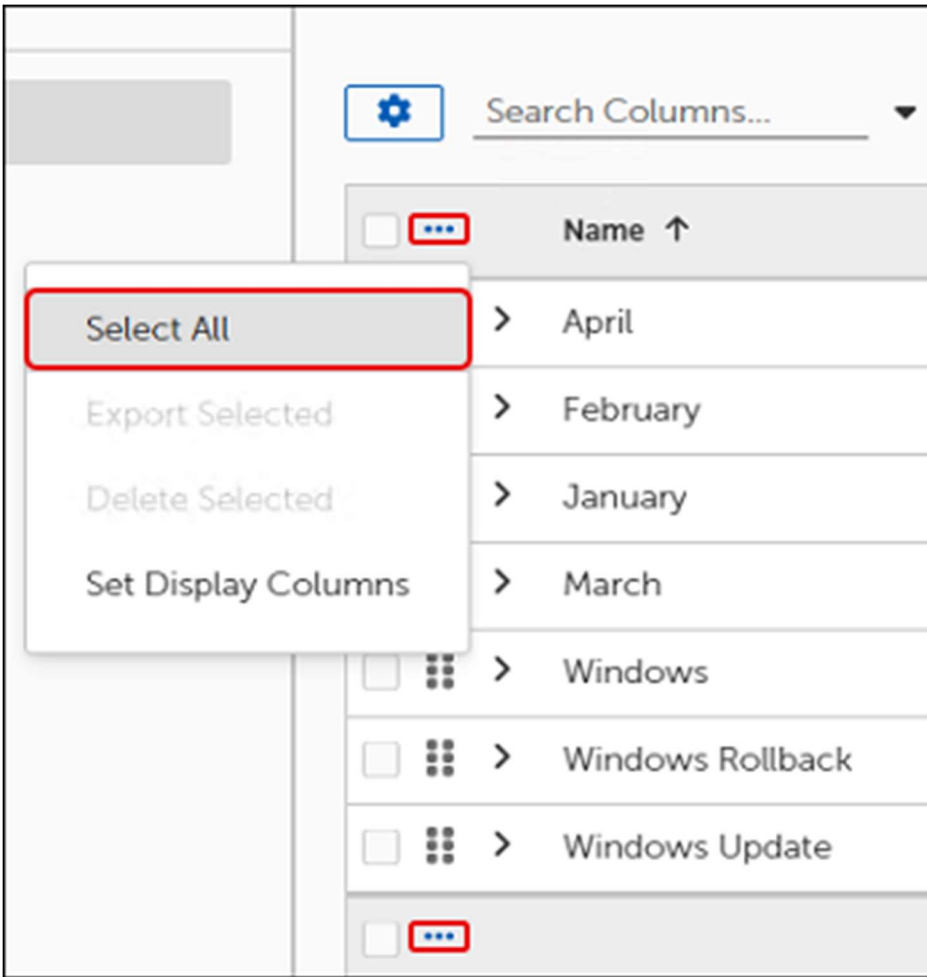
This opens the **Delete Selected Objects** dialog:



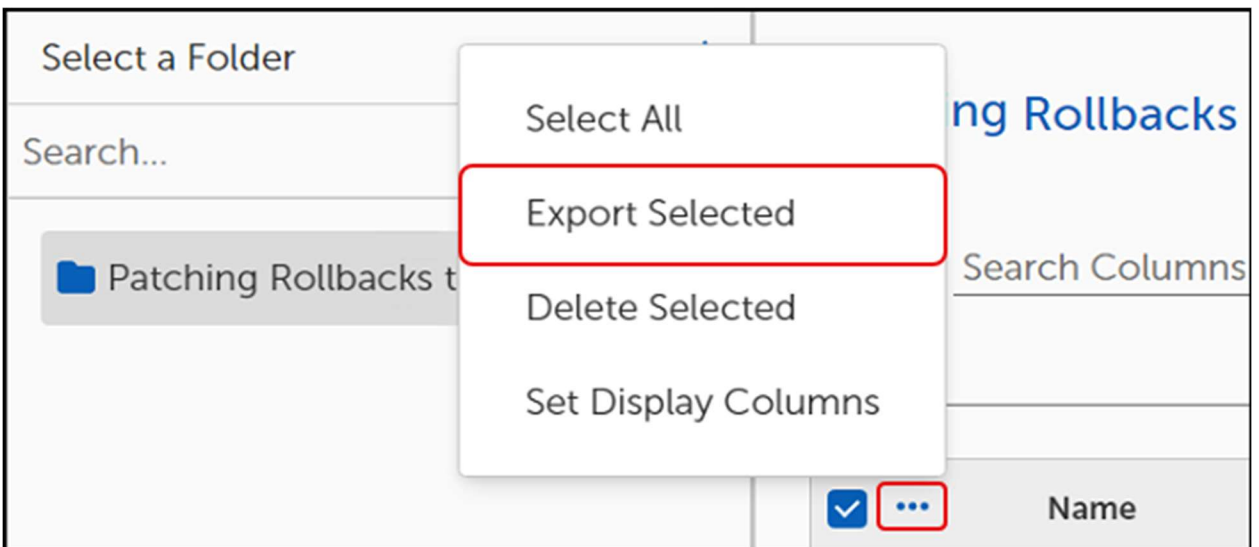
4. (Optional) Select **Export Logs** on the top-right corner of the **Delete Selected Objects** dialog to export trace logs. The trace logs download to your device as a file with a `.log` extension.
5. Select **OK** to delete the Rollbacks. This returns you to the **Patching Rollbacks to Version** table where the deleted Rollbacks no longer appear.

*Export Rollback to Version*

1. Open the **Patching Rollbacks** table (Flex Controls > Rollbacks > Rollback to Version).
2. Select a single **Patching Rollback** from the table, or click the **ellipsis (...)** next to Name, and then click **Select All** to export all Rollbacks



3. Select the **ellipsis (...)** next to Name again, and then click **Export Selected**.



This opens the **Object Export Settings**:

## Object Export Settings

Exporting Organization

Description

Export as JSON

Automatically Import

Objects Into the Specified Folder

Exporting Organization Name

---

Description

If Object Export Settings command returns an error similar to the following, see </document/preview/14345#UUID-8dd1ad08-6239-39ed-d91e-18e39741627c> errors:

Errors (1)

Search Columns... Search

	Name	Type	Error Description	Actions
<input type="checkbox"/>	Office Type	BusinessUnit	Children to export must be specified for Business unit	<a href="#">Resolve</a>
<input type="checkbox"/>	...			

Rows Per Page: 10 | 1 - 1 of 1 | 1 / 1

4. Continue to [Configure the Object Export Settings](#).

### Configure Object Export Settings

1. Complete the steps in [Export Rollback to Version](#) to open the **Object Export Settings** template.

▼ Object Export Settings ↕

Exporting Organization Exporting Organization Name

---

Description Description

Export as JSON

Automatically Import

Objects Into the Specified Folder

2. Enter an **Exporting Organization Name** and a **Description** of the settings you intend to create.
3. Toggle the **Export as JSON** switch to enable or disable (default) whether to export the settings as a JSON file.
4. Toggle the **Automatically Import ...** switch to enable or disable whether to select a specific folder to save the import.
5. Select **Export** on the bottom left corner of the Object Export Settings to export the selected objects.

**Important**

Tenable no longer supports the **Export to Linked Servers** functionality. Do not make any changes to the default settings.

*Show Rollback to Version References*

To view the folder location of a Rollback to Version template, complete the following steps:

1. Open the **Patching Rollbacks** table (Flex Controls > Rollbacks > Rollback to Version).
2. Select the **ellipses (...)** in the **Actions** column in the Patching Rollbacks to Version table, and then select **Show References**.



Patching Rollbacks to Version Show All + New

⚙️ Search Columns... × 🔍 Search

<input type="checkbox"/>	...	Name	Patch	Actions
<input type="checkbox"/>	⋮	> April Rollback	.NET 3.5 F...	⋮
<input type="checkbox"/>	⋮	> August Rollback		⋮
<input type="checkbox"/>	⋮	> December Rollback		⋮
<input type="checkbox"/>	⋮	> February Rollback	.NET 3.5 F...	⋮

Context menu for December Rollback:

- Show References
- Export

This opens the **[Rollback Name] Object References** dialog.

✕ December Rollback Object References

√ Root

√ Folder

    Folder Patching Rollbacks

OK

3. Select the **caret** next to the **Folder** icon to expand the folder and view the contents, if needed.
4. Select **OK** to return to the **Patching Rollbacks to Version** table.

# Approval Requests

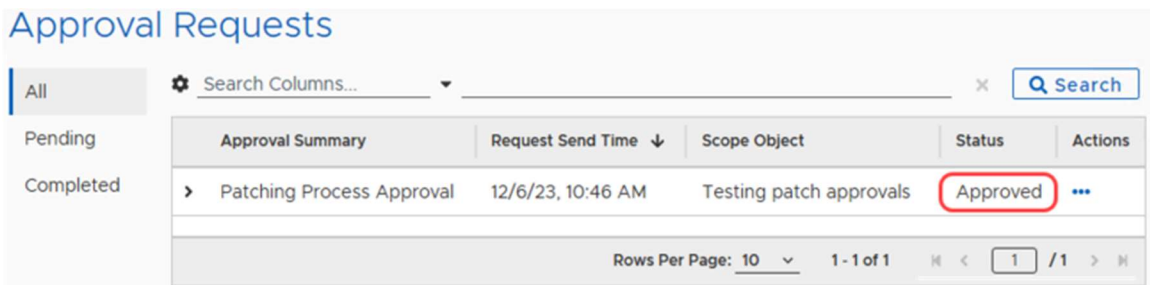
Some Patching Strategies require patch manager approval before beginning a patch cycle. The Patching Process looks for an Approval Chain to use when processing approvals and sends notification based on the communication process configured for each approver.

These approval communications include a link that takes the approver to the OneSite Admin Portal, which prompts the approver for authentication.

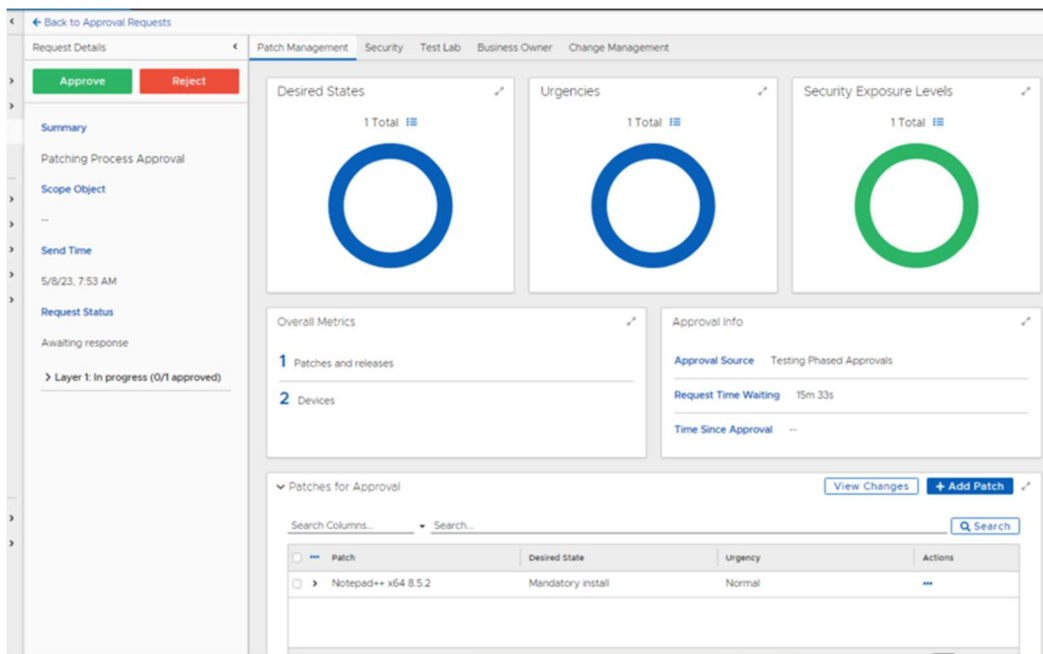
Administrators may see all pending and completed Approvals using the Tenable Patch Management dashboard.

## Approve or Reject a Patch Request

1. Select the **Status** of an item to view details of a request.



2. Select the **Patch** name to open the Patch and approval details, to review the details of the approval request, and then click **OK** at the bottom left of the dialog.



3. Select **Approve** or **Reject**:

- a. Select **Approve** to allow the Patching Process to continue processing the patches.
  - b. Select **Reject** to stop the Patching Process and update the status for the administrator.
4. Select **Back to Approval Requests** at the top of the screen to return to the **Approval Requests** dashboard.

# Auto Remediation

When enabled, the Auto Remediation configuration identifies the security exposure level of a threat, ascertains the scope of the issue, and then finds and installs the patches that resolve the exposure, all without user intervention. Investigation, diagnosis, and resolution occur automatically, sending notification of all activities to the PatchExpress.log file.

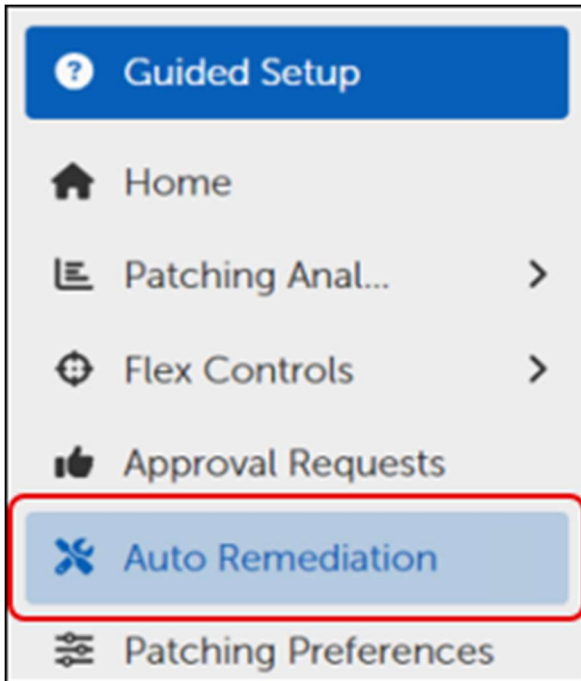
Tenable Patch Management includes the following configuration options for Auto Remediation:



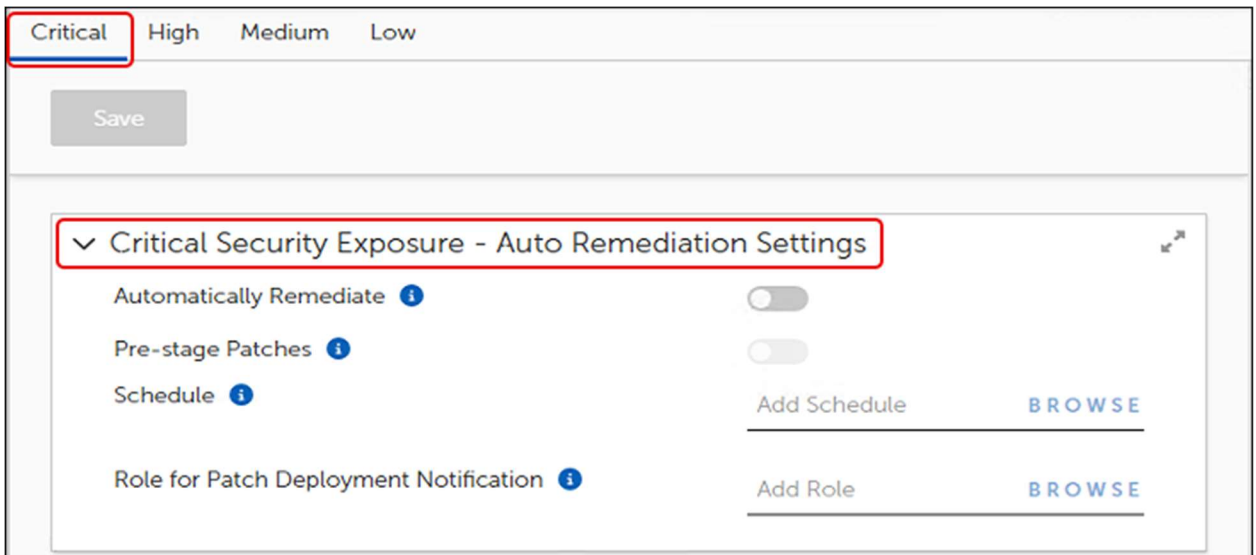
Tenable provides configuration options for Critical, High, Medium, or Low Security Exposure Levels.

## Access Auto Remediation and Deployment Settings

1. Select **Auto Remediation** on the left navigation menu of the [Tenable Patch Management Dashboard](#).



This opens the **Auto Remediation** workspace, which defaults to the Critical exposure level settings.

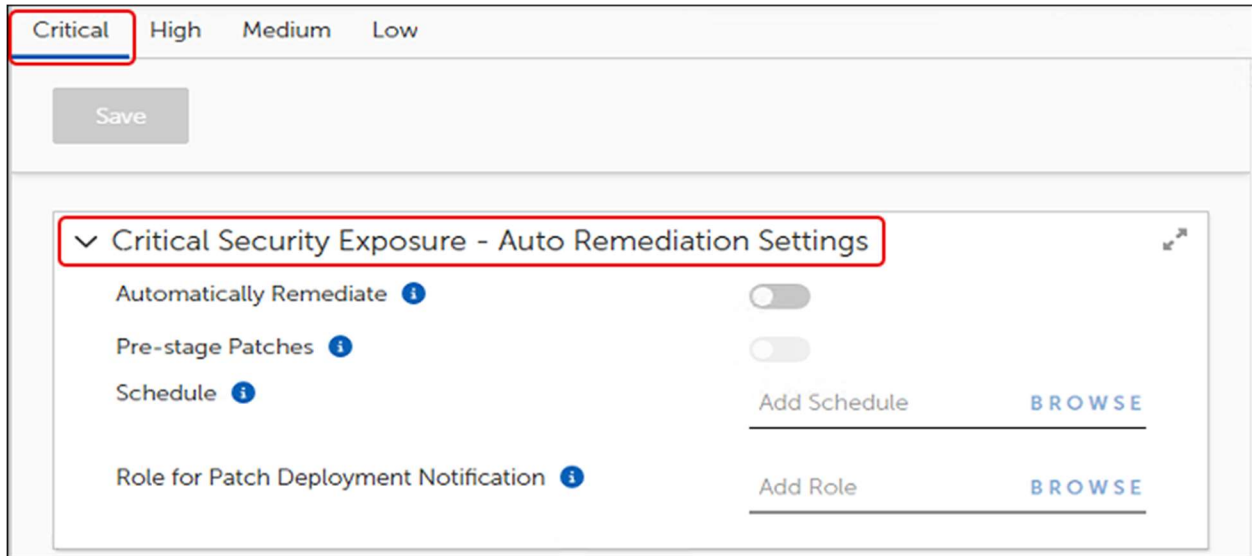


2. Select the tab at the top left – **Critical, High, Medium,** or **Low** – that corresponds to the exposure level setting you want to configure.

## Using Auto Remediation Settings

Enable automatic remediation to automatically correct all issues associated with a security level. With Auto Remediation enabled, you can also enable pre-staging of patches, which downloads the content to devices as soon as the patch becomes available. This makes the patch content

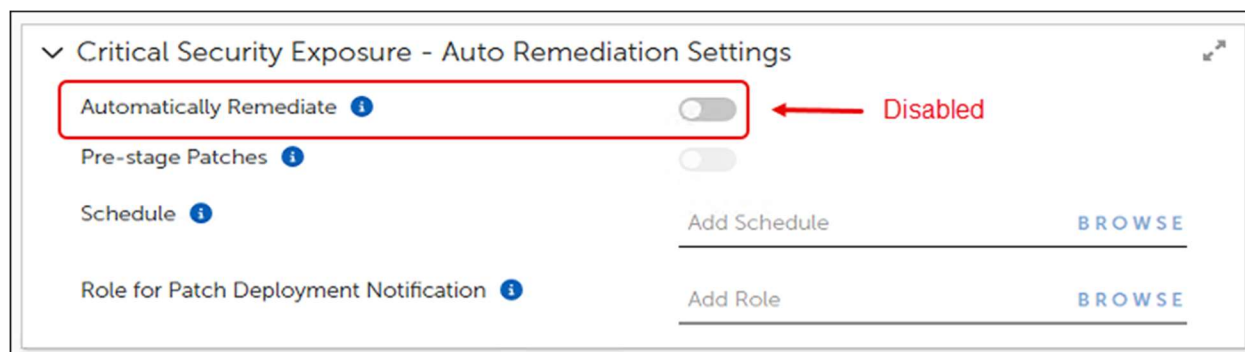
available on the devices at the scheduled deployment time, which reduces the time to complete the deployment.



