Tenable Patch Management Enterprise User Guide

Last Revised: December 20, 2024

Table of Contents

Getting Started with Tenable Patch Management

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

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

Access Server logs using the ⚙ on the Admin Portal or by navigating to `<path>///Tenable/PatchServer/Logs`.

Access Client logs from `<path>/Tenable/PatchServer///Logs`.

Customer Support

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

Tenable Patch Management Admin Portal

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

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 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 Tenable 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 **Log In**.

4. If you are unable to log in using your Active Directory login with Mozilla Firefox, see Resolve Mozilla Firefox Active Directory Login Issue.

   c.

Resolve Mozilla Firefox Active Directory Login Issue

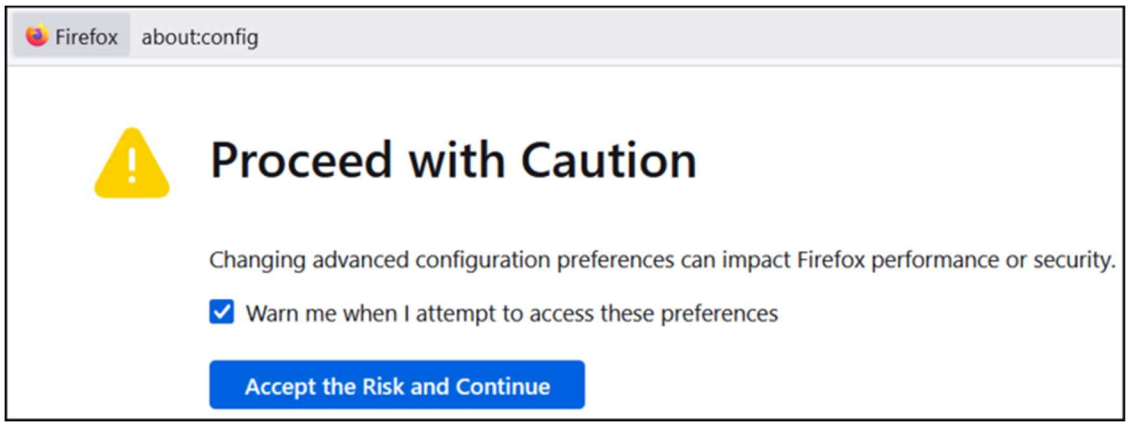
To access the Admin Portal using Active Directory, Mozilla Firefox requires adding the Tenable Server as a trusted URI to enable SSPI/Kerberos authentication. If you receive the following message when using Mozilla Firefox to log into into the Admin Portal using Active Directory, use the steps provided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

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

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

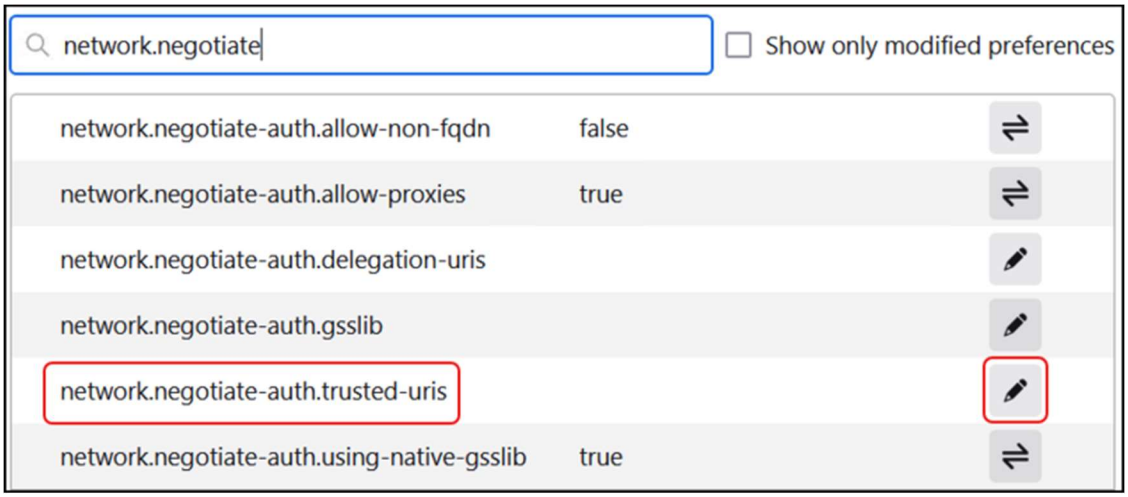
   `about:config`

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



7. 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.

8. Select **Log in with Active Directory**.

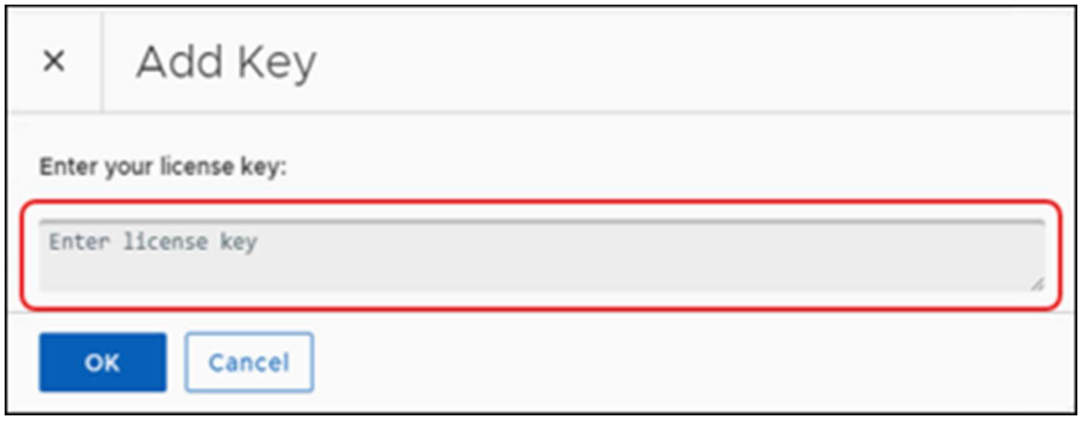
Licensing Tenable Patch Management

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. If you entered your license key during installation, you do not need to renter it here.

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, Tenable sends a status update when it has enabled the installed solution.

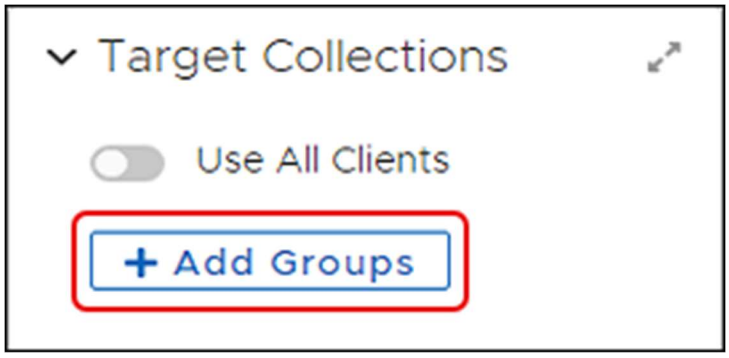
Add a Licensed Product to a Collection Group

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

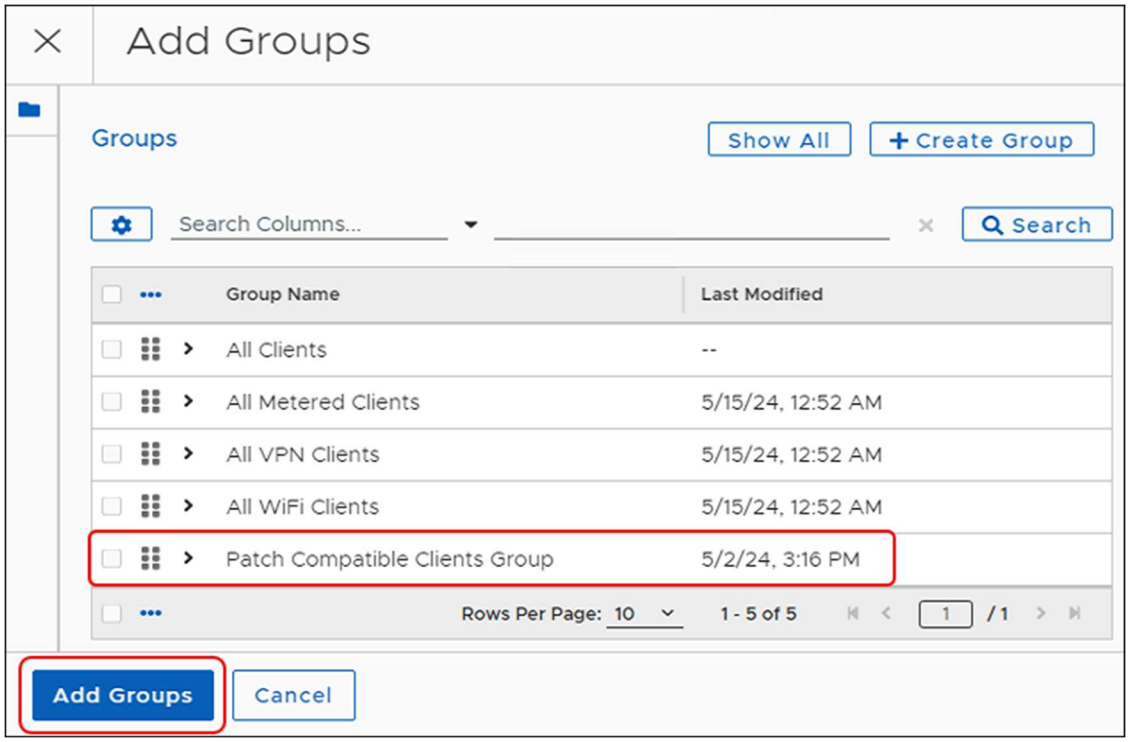
Caution

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

1. Select the Tenable Patch Management 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 Enterprise Dashboard

Use the Tenable Patch Management dashboard, available from the Tenable Admin Portal, to manage your patching strategies, review patching status, and more.

Access the Tenable Patch Management Dashboard

Open the Tenable Patch Management dashboard from the Tenable Admin Portal using one of the following methods:

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

  This opens the Tenable Patch Management Dashboard.

Integrate Tenable Vulnerability Management

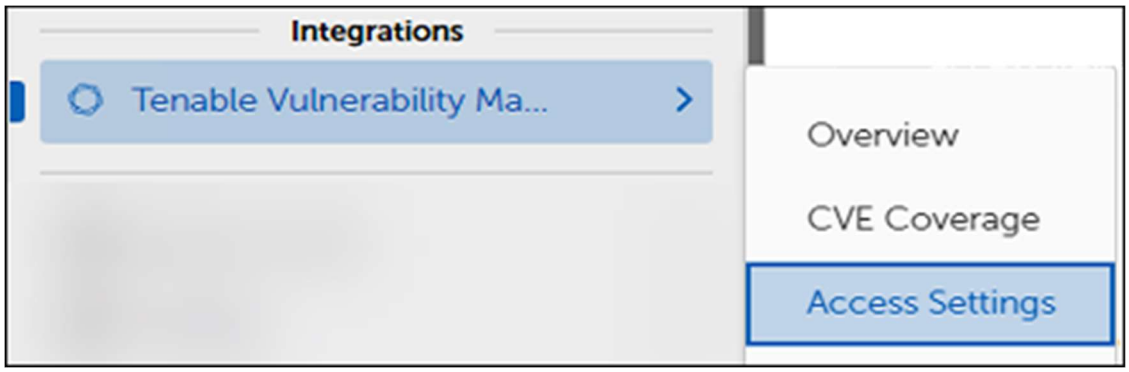
With this integration, a configuration automatically patches vulnerabilities identified by Tenable Security Center and Tenable Vulnerability Management. This integration bridges the gap between identifying vulnerabilities and immediately patching them, increasing the speed of securing multiple devices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

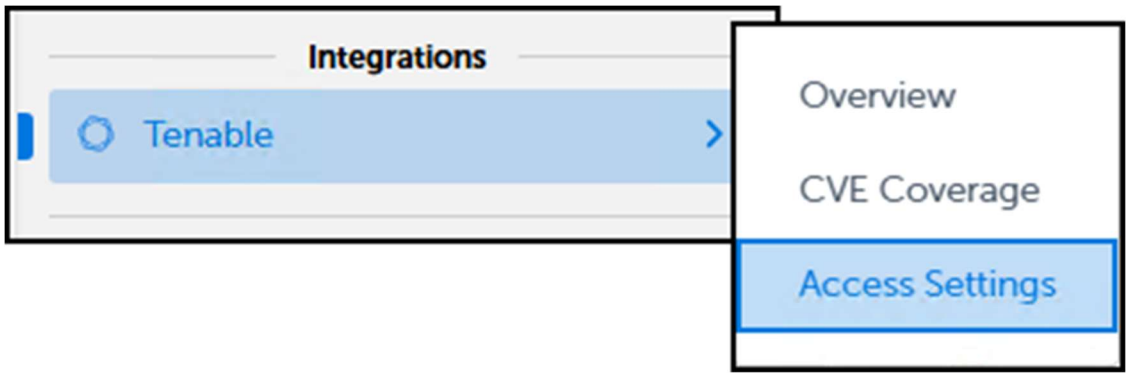


Add Tenable Access Settings to Tenable Patch Management

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 Admin Portal and open the Patch Dashboard.

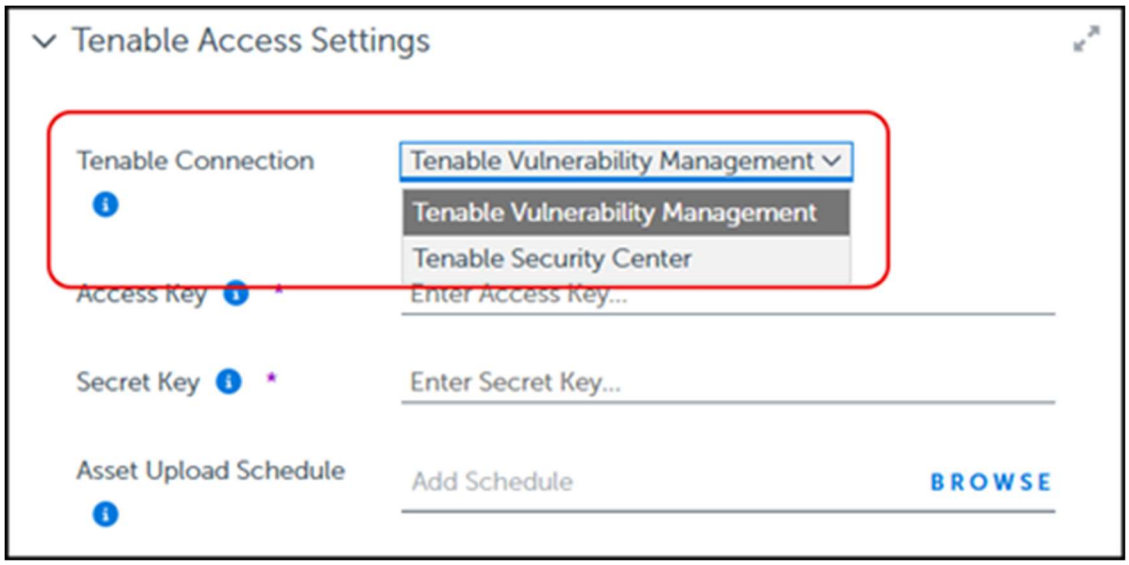
3. Select **Tenable** in the left navigation menu of the dashboard, and then select **Access Settings**.



4. Select the Tenable Connection you want to create:

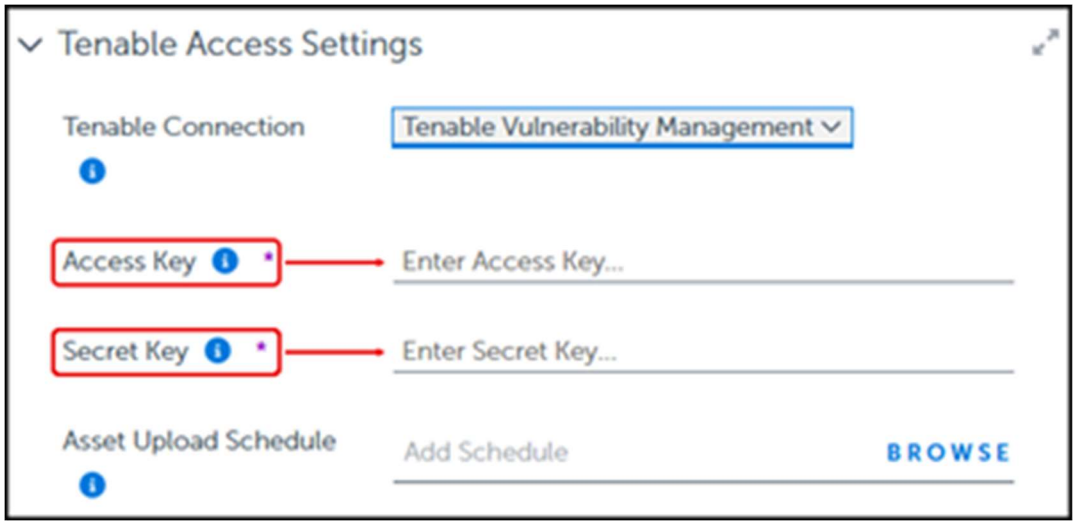
   a. Select Tenable Vulnerability Management, and then see Configure Tenable Vulnerability Management Settings.

   b. Select Tenable Security Center, and then see Configure Tenable Security Center Settings.



Configure Tenable Vulnerability Management Settings

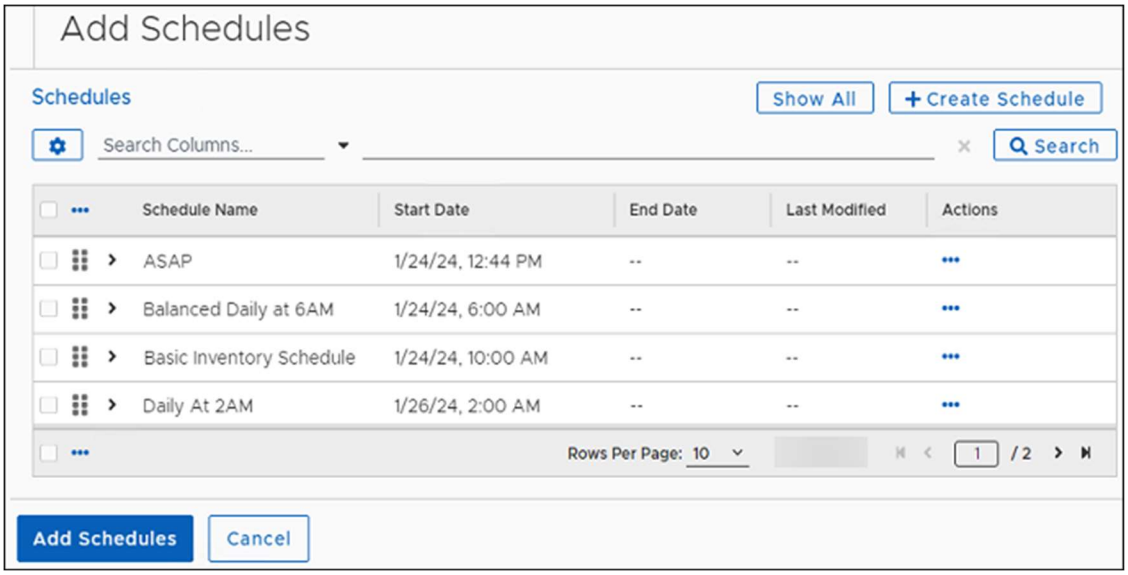
1. Enter the **Access Key** and the **Secret Key** for Tenable Vulnerability Management.



2. 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.



3. Select Save on the upper-left corner of the dialog:

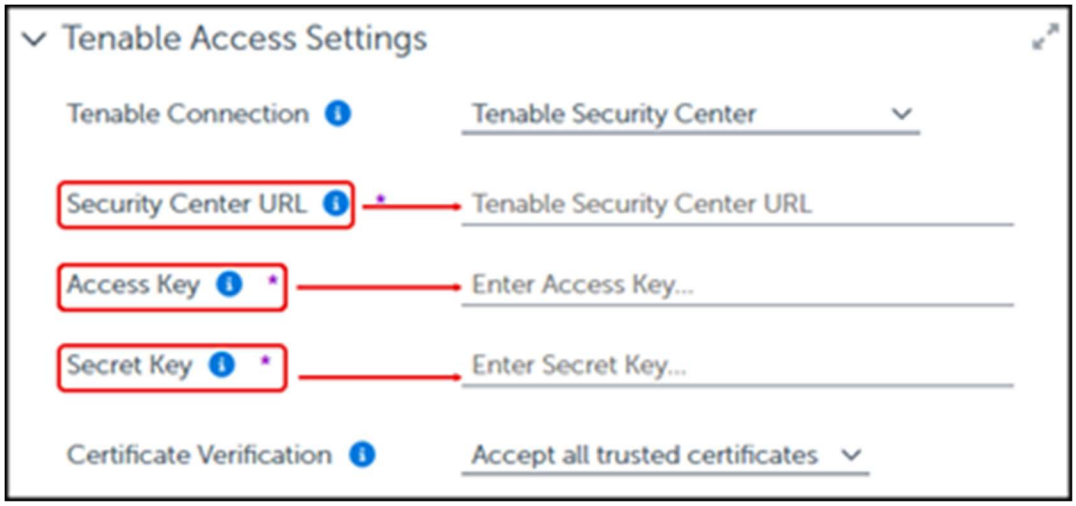
    a. Check the **Error View** and resolve any errors.

    b. Select **Save** again if you make any changes.

4. Select **Business Units**, and then select **Business Units** to verify your access to **Tenable ACR Business Units**.

Configure Tenable Security Center Settings

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

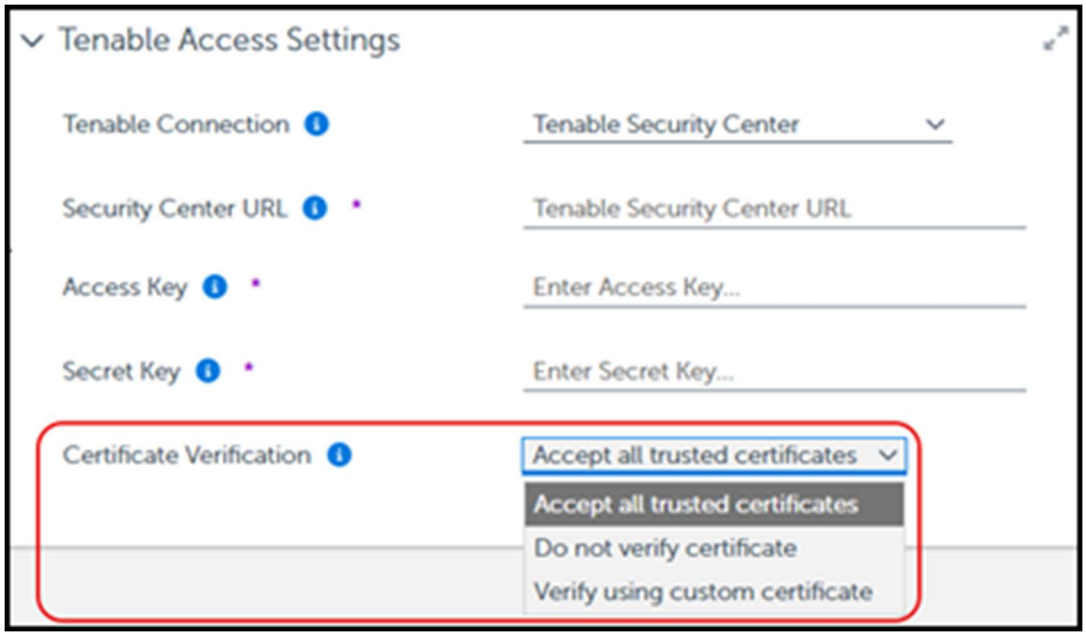


6. Select a Certificate Verification to use for Tenable Security Center APIs:

    c. Accept all trusted certificates:

    d. Do not verify certificate:

    e. Verify using custom certificate:



7. Select Save on the upper-left corner of the dialog:

    a. Check the **Error View** and resolve any errors.

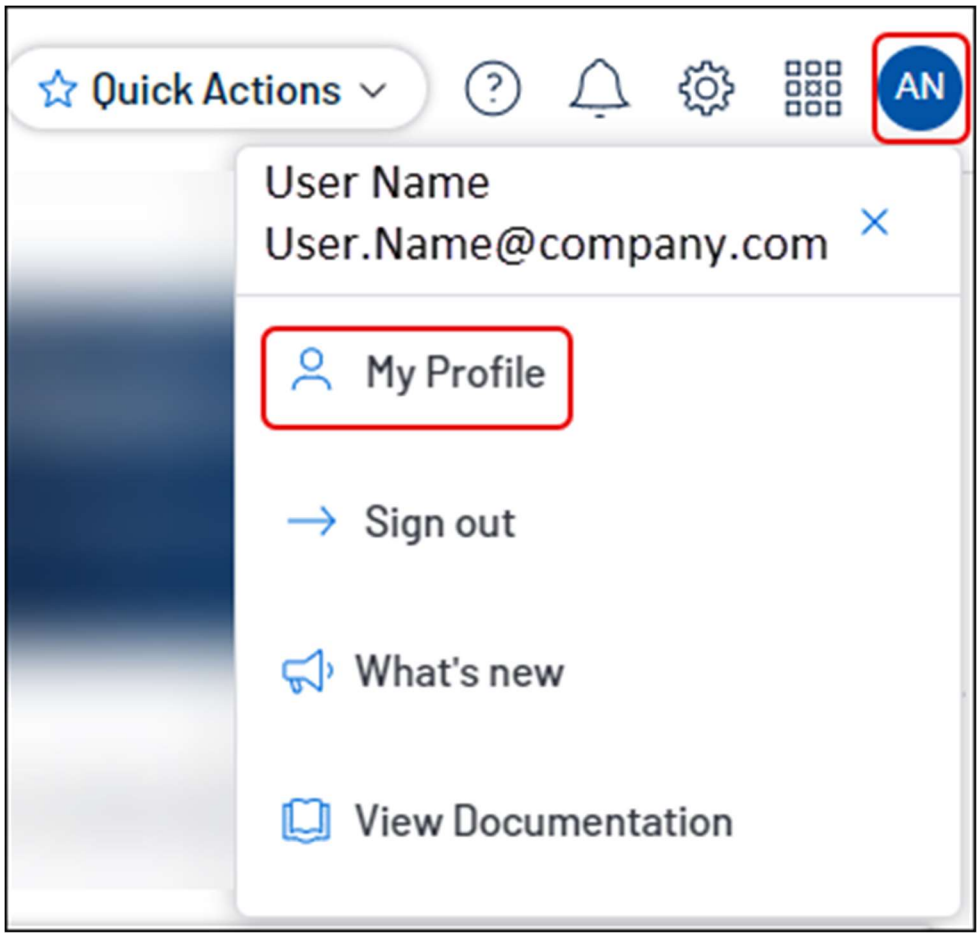
b. Select **Save** again if you make any changes.

8. Select **Business Units**, and then select **Business Units** to verify your access to **Tenable ACR Business Units**.

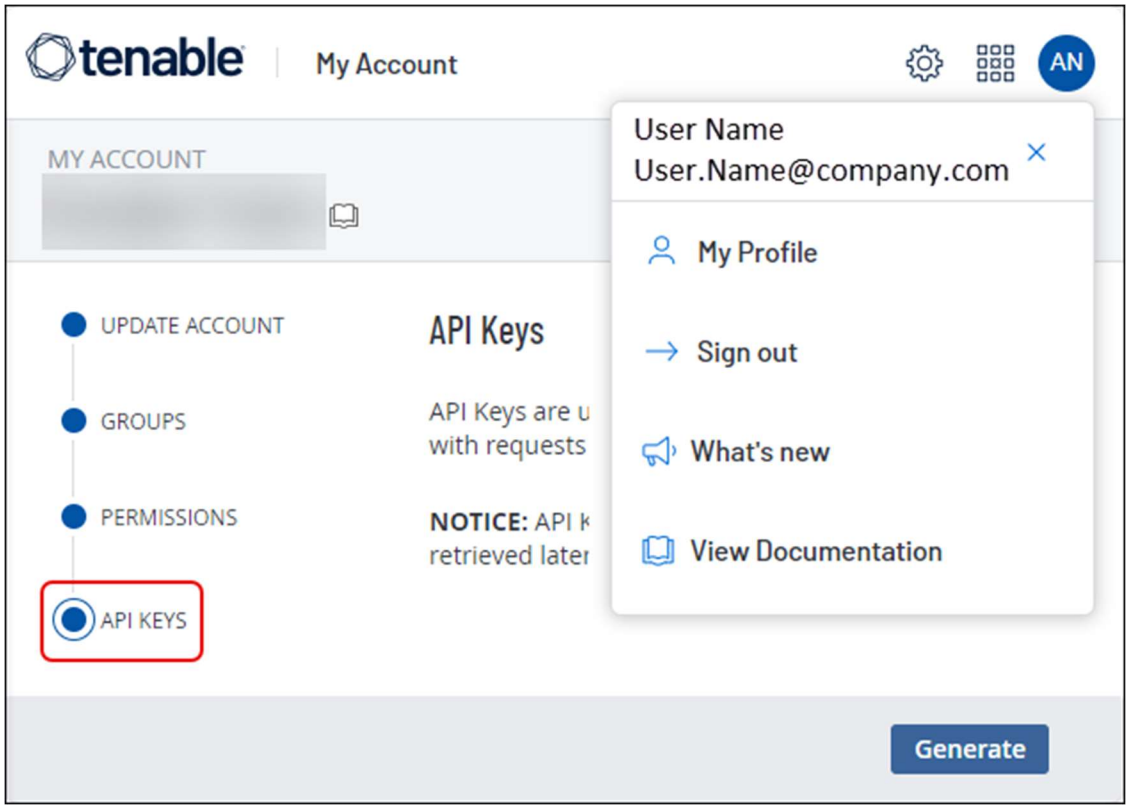
Create Tenable Access and Secret Key

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

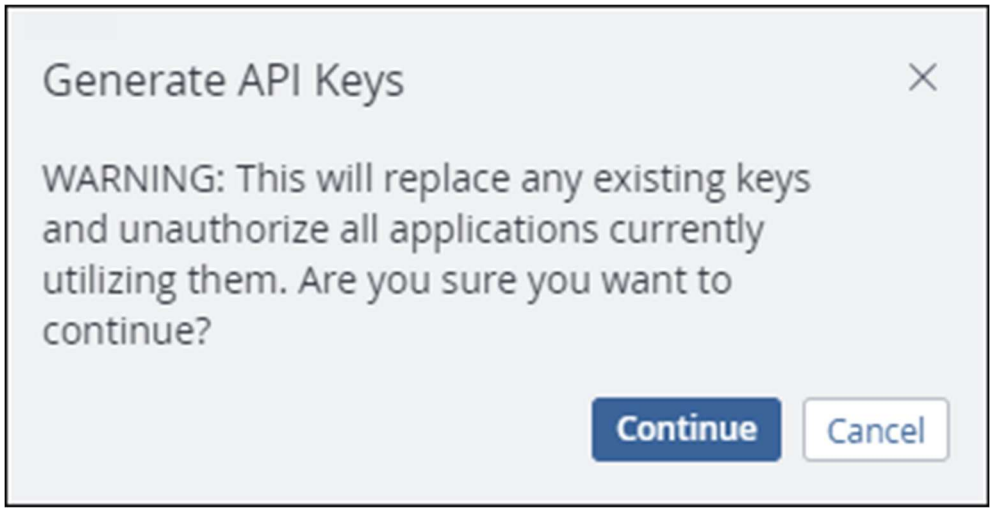
1. Log in to your **Tenable** account, and then click the user icon on the upper right.



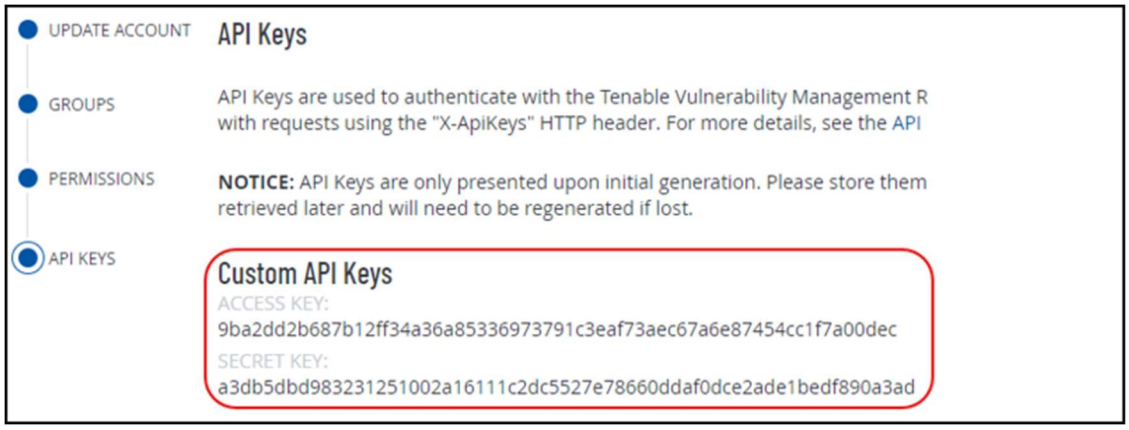
2. Select **My Profile**, and then click **API Keys**.



3. Select Generate and review the warning:



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



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.

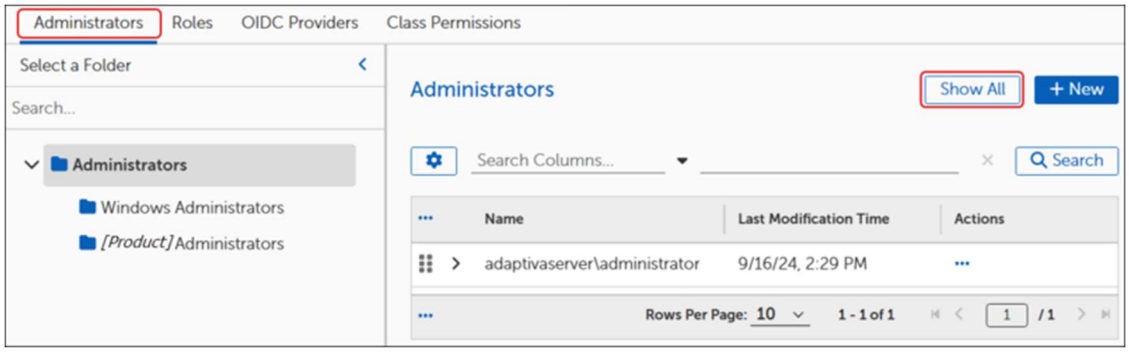
Administrators and Roles

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



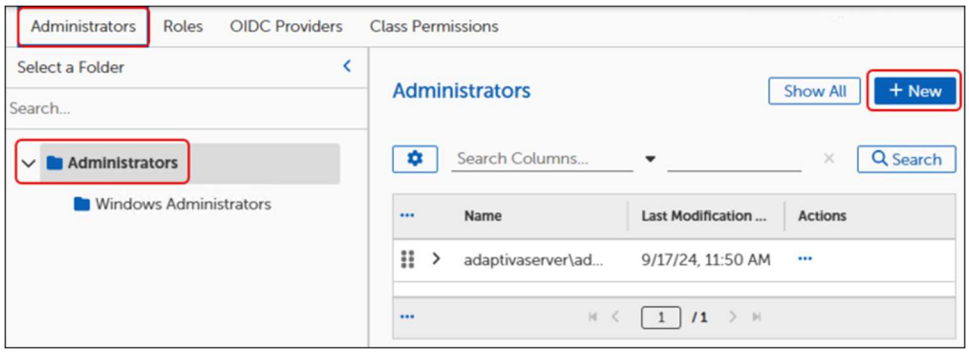
View Administrators

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

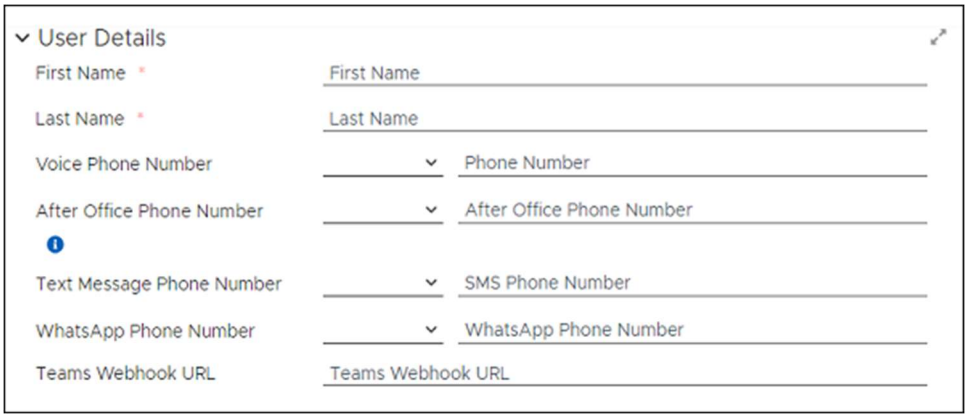
   To make any changes to Administrators, you must use the Tenable product.

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.

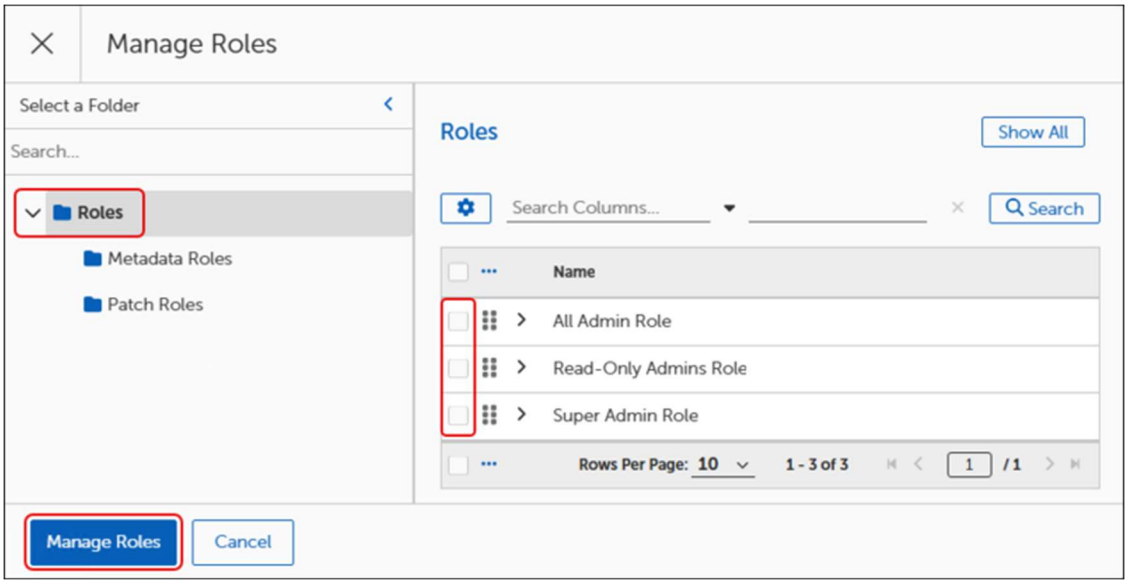


4. Assign **Direct Roles**:

   a. Select **+ Manage 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:

   a. 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.

   b. Go to Create an Incoming Webhook to create the Webhook URL.

2. Open the **Admin Portal**, and then navigate to **Settings > Security > Administrators**.

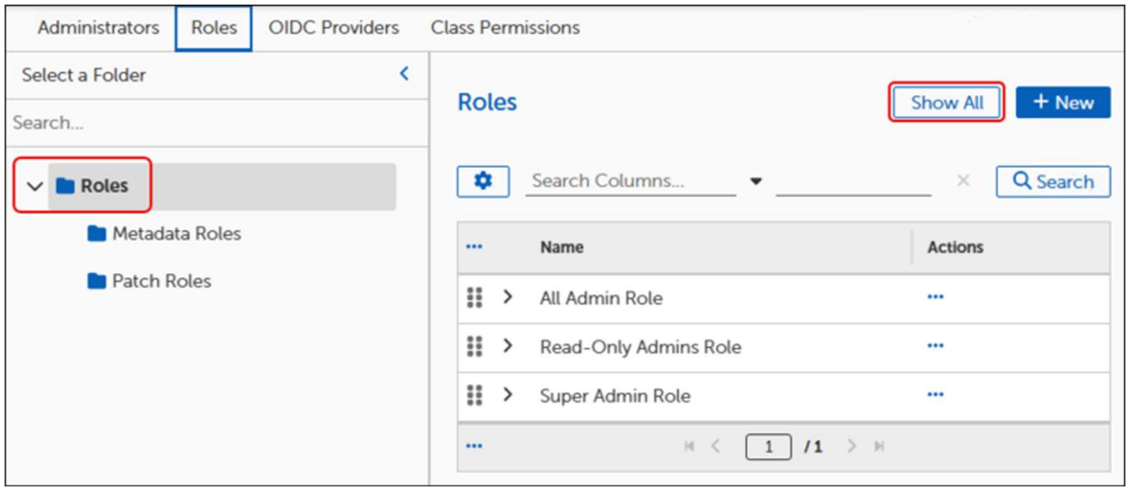
3. Open an existing administrator or select **+NEW** to create a new Administrator.

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.

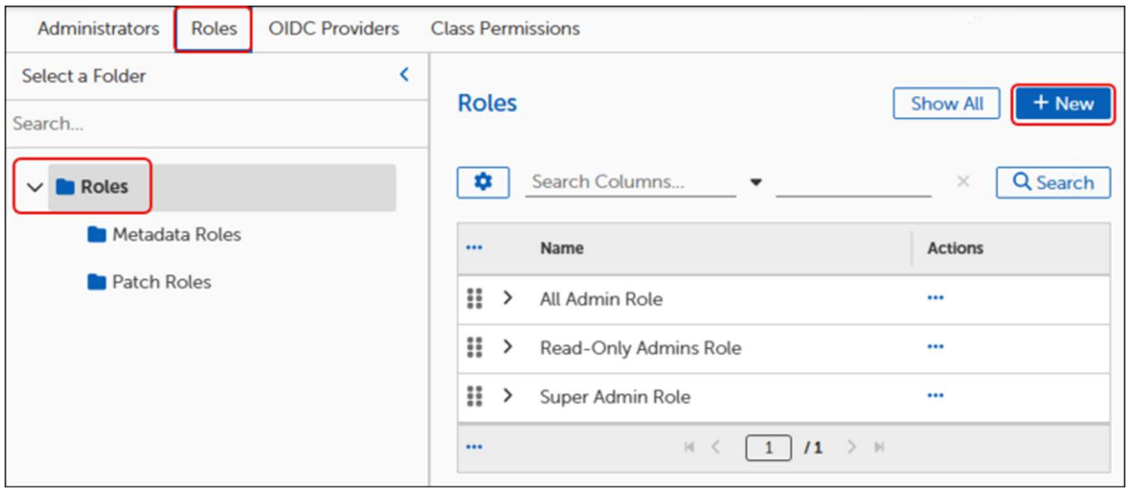


2. Select **Show All** to list all Roles in the selected folder.

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

Create a New Role

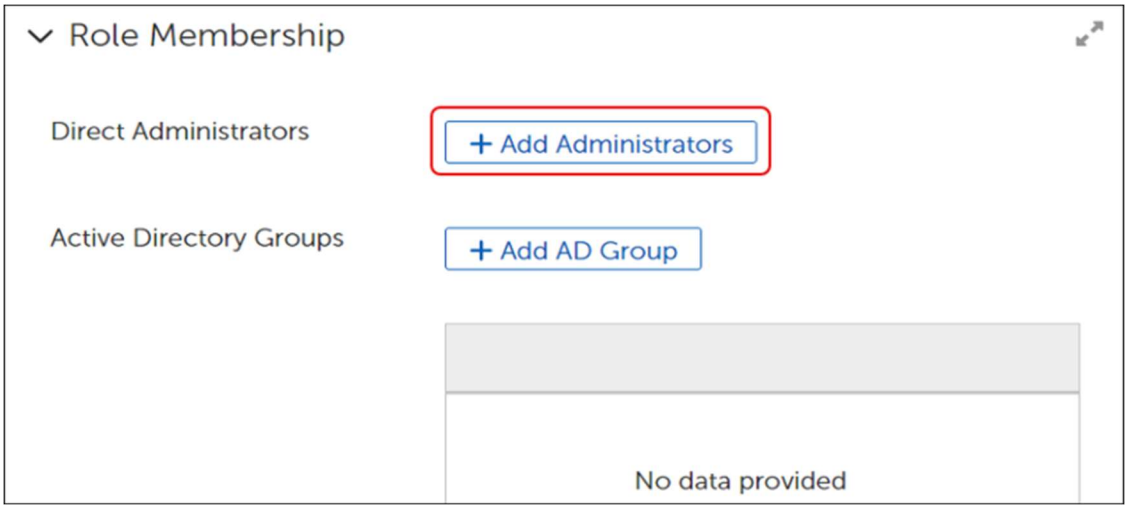
1. Select a **Roles** folder from the Roles tab of Security Settings, and then select **+ NEW** to open a new Role template.



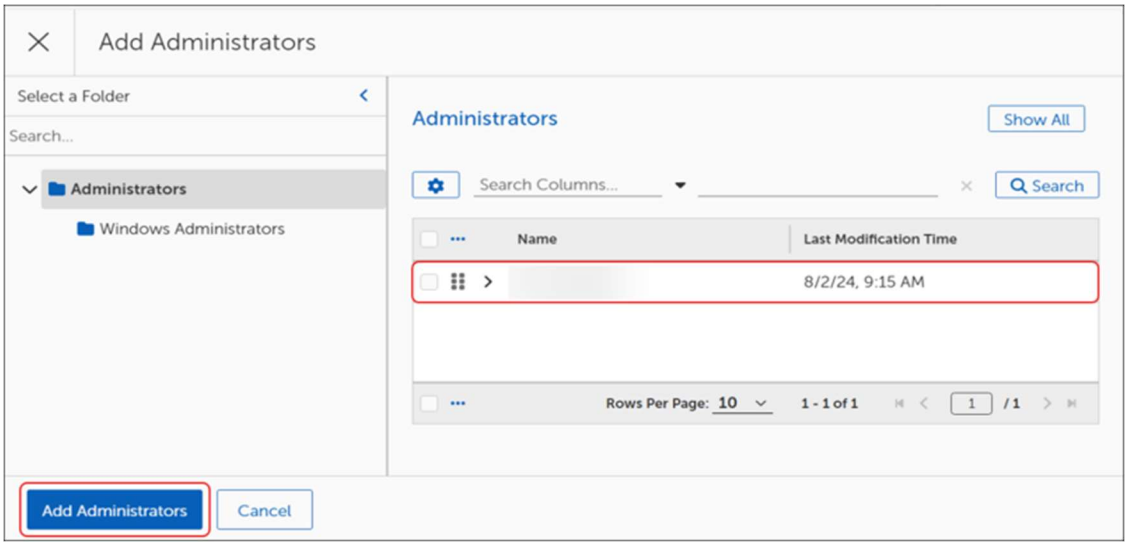
2. Enter a **Role Name** and a detailed **Role Description** in the **Role Properties** workspace.

3. Add one or more **Direct Administrators** in the **Role Membership** section:

    a. Select **Add Administrators** to open the **Add Administrators** dialog.



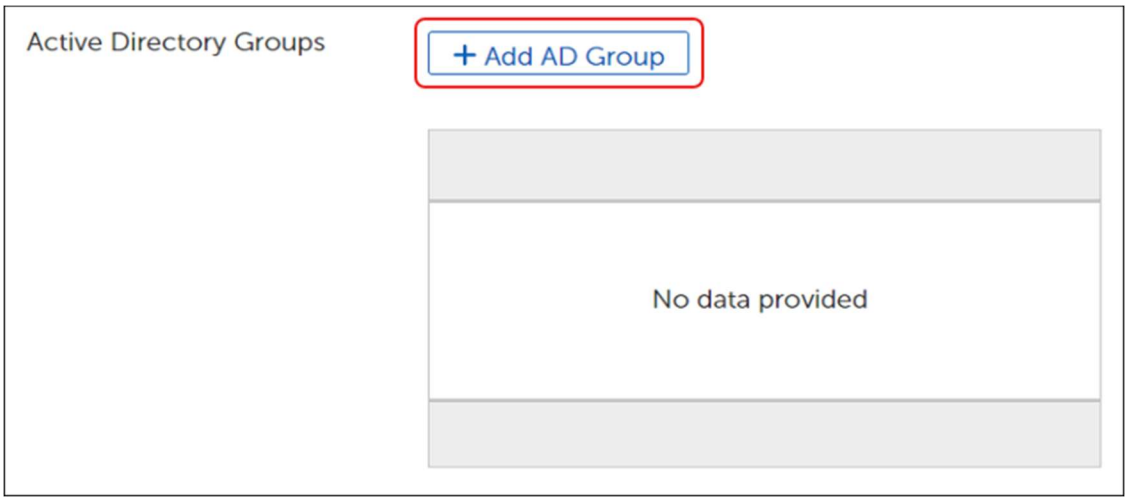
    b. Select one or more administrators from the table for the new role.



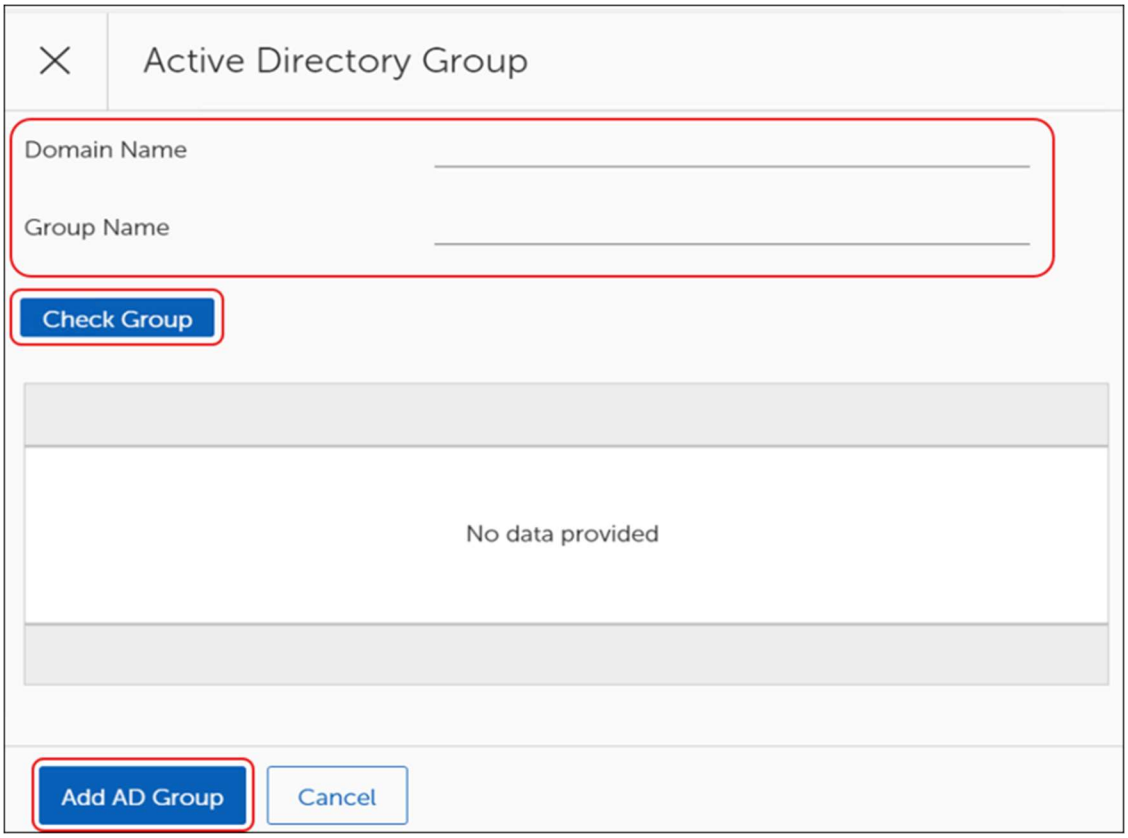
c. Select **Add Administrators** to return to the Role template.

4. Add an existing **AD Group** (Active Directory):

a. Select **Add AD Group** to open the **Active Directory Group** dialog.



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.



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.

Introduction to Patching Strategies

Creating a Patching Strategy is a great way to get started using Tenable Patch Management. Start with a common scenario, and then build a Patching Strategy to distribute a patch to active clients.

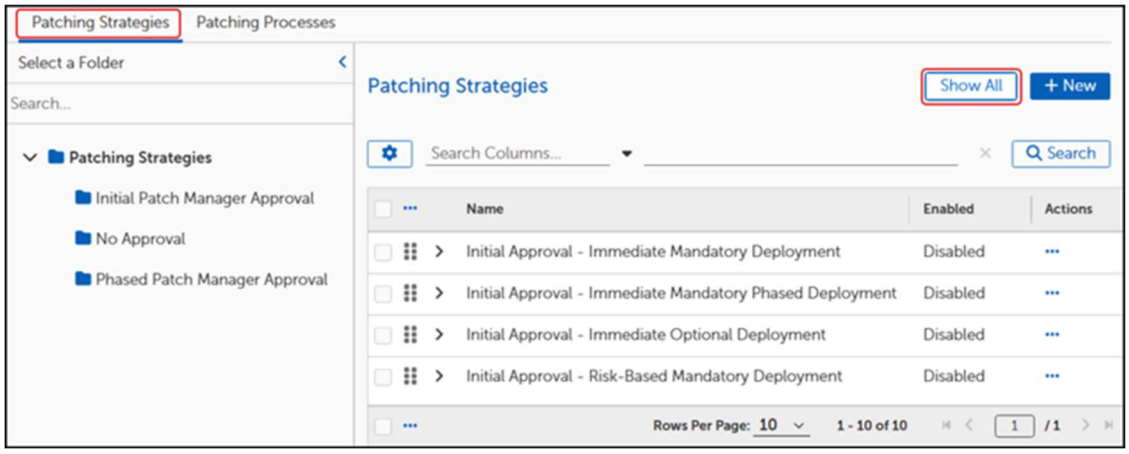
Patching Strategy Use Case

An administrator wants to build a Patching Strategy to update devices every day based on devices that have the following characteristics:

- Company-wide (all Clients).
- Within a Business Unit.
- Running a version of Google Chrome Enterprise other than the internally approved version.
- Initial approval needed.
- Immediate, mandatory update to approved version.

Open and Save a Patching Strategy Template

1. Follow the instructions in Create a New Folder for Objects.
2. Hover over or click **Strategy** in the left navigation menu of the Tenable Patch Management Enterprise Dashboard, and then select **Patching Strategies**.
3. Select **Show All** to see all available Patching Strategies. This populates the **Patching Strategies** table with the available templates.



   For descriptions of each template type, see Patching Strategy Templates.
4. Enter the **Name** of an existing strategy on the Search bar, and then click **Search**.
5. Select the **Name** of the strategy to open it.

6. Select **More** in the upper left corner of the template, and then select **Save Patching Strategy As**:

    a. Enter a unique name that reflects what the strategy does conceptually. For example, ITS Immediate Daily Product Patching.

    b. Select **OK**. This opens your strategy template with all the default entries for the built-in strategy, including a detailed description.

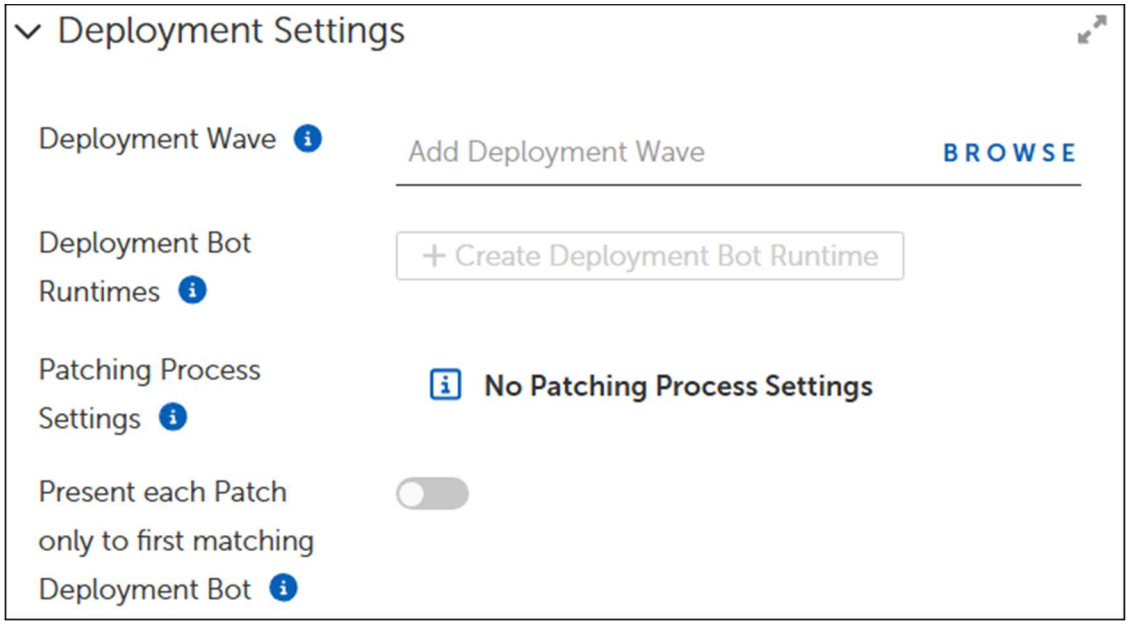
    c. Enter a detailed **Description** of your new template or keep the existing detail, and then click **Save** on the upper-left corner of the dialog.

Tip

Remember to click Save on the upper left corner to save your progress. After completing the Patching Strategy configuration, you must save and enable the completed strategy to make it available for use.

Configure Deployment Settings

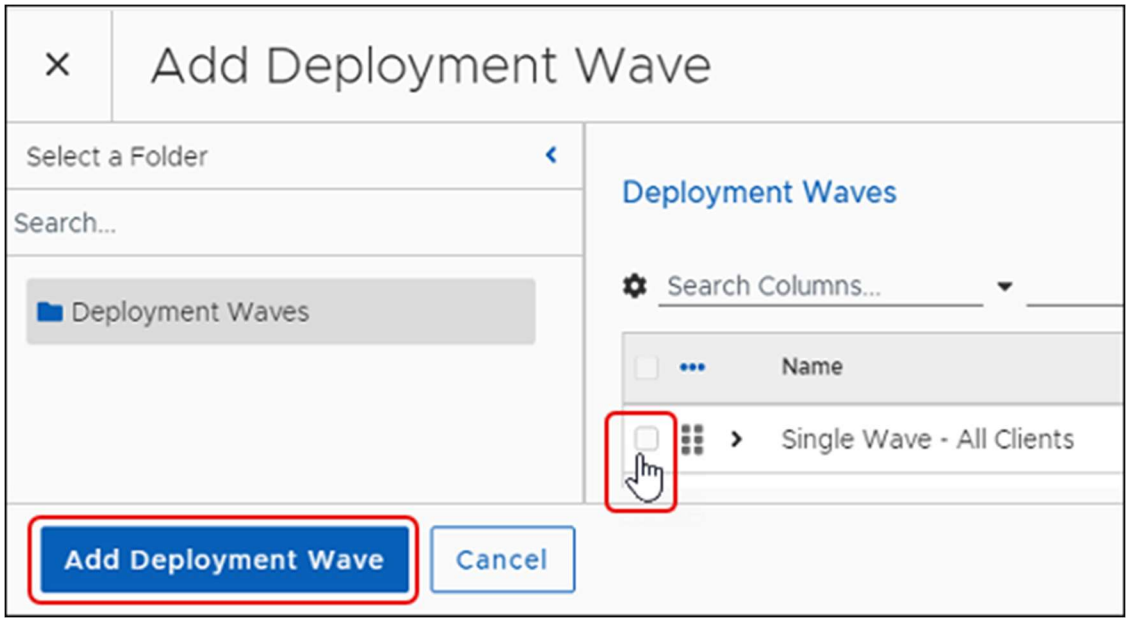
Deployment Settings for quick start purposes include selecting a built-in Deployment Wave, which already includes a Business Unit. For details on Deployment Waves, see Deployment Waves. When customizing an existing template, process and deployment fields may include tables with existing configuration selections.