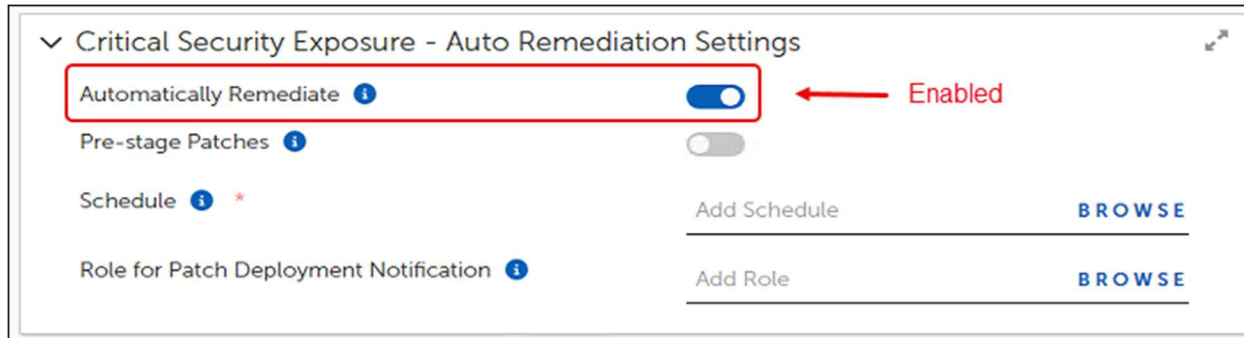
Additional settings include adding a schedule to begin the remediation process and identifying roles that receive notification of the deployment. Repeat the Auto Remediation steps for each urgency level that will use auto remediation. At any time during these configuration steps, click **Save** on the upper-left corner of the template to save your changes.

## Enable Auto Remediation

1. Select the **Automatically Remediate** toggle in the **Auto Remediation Settings** section of the workspace.
  - a. When disabled, no auto remediation of vulnerabilities occurs for this security level (default).



- b. When enabled, Tenable Patch Management remediates all vulnerabilities at the security level of the template.



2. Select the **Pre-stage Patches** toggle to enable the automatic download of patch content to all applicable and licensed devices as soon as the patch becomes available.

### Important

Pre-staging does not install any content on devices. It downloads the content to the target devices, where it waits until the auto remediation schedule begins.

3. Select **Browse** next to **Schedule** to select the time parameters for running auto remediation:

Schedules Show All + Create Schedule

Search Columns... × Q Search

<input type="checkbox"/>	Schedule Name	Start Date	End Date	Last Modified
<input type="checkbox"/>	> ASAP	7/28/24, 7:29 AM	--	--
<input type="checkbox"/>	> Balanced Daily at 6AM	7/28/24, 6:00 AM	--	--
<input type="checkbox"/>	> Basic Inventory Schedule	7/28/24, 10:00 AM	--	--
<input type="checkbox"/>	> Daily At 2AM	7/30/24, 2:00 AM	--	--
<input type="checkbox"/>	> Every 12 Hours	7/30/24, 2:00 AM	--	--
<input type="checkbox"/>	> Every 15 Minutes	7/28/24, 7:29 AM	--	--
<input type="checkbox"/>	> Every Day	7/28/24, 7:29 AM	--	--
<input type="checkbox"/>	> Every Hour	7/28/24, 7:29 AM	--	--
<input type="checkbox"/>	> Every Month	7/30/24, 2:00 AM	--	--
<input type="checkbox"/>	> Every Sunday At 1 AM	7/30/24, 1:00 AM	--	--

Rows Per Page: 10 1 - 10 of 12 1 / 2

- a. Select **Show All** to see the available roles.
  - b. Select a Schedule on which to run auto remediation.
  - c. Select **Add Schedule** at the bottom left to save your changes.
4. Select **Browse** next to **Role for Patch Deployment Notification** to select the role of the administrators who require notification of this deployment:

- a. Select **Show All** to see the available schedules.
- b. Select a **Role** to identify who receives notification of this deployment.
- c. Select **Add Role** at the bottom left to save your changes.

## Vulnerability Detection Source Settings

These settings determine which critical vulnerabilities Auto Remediation automatically resolves based on which service reports the vulnerability. You may enable one or more source settings.

Select the toggle next to the source you want to enable or disable. When enabled, Auto Remediation occurs for critical patch vulnerabilities reported by the source.

## Production Deployment Settings for Auto Remediation

Configure the deployment settings for Auto Remediation in the production environment. These three settings identify the roles that provide initial approval prior to deployment, the amount of time to wait for the approval, and a period of load leveling across all target machines for patch installation.

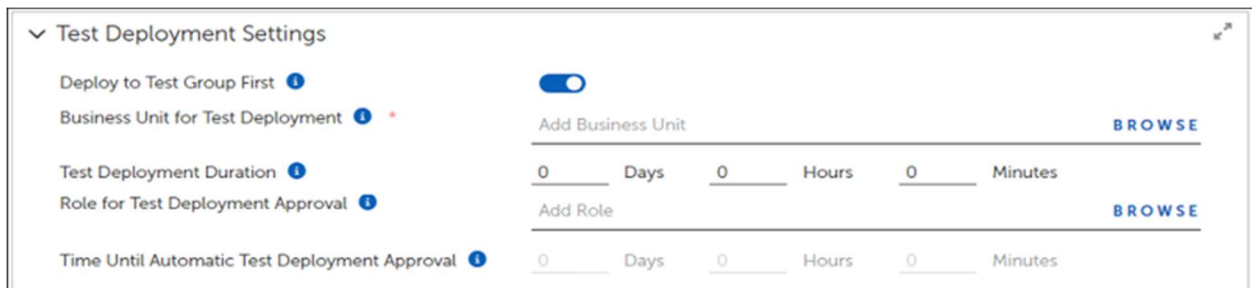
**Approval Role:** Roles that provide initial approval prior to deployment.

**Approval Time Frame:** A zero value means that the deployment waits for approval indefinitely. A non-zero value means that deployment begins after the wait time passes, even if no one has approved.

**Load Leveling:** A zero value means that, after approval, deployment begins immediately on all devices. A non-zero value creates a window during which load balancing for production patch installation occurs across all target devices.

## Test Deployment Settings for Auto Remediation

Use test deployment settings to deploy patches to a specific Business Unit first, such as test or lab units, to test deployment prior to initiating a deployment to the production environment. When enabled, complete the following steps to configure the test settings.



The screenshot shows the 'Test Deployment Settings' workspace. It contains the following configuration options:

- Deploy to Test Group First:** A toggle switch that is currently turned on.
- Business Unit for Test Deployment:** A field with an 'Add Business Unit' button and a 'BROWSE' button.
- Test Deployment Duration:** A time picker set to 0 Days, 0 Hours, and 0 Minutes.
- Role for Test Deployment Approval:** A field with an 'Add Role' button and a 'BROWSE' button.
- Time Until Automatic Test Deployment Approval:** A time picker set to 0 Days, 0 Hours, and 0 Minutes.

1. Select the **Deploy to Test Group First** toggle in the **Test Deployment Settings** workspace of Auto Remediation Settings. This enables automatic deployment of the Auto Remediation Settings to a test group.



2. Select **Browse** to select a **Business Unit** as the test destination.
3. Enter numbers for **Days**, **Hours**, and **Minutes** to set the **Test Deployment Duration**, which indicates how long production deployment waits after initiating test deployment to begin production deployment.
4. Select **Browse** to select a Role to receive deployment notification. This enables the **Time Until Automatic Test Deployment Approval** settings.
5. Enter numbers for **Days**, **Hours**, and **Minutes** to set the **Test Deployment Duration**, which indicates how long to wait for approval. A zero value means that the deployment waits indefinitely for approval. A non-zero value means deployment begins after the wait time passes, even if no one has approved.
6. Select **Save** on the upper left to save the test settings for the Auto Remediation.
  - a. Future deployments that match the exposure level you modified deploy to your test environment.
  - b. After verifying the operation of the remediation in your test lab, you can disable Deploy to Test Group First in the Auto Remediation Settings.

## Verify that Auto Remediation Works as Expected

1. Select **Home** on the left navigation menu of the [Tenable Patch Management Dashboard](#). Here you can view the high level-details of the patch environment. For more information, see [Tenable Patch Management Home Dashboard and Performance Widgets](#).
2. Mouse over or click **Patching State** in the left navigation menu, and then select **Devices**. For more information, see [Patching State Dashboard](#).

# Patching Preferences

A Patching Preferences configuration applies a preferred maintenance window and user interaction settings to the target devices in a specified Business Unit. Administrators may create a different patching preference configuration for each Business Unit or for as many different Business Units as they choose. A Business Unit may belong to only one Patching Preferences configuration.

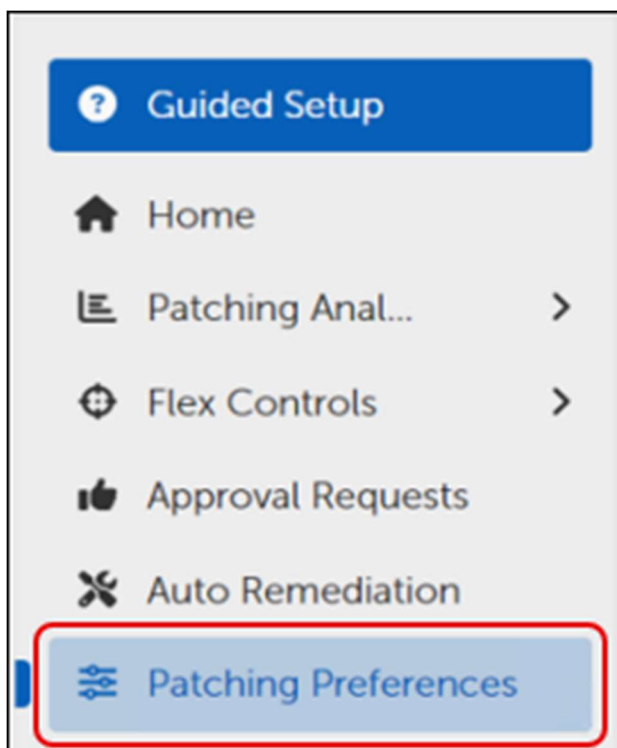
Each Patching Preference object creates its own Business Unit, which users may not edit. The Patching Preference Business Unit shares the same members (devices) as its target Business Unit, as well as any customized preferences.

## Using Patching Preferences

Administrators can set preferences for Maintenance Window and User Interaction Settings and apply those preferences to a specific Business Unit. In Patching Preferences, you may set preferences for either a Maintenance Window or for Server User Interaction Settings, or both.

## Access Patching Preferences

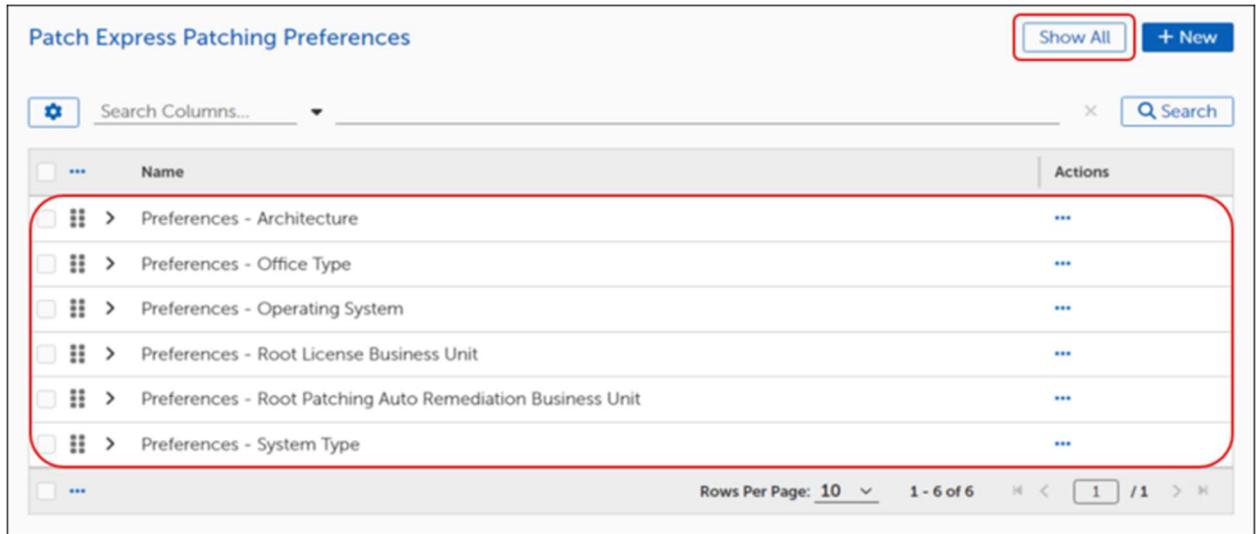
1. Select **Patching Preferences** on the left navigation menu.



This opens the **Patch Express Patching Preferences** dialog.

### Tip

The table is empty until you [create a Patching Preference](#).



2. Select **Show All** to view all available Patching Preferences:
  - c. Select a Patching Preference from the table.
  - d. To search for an existing Patching Preference, enter a search term, and then click **Search**.

## Create a New Patching Preference

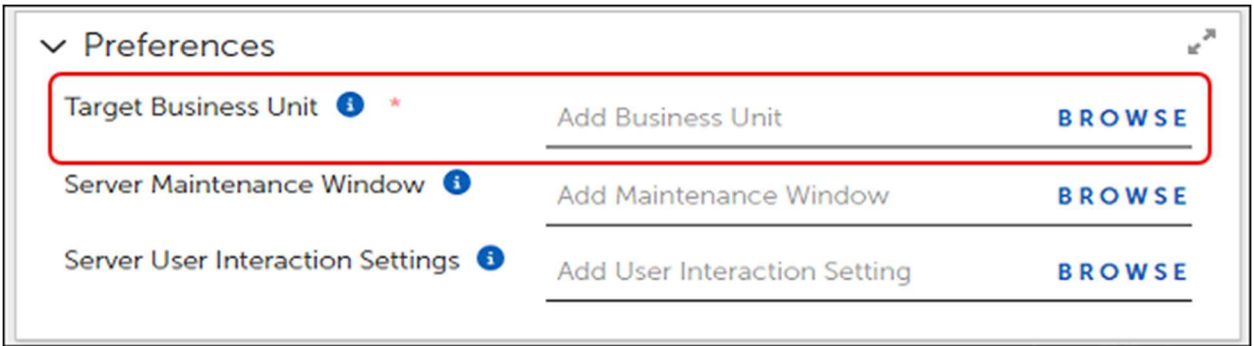
Create a patching preference for each Business Unit that requires unique maintenance window or user interaction settings. At any time during these configuration steps, click **Save** in the upper-left corner of the template to save your changes.

1. In an open Patching Preferences template (**+ New**), enter a Description of the preference you are creating. The system automatically generates a Name based on the target Business Unit.
2. When you finish modifying and saving the new patching preferences, click **Save** at the upper-left corner of the template.

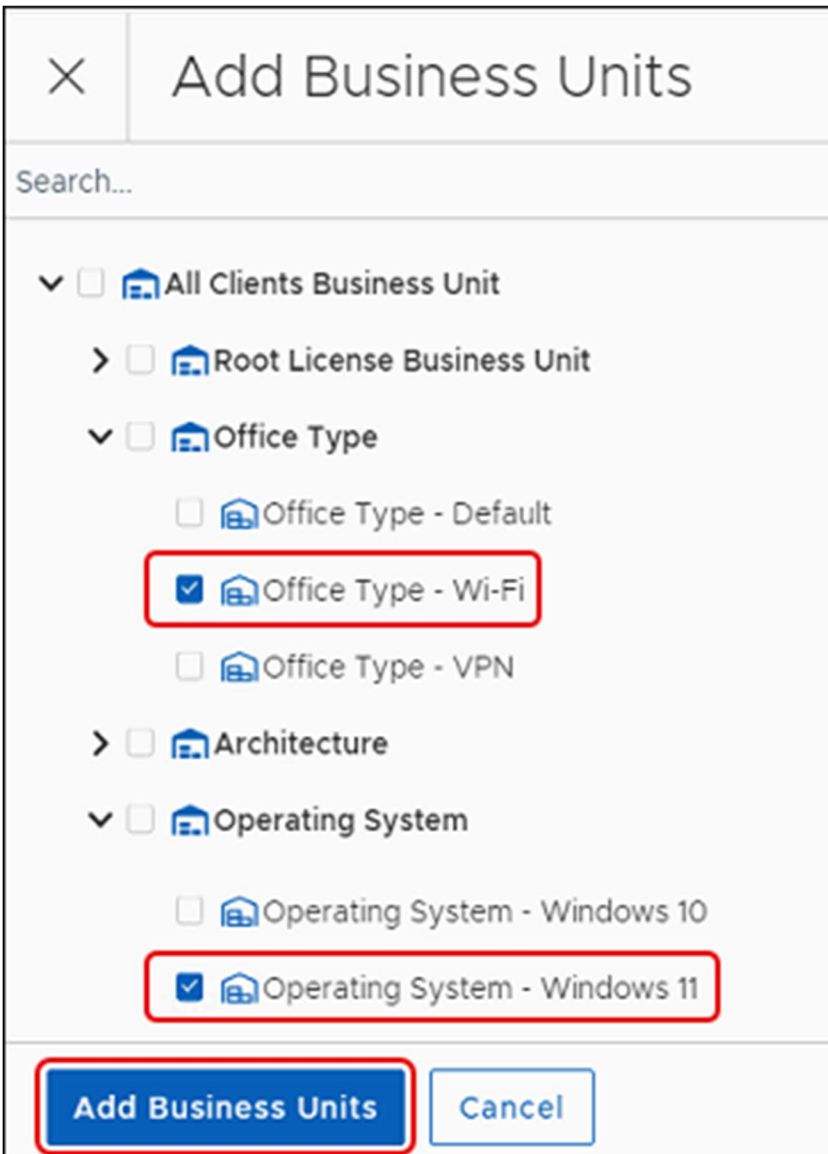
## Add a Target Business Unit

Add a Target Business Unit using the following steps:

1. Select **Browse** next to **Target Business Unit** in the **Preferences** workspace.



This opens the **Add Business Unit** dialog. The example shows possible choices.

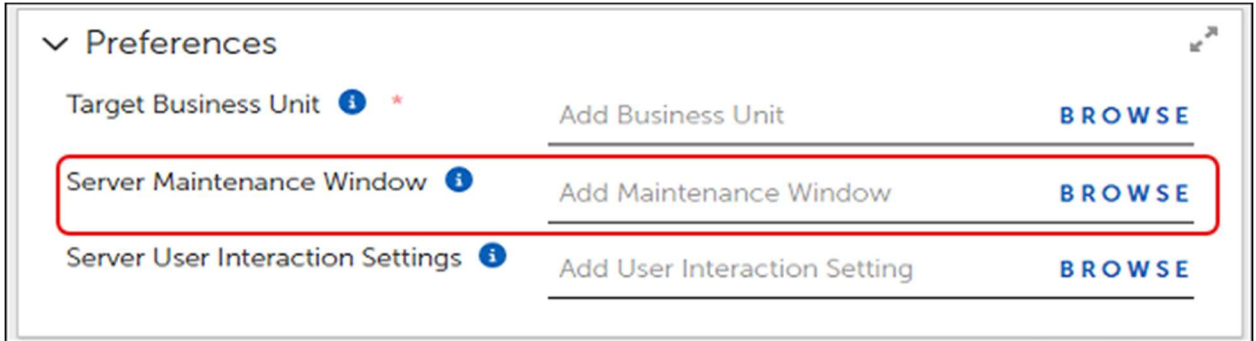


2. Select the Business Unit you want to target.

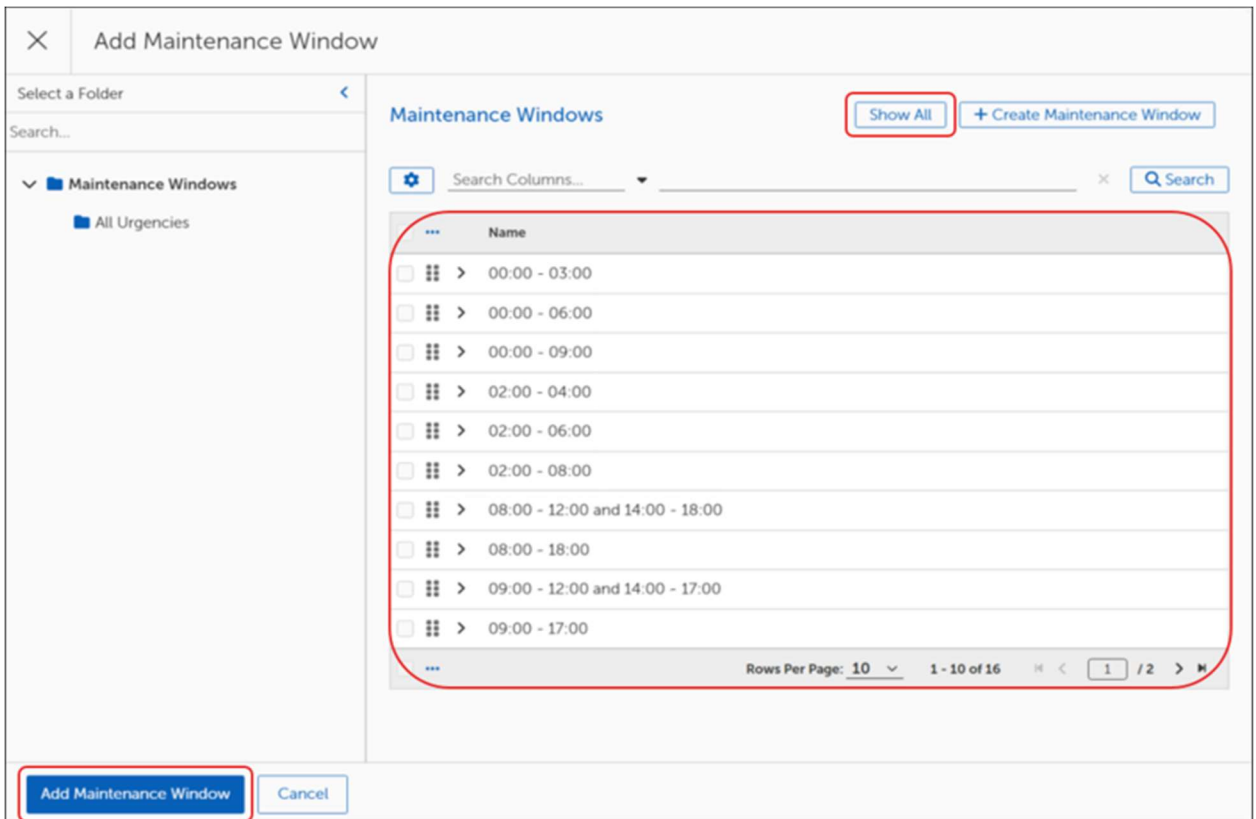
3. Select **Add Business Unit** on the bottom left of the dialog.

## Select a Server Maintenance Window

1. Select **Browse** next to **Server Maintenance Window**.



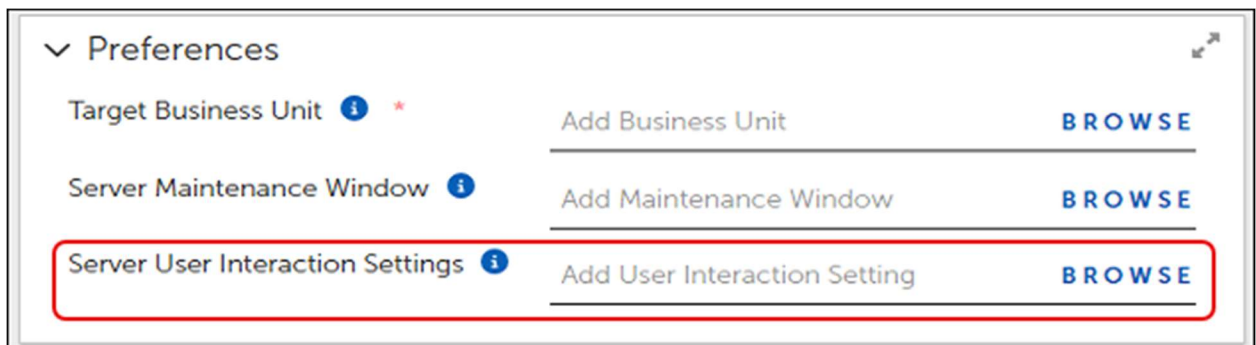
This opens the **Add Maintenance Window** dialog.



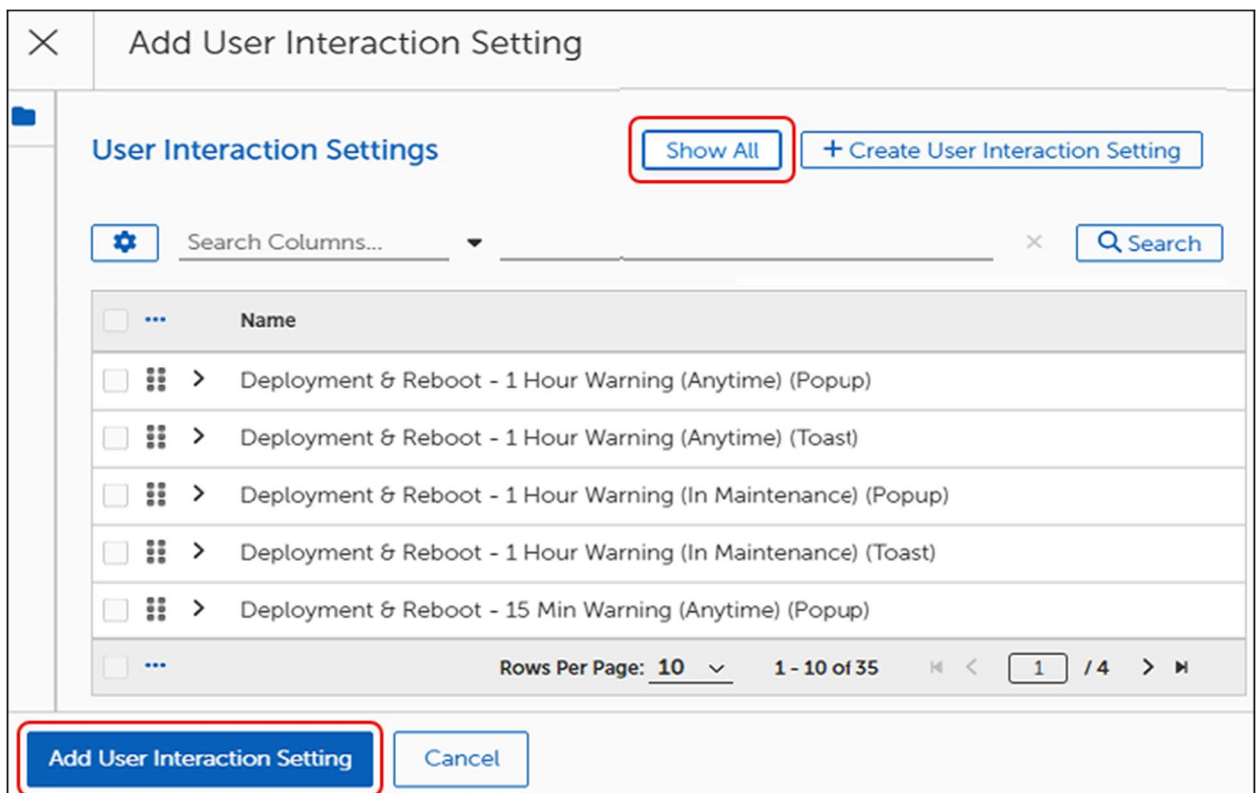
2. Select **Show All** at the upper right to view the available Maintenance Window settings.
3. Select the checkbox aligned with the setting you want to use. To create a new Maintenance Window setting, see [Maintenance Windows](#), then return and repeat this step.
4. Select **Add Maintenance Window** on the lower-left corner of the **Add Maintenance Window** dialog.

## Select Server User Interaction Settings

1. Select **Browse** at the far right of **Server User Interaction Settings**.



This opens the **Add User Interaction Setting** dialog.



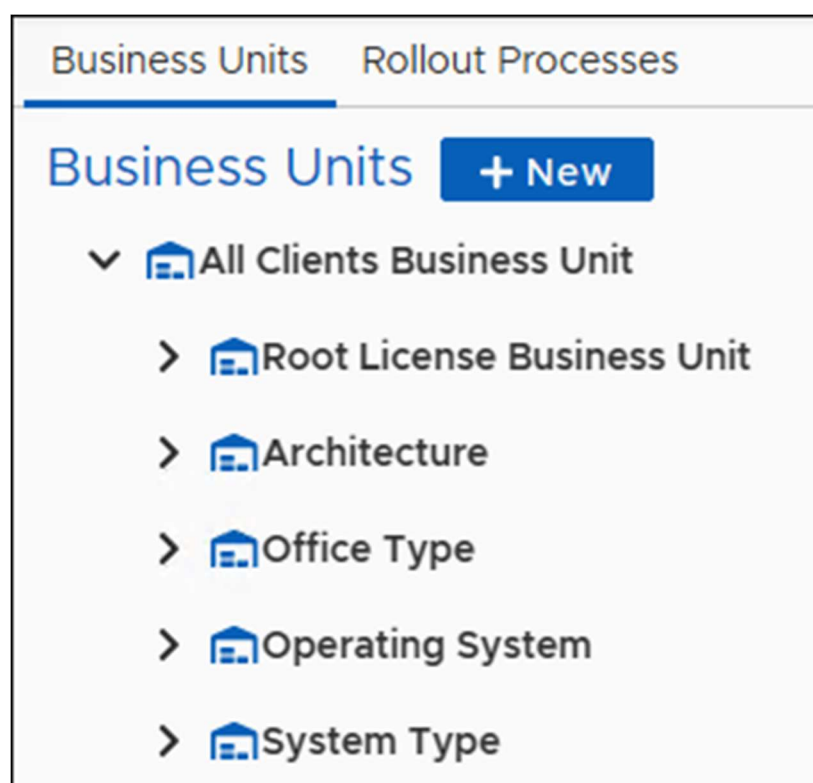
2. Select **Show All** at the upper-right corner to view the available options, and then select the checkbox aligned with the options you want to use. To create a new setting, see [User Interaction Settings](#), then return and repeat this step.
3. Select **Add User Interaction Setting** on the lower-left corner of the dialog. This returns you to the **Patching Exceptions** template.
4. Select **Save** at the upper-left corner of the template.

# Business Units

## Understanding Business Units

Business Units target specific groups of devices that share an attribute such as location, device type, or connectivity. They use Rollout Processes to manage notifications and approvals and manage deployment. Each Business Unit can have its own unique settings and policies that apply to its member devices. These settings include rollouts, interaction settings, and more.

In addition, children of Business Units inherit settings from parent Business Units to reduce the administrative burden of managing settings across multiple units. Tenable Patch Management includes a Parent Business Unit for All Clients, and Child Business Units that address most device grouping scenarios.



Related business units, including Child Business Units or Lab Business Units, provide another level of detail that administrators can use to further customize a patching environment.

### **Important**

When adding Business Units to a Patching Strategy, make sure that the Patch Deployment Bot for that Strategy specifies the same Business Units.

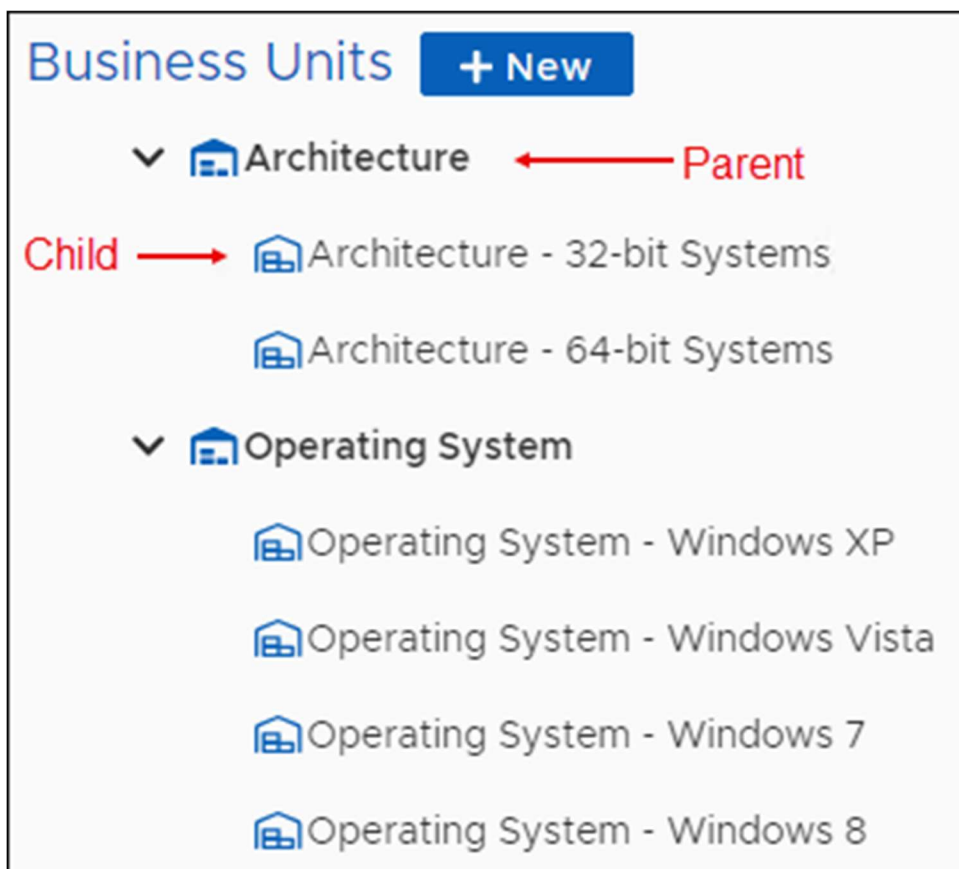
In addition to identifying the devices to include in a Business Unit, you can also identify many aspects of patching for endpoints, such as rollout processes, maintenance windows, approvals, and more.

## Parent and Child Business Units

Business Unit objects use a parent-child hierarchy. A parent Business Unit may have multiple child Business Units, but a child Business Unit may have only one parent. The folder structure used in Tenable Patch Management shows the parent as the top-level folder and the child units as sub folders of a parent. This structure gives you the freedom to create patching hierarchies that match any endpoint landscape.

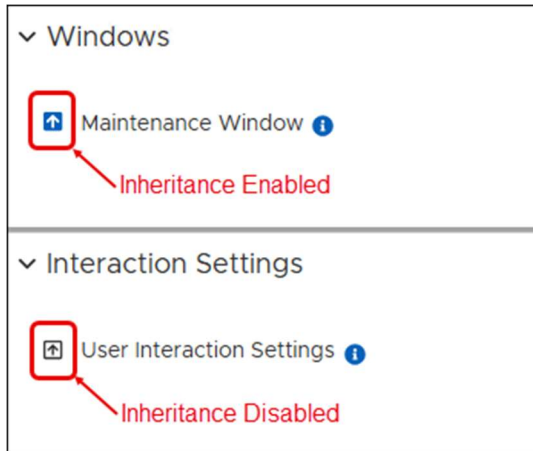
### Important

Child Business Units may only contain devices that the Parent Business Unit also manages. For example, if a Parent Business Unit has devices A, B, C, and D, and the Child Business Unit has devices C, D, E, and F, the resulting devices in the Child Business Unit include C and D only.



There is no functional difference between parent and child Business Units. The purpose of the parent/child hierarchy is to allow a child Business Unit to inherit settings from a Parent, which can simplify the creation of Business Units with both distinct and common requirements. An up-arrow with a blue background preceding a setting or process shows an inherited setting.



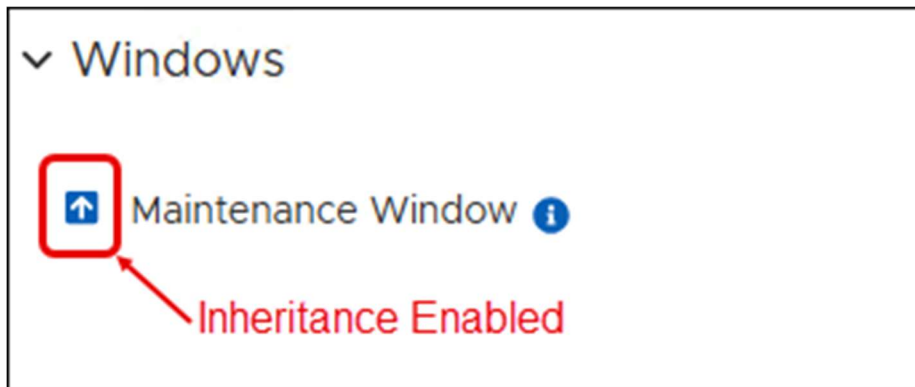


The hierarchical nature of Business Units allows a child Business Unit to inherit settings from its parent. An up-arrow with a blue background preceding a setting or process shows an inherited setting.

Tenable Patch Management accommodates an unlimited number of parent or top-level Business Units. Create many different Business Unit hierarchies based on details that model requirements and processes in your environment.

## Managing Inheritance Settings

In Tenable Patch Management, inheritance defaults to Enabled.



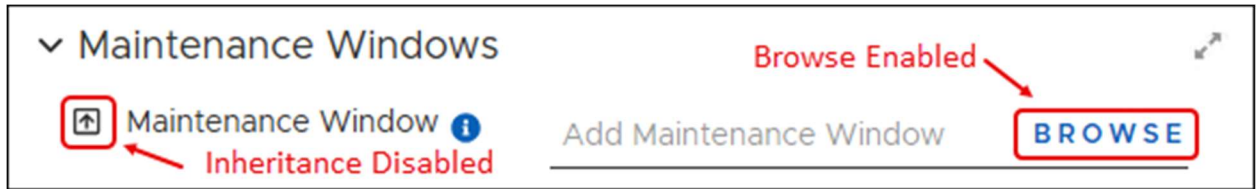
### Important

The colors shown here are default color settings. If you change the Admin Portal theme settings to use different colors, your arrows and backgrounds might be different.

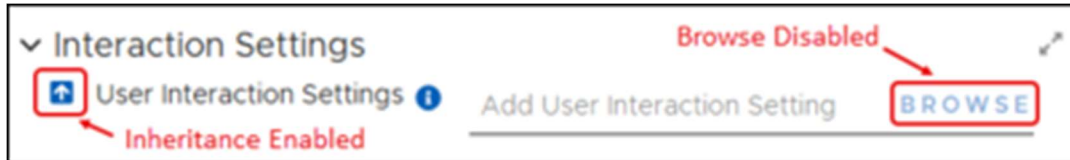
## Enable Inheritance

A white up-arrow with a blue background preceding a setting or process shows an inherited setting. Enabling inheritance disables the **Browse** button for the setting because you may not make any changes.

1. Check the up-arrow next to **Maintenance Window** in an open Business Unit template to determine its inheritance status.