Add a Deployment Wave

1. Scroll down to **Deployment Settings** in an open Patching Strategy template.
2. Select **Browse** next to **Add Deployment Wave**.

This opens the **Add Deployment Wave** dialog.



3. Select **Single Wave – All Clients**.

   This Deployment Wave includes a Business Unit called **All Clients Business Unit**. For information about Business Units, see Business Units and Rollout Processes.

4. Select **Add Deployment Wave** on the bottom-left corner of the dialog.

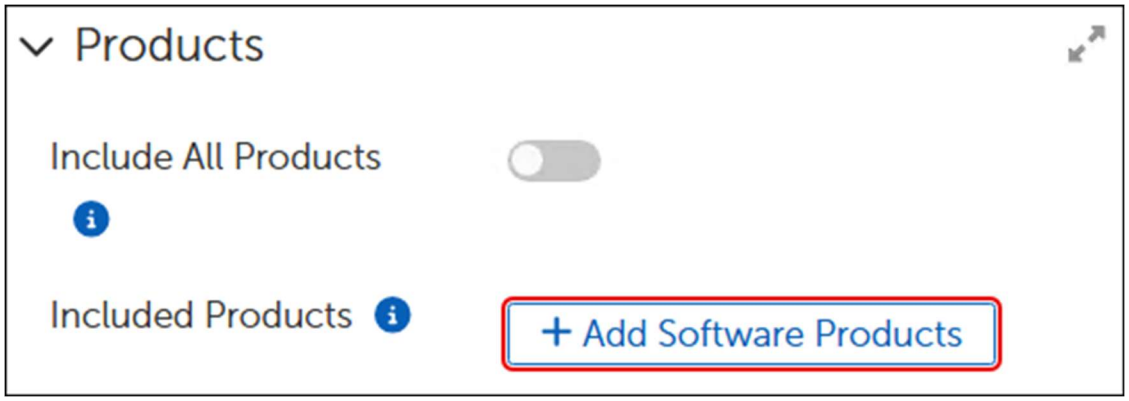
   a. This returns you to the object template.

   b. There is no need to modify the Deployment Bot Runtime settings for purposes of this exercise, but it is an important part of a Patching Strategy template. Be sure to review the Deployment Bot Runtime settings when you are creating your own Patching Strategies (see Deployment Bot Runtime Settings).

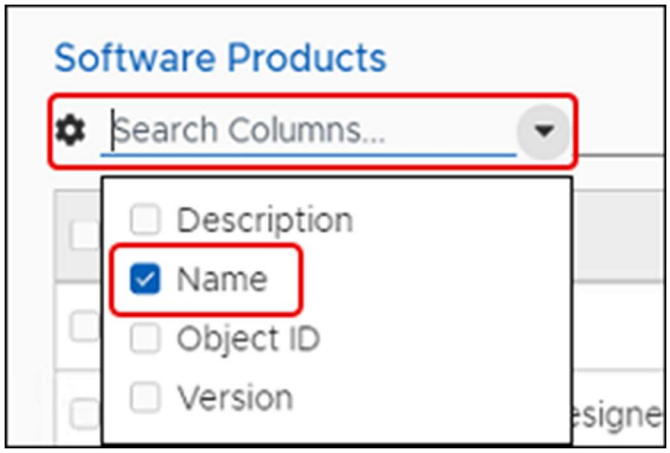
Add Software Products

For this exercise, we will add one product using the Products workspace near the top of an open Patching Strategy template.

1. Select **+ Add Software Products** in the **Products** workspace of an open Patching Strategy template.

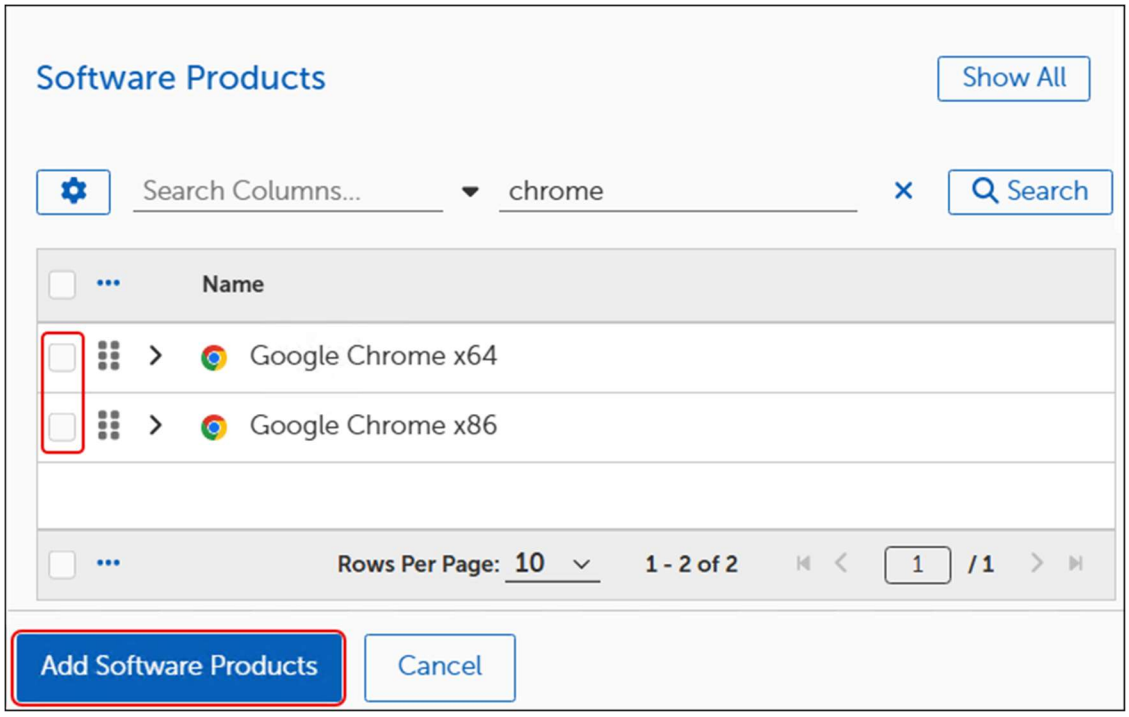


2. Select the **Down Arrow** next to **Search Columns** and verify that the only box checked is next to **Name**.



3. Enter **Chrome** on the search line, and then click **Search**.

4. Select **Google Chrome x64**, and then click **Add Software Products** on the lower-left corner of the dialog.

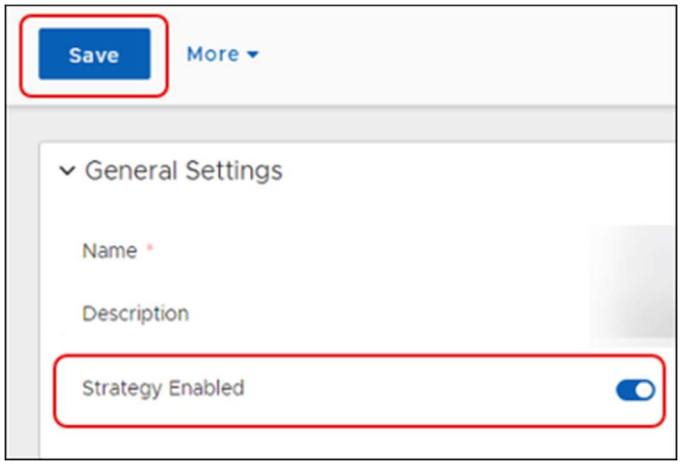


5. Scroll up to **General Settings** to enable the strategy.

Enable the Patching Strategy

After completing the Patching Strategy configuration, including Add Software Products, you must enable the Patching Strategy. When enabled, the strategy runs according to the configured schedules.

1. In **General Settings** at the top of the Patching Strategy template**,** click the **Strategy Enabled** toggle to enable the strategy and make it available for use.



2. Select **Save** on the upper-left corner of the workflow to save the strategy:

    a. Check the **Error View** and resolve any errors.

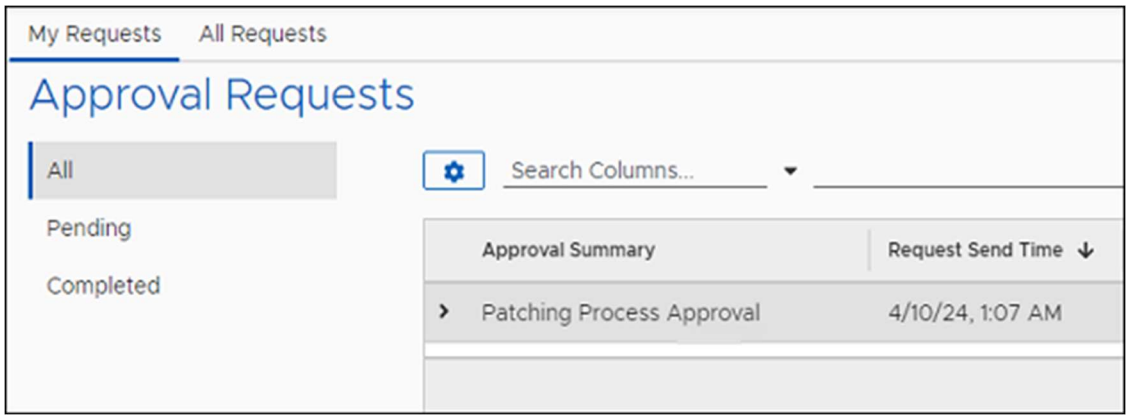
b. Select **Save** again if you make any changes.

3. *Move the saved template to your folder*.

View the Staged Patching Strategy

After you Enable the Patching Strategy, you can view the pending approval request.

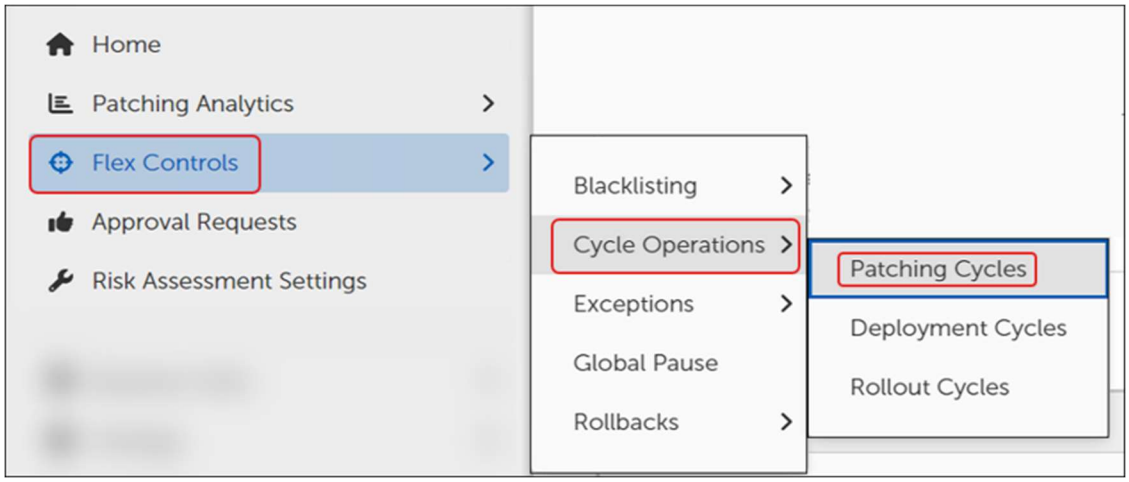
1. Select the **Approval Requests** in the left navigation menu of the Tenable Patch Management Dashboard.



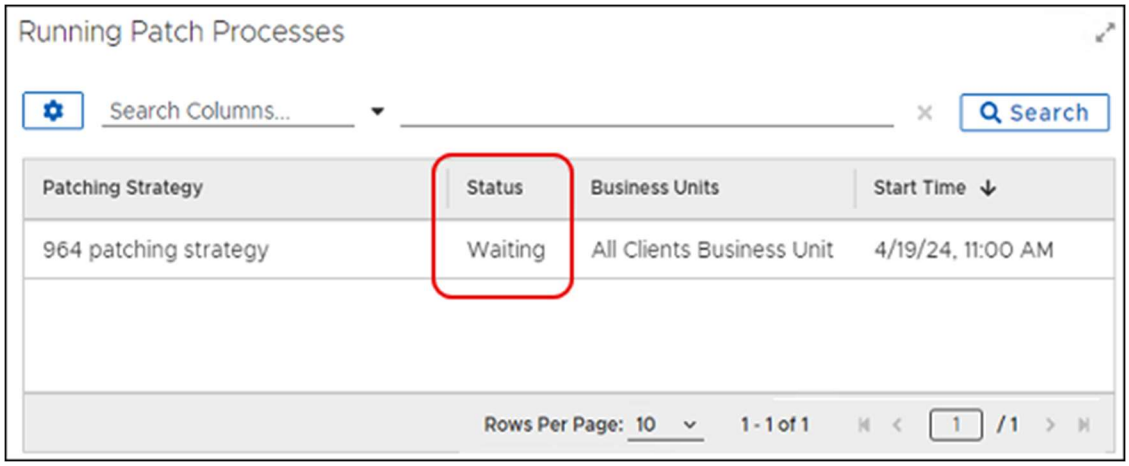
c. The view defaults to **All** requests, which includes pending and completed.

d. The Patching Strategy you just enabled appears in the **Approval Summary** table with a **Request Status** of **In Progress and Awaiting Response**.

2. Select **Flex Controls > Cycle Operations > Patching Cycles** from the left navigation menu of the Tenable Patch Management Dashboard.



3. Check the **Running Patch Processes** table, which lists the status of the **Patching Strategy** as **Waiting**.



4. Select **Approval Requests** in the left navigation menu, and then click the **Patching Strategy** in the table.

5. Select **Approve**, and then click **Back to Approval Requests**. You can wait until the patch time passes, or you can start the deployment manually.

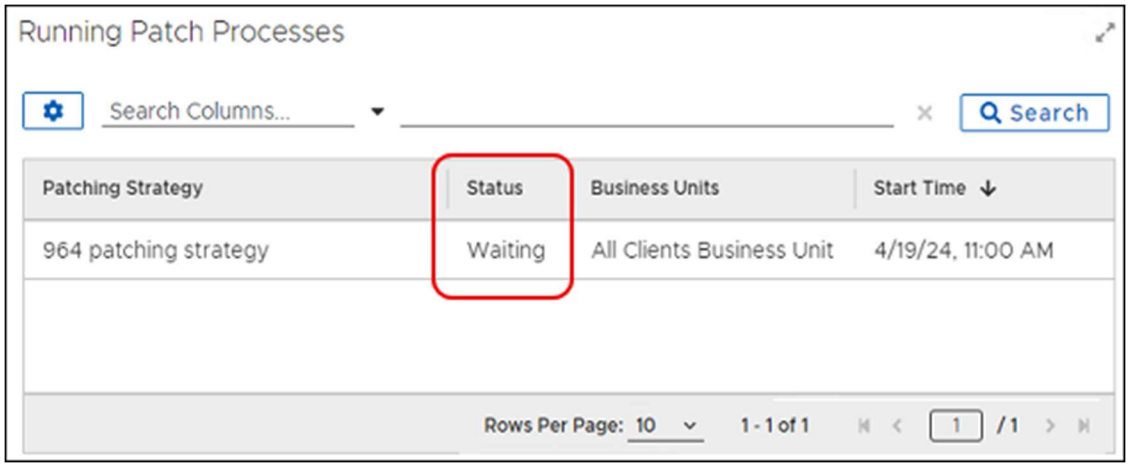
Important

When you add a new device (Tenable Server) to your network after this strategy has scanned and updated all associated devices, Tenable Patch Management automatically adds any new devices to the strategy if the next scan detects an earlier version of Chrome.

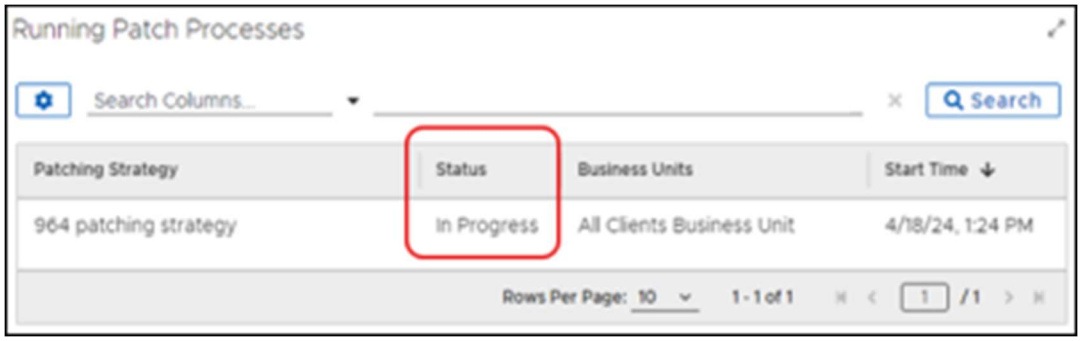
Start the Patching Strategy Manually

After the Patching Strategy approval process status shows **Completed**, you can wait until the time setting for patch deployment, or you can start the deployment immediately.

1. Select **Flex Controls > Patching Cycles**, and then click the name of the Patching Strategy to open the **Cycle Information**.



2. Select Play under **Cycle Information**, and then click **Close**. This returns you to the **Patching Cycles** workspace where you can view **Running Patch Processes**.



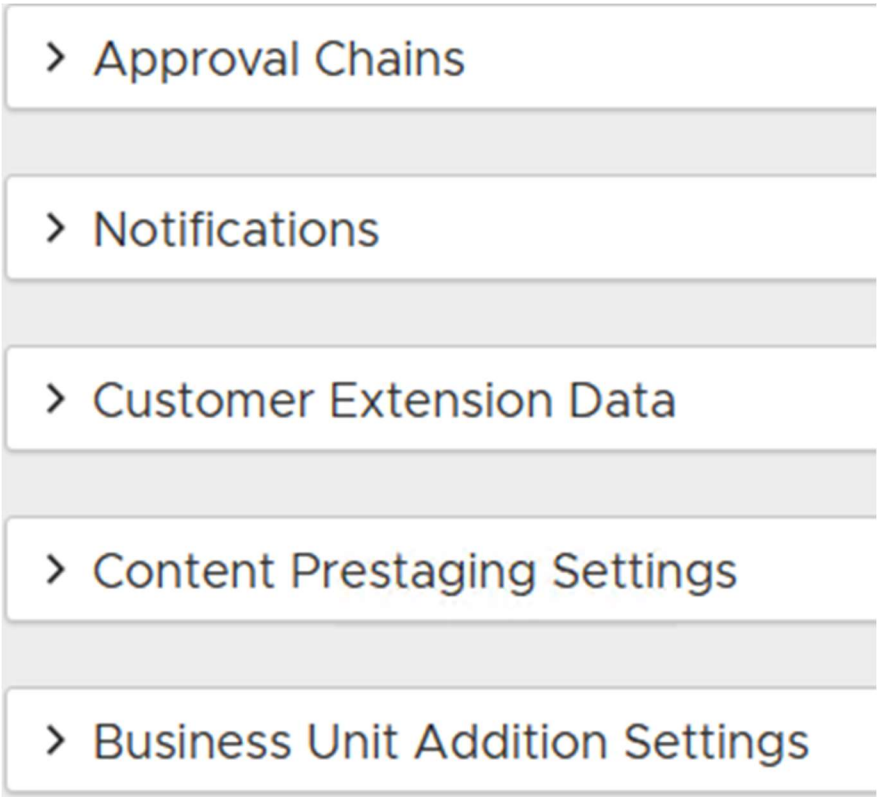
3. Select the **Patching Strategy** name to view details about the patching process.

Optional Objects in Patching Strategy Templates

The exercise in Introduction to Patching Strategies uses the minimum requirements for a Patching Strategy.

Additional settings in the Patching Strategy template include those listed below, though you do not need them for quick start purposes. Configuration steps for each are documented as part of Creating a Patching Strategy.

- Chains(Approval and Notification)
- Customer Extension Data
- Content Prestaging Settings
- Business Unit Addition Settings



Organize New Patch Objects

Throughout your patch management journey, you will customize object templates to meet the needs of your business environment. Tenable recommends setting up your own folder to hold object templates that you customize or create, to keep them separate from those provided by Tenable.

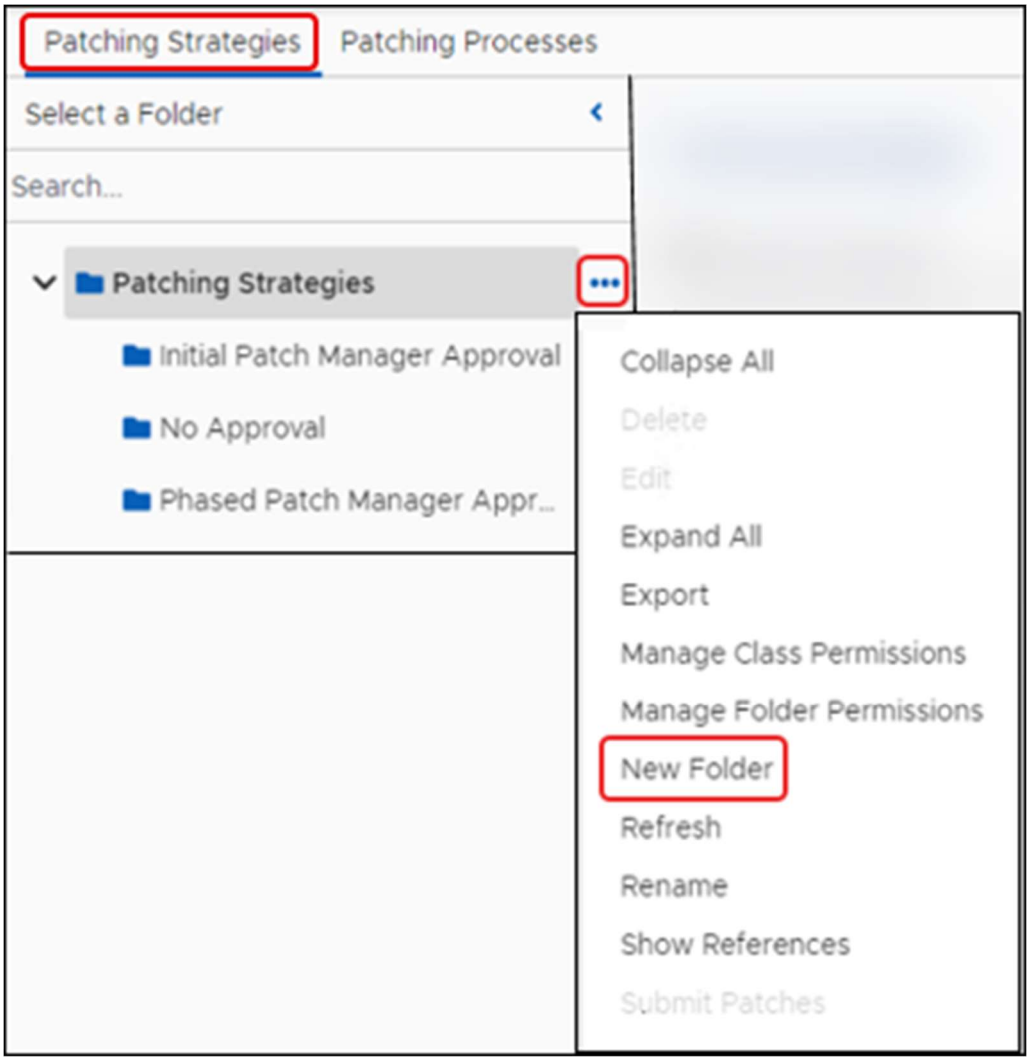
Create a New Folder for Objects

When creating new templates for most objects or when customizing (save as) existing templates, create a location under each object to hold your templates separately from those provided by Tenable.

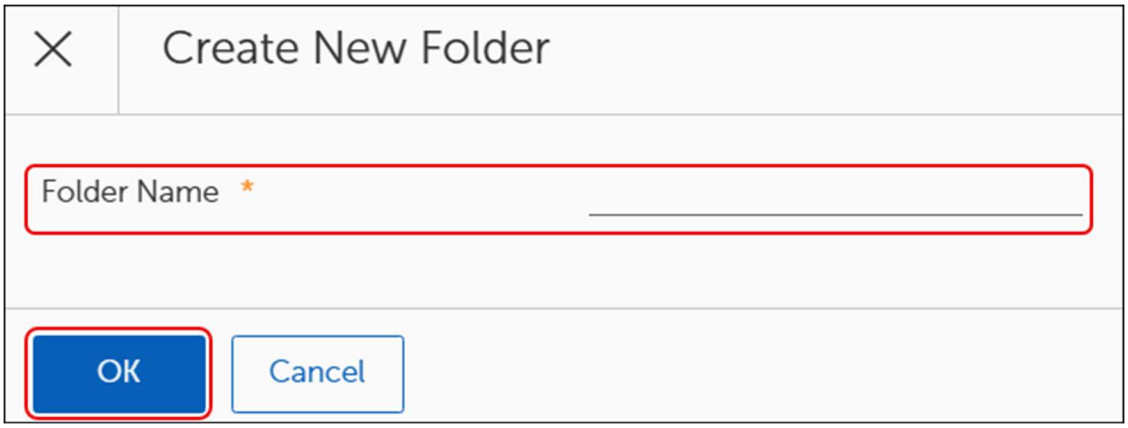
1. Select an object on the left navigation menu of the Tenable Patch Management dashboard. This example uses **Strategy > Patching Strategies**.

2. Create a new folder to hold your Patching Strategies:

    a. Select the **ellipsis (...)** to the right of the Patching Strategies Folder, and then select **New Folder**.



This opens the **Create New Folder** dialog.



b. Enter a descriptive **Name** for the folder, and then click **OK** on the bottom-left corner of the dialog.

- This creates the new folder structure showing both your folder and the Patching Strategies folder.

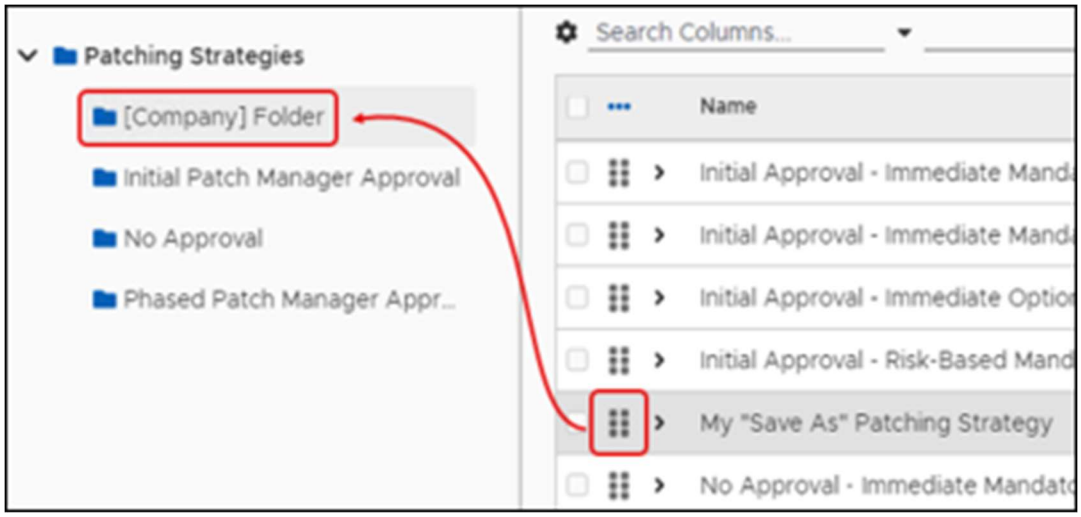
- When you create new strategies or modify existing strategies, move them to your folder location (see Move an Object Template Between Folders).

Move an Object Template Between Folders

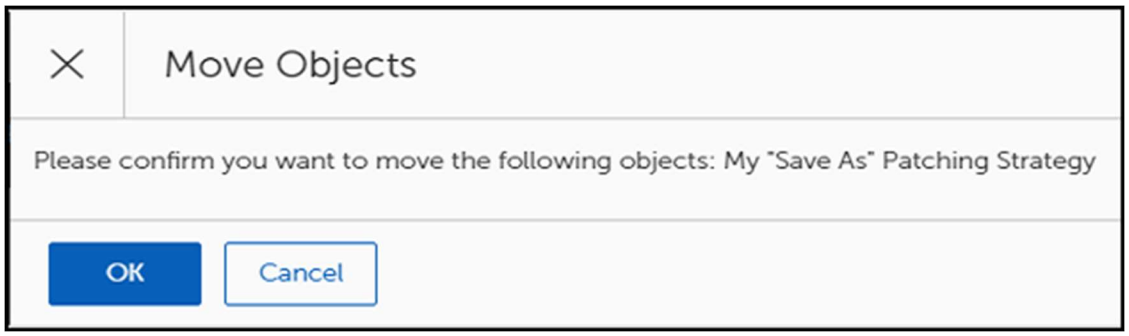
After creating an object template and creating a new folder to hold your object templates, use the following procedure to move saved templates from one folder to another. This example uses **Strategy > Patching Strategies**.

1. Select and hold the **stacked icon** next to the template you want to drag and drop to the new folder.

2. Drag the **stacked icon** over the folder, and then release it.

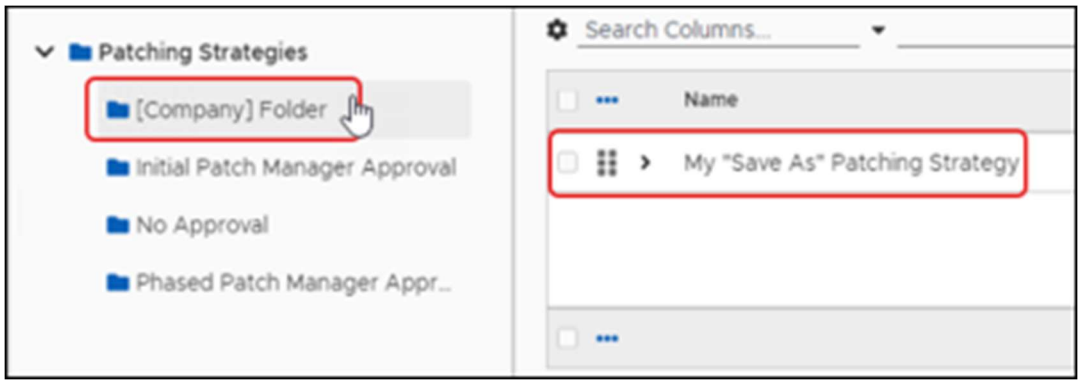


This opens the **Move Objects** dialog.



3. Select **OK** to confirm the move.

4. Select the designated folder to view its content and verify that the list includes the template you moved.



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 Strategies and Patch Content in the left navigation menu of the Tenable Patch Management dashboard. For descriptions of each menu item, see Tenable Patch Management Menus.

Business Units and Rollout Processes

Business Units are a fundamental organizational unit of the Tenable Platform. Business Units provide the ability to logically group and manage devices, settings, and other resources within a hierarchical structure.

Tenable Patch Management uses Business Units to group devices that share common attributes such as location, purpose, users, corporate structures, or other criteria. These logical groupings allow distribution of patches to various devices depending on the needs of the Business Unit.

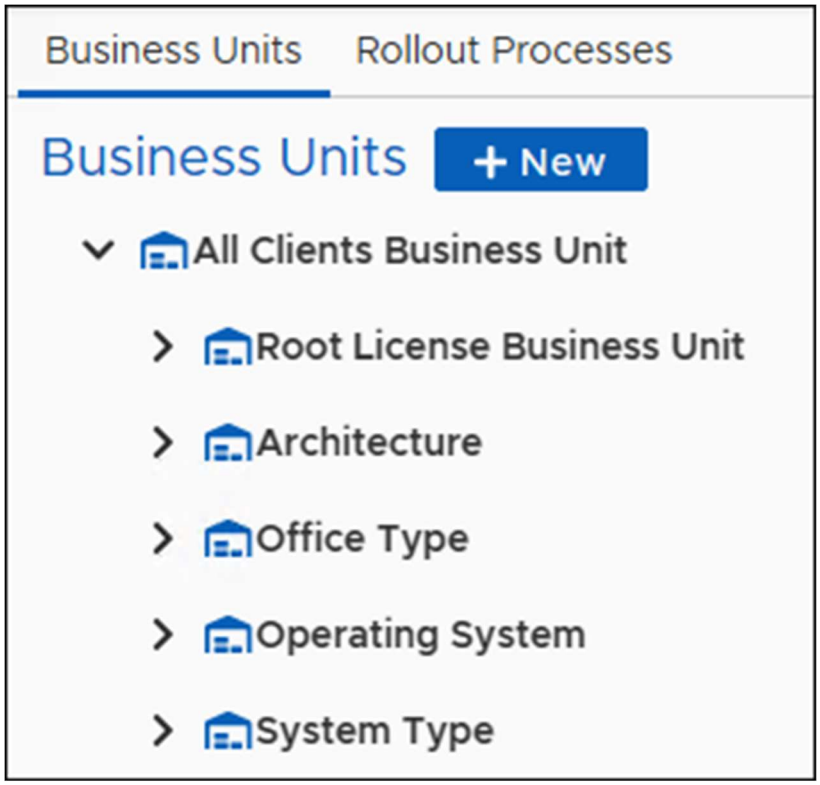
A Rollout Process runs at the Business Unit level to define and direct the rollout requirements of a Business Unit. This includes separating patch approvals, submitting them to a specified Business Unit, and sending a system request to begin the patch rollout for the Business Unit after receiving notification of approval.

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.

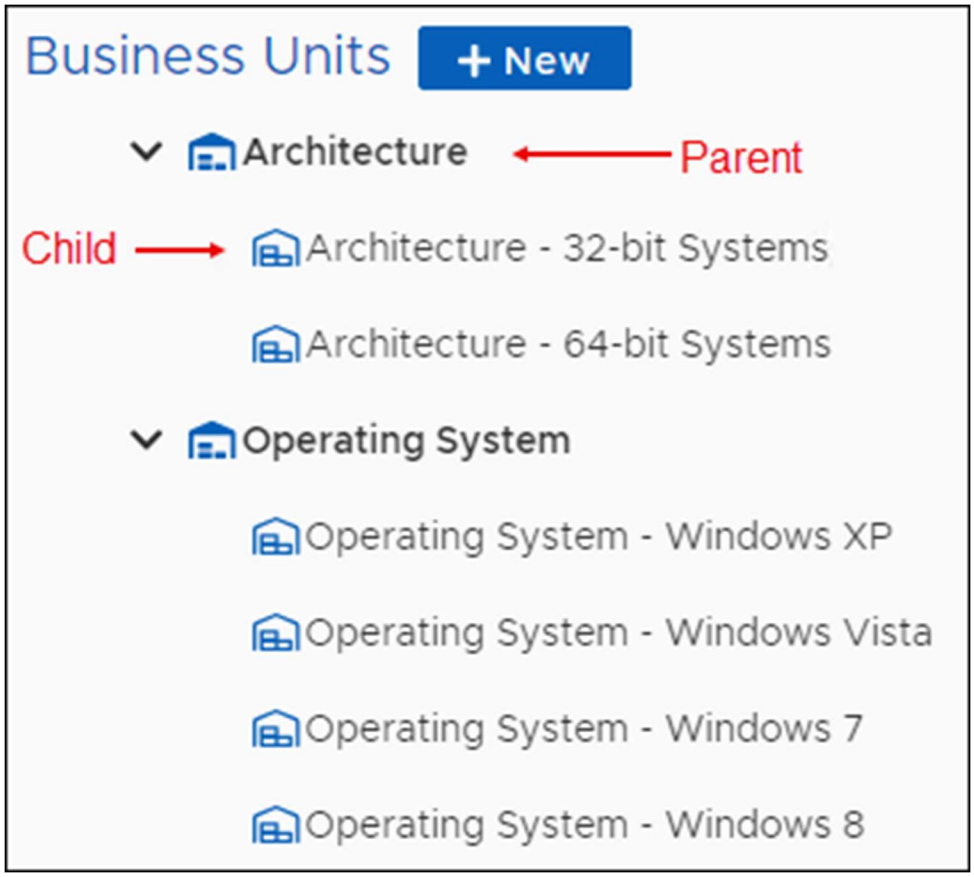
In addition to identifying the devices to include in a Business Unit, you can also identify many aspects of patching for endpoints, such as rollout processes, maintenance windows, approvals, and more.

Parent and Child Business Units

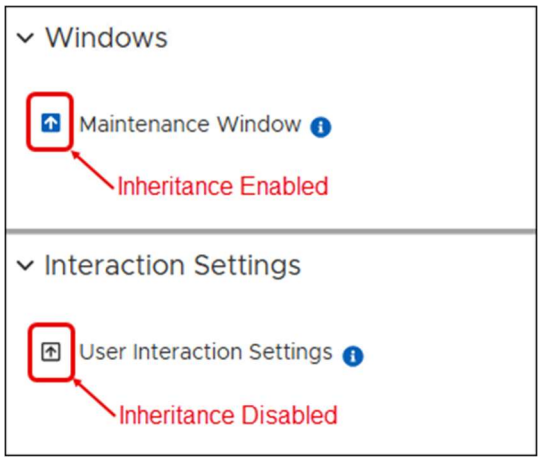
Business Unit objects use a parent-child hierarchy. A parent Business Unit may have multiple child Business Units, but a child Business Unit may have only one parent. The folder structure used in Tenable Patch Management shows the parent as the top-level folder and the child units as sub folders of a 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.

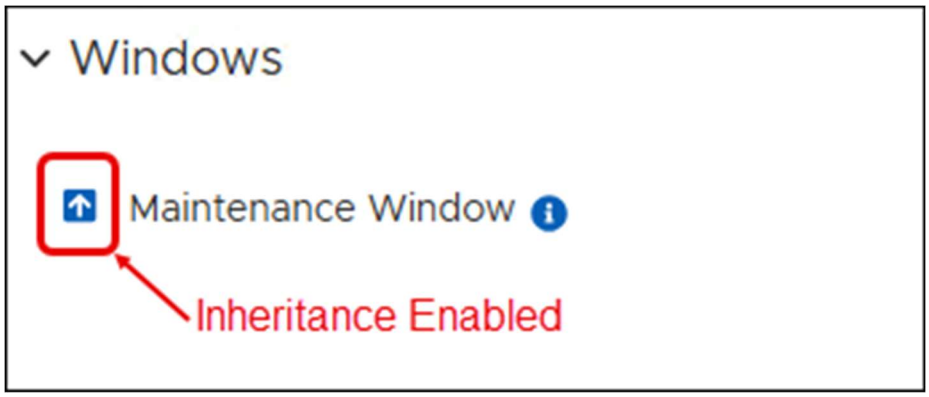


The hierarchical nature of Business Units allows a child Business Unit to inherit settings from its parent. An up-arrow with a blue background preceding a setting or process shows an inherited setting.

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.

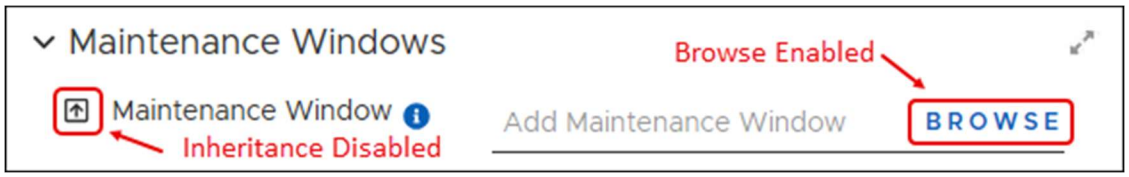
2. Select the up-arrow icon to enable inheritance

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

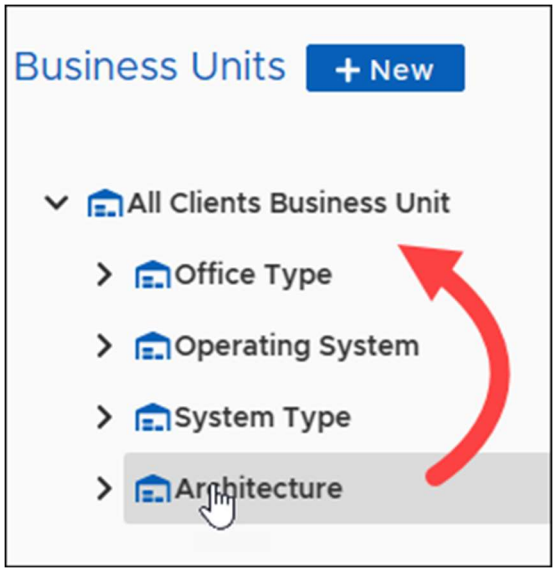
In the Business Unit hierarchy shown in the Tenable Patch Management dashboard, the Business Unit at the top of the list has the lowest priority. When changing the priority of a Business Unit in the hierarchy, consider the following items:

- **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?

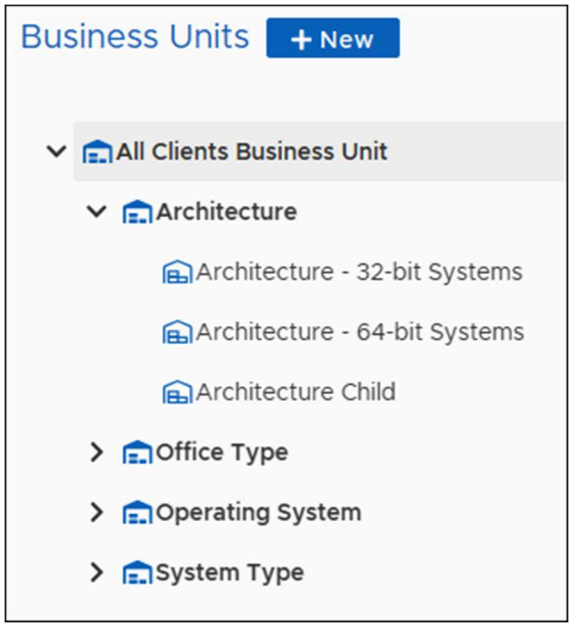
Further, is the new parent, or any ancestors, included in a Wave Entry that includes descendants? If yes, do you want the new BU included in those deployments?

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 Tenable 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.

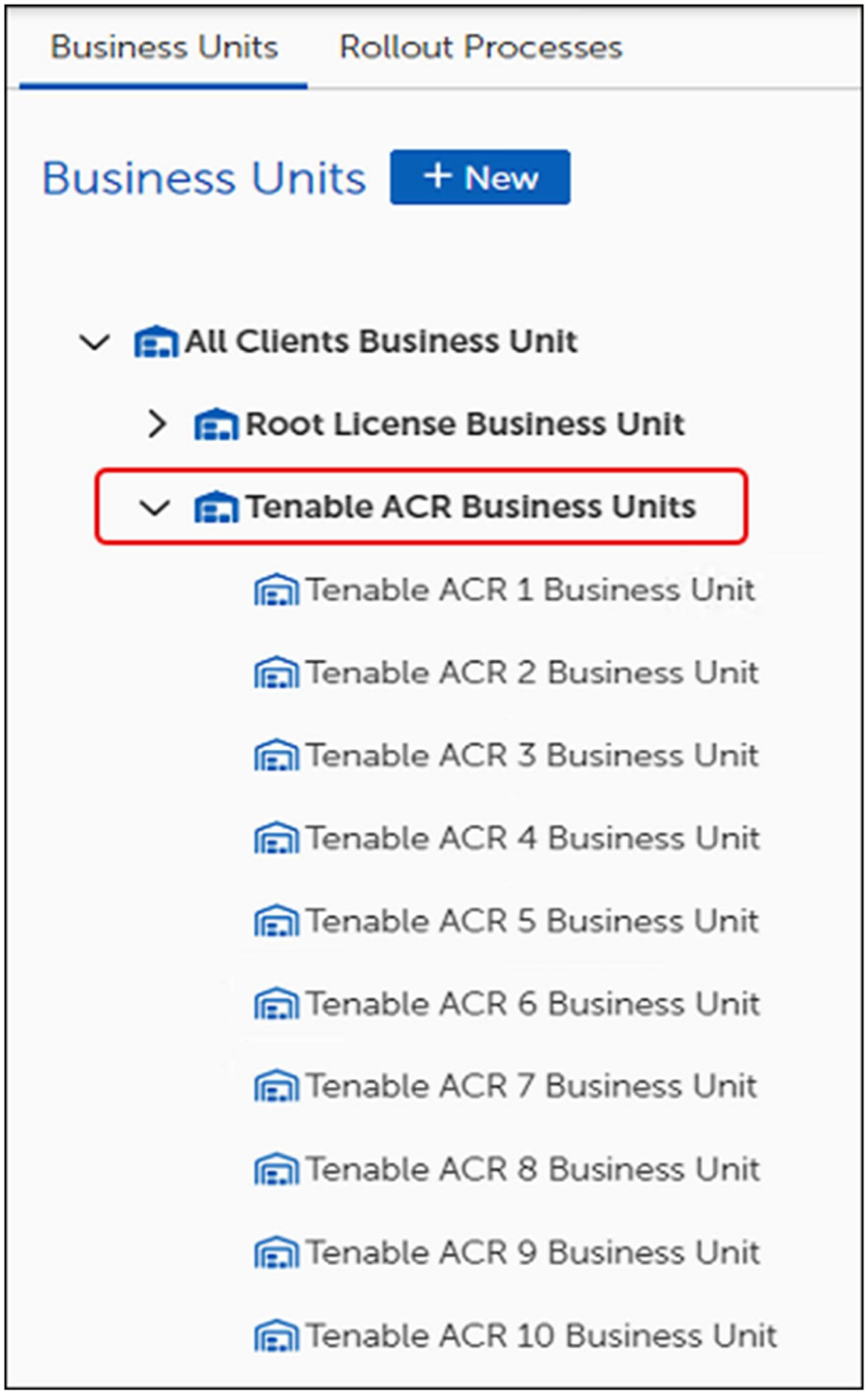
Related Business Units, including Child Business Units or Lab Business Units, provide another level of detail that administrators can use to further customize a patching environment.

Open and Save a Business Unit Template

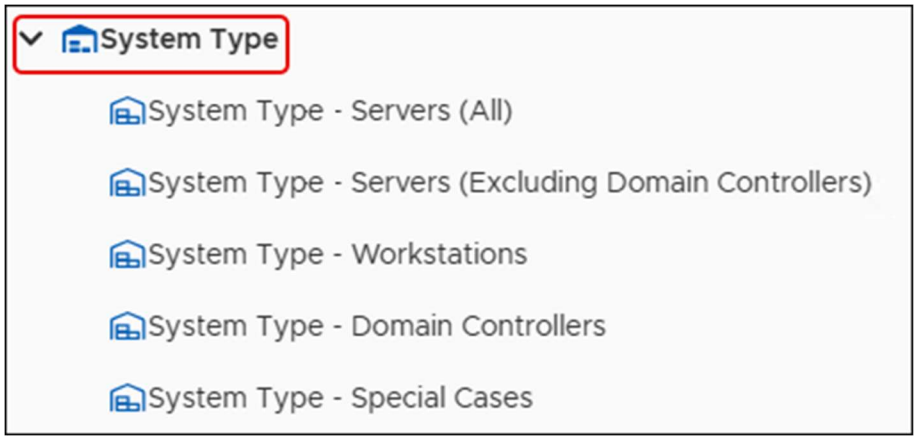
Each of the default Business Units provided by Tenable target production devices. Tenable recommends copying and creating new Business Units and to create Business Units for test purposes. Except for Business Units provided for Root, you can copy the default templates and save them with new details,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



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 Organize New Patch Objects).

Add Evaluation Schedules to a Business Unit

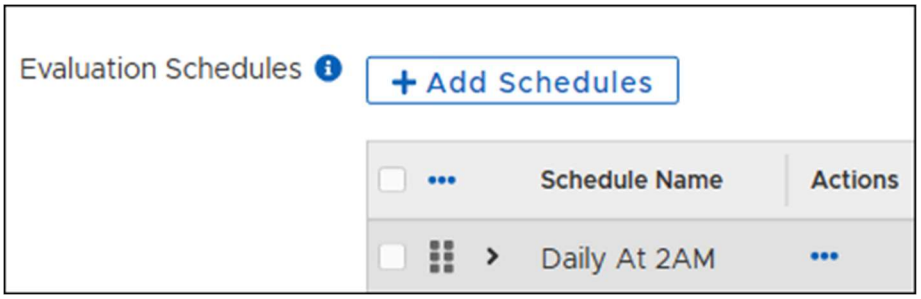
For Business Units with dynamic membership that may change over time, evaluation schedules determine when to check the membership of a Business Unit. Dynamic membership can occur based on Location or Sensor scopes where a device moves between locations or Sensor results change over time.

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.

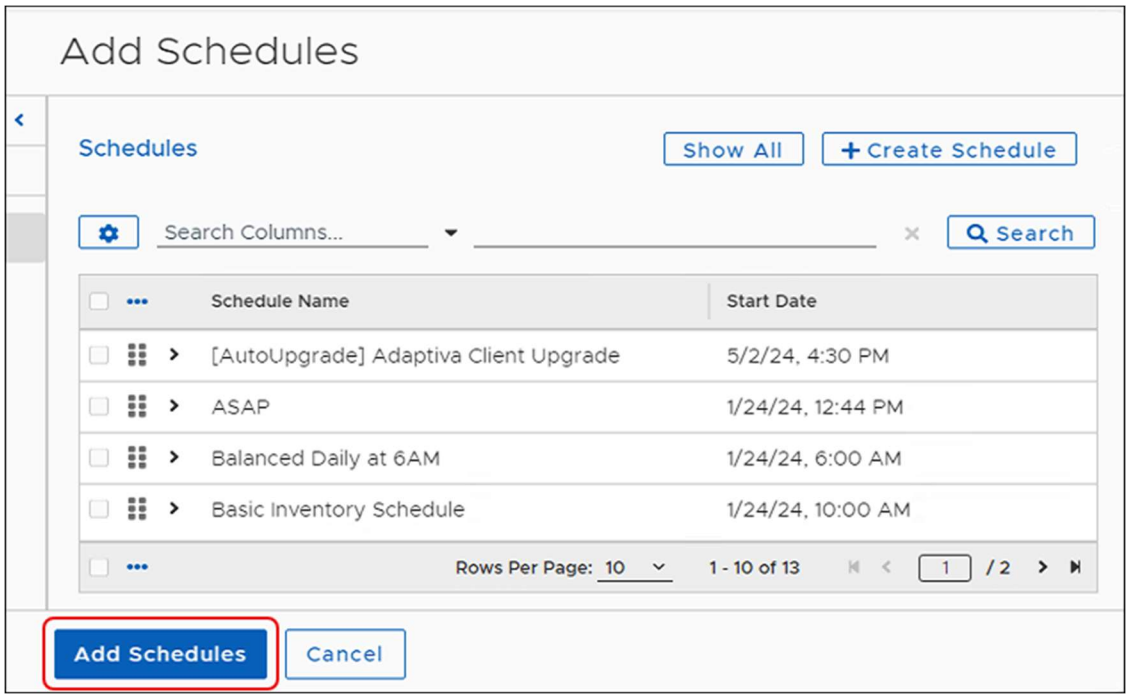
1. From an open Business Unit Template, review the selected schedules (if any).

    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.

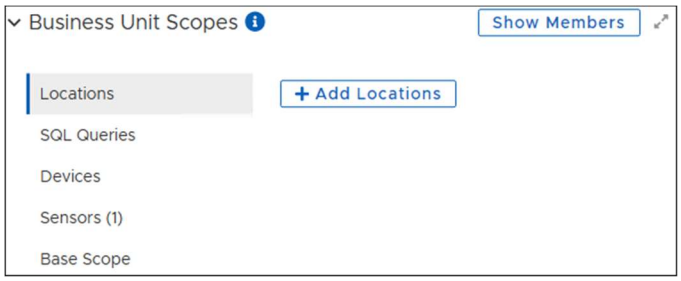
Configure Business Unit Scopes

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**.

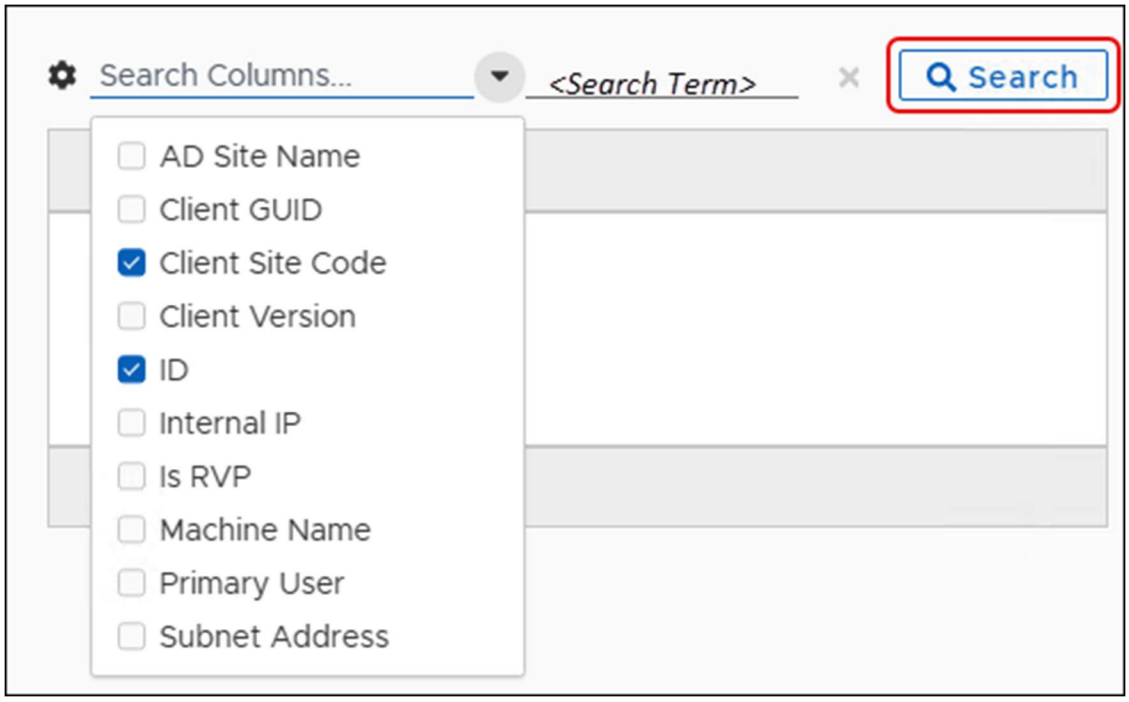
2. Select one or more Location Names from the **Add Locations** table to assign them to the Business Unit.
3. Select **Add Locations** in the lower-left corner of the dialog. This returns you to the Business Unit template and populates a table with the selected Locations.

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.

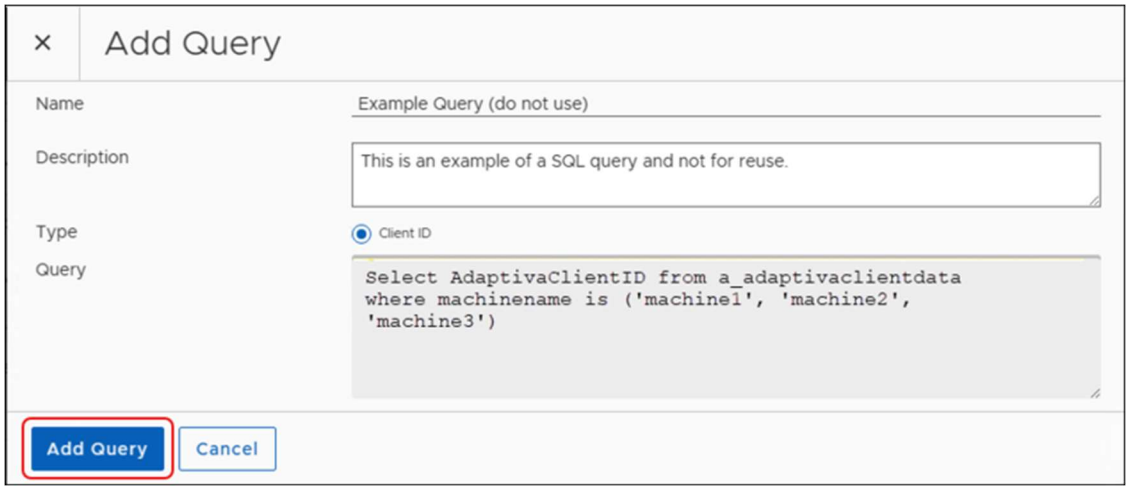
Add SQL Queries

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.

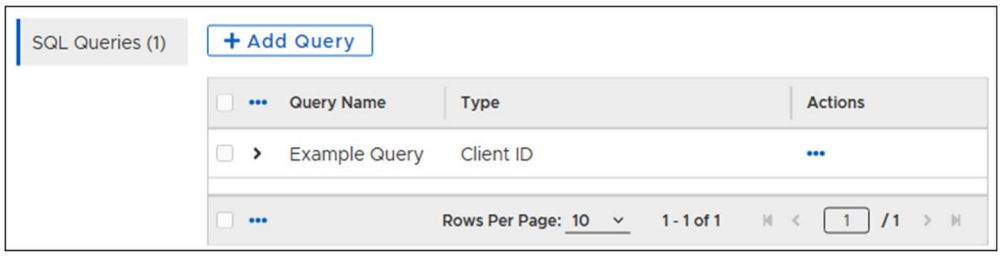
3. Write your SQL query in the **Query** text box.



Important

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

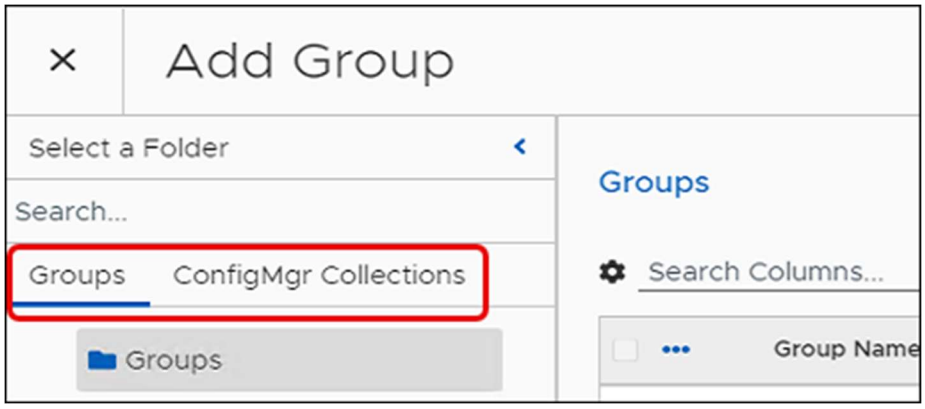
4. Select **Add Query** at the bottom left of the dialog. This returns you to the Business Unit template and populates a table with the new SQL query.