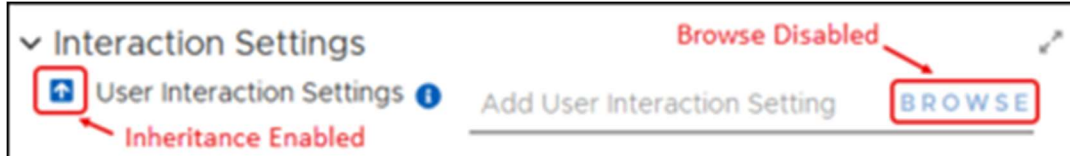
2. Select the up-arrow icon to enable inheritance



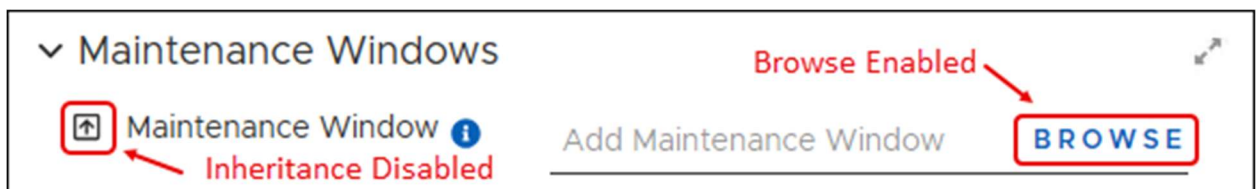
## Disable Inheritance

A black up-arrow with a white background preceding a setting or shows a disinherited setting. Disabling Inheritance enables the **Browse** button for the setting, which allows you to change the settings.

1. Check the up-arrow next to **Maintenance Window** in an open Business Unit template to determine its inheritance status.



2. Select the up-arrow icon to disable inheritance.



## Organizing the Business Unit Hierarchy

You can arrange the Business Unit view in hierarchies that meet the needs of your environment. Parent Business units – bold, top-level folders – pass attributes to child Business Units – sub-folders – so it is important to maintain those relationships where they exist.

In addition, when a device is part of multiple Business Units, the device inherits the settings of the highest priority Business Unit. This occurs even when the patch information comes from a Business Unit with different settings than the highest priority Business Unit.

## Best Practices when Changing Priorities

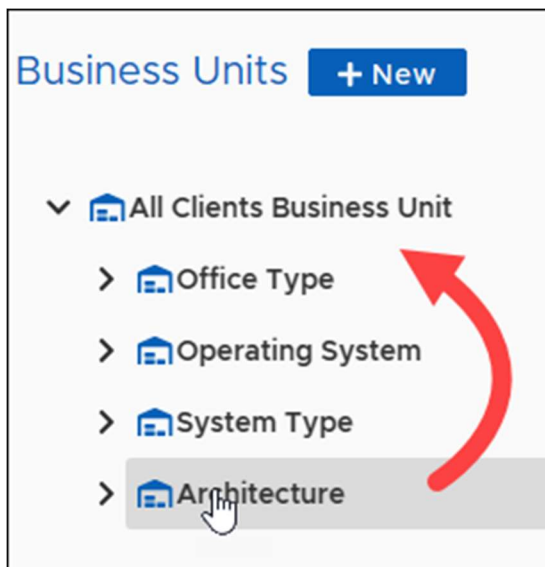
In the Business Unit hierarchy shown in the Tenable Patch Management dashboard, the Business Unit at the top of the list has the lowest priority. When changing the priority of a Business Unit in the hierarchy, consider the following items:

- **Priority** – Do the settings and desired state of the new priority Business Unit match your expectations for the moved Business Unit?
- **Membership** – Are the devices in the moved Business Unit compatible with the new priority Business Unit?
- **Inheritance** – Are the inheritance settings for the moved Business Unit still accurate in this new location?
- **Deployment Waves** – Is the Business Unit you are moving, or any of its ancestors included in a Wave Entry that includes descendants? If so, are those deployments still necessary?

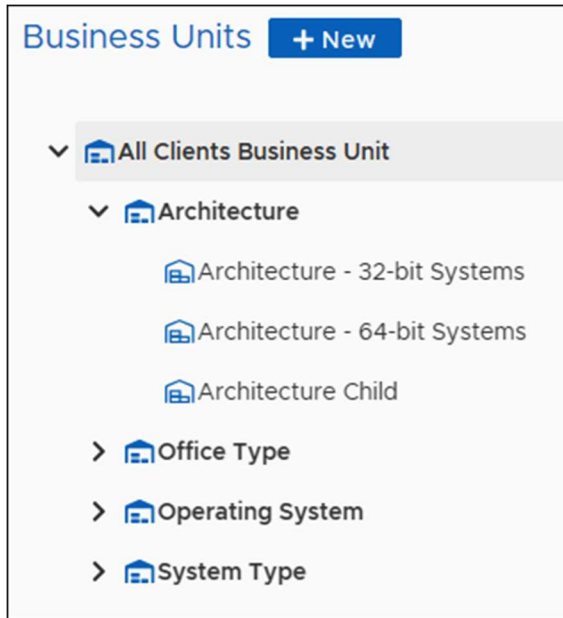
Further, is the new parent, or any ancestors, included in a Wave Entry that includes descendants? If yes, do you want the new BU included in those deployments?

## Change the Order of the Hierarchy

1. Follow the steps to [create a Business Unit](#), and then drag and drop a parent Business Unit to a new location.



2. Select **OK** at the prompt to verify your intended move. The new hierarchy structure shows the parent Business Unit and all child Business Units moved to the new location.



## Creating a Business Unit

Tenable provides default settings for the included templates. Except for the Business Unit templates provided for Root, you can copy the default templates and save them with new details, or you can create a new Business Unit. Related Business Units, including Child Business Units or Lab Business Units, provide another level of detail that administrators can use to further customize a patching environment.

Related Business Units, including Child Business Units or Lab Business Units, provide another level of detail that administrators can use to further customize a patching environment.

## Open and Save a Business Unit Template














Each of the default Business Units provided by Tenable target production devices. Tenable recommends copying and creating new Business Units and to create Business Units for test purposes. Except for Business Units provided for Root, you can copy the default templates and save them with new details, or you can create a new Business Unit.

1. Mouse over or click **Business Units** in the left pane [Tenable Patch Management Dashboard](#), and then select **Business Units**.
2. Select the right arrow to the left of any folder to expand the list of available templates.

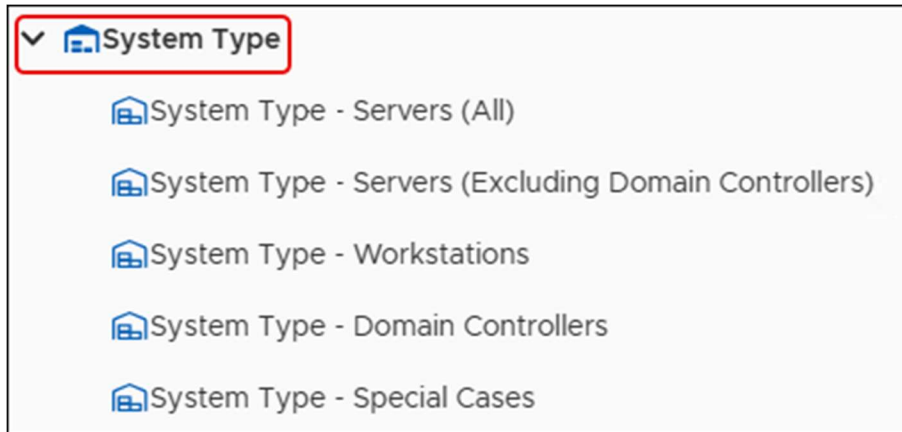
Business Units   Rollout Processes

---

Business Units [+ New](#)

- ▼  All Clients Business Unit
  - >  Root License Business Unit
    - ▼  Tenable ACR Business Units
      -  Tenable ACR 1 Business Unit
      -  Tenable ACR 2 Business Unit
      -  Tenable ACR 3 Business Unit
      -  Tenable ACR 4 Business Unit
      -  Tenable ACR 5 Business Unit
      -  Tenable ACR 6 Business Unit
      -  Tenable ACR 7 Business Unit
      -  Tenable ACR 8 Business Unit
      -  Tenable ACR 9 Business Unit
      -  Tenable ACR 10 Business Unit

3. Select the Name of a template to open it.



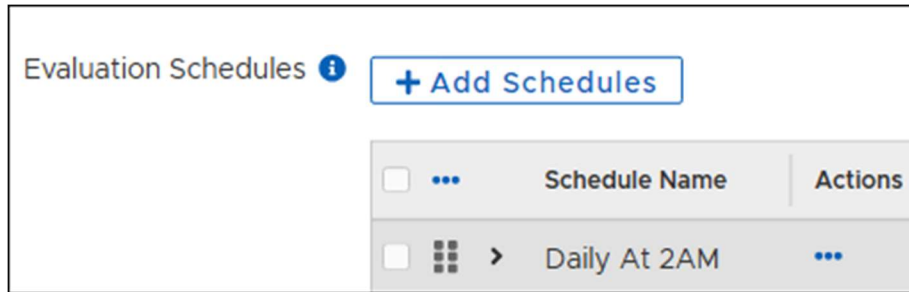
4. Save the template with a new title:
  - a. Select **More** in the upper-left corner of the template, and then select **Save <object> As**.
  - b. Enter a new Name for the template, and then click **OK** on the lower-left corner of the naming dialog. This returns you to the template with the new name.
  - c. Enter a detailed **Description** of the process covered in this template or leave the prepopulated description. Add a character to enable the **Save** button.
5. Select **Save**. When you have finished modifying your new template, you can drag and drop it into the folder you created (see </document/preview/447#UUID-eab9f6cf-5f54-57b7-8ef2-4c0bdb348e5f>).

## Add Evaluation Schedules to a Business Unit

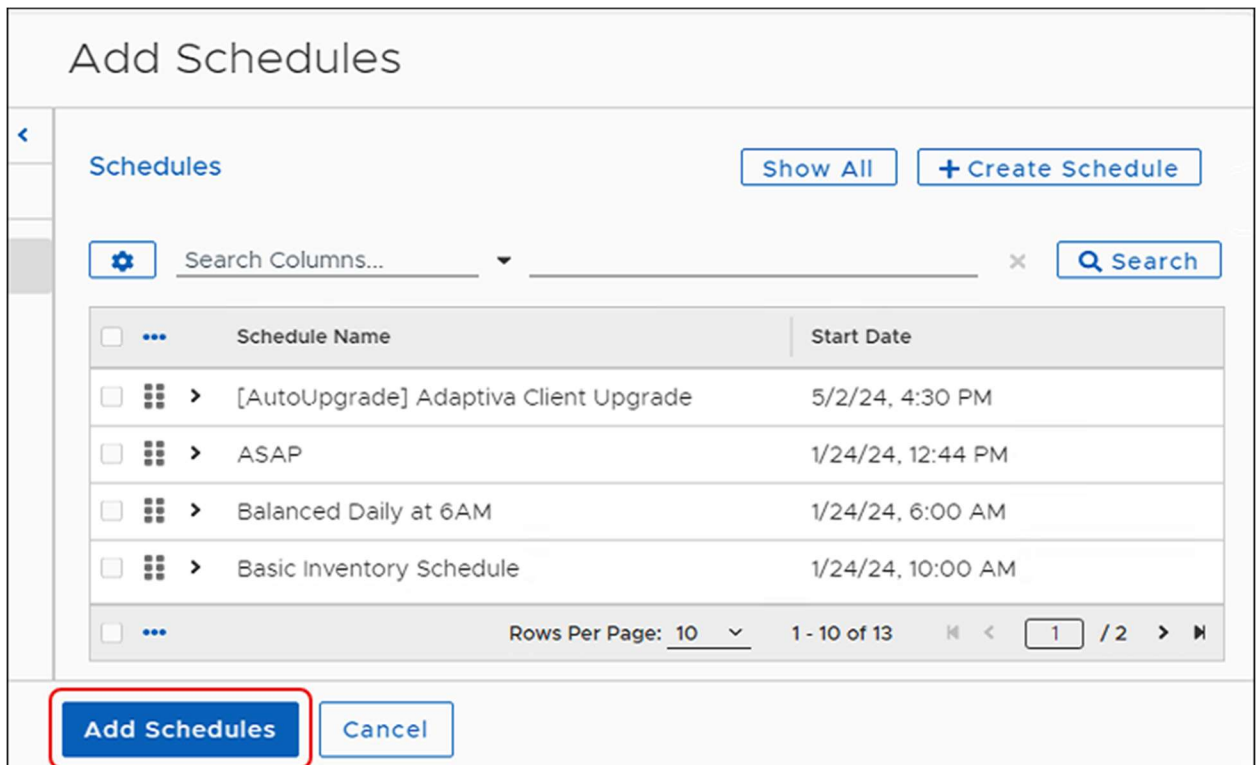
For Business Units with dynamic membership that may change over time, evaluation schedules determine when to check the membership of a Business Unit. Dynamic membership can occur based on Location or Sensor scopes where a device moves between locations or Sensor results change over time.

The Evaluation Schedules added here trigger Group Membership evaluations for this Business Unit to regularly check for group membership changes. The schedule listing uses the same set of schedules created for Patching purposes, but in this context, only triggers group membership evaluation.

1. From an open [Business Unit Template](#), review the selected schedules (if any).
  - a. If you choose to use the existing schedules, skip to [Configure Business Unit Scopes](#).
  - b. Otherwise, click **+ Add Schedules**, and then continue with the next step.



2. Select one or more **Schedule Names** from the **Add Schedules** table, and then click **Add Schedules** on the lower-left corner of the dialog.



3. Select **Save** on the upper-left corner of the dialog to save your progress:
  - a. Check the **Error View** and resolve any errors.
  - b. Select **Save** again if you make any changes.

## Configure Business Unit Scopes

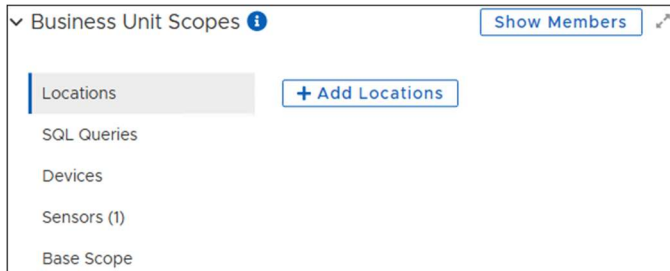
Business Unit Scopes define the rules used to find and include devices in a named Business Unit. Tenable Patch Management supports using one or more scopes to create a Business Unit.

### Tip

If the scope type (Locations, and so on) has a number in parenthesis after the name, the template you copied included one or more of the identified scopes. Select the scope

type to view the setting. You can either keep the included scope or click the **ellipsis (...)** after the scope name in the table to edit (if allowed) or delete it.

1. Scroll down to **Business Unit Scopes** in an open [Business Unit](#) template,
2. Select the Scope you want to use for this Business Unit.



### Add Locations

Use this option to define the Business Unit based on the location of devices. For example, you might want this Business Unit to include all devices in an office located in Chicago.

1. Select **Locations** from Business Unit Scopes, and then click **+ Add Locations**.

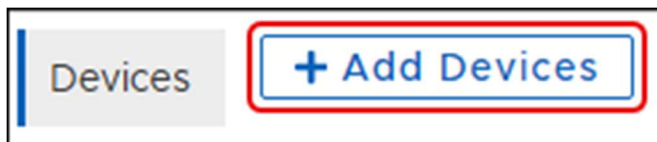


2. Select one or more Location Names from the **Add Locations** table to assign them to the Business Unit.
3. Select **Add Locations** in the lower-left corner of the dialog. This returns you to the Business Unit template and populates a table with the selected Locations.

### Add Devices

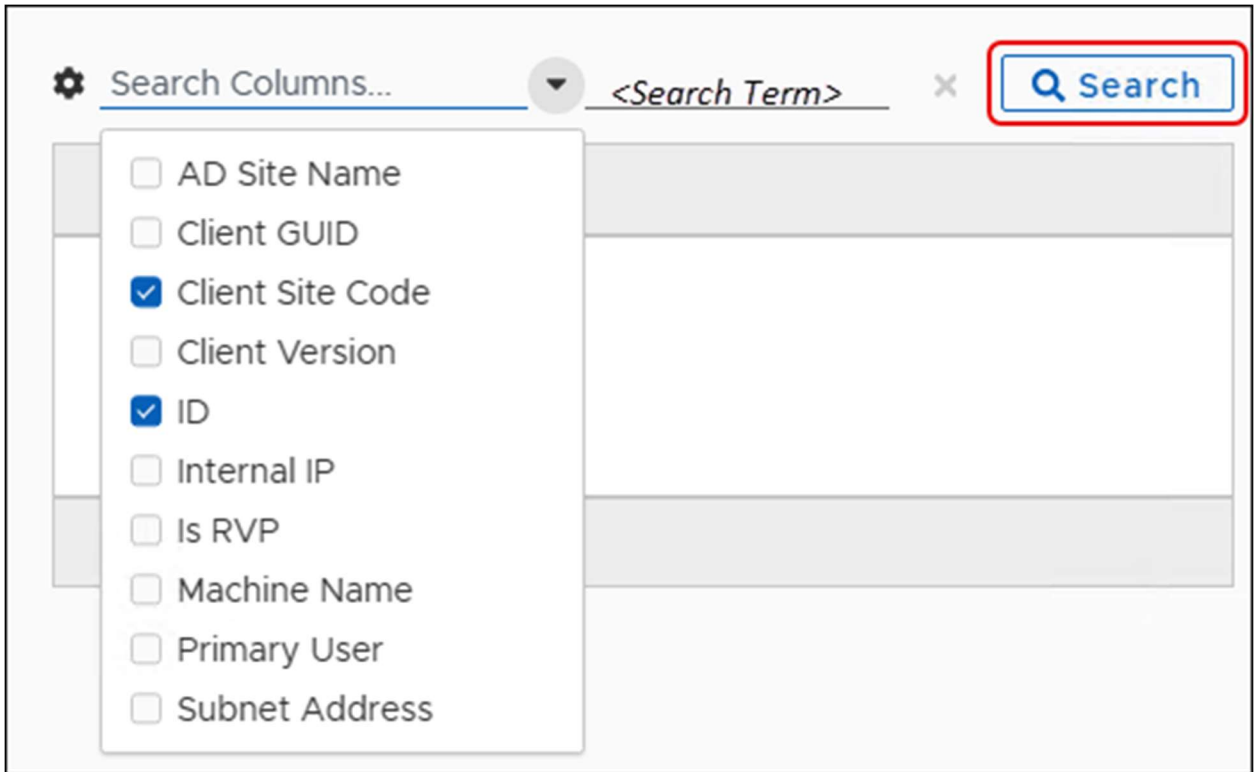
Choose one or more individual devices as members of this Business Unit.

1. Select **Devices** from **Business Unit Scopes**, and then click **+ Add Devices**.



2. Use **Search** to define one or more search details you want to use to locate specific client devices.
3. Enter your search term, and then click **Search**.





4. Select one or more devices to add to this Business Unit, and then click **Add Devices** on the lower-left corner of the dialog.

#### Add SQL Queries

Design your own SQL queries to define the scope of devices to include in this Business Unit.

1. Select **SQL Queries** from **Business Unit Scopes**, and then click **+ Add Query**. This opens the **Add Query** dialog.

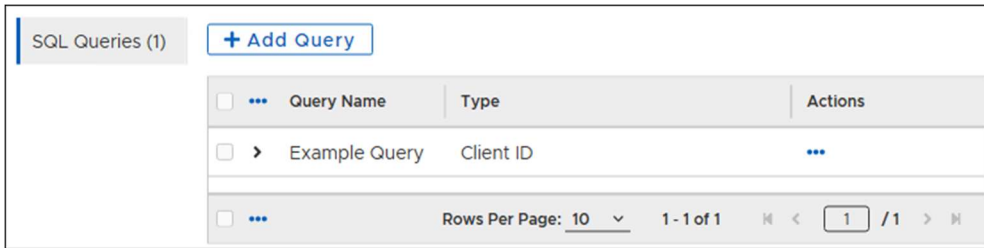


2. Enter a **Name** for the Query, and then add a detailed **Description**. The **Type** field defaults to **Client ID**, meaning that the software returns a list of Client IDs regardless of what the query might request.
3. Write your SQL query in the **Query** text box.

#### Important

Tenable recommends testing your sample query using SQL Server Management Studio.

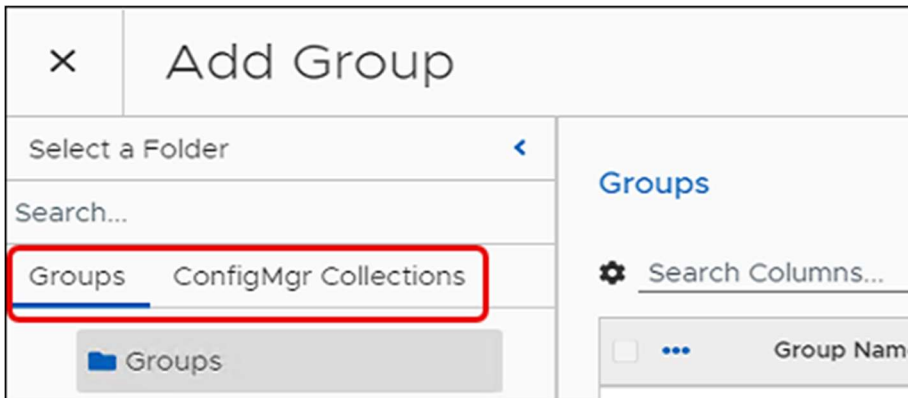
4. Select **Add Query** at the bottom left of the dialog. This returns you to the Business Unit template and populates a table with the new SQL query.



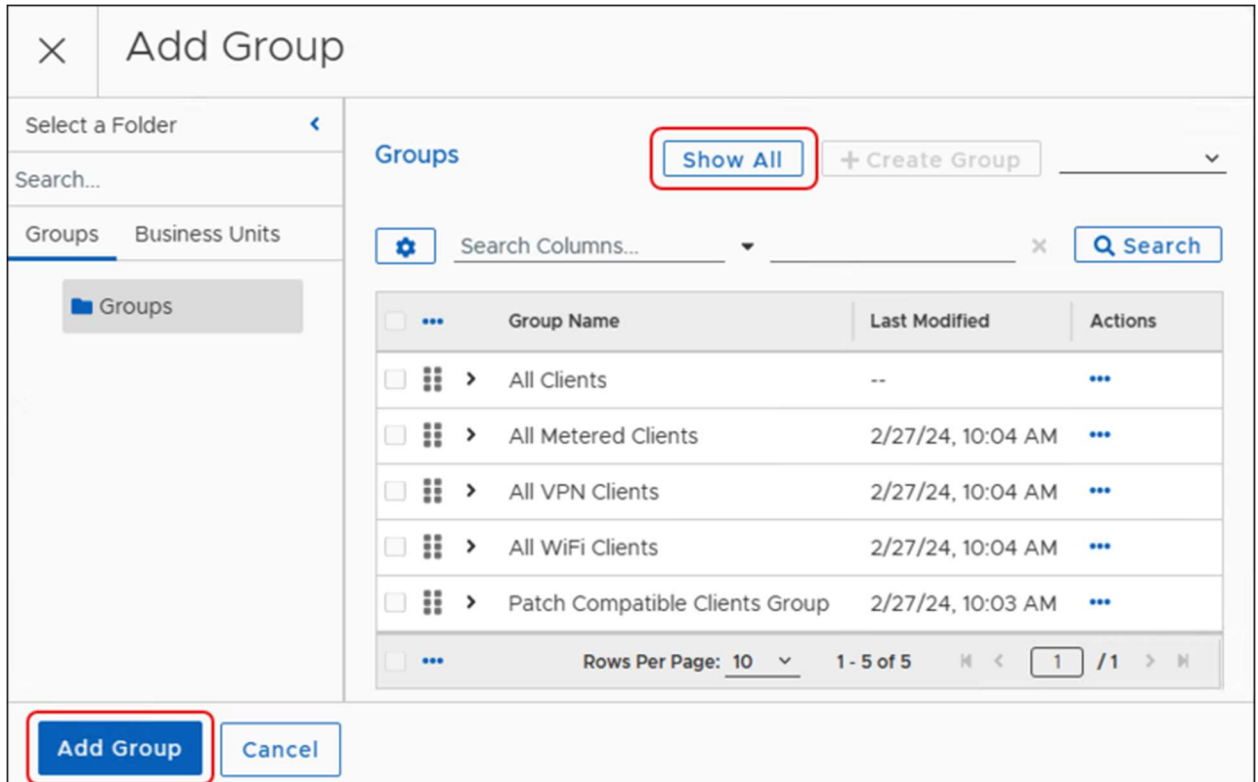
### Set Base Scope

Use Base Scope settings to add or exclude devices in a Business Unit based on chosen standards. Using Operators and Conditions, you can extend Business Unit membership and group multiple devices together.

1. Select **Base Scope** from **Business Unit Scopes**.
2. Select the **ellipsis (...)** to the right of **Select Operator**, and then click **Add Group**.
3. Select either **Groups** or **Business Units** at the top left of the dialog.



4. Select **Show All** to list all available options, and then select one to add to the **Base Scope**.



5. Select **Add Group** on the lower-left corner of the dialog. The entry under Business Unit Scopes shows the **AND** operator and the item you chose.

### Add Sensors

Sensors mark device inventory using technology settings such as Java, PowerShell, WMI, and so on. Tenable Patch Management includes choices for common sensor settings, or you can create your own.

#### Tip

Selecting a Sensor from this location assumes you have already created the Sensor type you want to use, or that you intend to use one of the default sensors provided by Tenable.

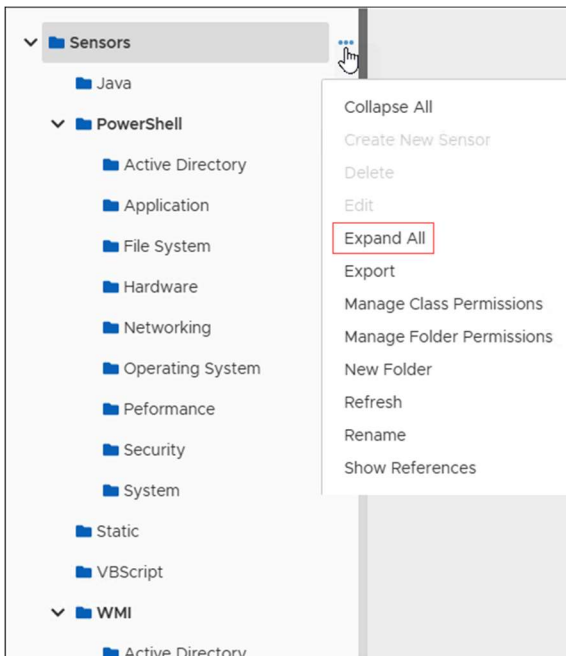
To include devices in this Business Unit based on sensor settings, complete the following steps:

1. Select **Sensors** from **Business Unit Scopes**, and then click **+ Add Sensor Group Scope**.



2. Enter a **Name** and a detailed **Description** of the Sensor Group in the **Sensor Group Scope** dialog.

3. Select **Browse** to choose a Sensor.
4. Select the **ellipsis (...)** next to **Sensors**, and then select **Expand All** to view the list of available Sensor settings.

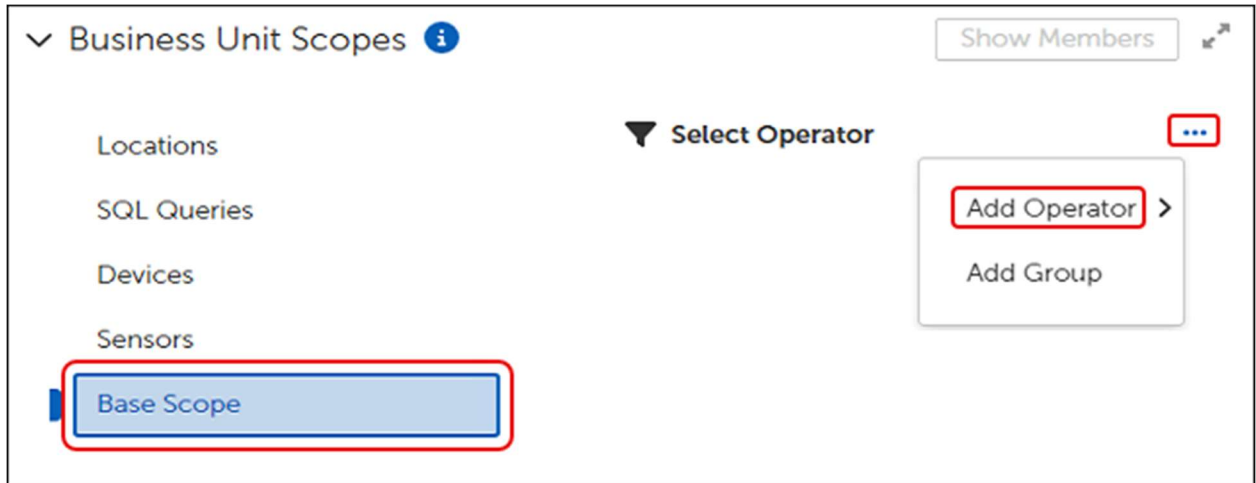


5. Select an item to use in your Sensor Group, and then click **Add Sensor**. This returns you to the **Sensor Group Scope** dialog.
6. Select **OK** to return to the Business Unit template or change *Base Scope* settings.

## Add Multiple Groups or Business Units

After setting the initial Base Scope, use this procedure to add additional Groups or Business Units to include in the Base Scope. You can add or exclude other Groups or Business Units or change Operators to customize your Base Scope depending on your needs.

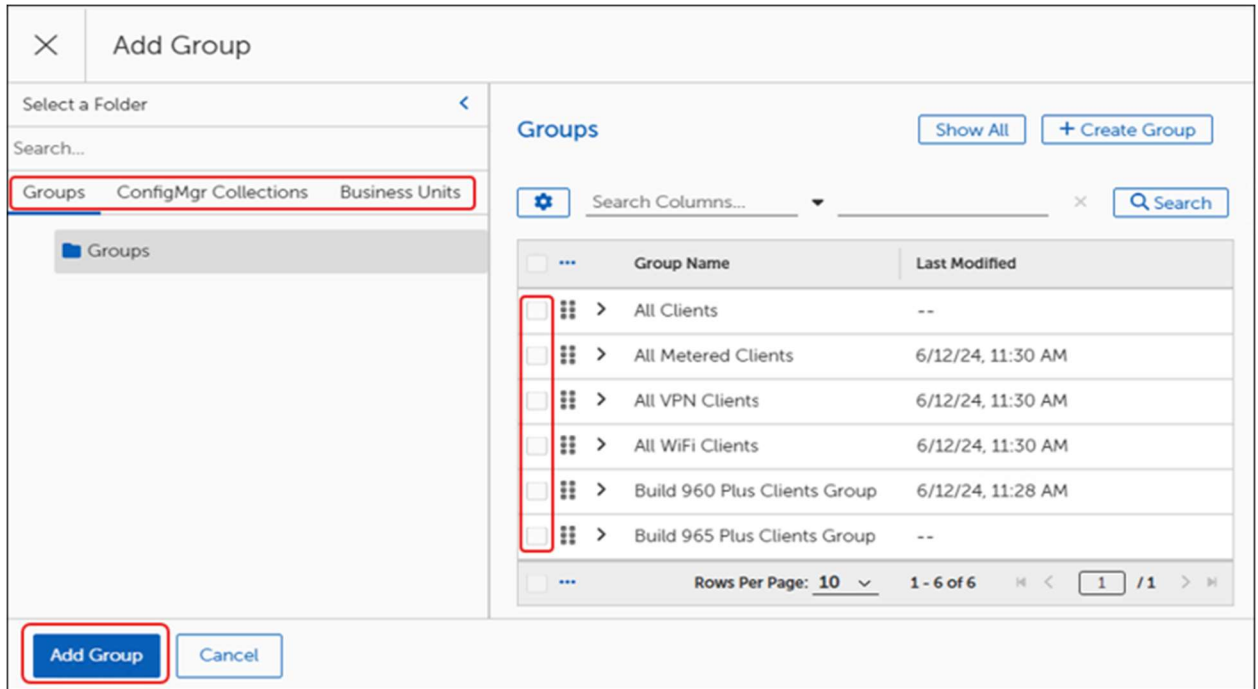
1. In the **Business Unit Scopes** section of an object template, click **Base Scope**.



2. Select the **ellipsis (...)** to the right of **Select Operator** (or any existing Operator), and then select **Add Operator**.
3. Select the **Operator** you want to include (AND, OR, NOT). This populates the workspace with the operator you chose.
4. Select the **ellipsis (...)** next to the operator, and then select **Add Group**. This opens the **Add Group** dialog.



5. Select one item from either **Groups**, **ConfigMgr Collections**, or **Business Units**, and then click **Add Group** on the lower-left corner of the dialog.



- Repeat steps **1 through 5** to continue modifying the Base Scope to meet your needs.

### Remove Groups or Operators

Select the **ellipsis (...)** to the right of an Operator or a Group, and then select **Remove**.

- Removing the top-level Operator removes everything beneath it.
- Removing a nested Operator also removes the associated Group or Business Unit.
- Removing a Group or Business Unit removes only that Group or Business Unit.

## Verify Business Unit Members

After saving the Business Unit, click **Show Members** to display the members of the Business Unit and verify that you have populated the Business Unit as you intend.

## Create a Lab Business Unit

Designate Lab Business Units to use for testing purposes prior to production deployment.

- Make sure that the devices you want to use in the lab have the TenableClient installed and are associated with an TenableServer.
- Follow the steps to [Create a Business Unit](#). When defining the Business Unit Scopes, use **Add Devices** to identify the devices in your lab or test environment and include them in the Lab Business Unit.
- Define any other characteristics appropriate to your Lab Business Unit.

## Test Deployment Settings for Auto Remediation

Use test deployment settings to deploy patches to a specific Business Unit first, such as test or lab units, to test deployment prior to initiating a deployment to the production environment. When enabled, complete the following steps to configure the test settings.

Test Deployment Settings

Deploy to Test Group First ?

Business Unit for Test Deployment ? \*  [BROWSE](#)

Test Deployment Duration ?  Days  Hours  Minutes

Role for Test Deployment Approval ?  [BROWSE](#)

Time Until Automatic Test Deployment Approval ?  Days  Hours  Minutes

1. Select the **Deploy to Test Group First** toggle in the **Test Deployment Settings** workspace of Auto Remediation Settings. This enables automatic deployment of the Auto Remediation Settings to a test group.
2. Select **Browse** to select a **Business Unit** as the test destination.
3. Enter numbers for **Days**, **Hours**, and **Minutes** to set the **Test Deployment Duration**, which indicates how long production deployment waits after initiating test deployment to begin production deployment.
4. Select **Browse** to select a Role to receive deployment notification. This enables the **Time Until Automatic Test Deployment Approval** settings.
5. Enter numbers for **Days**, **Hours**, and **Minutes** to set the **Test Deployment Duration**, which indicates how long to wait for approval. A zero value means that the deployment waits indefinitely for approval. A non-zero value means deployment begins after the wait time passes, even if no one has approved.
6. Select **Save** on the upper left to save the test settings for the Auto Remediation.
  - a. Future deployments that match the exposure level you modified deploy to your test environment.
  - b. After verifying the operation of the remediation in your test lab, you can disable Deploy to Test Group First in the Auto Remediation Settings.

## Create a Custom Lab Business Unit

Designate Custom Business Units that a Lab Business Unit may use for testing purposes. If inherited from a parent Business Unit, values merge with the custom lab values of the parent and supersede parent values when conflicting.

## Open and Save a Business Unit Template

Each of the default Business Units provided by Tenable target production devices. Tenable recommends copying and creating new Business Units and to create Business Units for test purposes. Except for Business Units provided for Root, you can copy the default templates and save them with new details, or you can create a new Business Unit.














1. Mouse over or click **Business Units** in the left pane [Tenable Patch Management Dashboard](#), and then select **Business Units**.
2. Select the right arrow to the left of any folder to expand the list of available templates.



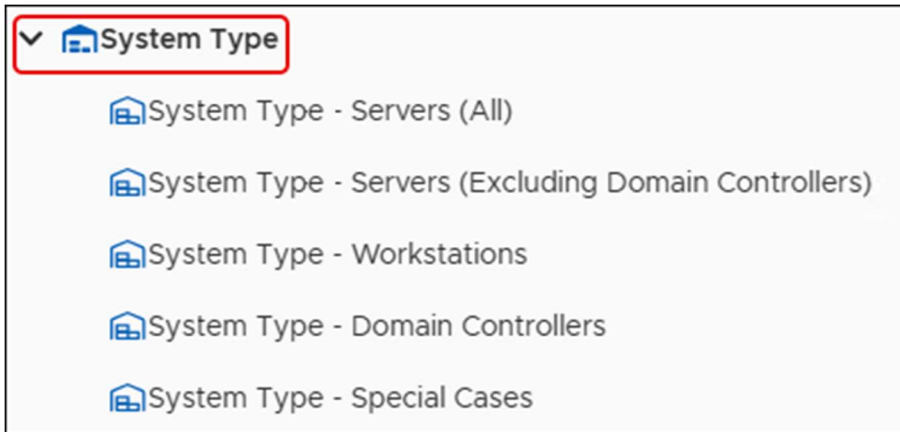
Business Units    Rollout Processes

---

Business Units [+ New](#)

- ▼  All Clients Business Unit
  - >  Root License Business Unit
    - ▼  Tenable ACR Business Units
      -  Tenable ACR 1 Business Unit
      -  Tenable ACR 2 Business Unit
      -  Tenable ACR 3 Business Unit
      -  Tenable ACR 4 Business Unit
      -  Tenable ACR 5 Business Unit
      -  Tenable ACR 6 Business Unit
      -  Tenable ACR 7 Business Unit
      -  Tenable ACR 8 Business Unit
      -  Tenable ACR 9 Business Unit
      -  Tenable ACR 10 Business Unit

3. Select the Name of a template to open it.



4. Save the template with a new title:
  - a. Select **More** in the upper-left corner of the template, and then select **Save <object> As**.
  - b. Enter a new Name for the template, and then click **OK** on the lower-left corner of the naming dialog. This returns you to the template with the new name.
  - c. Enter a detailed **Description** of the process covered in this template or leave the prepopulated description. Add a character to enable the **Save** button.
5. Select **Save**. When you have finished modifying your new template, you can drag and drop it into the folder you created (see </document/preview/447#UUID-eab9f6cf-5f54-57b7-8ef2-4c0bdb348e5f>).

## Verify Business Unit Members

After saving the Business Unit, click **Show Members** to display the members of the Business Unit and verify that you have populated the Business Unit as you intend.

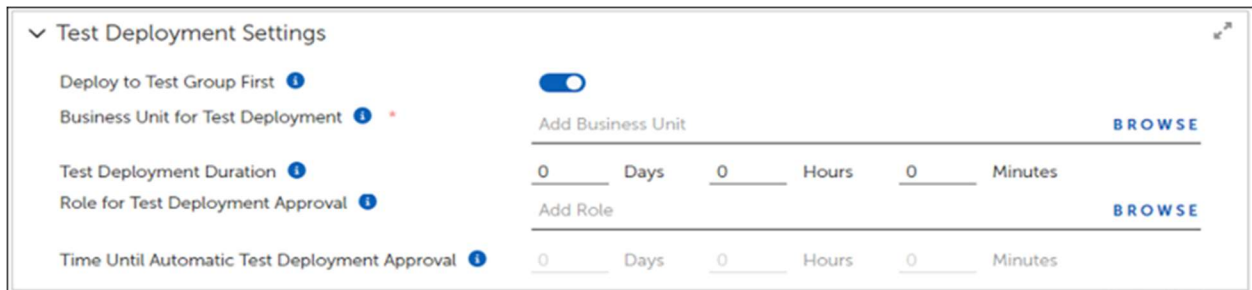
## Create a Lab Business Unit

Designate Lab Business Units to use for testing purposes prior to production deployment.