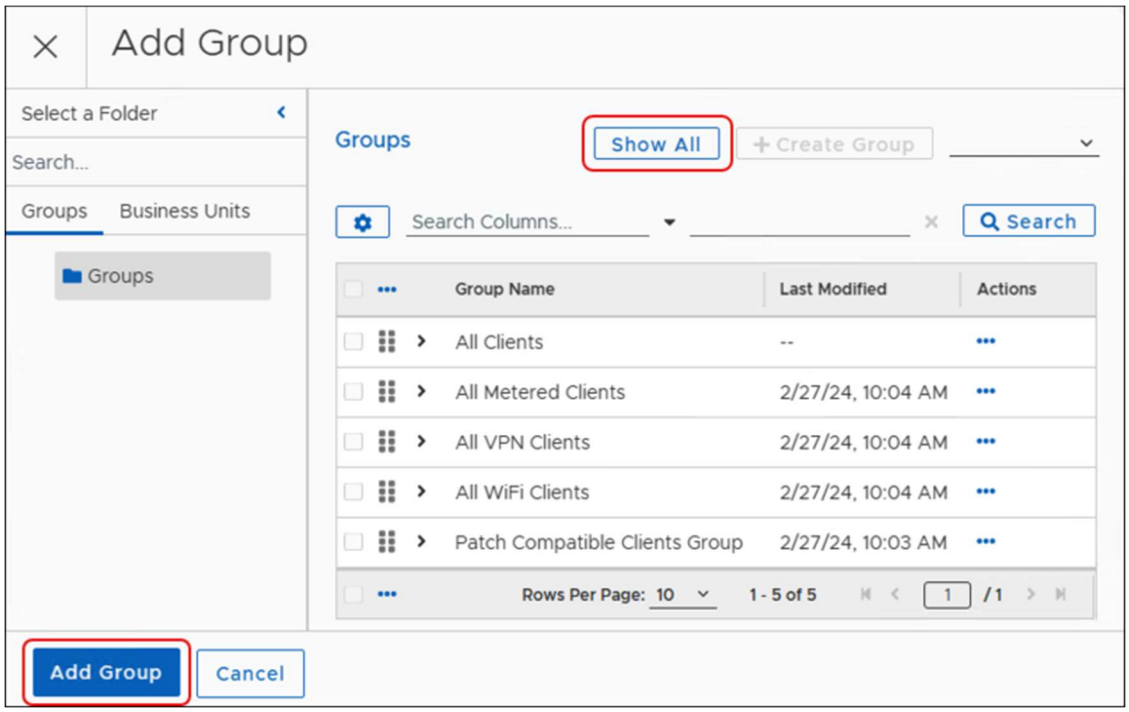
Set Base Scope

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

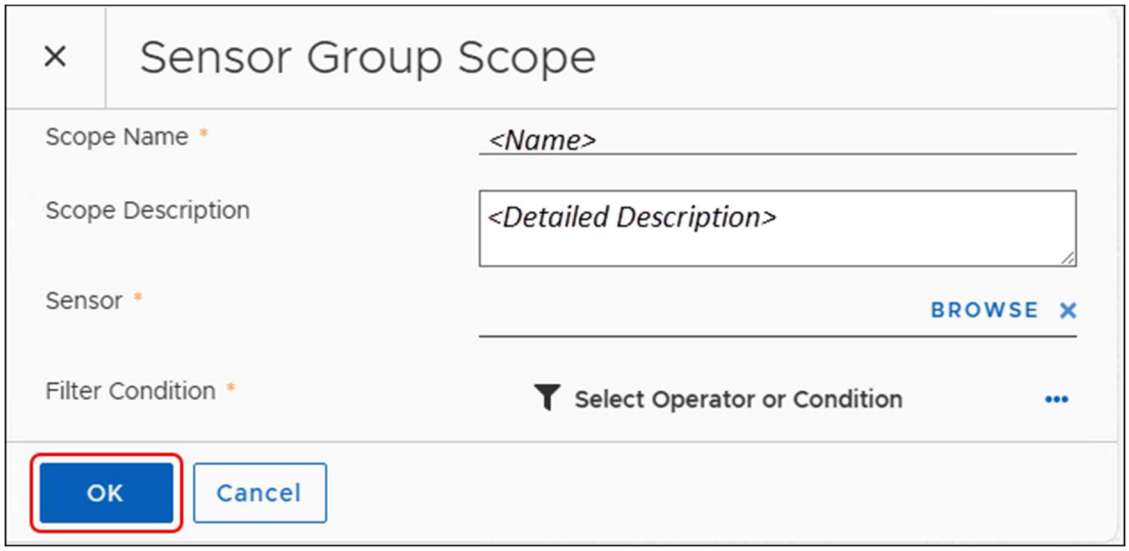
Sensors mark device inventory using technology settings such as Java, PowerShell, WMI, and so on. Tenable Patch Management includes choices for common sensor settings.

> **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:

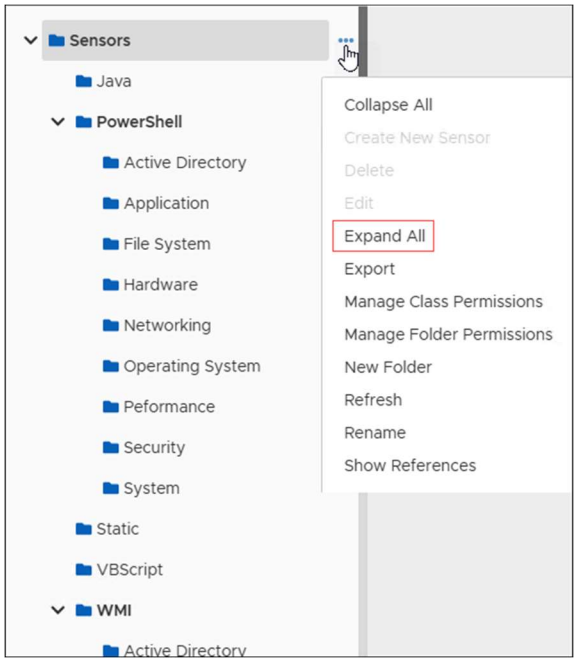
1. Select **Sensors** from **Business Unit Scopes**, and then click **+ Add Sensor Group Scope**.

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.



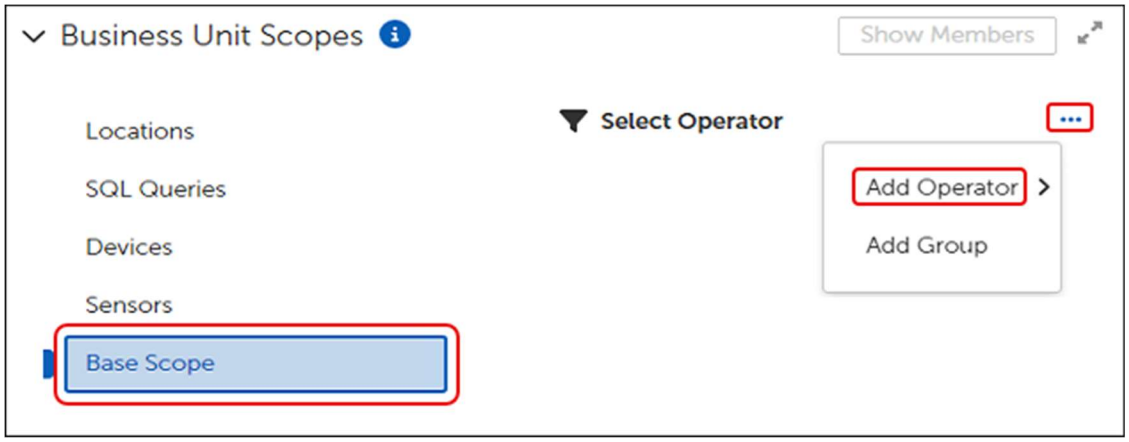
5. Select an item to use in your Sensor Group, and then click **Add Sensor**. This returns you to the **Sensor Group Scope** dialog.

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.

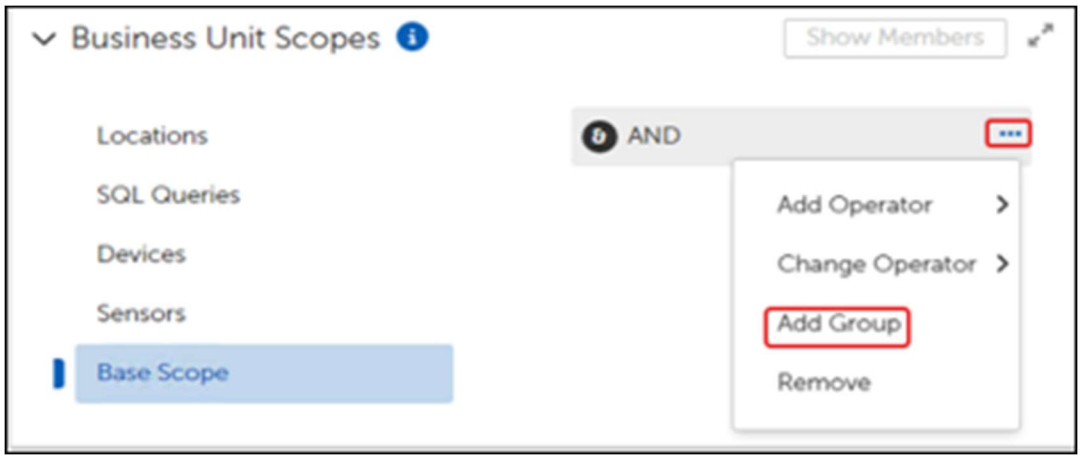
1. In the **Business Unit Scopes** section of an object template, click **Base Scope**.



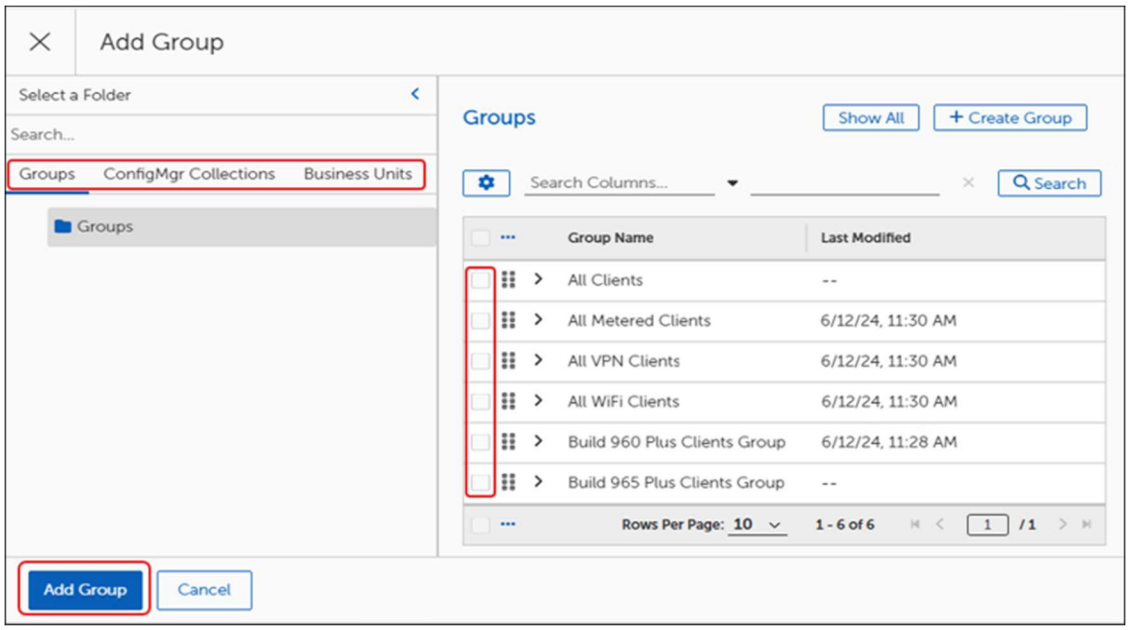
2. Select the **ellipsis (...)** to the right of **Select Operator** (or any existing Operator), and then select **Add Operator**.

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.



6. 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.

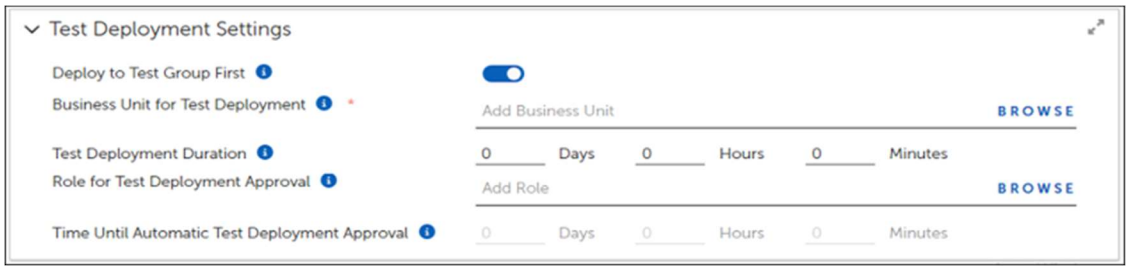
1. Make sure that the devices you want to use in the lab have the TenableClient installed and are associated with a TenableServer.

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.



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.

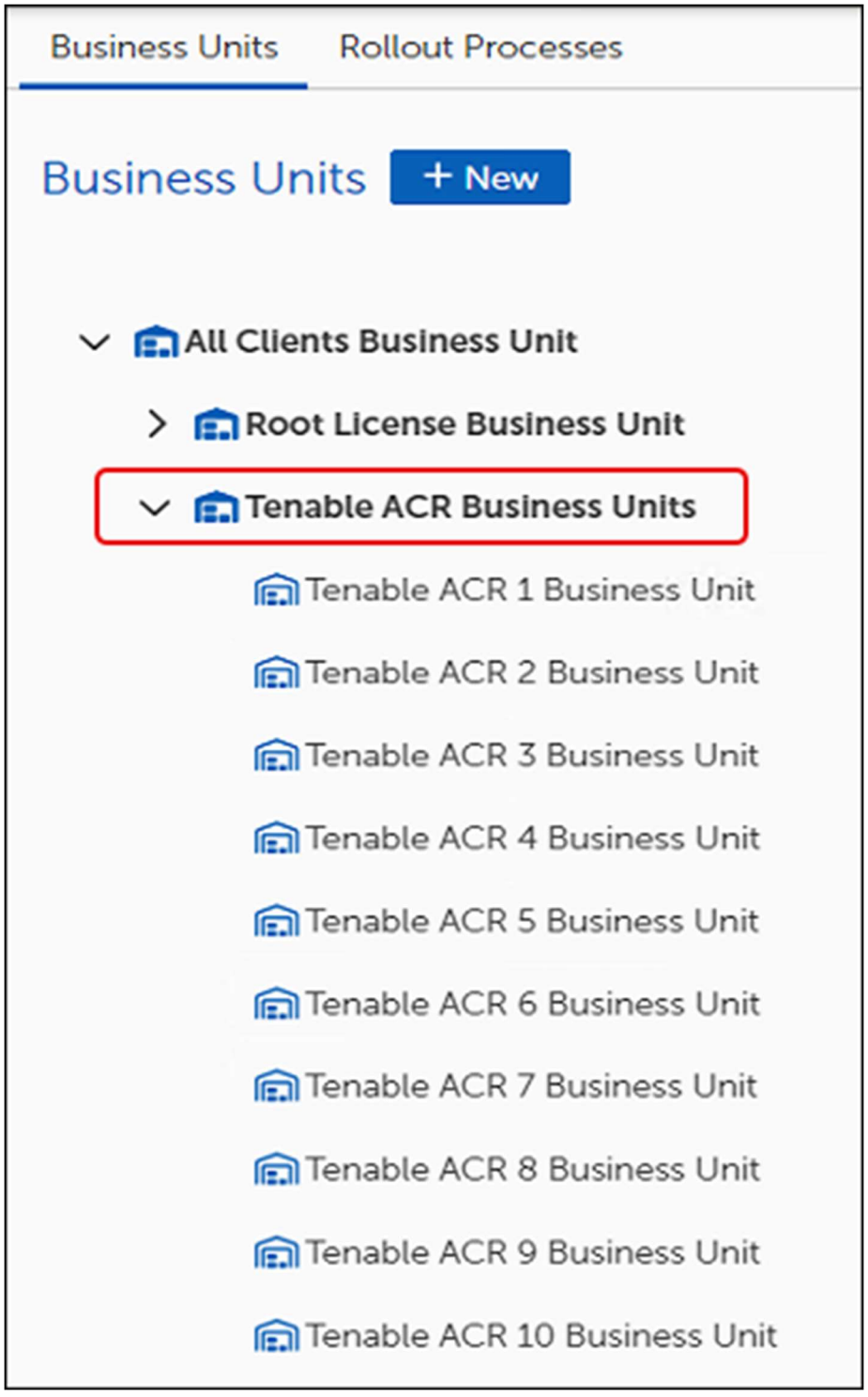
Open and Save a Business Unit Template

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

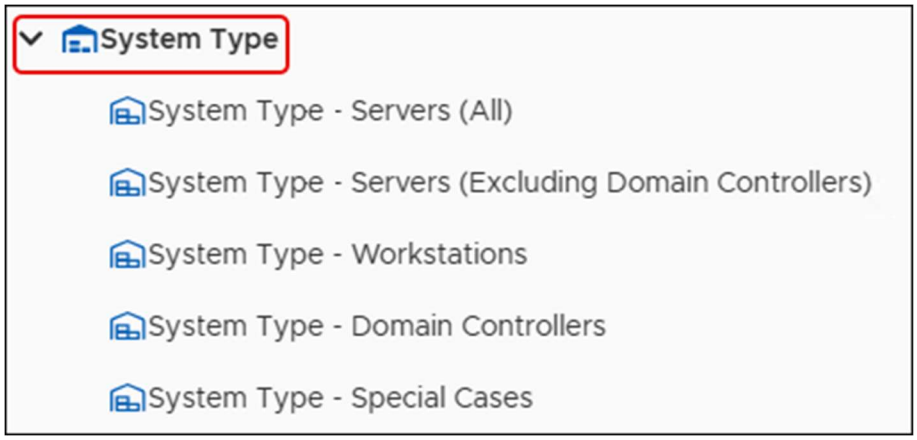
purposes. Except for Business Units provided for Root, you can copy the default templates and save them with new details, or you can create a new Business Unit.

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.



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 Organize New Patch Objects).

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.

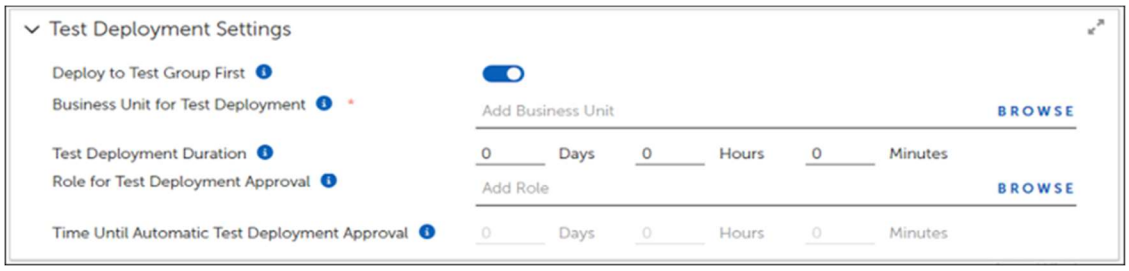
1. Make sure that the devices you want to use in the lab have the TenableClient installed and are associated with a TenableServer.

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.



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.

    c. Future deployments that match the exposure level you modified deploy to your test environment.

    d. 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

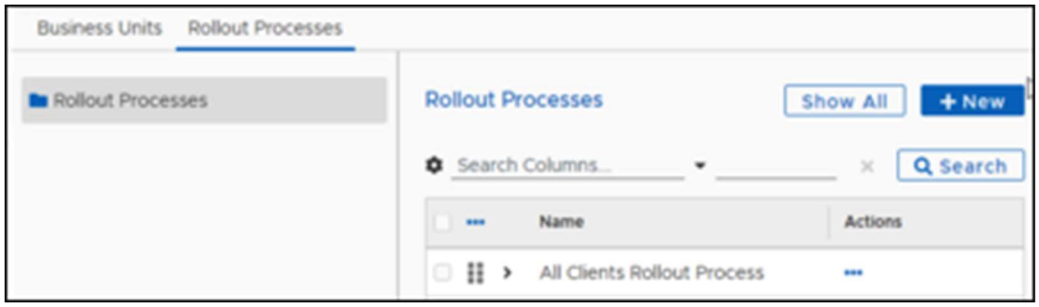
Designate Custom Business Units that a Lab Business Unit may use for testing purposes. If inherited from a parent Business Unit, values merge with the custom lab values of the parent and supersede parent values when conflicting.

Rollout Processes

Business unit rollout processes define which clients receive patches first and are the last step before patches reach clients. For example, a Business Unit rollout process can define rolling out to clients in batches of one hundred to allow administrators to view progress and catch any errors that occur before rolling out to additional devices.

After Patching Processes and Deployment Channel processes supply the details for the required activity, they delegate the rollout task to each Business Unit. The Business Unit manages its own rollout based on the customized **All Clients Rollout Process** workflow.

Before creating a custom Rollout Processes, enter a support ticket and request help from Tenable Customer Support.



Including Rollouts in Business Units

The Rollout process executes a workflow that queries information contained within a Business Unit template, such as Approval Chains, Notification Chains, and Related Business Units. The Business Unit uses this information to control the approval and deployment logic for new patches. The Rollouts also perform the actual client deployment to devices within the Business Unit.

New child Business Unit configurations automatically inherit the Rollout Process from the parent Business Unit. In most cases, this is the **All Clients Rollout Process**.

The Business Unit template you are editing might use a Rollout Process inherited from a parent Business Unit. Before you can change an inherited Rollout Process, you must turn off inheritance.

Patching Strategies

Patching Strategies are the central management objects in Tenable Patch Management because they group the details that define how, when, and where to patch third-party products. Tenable Patch Management includes prepopulated templates that address most patching scenarios. You can save these templates using your own titles and descriptions, and then customize them to your environment.

Purpose of a Patching Strategy

Each Patching Strategy uses building blocks that can include Schedules, Notifications (Chains), Deployment Channels, and Bots to define a given patching scenario. At minimum, a Patching Strategy must include a Patching Process and a Deployment Bot.

Functionally, a Patch Strategy performs the following:

Automated handling of new patches

Automatically discovers new patches and uses the Deployment Bot to match new patches to the Patching Strategy. The Patching Process queues patches for processing and, according to the set schedule, activates patch deployment in groups to minimize the impact on endpoints and end users.

Customized targeting of patches

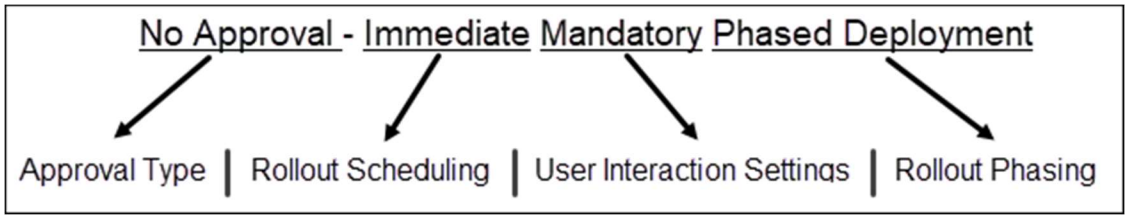
Administrators can target specific products and high-profile patches that trigger a Deployment Bot based on individual products. Targeting is particularly useful when you first install Tenable Patch Management, have a considerable number of products that require patching, and you prefer to review the progress of patching before fully automating the process.

Reuse Intent Schema Objects

All objects in Tenable Patch Management are interoperable and designed for use in any Patching Strategy. Create a patching process, schedule, notification or approval chain, or deployment process once, and then use them in various Patching Strategies depending on your needs.

Patching Strategy Template Naming Conventions

Tenable Patch Management Patching Strategy templates cater to four specific use cases: Approval Types, Rollout Scheduling, User Interaction Settings, and Rollout Phasing. When deciding which Patching Strategy to choose, consider the following example to understand naming:



By offering various combinations of these parameters, the templates are a versatile framework that can accommodate a wide range of patching scenarios.

Minimal customization includes adding the products to patch and a schedule. This flexibility allows for efficient patch management without the need for extensive customization or the creation of new strategies.

- **Approval Type**: Level of approval needed prior to deployment:
    a. **No Approval:** Deploys at once.
    b. **Initial Approval**: Requires approval prior to deploying.
    c. **Phased Approval**: Requires approval between each wave in the Deployment Waves object.
- **Rollout Scheduling**: Defines the schedule and impact of a deployment.
    a. **Immediate**: All product patches deploy at once.
    b. **RiskBased**: Targeted and controlled deployment based on specific risk levels (low, medium, high, critical). Schedule and run patch deployments based on risk levels. Uses Deployment Channels.
- **User Interaction**: Defines permitted user actions related to the patch installation.
    a. **Mandatory**: Alerts the end user who can postpone depending on User Interaction Settings but cannot not decline. All product patches deploy at once.
    b. **Options**: Alerts the end user. Otherwise, functionality not available in this release.
- **Rollout Phasing**: Deploys in separate phases to allow a review before continuing.
    a. Minimal customization includes adding the products to patch and a schedule.
    b. This flexibility allows for efficient patch management without the need for extensive customization or the creation of new strategies.

Patching Strategy Templates

Effective management and deployment of software patches is crucial for maintaining the security and stability of an IT infrastructure. The included Patching Strategies address various deployment scenarios and considerations.

Recommended Use

You can choose a Patching Strategy template, save it under a descriptive local naming convention, and then customize it as needed. Patching Strategy templates reference objects that include the minimum requirements for a successful patching strategy: Deployment Wave, Deployment Bot, and Patching Process.

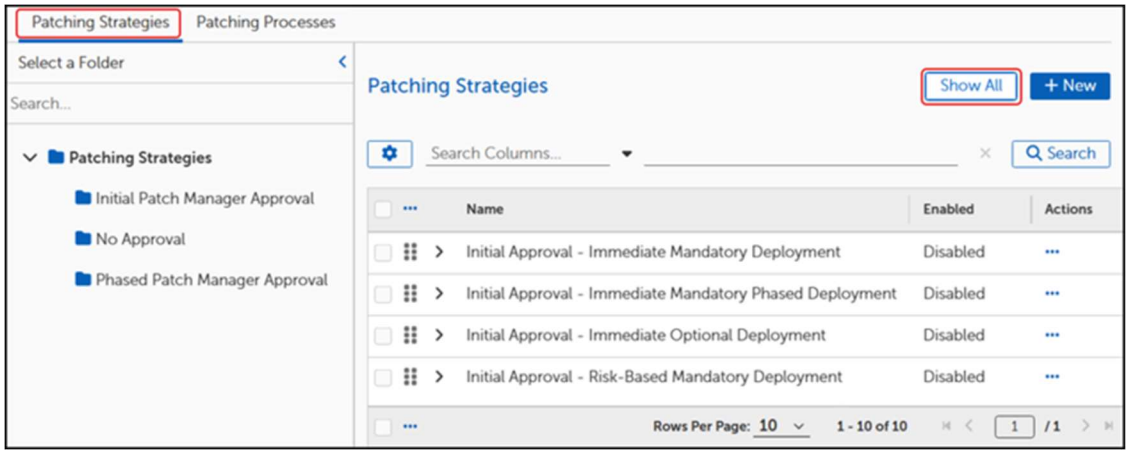
Tenable recommends creating a folder to hold all new or customized strategies. This separates them from the strategies provided by Tenable (see Create a New Folder for Objects).

View built-in Patching Strategies

These built-in strategies are often enough to get an organization started with a patch deployment scenario. To build a Patching Strategy using an Tenable template, see Creating a Patching Strategy.

1. Hover over or select the right-arrow next to **Strategy** in the left pane of the Tenable Patch Management dashboard, and then select **Patching Strategies**.

2. Select any **Patching Strategy** to see the available templates associated with that strategy.



Initial Patch Manager Approval Strategies

Each of these strategies requires an approval step before deploying updates. Except for Risk Based Mandatory Deployment, the Patching Process within these strategies manages the deployment process exclusively and does not use Deployment Channels.

Similarly, the Deployment Bot does not apply any filtering mechanism, so the Patching Process manages all updates related to the products included in the non-risk strategies.

- **Initial Approval - Immediate Mandatory Deployment**

  Approval required prior to deployment, then deploys at once with no user interaction.

- **Initial Approval - Immediate Mandatory Phased Deployment**

  Approval required prior to deployment, then deploys at once in a phased manner, rolling out to each wave of business units sequentially with no user interaction control.

- **Initial Approval - Immediate Optional Deployment**

  Approval required prior to deployment, then deploys at once in a phased manner, rolling out to each wave of business units sequentially. User interaction allowed.

- **Initial Approval - Risk-Based Mandatory Deployment**

  Approval required prior to deployment, and then deploys at once to all devices in the targeted business units based on the patch risk levels.

  Uses both Deployment Waves and Deployment Channels. Higher-risk updates have priority in high-frequency Deployment Channels. Lower-risk updates belong to lower-frequency Channels.

  Also uses Deployment Bot to filter patches based on risk level, and then sends the final wave to the proper Deployment Channels.

  Ensures processing and deployment of the final wave through the most suitable Deployment Channel and adds a layer of control and customization to the deployment process.

No Approval Strategies

Each of these strategies requires no approval before deploying updates. Except for Risk Based Mandatory Deployment, the Patching Process within these strategies manages the deployment process exclusively and they do not use Deployment Channels.

Additionally, the Deployment Bot does not apply any filtering mechanism, so the Patching Process manages all updates related to the products included in the non-risk strategies.

- **No Approval - Immediate Mandatory Deployment**

  No approval needed prior to deployment. Deploys at once with no user interaction.

- **No Approval - Immediate Mandatory Phased Deployment**

  No approval needed prior to deployment. Deploys at once in a phased manner, rolling out to each wave of Business Units sequentially. No user interaction.

- **No Approval - Immediate Optional Deployment**

  No approval needed prior to deployment. Deploys at once to all devices in the targeted business unit. User interaction allowed.

- **No Approval - Risk-Based Mandatory Deployment**

  No approval needed prior to deployment. Deploys at once to all devices in the targeted business units based on the patch risk levels. No user interaction.

  Uses both Deployment Waves and Deployment Channels. Higher-risk updates have priority in high-frequency Deployment Channels. Lower-risk updates belong to lower-frequency Channels.

  Also uses Deployment Bot to filter patches based on risk level, and then sends the final wave to the proper Deployment Channels.

Ensures processing and deployment of the final wave through the most suitable Deployment Channel and adds a layer of control and customization to the deployment process.

Phase Approval Strategies

Each of these strategies requires phased approvals before deploying updates. Except for Risk Based Mandatory Deployment, the Patching Process within these strategies manages the deployment process exclusively without using Deployment Channels.

Similarly, the Deployment Bot does not apply any filtering mechanism, so the Patching Process manages all updates related to the products included in the non-risk strategies.

- **Phase Approval - Immediate Mandatory Phased Deployment**

  Approval required between each wave of the deployment, and then deploys the updates in a phased manner, rolling out to each wave of business units sequentially. No user interaction.

- **Phase Approval - Risk-Based Mandatory Deployment**

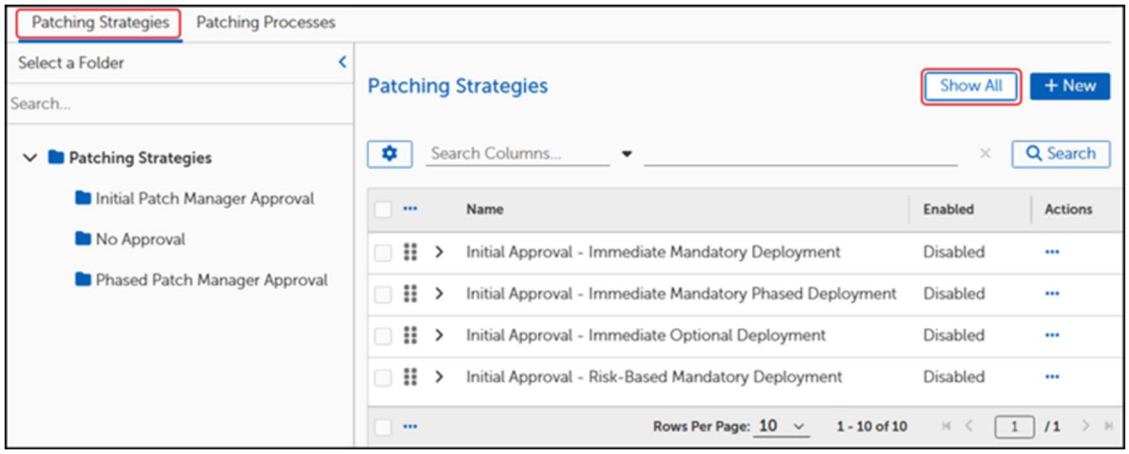
  Approval step required between each wave of the deployment, and then deploys the updates at once to all devices in the targeted business units based on risk levels. No user interaction.

Creating a Patching Strategy

A Patching Strategy template contains specific fields that you can configure to make a unique Patching Strategy for your environment. Tenable recommends opening an existing strategy that contains most of the configurations items you want, and then saving it with a new name and description. The configuration options are the same whether you create a new strategy or modify an existing strategy.

Open and Save a Patching Strategy Template

1. Follow the instructions in Create a New Folder for Objects.
2. Hover over or click **Strategy** in the left navigation menu of the Tenable Patch Management Enterprise Dashboard, and then select **Patching Strategies**.
3. Select **Show All** to see all available Patching Strategies. This populates the **Patching Strategies** table with the available templates.

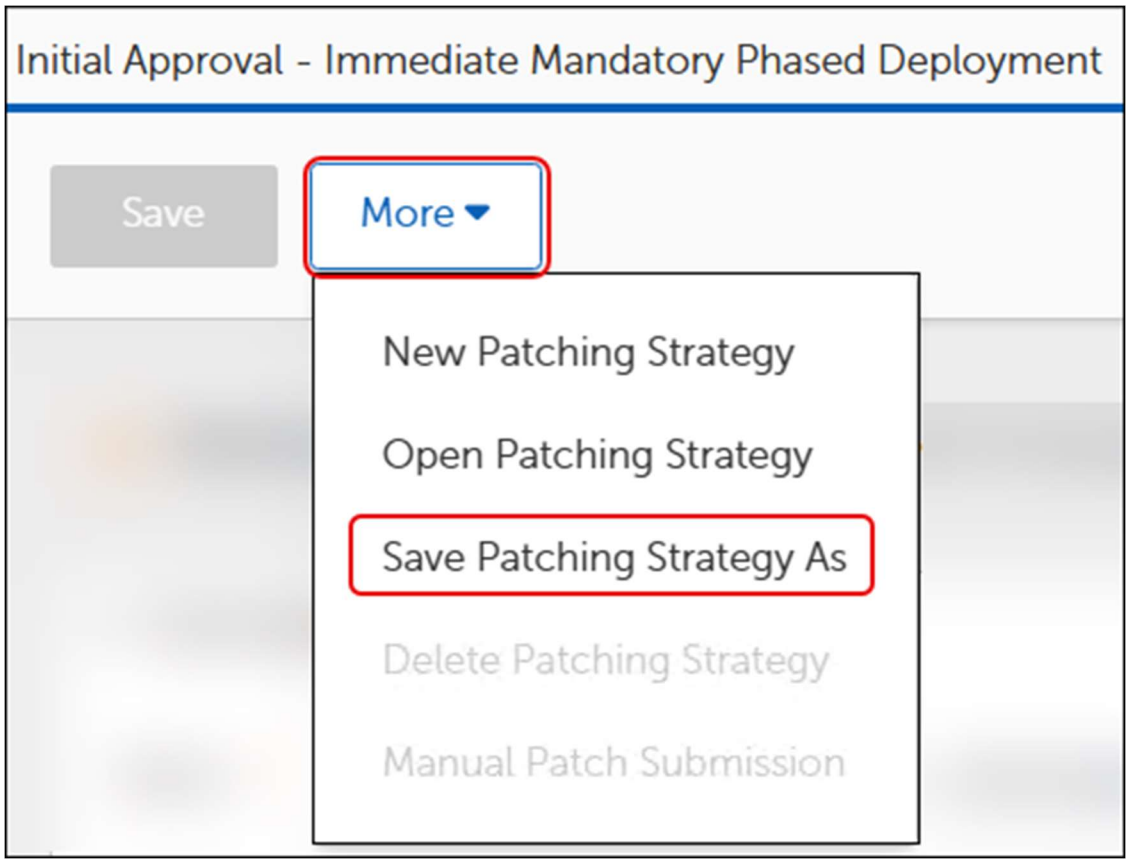


For descriptions of each template type, see Patching Strategy Templates.

4. Enter the **Name** of an existing strategy on the Search bar, and then click **Search**.

5. Select the **Name** of the strategy to open it.

6. Select **More** in the upper left corner of the template, and then select **Save Patching Strategy As**:



a. Enter a unique name that reflects what the strategy does conceptually. For example, ITS Immediate Daily Product Patching.

b. Select **OK**. This opens your strategy template with all the default entries for the built-in strategy, including a detailed description.

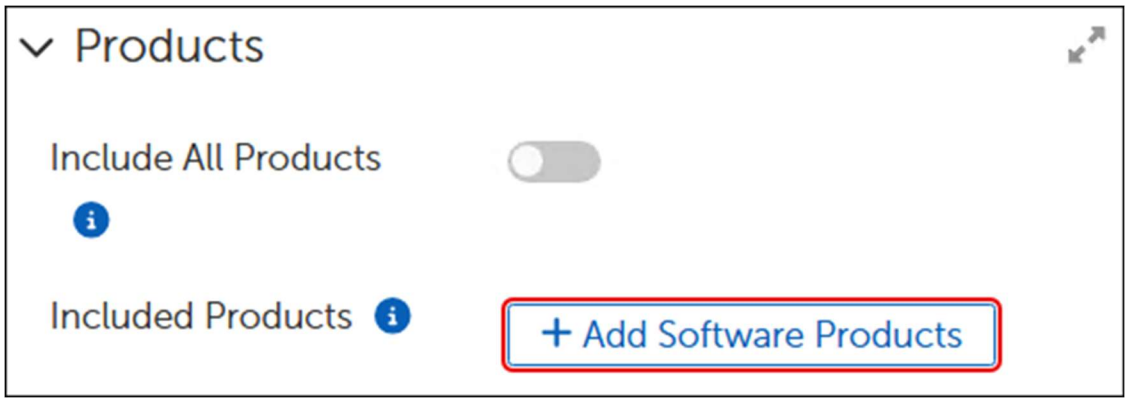
c. Enter a detailed **Description** of your new template or keep the existing detail, and then click **Save** on the upper-left corner of the dialog.

Tip

Remember to click Save on the upper left corner to save your progress. After completing the Patching Strategy configuration, you must save and enable the completed strategy to make it available for use.

Add Software Products

1. Scroll to the **Products** workspace in an open Patching Strategy template:



   a. To include all products (not recommended), click the **Include All Products** toggle to enable it.

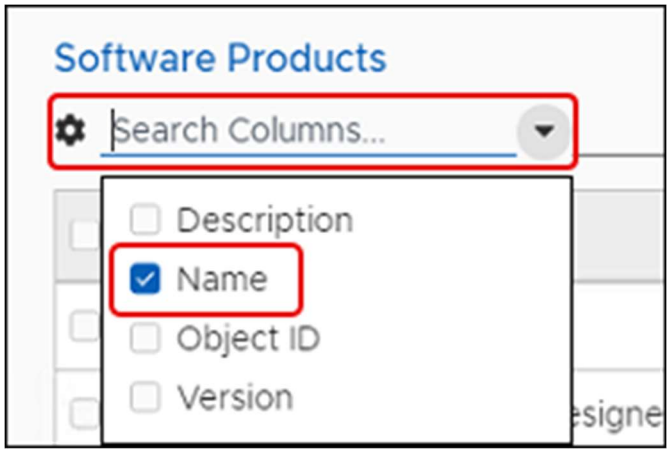
   Caution

   Tenable recommends including only the specific products used in your environment. Including all products means using the entire Tenable library of products.

   b. To include specific products (recommended), click **Add Software Products**.

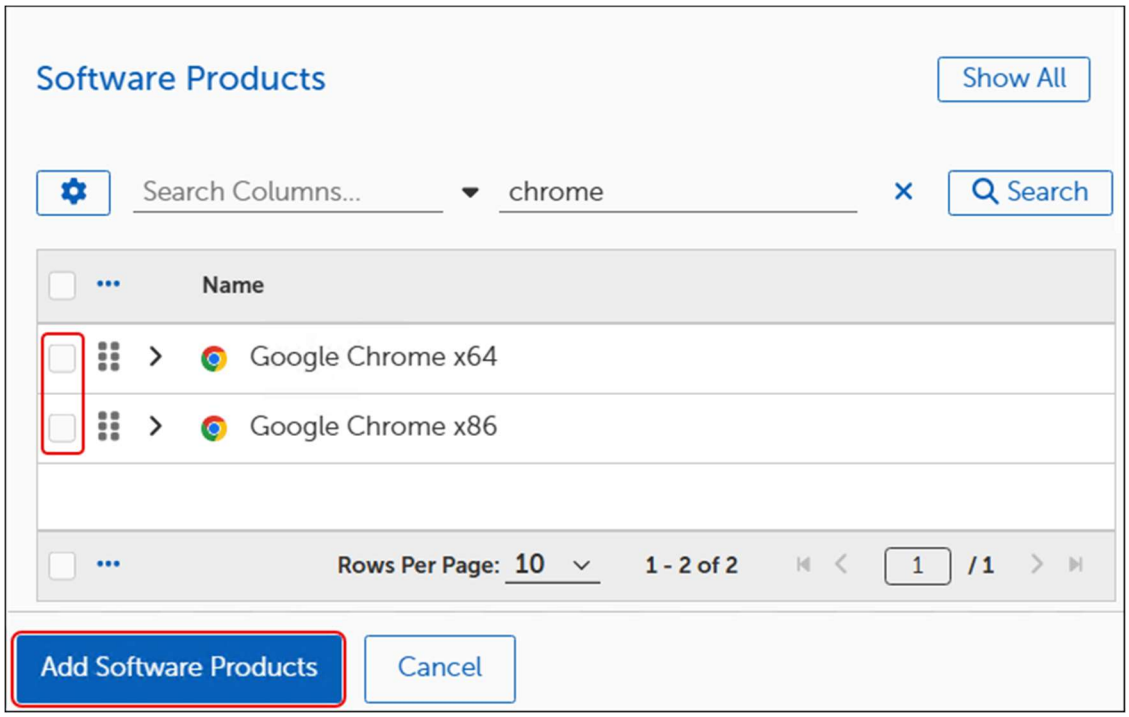
2. Select **+ Add Software Products.**

3. Select the **Down Arrow** next to **Search Columns** and select the search information type that identifies the product you want to include.



4. Enter the **product information** on the search line, and then click **Search**.

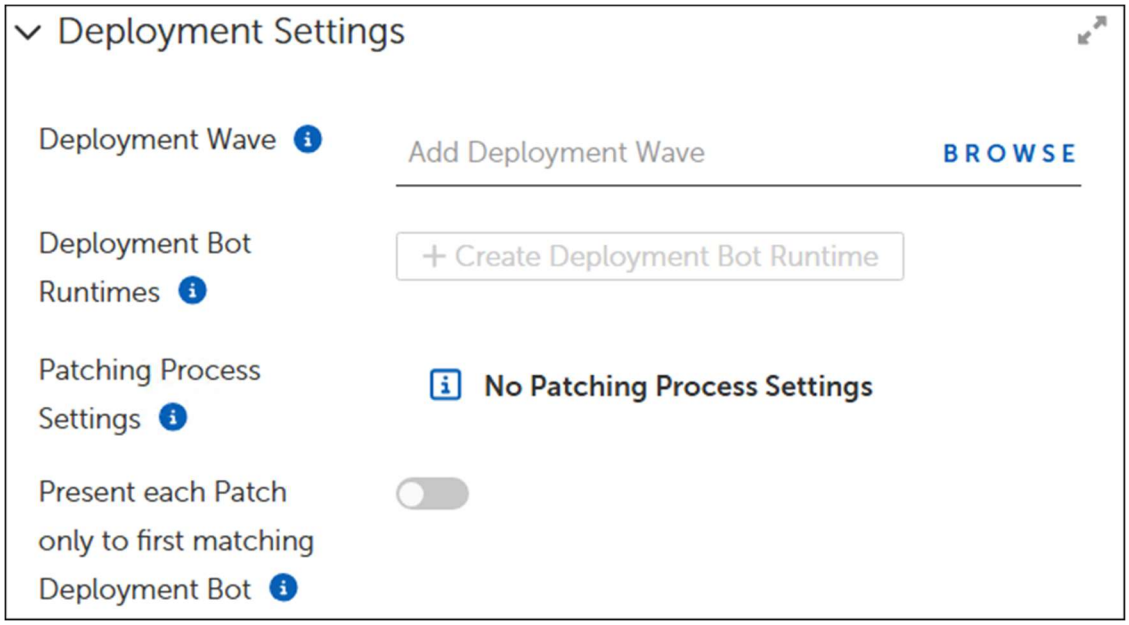
5. Select the **box** next to the product you want to add. You may search for and include as many products as you need for this strategy, and then click **Add Software Products** at the bottom left of the dialog.



6. Select **Add Software Products** on the bottom left of the dialog to save your additions.

Deployment Settings

Deployment settings in a Patching Strategy include selecting a Deployment Wave, Creating Deployment Bot Runtime configurations, and choosing whether to present each patch to the first matching Deployment bot only (defaults to enabled). When customizing an existing Patching Strategy (recommended), settings may include tables with configuration selections other than the default.

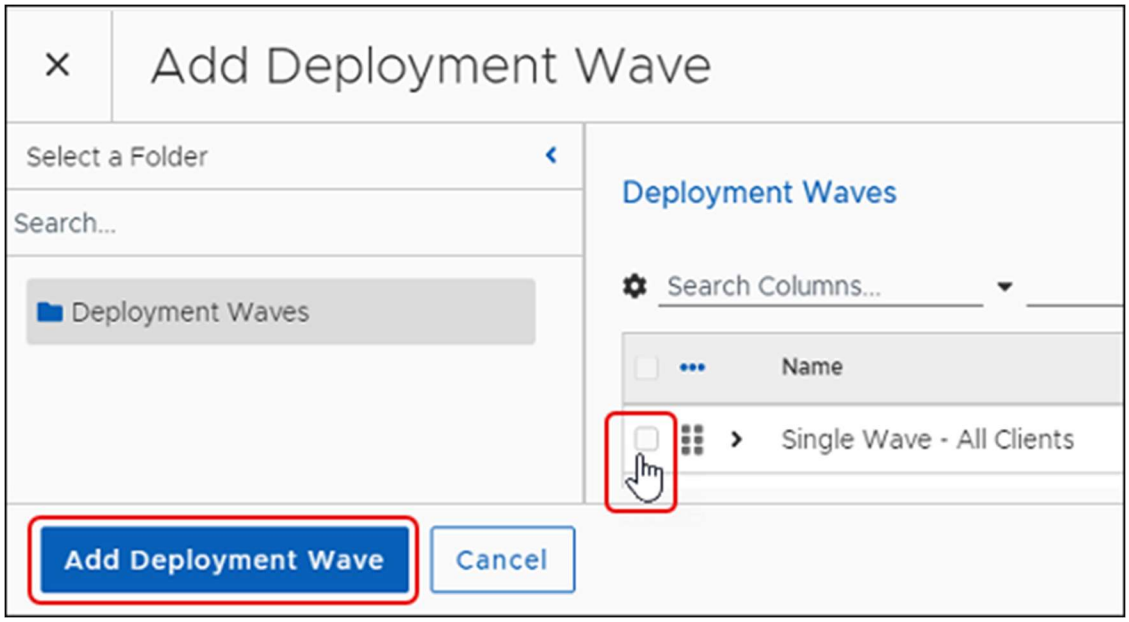


Begin by adding a Deployment Wave.

Add a Deployment Wave

1. Select **Browse** next to **Add Deployment Wave** in the **Deployment Settings** workspace of an open Patching Strategy template.

This opens the **Add Deployment Wave** dialog.



2. Select a **Deployment Wave** from the list. Tenable provides a **Single Wave-All Clients** Deployment Wave, which includes a Business Unit called **All Clients Business Unit**.

3. Select **Add Deployment Wave** on the bottom left of the dialog. This returns you to the Patching Strategy template.

Deployment Bot Runtime Settings

In Patching Strategy templates, the **Create Deployment Bot Runtime** dialog provides a single location to add processes to your Patching Strategy. Use these settings for more advanced operations. For example, when you have multiple Business Units that require the same Patch Deployment Bot but use a different Patching Process and schedule, you can create multiple Deployment Bot Runtime combinations to patch according to different requirements.

See also:

Bots – Patch Deployment and Notification Bots

Patching Processes

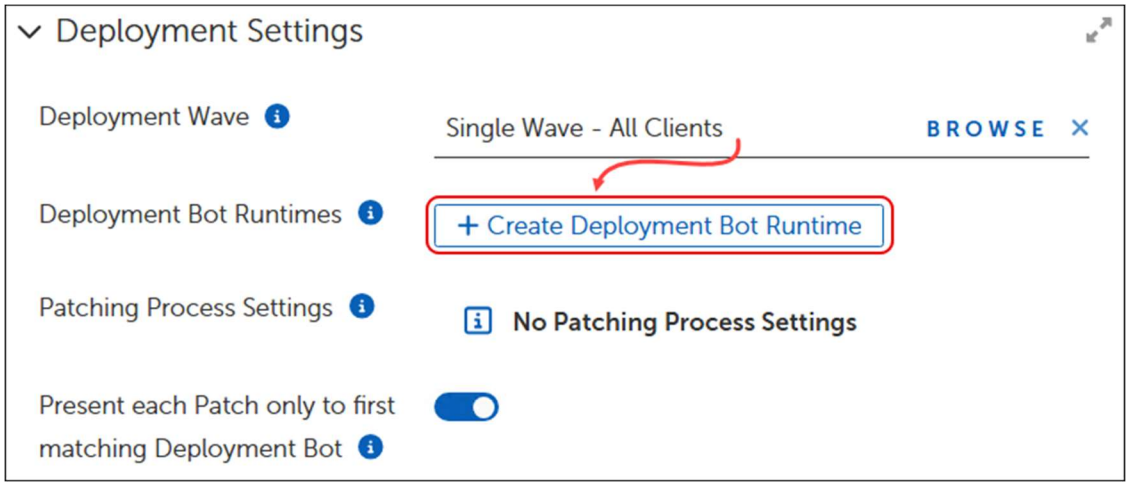
Deployment Channels and Deployment Channel Processes

Business Units and Rollout Processes

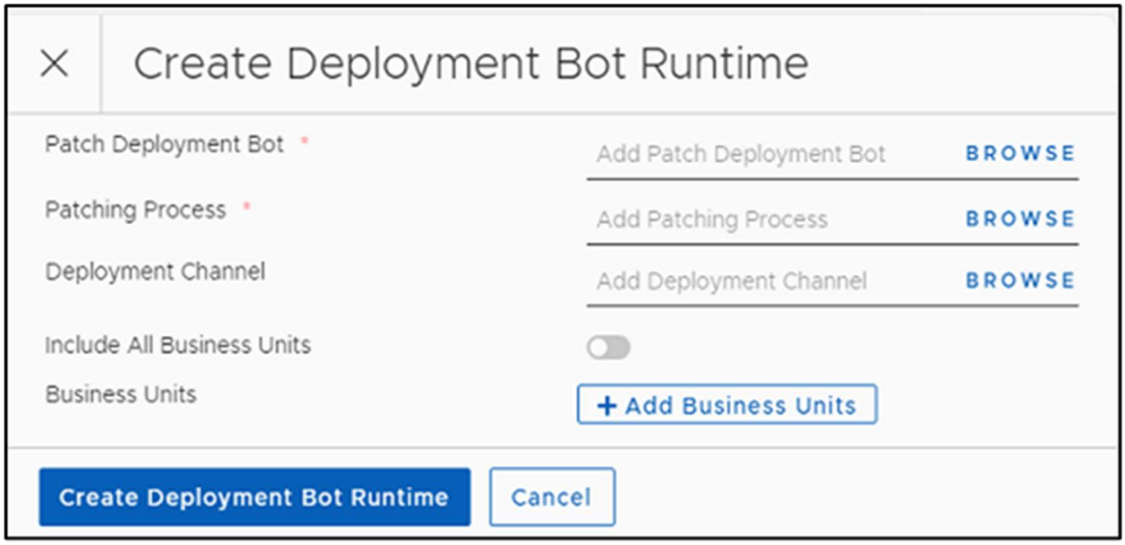
Create one or more Deployment Bot Runtime Scenarios

After adding a Deployment Wave to the Patching Strategy Deployment Settings, you can configure Deployment Bot Runtime scenarios. These copnfiguration options allow you to create scenarios that use the same Deployment Bot with different Patching Processes (schedules) for the same or different Business Units. Follow these procedures for each Deployment Bot Runtime you need to create.

Select **+ Create Deployment Bot Runtime** from the **Deployment Settings** workspace of an open Patching Strategy template.



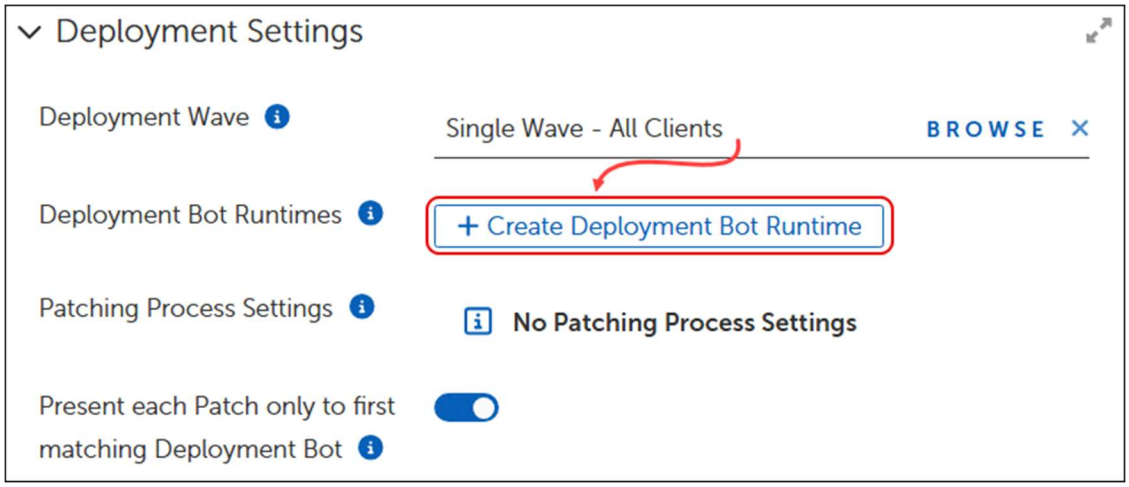
This opens the Create Deployment Bot Runtime dialog:



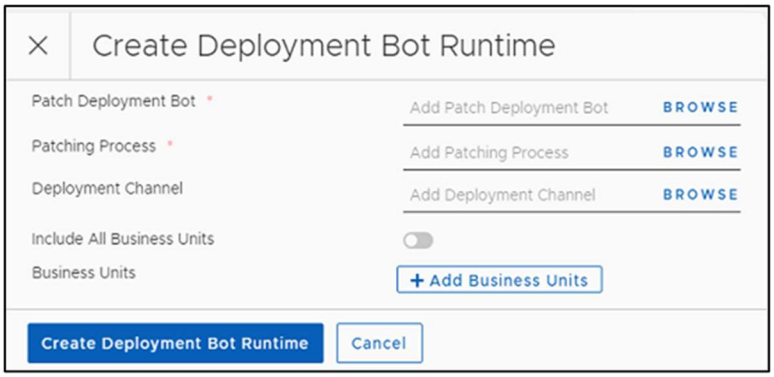
1. Begin by adding a Patch Deployment Bot.

Add a Patch Deployment Bot (Required)

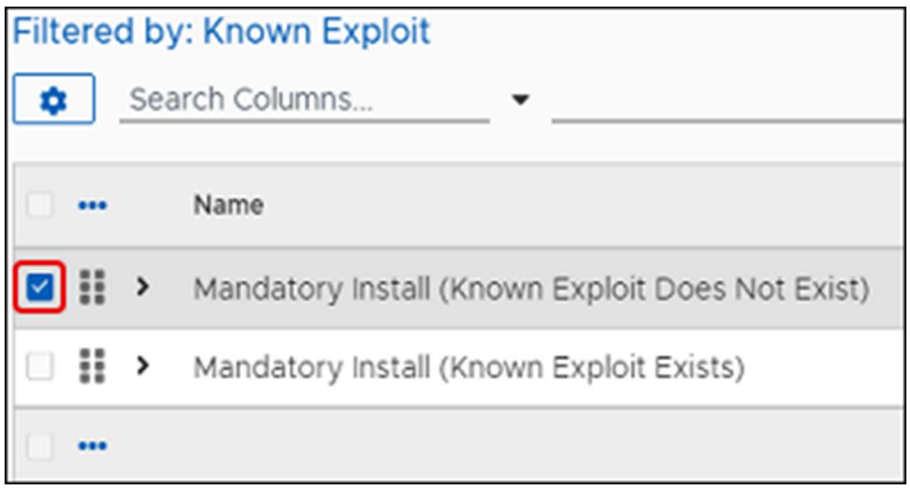
1. Add a Deployment Wave in the **Deployment Settings** workspace of an open Patching Strategy template. This enables +Create Deployment Bot Runtime.



2. Select **+Create Deployment Bot Runtime** to open the configuration dialog.



3. Select **Show All** to see the available templates or click **Filtered by:** in the Bots list to see only the templates associated with that filter.



Important

A Patching Strategy presents each applicable patch sequentially to each Deployment Bot in the Runtime, from top to bottom. Be sure to organize the Deployment Bots in

the Runtime from most important to least. You can enable or disable whether the Patching Strategy stops presenting patches to later Deployment Bots after discovering a match.

4. Select the template you want to use. For example, in **Filtered by: Known Exploit**, select **Mandatory Install (Known Exploit Exists)**.

5. Select **Add Patch Deployment Bot** on the bottom left of the dialog.

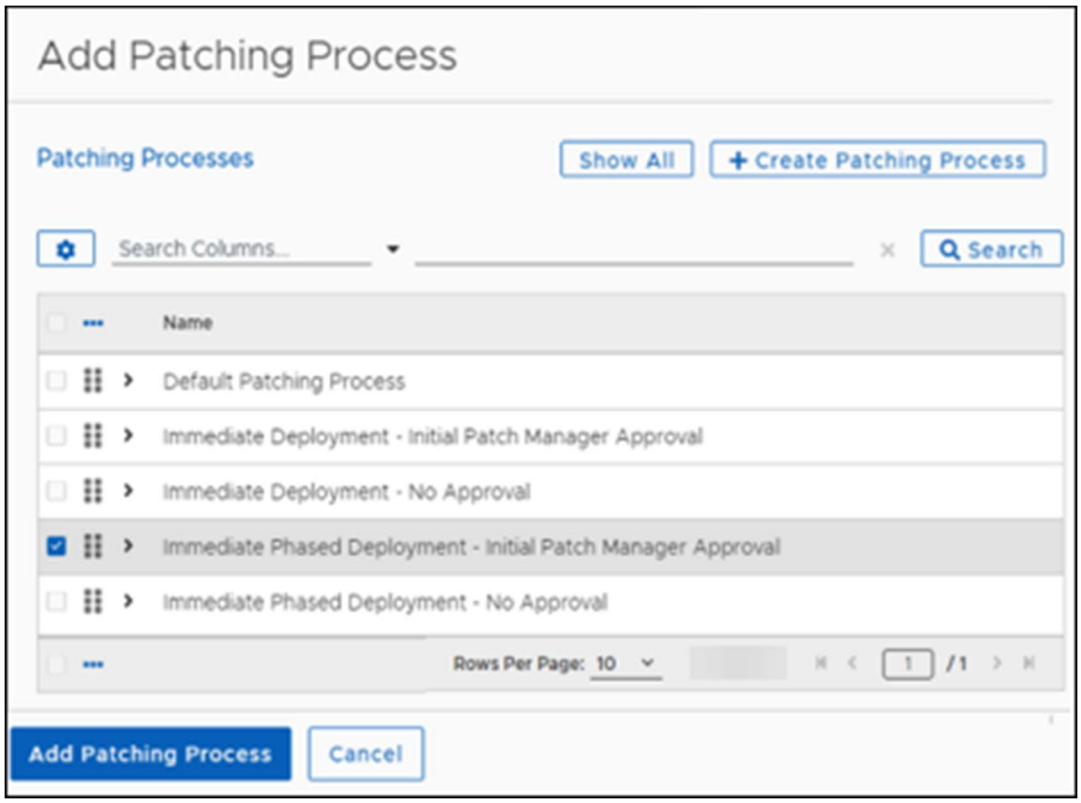
Add a Patching Process (Required)

1. Select **Browse** next to **Add Patching Process** in the Create Deployment Runtime dialog.

2. Select **Show All** to see the available processes.

3. Select the process you want to use. For example, select **Immediate Phased Deployment – Initial Patch Manager Approval)**.