1. Make sure that the devices you want to use in the lab have the TenableClient installed and are associated with an TenableServer.
2. Follow the steps to [Create a Business Unit](#). When defining the Business Unit Scopes, use **Add Devices** to identify the devices in your lab or test environment and include them in the Lab Business Unit.
3. Define any other characteristics appropriate to your Lab Business Unit.

# Test Deployment Settings for Auto Remediation

Use test deployment settings to deploy patches to a specific Business Unit first, such as test or lab units, to test deployment prior to initiating a deployment to the production environment. When enabled, complete the following steps to configure the test settings.



The screenshot shows the 'Test Deployment Settings' workspace. It contains five main settings:

- Deploy to Test Group First**: A toggle switch that is currently turned on.
- Business Unit for Test Deployment**: A field with the text 'Add Business Unit' and a 'BROWSE' button to the right.
- Test Deployment Duration**: Three input fields for 'Days', 'Hours', and 'Minutes', each with a '0' value.
- Role for Test Deployment Approval**: A field with the text 'Add Role' and a 'BROWSE' button to the right.
- Time Until Automatic Test Deployment Approval**: Three input fields for 'Days', 'Hours', and 'Minutes', each with a '0' value.

1. Select the **Deploy to Test Group First** toggle in the **Test Deployment Settings** workspace of Auto Remediation Settings. This enables automatic deployment of the Auto Remediation Settings to a test group.
2. Select **Browse** to select a **Business Unit** as the test destination.
3. Enter numbers for **Days**, **Hours**, and **Minutes** to set the **Test Deployment Duration**, which indicates how long production deployment waits after initiating test deployment to begin production deployment.
4. Select **Browse** to select a Role to receive deployment notification. This enables the **Time Until Automatic Test Deployment Approval** settings.
5. Enter numbers for **Days**, **Hours**, and **Minutes** to set the **Test Deployment Duration**, which indicates how long to wait for approval. A zero value means that the deployment waits indefinitely for approval. A non-zero value means deployment begins after the wait time passes, even if no one has approved.
6. Select **Save** on the upper left to save the test settings for the Auto Remediation.
  - a. Future deployments that match the exposure level you modified deploy to your test environment.
  - b. After verifying the operation of the remediation in your test lab, you can disable Deploy to Test Group First in the Auto Remediation Settings.

## Create a Custom Lab Business Unit

Designate Custom Business Units that a Lab Business Unit may use for testing purposes. If inherited from a parent Business Unit, values merge with the custom lab values of the parent and supersede parent values when conflicting.

# Maintenance Windows

A Maintenance Window defines a period during which system maintenance occurs on a device. Business Unit configurations include Maintenance Window settings so administrators can schedule maintenance activities. Tenable Patch Management installs patches only during the defined Maintenance Window.

Maintenance Windows can include one or more schedules that deploy based on urgency settings (Low, Normal, High, and Critical). Urgency settings are cumulative, so higher urgencies inherit any settings specified at lower urgencies.

Overlapping time settings do not have a restrictive effect, but Tenable recommends keeping your Maintenance Window time settings simple. When a patch encounters multiple time settings for Maintenance Windows, it reviews one after another until it finds a match.

Tenable Patch Management provides built-in Start Time objects, available from the following path:

Schedules\Patching Schedules\Window Start

## Open and Save a Maintenance Window Template

1. Select **Maintenance Windows** in the left navigation menu of the [Tenable Patch Management Dashboard](#), and then click **Show All** to display the available Maintenance Window settings.

### Important

When choosing a Maintenance Window template, be sure to consider whether patch installation requires a restart. A narrow Maintenance Window can cause the restart to occur after the Maintenance Window ends.

2. Select the **Name** of an existing template to open it, and then save the template with a new Name:
  - a. Select **More** in the upper-left corner of the template, and then select **Save <object> As**.
  - b. Enter a new Name for the template, and then click **OK** on the lower-left corner of the naming dialog. This returns you to the template with the new name.
  - c. Enter a detailed **Description** of the process covered in this template or leave the prepopulated description. Add a character to enable the **Save** button.

## Add Dynamic Detection Workflow (Optional)

A Dynamic Detection workflow sets the patching Maintenance Window based on the selected workflow rather than a set schedule. For more information, enter a support ticket and request help from Tenable Customer Support.

1. Scroll down to **Dynamic Settings**, in an open Maintenance Window template.

2. Select **Browse** to the right of **Add Workflow**. This opens the **Add Workflow** dialog.
3. Select a workflow from the table, and then click **Add Workflow** in the lower-left corner.

## Apply to All Urgencies

When enabled (default) all patches use the same Maintenance Window based on the highest level of urgency.

1. Select **+ Create Maintenance Window** in the **Maintenance Windows by Urgency** section of the Maintenance Window template.
2. Select **Apply to All Urgencies** to enable or disable using the same Maintenance Window settings for all urgencies:
  - a. If you enable this setting (default) you do not need to create a Maintenance Window for all urgencies. Skip to [Save and Deploy the Maintenance Window](#).
  - b. If you disable this setting, continue to [Create a Maintenance Window](#).

## Set Maintenance Windows by Urgency

To set a Maintenance Window to deploy patches that have Low and Normal urgency settings and ignore patches with High and Critical urgency settings, leave the High and Critical urgency settings in their respective default settings of NULL.

## Create a Maintenance Window

The configurations use the same template requirements to create a single maintenance window for all urgencies or to create individual windows for specific urgency levels. The difference between where you access the appropriate templates is whether you choose the enable Apply to All Urgencies to create a single maintenance window or disable it to create individual maintenance windows for each urgency level.

1. Select **+ Create Maintenance Window** in the **Maintenance Windows by Urgency** section of the Maintenance Window template.
2. Select **Browse** next to **Add Schedule**, and then expand the **Patching Schedules** folder to see available schedules.
3. Select a schedule that sets the start time for the Maintenance Window, and then click **Add Schedule** to close the dialog.
4. Enter the number of Hours, Minutes, or Seconds until the Maintenance Window closes, and then click **Create Maintenance Window**.

## Set the All Urgencies Override Duration

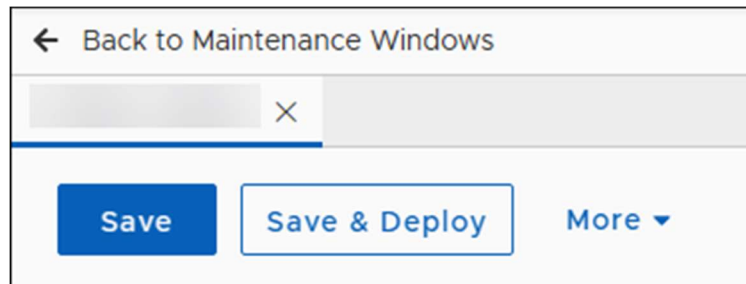
An override duration for the **All Urgencies Maintenance Window** sets the amount of time to wait for the Maintenance Window to open for all urgency level updates. After this time, the system overrides the Maintenance Window setting.

Enter the number of Hours, Minutes, or Seconds to wait for the Maintenance Window to open before allowing an override.

## Save and Deploy the Maintenance Window

You must deploy a Maintenance Window to make it available for use in a template. If you update a Maintenance Window template that was previously deployed, you must save and deploy it again for the changes to take effect.

1. Complete the Maintenance Window configuration (see [Open and Save a Maintenance Window Template](#)).
2. Select **Save & Deploy** to save and deploy your configuration:
  - a. If you want to deploy later, click **Save**.
  - b. Be sure to return and **Deploy** the Maintenance Window template to make it available for use.



# User Interaction Settings

User Interaction Settings control what the user sees and what options they have for interacting with patching notifications and required reboots. These settings use either Toast notifications or Popup notifications. A User Interaction configuration may use the same settings for all urgencies or use them separately for individual urgency settings (Low, Normal, High, and Critical).

## Understanding User Interaction Settings

You can customize User Interaction Settings and add them to a patch deployment for Business Units. Child Business Units may inherit these settings from a parent Business Unit. Depending on the urgency of the notification, you can set interaction options for the following scenarios:

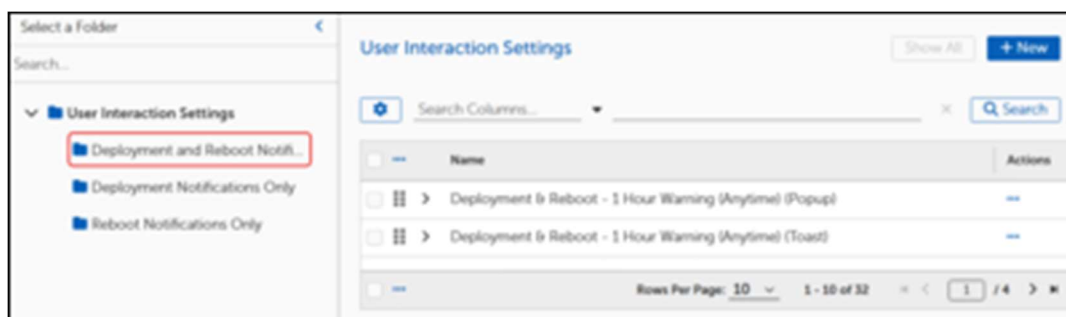
- Pre-install Notification
- Install Notification
- App Closure Notification
- Reboot Notification

You can customize the notification text, set the time between notifications, and set the maximum deferral time.

## Create User Interaction Settings

### Open and Save a User Interaction Template

1. Select **User Interaction Settings** in the left navigation menu of the [Tenable Patch Management Dashboard](#).

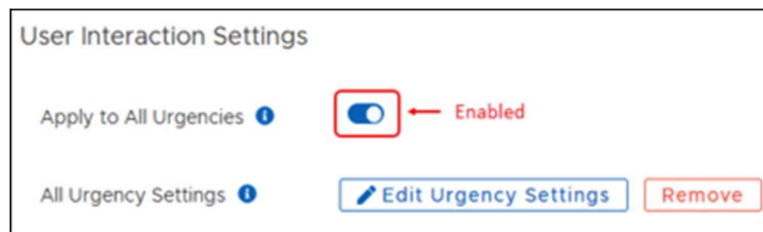


2. Select the Name of an existing template to open it. This example uses the Deployment & Reboot - 1 Hour Warning (Anytime)(Toast) template.
3. Save the template with a new Name:
  - a. Select **More** in the upper-left corner of the template, and then select **Save <object> As**.

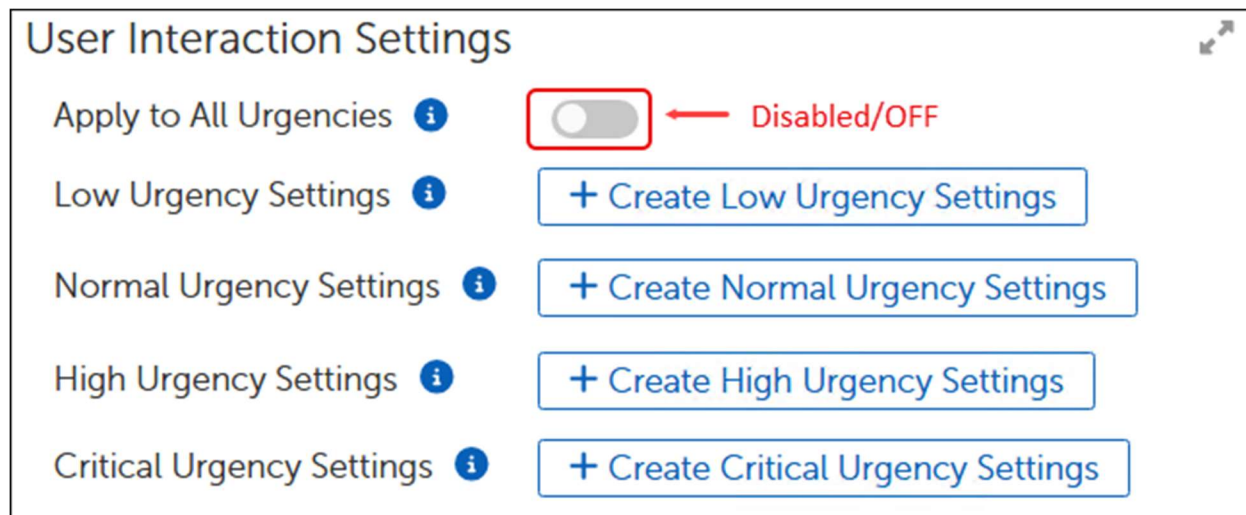
- b. Enter a new Name for the template, and then click **OK** on the lower-left corner of the naming dialog. This returns you to the template with the new name.
- c. Enter a detailed **Description** of the process covered in this template or leave the prepopulated description. Add a character to enable the **Save** button.

## Edit or Create Urgency Settings

1. Scroll down to **User Interaction Settings** in an open User Interaction Settings template:
  - a. When working from an existing template, these settings reflect the needs of the template you chose to modify. With **Apply to All Urgencies** enabled, you have the option to create a single set of urgency settings that apply to all urgency levels (Low, Normal, High, and Critical).



- b. When working from a new template, these settings reflect the default settings for a new User Interaction Settings template ( **+ New** ). With **Apply to All Urgencies** disabled, you have options to create urgency settings for each level.



2. Select the **Apply to All Urgencies** toggle to enable or disable whether to set urgencies the same for all levels:
  - a. Each setting, including **Apply to All Urgencies**, uses the same template layout and fields.
  - b. This example uses the **Apply to All Urgencies** setting.
3. [Set deployment notification settings.](#)



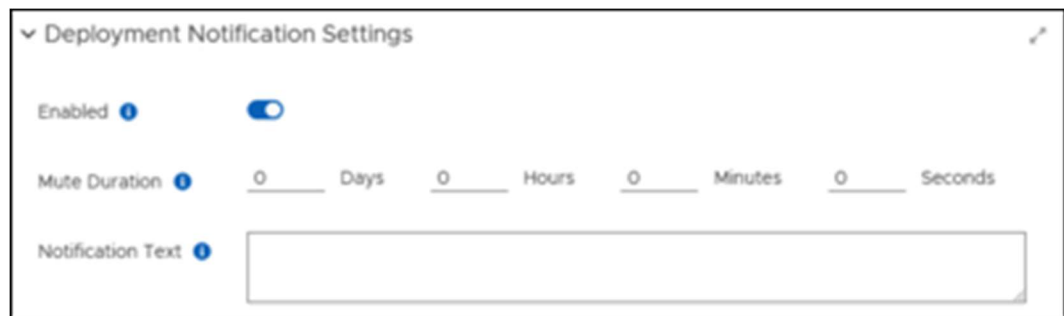
## Set Deployment Notification Settings

1. Select **Edit Urgency Settings** in an open User Interaction Settings template.

### Tip

When you need to exit the urgency settings for User Interaction Settings, click **OK** on the lower-left corner of the dialog to return to the User Interaction Settings template.

2. In the **Deployment Notification Settings**, click the **Enabled** toggle to enable or disable whether users see this notification when a deployment begins on their device:
  - a. If enabled, continue with the next step.
  - b. If disabled, skip to [Create System Reboot Notification Settings](#).



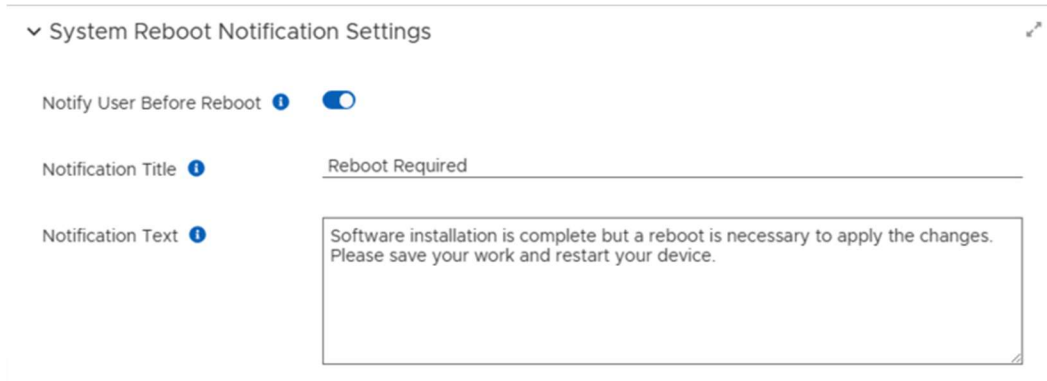
The screenshot shows a dialog box titled "Deployment Notification Settings". It contains three main sections: "Enabled" with a toggle switch that is currently turned on; "Mute Duration" with four input fields for "Days", "Hours", "Minutes", and "Seconds", all of which are set to "0"; and "Notification Text" with an empty text input box.

3. Set the **Mute Duration** to the number of Hours, Days, Minutes, or Seconds that the user may choose to mute the notification. When set to zero (0), the user does not receive any mute options.
4. Enter **Notification Text** in the text box. The user will see this text when the notification arrives on their device.
5. [Create System Reboot Notification Settings](#).

## Create System Reboot Notification Settings

To notify users when an update requires a reboot, complete the following steps:

1. Scroll down to **System Reboot Notification Settings** in an open User Interaction Settings template.
2. Decide whether to apply the settings to All Urgencies (defaults to disabled):

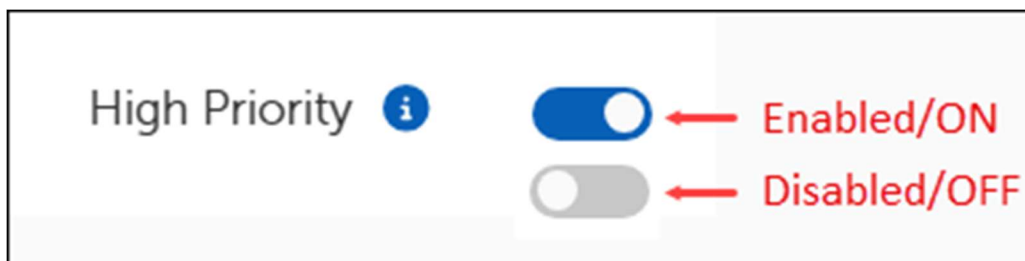


- a. If yes, click the **Apply to All Urgencies** toggle to enable the same User Interaction Settings for all users, and then continue with the next step.
  - b. If no, click the **Apply to All Urgencies** toggle to disable (default) user notification, and then click **OK** at the bottom left of the dialog to return to the settings template.
3. Enter a **Notification Title**, and then enter the **Notification Text** in the text box. This is the information the user sees when the notification arrives on the device.
  4. <urn:resource:component:611>

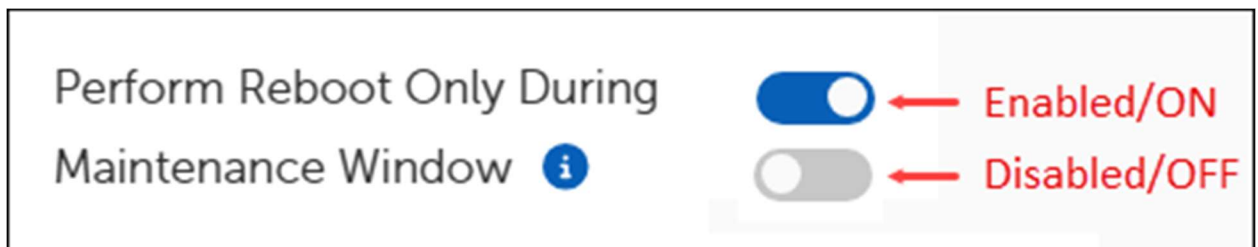
#### Configure Reboot Notification and Snooze Settings

With **Notify User Before Reboot** enabled, you may set other conditions related to the reboot:

1. Select the **High Priority** toggle to enable or disable whether the user may dismiss notifications generated by the User Interaction Settings. Defaults to disabled in a new template:



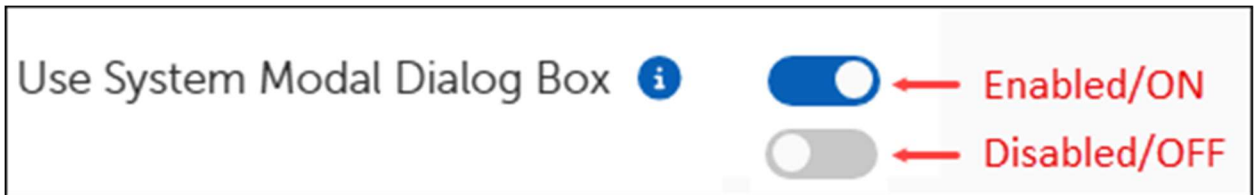
2. Select the **Perform Reboot Only During Maintenance Window** toggle to enable or disable whether reboots occur only during a maintenance window. Defaults to disabled in a new template:



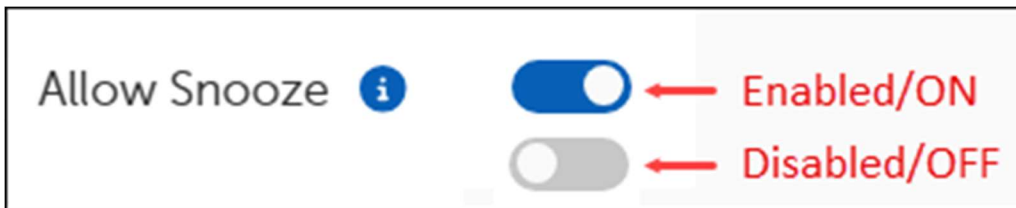
3. Enter the number of **Days, Hours, Minutes, or Seconds** the user has until the reboot occurs. If zero, OneSite provides no warning to the user. Other settings tell the user how much time they have before the reboot occurs.