4. Select **Add Patching Process** on the bottom left of the dialog.



Add a Deployment Channel (Optional)

1. Select **Browse** next to **Add Deployment Channel**.

2. Select **Show All** to see the available channels.

3. Select the channel you want to use. For example, select **Daily (13hrs)** to run the Deployment Channel at 1:00 pm every day.

4. Select Add Deployment Channel on the bottom left of the dialog.

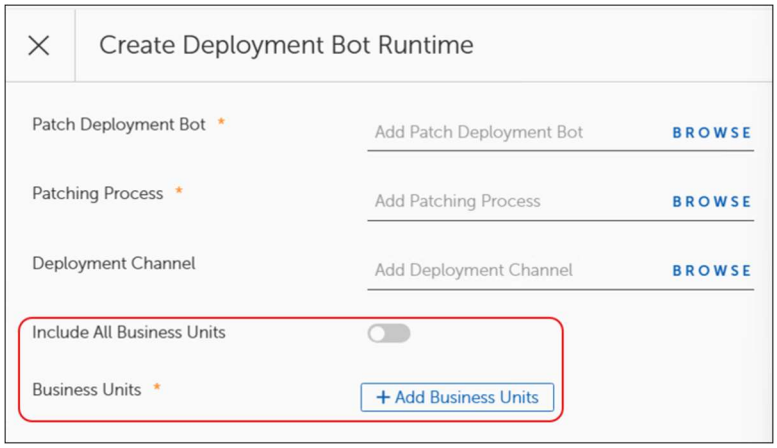
Add Business Units (Optional)

Important

The Business Units you add here must be the same Business Units included in the Patching Strategy Deployment Wave. If you select other Business Units here or select All Business Units, the Patching Strategy will take no action on those that do not match the Deployment Wave settings.

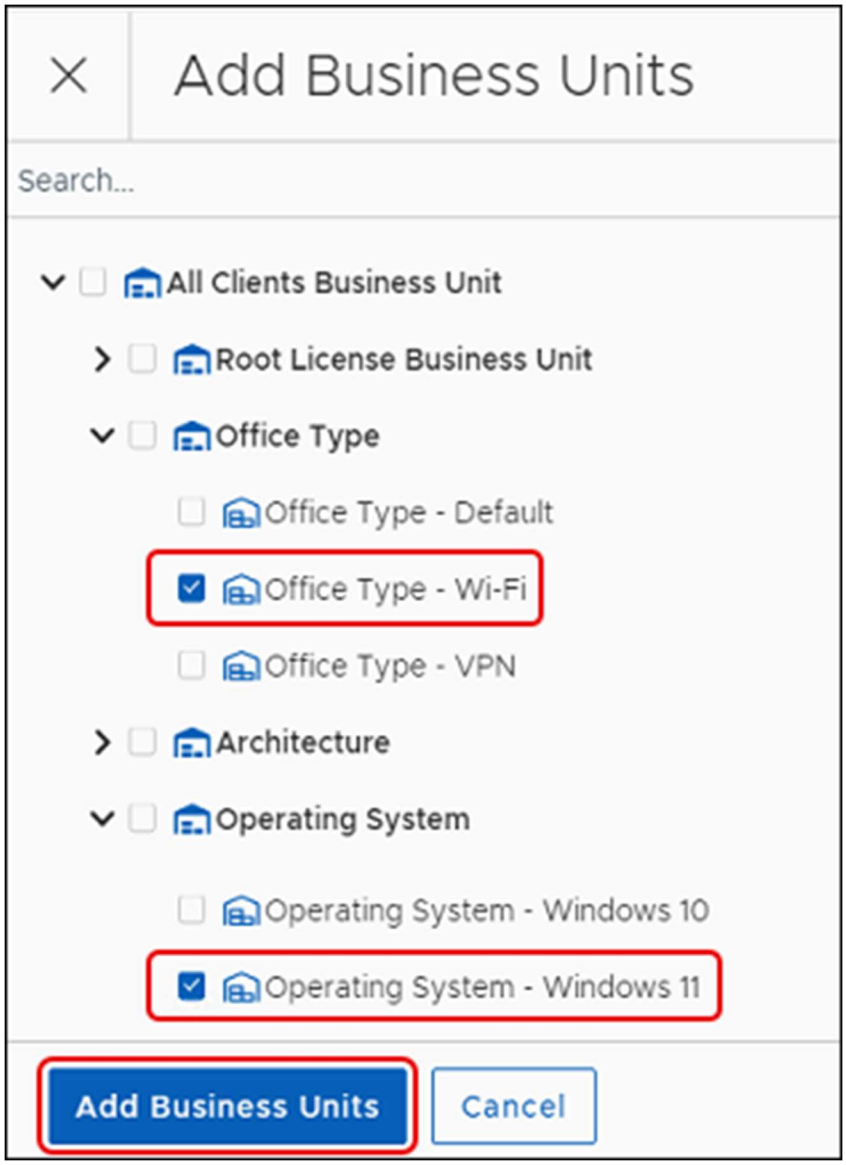
1. Decide whether to include all Business Units in this Deployment Bot Runtime, or to add specific Business Units:

   To include all Business Units, click the **Include All Business Units** toggle to enable running this configuration on all Business Units, and then skip to step 3.



   c. To choose specific Business Units to use this Runtime, click **+ Add Business Units**, and then continue with the next step.

2. Select one or more **Business Units** to add to this Runtime. For example, to use this Runtime on all Windows 11 systems using a Wi-Fi connection, select **Operating System – Windows 11** and **Office Type – WiFi**.



3. Select **Add Business Units** on the bottom left of the dialog to view the completed Runtime Bot.

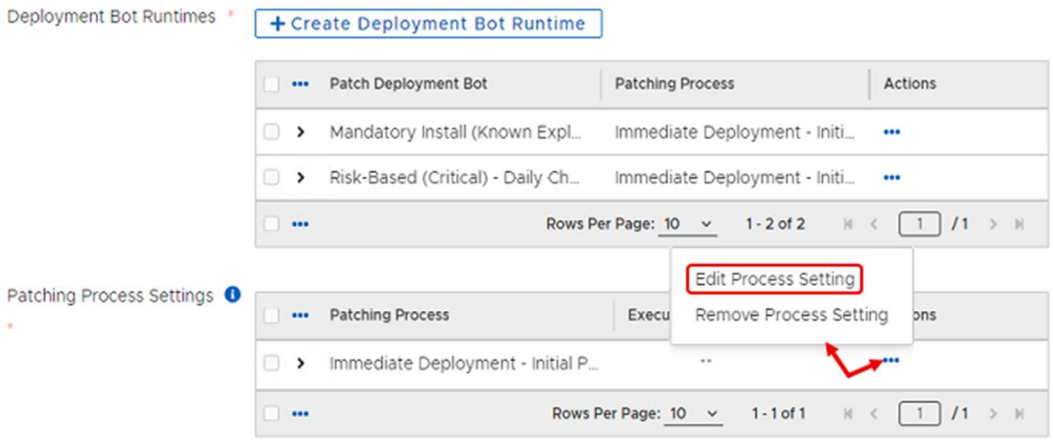
4. Select **Create Deployment Bot Runtime** on the bottom-left corner of the dialog to return to the Patching Strategy.

5. Return to Create one or more Deployment Bot Runtime Scenarios to add more Deployment Bot/Patching Process pairs to this Patching Strategy.

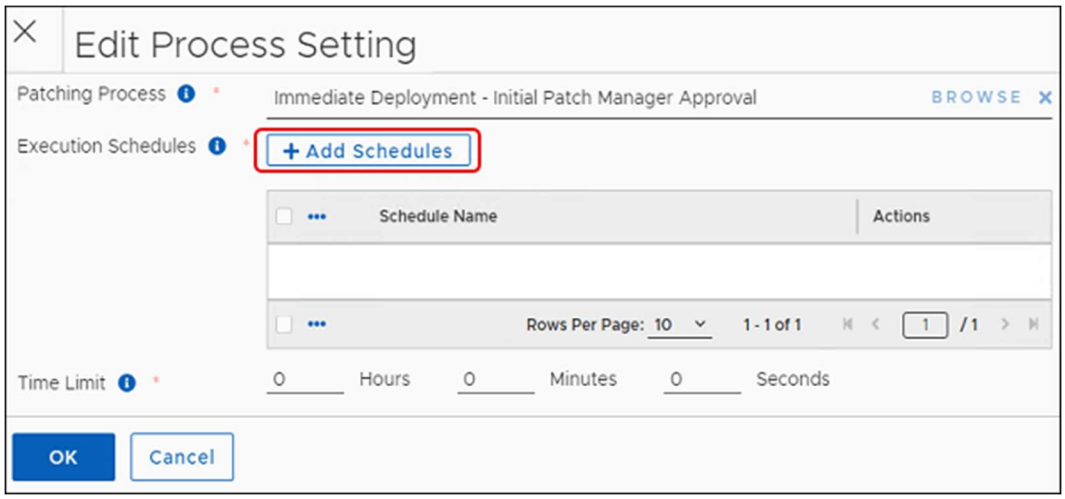
Set the Patching Process Runtime

After creating a Deployment Bot Runtime, set the runtime schedule for each Patching Process.

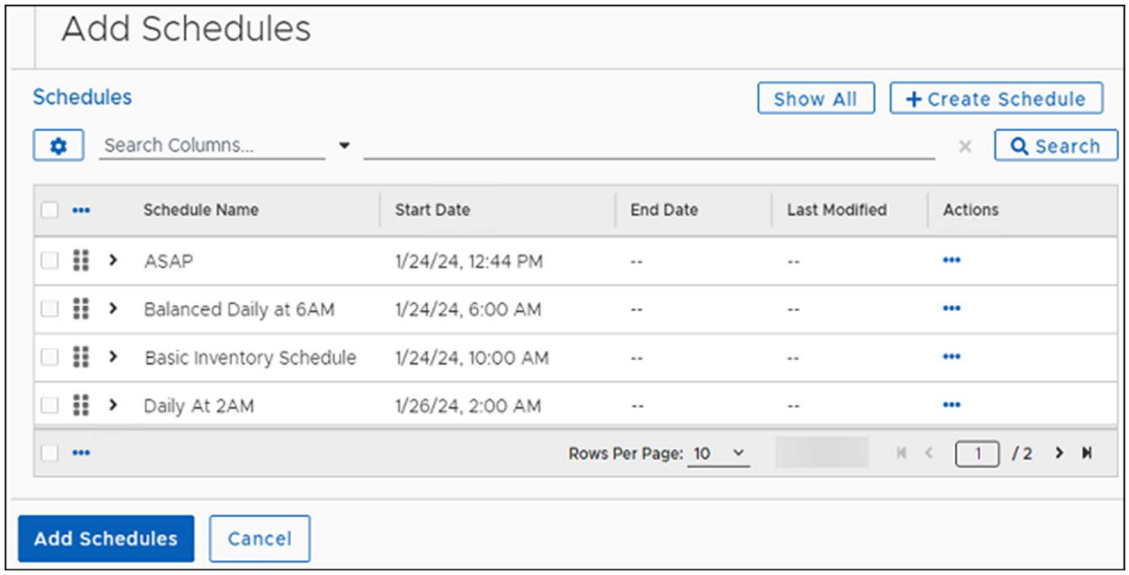
1. Select the **ellipsis (...)** under **Actions** in the **Patching Process Settings** table of an open Patching Strategy template, and then select **Edit Process Setting**.



2. Select **+ Add Schedules**.



3. Select the **Schedules** you want to use for the Process Setting. All Deployment Bot Runtime pairs that use the same Patching Process in this Patching Strategy will run on the schedules you choose.

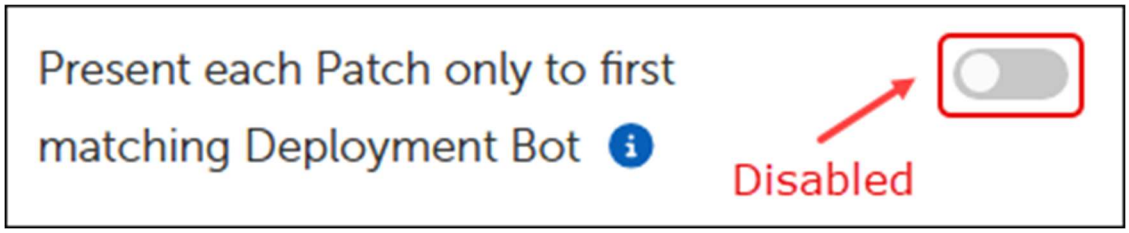


4. Select **Add Schedules**, and then click **OK** to return to the Patching Strategy workspace.

Present Patches to the First Matching Deployment Bot

This toggle switch enables or disables whether the Patching Strategy stops presenting patches to Deployment Bots as soon as it discovers the first matching Deployment Bot. If you choose to enable this behavior, be sure to order the Bots in your Deployment Bot Runtime from most important to least.

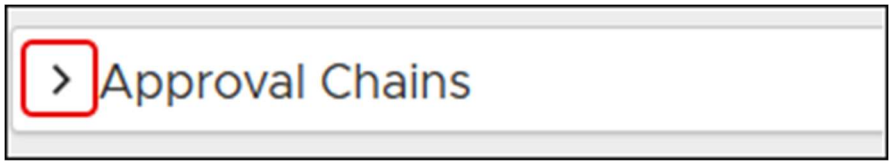
1. Scroll down to the bottom of the **Deployment Settings** workspace of an open Patching Strategy.



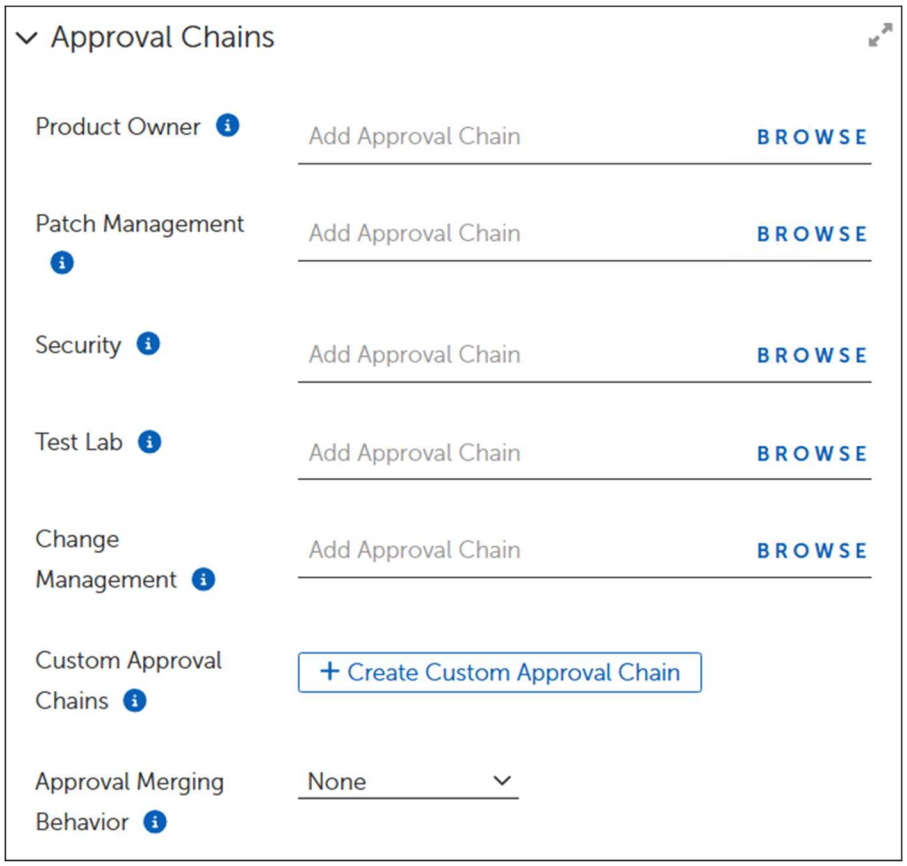
2. Select the **Present each Patch only...** toggle to enable or disable (default) whether the Patching Strategy stops presenting patches to later Bots after discovery of a matching Bot.

Add Approval Chains to a Patching Strategy

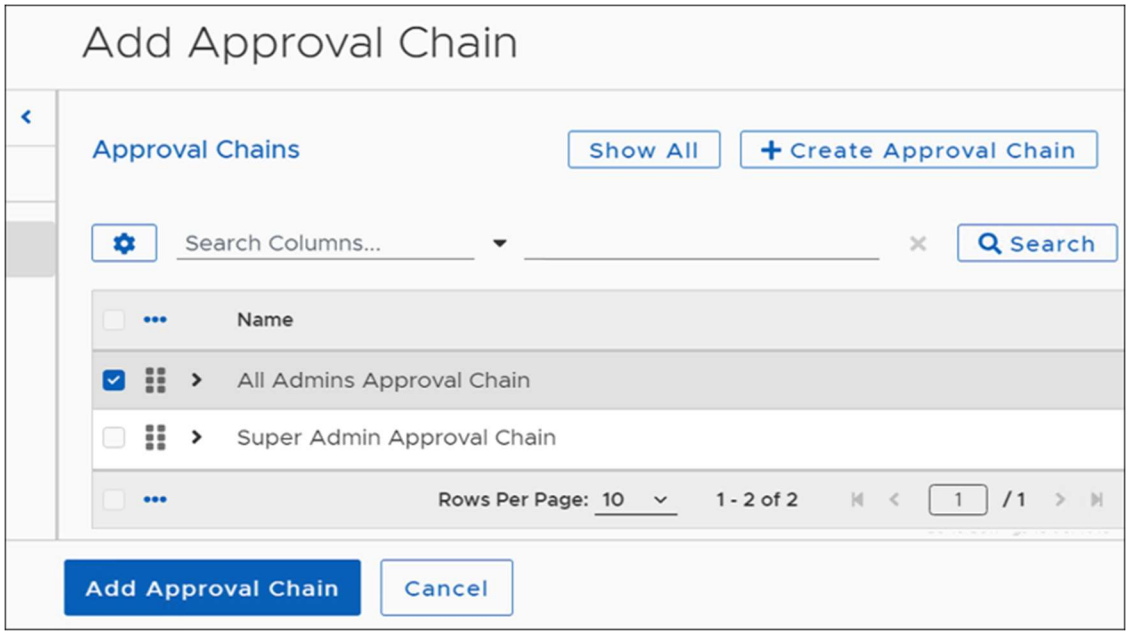
1. Select **Approval Chains** to open the **Approval Chains** workspace in an open Patching Strategy template.



2. Select **Browse** next to the type of Approval chain you want to add (Product Owner, Patch Management, Security, and so on).



3. Select an **Approval Chain** from the **Approval Chains** table. This example uses an **All Admins Approval Chain**.



4. Select **Add Approval Chain** to return to the Patching Strategy template.
5. Repeat Steps 2 through 5 for each of the groups listed in the **Approval Chains** workspace:
    a. Skip any groups that do not apply to your situation.
    b. When each group from which you need an approval contains an approval chain, continue with the next step.
6. 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.

Managing Notification Settings

Patching Strategy, Deployment Channel, and Business Unit objects include a **Notifications** dialog where you can configure notification details. The configuration choices differ slightly for each object.

Important

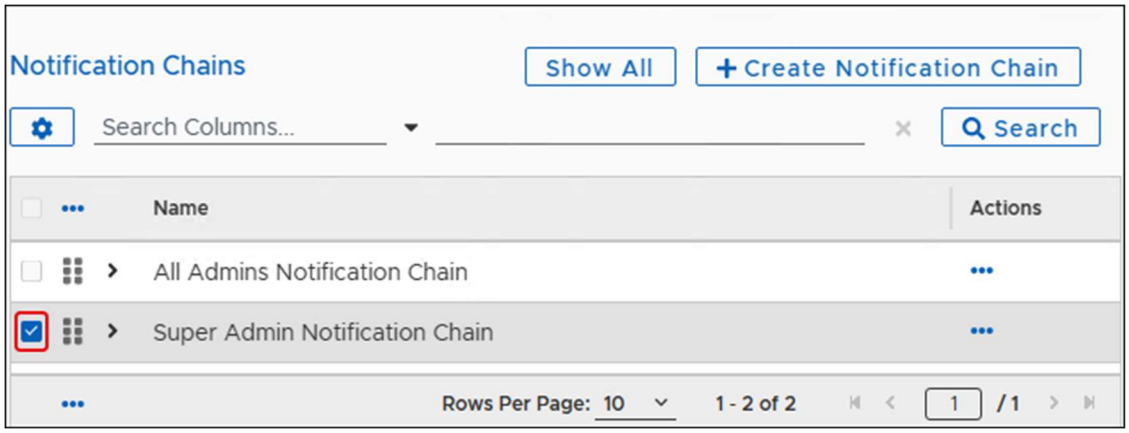
This configuration requires selecting a specific type of Notification Cycle template. Contact Tenable Customer Support for assistance with this configuration and for information about choosing the correct template.

Add a Notification Chain

Notification Chain settings exist in the object templates for Patching Strategies, Deployment Channels, and Business Units.

1. Expand the **Notifications** box in an open object template to show the available configuration options.

2. Select **Browse** next to **Notification Chain**. This opens the Notifications Chain dialog.



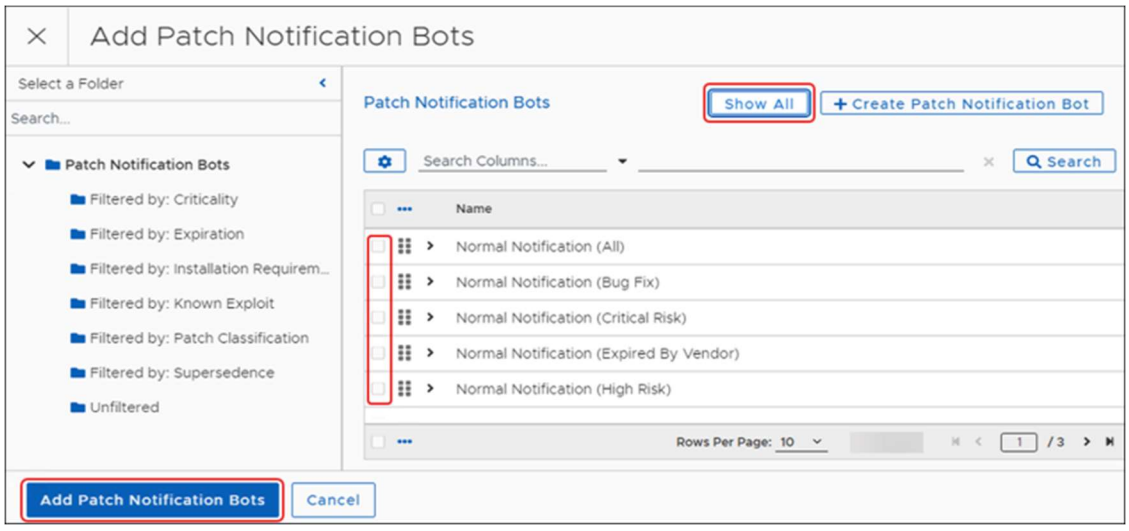
3. Select **Show All** to see the available templates.
4. Select a **Notification Chain** from the table. To edit or create Notification Chains, see Using Notification Chains.
5. Continue editing the **Notification** settings or click Create Notification Settings to return to the template.

Add Patch Notification Bots

Both Patching Strategies and Deployment Channel templates have an option to **Add Patch Notification Bots**.

1. Select **+ Add Patch Notification Bots** from the **Notifications** box in the object template.

This opens the **Add Patch Notification Bots** dialog.



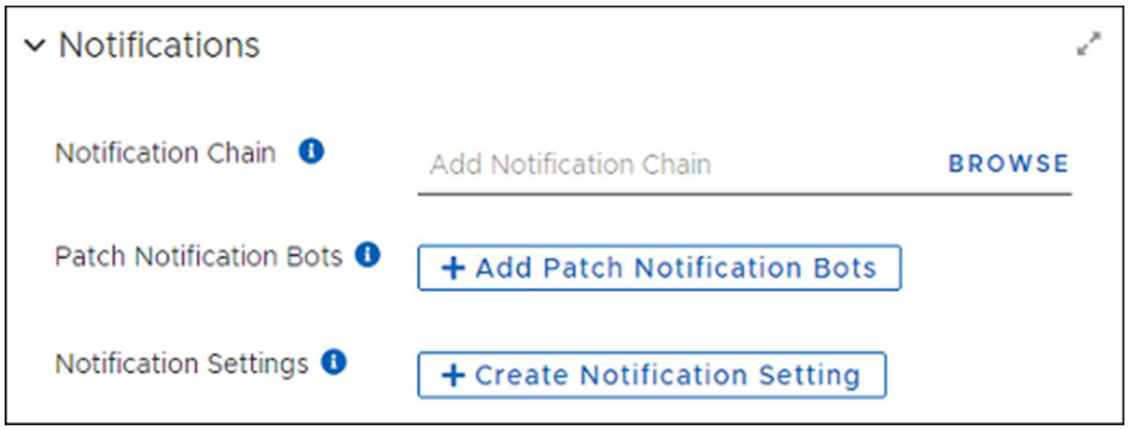
2. Select **Show All** to list all available **Patch Notification Bots** or click any **Filtered by:** folder to see the Bots associated with that filter.
3. Choose one or more **Notification Bots** to set requirements for this template. To create more Notification Bots, see Creating Notification Bots.
4. Select **Add Patch Notification Bots** on the bottom left of the dialog to return to the starting template settings for Notifications.

Create Notification Settings

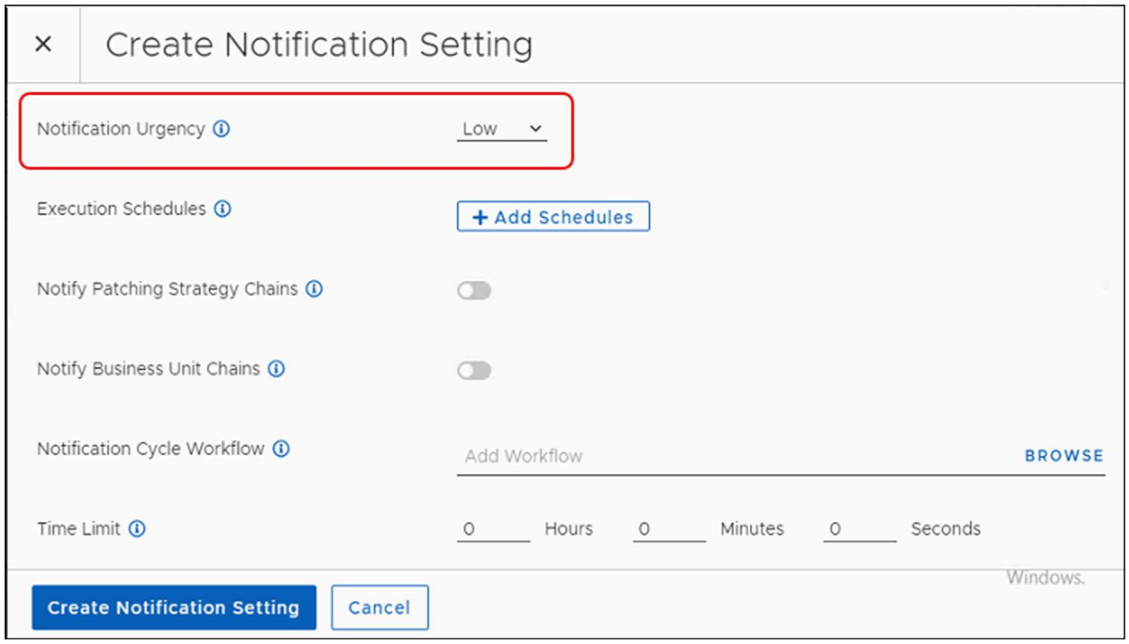
Set Notification Urgency

These values must match the corresponding values defined in the Notification Bots. Otherwise, the Notification Cycle does not send a notification.

1. Select **+ Create Notification Setting** in the Notifications box of the object template.



2. Expand the list of options next to **Notification Urgency**, and then select the urgency setting that matches the Notification Bot.



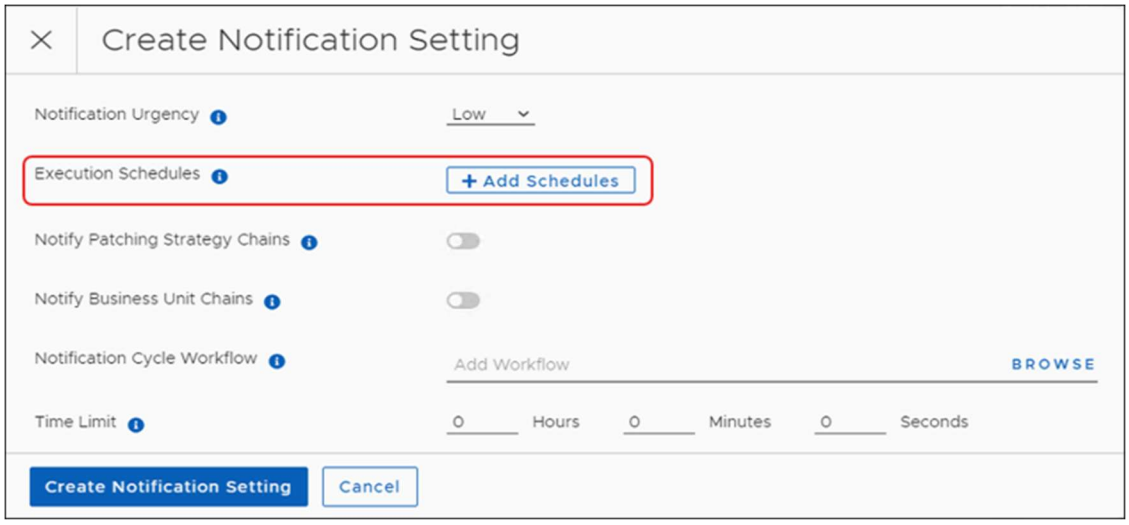
3. Continue editing the **Notification** settings or click Create Notification Settings to return to the template.

Add Execution Schedules

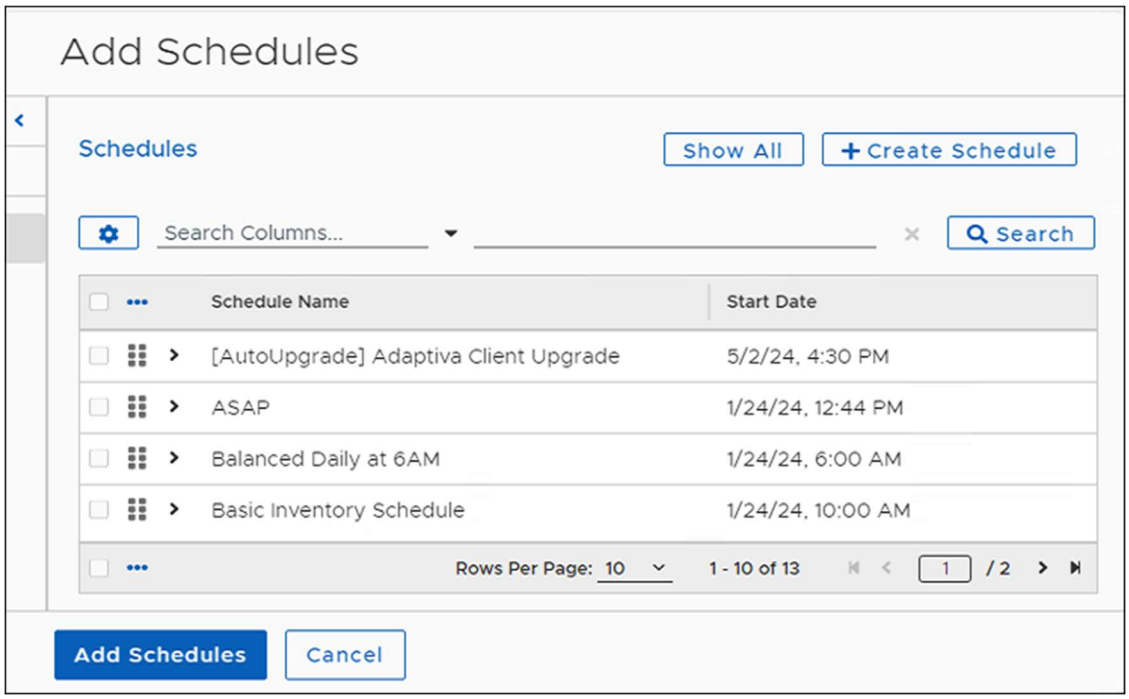
Execution Schedules control when and how often a Notification Cycle sends notifications. Choose schedules based on when and how often receiving parties require notification.

1. Select **+ Create Notification Setting** from the **Notifications** workspace of a object template.

2. Select **+Add Schedules** to display the **Create Notification Setting** dialog.



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



4. Continue editing the notification settings or click Create Notification Settings to return to the template.

Enable Notifications for Patching Strategy and Business Unit Chains

When enabled, sends notifications to the Roles shown in the Notification Chain associated with the Patching Strategy or Deployment Channel template. Defaults to disabled.

1. In the **+ Create Notification Setting** dialog in the Patching Strategy or Deployment Channel template, decide whether to enable notifications:

a. Select the **Notify Patching Strategy Chains** toggle to enable or disable (default) whether the notification cycle sends notifications to the chains included in the strategy.

b. Select the **Notify Business Unit Chains** toggle to enable or disable (default) whether the notification cycle sends notifications to Business Unit chains included in the strategy.

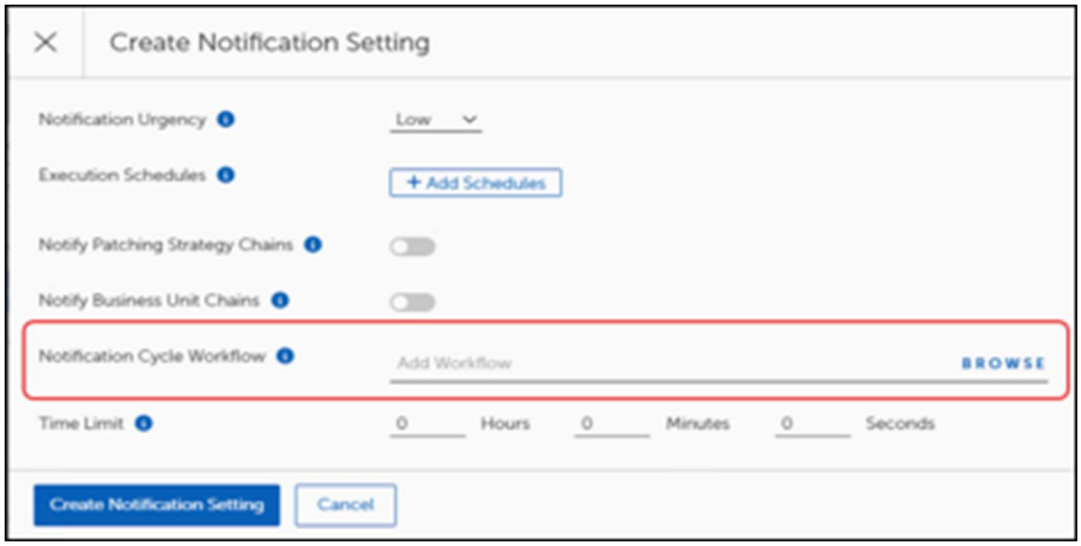
2. Continue editing the **Notifications** settings or click Create Notification Settings to return to the template.

Choose a Notification Cycle Workflow

This setting names the Notification Cycle that processes the Notifications for the Patching Strategy or Deployment Channel. Notification Cycle workflows are customized for specific uses. Tenable does not provide sample Notification Cycle templates. These templates exist only if you create them for your environment.

1. Select **+ Create Notification Setting** from the Notifications box in the object template.

This opens the **Create Notification Setting** dialog.



2. Select **Browse** on the **Add Workflow** line. This opens the list of available workflows.

3. Select your custom workflow from the list, and then click **Add Workflow** on the lower-left corner of the dialog.

4. Continue editing the **Notification** settings or click Create Notification Settings to return to the template.

Set the Time Limit

Specifies the maximum length of time that the Notification Cycle Workflow runs before timing out. If set to all zeros (default) the workflow may run indefinitely. Choose this setting with care. If the notification times out before sending all notifications, the next cycle triggers the notifications again.

1. Select **+ Create Notification Setting** the Notification box of the object template.
2. Next to **Time Limit**, set the **Hours**, **Minutes**, or **Seconds** that the Notification Cycle will run, or leave the setting default at 0 for each item to allow the workflow to run indefinitely.
3. Continue editing the **Notification** settings or click Create Notification Settings to return to the template.

Customer Extension Data

Customer Extension Data is an advanced feature of Tenable Patch Management. The Customer Extension Data fields allow advanced users to specify different key/value pairs for use in customized Patching Strategies, Deployment Chains, or Business Units when necessary to achieve different results.

Customer Extension Data fields relate directly to fields in a customized template. If you do not have customized templates with key/value pairs you can modify, you do not need to configure or use this feature.

Content Prestaging Settings

The Content Prestaging feature enables Tenable Patch Management to provide deployment content to devices ahead of the scheduled deployment, either pushing content to a location or allowing a client to pull content. Prestaging content makes the content available on the device locally when the deployment time arrives. This reduces the deployment time and minimizes the chances of missing service windows or having devices going offline before a content download finishes.

You can create Content Prestaging Settings within the Patching Strategy, Business Unit, or Deployment Channel templates.

Defining Content Prestaging Settings

The templates for Patching Strategies, Deployment Channels, and Business Units include the choice to set Content Prestaging settings. Settings default to **Not Enabled**.

Content Prestaging settings include two options:

- **Server Content Push (Recommended)** – The Tenable Server pushes the content to the best-suited sources in all locations that require the content. Tenable recommends this type of prestaging when the Deployment Strategy targets only a subset of devices. High-availability machines receive the content and function as local sources during discovery and deployment.
- **Client Content Pull** – This option enables any client that requires the content to download and cache it before deployment. Suitable when a Deployment Strategy targets all clients that need the updated content.

Push Content

- **Not Enabled** -- Disables any prestaging as part of the Patching Process workflow or Patching Strategy.
- **Handled by System** – The Tenable Patch Management system handles the prestaging automatically and pushes content to three automatically chosen devices within the office that require the content.

  This push occurs at once when the metadata updates include the latest content that meets patching requirements.
- **Handled by Workflow** – When enabled as part of a Patching Process, Deployment Channel, or Business Unit template, pushes the content upon deployment of the Patching Process.

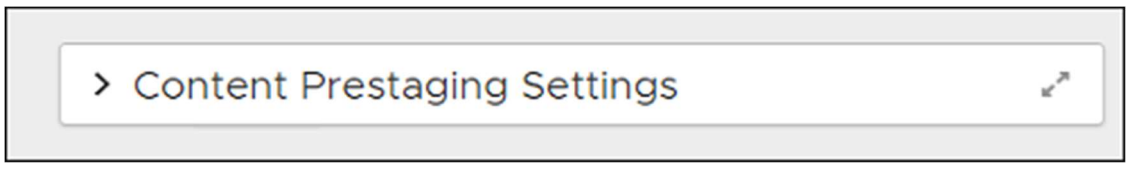
Pull Content

- **Not Enabled** -- Disables any prestaging as part of the Patching Process workflow or Patching Strategy.
- **Handled by System** – The Tenable Patch Management system handles the prestaging automatically. The Client pulls content from the Server and instructs all Clients that require the content to download and cache it ahead of any deployment.
- **Handled by Workflow** – When enabled as part of a Patching Process, Deployment Channel, or Business Unit template, the Client pulls the content upon deployment.

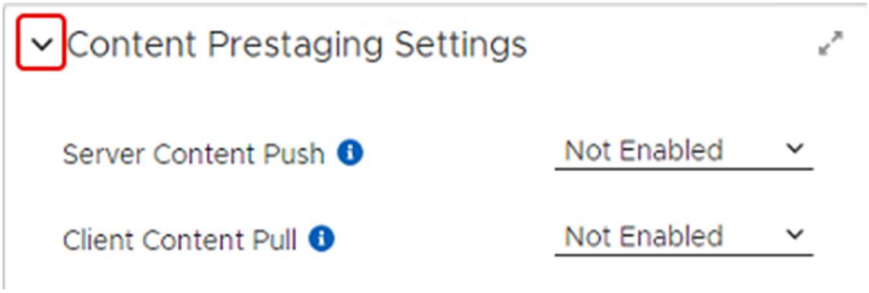
Set Content Prestaging Settings

Use this procedure to add or change Content Prestaging Settings in Patching Strategy, Business Unit, or Deployment Channel templates.

1. Expand the **Notifications** box in an open object template, and then scroll down to the Content Prestaging Settings.



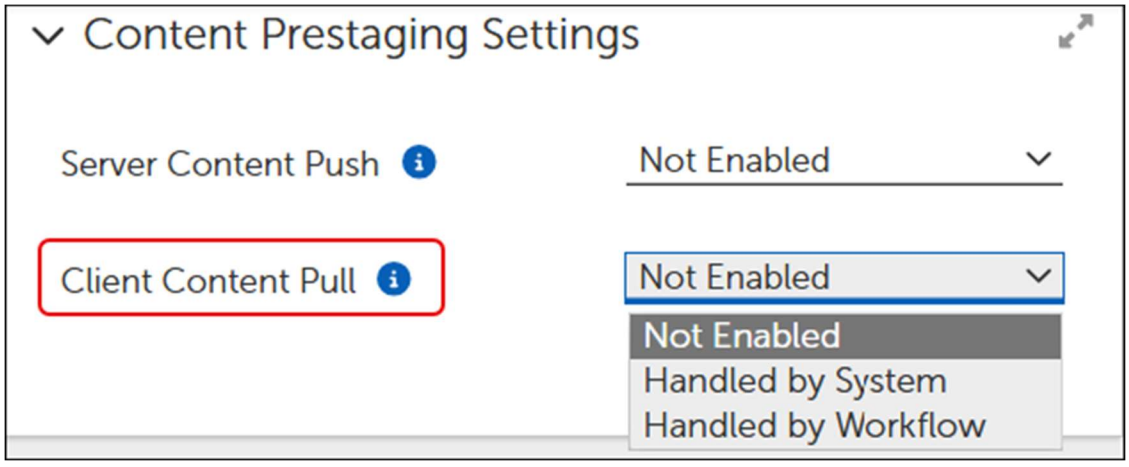
2. Expand the Content Prestaging Settings box to view the available settings.



Enable Client Content Pull

Client Content Pull defaults to Not Enabled. To enable pull settings, complete the following steps in the Content Prestaging Settings of a Patching Strategy, Business Unit, or Deployment Channel template:

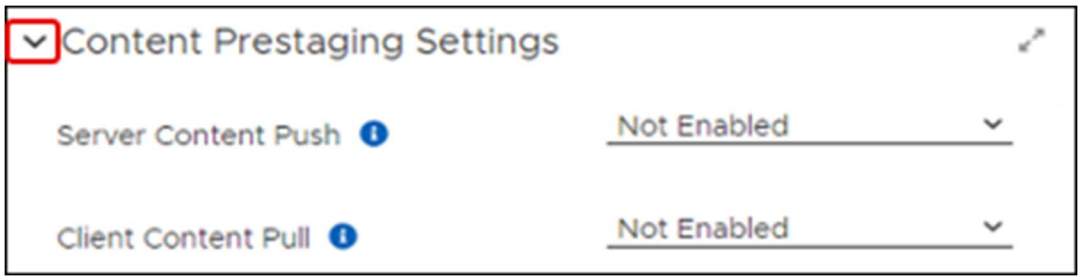
1. Select the arrow to the right of **Client Content Pull** to expand the menu of available options.



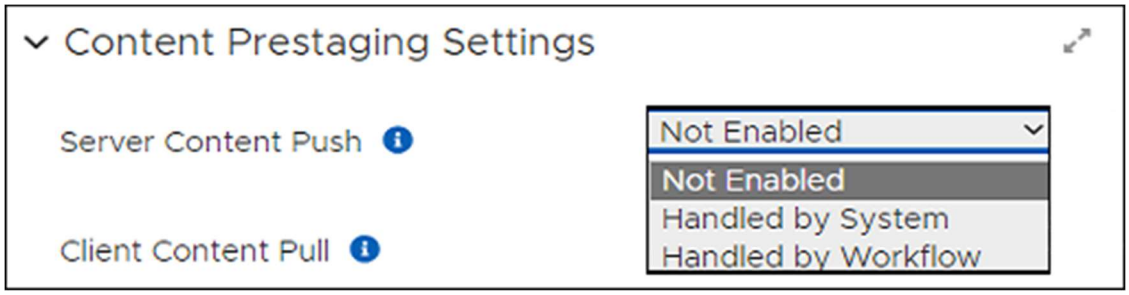
2. Select the option you need for the object template you are using. For definitions of push options, see Defining Content Prestaging Settings.
3. Select **Save** on the upper left to save your changes:
    a. Check the **Error View** and resolve any errors.
    b. Select **Save** again if you make any changes.

Enable Server Content Push

Server Content Push defaults to Not Enabled. To enable push settings, complete the following steps in the Content Prestaging Settings of a Patching Strategy, Business Unit, or Deployment Channel template, complete the following steps:



1. Select the arrow to the right of **Server Content Push** to expand the menu of available options.



2. Select the option you need for the object template you are using. For definitions of push options, see Defining Content Prestaging Settings.
3. Select **Save** on the upper left to save your changes:
    a. Check the **Error View** and resolve any errors.
    b. Select **Save** again if you make any changes.

Business Unit Addition Settings

Business Unit Addition Settings do not have a separate menu item. Configure these settings from the Business Unit Addition Settings dialog in a Patching Strategies template.

Business Unit Addition Settings in Patching Strategies

When you have added a new Business Unit to an enabled Patching Strategy, which has already completed a current patching cycle, you must use the **Business Unit Addition Settings** to add the Business Unit. This ensures that the new Business Unit receives the current updates the next time the strategy runs. Adding new Business Units using these dialoges ensures that the Business Units inherit the Patches and Patch Approval Settings set up in the original template.

Adding Business Units and associated Patching Processes separately means the new Business Units inherit Patches and Patch Approval Settings from the overall schema, but the associated Patching Process manages the customized deployment process for the new Business Units.

The Business Unit you specify here includes the patch approvals the Patching Strategy will use for any Business Units you add to the Strategy after the Strategy has run.

The Patching Process you select here is the same process you identified in the Deployment Bot Runtime configuration of the Patching Strategy.

Configure Business Unit Addition Settings

1. Select **Strategy > Patching Strategies** from the left navigation menu of the Tenable Patch Management Dashboard.
2. Scroll down to **Business Unit Addition Settings** and then click the **right arrow** to expand the box.

Select a Business Unit

Specify the parent Business Unit of this strategy so that when new Business Units become part of the strategy after its initial creation, those Business Units inherit settings from the same parent.

1. Select **Browse** next to **Template Business Unit** in the **Business Unit Addition Settings** dialog of an open Patching Strategy template.
2. Select **Save** on the upper left to save your changes:
    a. Check the **Error View** and resolve any errors.
    b. Select **Save** again if you make any changes.

Select a Patching Process

Identify the Patching Process that controls the approval and deployment logic for the existing Business Units in this strategy. This is the same Patching Process identified in the Deployment Bot Runtime, which is the only Patching Process you can choose here. This ensures that any Business

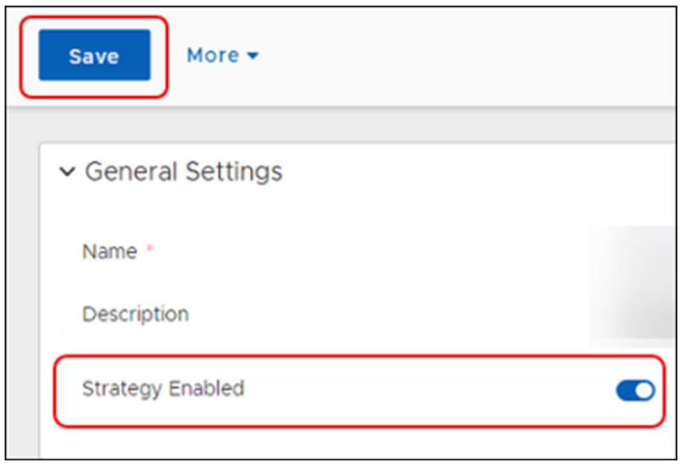
Units added after initial creation of this strategy use the same Patching Process as the existing Business Units.

1. Verify that the **Deployment Bot Runtime** details are accurate. The Patching Process settings needed for identified there Business Unit Addition settings are the same as those used in the Deployment Bot Runtime.
2. Select **Browse** next to **Patching Process** in the Business Unit Additions dialog of an open Patching Strategy. If Browse is disabled, check the Deployment Bot Runtime Settings.
3. Select the available Patching Process, and then click **Add Patching Process**.
4. Select **Save** on the upper left to save your changes:
    a. Check the **Error View** and resolve any errors.
    b. Select **Save** again if you make any changes.

Enable the Patching Strategy

After completing the Patching Strategy configuration, including Add Software Products, you must enable the Patching Strategy. When enabled, the strategy runs according to the configured schedules.

1. In **General Settings** at the top of the Patching Strategy template**,** click the **Strategy Enabled** toggle to enable the strategy and make it available for use.

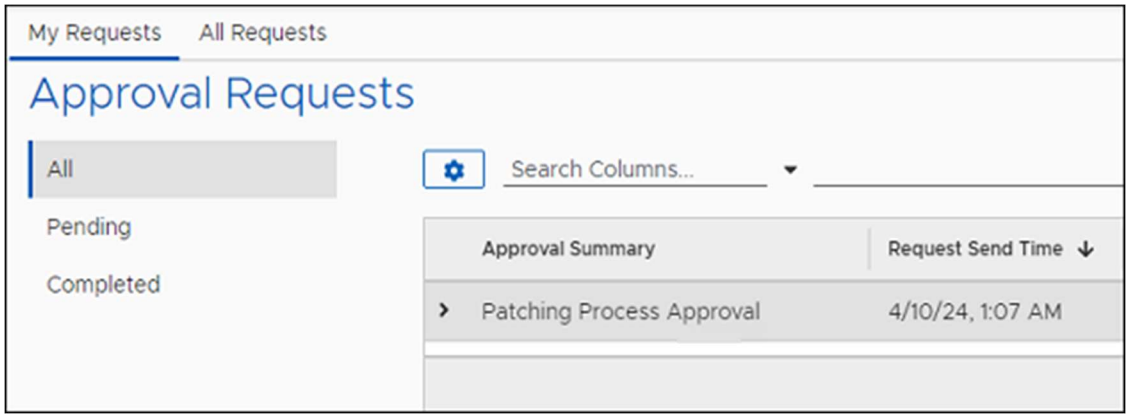


2. Select **Save** on the upper-left corner of the workflow to save the strategy:
    a. Check the **Error View** and resolve any errors.
    b. Select **Save** again if you make any changes.
3. *Move the saved template to your folder*.

View the Staged Patching Strategy

After you Enable the Patching Strategy, you can view the pending approval request.

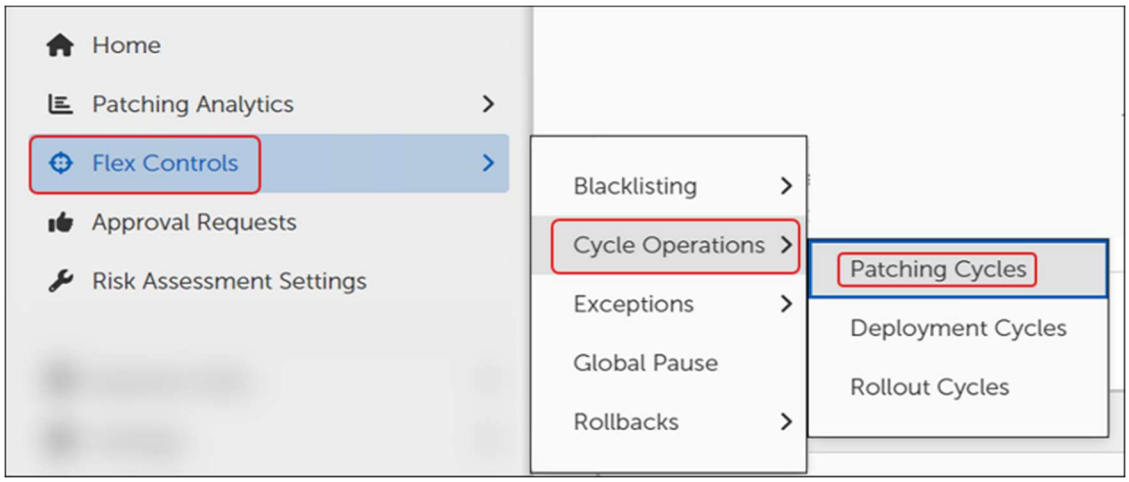
1. Select the **Approval Requests** in the left navigation menu of the dashboard.



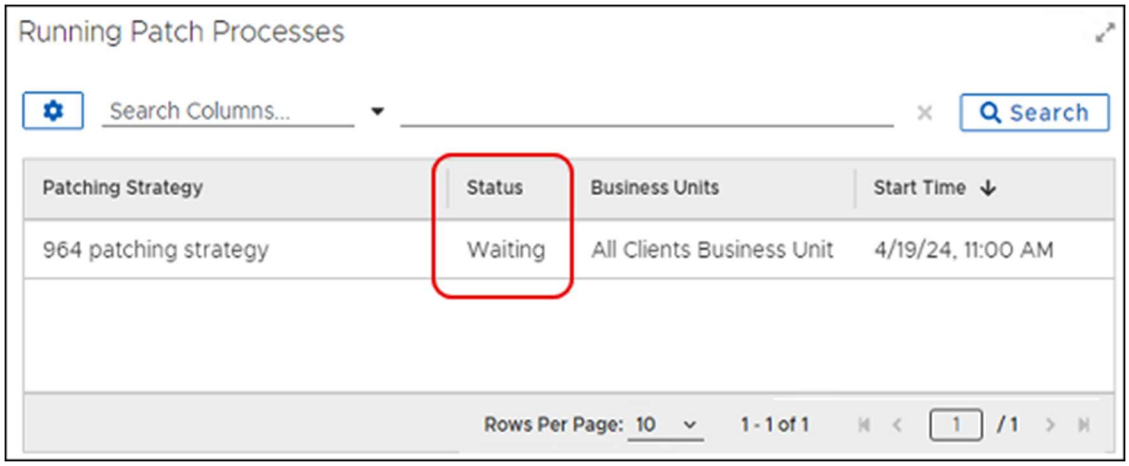
   a. The view defaults to **All** requests, which includes pending and completed.

   b. The Patching Strategy you just enabled appears in the **Approval Summary** table with a **Request Status** of **In Progress and Awaiting Response**.

2. Select **Flex Controls > Cycle Operations > Patching Cycles** from the left navigation menu.



3. Check the **Running Patch Processes** table, which lists the status of the **Patching Strategy** as **Waiting**.



4. Select **Approval Requests** in the left navigation menu, and then click the **Patching Strategy** in the table.

5. Select **Approve**, and then click **Back to Approval Requests**. You can wait until the patch time passes, or you can start the deployment manually.

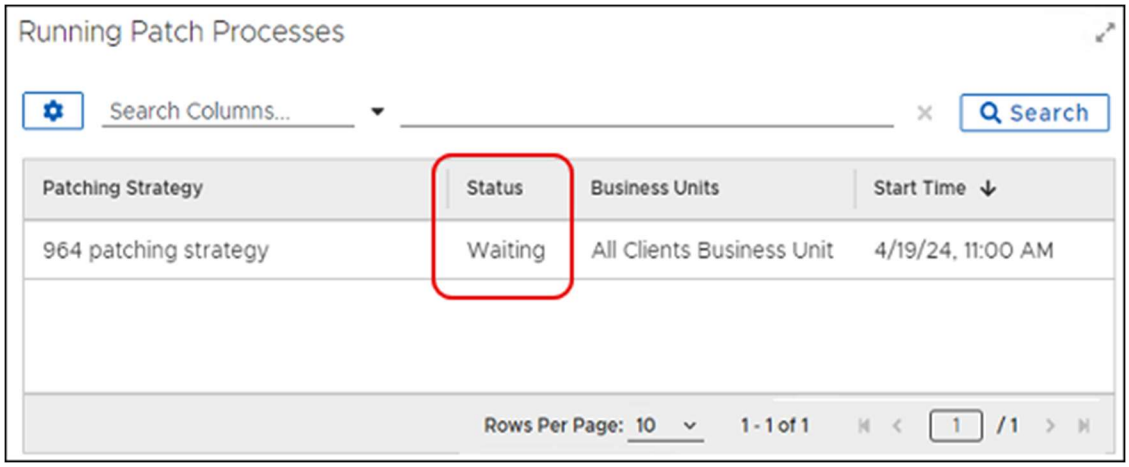
Important

When you add a new device (Tenable Server) to your network after this strategy has scanned and updated all associated devices, Tenable Patch Management automatically adds any new devices to the strategy if the next scan detects an earlier version of Chrome.

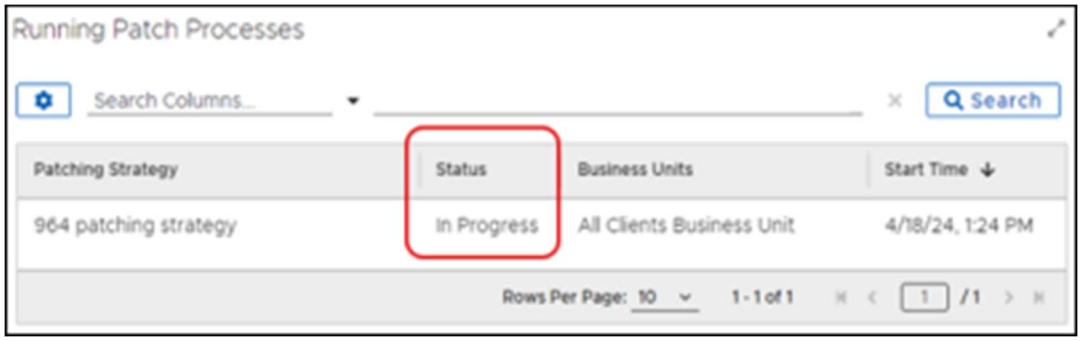
Start the Patching Strategy Manually

After the Patching Strategy approval process status shows **Completed**, you can wait until the time setting for patch deployment, or you can start the deployment immediately.

1. Select **Flex Controls > Patching Cycles**, and then click the name of the Patching Strategy to open the **Cycle Information**.



2. Select Play under **Cycle Information**, and then click **Close**. This returns you to the **Patching Cycles** workspace where you can view **Running Patch Processes**.



3. Select the **Patching Strategy** name to view details about the patching process.

Patching Processes

Patching Processes serve as the primary method for deploying patches to Business Units or adding Patches to a Deployment Channel. As with Patching Strategies, Tenable Patch Management includes prepopulated Patching Process templates that address most processing scenarios.

Patching processes define the Patching Strategy logic based on Patching Strategy settings, such as the following:

- Approval processes for patches.
- User notifications.
- Prestaging content.
- Deploying to test labs before production.
- Routing patches to appropriate deployment channels, or directly routing them to business units for deployment.

Creating Patching Processes

If you want to create your own Patching Processes, enter a support ticket and request help from Tewnable Customer Support.

Patching Process Templates

Immediate Deployment, No Phasing, Initial Patch Manager Approval

Each of these processes requires an approval step before deploying updates.

Immediate Deployment- Initial Patch Manager Approval

Approval required prior to deployment, then deploys at once.

Immediate Deployment, No Approvals Needed

Except for the Default Patching Process, each of these strategies requires no approval before deploying updates.

- **Default Patching Process**
- **Phased Deployment No Approval**

  No approval needed prior to deployment. Deploys in phases
- **Immediate Deployment No Approval**

No approval needed prior to deployment. Deploys at once.

- **Immediate Phased Deployment No Approval**

  No approval needed prior to deployment. Deploys in phases.

Phased Deployment Processes, Approval Required

- **Immediate Phased Deployment - Initial Patch Manager Approval**

  Approval required prior to deployment. Deploys in phases.