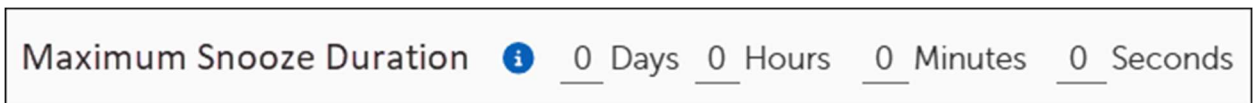
4. Select the **Use System Modal Dialog Box** to enable or disable whether the Dialog is a system modal. When enabled, the dialog appears in front of, and disables, the main window.



5. Select the **Allow Snooze** toggle to enable or disable whether the user may snooze the reboot:



Set the maximum snooze duration a user may select. The user sees only the options for which you set a duration.



6. Select **OK** to return to the User Interaction Settings template, and then [Save and Deploy User Interaction Settings](#)

## Save and Deploy User Interaction Settings

After creating and configuring or editing User Interaction Settings, you must deploy them. Otherwise, the User Interaction Settings are not available in the list of templates when you add **User Interaction Settings** to a Business Unit.

1. Select **User Interaction Settings** from in the left navigation menu of the [Tenable Patch Management Dashboard](#).
2. Select the **Name** of a User Interaction template to open it or [Create User Interaction Settings](#).

3. Make any necessary changes using the tasks provided in [Create User Interaction Settings](#) and save them so that you return to the **General Settings** section of the template.
4. Choose whether to **Save**, **Deploy**, or **Save & Deploy** the template.
  - a. If you created a new User Interaction template and it is ready to deploy, click **Deploy** next to **Deployment Status** in the upper-left corner of the template.
  - b. If you changed an existing template and it is ready to deploy, click **Save & Deploy**.
  - c. If you intend to make more changes before deploying, click **Save**.
5. Select **<- Back to User Interaction Settings**.

# Customized Products

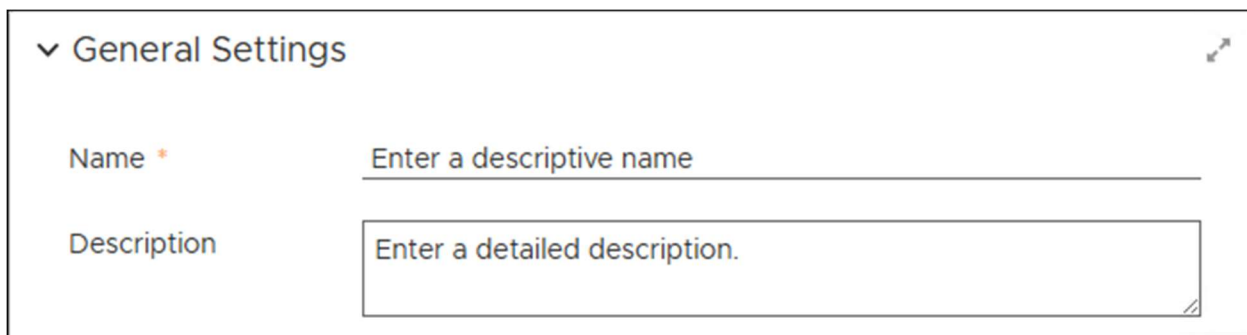
Software products and patches sometimes require user interaction when installing. Users enter details such as license information or request to show a menu at startup. Other default settings include auto update, or desktop shortcuts.

Tenable Patch Management uses Customized Product settings to include information or change defaults when installing products on managed devices.

## Manage Settings for Customized Products

### Open and Save a Customized Product Template

1. Select **Customized Products** on the left navigation menu of the [Tenable Patch Management Dashboard](#).
2. Select **+ New** in the upper-right corner to open a new template:



▼ General Settings

Name \*

Description

- a. Enter a **Name** that identifies your template.
  - b. Enter a detailed **Description**, and then click **Save** on the upper left corner.
3. Continue with [Add a Deployment Wave](#).

### Add a Deployment Wave to a Customized Product Template

The Deployment Wave contains the Business Units that use the product you intend to target.

1. Select **Browse** next to **Add Deployment Wave** in an open [Customized Product Template](#).

General Settings

Name \*

Description

Deployment Wave ⓘ \*

Target Product ⓘ \*

2. Select the **Deployment Wave** to which these Customized Product settings apply on the **Deployment Waves** dialog.
3. Select **Add Deployment Wave** on the lower-left corner of the **Deployment Waves** dialog.
4. Select **Save** on the upper-left corner of the template to save your changes and continue editing.
5. Continue with [Add a Target Product](#).

## Add a Target Product

1. Select **Browse** next to **Add Software Product** in an open [Customized Product Template](#).
2. Enter the Name of the product you want to customize in the search field, and then click **Search**.

Software Products

Search Columns...

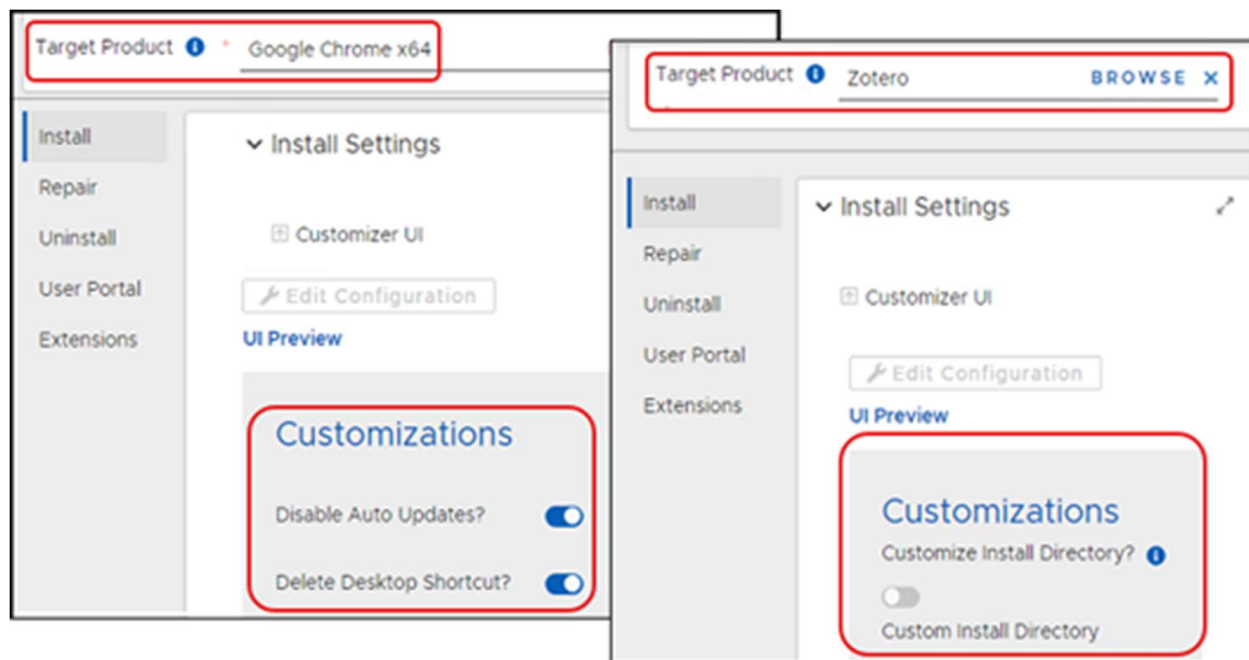
<input type="checkbox"/>	...	Name	Actions
<input checked="" type="checkbox"/>	>	Google Chrome x64	...
<input type="checkbox"/>	>	Google Chrome x86	...

3. Select the **Software Product** you want to customize. You can target only one Software Product in each Customized Product entry.

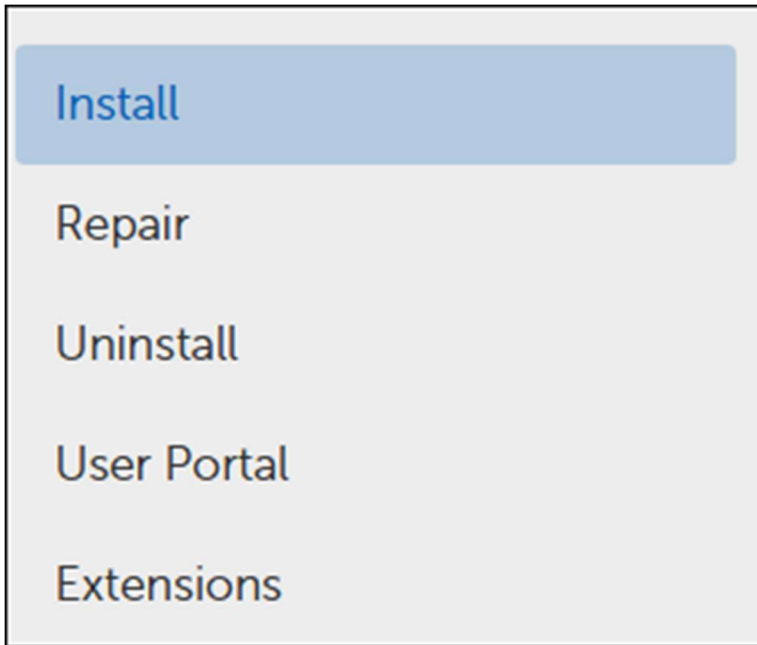
4. Select **Add Software Product** to populate the configurable items in the static list of **Install Settings**. Settings change depending on the Target Product.
5. Select **Save** in the upper-left corner of the template to save your changes.
6. Continue with [Configure Software Install Settings](#).

## Configure Software Install Settings

1. Select **Install** in the left column of **Install Settings**.
  - a. The list of available customizations reflects the settings you can customize in the software product you selected.
  - b. Settings change depending on the Target Product.



2. Select each of the remaining items in the list of customizations. If the software you chose allows changes or input for any of these settings, review and create the responses you need.



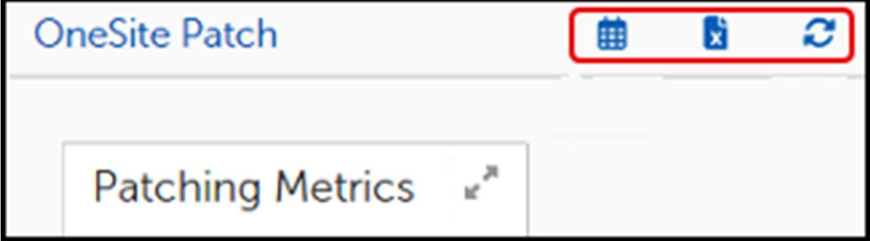
3. Select **Save** at the upper left to save your progress:
  - a. Check the **Error View** and resolve any errors.
  - b. Select **Save** again if you make any changes.
4. Select **<-- Back to Customized Products** above the **General Settings** box. The changes you have made take effect the next time the associated Deployment Wave runs.



# Navigating the Tenable Patch Management Dashboard


## Date Settings, Export, and Refresh

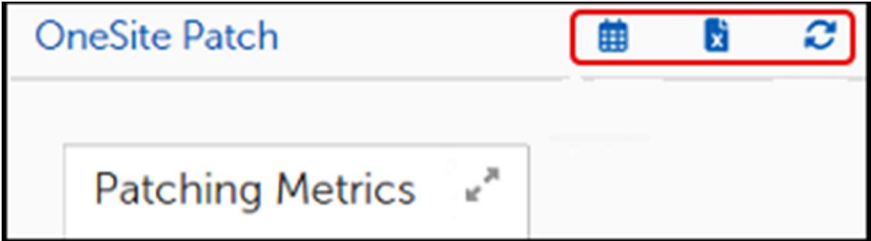
The three small icons (Calendar, Export and Refresh) on the upper right of the Tenable Patch Management Home page and on any of the Patching Analytics pages (Overview, Products, Patches, or Devices) provide options to customize the date settings to a particular date range, choose some or all widgets on the page for exporting data, and refresh the data shown on the page.



## Set Dates for Status Views

The dashboard Date Settings default to the current day. Use the following steps to change the date settings:

1. Select  on the upper-right corner of the **Home** page or from any **Patching Analytics** page.



2. Enter the **starting and ending dates** for the range you want to view or use the calendar icon to the right of each date field to choose a date from the calendar.

Dashboard Date Settings

Start Time Choose Date

End Time Choose Date

Window Type

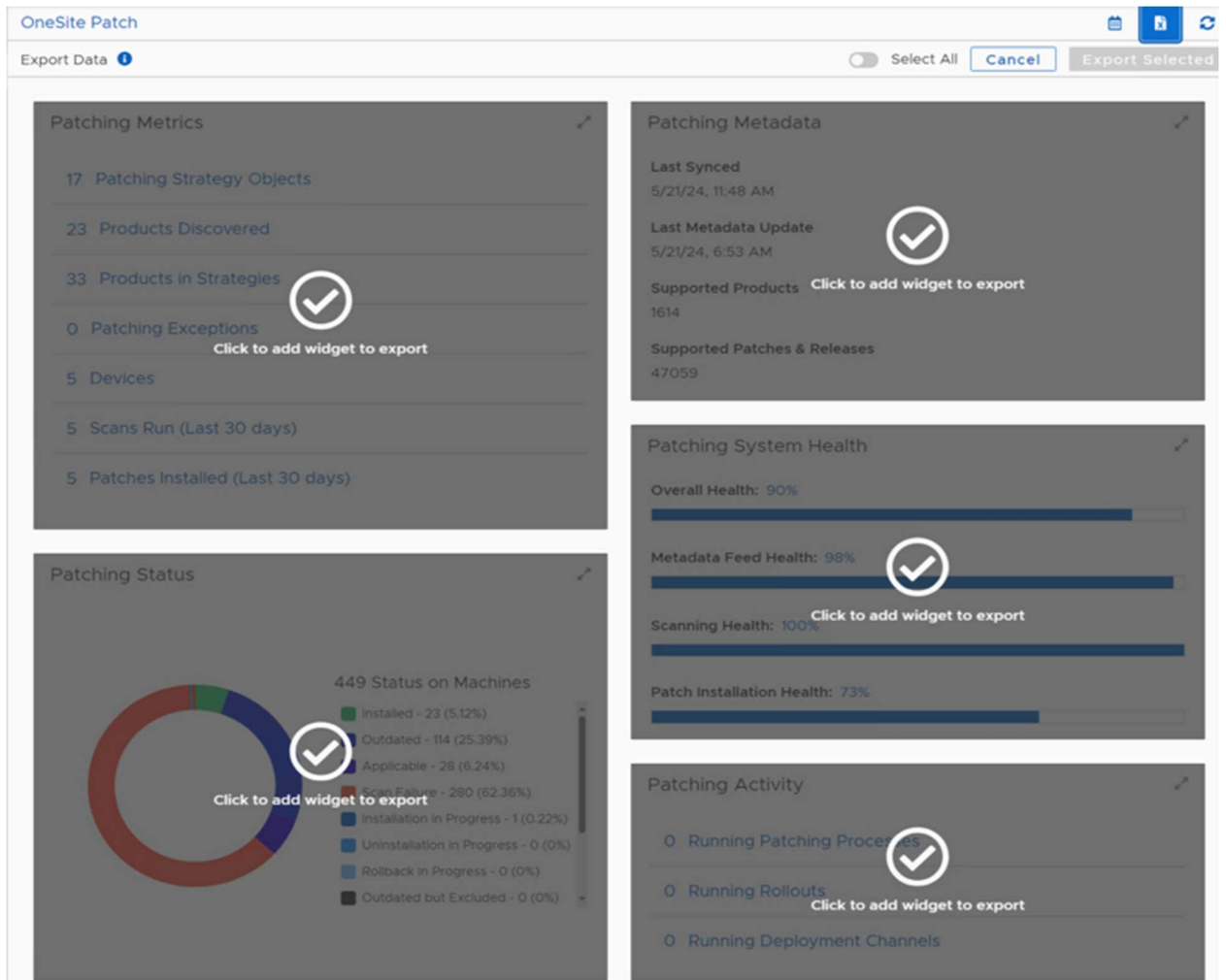
- Day
- Week
- Month
- Quarter
- Year

Update Cancel

3. Select the **Window Type** setting, and then select whether to view data by **Day**, **Week**, **Month**, **Quarter**, or **Year** from the dropdown menu.
4. Select **Update** to save the settings. The view details update automatically for the date range you entered.

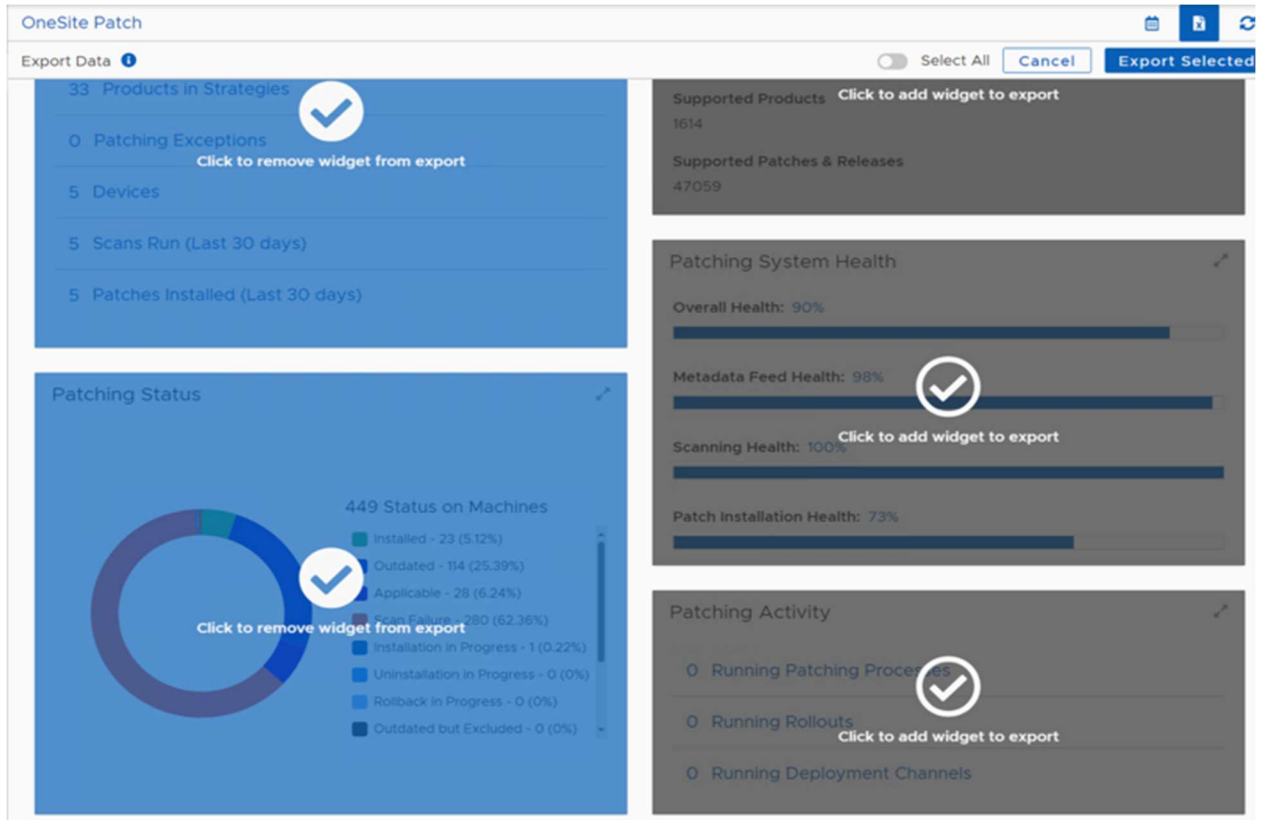
## Export Widget Data

1. Select the Export icon on the upper-right corner of the **Home** page or on any **Patching Analytics** page. This changes the view to an **Export Data** page, which highlights in gray the widgets you can export.




2. Choose which widgets to export:

- a. Select **Select All** at the top of the page to export all widgets.
- b. Select an individual widget to export a single widget, or click multiple widgets to export.



3. Select **Export Selected** on the upper-right corner. The system downloads the export to the server with an `.xlsx` extension.

## Refresh the Status View

Select the Refresh icon  on the upper-right corner of the **Home** page or on any **Patching Analytics** page. This refreshes the data on the status pages to reflect the most current information if your customized date range includes the current date.

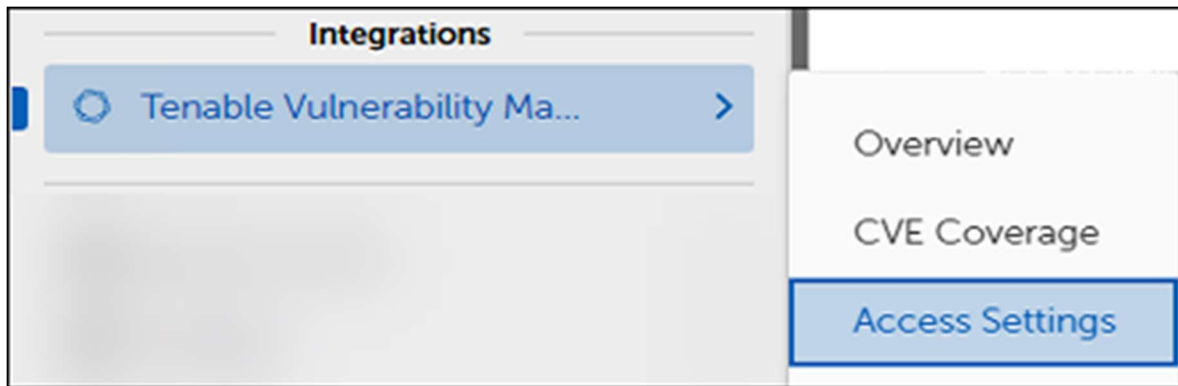
## Tenable Patch Management Menu

The left navigation menu lists the object available for configuring or monitoring in the Tenable Patch Management product. Those items with additional choices include a pop-out menu indicated by a right-angle bracket (`>`).

The left pane stays the same, regardless of which object you choose, and consists of three sections.

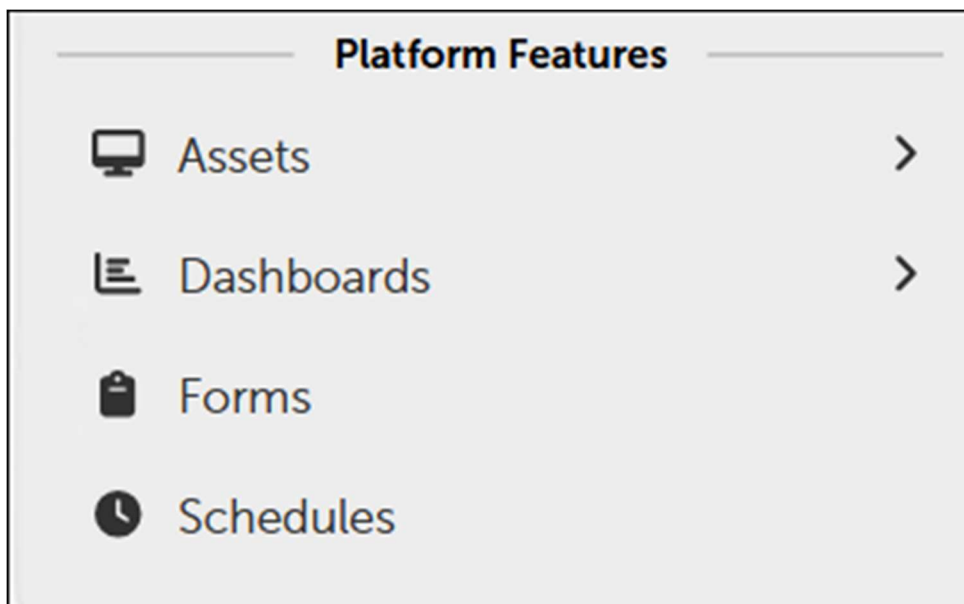
## Integration Menu

The Integrations menu provides access for Tenable partners to integrate client data and create patching scenarios to update their hosts or or devices.




## Platform Features Menu

These are common features available from every menu in Tenable Patch Management and across the full platform of OneSite products.



## Tenable Patch Management Dashboard and Performance Widgets

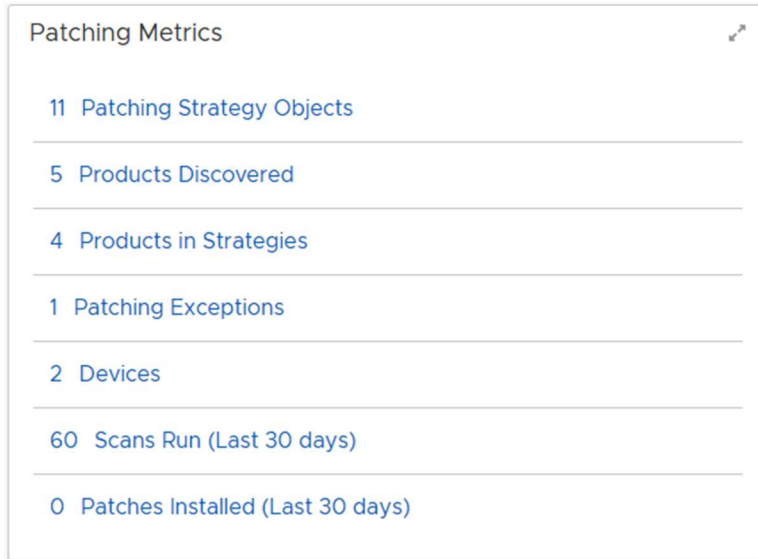
The Tenable Patch Management Home page shows several widgets that provide patching details for the environment. You can expand each widget to a full page using the  icon at the upper-right corner of each widget.

The layout of these widgets depends on the size of your computer monitor.

Collectively, these widgets supply information about the overall state of patches in your environment based on Tenable Patch Management system scans. The **Patching Analytics** menus show more detail about specific products, patches, and devices.

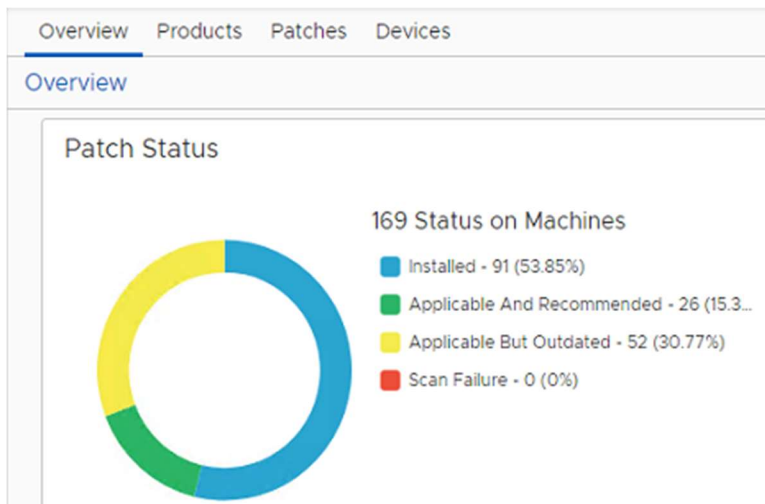
## Patching Metrics

Accessed from the **Home** screen, **Patching Metrics** show basic patch related information specific to your environment based on scanning requirements. Details include a quantitative summary of the item within the environment. Each item links to the **Patching Analytics Overview**, which includes a separate and detailed view for **Products**, **Patches**, or **Devices**.



## Patching Status

Provides an aggregate view of patching statuses reported in the environment including the combined total of statuses from all machines. The percentages that follow show what percentage of the reported statuses fall into each category.



## Overall Compliance

Graphs the overall compliance of devices in the environment with the patch requirements.

### Overall Compliance

100%

Overall Compliance



## Risk Score

Returns the average risk score for all products identified in the metadata, and shows the average Risk Score. Depending on the dates chosen for the dashboard reporting, the administrator can see the changes in risk over time. See [Date Settings for Status Views](#) for more information.

### Risk Score

0

Average Risk Score



The average number reported here reflects a customized risk assessment for each product based on patch status, applicability, and weight of risk.

## Patching Metadata

Summarizes the status of the latest endpoint scans and client product inventory updates. Metadata includes details about the products, patches, and updates approved by the company for installation. The **Patch Metadata** summary tells the administrator when the TenableServer and TenableClients last synchronized with the Metadata Server and when the last sync resulted in an update to the clients.

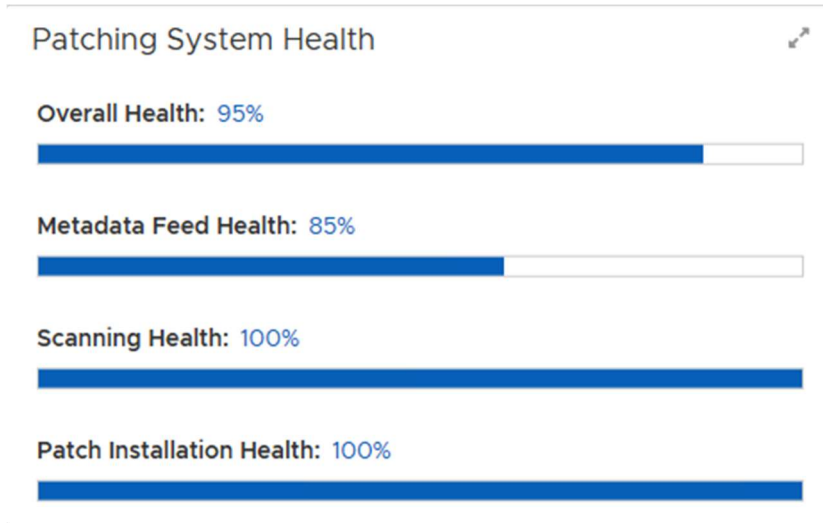
### Patching Metadata

Last Synced	9/29/23, 2:16 PM
Last Metadata Update	9/26/23, 7:06 AM
Supported Products	818
Supported Patches & Releases	18670

In addition, the **Patching Metadata** summary shows the number of supported products in the environment and the number of support patches and releases related to those supported products.

## Patching System Health

Shows the health of the overall patching system, including metadata feed, scanning, and patch installation. Use this information to identify any issues that require attention.



## Patching Activity

Shows a quantitative summary of the number of currently running patch processes, rollouts, and deployment channels in the environment.





## Top 5 Non-Compliant Products

Displays the products that are most out of compliance and by what percentage. Scanning compares the detected product versions with the established current product version and reports the top five products contributing to the [Overall Compliance](#) score.

If compliance is the main area of concern, the administrator can review these top five products and take direct action to reduce their non-compliance.

Top 5 Non-Compliant Products			
<input type="checkbox"/> ...	Product Name	Compliance Status	Actions
<input type="checkbox"/>	Microsoft Analysis Services OLE DB Provider ...	<input type="text"/> 0%	...
<input type="checkbox"/>	Microsoft Orca	<input type="text"/> 0%	...
<input type="checkbox"/>	Microsoft Visual C++ 2015-2022 Redistribut...	<input type="text"/> 0%	...
<input type="checkbox"/>	Microsoft Visual C++ 2015-2022 Redistribut...	<input type="text"/> 0%	...
<input type="checkbox"/>	SQL Server Management Studio x64	<input type="text"/> 0%	...

Rows Per Page:  1 - 5 of 5  1 / 1

## Top 5 Missing Patches

Displays the most critical patches contributing to the Risk Score and by what percentage (highest to lowest). Scanning compares the risk score of missing patches and reports these top five as those contributing most to the [Risk Score](#).

Top 5 Missing Patches	
No data provided	

If risk is the main area of concern, the administrator can review each of these top five patches and take direct action to complete the updates and reduce the Risk Score.

# Appendices

## Software Products Library

Tenable Patch Management supports patching for multiple versions of products through a partnership with Tenable. A dedicated team of metadata analysts constantly expands the Software Products Library (metadata catalog) with new products and new releases for existing products, covering most of the installed software within your environment.

## Metadata Catalog

Tenable has a dedicated team that focuses on metadata. This team monitors the vendors and products we support and regularly searches for additional products to add to our metadata catalog.

The metadata team receives automatic notification within 24 hours of an update release. The team uses Virus Total to scan all downloaded content in an isolated and secured environment. The Virus Total score for the content must be zero (0) before Tenable publishes the content to the Content Delivery Network (CDN). The CDN converts the update to our native content format and makes it accessible to Tenable customers.

When testing a new release, the team installs the prior version. The team also tests the upgrade using the new release. After a successful upgrade, the team opens the application to verify a quality installation. The team contacts the vendor for support if it identifies issues during installation.

After confirming a successful update, the team creates, reviews, and approves the metadata before adding it to the metadata catalog. Every customer server with a license downloads the metadata catalog update.

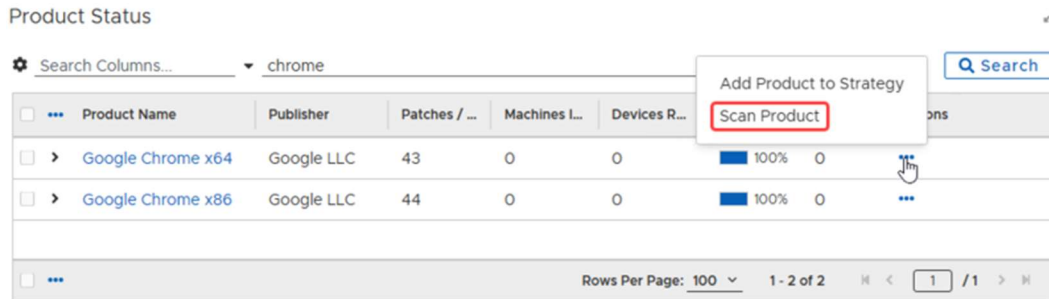
## Endpoint Scans

The endpoint scanning timeline for patch and product status defaults to once daily. Administrators can start and customize scans at any time using the **Request Scan** feature.

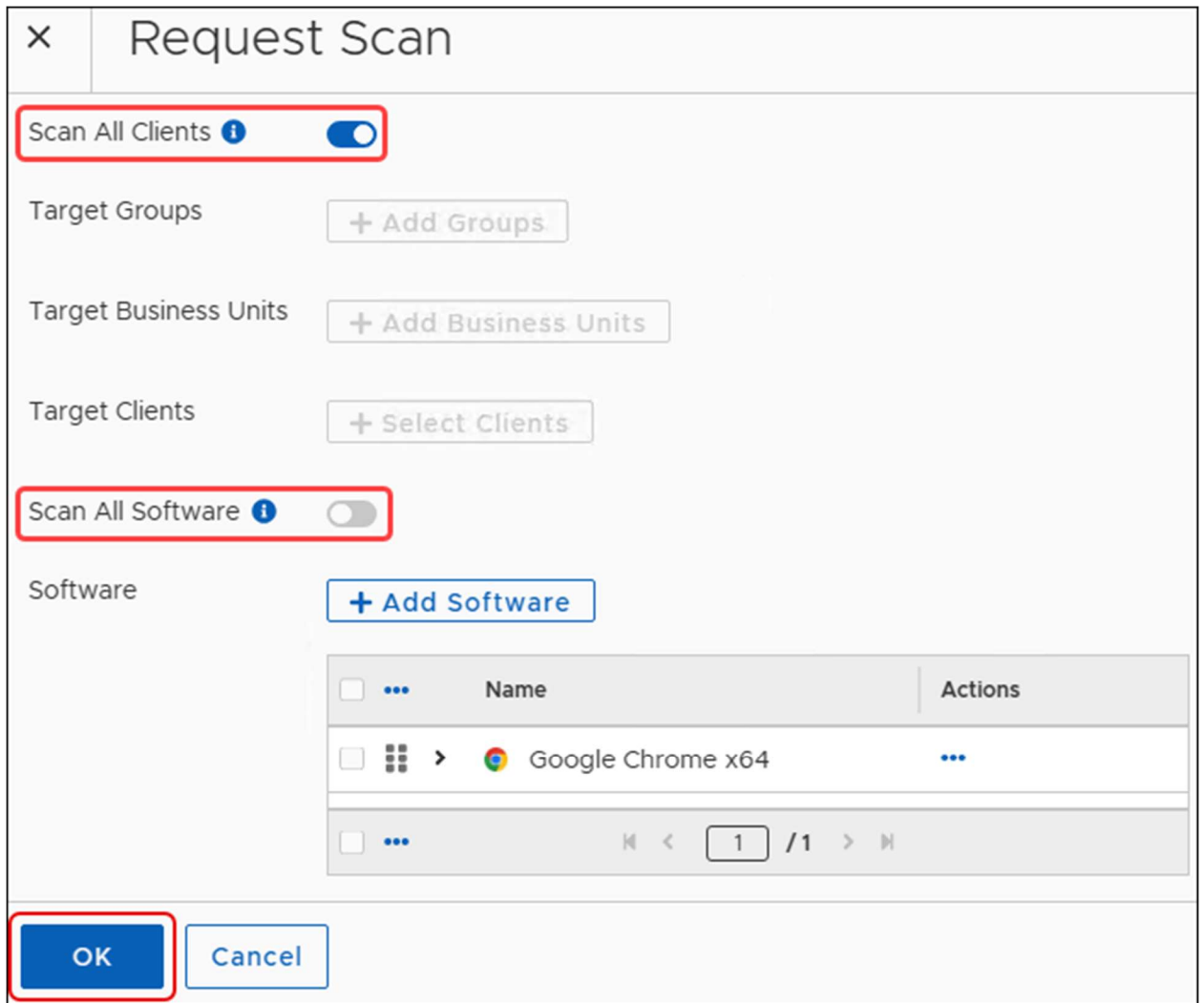
## Request a Scan

1. From the Tenable Patch Management Home menu in the left navigation panel, hover over **Patching Analytics**, and then select **Overview**, **Products**, **Patches**, or **Devices**.
2. Scroll down to the last table on the screen. The table name changes depending on the option you choose:
  - a. **Overview – Product Status** table; Actions include Scan Product and Reset Deployment Failures for Product.
  - b. **Products – Product Status** table; Actions include Scan Product and Reset Deployment Failures for Product.

- a. **Patches – Patch Status** table. Actions include Scan Patch and Reset Deployment Failures for Patch.
  - b. **Devices – Device Status** table; Actions include Scan Product
3. Select the **ellipsis (...)** in the **Actions** column for the product, overview, or device you want to scan.



4. Select **Scan Product**.
  - a. This opens the **Request Scan** dialog and prepopulates the Software section with all the software available on the item you chose to scan.
  - b. **Request Scan** defaults to Scan All Software.
5. Select the **Scan All Clients** toggle to enable or disable scanning all clients. If disabled, add targets to scan.



6. Select the **Scan All Software** toggle to enable or disable (default) scanning all software.
7. Select **OK**. The system briefly displays a message Successfully Requested Client Scan.