- **Phased Deployment - Initial Patch Manager Approval**

  Approval needed prior to deployment. Deploys in phases.

- **Phased Deployment - Phase Patch Manager Approval**

  Approval needed prior to deployment. Deploys in phases.

Bots – Patch Deployment and Notification Bots

A Deployment Bot generates patch approvals and assigns specific configurations to those approvals, such as the Patching Process and the Deployment Channel.

Notification Bots exist only as optional components of Patching Strategies and Deployment Channels and deploy or generate notifications based on settings in the Notification Bot template. Notifications can alert administrators about the release or deployment of new patches or inform interested parties about newly published updates. Notification Bots do not execute independently.

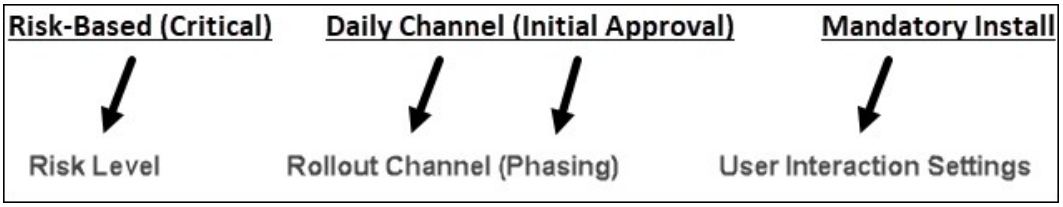
Deployment Bots

Patch Deployment Bot Template Naming Conventions

Tenable Patch Management Deployment Bot templates include various filtering scenarios to cover most filtering requirements in an enterprise. When deciding which Bot filter to choose, consider the following examples to understand naming conventions for the different filter types.

Risk-Based Filters

These templates filter several aspects of patches based on risk. They include different rollout schedules and approval levels, and all require mandatory installation.



Mandatory Installation for Specific Categories

These templates filter specific categories of patches, including bug fixes, expired by vendor, known exploit, and so on. These bots filter based on category and then approve installation for all patches included in that category.

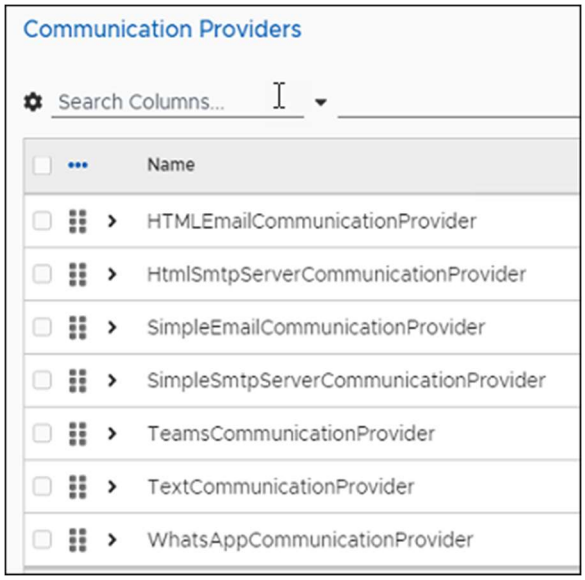
Descriptions of Bot Settings

The Bot templates provided by Tenable include the following settings:

- **Bot Settings**: Used by both Deployment Bots and Notification Bots. Choices are Deployment/Notification Settings or Bot Workflow. Both templates default to Deployment/Notification Settings. To create a Bot Workflow, request help from Tenable Customer Support.
- **Desired State**: Used by Deployment Bots only. When patches match the patch filter settings, this field specifies what action the Deployment Bot takes:

Desired State	Description
Mandatory Install	Force installation onto the end-user device.
Do Not Install	Do not install onto the end-user device.
Rollback	Roll back the patch to the last approved version.
Uninstall	Perform an uninstallation of the patch.

- **Urgency**: Used by both Deployment Bots and Notification Bots to specify the urgency setting (Low, Normal, High, Critical) for patches or notifications that meet the patch filter requirements. The Bot compares this setting against the urgency defined in the Patching Strategy or Deployment Channel to which this bot belongs. If the urgency settings do not match, the Bot does not deploy or send notification.
- **Business Units**: Deployment Bots Only. Business Units are a fundamental organizational unit in Tenable Patch Management and logically group and manage devices, settings, and other resources according to business needs. Groupings include geographic location, department, or business function. For details, see Business Units.
- **Output Expression**: Notification Bots only. The Output Expression is a free text field used to enter the text of the notification (E-Mail body, SMS/Text Message, Microsoft Teams message, or WhatsApp message).
- **Communication Providers**: Notification Bots only. Communication Provider settings define the type of communication to send when a Bot processes a patch that matches the Filter Settings. Choose one or more of the built-in Communication Providers.



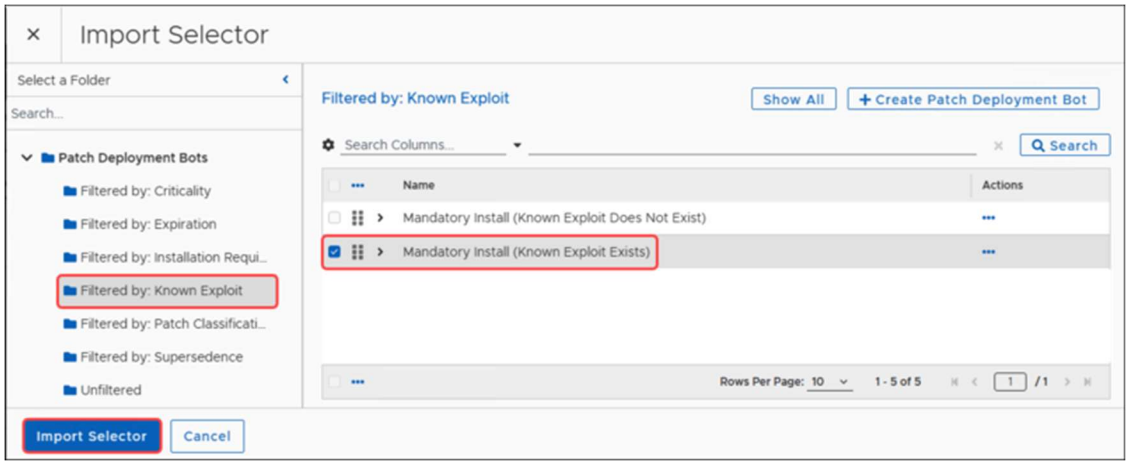
Open and Save a Patch Deployment Bot Template

Tenable Patch Management includes prepopulated templates that address most filtering scenarios. You can save these templates using a descriptive local naming convention, and then customize them to your environment.

Tip

To create customized Deployment Bots, Tenable recommends entering a support ticket and requesting help from Tenable Customer Support.

1. Follow the instructions in Create a New Folder for Objects.
2. Hover over or click **Bots** in the left navigation menu of the Tenable Patch Management Admin Portal, and then select **Patch Deployment Bots**. The top folder lists the templates provided by Tenable.
3. Select **Show All** to see the available templates or click **Filtered by:** in the Bots list to see only the templates associated with that filter.
4. Select the **Name** of a template to open it. For example, in **Filtered by: Known Exploit**, click **Mandatory Install (Known Exploit Exists)**.



5. 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.

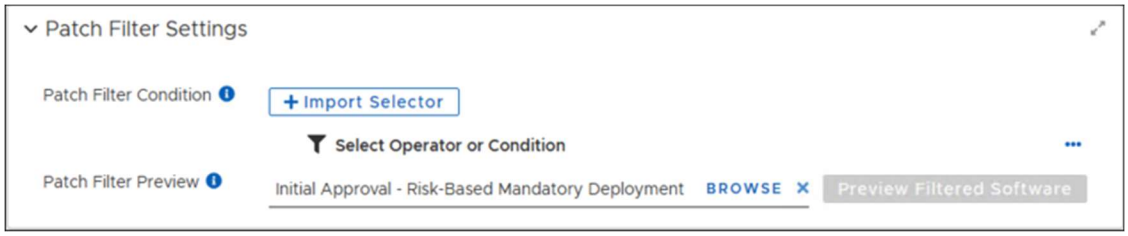
6. Continue to

Patch Filter Conditions

The Tenable Deployment Bot and Notification Bot templates include Patch Filter Settings that provide the Bot with the details needed to approve patches for installation or to ignore specific patches, updates, or vendor content.

Proceed carefully when customizing Patch Filter Settings. Enter a support ticket and request help from Tenable Customer Support.

Used by both Deployment Bots and Notification Bots. New patches must meet the filter criteria before the Bot submits them to the Patching Cycle. After approving a patch that meets the Patch Filter Settings, the Bot forwards patch information to the Patching Process and the Deployment Wave associated with the Patching Strategy.



Configurable conditions include using **+ Import Selector**, which allows you to use an existing Patch Filter to validate new patches submitted to this Bot. You can also use the **Select Operator or**

Condition to create a flexible patch filtering process. With no filter settings applied, the Bot processes all patches.

Edit or Remove Existing Patch Filter Conditions

In a Patch Deployment Bot template, scroll down to **Patch Filter Settings**:

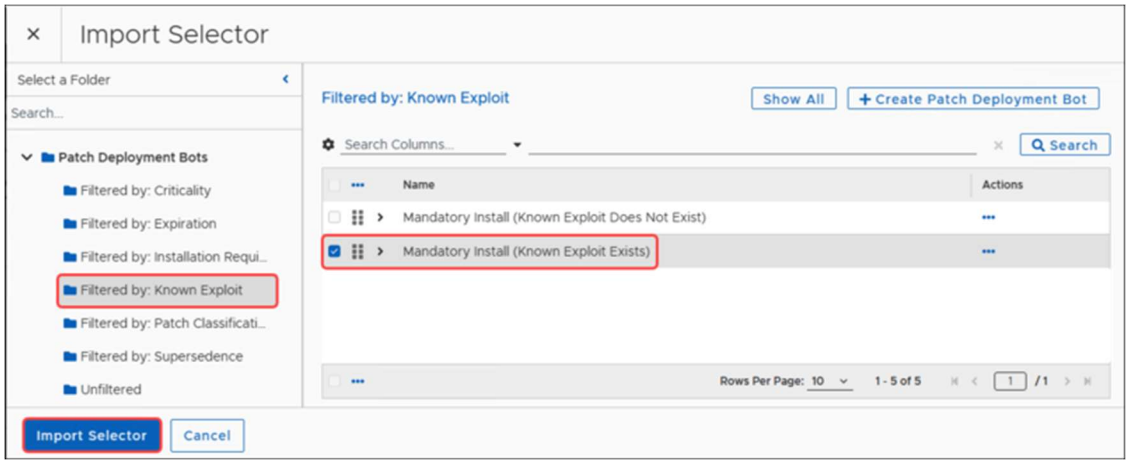
- If your template includes a patch filter condition that you want to modify, click the **ellipsis (...)**, and then select **Edit Condition**.
- If you want to remove a **Patch Filter Condition**, click the **ellipsis (...)**, and then select **Remove**.

Add Patch Filter Conditions

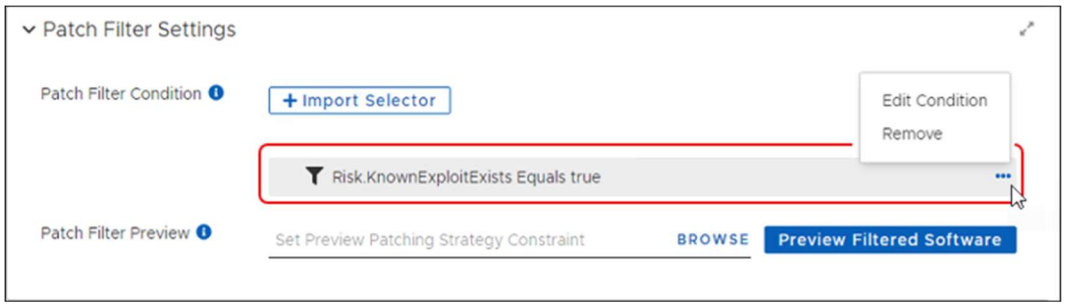
Allows you to select one or more, existing filter conditions to use for this Bot. If you want to add multiple conditions, see Set and Change Patch Filter Conditions. This example uses an existing Tenable patch filter that tells the Bot to include patches based on the imported filter settings.

1. Select **+ Import Selector** in the **Patch Filter Settings** dialog of an open Bot template.
2. Select an existing **Filtered by:** folder from the list of **Patch Deployment Bots**, and then select one or more filters to use in this Bot.

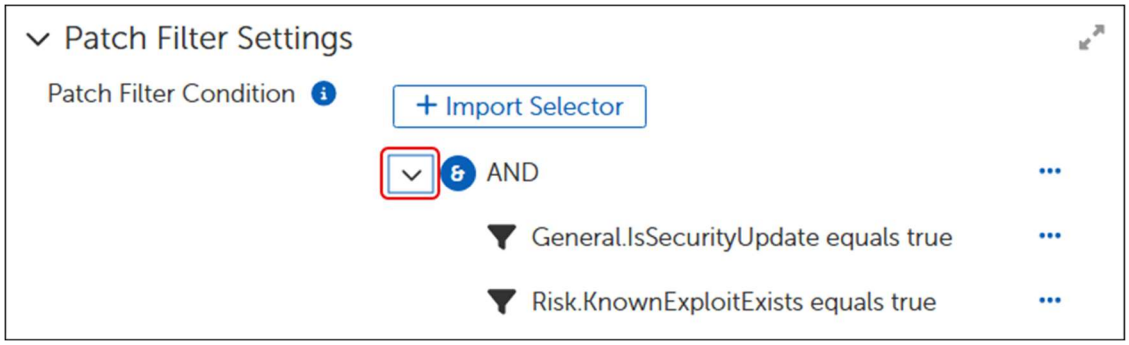
   For example, in **Filtered by: Known Exploit**, select **Mandatory Install (Known Exploit Exists)**.



3. Select **Import Selector** at the bottom left of the dialog. This returns you to the **Patch Filter Settings** where the condition logic now displays as Risk.KnownExploitExists Equals true.



If you chose more than one filter, the condition displays the **AND** operator and lists your selections:



Set and Change Patch Filter Conditions

Use Operating Conditions and Operators to manually set multiple Patch Filter Conditions to use for this Bot. You must add the operator before you can add the condition. To add multiple conditions, repeat this section as needed.

Tip

When using a template that already includes a Patch Filter Condition, you must remove that condition before you can add multiple conditions. You can add the original condition back in as part of setting multiple conditions.

Add or Remove an Operator

1. In the Patch Filter Settings of an open Bot template, delete any existing Filter Conditions.

    a. To **remove** an existing condition, click the ellipsis to the right of the existing filter, and select Remove.

    b. To **add** the condition in again as part of a string, make note of the name for later use.

2. Select the **ellipsis (...)** to the right of **Select Operator or Condition**, and then select **Add Operator**.

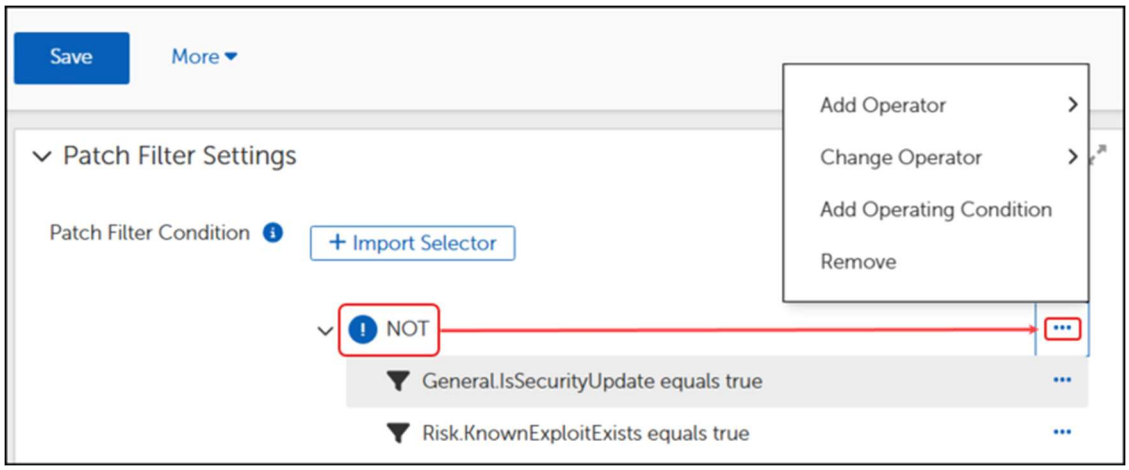
3. Select the **operator** you want to use (AND, NOT, OR). For example, to filter out specific patches, select **NOT**.

This returns you to the **Patch Filter Settings**, which shows the operator you selected.

4. Continue to Add an Operating Condition.

Change an Operator

1. Select the **ellipsis (...)** next to the existing filter in the Patch Filter Settings of an open Bot template.



2. Select **Change Operator**, and then select the operator you prefer.

3. Select **Save** on the upper left-hand corner of the **Patch Filter Settings** workspace:

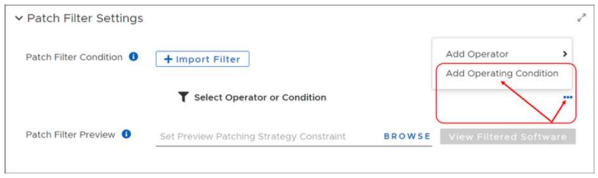
    a. Check the **Error View** and resolve any errors.

    b. Select **Save** again if you make any changes.

Add an Operating Condition

After adding the Operator, add the Operating Condition. This example filters out all patches for Windows Server Update Services (WSUS).

1. Select **ellipsis (...)** to the right of **Select Operator or Condition**, and then select **Add Operating Condition**.



2. Expand the list next to **Data Column** and select the filter you want to use. For example, select **WSUS Classification**.

    a. If you removed a Patch Filter Condition previously, you may add it back here.

3. Set the **Operating Condition** to **Equals**, and then choose one of the following for the **Value**:

    a. **Updates** – Exclude Windows updates.

    b. **Upgrades** –Exclude Windows upgrades.

    c. **Windows 11 upgrades** – Exclude upgrades to Windows 11.

4. Select **OK**. This returns you to **Patch Filter Settings**, which now shows **WSUS.Classification Equals *<selected value>*** as a condition for excluding patches.

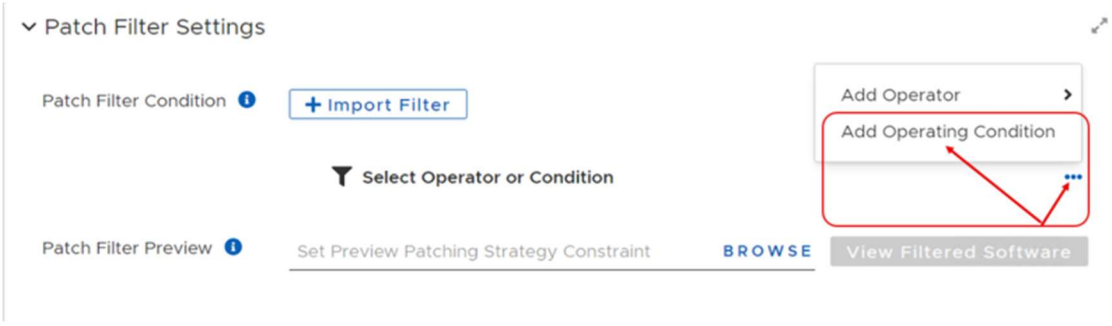
5. See Preview Software Filtered by Conditions to confirm that the **Software Patches** listed do not include those you excluded.

Filter Out Specific Patches by Product ID

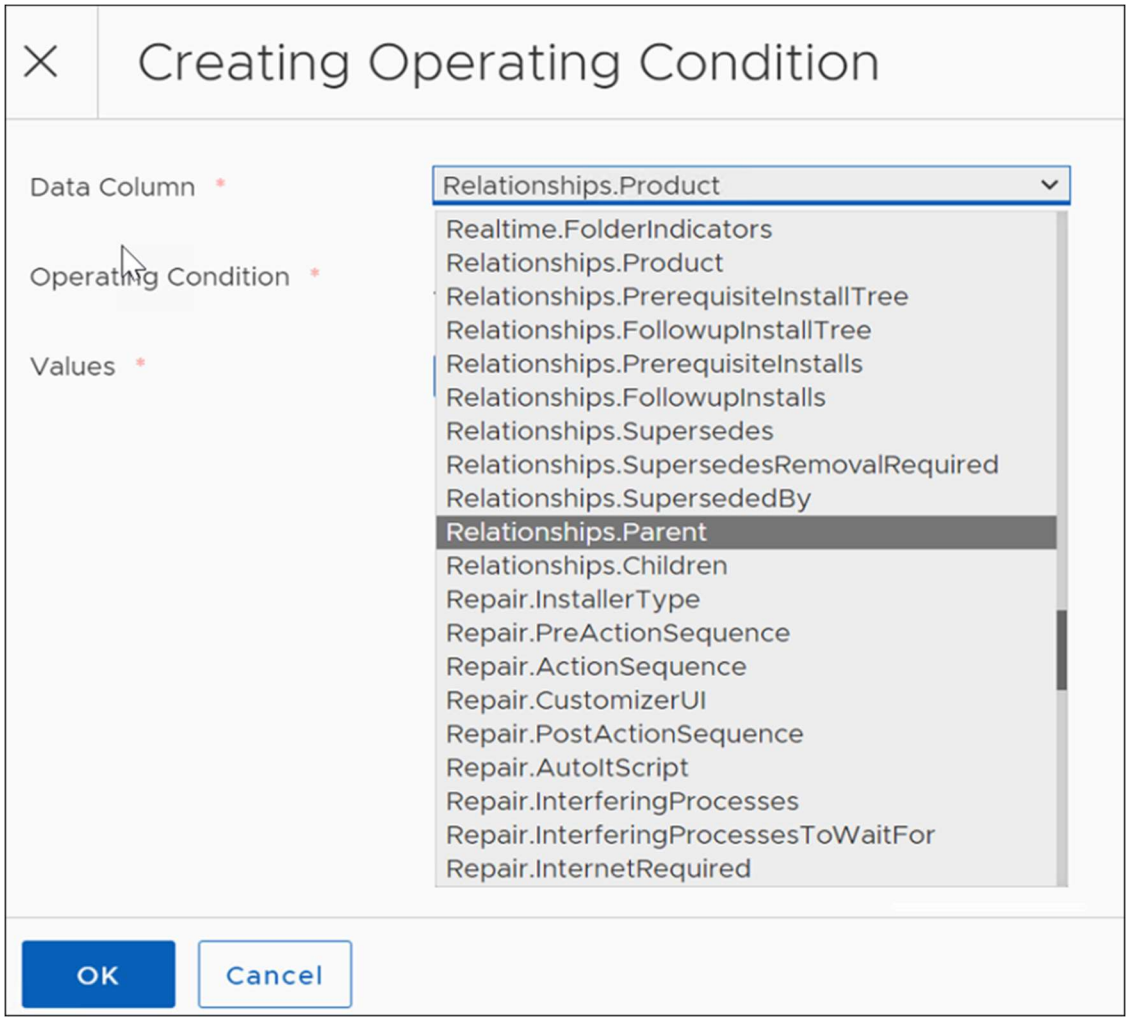
The Product ID is the number assigned by Tenable to all patches from a specific vendor.

1. Contact Tenable Customer Support to obtain the Product ID for the vendor patches you want to filter.

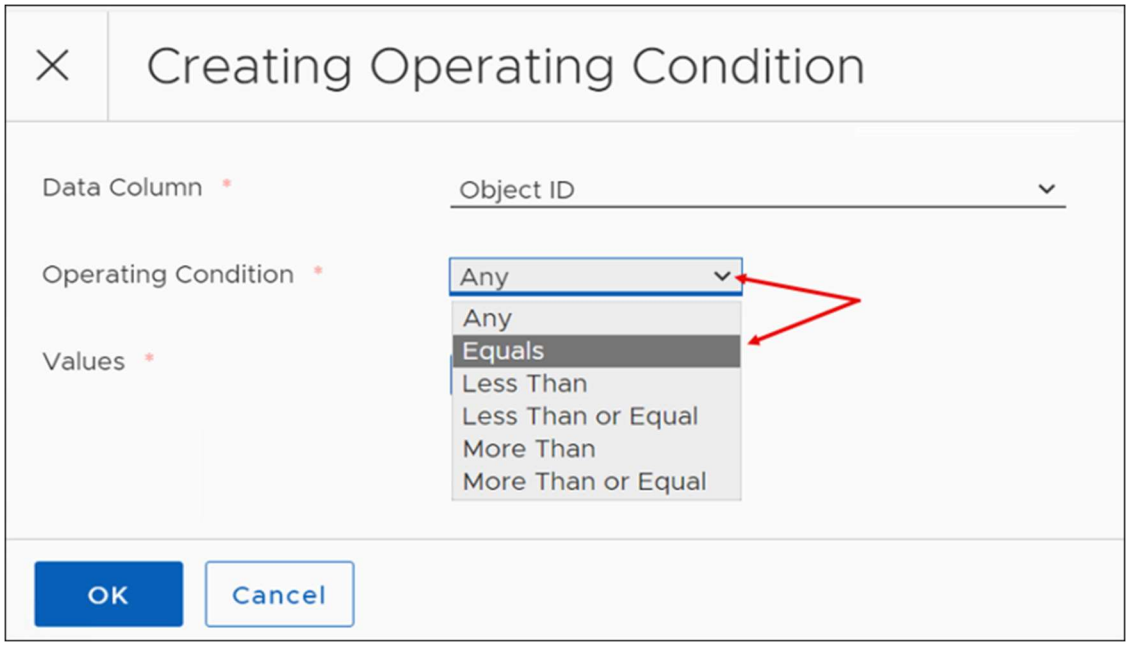
2. Select **ellipsis (...)** to the right of **Select Operator or Condition**, and then select **Add Operating Condition**.



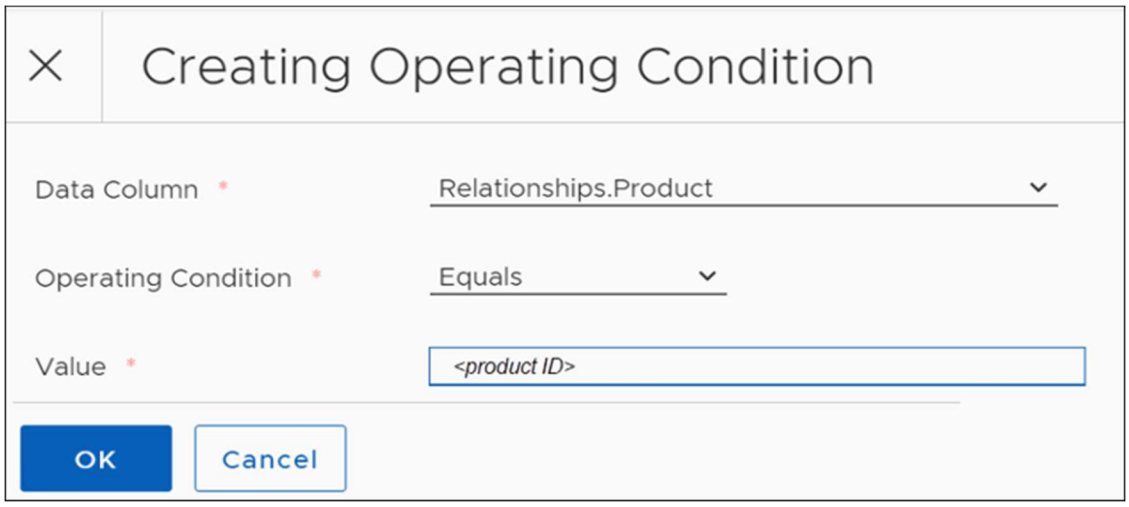
3. Expand the list next to **Data Column** and select **Relationships.Parent** as the Object ID.



4. Set the **Operating Condition** to **Equals**.



5. Enter the Product ID, and then click **OK**. This returns you to **Patch Filter Setting**s, which now shows **Parent ID Equals <product ID>** as a condition for excluding patches.



6. See Preview Software Filtered by Conditions to confirm that the **Software Patches** listed do not include those you excluded.

Preview Filtered Patches

Preview Software Filtered by Conditions

Preview a list of software filtered by this Bot based on the patch filter condition.

1. Select **Preview Filtered Software** on the lower-right corner of the **Patch Filter Settings**.

2. Select the **Software Patches** tab to see the Software Patches included in this Bot with your filter.
3. Select the **Software Releases** tab to see the Software Releases included in this Bot with your filter.
4. Select **OK** to return to the **Patch Filter Settings**.

Preview Software Filtered by a Strategy

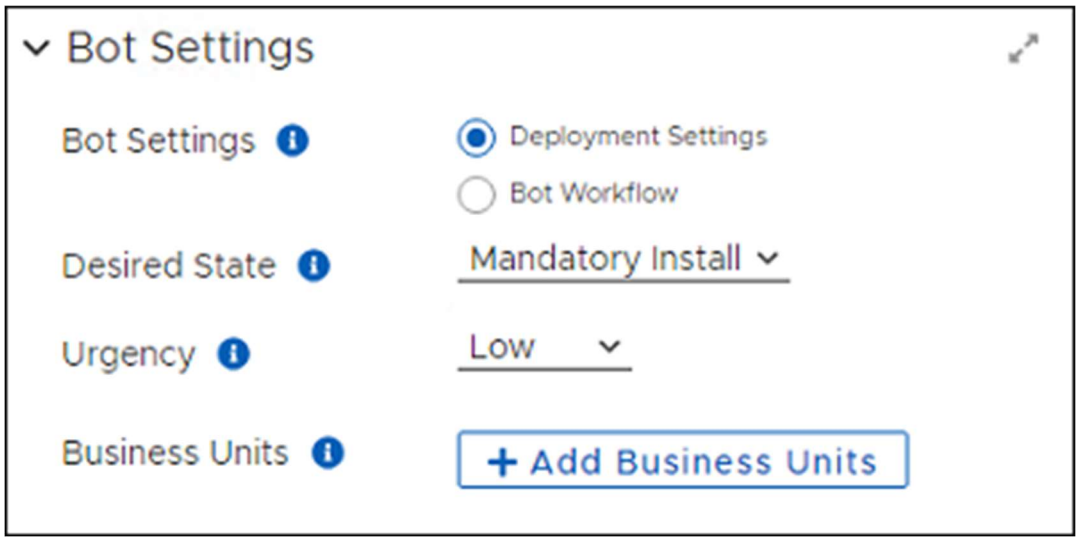
Using the Patch Filter Settings in a Deployment Bot template, you can preview the software filtered out by the Patch Filter Conditions you set. You can enhance these filter conditions by specifying a Patching Strategy to further constrain the preview results

1. Select **Browse** next to **Patch Filter Preview** in the **Patch Filter Settings** of an open Deployment Bot template.
2. Select a Patching Strategy you want to preview, and then click **Set Preview Patching Strategy Constraint**.
3. Select **Preview Filtered Software** to see the patches or releases filtered by the Patching Strategy.
4. Select **OK** to return to the **Patch Filter Settings**.

Configure Bot Settings

Select Deployment Settings

In the Bot settings workspace of a Deployment Bot template, the default **Deployment Settings** require a Desired State, an Urgency level, and designated Business Units.



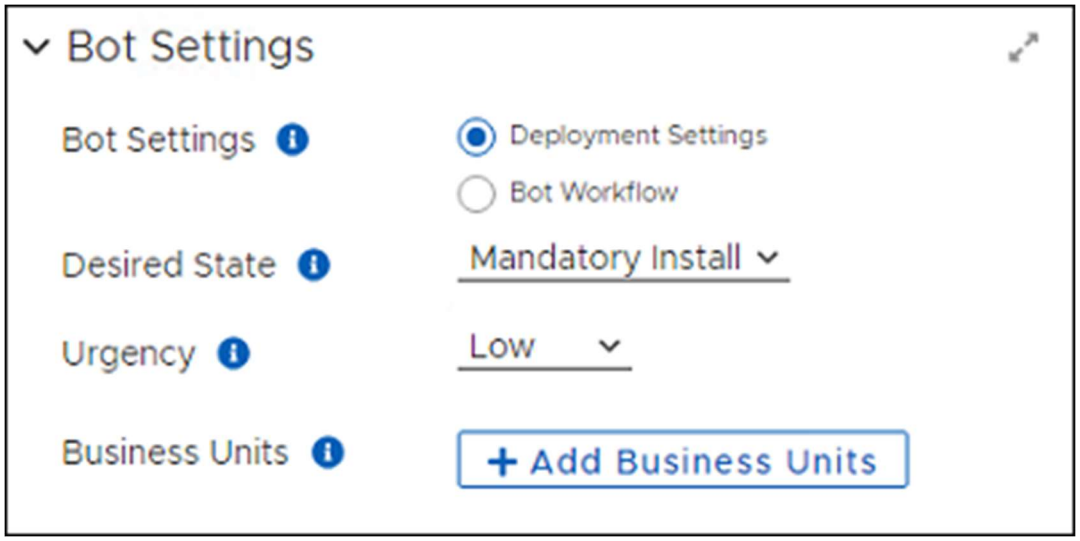
With Deployment Settings selected, complete the following steps.

1. Set the Desired State:
    a. Select the input line for **Desired State** to view the menu options.
    b. Select a **State** from the list (Mandatory Install, Do Not Install, Rollback, Uninstall).
2. Set the Urgency:
    a. Select the input line for **Urgency** to view the menu options.
    b. Select an **Urgency** setting from the list (Low, Normal, High, Critical).
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. Continue with Add Business Units.

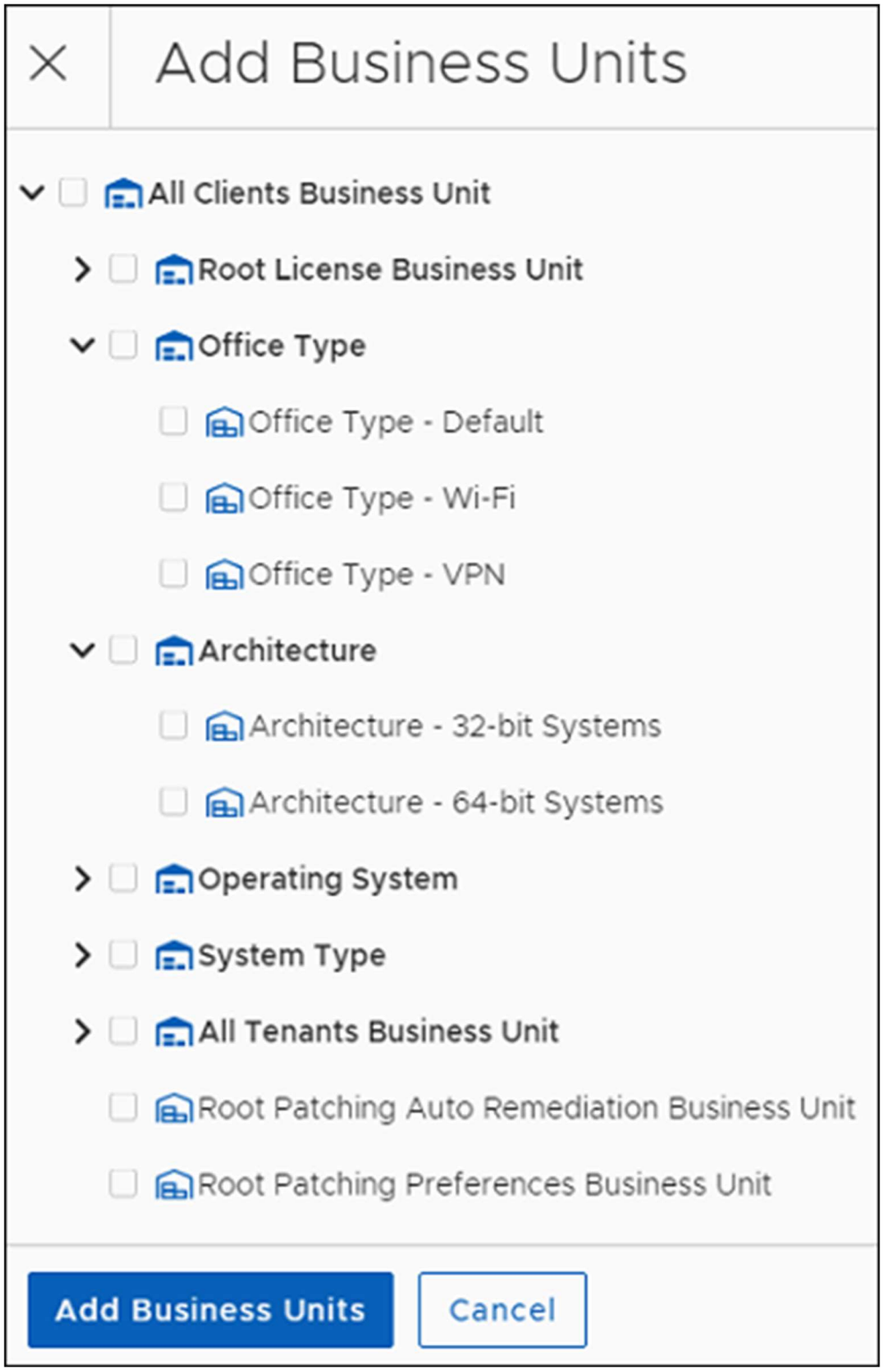
Business Units for Bot Deployment Settings

In the **Bot Settings** workspace of an open Deployment Bot template with **Deployment Settings** selected, complete the following steps:

1. Select **+ Add Business Units**:



    a. With no Business Units added to the Bot, the patching cycle patches the devices in all Business Units identified in the Patching Strategy.
    b. With one or more Business Units added to the Bot, the patching cycle patches the devices in the Business Units. The Patching Strategy must include the same Business Units as part of its assigned Deployment Wave (see Deployment Settings).
2. Select the right arrow next to a Business Unit type to expand one or more **Business Unit** structures.



3. Select one or more **Business Units** to include in this Deployment Bot.
4. Select **Add Business Units** on the bottom left to return to the Deployment Bot template.

5. Select **Save** at the upper left to save your progress:

    a. Check the **Error View** and resolve any errors.

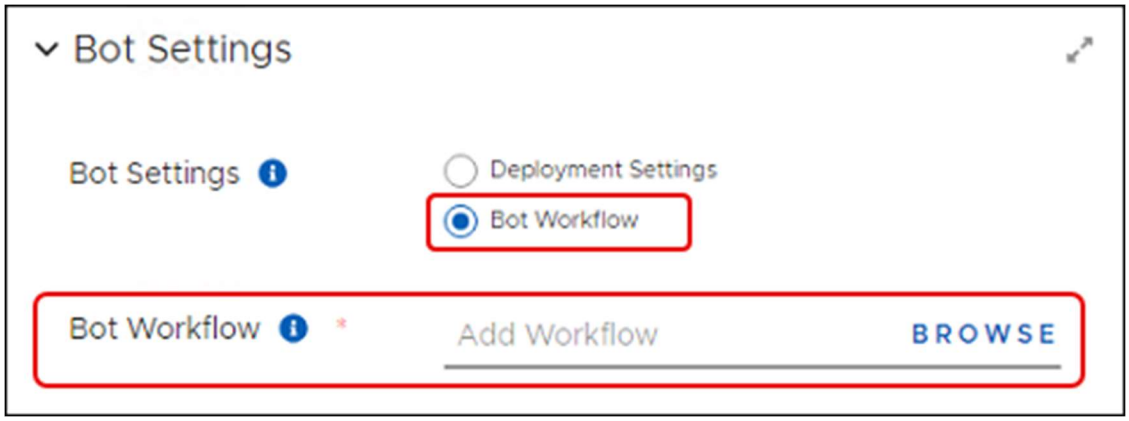
    b. Select **Save** again if you make any changes.

    Now, when you need to add this Deployment Bot to a Patching Strategy or other object, you will see it in the list of available Deployment Bots.

Use a Custom Deployment Bot Workflow

If you have not created a custom workflow, contact Tenable Customer Support and request assistance. To add a customer workflow, go to the **Bot Settings** workspace of an open Deployment Bot template with **Bot Workflow** selected and complete the following steps.

1. Select **Browse** next to **Bot Workflow** to open the list of available workflows.



2. Select **Show All** to view all available workflows for this setting.

    Important

    If you have created a custom Deployment Bot Workflow, you will see it listed here. If not, contact Tenable Customer Support to create a Deployment Bot Workflow for use with these settings.

3. Select the workflow **Name**, and then click **Add Workflow** on the bottom left to include the workflow in the Bot Settings.

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.

Notification Bots

Patch Notification Bots generate notifications to alert administrators or users about the release or deployment of new patches that meet Patch Filter Settings in the Bot. When the Notification Bot detects patches that match a specified filter expression, the Bot generates a notification to

include in the notification cycle. The notification cycle follows the Patching Strategy or Deployment Channel configuration that contains the Notification Bot.

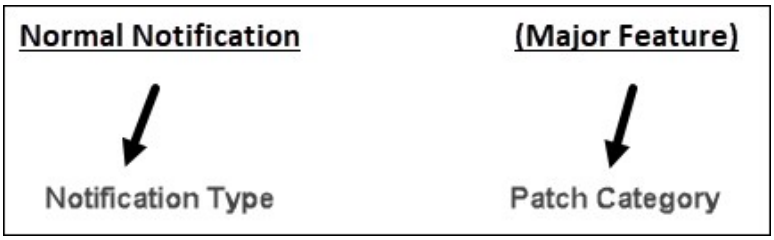
Notification Bots are optional components of Patching Strategy templates and Deployment Channel templates and exist only within these templates.

Patch Notification Bot Template Naming Conventions

Tenable Patch Management Deployment Bot templates include various filtering scenarios to cover most filtering requirements in an enterprise. When deciding which Bot filter to choose, consider the following examples to understand naming conventions for the different filter types.

Normal Notification

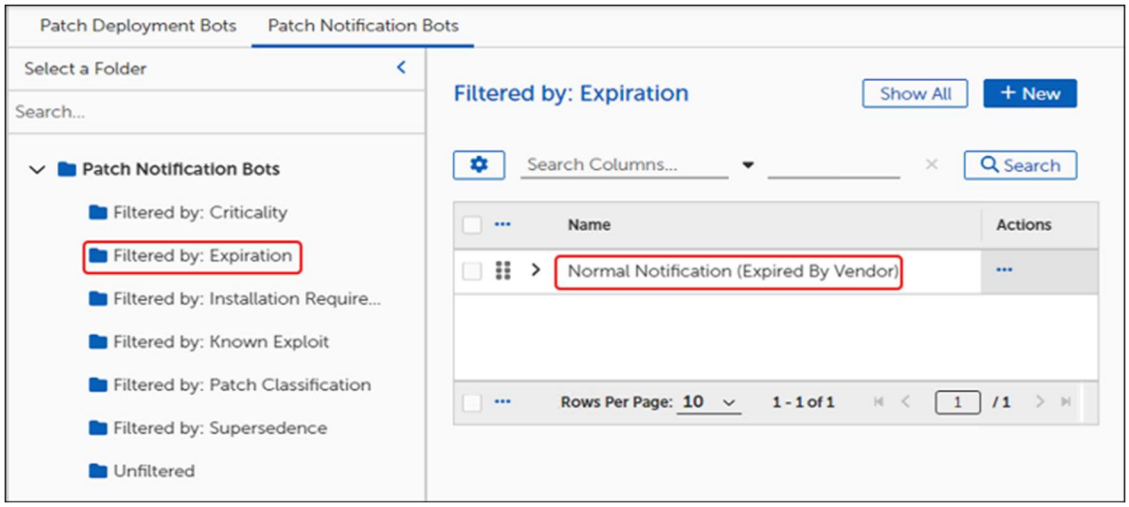
These templates filter several aspects of patches based on risk. They include different rollout schedules and approval levels, and all require mandatory installation.



Creating Notification Bots

Open and Save a Patch Notification Bot Template

1. Follow the instructions in Create a New Folder for Objects.
2. Mouse over or click **Bots** in the left navigation menu of the Tenable Patch Management Dashboard and then select **Patch Notification Bots**. The top folder lists the templates provided by Tenable.
3. Select the **Show All** to see the available templates or click **Filtered by:** in the Bots list to see only the templates associated with that filter.
4. Select the **Name** of a template to open it. For example, in **Filtered by: Expiration**, click **Normal Notification (Expired by Vendor)**.



5. 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.

6. Select **Save**. When you have finished modifying your new template, you can drag and drop it in the folder you created (see Tenable Patch Management Object Management).

Create an Output Expression

The Output Expression field is a text box that allows you to provide a more meaningful notification to users that informs them of the pending changes.

Configure Notification Bot Settings

Except for Communication Providers, use the previously configured settings in the template. For details, see Communication Providers.

1. In the Notification Bot template, scroll down to **Communication Providers**, and then click **+ Add Communication Providers**.

    a. Select one or more providers to use for notifications by this Bot.

    b. If you do not see the provider you want to use, see Communication Providers to add it.

2. Select **Save** at the upper left to save your progress:

3. Check the **Error View** and resolve any errors.

4. Select **Save** again if you make any changes.

Chains

Tenable Patch Management uses Approval Chains and Notification Chains to manage communication about, and seek approvals for, patch updates and installations.

Approval Chains: Include details such as approval layers, backup roles, reminder intervals, and more.

Notification Chains: Include details about which parties to notify for what kinds of activities and business units, as well as identifying carrier services.

After you have created Approval Chains and Notification Chains using the Chains workspace, you can assign the chains to a Patching Strategy, a Business Unit, or a Deployment Channel.

Approval Chains

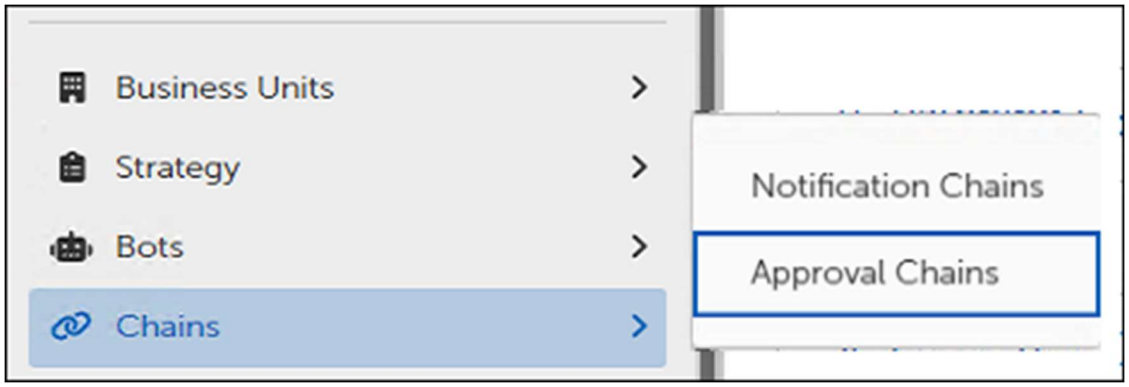
Using Approval Chains

Approval Chains allow the administrator to specify users who will receive patch approval requests for Patching Strategies or Business Units.

Tenable Patch Management includes suggested Approval Chain personas, such as Product Owner, Patch Management, Security, Test Lab, and Change Management. You can customize and layer these roles to model the natural approval structure in your environment, including backup approvers and timeout settings to allow for automatic escalation. You can also omit layers based on patch criticality/urgency.

Open and Save an Approval Chain Template

1. Mouse over or click **Chains** in the left navigation menu of the Tenable Patch Management Enterprise Dashboard, and then select **Approval Chains**.



2. Select the **Name** of a template to open it, and then save the template with new information:

    a. Select **More** in the upper-left corner of the template, and then select **Save *<object>* As**.

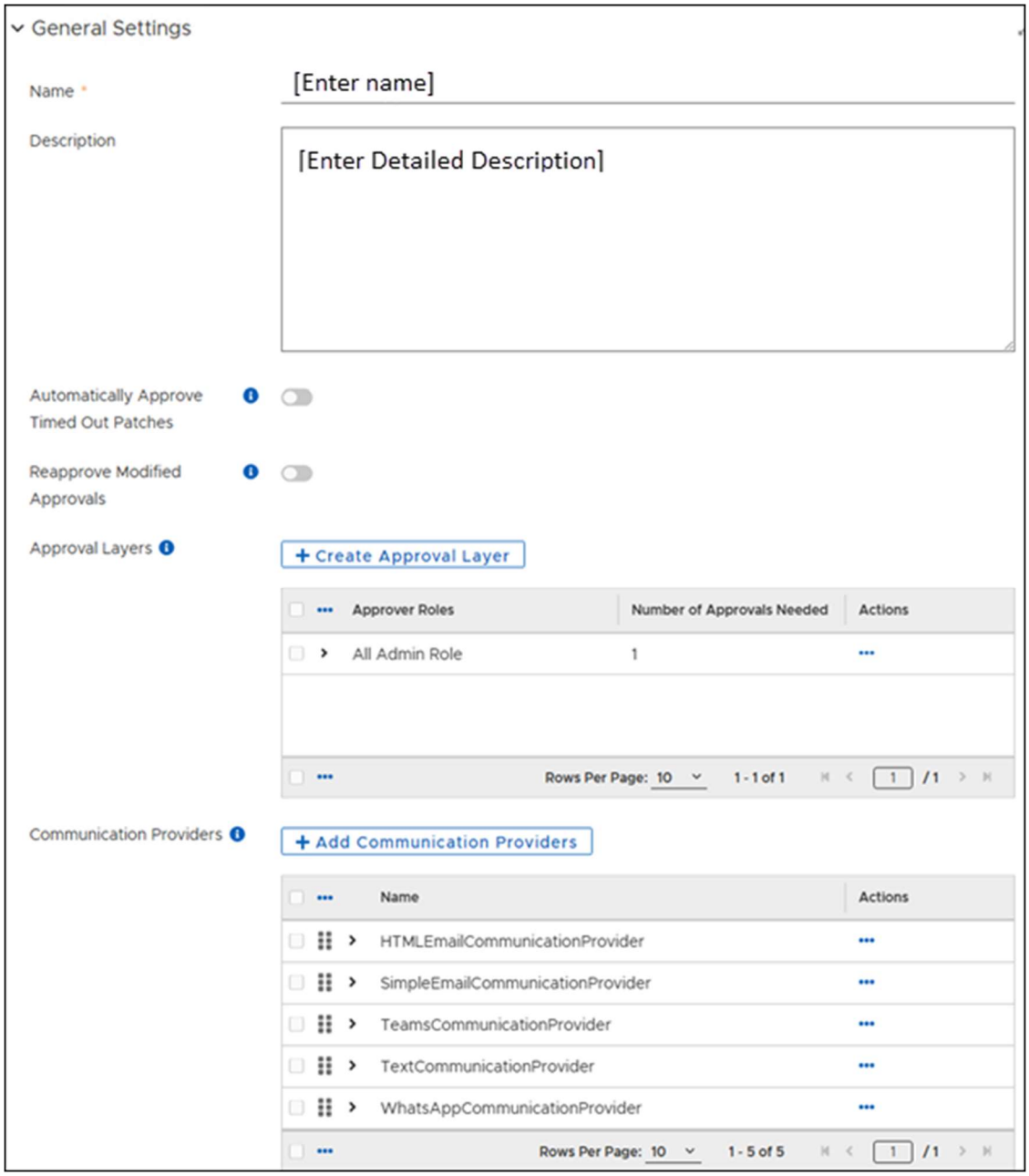
    b. Enter a new Name for the template, and then click **OK** on the lower-left corner of the naming dialog. This returns you to the template with the new name.

    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.

Managing Approval Chain Settings

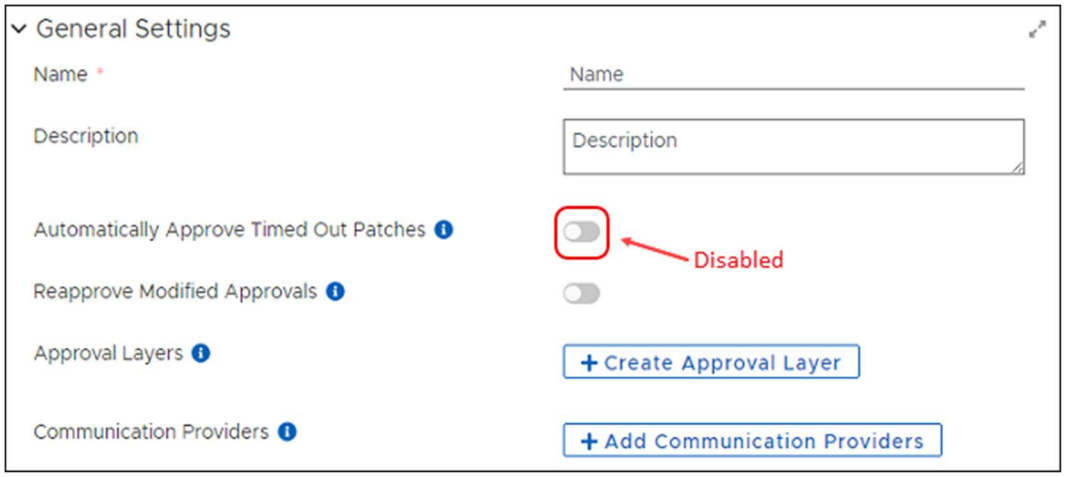
Approval Chain management choices include approval of timed out patches, reapproval of modified approvals, setting approval layers, and choosing communication providers.

Each of these tasks assumes you have opened and saved an Approval Chain template and you are ready to complete the General Settings configuration.



Enable or Disable Automatic Approval of Timed Out Patches

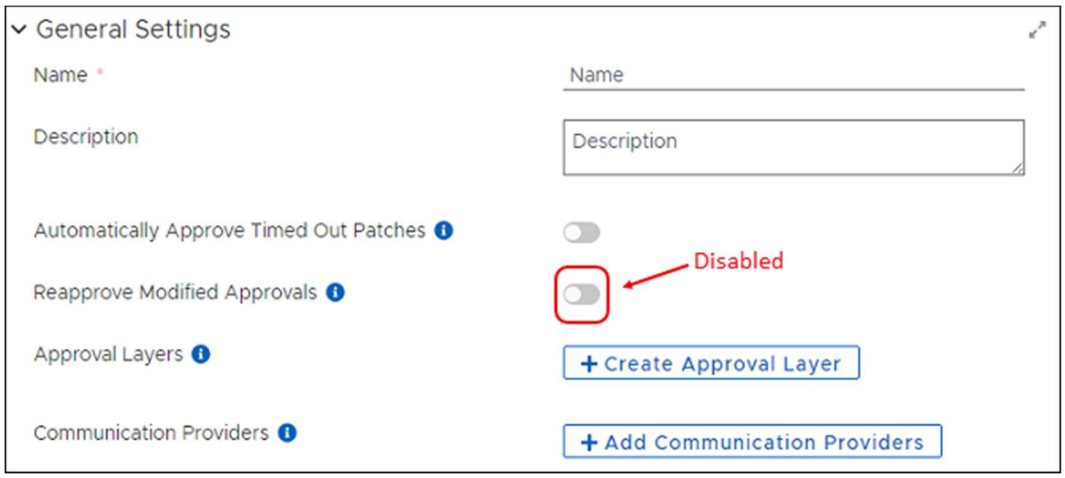
When enabled, this setting automatically approves patches when reviewers do not respond within the timeout duration specified in the Approval Layer.



Select the **Automatically Approve Timed Out Patches** toggle to enable or disable (default) this feature.

Enable or Disable Reapproval for Modifications after Approval

When enabled, this setting resends an approval request to earlier approvers if a later approver makes modifications.



Select the **Reapprove Modified Approvals** toggle to enable or disable (default) this feature.

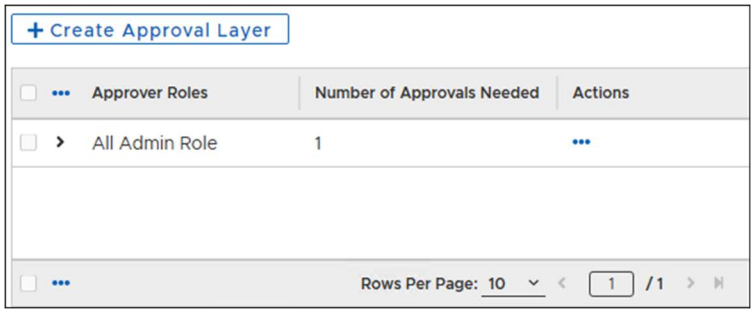
Create an Approval Layer

Any object that uses this Approval Chain will process approvals top to bottom in the order listed in the approval layers.

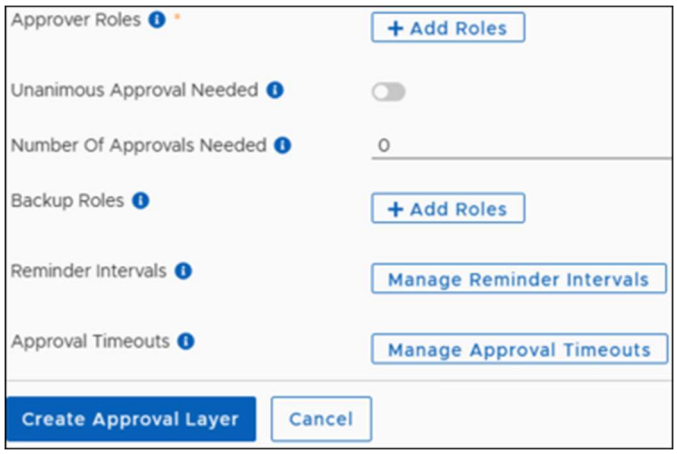
1. Scroll down to **Approval Layers** in an Approval Chain template.

    a. For a new approval Layer, click **+ Create Approval Layer**.

    b. To change an existing Approval Layer, click the **ellipsis (...)** in the Actions column for the role you want to change, and then select **Edit Approval Layer**.



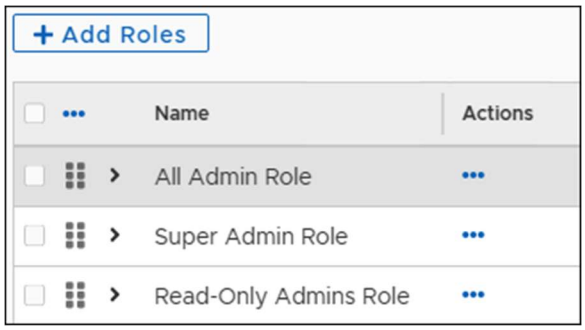
2. This opens the **Create Approval Layer** dialog.



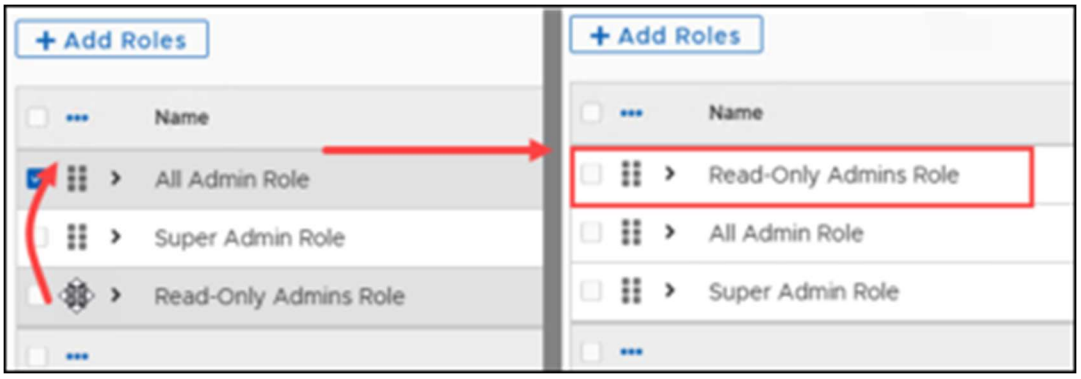
Add and Order Approval Roles

The processing order sends approvals from the top to bottom based on the order of the listed roles.

1. Select **+ Add Roles** on the **Approval Layer** page.
2. Select one or more existing **Names** from the **Roles** table, and then click **Add Roles** at the bottom left of the page. This returns you to the **Approval Layer** dialog.



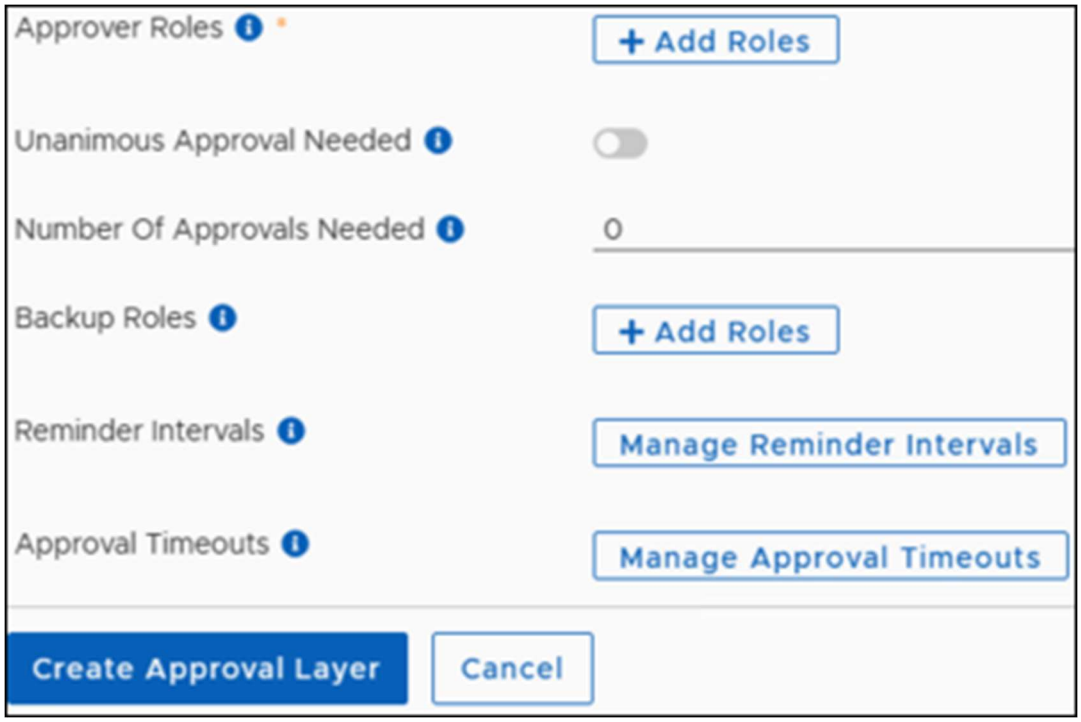
3. Reorder the roles to reflect the processing order you want the strategy to use:
    a. Select and hold the **stacked dots** for the role you want to move.
    b. Drag the **role** up or down to move it in the list.



Add Approval Roles to an Approval Layer

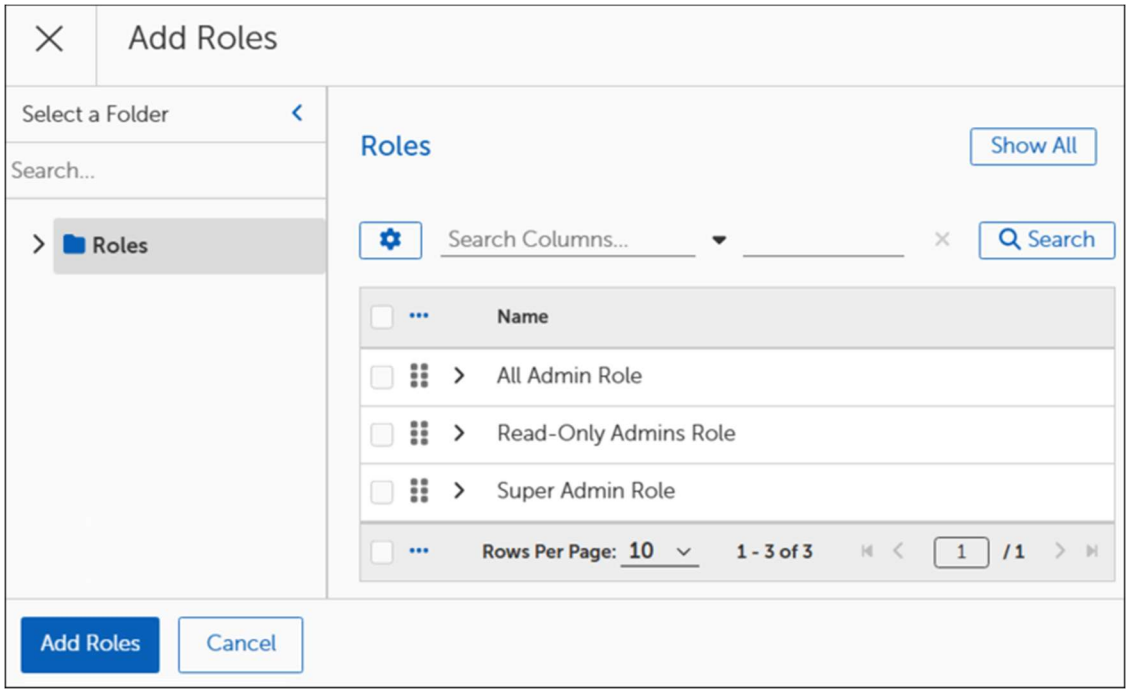
Tenable Patch Management includes templates for commonly required roles. You can add these existing roles to the Chains you create by creating approval layers.

1. Select **+ Create Approval Layer** in an open **Approval Chain** template. This opens the **Create Approval Layer** dialog.



2. Select **Add Roles** next to **Approver Roles**.

3. Select the **Show All** on the upper right to view the available Roles.
4. Select one or more **Roles** to add to the **Approval Layer**.

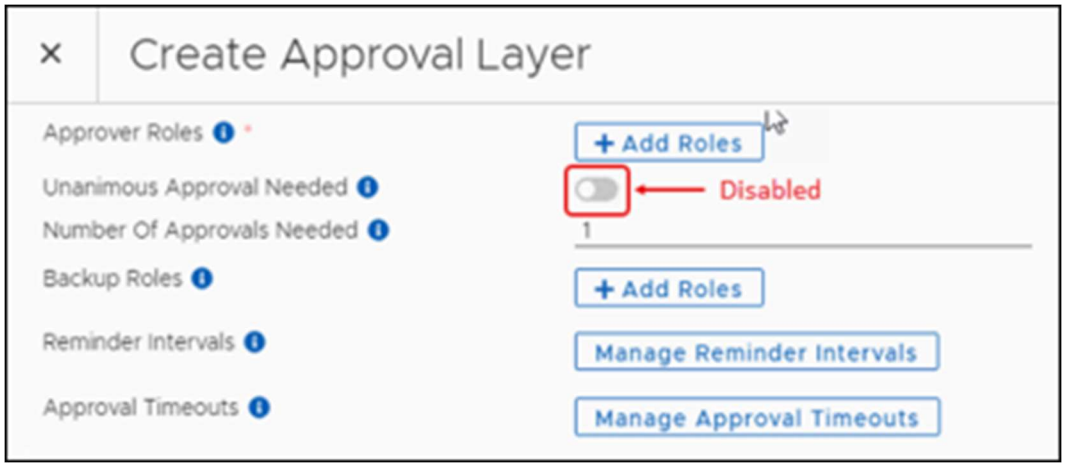


5. Select **Add Roles** at the bottom left of the page.

Set Unanimous Approval or Number of Approvals Needed

Choose the number of approvers who must approve patches to satisfy this Approval Layer:

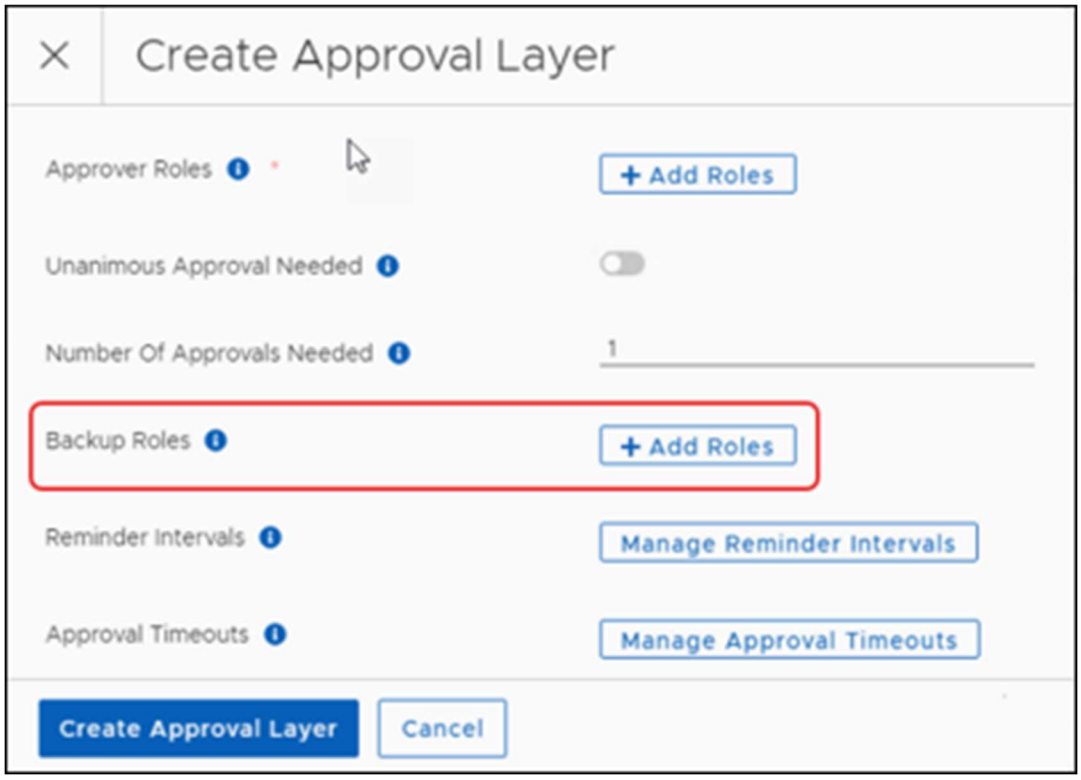
- **Enable Unanimous Approval**: Select the **Unanimous Approval Needed** toggle to enable the unanimous approval requirement. All approvers must approve before deployment continues. Defaults to disabled.
- **Disable Unanimous Approval**: If you choose not to enable this feature, you must enter the Minimal Number of Approvals Needed.



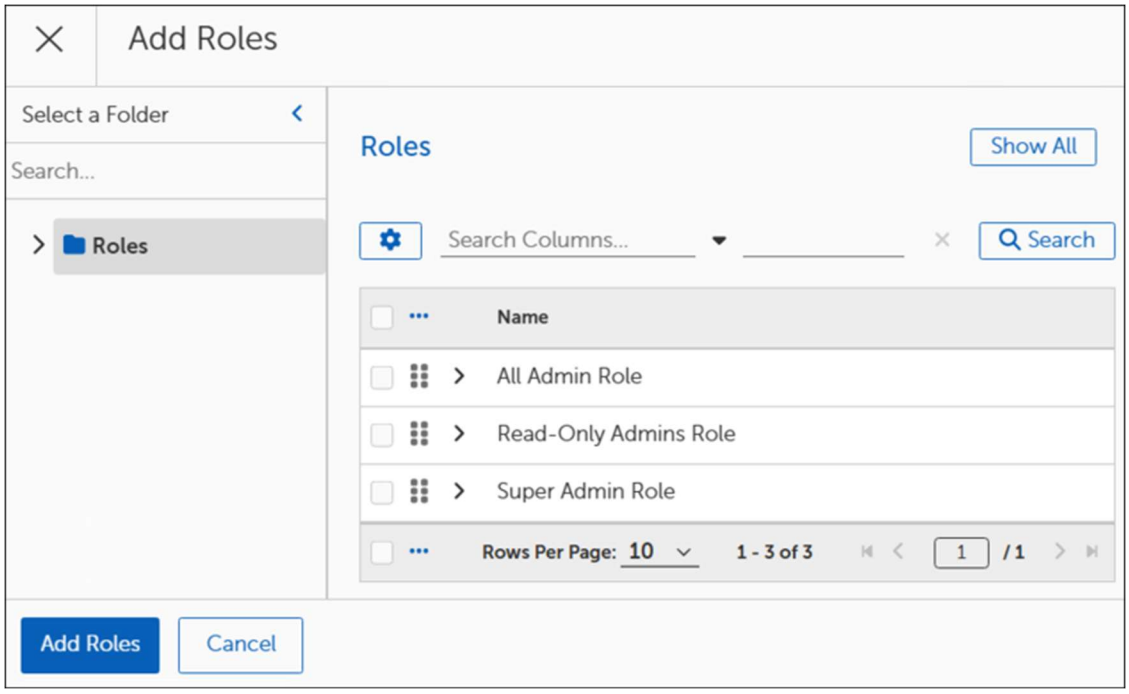
Add Backup Roles to an Approval Layer

Select backup approvers for this approval chain layer. If backup approvers do not approve within the approval timeout duration, the approval request fails.

1. Select **+ Add Roles** next to **Backup Roles** in the **Create Approval Layer** dialog.



2. Select **Show All** on the upper right to view all available Roles.
3. Select one or more **Roles** to add.

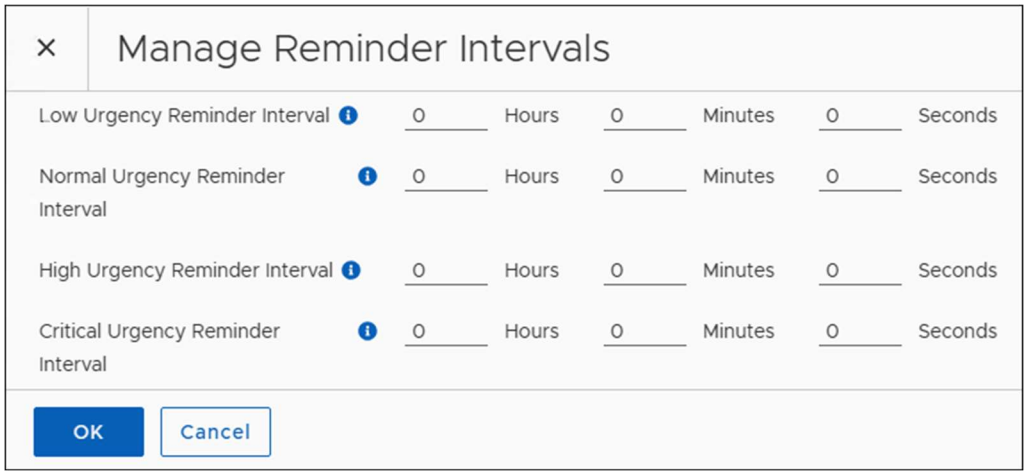


4. Select **Add Roles** at the bottom left of the page.

Set Reminder Intervals

These settings define when to send approval reminders to approvers who have not responded. You can specify different reminder intervals for each urgency level. A setting of zero (0) sends no reminders.

1. Select **Manage Reminder Intervals** below to **Approver Roles**.



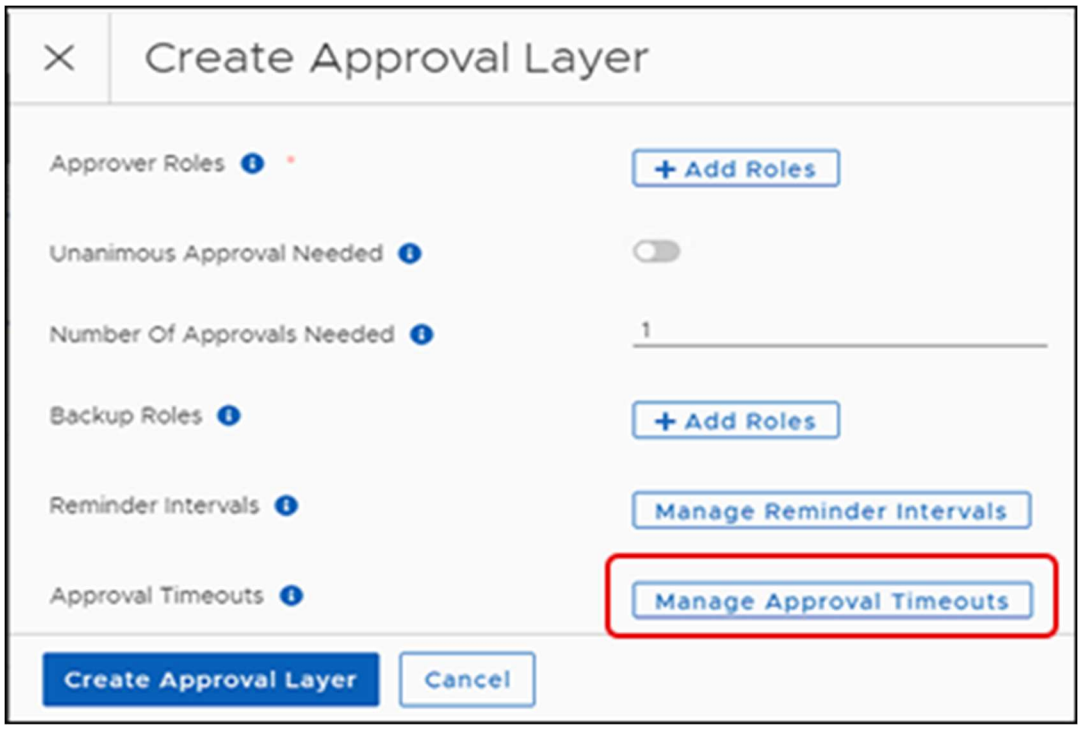
2. Enter a number for the **Urgency Reminder Interval** (Low, Normal, High, Critical).
    a. At zero (0) the strategy sends no reminder.
    b. When the request times out, the approval request fails.

3. Select **OK** at the bottom left of the page.

Set Approval Timeouts

These settings define the time out variables for the approval request . You can specify different reminder intervals for each urgency level. A setting of zero (0) sends no reminders.

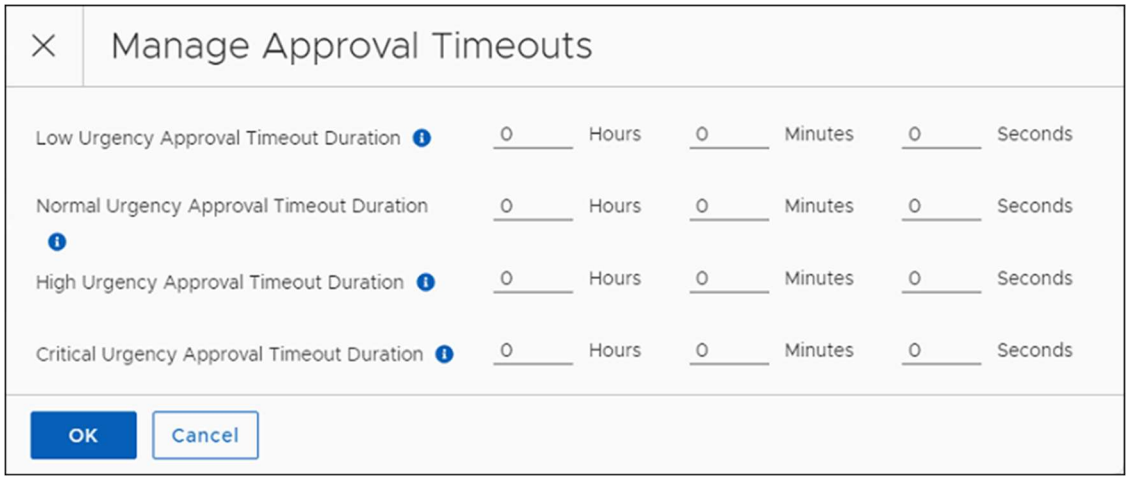
1. Select **Manage Approval Timeouts** in the **Create Approval Layer** dialog of the Approval Chain template.



2. Enter a number for the **Urgency Approval Timeout Duration** (Hours, Minutes, or Seconds) of the urgency level required:

    a. At zero (0) the strategy sends no reminder.

    b. If the request times out, the approval request fails.



3. Select OK on the bottom left of the **Manage Approval Time Outs** dialog.
4. Select Create Approval Layer to save your changes and return to the Approval Chains template.

Add Communication Providers to an Approval Layer

Tenable Patch Management supplies default Communication Providers that you can use here, or you can create your own. To create new Communication Providers that you can choose when creating Chains, see Communication Providers.

1. Select **+ Add Communication Providers** to open the **Add Communication Providers** dialog.
2. Select one or more providers to add to the Approval Chain.
3. Select **Add Communication Providers** at the bottom left of the page.
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.

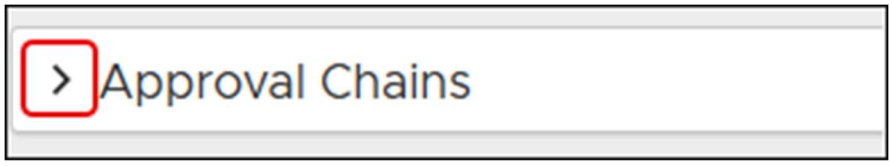
Managing Approval Settings in Object Templates

Patching Strategy and Business Unit object templates include an **Approval Chains** dialog so you can define administrative approval details as part of the object. To see links to other settings for Patching Strategies, see Optional Objects in Patching Strategy Templates.

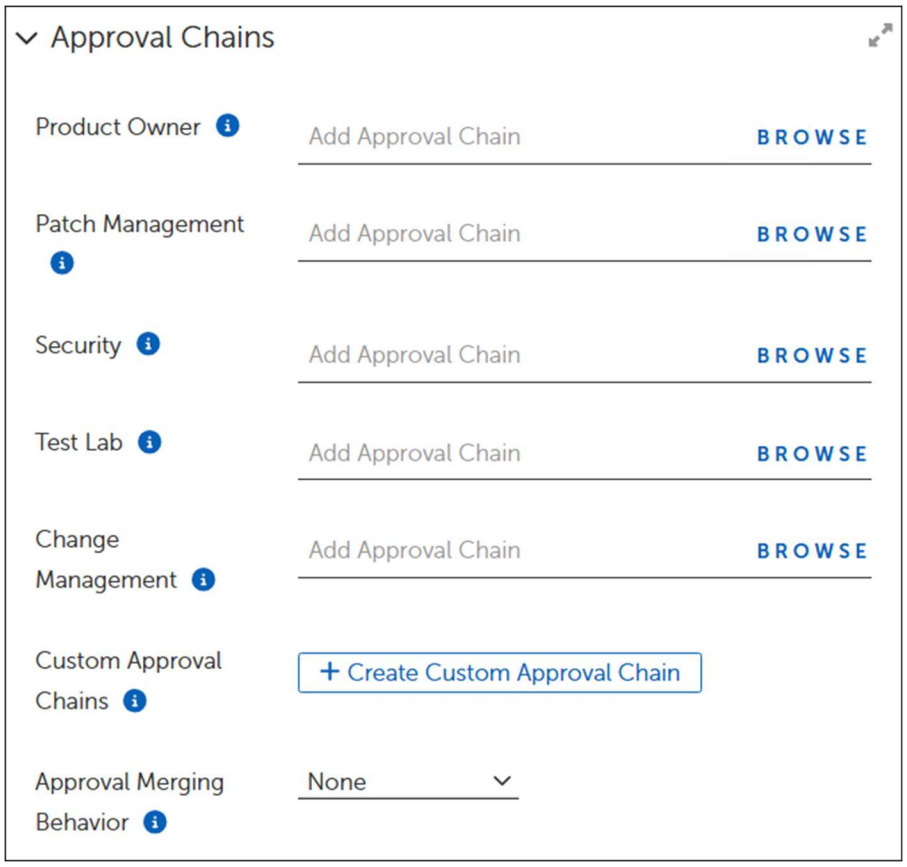
Use this procedure to assign existing **Approval Chains** to a Patching Strategy or Business Unit template. This procedure assumes you have opened and saved an object template and are ready to configure the Approval Chains.

Add Approval Chains to a Patching Strategy

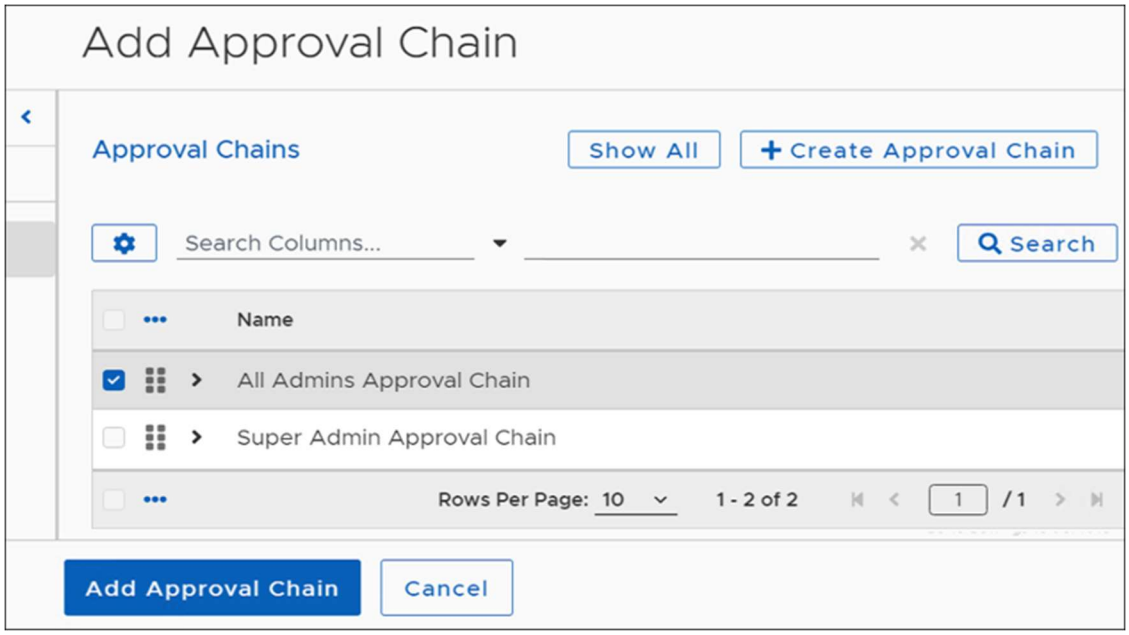
1. Select **Approval Chains** to open the **Approval Chains** workspace in an open Patching Strategy template.



2. Select **Browse** next to the type of Approval chain you want to add (Product Owner, Patch Management, Security, and so on).



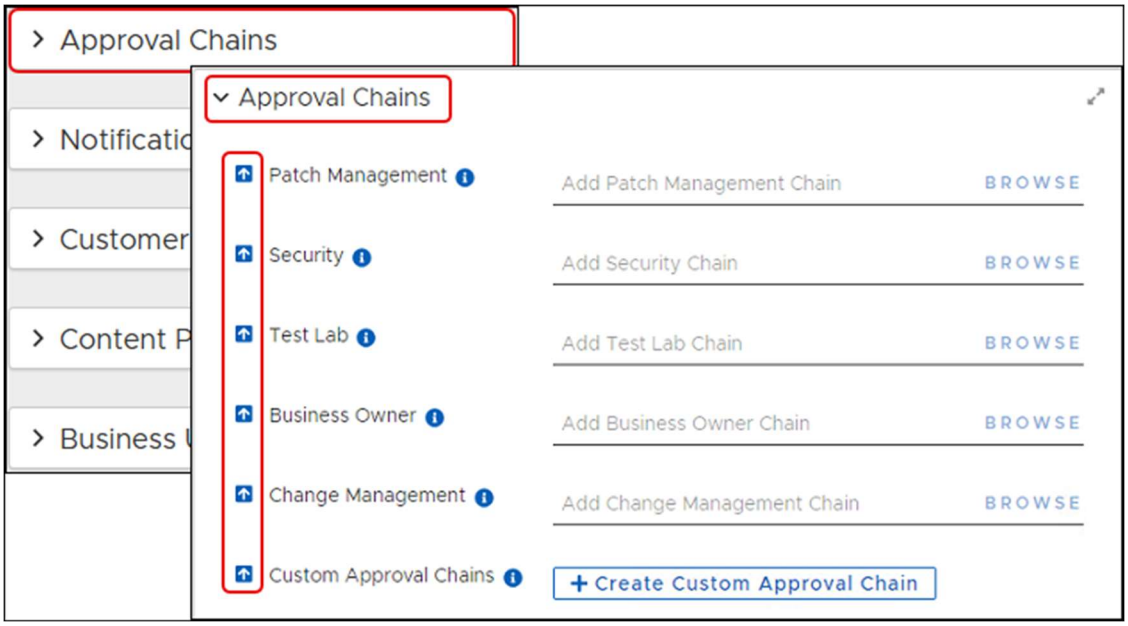
3. Select an **Approval Chain** from the **Approval Chains** table. This example uses an **All Admins Approval Chain**.



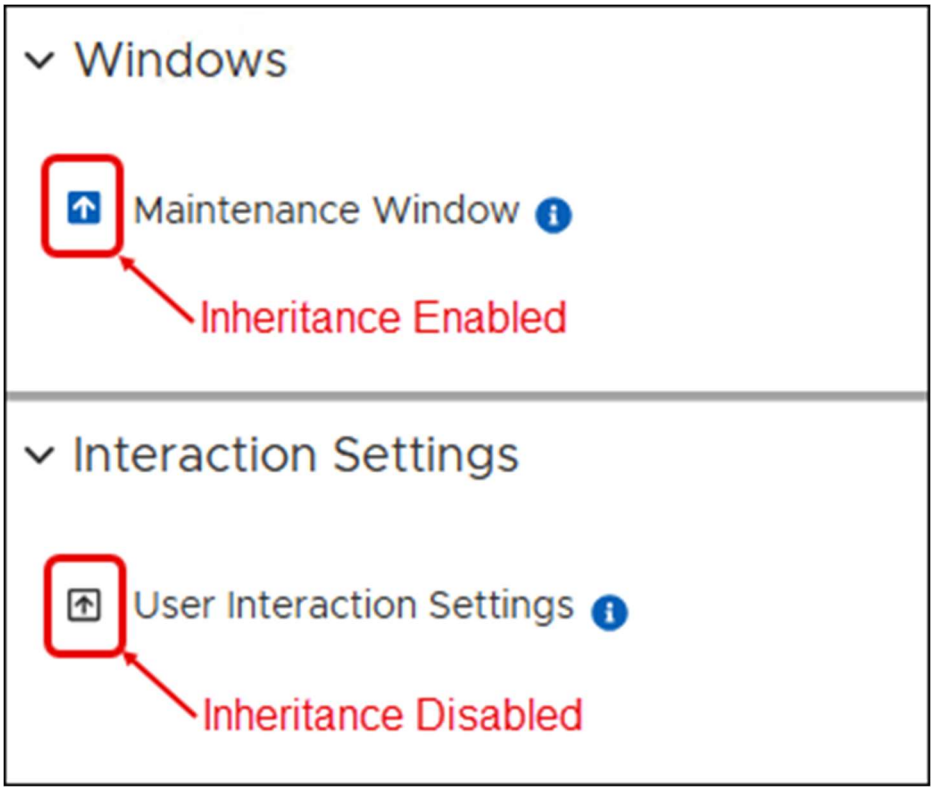
4. Select **Add Approval Chain** to return to the Patching Strategy template.
5. Repeat Steps 2 through 5 for each of the groups listed in the **Approval Chains** workspace:
    a. Skip any groups that do not apply to your situation.
    b. When each group from which you need an approval contains an approval chain, continue with the next step.
6. 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.

Add Approval Chains to a Business Unit Object

1. In an open Business Unit template, click **Approval Chains**. This opens the **Approval Chains** workspace.
    a. Business Units inherit these settings from a parent by default. For more information about inheritance, see Parent and Child Business Units

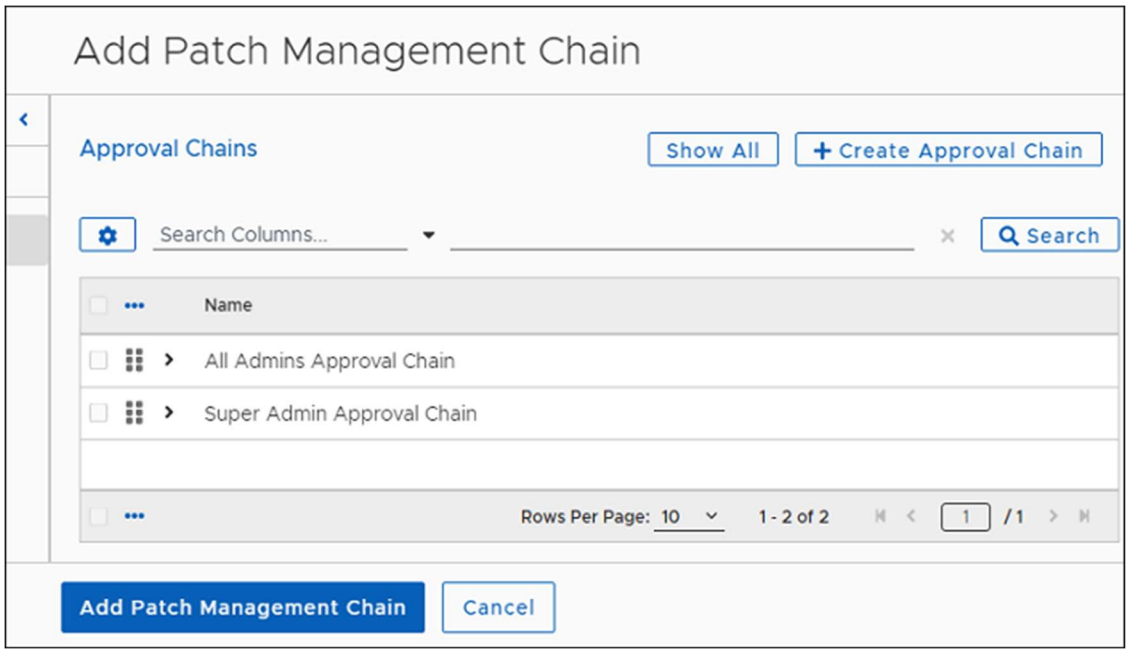


b. Disable inheritance to enable Browse and assign a different Approval Chain to a setting.



2. Select **Browse** next to the type of Approval chain you want to add (Product Owner, Patch Management, Security, and so on).

3. Select an **Approval Chain** from the **Approval Chains** table. This example uses an All Admins Approval Chain for a Patch Management Chain.



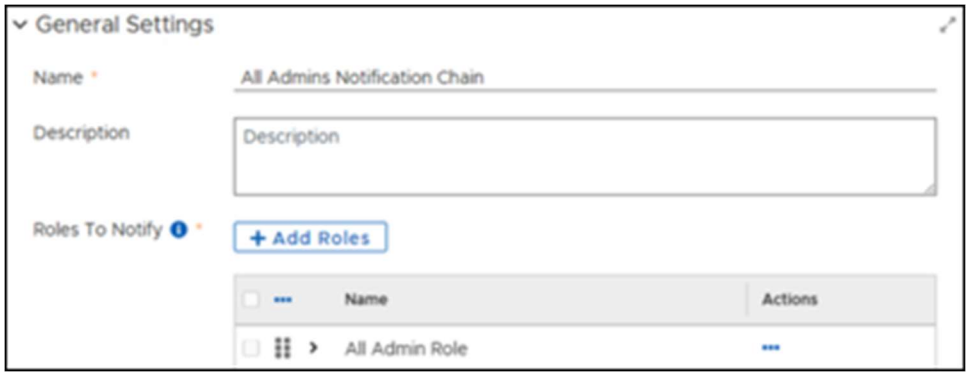
4. Select Add ... Chain on the bottom left to return to the **Approval Chains** workspace.
5. Repeat Steps 2 through 5 for each of the groups listed in the **Approval Chains** workspace:
    a. Skip any groups that do not apply to your situation.
    b. When each group from which you need an approval contains an approval chain, continue with the next step.
6. 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.

Notification Chains

Using Notification Chains

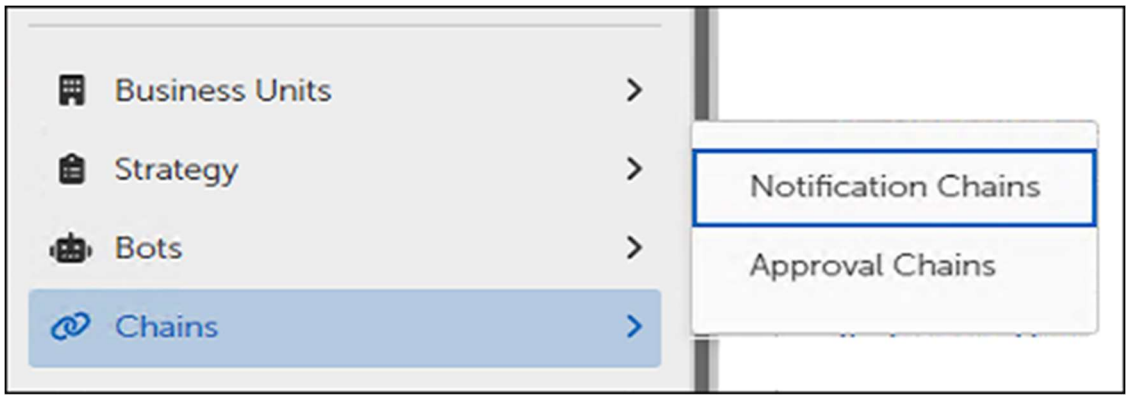
Notification Chains send notifications to the administrator roles you specify to inform them about pending deployments. In addition to creating Notifications Chains here, you can also view and create them in object templates for Patching Strategies and Business Units (see Managing Notification Settings, and for Deployment Channels (see something else).

Notification Chains allow administrators to specify who will receive notifications about patches and deployments and by what method, such as email, Teams, SMS text, or WhatsApp.



Open and Save a Notification Chain Template

1. Mouse over **Chains** or click the right arrow next to **Chains** in the left navigation menu of the Tenable Patch Management dashboard, and then select **Notification Chains**.



2. Select the title of a template to open the template, and then save the template with a new title:

    a. Select **More** in the upper-left corner of the template, and then select **Save *<object>* As**.

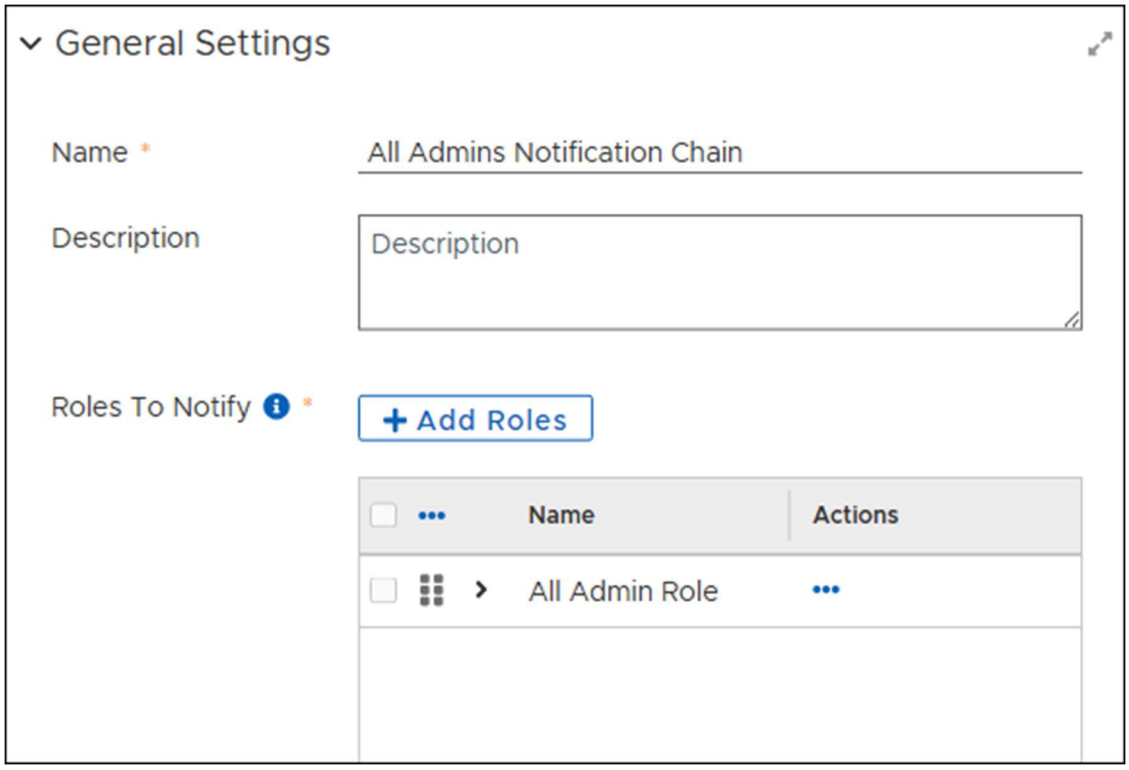
    b. Enter a new Name for the template, and then click **OK** on the lower-left corner of the naming dialog. This returns you to the template with the new name.

    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.

Manage Notification Chain Settings

Notification management configuration means identifying the Roles that require notification for the associated patches.

Each of these tasks assumes you have opened and saved a Notification Chain template and you are ready to complete the General Settings configuration.



Add Roles to Notify

Add existing Roles to a Notification Chain. Scroll down to **Roles to Notify**. If a table appears, check to see whether the existing roles apply:

a. To remove a Role from the table, click the **ellipsis (...)** in the **Actions** column, and then click **Remove**.

b. To add Roles to the table, click **+ Add Roles,** and then continue with the next step.

1. Select one or more **Roles** from the Roles table, and then click **Add Roles** at the bottom left of the dialog.
2. Select **Save** to save your progress and check for errors:

   a. Check the **Error View** and resolve any errors.

   b. Select **Save** again if you make any changes.

Managing Notification Settings

Patching Strategy, Deployment Channel, and Business Unit objects include a **Notifications** dialog where you can configure notification details. The configuration choices differ slightly for each object.

Important

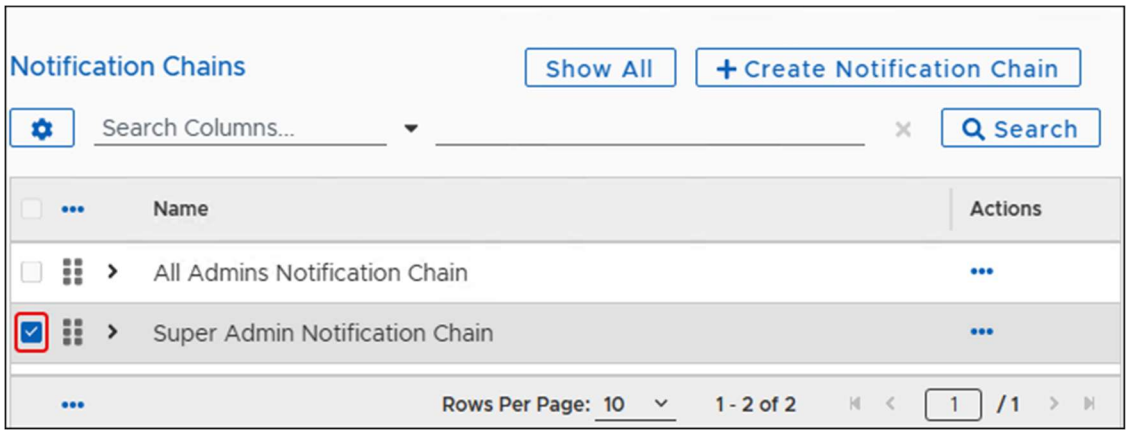
This configuration requires selecting a specific type of Notification Cycle template. Contact Tenable Customer Support for assistance with this configuration and for information about choosing the correct template.

Add a Notification Chain

Notification Chain settings exist in the object templates for Patching Strategies, Deployment Channels, and Business Units.

1. Expand the **Notifications** box in an open object template to show the available configuration options.

2. Select **Browse** next to **Notification Chain**. This opens the Notifications Chain dialog.



3. Select **Show All** to see the available templates.

4. Select a **Notification Chain** from the table. To edit or create Notification Chains, see Using Notification Chains.

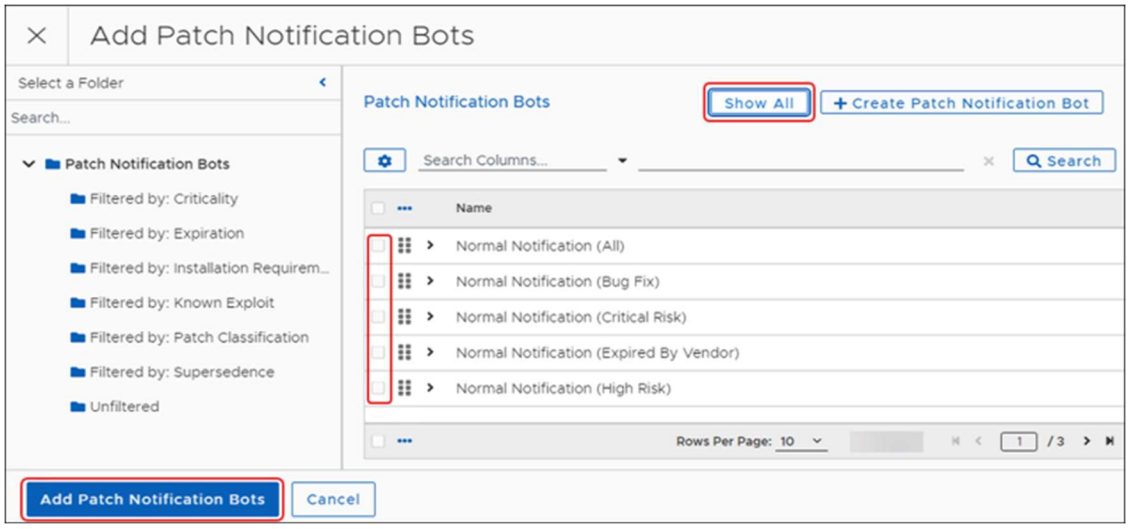
5. Continue editing the **Notification** settings or click Create Notification Settings to return to the template.

Add Patch Notification Bots

Both Patching Strategies and Deployment Channel templates have an option to **Add Patch Notification Bots**.

1. Select **+ Add Patch Notification Bots** from the **Notifications** box in the object template.

This opens the **Add Patch Notification Bots** dialog.



2. Select **Show All** to list all available **Patch Notification Bots** or click any **Filtered by:** folder to see the Bots associated with that filter.

3. Choose one or more **Notification Bots** to set requirements for this template. To create more Notification Bots, see Creating Notification Bots.

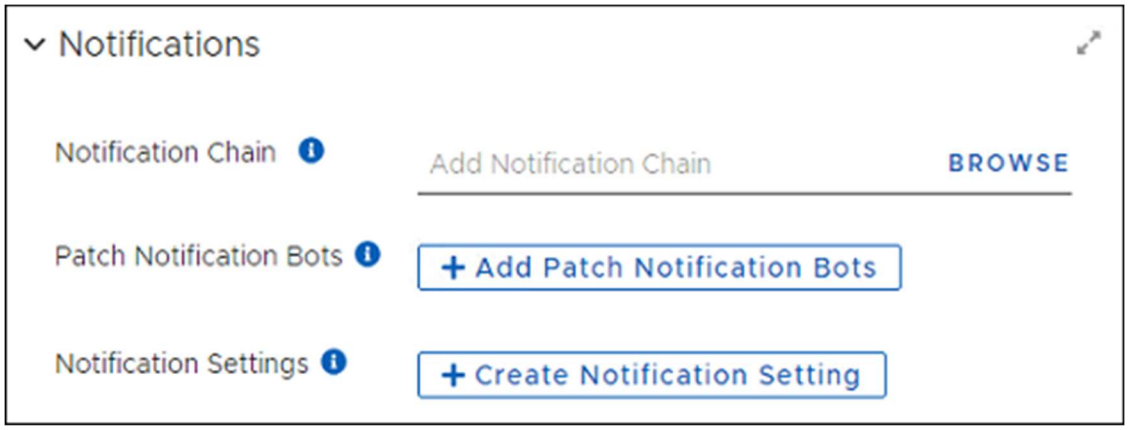
4. Select **Add Patch Notification Bots** on the bottom left of the dialog to return to the starting template settings for Notifications.

Create Notification Settings

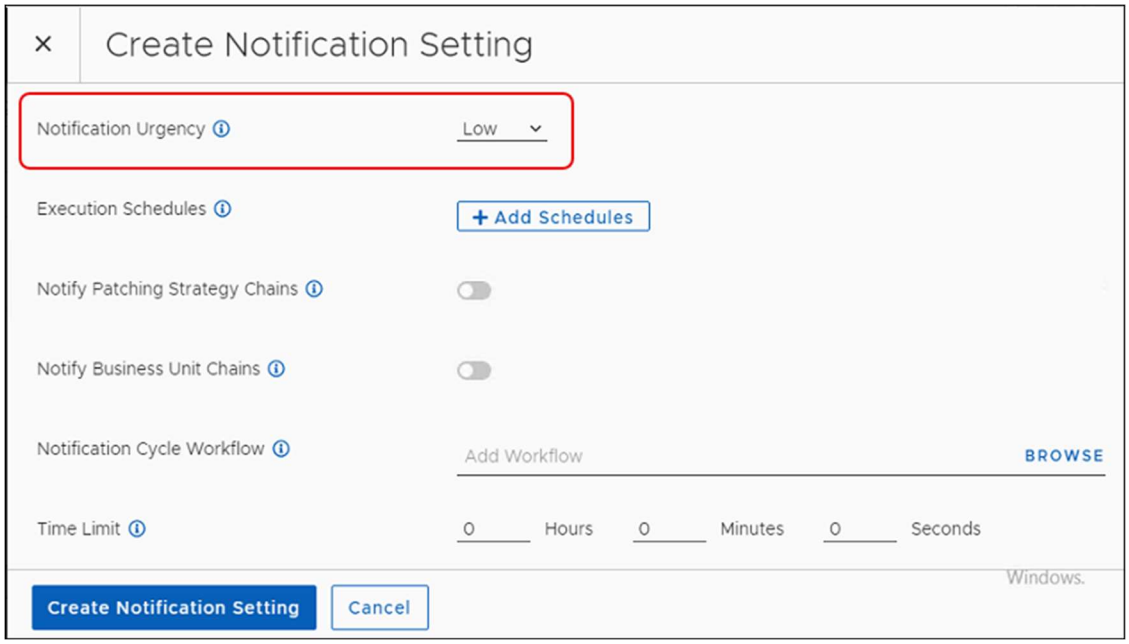
Set Notification Urgency

These values must match the corresponding values defined in the Notification Bots. Otherwise, the Notification Cycle does not send a notification.

1. Select **+ Create Notification Setting** in the Notifications box of the object template.



2. Expand the list of options next to **Notification Urgency**, and then select the urgency setting that matches the Notification Bot.



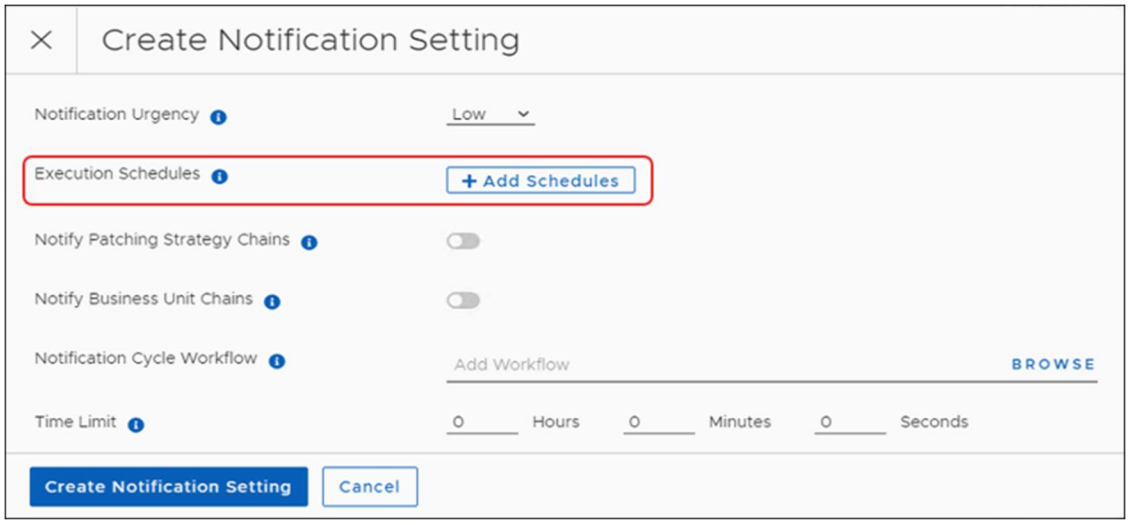
3. Continue editing the **Notification** settings or click Create Notification Settings to return to the template.

Add Execution Schedules

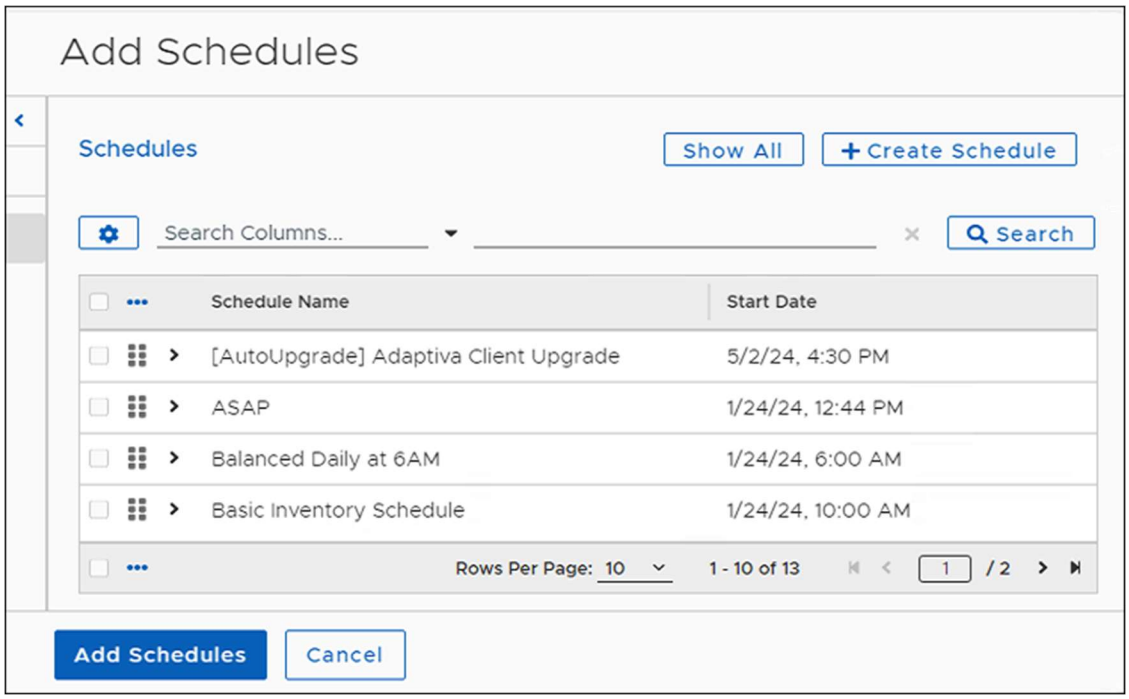
Execution Schedules control when and how often a Notification Cycle sends notifications. Choose schedules based on when and how often receiving parties require notification.

1. Select **+ Create Notification Setting** from the **Notifications** workspace of a object template.

2. Select **+Add Schedules** to display the **Create Notification Setting** dialog.



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



4. Continue editing the notification settings or click Create Notification Settings to return to the template.

Enable Notifications for Patching Strategy and Business Unit Chains

When enabled, sends notifications to the Roles shown in the Notification Chain associated with the Patching Strategy or Deployment Channel template. Defaults to disabled.

1. In the **+ Create Notification Setting** dialog in the Patching Strategy or Deployment Channel template, decide whether to enable notifications:

a. Select the **Notify Patching Strategy Chains** toggle to enable or disable (default) whether the notification cycle sends notifications to the chains included in the strategy.

b. Select the **Notify Business Unit Chains** toggle to enable or disable (default) whether the notification cycle sends notifications to Business Unit chains included in the strategy.

2. Continue editing the **Notifications** settings or click Create Notification Settings to return to the template.

Choose a Notification Cycle Workflow

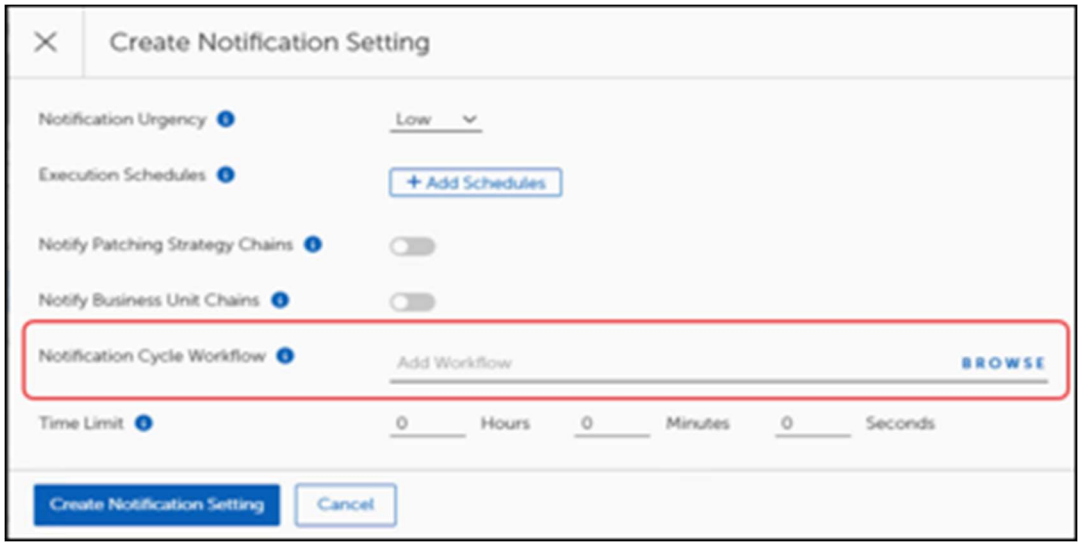
This setting names the Notification Cycle that processes the Notifications for the Patching Strategy or Deployment Channel. Notification Cycle workflows are customized for specific uses. Tenable does not provide sample Notification Cycle templates. These templates exist only if you create them for your environment.

Important

Contact Tenable Customer Support for assistance with Notification Cycle templates.

1. Select **+ Create Notification Setting** from the Notifications box in the object template.

This opens the **Create Notification Setting** dialog.



2. Select **Browse** on the **Add Workflow** line. This opens the list of available.

3. Select your custom workflow from the list, and then click **Add Workflow** on the lower-left corner of the dialog.

4. Continue editing the **Notification** settings or click Create Notification Settings to return to the template.

Set the Time Limit

Specifies the maximum length of time that the Notification Cycle Workflow runs before timing out. If set to all zeros (default) the workflow may run indefinitely. Choose this setting with care. If the notification times out before sending all notifications, the next cycle triggers the notifications again.

1. Select **+ Create Notification Setting** the Notification box of the object template.
2. Next to **Time Limit**, set the **Hours**, **Minutes**, or **Seconds** that the Notification Cycle will run, or leave the setting default at 0 for each item to allow the workflow to run indefinitely.
3. Continue editing the **Notification** settings or click Create Notification Settings to return to the template.

Deployment Channels and Deployment Channel Processes

Deployment Channels serve as a virtual queuing system for updates that helps prevent constant disruptions to end-users. Rather than deploying updates at once upon release, Tenable Patch Management adds updates to the Deployment Channel queues and releases the patches at a scheduled installation time. This approach combines process terminations, notifications, and device reboots into a single cycle, reducing the impact and disruption to users.

Deployment Channel Processes are responsible for deploying patches to Business Units, and specifying the deployment schedule. When a patch is ready for deployment, it is queued and held until the next scheduled execution. At that point, the Deployment Channel Process activates, processes all queued patches, and deploys them to the appropriate Business Units.

Deployment Channels

Configuration options include classifying different patches and adding them to various Deployment Channels based on a desired execution schedule. For example, you can add critical updates to a Daily channel that deploys critical patches within 24 hours and add less critical updates to a monthly channel which deploys all queued updates on a chosen date every month. The scheduling and frequency are completely customizable. Tenable Patch Management includes multiple, preconfigured Deployment Channels. Administrators can modify existing configurations or create new Deployment Channels.

Understanding Channel Merging Rules

Channel Merging Rules use a designated Target Channel and a defined Merging Duration to govern the merge of patch deployments from multiple Deployment Channels. The purpose of this merger is to prevent multiple channels from executing at the same time. So, when a daily channel overlaps a weekly channel once per week and the weekly channel overlaps the monthly channel once every four or five weeks, Channel Merging Rules prevent multiple channels from executing at the same time.

You can create several Channel Merging Rules for a Deployment Channel to cover multiple potential scheduling issues. The Deployment Channel evaluates the rules according to the hierarchy, so place higher priority rules before lower priority rules in the Channel Merging Rule dialog. The Deployment Channel evaluates each rule and when one rule matches, evaluation stops. Then, all submitted patches in this Deployment Channel merge with the target channel specified.

Creating a Deployment Channel

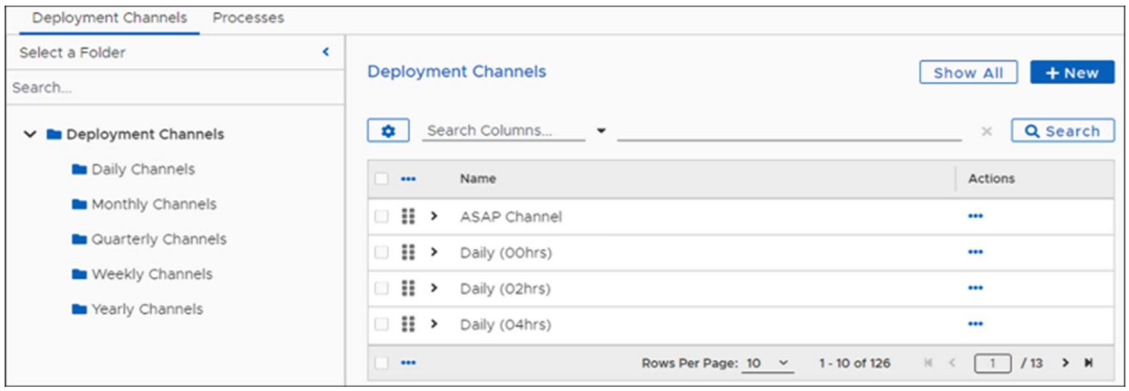
Settings in a Deployment Channel template allow you to create a deployment that meets the needs of your organization. Deployment Channels require some settings, such as a designated channel process and a Deployment Wave, and several optional configurations, including Approvals, Notifications and Content Prestaging.

Open and Save a Deployment Channel Template

1. Hover over or select **Deployment Channels** in the left navigation menu of the Tenable Patch Management Enterprise Dashboard, and then select **Deployment Channels**. This opens the table of existing Deployment Channel templates.

2. Create a New Folder for Objects in the Deployment Channels Menu.

3. Select Show All to view the available templates.



4. Select the **Name** of an existing Deployment Channel template to open it.

5. 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.

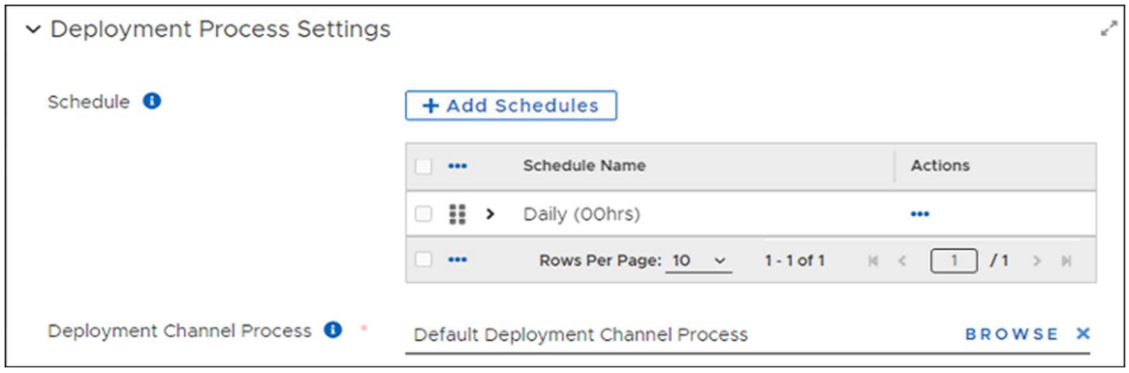
6. Move the new template to the folder you created, either now or when you complete your changes.

Deployment Process Settings

To add Deployment Process Settings to a Deployment Channel template:

Open a Deployment Channel template, and then scroll down to **Deployment Process Settings** in an open Deployment Channel template.

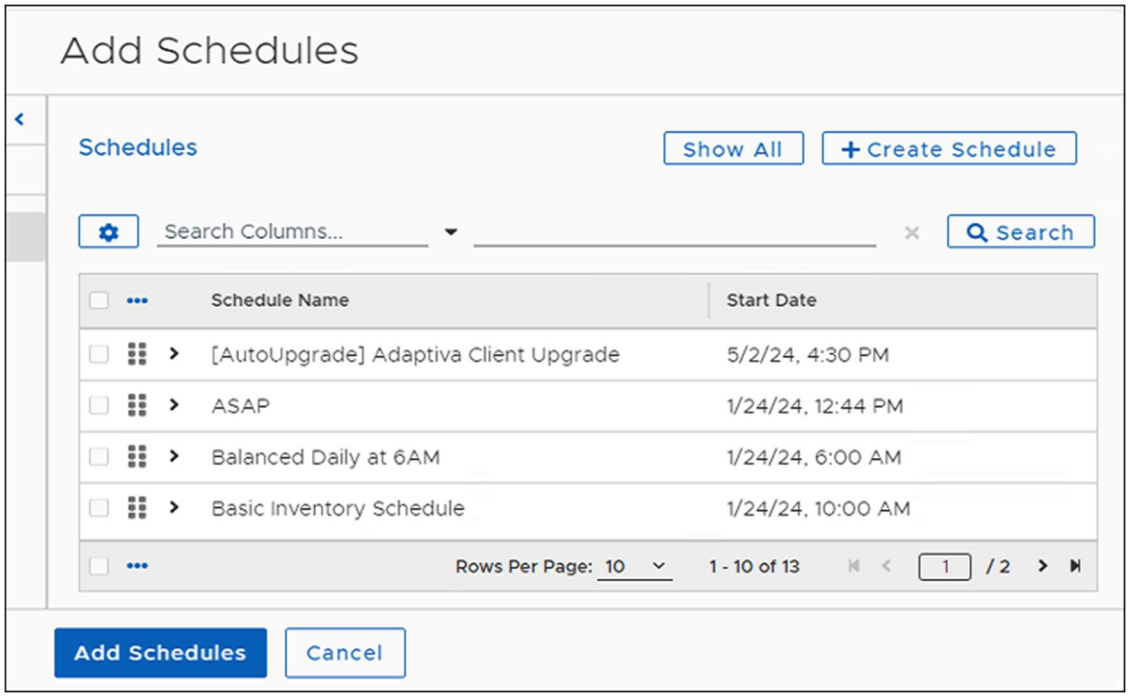
This opens the Deployment Process workspace.



Add or Change a Deployment Process Schedule

1. Select **+ Add Schedules** from the Deployment Process Settings workspace of an open Deployment Channel template.

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 to save your changes:

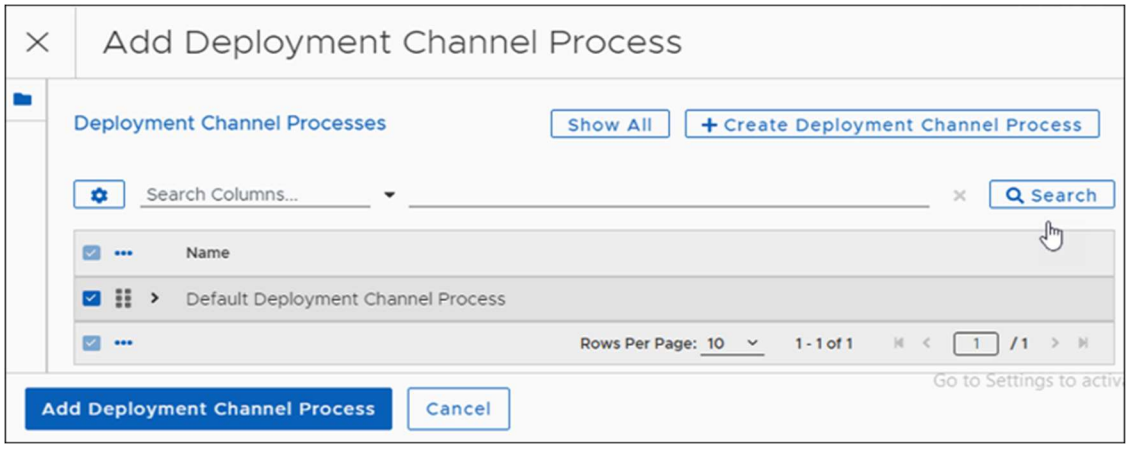
    a. Check the **Error View** and resolve any errors.

    b. Select **Save** again if you make any changes.

Add or Change a Deployment Channel Process

1. Select **+ Add Schedules** from the Deployment Process Settings workspace of an open Deployment Channel template.

2. Select **Show All** to see the available processes, and the select the **Process** to use for this Deployment Channel.



3. Select **Add Deployment Channel Process** on the bottom left to return to the template.

Deployment Control

Deployment Control settings in a Deployment Channel template allow you to choose whether to use this Deployment Channel to deploy patches to all approved Business Units or to add a Deployment Wave and restrict deployment to authorized Business Units only. For more information about Deployment Waves, see Deployment Waves.

To configure Deployment Control:

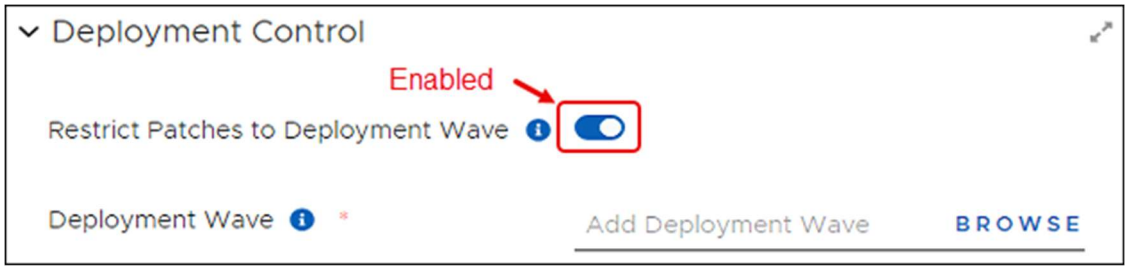
Open a **Deployment Channel template**, and then scroll down to the **Deployment Control** workspace.

Enable Deployment Control

The Deployment Control setting defaults to disabled, which allows deployment of patches using this Deployment Channel to all Business Units.

To enable Deployment Control:

1. Select the **Restrict Patches to Deployment Wave** toggle to enable using a Deployment Wave to manage deployments in this Deployment Channel.



2. Select **Browse** next to **Add Deployment Wave**.

3. Select a **Deployment Wave**, and then click Add Deployment Wave on the bottom left of the dialog. To create a new Deployment Wave, see Open and Save a Deployment Wave Template.

4. Select **Save** on the upper left to save your changes:

    a. Check the **Error View** and resolve any errors.

    b. Select **Save** again if you make any changes.

Disable Deployment Control

The Deployment Control setting defaults to disabled, which allows deployment of patches using this Deployment Channel to all Business Units.

1. Select the **Restrict Patches to Deployment Wave** toggle to disable it.

2. Select **Save** on the top left to save your changes:

a. Check the **Error View** and resolve any errors.

b. Select **Save** again if you make any changes.

Approval Chains

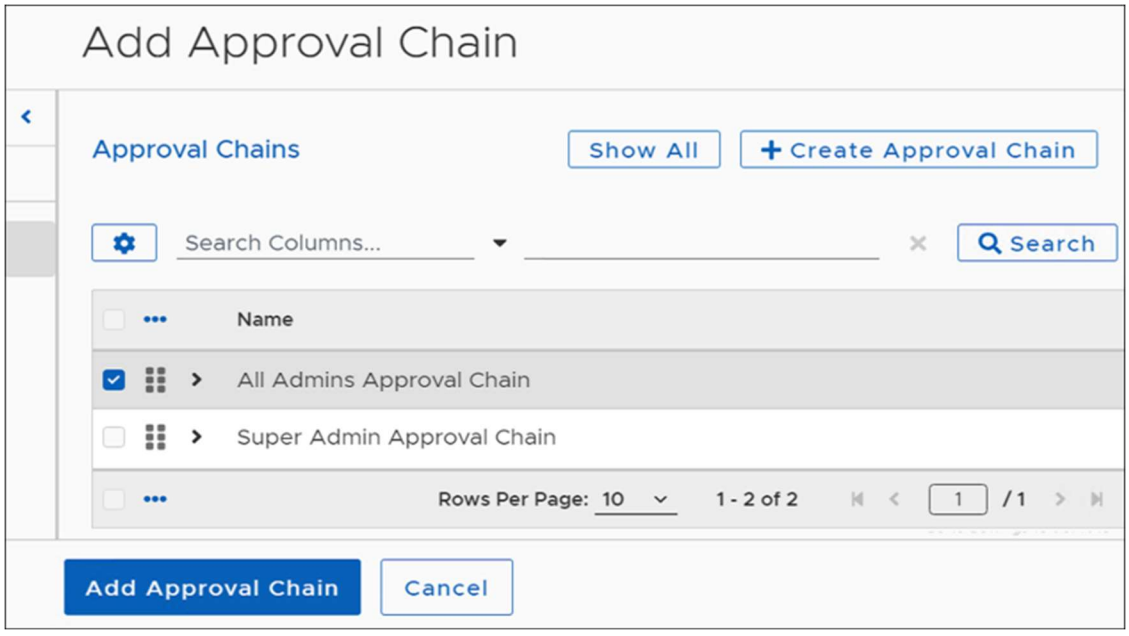
Approval Chains define and manage the approvals required before the Deployment Channel deploys patches to Business Units. Including an Approval Chain in a Deployment Channel template requires selecting an existing Approval Chain and saving it in the Deployment Channel template. For more information about Approval Chains, see Using Approval Chains.

Add an Approval Chain

Add an Approval Chain to the Deployment Channel to request approval before deploying patches to Business Units. For more information about Approval Chains, see Using Approval Chains.

1. In a open **Deployment Channel** template scroll down to the **Approval Chain** workspace.

2. Select **Browse** next to **Add Approval Chain**. This opens the table of existing Approval Chains.



3. Select an **Approval chain**, and then click Add Approval Chain to return to the Deployment Channel template.

Notifications

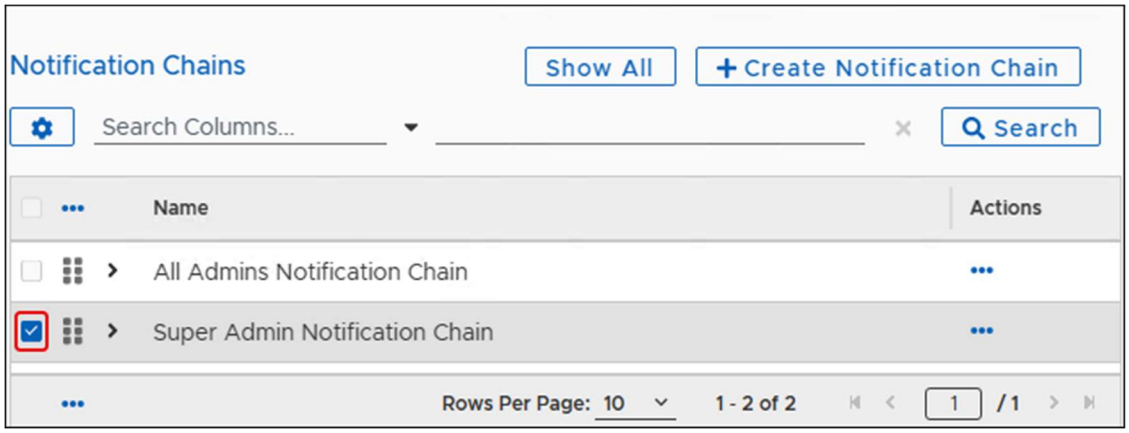
Notification settings in the Deployment Channel template include adding a Notification Chain and and Patch Notification Bots, as well as creating Notification Settings and Channel Merging Rules.

Add a Notification Chain

Notification Chain settings exist in the object templates for Patching Strategies, Deployment Channels, and Business Units.

1. Expand the **Notifications** box in an open object template to show the available configuration options.

2. Select **Browse** next to **Notification Chain**. This opens the Notifications Chain dialog.



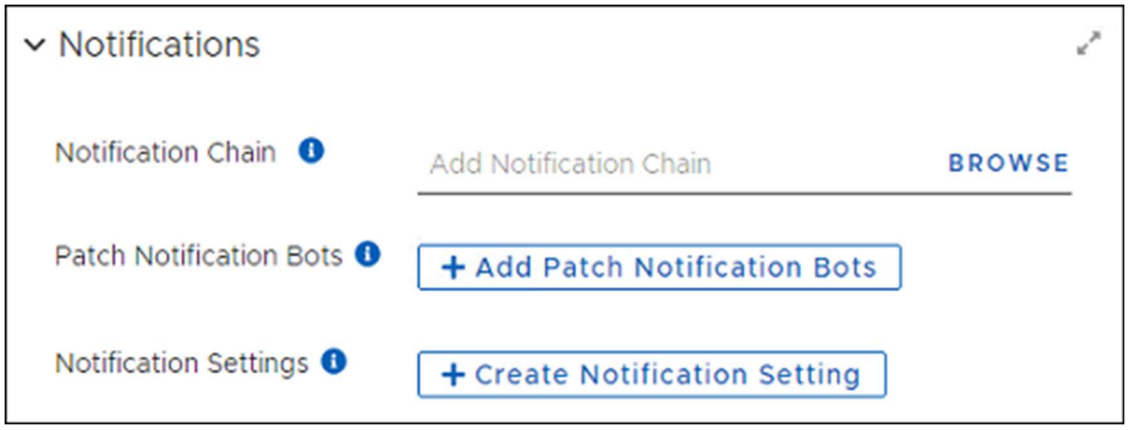
3. Select **Show All** to see the available templates.
4. Select a **Notification Chain** from the table. To edit or create Notification Chains, see Using Notification Chains.
5. Continue editing the **Notification** settings or click Create Notification Settings to return to the template.

Create Notification Settings

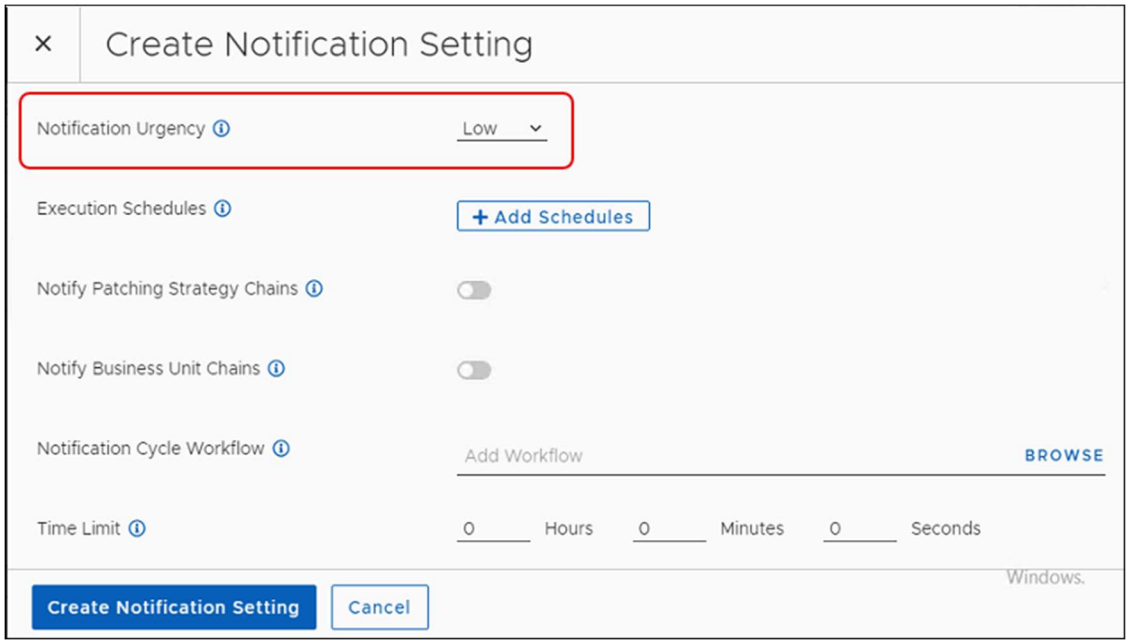
Set Notification Urgency

These values must match the corresponding values defined in the Notification Bots. Otherwise, the Notification Cycle does not send a notification.

1. Select **+ Create Notification Setting** in the Notifications box of the object template.



2. Expand the list of options next to **Notification Urgency**, and then select the urgency setting that matches the Notification Bot.



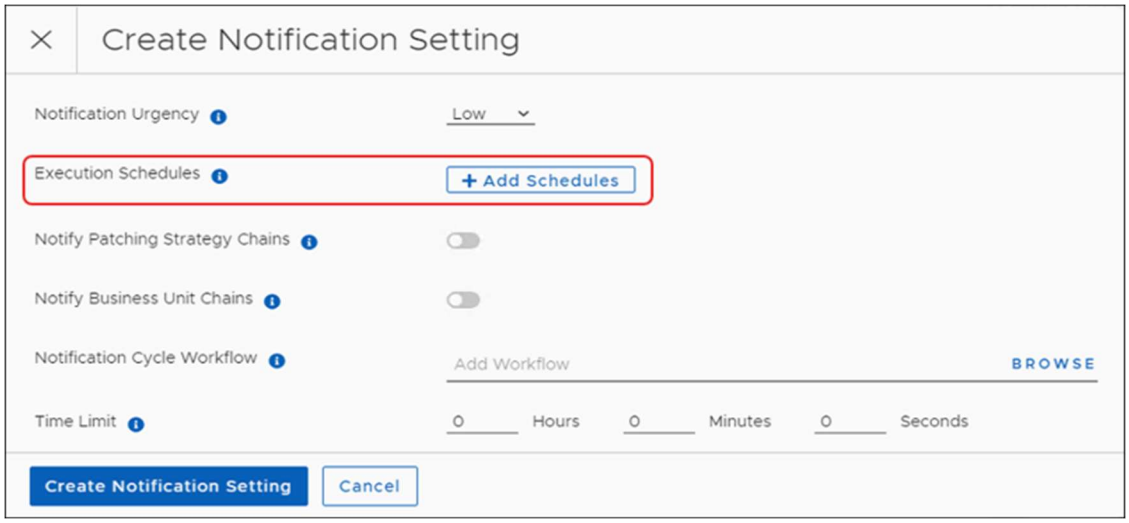
3. Continue editing the **Notification** settings or click Create Notification Settings to return to the template.

Add Execution Schedules

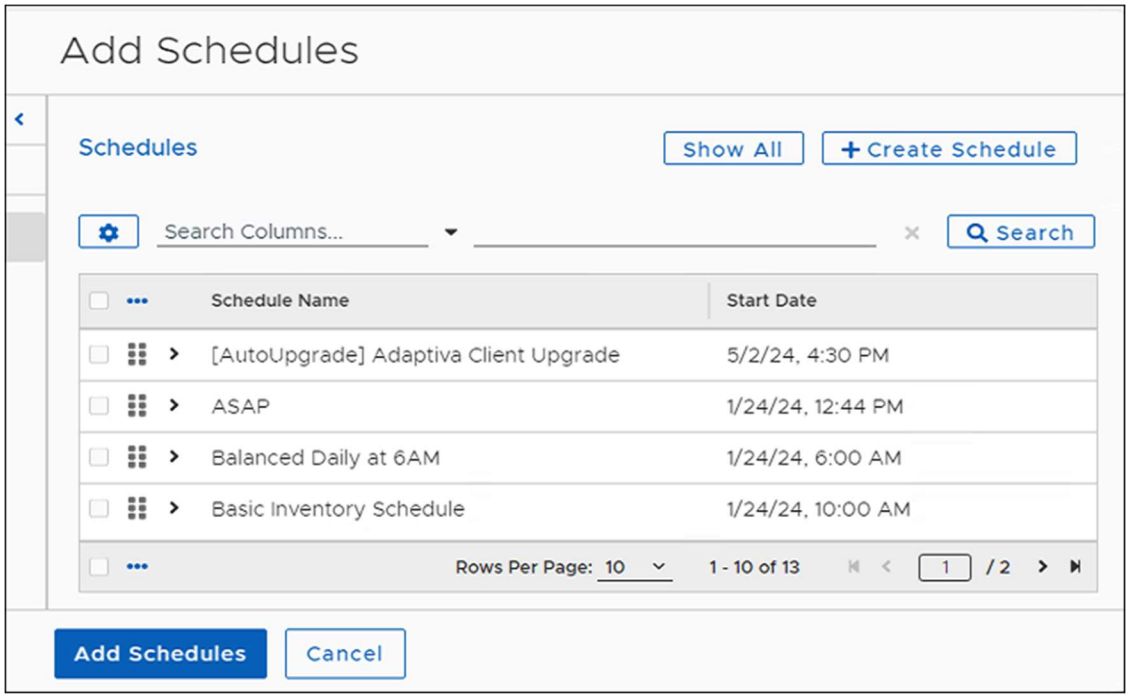
Execution Schedules control when and how often a Notification Cycle sends notifications. Choose schedules based on when and how often receiving parties require notification.

1. Select **+ Create Notification Setting** from the **Notifications** workspace of a object template.

2. Select **+Add Schedules** to display the **Create Notification Setting** dialog.



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



4. Continue editing the notification settings or click Create Notification Settings to return to the template.

Enable Notifications for Patching Strategy and Business Unit Chains

When enabled, sends notifications to the Roles shown in the Notification Chain associated with the Patching Strategy or Deployment Channel template. Defaults to disabled.

1. In the **+ Create Notification Setting** dialog in the Patching Strategy or Deployment Channel template, decide whether to enable notifications:

    a. Select the **Notify Patching Strategy Chains** toggle to enable or disable (default) whether the notification cycle sends notifications to the chains included in the strategy.

    b. Select the **Notify Business Unit Chains** toggle to enable or disable (default) whether the notification cycle sends notifications to Business Unit chains included in the strategy.

2. Continue editing the **Notifications** settings or click Create Notification Settings to return to the template.

Choose a Notification Cycle Workflow

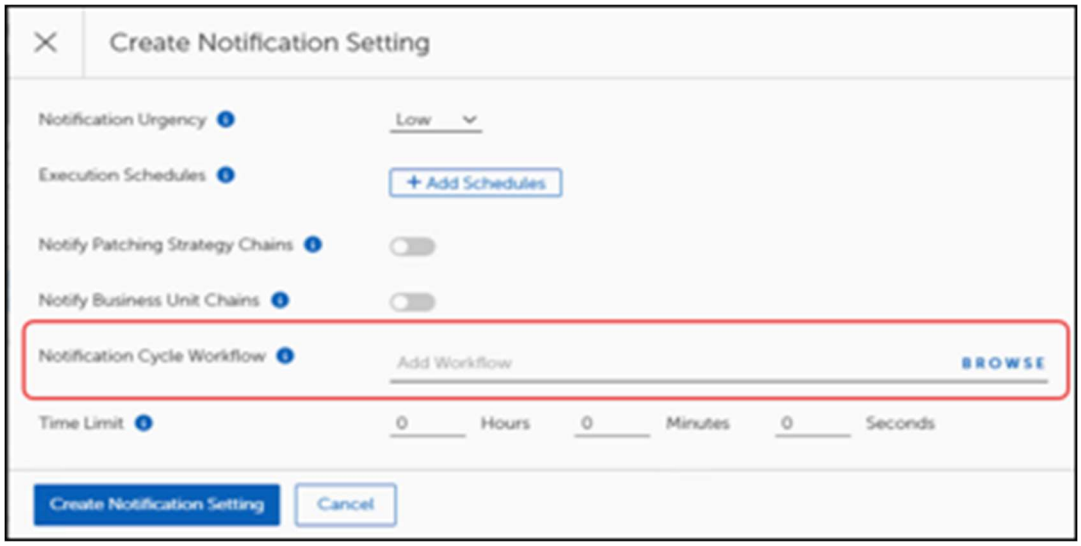
This setting names the Notification Cycle that processes the Notifications for the Patching Strategy or Deployment Channel. Notification Cycle workflows are customized for specific uses. Tenable does not provide sample Notification Cycle templates. These templates exist only if you create them for your environment.

Important

Contact Tenable Customer Support for assistance with Notification Cycle templates.

1. Select **+ Create Notification Setting** from the Notifications box in the object template.

This opens the **Create Notification Setting** dialog.



2. Select **Browse** on the **Add Workflow** line. This opens the list of available.

3. Select your custom workflow from the list, and then click **Add Workflow** on the lower-left corner of the dialog.

4. Continue editing the **Notification** settings or click Create Notification Settings to return to the template.

Set the Time Limit

Specifies the maximum length of time that the Notification Cycle Workflow runs before timing out. If set to all zeros (default) the workflow may run indefinitely. Choose this setting with care. If the notification times out before sending all notifications, the next cycle triggers the notifications again.

1. Select **+ Create Notification Setting** the Notification box of the object template.

2. Next to **Time Limit**, set the **Hours**, **Minutes**, or **Seconds** that the Notification Cycle will run, or leave the setting default at 0 for each item to allow the workflow to run indefinitely.

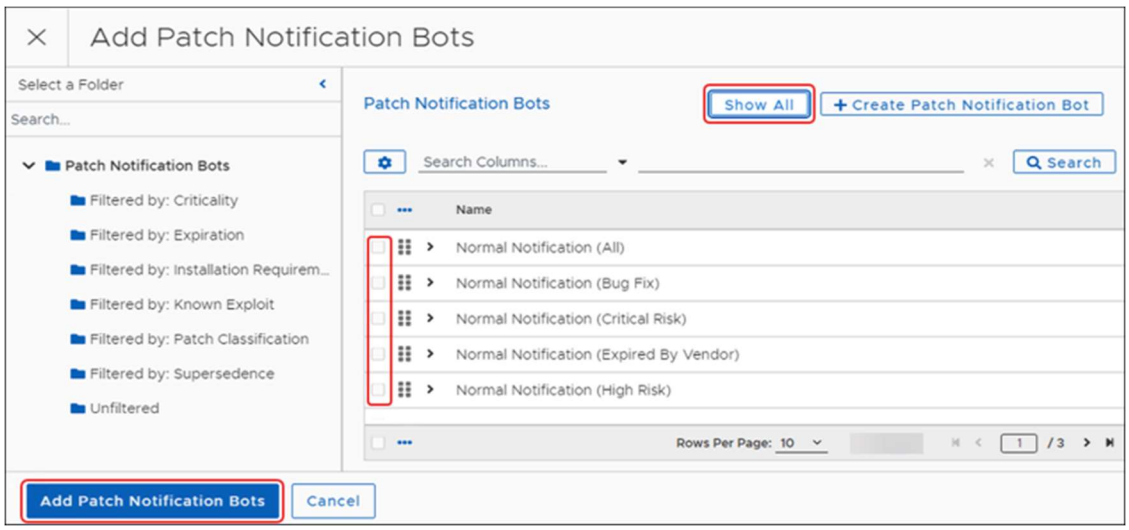
3. Continue editing the **Notification** settings or click Create Notification Settings to return to the template.

Add Patch Notification Bots

Both Patching Strategies and Deployment Channel templates have an option to **Add Patch Notification Bots**.

1. Select **+ Add Patch Notification Bots** from the **Notifications** box in the object template.

This opens the **Add Patch Notification Bots** dialog.



2. Select **Show All** to list all available **Patch Notification Bots** or click any **Filtered by:** folder to see the Bots associated with that filter.

3. Choose one or more **Notification Bots** to set requirements for this template. To create more Notification Bots, see Creating Notification Bots.

4. Select **Add Patch Notification Bots** on the bottom left of the dialog to return to the starting template settings for Notifications.

Create Channel Merging Rules

Channel Merging Rules merge patch deployments from multiple Deployment Channels when deployment schedules from two or more channels overlap. Settings here include adding a Deployment Channel to serve as a Target Channel and setting the timing for Merge Duration. See *Understanding Channel Merging Rules* for more information.

1. Select **Browse** next to **Add Deployment Channel**, and then select a **Deployment Channel**.

2. Select **+ Create Channel Merging Rule** from the Notification box of a Deployment Channel template.

3. Select **Add Deployment Channel** at the bottom left to return to the Channel Merging Rule template.

4. Set the **Merging Duration** to the number of hours, minutes, or seconds before this Deployment Channel executes.

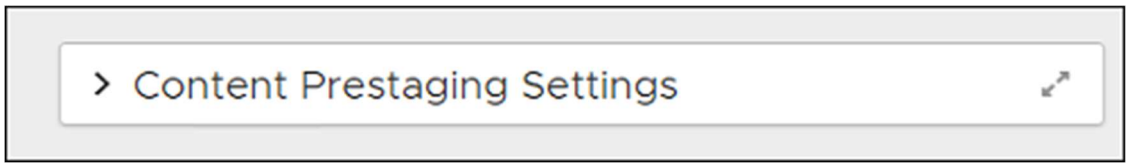
Content Prestaging Settings

The Content Prestaging feature enables Tenable Patch Management to provide deployment content to devices ahead of the scheduled deployment, either pushing content to a location or allowing a client to pull content. Prestaging content makes the content available on the device locally when the deployment time arrives. This reduces the deployment time and minimizes the chances of missing service windows or having devices going offline before a content download finishes.

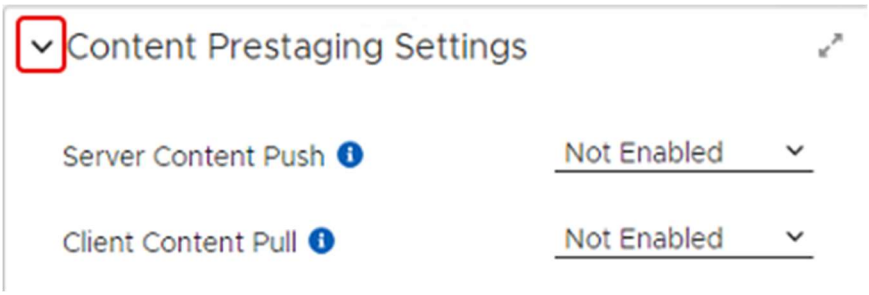
Set Content Prestaging Settings

Use this procedure to add or change Content Prestaging Settings in Patching Strategy, Business Unit, or Deployment Channel templates.

1. Expand the **Notifications** box in an open object template, and then scroll down to the Content Prestaging Settings.



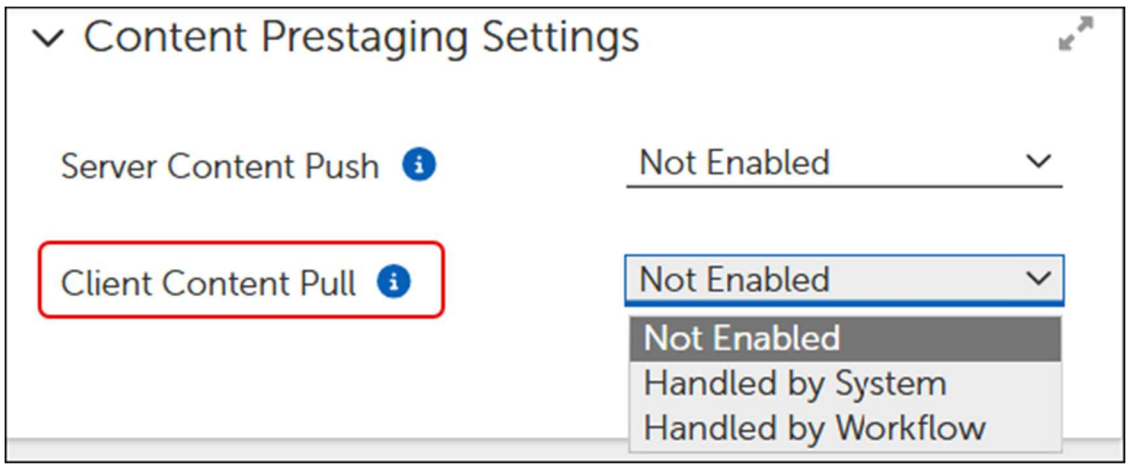
2. Expand the Content Prestaging Settings box to view the available settings.



Enable Client Content Pull

Client Content Pull defaults to Not Enabled. To enable pull settings, complete the following steps in the Content Prestaging Settings of a Patching Strategy, Business Unit, or Deployment Channel template:

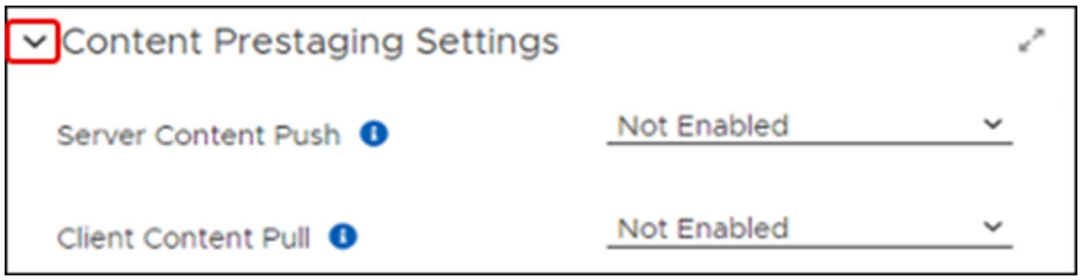
1. Select the arrow to the right of **Client Content Pull** to expand the menu of available options.



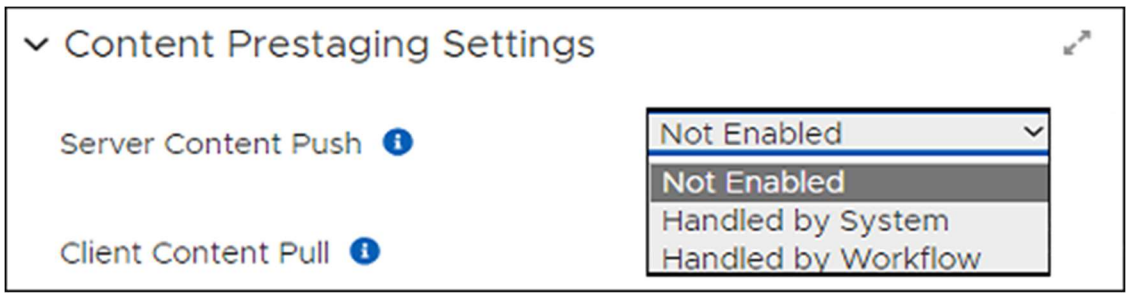
2. Select the option you need for the object template you are using. For definitions of push options, see Defining Content Prestaging Settings.
3. Select **Save** on the upper left to save your changes:
    a. Check the **Error View** and resolve any errors.
    b. Select **Save** again if you make any changes.

Enable Server Content Push

Server Content Push defaults to Not Enabled. To enable push settings, complete the following steps in the Content Prestaging Settings of a Patching Strategy, Business Unit, or Deployment Channel template, complete the following steps:



1. Select the arrow to the right of **Server Content Push** to expand the menu of available options.



2. Select the option you need for the object template you are using. For definitions of push options, see Defining Content Prestaging Settings.

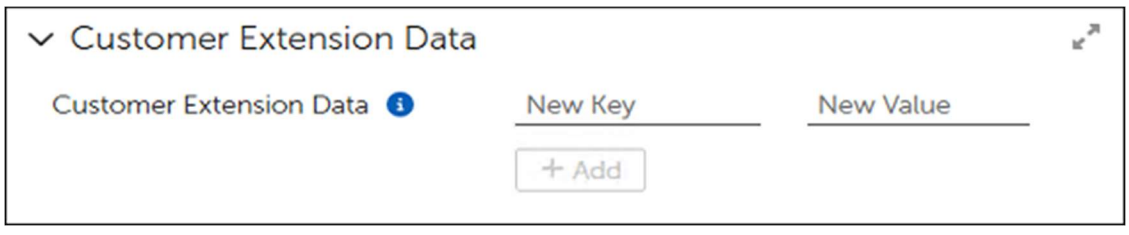
3. Select **Save** on the upper left to save your changes:

    a. Check the **Error View** and resolve any errors.

    b. Select **Save** again if you make any changes.

Customer Extension Data

Customer Extension Data is an advanced feature of Tenable Patch Management. The Customer Extension Data fields allow advanced users to specify different key/value pairs for use in customized Patching Strategies, Deployment Chains, or Business Units when necessary to achieve different results.



Customer Extension Data fields relate directly to fields in a customized template. If you do not have customized templates with key/value pairs you can modify, you do not need to configure or use this feature.

If you want to create customized templates that use key/value pairs for some settings, contact Tenable Customer Support.

Deployment Channel Processes

Deployment channel processes collect patch approvals, and then execute according to the schedule defined in the Deployment Channel. The logic in the Channel Process defines how to roll out patches to Business Units (one at a time or following the deployment waves, and so on).

Creating Deployment Channel Processes

If you want to create your own Channel Processes, enter a support ticket, and request help from Tenable Customer Support. Customer Support will help you understand the nuances of Channel Processes and assist with creating templates that support your requirements.

Deployment Waves

Deployment Waves allow deployment of patches progressively to devices contained in different Business Units. Because Waves execute in top-to-bottom order, less Critical Business Units appear higher in the priority. This prioritizes deployment to non-mission critical business units or smaller groups of endpoints first, followed by more critical or larger groupings of endpoints.

Using Deployment Waves

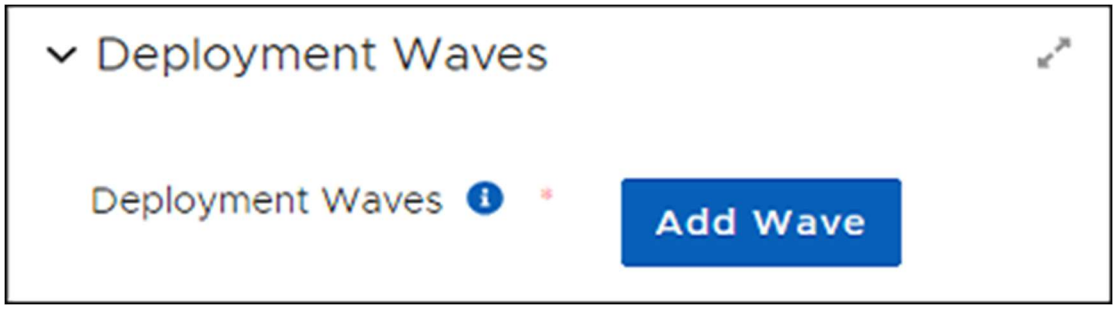
Entries for Deployment Wave settings exist in the object templates for Business Units, Deployment Channels, and Customized Products templates. All methods use the same process.

Open and Save a Deployment Wave Template

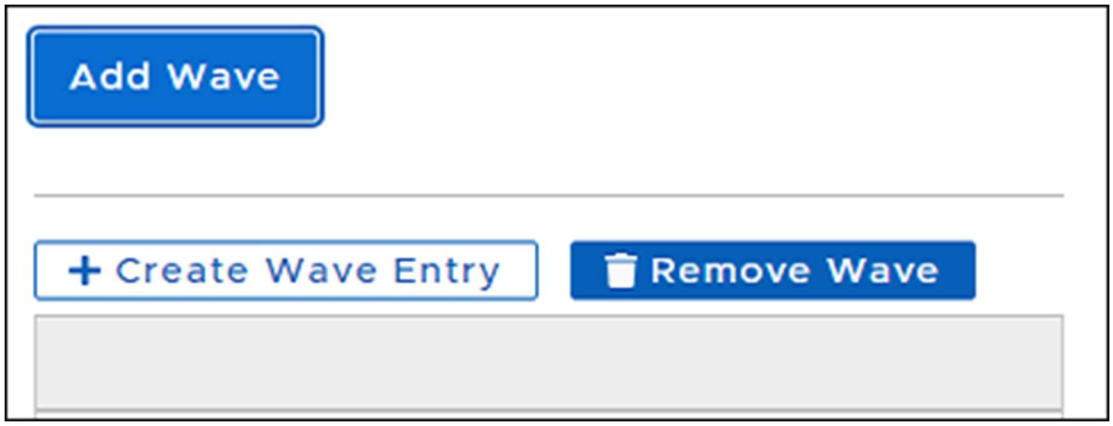
1. Select **Deployment Waves** in the left navigation menu of the Tenable Patch Management Enterprise Dashboard.
2. Select the **Name** of a template to open it, and then save the template with a new title:
    a. Select **More** in the upper-left corner of the template, and then select **Save *<object>* 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.

Add a Deployment Wave Entry

1. Scroll down to **Deployment Waves** in an open Deployment Wave template.
2. Select **Add Wave**. This creates a new table to hold another Wave in the template.



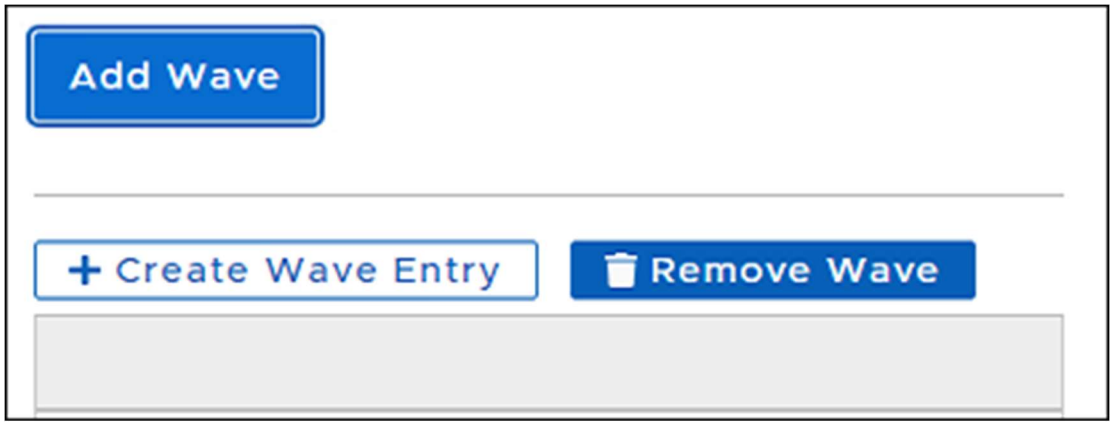
3. Select **+ Create Wave Entry** to open the **Wave Entry** dialog.



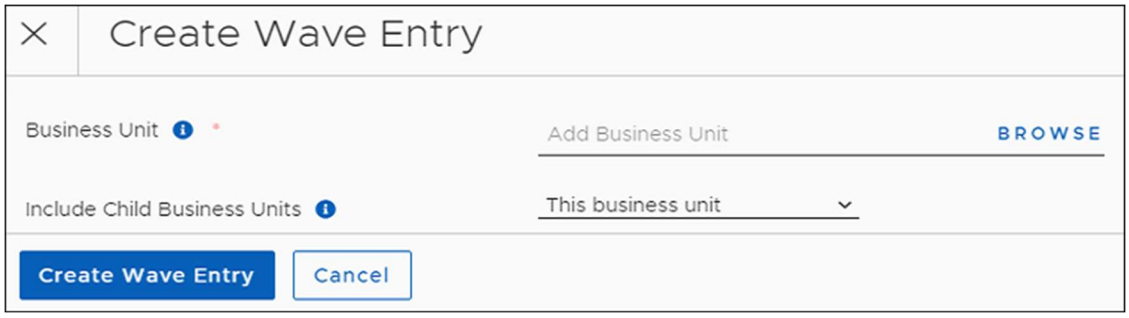
4. Select **Browse** next to **Add Business Unit**:
    a. Navigate to and select the Business Unit to which the Wave Entry applies.
    b. Expand the **Include Child Business Units** menu to include one or more child Business Units of the selected parent.
    c. Select the **item** that best describes how you want this wave to manage this deployment to child Business Units.
5. Select **Create Wave Entry** to return to the **Deployment Wave** template.
6. 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.

Create a Wave Entry

1. Scroll down to **Deployment Waves** in an open Deployment Wave template:



2. Select **Add Wave**, and the select **+ Create Wave Entry**. This opens the **Create Wave Entry** dialog.



3. Select **Browse** next to **Add Business Unit**:
    a. Navigate to and select the **Business Unit** to which the Wave Entry applies.
    b. Select **Add Business Unit** on the bottom left.
4. Expand the **Include Child Business Units** menu to include one or more child Business Units of the selected parent.
5. Select **Create Wave Entry** to return to the Deployment Wave template.
6. 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.

Edit or Remove a Wave Entry

1. Select **Deployment Waves** in the left navigation menu of the Tenable Patch Management dashboard, and then click Show All on the upper right.
2. Open the **Deployment Wave template** you want to change.
3. Scroll down to the Deployment Waves table that shows the Wave Entry you want to edit or remove.
4. Select the **ellipsis (...)** in the **Actions** column, and then choose an option:
    a. To remove the Wave, select **Remove Wave Entry**.
    b. To Edit the Wave, select **Edit the Remote Wave Entry**, and then make any necessary changes.
5. 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.

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

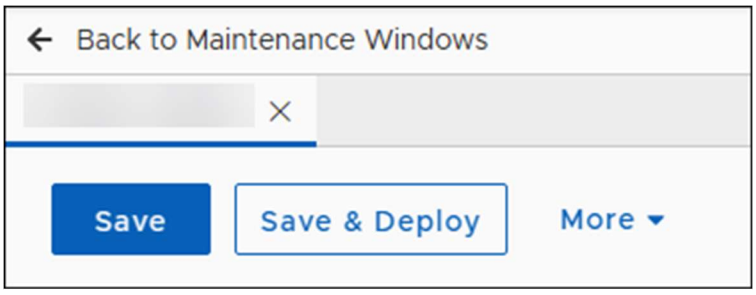
An override duration for the **All Urgencies Maintenance Window** sets the amount of time to wait for the Maintenance Window to open for all urgency level updates. After this time, the system overrides the Maintenance Window setting.

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.



Communication Providers

The Communication Providers template lists the available notification methods used to send notifications to administrators, approvers, and others.

The basic built-in Communication Providers included with Tenable Patch Management are HTML email, Simple email, HTML SMTP, Simple SMTP, SMS/Text, Microsoft Teams Notification, or WhatsApp notification.

Using Communication Providers

Tenable Patch Management has several common Communication Providers configured for notification purposes. You can add new communication providers if the existing choices do not meet your needs.

Open and Save a Communication Provider Template

1. Select **Communication Providers** in the left navigation menu of Tenable Patch Management Dashboard.

2. Select the **Name** of an existing template to open it, and then 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.

Set Communication Provider Properties

1. Scroll down to **Communication Provider Properties** box in an open Communication Provider template, and then choose a **Media Type**. This is the media type used by the provider you are creating.

    a. If the **Media Type** is related to an **SMTP Server**, **skip to Step 5**. These Media Types use neither Message Aggregation nor Subject Line indicators. Both items default to disabled.

    b. Otherwise, **continue with Step 2**.

2. Select the **Supports Message Aggregation** toggle to enable or disable (default) whether this Communication Provider supports the aggregation of multiple messages into a single message. Defaults to enabled.

3. Select the **Supports Subject Line** button to enable or disable (default) whether this Communication Provider supports the ability to include a subject line with its messages.

4. Enter the **From Address** to use for communication using SMTP Server settings if the Communication Provider supports this field. If not, leave the field blank.

5. Select **Save** on 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.

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:

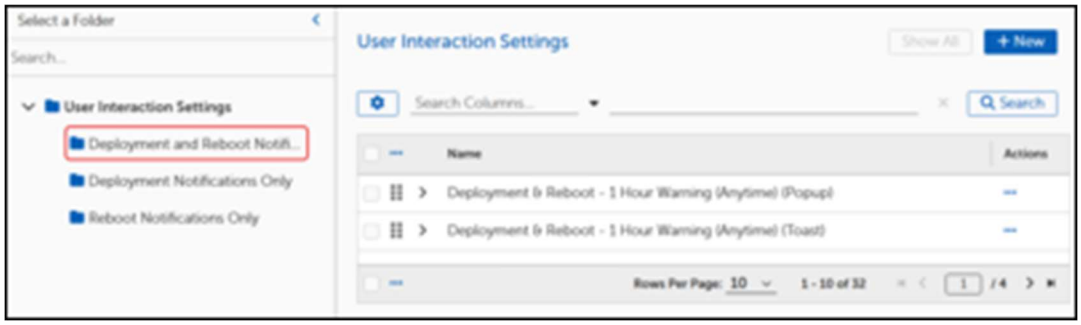
- Pre-install Notification
- Install Notification
- App Closure Notification
- Reboot Notification

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.

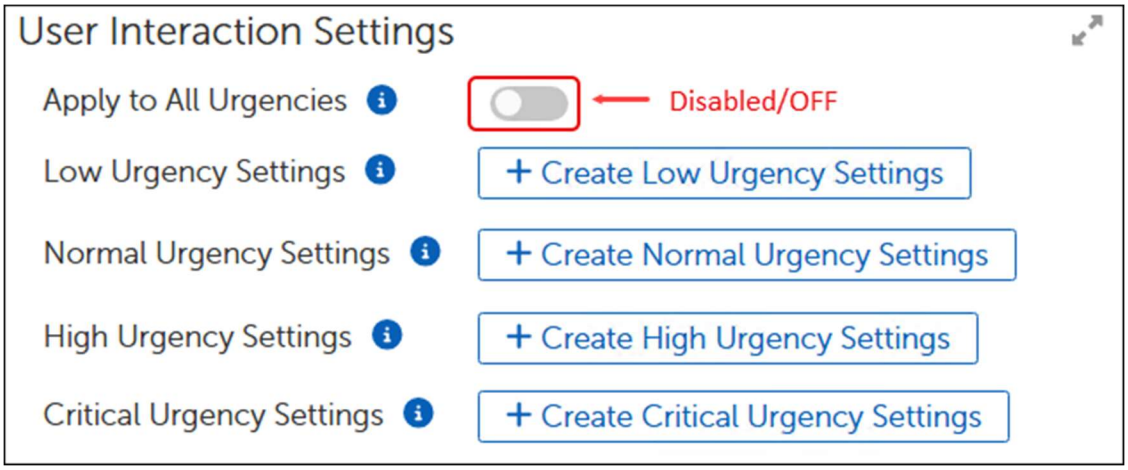
c. Enter a detailed **Description** of the process covered in this template or leave the prepopulated description. Add a character to enable the **Save** button.

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.

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.

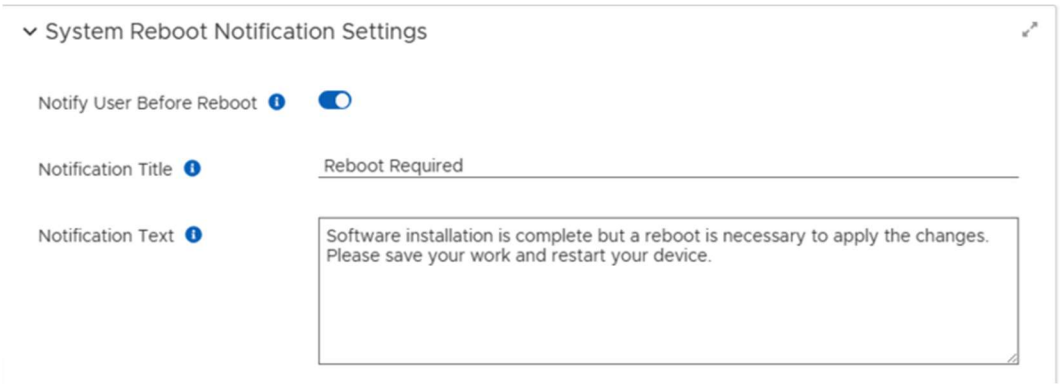
5. Create System Reboot Notification Settings.

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.

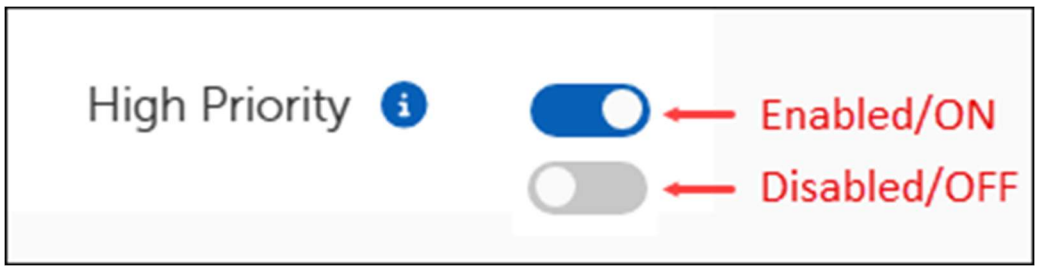
3. Enter a **Notification Title**, and then enter the **Notification Text** in the text box. This is the information the user sees when the notification arrives on the device.

4. urn:resource:component:611

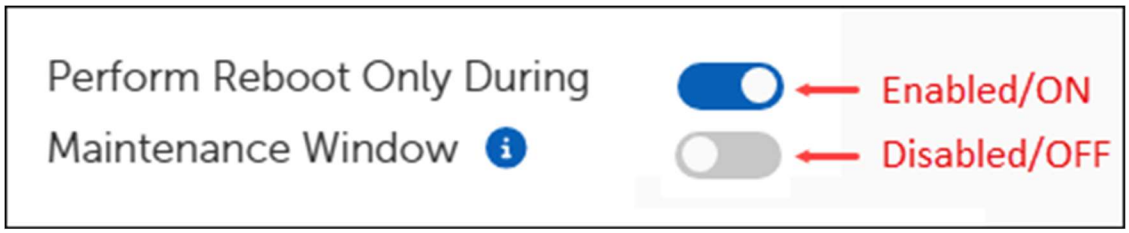
Configure Reboot Notification and Snooze Settings

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

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



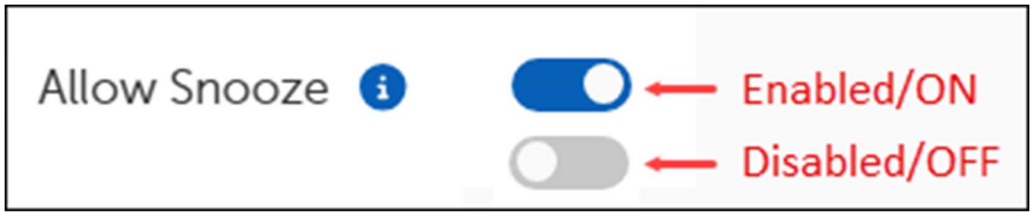
2. Select the **Perform Reboot Only During Maintenance Window** toggle to enable or disable whether reboots occur only during a maintenance window. Defaults to disabled in a new template:



3. Enter the number of **Days, Hours, Minutes, or Seconds** the user has until the reboot occurs. If zero, Tenable 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

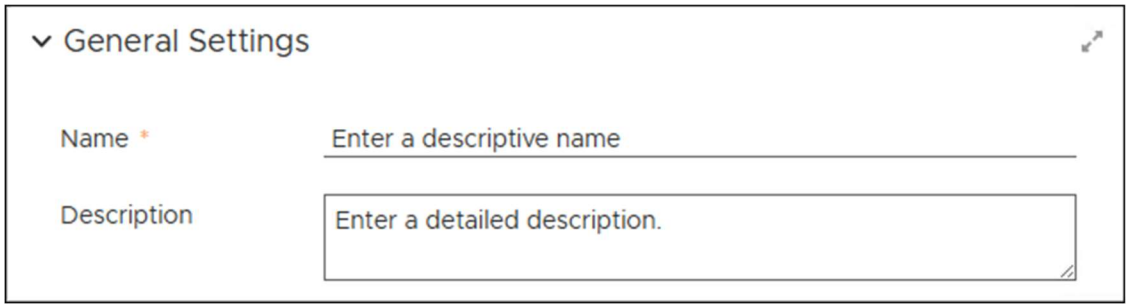
Software products and patches sometimes require user interaction when installing. Users enter details such as license information or request to show a menu at startup. Other default settings include auto update, or desktop shortcuts.

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:



   a. Enter a **Name** that identifies your template.

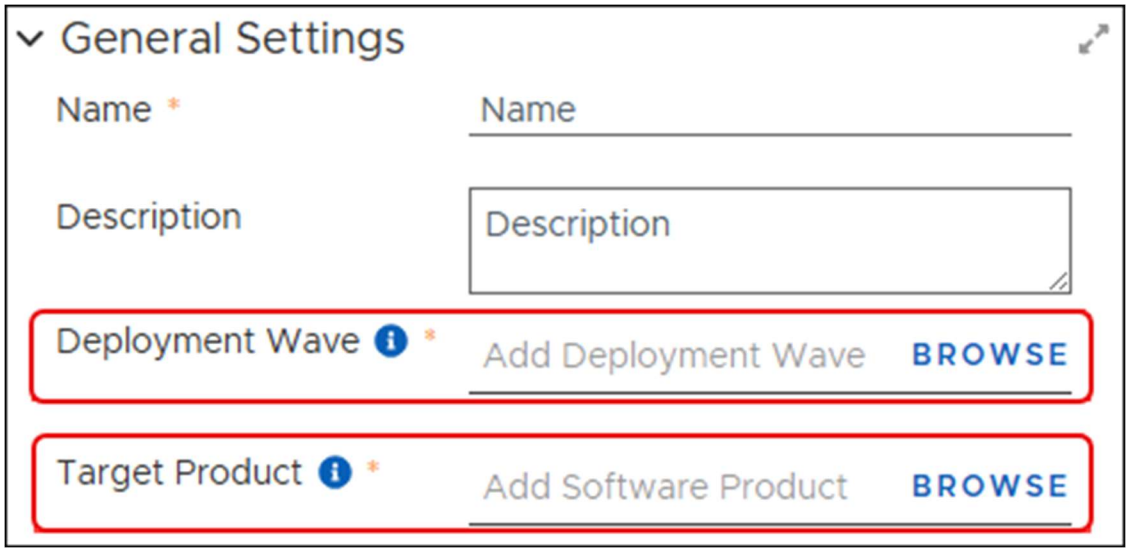
   b. Enter a detailed **Description**, and then click **Save** on the upper left corner.

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.

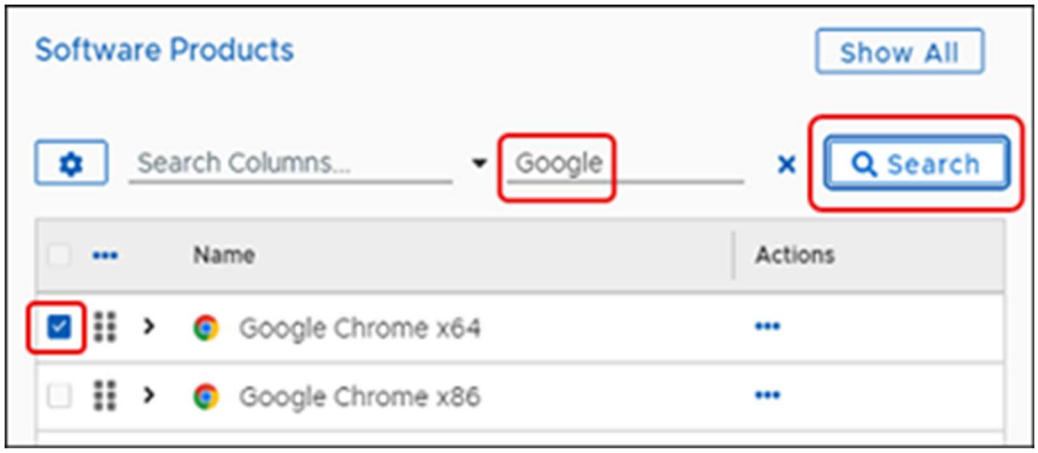
1. Select **Browse** next to **Add Deployment Wave** in an open *Customized Product Template*.



2. Select the **Deployment Wave** to which these Customized Product settings apply on the **Deployment Waves** dialog. See *Deployment Waves* for details.
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**.

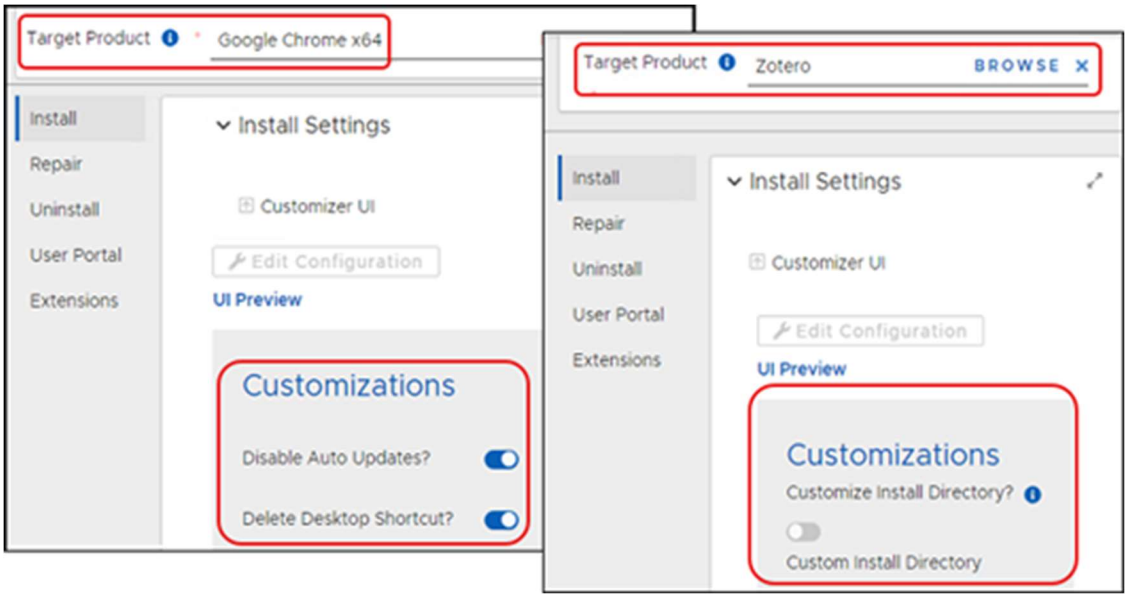


3. Select the **Software Product** you want to customize. You can target only one Software Product in each Customized Product entry.

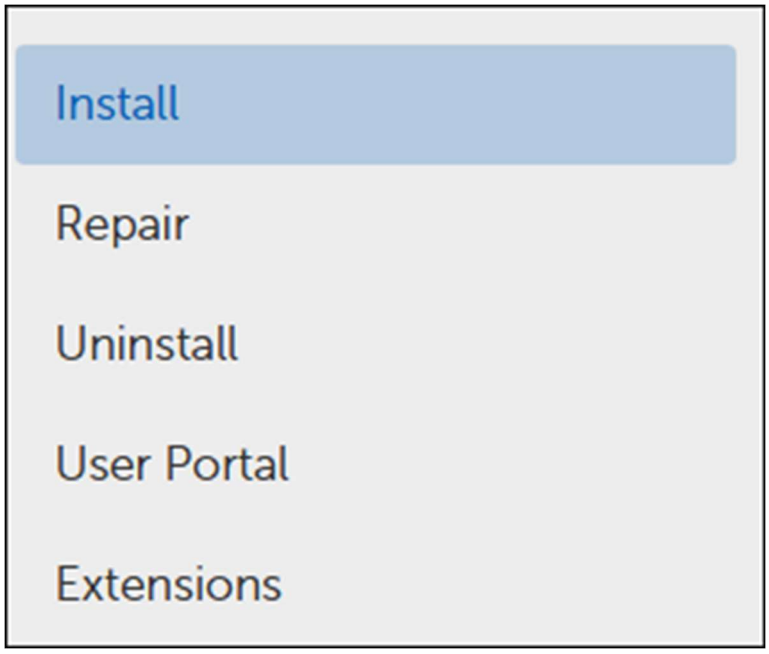
4. Select **Add Software Product** to populate the configurable items in the static list of **Install Settings**. Settings change depending on the Target Product.
5. Select **Save** in the upper-left corner of the template to save your changes.
6. Continue with Configure Software Install Settings.

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.

Patch Content

When patch activity occurs, the information associated with a given Patch Strategy appears in a table under Patch Content. A table entry includes information about the patch based on the patch content ID.

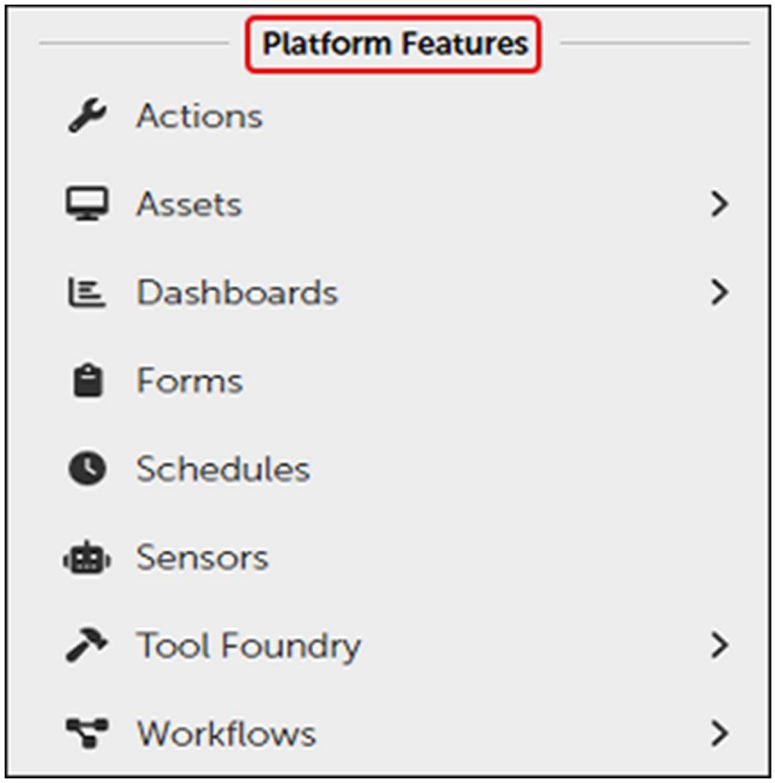
Select **Content Name** in the table to view the patch details. Information provided in the individual report includes Patch ID, Version, Content Size, Publication Status, and Content Details.

Patching Schedules

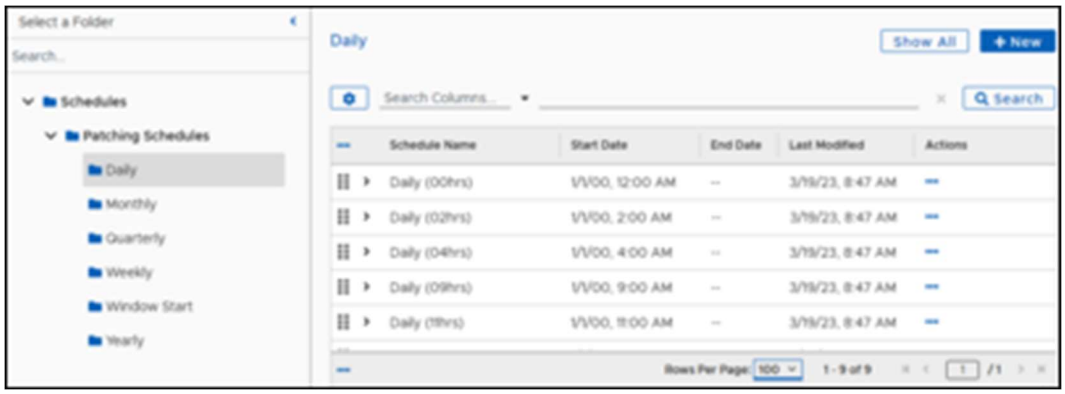
Tenable Patch Management uses schedules throughout the product to automate patching processes that include content push, updating custom groups, setting maintenance windows, and more. Tenable provides several default schedules you can customize for your environment, or you can create new schedules.

View Available Schedules

1. Select **Schedules** in the **Platform Features** menu of the *Tenable Patch Management Enterprise Dashboard*.



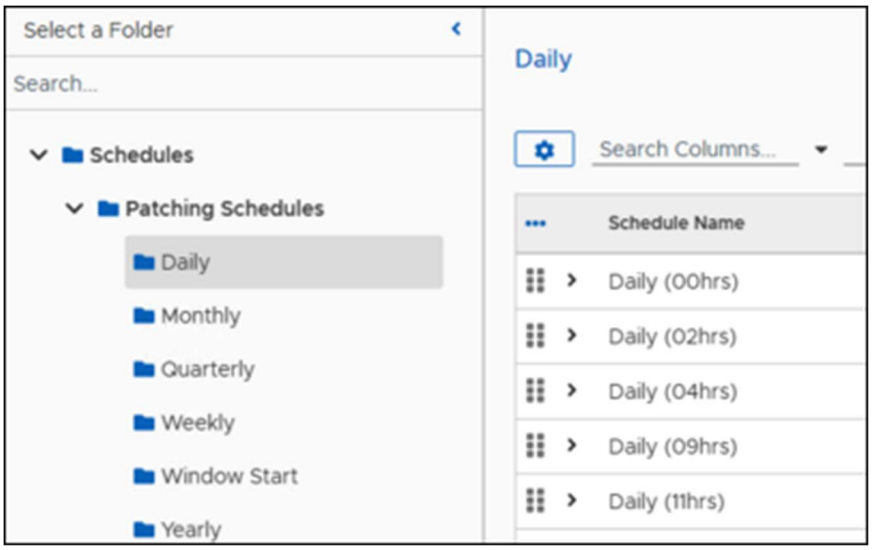
This opens the list of available schedules.



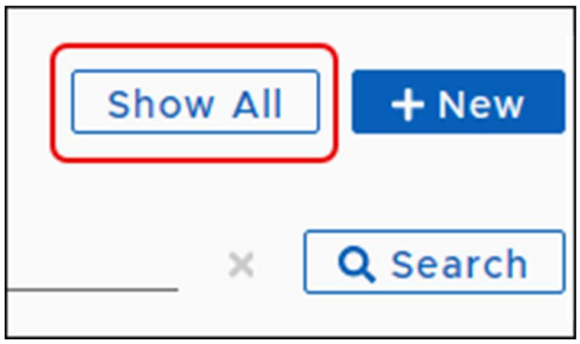
2. Choose how you want to view schedules:

    a. Select one of the **Patching Schedule** folders listed in the left navigation pane. These choices list the available schedules for each category.

    b. Select the **Schedule Name** to open it and view the details.



3. Select **Show All** at the upper right to view all available schedules. This list contains over 100 available schedules.

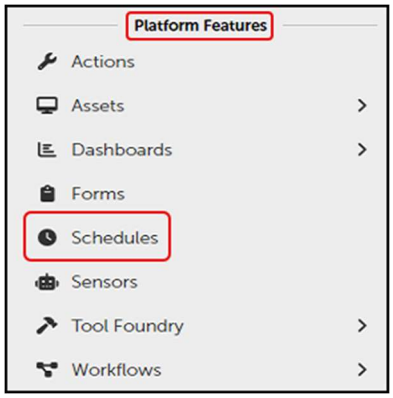


Create a Custom Schedule

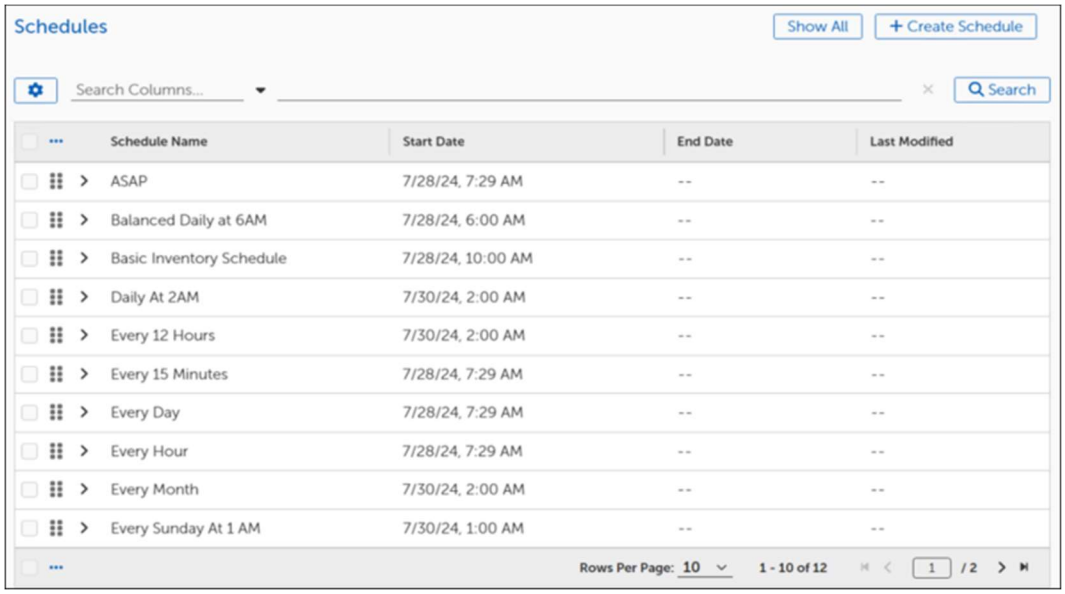
This example customizes an existing schedule template. You can also create a new schedule template under **+ New**. The template layout for either includes the same choices and fields.

Open and Save a Schedule Template

1. Select **Schedules** in the **Platform Features** menu of the *Tenable Patch Management Dashboard*.



This opens the list of available schedules.



2. Select a **Schedule Name** from the table to open that scheduling 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.

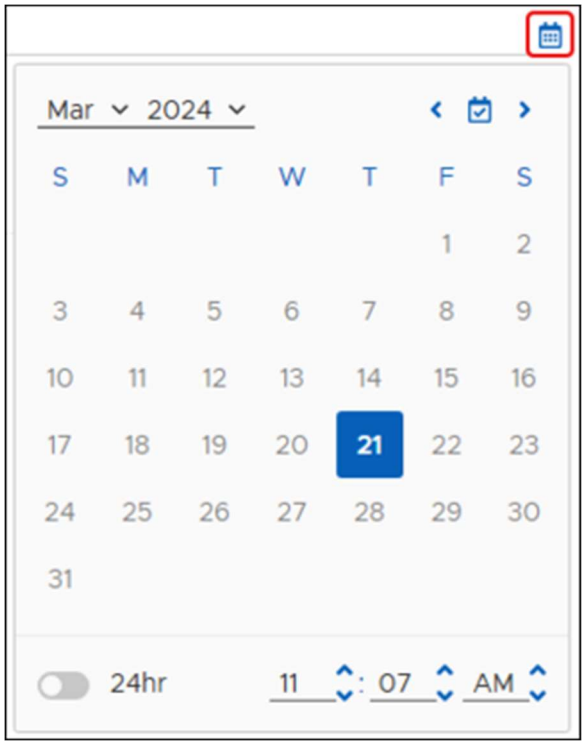
Create Schedule Settings

1. Scroll down to **Schedule Settings** in an open schedule template.

2. Select the **Use Server Timezone** toggle to enable or disable using the time zone of the Tenable server running this schedule.

Set Start Time (Required) and End Time (Optional)

1. Select the **calendar icon** to the right of Start Time to choose the starting day and time for the schedule.



2. Navigate through the open calendar to change the start day and time:

    a. Select the **calendar icon** with the check mark to move to the current day and time, and then use the left and right arrows to change the month.

    b. Select a **month** using the down arrow next to the month.

    c. Select any **date** in the calendar to select that day.

    d. Select the **24hr** toggle to display the time using the 24 hour clock.

    e. Select a **year** using the down arrow next to the year.

    f. Change the **start time** for the schedule using the up and down arrows next to the time settings.

3. Select the **Enable End Time** toggle to enable or disable setting an end time.

Set Repeat and Recurrence Intervals

Select a **Schedule Repeat** setting from the list. Options include the following:

Non-Recurring

- **ASAP:** Run the process immediately using this schedule. One time only.
- **Not Recurring:** Run the process on the set schedule one time only.

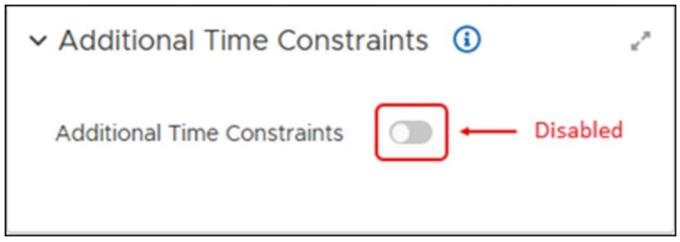
Recurring

- **Recurring Interval:** Set the number of recurrences and whether they repeat by Minute (up to 60), Hours (up to 24), or Days (up to 100).
- **Recurring By Day:** Set the schedule to run one or more days per week, or to run the schedule every day.
- **Recurring By Week:** Run the schedule on a specific day of the week and set the schedule to run again on the same day for up to 127 weeks.
- **Recurring Monthly by Date:** Run the schedule on a specific day of the month and set the schedule to run again on the same day every month (up to 127).
- **Recurring Monthly By Last Day:** Run the schedule on the last day of the month and set the schedule to run for one or more months (up to 127).
- **Recurring Monthly By Day of Week:** Choose whether to run the schedule on a specific day of the week every month, a specific week of any month (up to 4), or run the schedule during the last week of the month. Set the Recurring Interval in Months (up to 127).

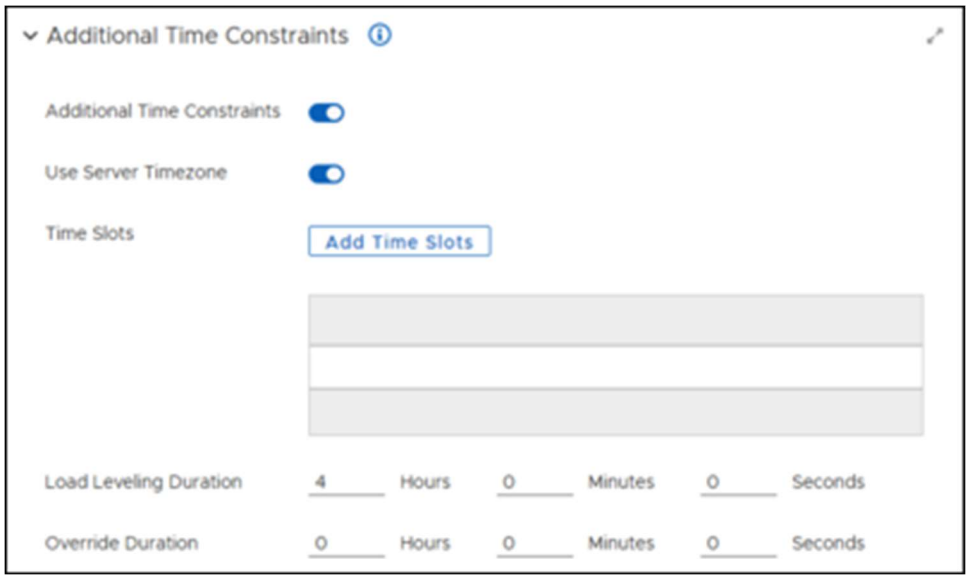
Set Additional Time Constraints

Configuring a constraint means that the schedule settings in this template run only within the time range provided in this constraint.

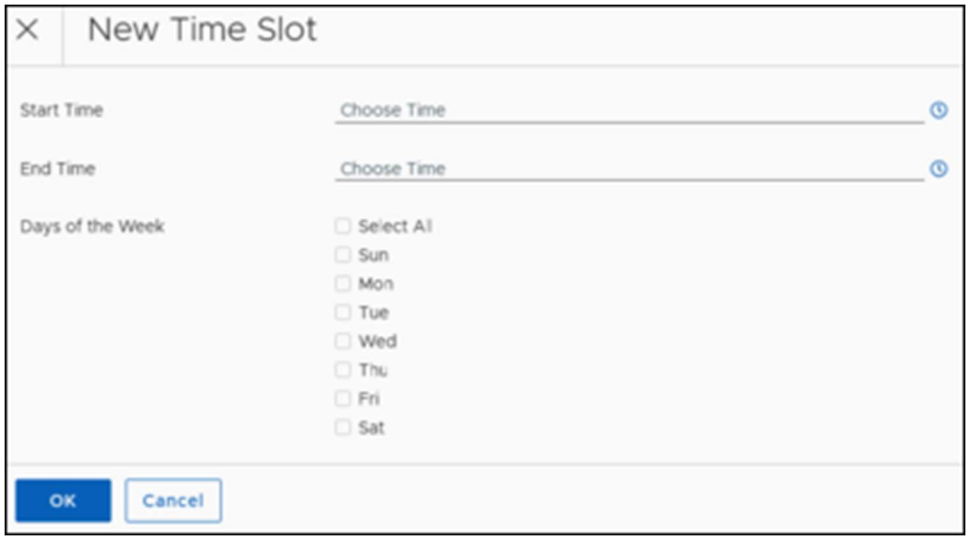
1. Scroll down to **Schedule Settings** in an *open schedule template*.
2. Select the **Additional Time Constraints** toggle to enable or disable their use.



3. Select the **Use Server Timezone** toggle to enable or disable using the timezone of the Tenable Server running the schedule.



4. Select **Add Time Slots** to define a time slot for this schedule. This opens the New Time Slot dialog.



5. Enter a **Start Time** and an **End Time** in the specified field or click the clock icon to customize the clock and time settings for each field.

6. Select **OK** to save the settings and return to the **Additional Time Constraints** configuration.

Set Load Leveling Duration

Set the Load Leveling Duration in days, hours, or minutes. Tenable Patch Management balances the target of list of devices using this schedule across the time interval you set here.

Set Override Duration

Set the Override Duration in days, hours, or minutes. When the Override Duration expires, schedules start immediately.

Deploy Schedules

After saving the changes to the schedule template, you must deploy it. Deploying the schedule makes it available for use in any object that requires selecting a schedule.

1. Select **Deploy** or click **Save & Deploy** in an open Schedule template.
2. Verify that **Deployment Status** shows **Deployed**, and then click **Back to Schedules** or select another object from the left navigation menu of the dashboard.

Delete a Schedule

If you have created a schedule that you no longer need, you can delete it from the list of schedules. You cannot delete any schedules provided by Tenable.

1. Select **Schedules** in the **Platform Features** menu of the *Tenable Patch Management Dashboard*.
2. Set **Rows Per Page** at the bottom right to a larger number to see all available schedules, and then scroll down the table to the schedule you want to delete.
3. Enter a search term on the search line, and then click **Search**.
4. Locate the schedule you want to delete:
    a. Select the **ellipsis (...)** under **Actions** for the schedule you want to delete.
    b. Select **Delete** from the list.
5. When prompted, click **OK** to delete the schedule. You may not undo this action.

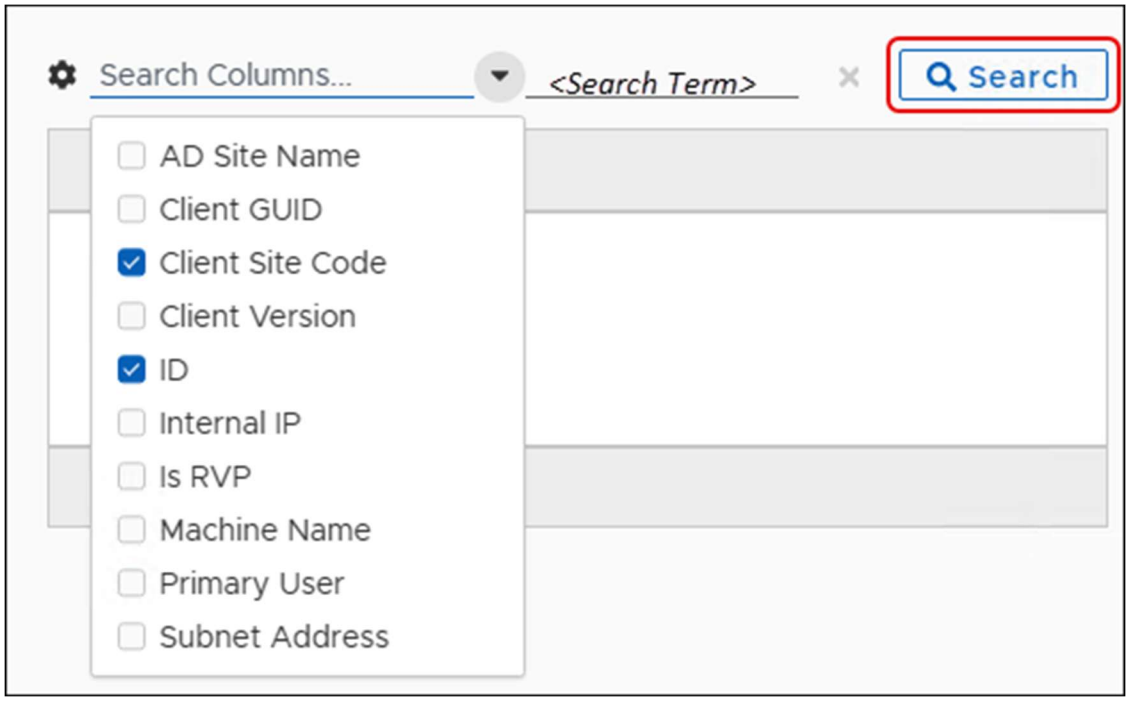
Patching Analytics Dashboards

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

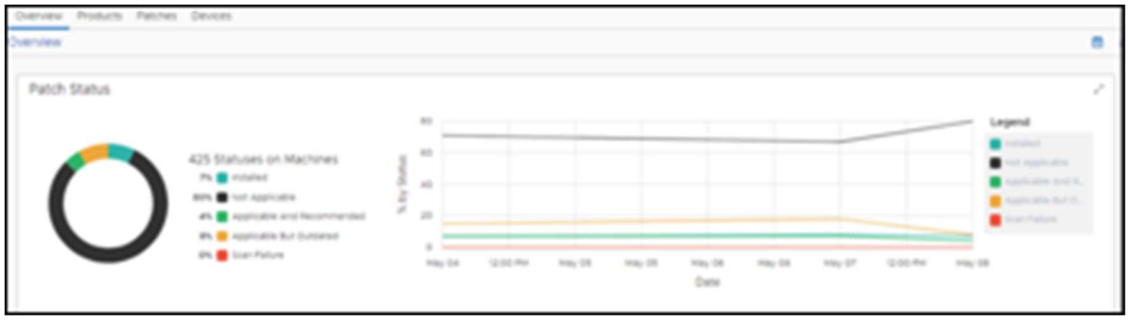
For tables in any dashboard view, the drop-down list next to **Search** allows you choose a column to search within. This provides several options for searching depending on the search term you have selected. Column choices change depending on the menu object.



Patching Analytics Overview

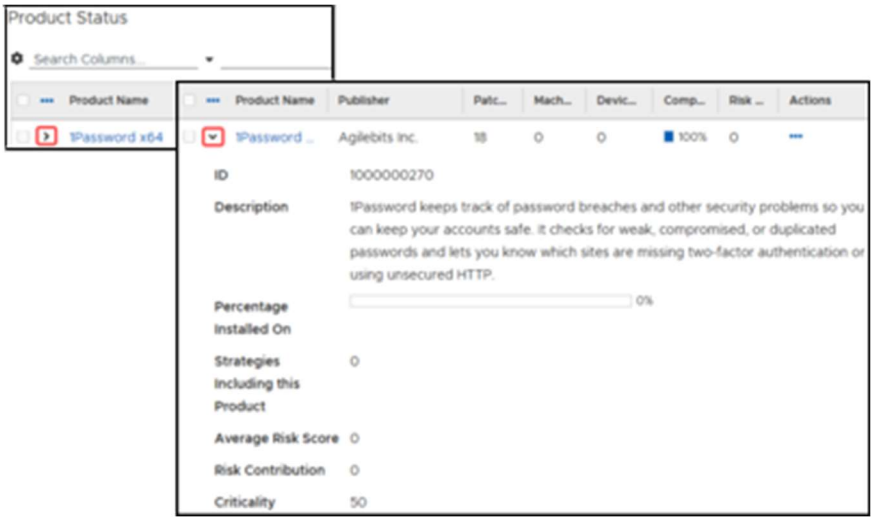
The **Overview** summarizes the state of all patches in the environment. This view includes Patch Status and Product Status widgets.

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.

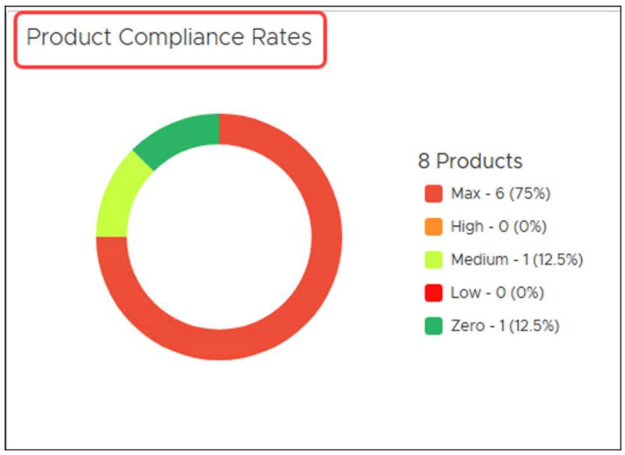


Products View

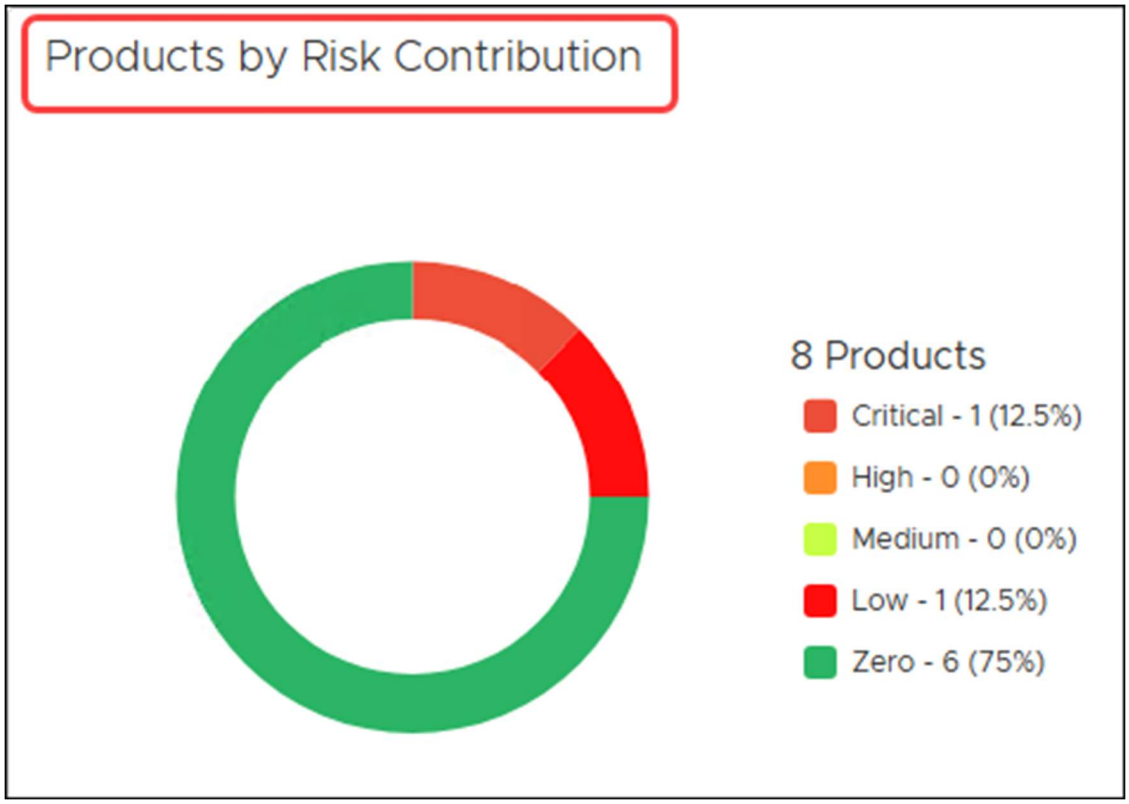
The **Products** view summarizes information from the product perspective.

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.



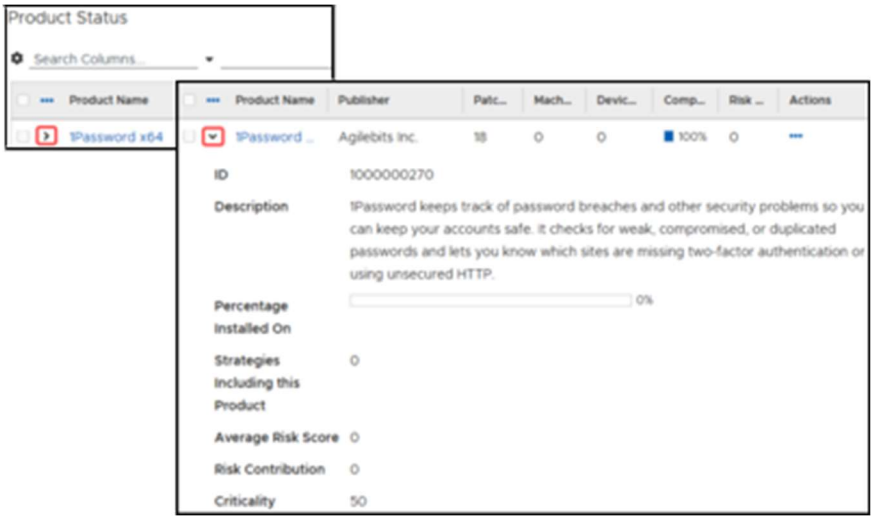
Risk Contribution shows the number of products in the environment and the risk rates (Critical, High, Medium, Low, Zero) by percentage. The chart tracks risk levels over time.



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 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.



Patches View

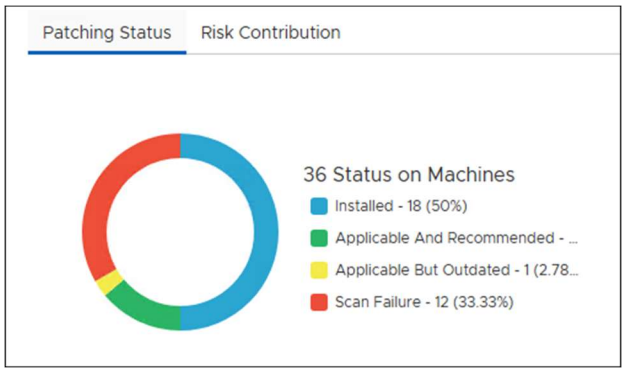
The **Patches** view summarizes information from the patch perspective.

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

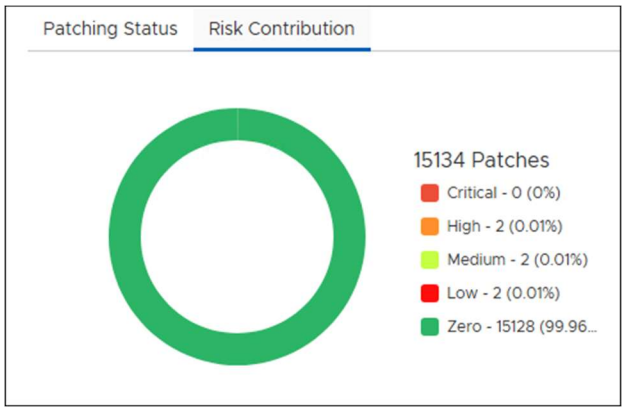
Active Product Deployments provides the number of patches undergoing installation and the percentage of completion**.**

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

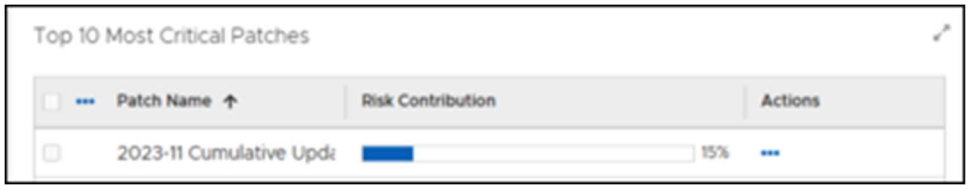
Patching Status shows the status of all patches, the number of machines tracked in the environment, and the number of patches in each status (Installed, Applicable and Recommended, Applicable but Outdated, Scan Failure) by percentage. The chart shows patching status over time.



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.

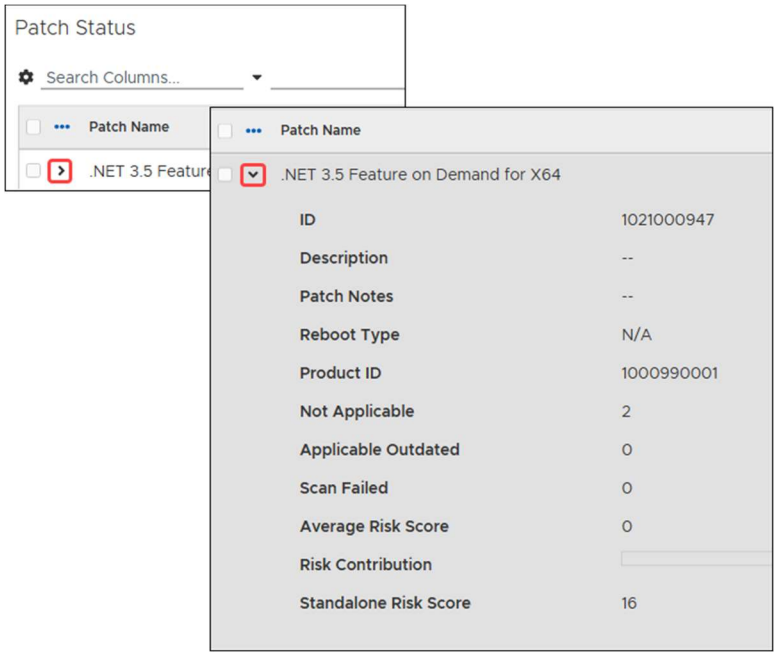


Top 10 Most Critical Patches tracks the risk contribution of the top ten most critical patches in the environment.



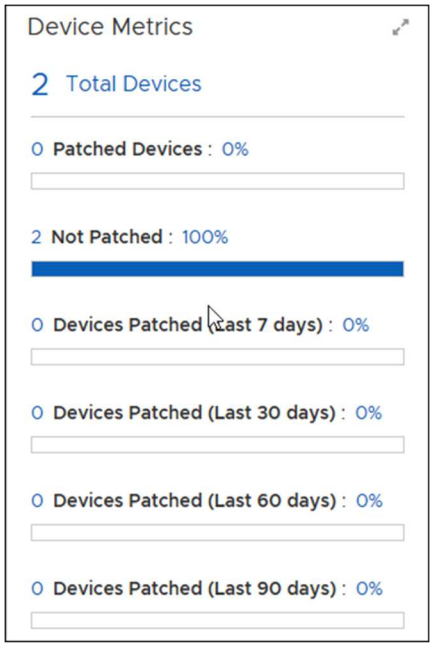
Patch Status is a table that lists each patch that Tenable Patch Management looks for during a scan, the installation/applicability status of each, and the status, compliance, and Risk Score for each.

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

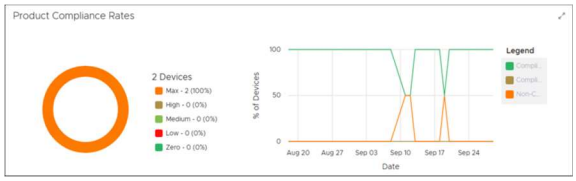


Devices View

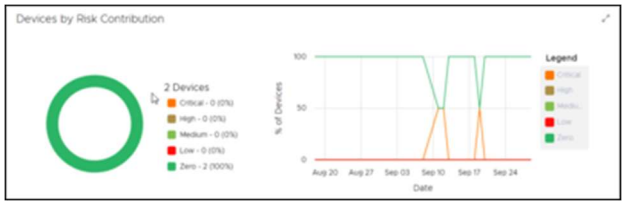
The **Device Metrics** widget shows the total number of devices in the environment, the percentage of patched and unpatched devices, and the percentage of devices patched in the last 7-, 30-, 60-, and 90-days.



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.

Blocklisting	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 Blocklisting.
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. See Cycle Operations.
Exceptions	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 Patching Exceptions.
Global Pause	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 Global Pause.
Rollbacks	Create a Rollback object to rollback one or more patches to a system determined or specified version. See Rollbacks.

Blocklisting

includes an extra level of protection for customer devices and patching processes called Blocklisting. The Tenable metadata team, as always, 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 Tenable metadata 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

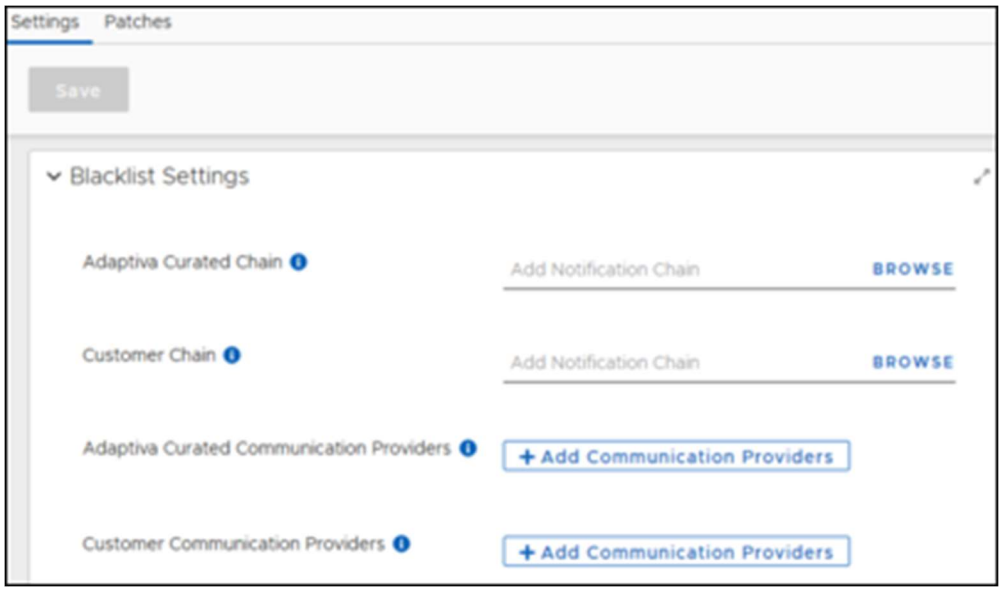
Set categories of notification by selecting a Notification Chain to use when Tenable blocklists a patch/release. Select the same or different Notification Chain to notify administrators when you blocklist a patch or a release. You can also select specific communication providers for either category of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

View Blocklist Settings

Blocklist Settings include notification details for blocklisted patches including Notification Chains and Communication Providers. You can use the Tenable 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, Tenable 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, 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**.

   Expand the **Blocklisted Patches** folder, and then select either the **Tenable** folder or the **Customer** folder to view blocklisted patches.

   This displays the list of Tenable Blocklisted Patches.

3. 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

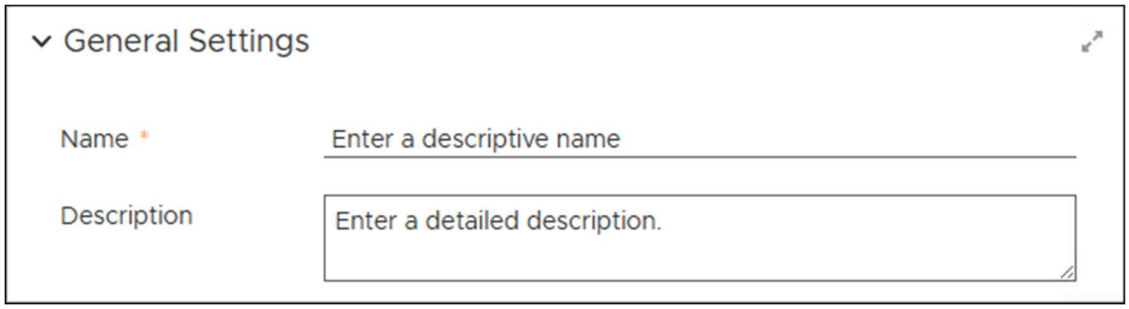
   Enabling customer suppression means you expressly choose to ignore this blocklist recommendation from the Tenable metadata team.
3. Select **Save**, and then click **<-- Back** at the upper left to return to the list of blocklisted patches.

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.

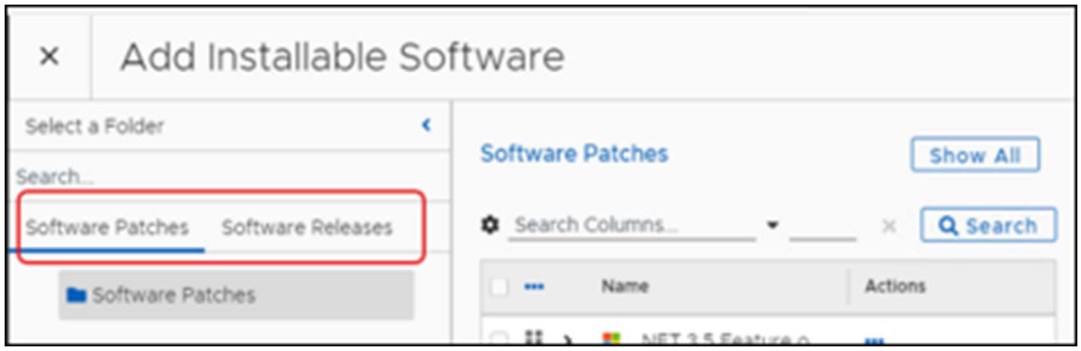
4. Enter a **Name** and **Description** for the patch you intend to blocklist.



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).

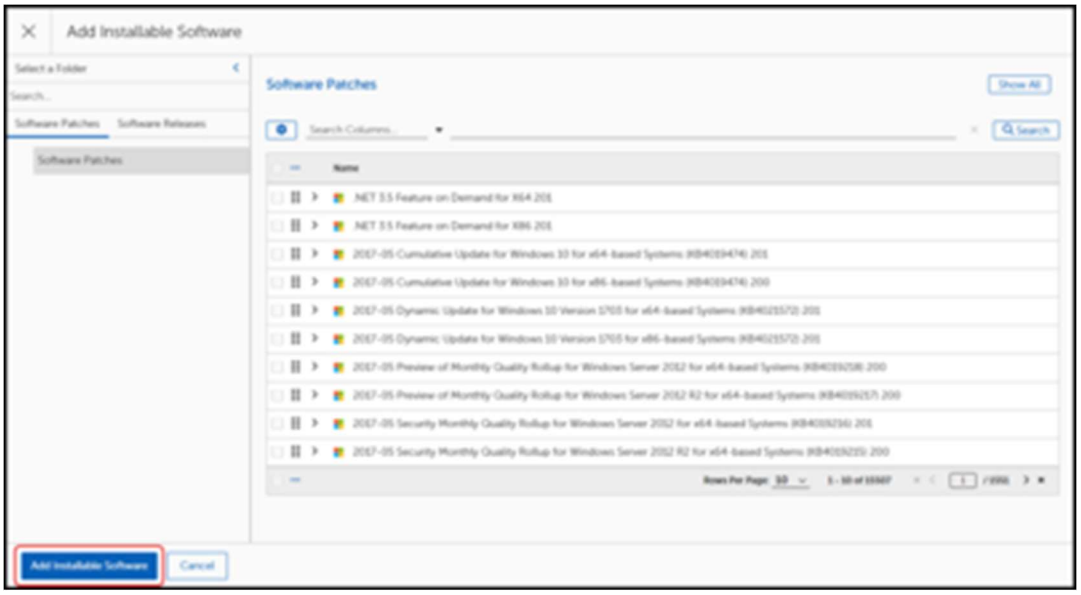
   This opens the **Add Installable Software** dialog with a list of all available software or patches.



   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.

2. Select the **Name** of the patch to blocklist, and then click **Add Installable Software** at the bottom left of the dialog.
3. 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.

4. 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.

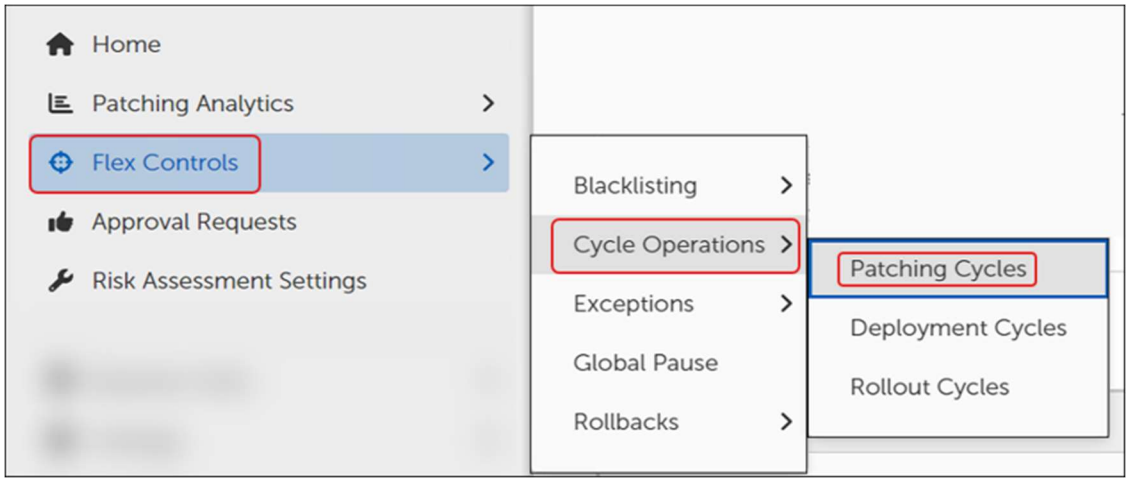
- **Cycle Logs**: Display events relating to the Patch Process. For instance, the Cycle Operation Logs can show the administrator who manually started a Patch Cycle and at what time.

Patching Cycles

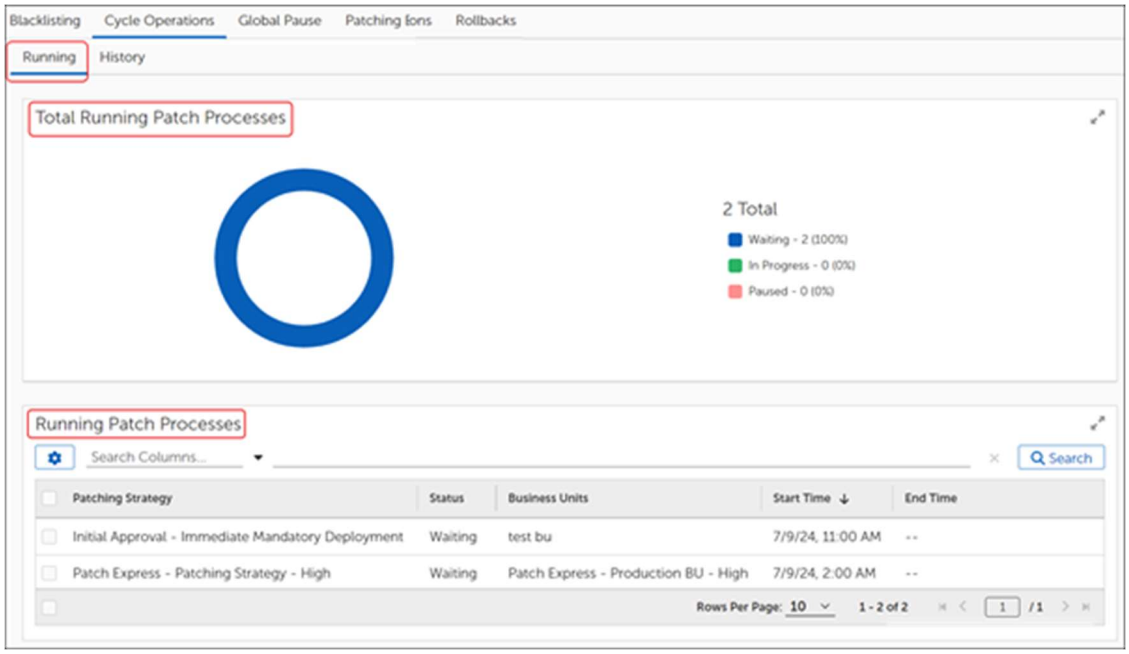
This dashboard shows information about the active Patch Processes in the environment. Patch Processes represent the workflow that models and performs the defined patching routine. As part of the overall Patching Strategy, Patch Deployment Bots use configured criteria to identify patches that apply to 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**.



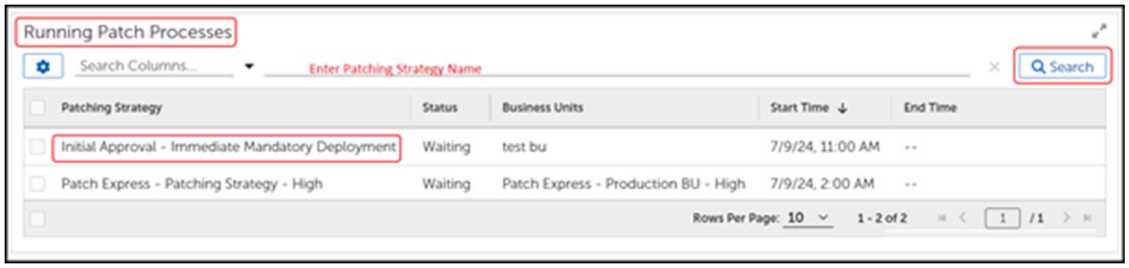
This opens to the **Running** tab of the Patching Cycles workspace:



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.

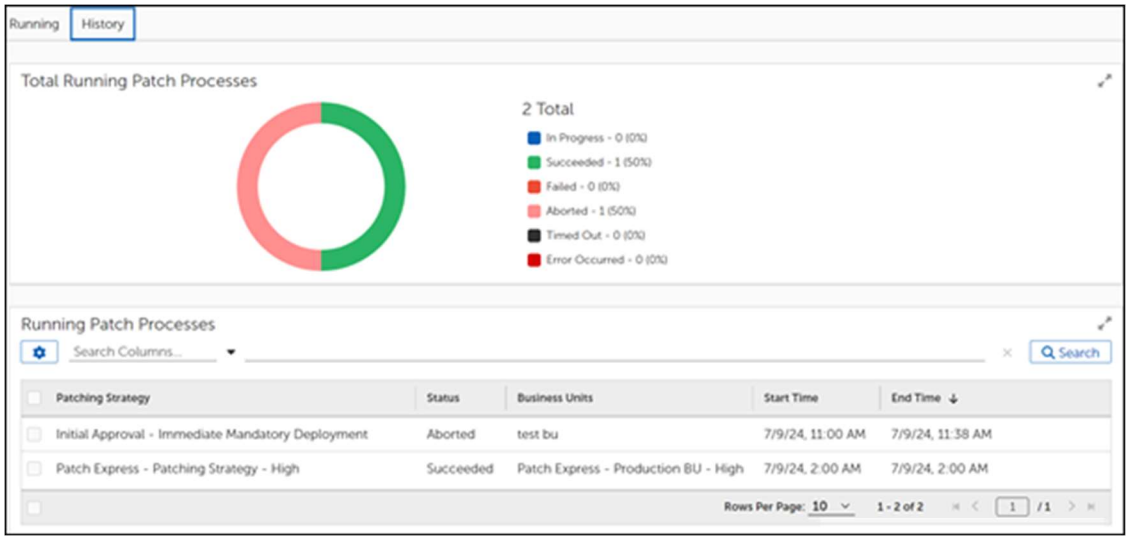
2. Enter a **Patching Strategy** name on the search bar above the **Running Patch Processes** table, and then click **Search**.



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**.

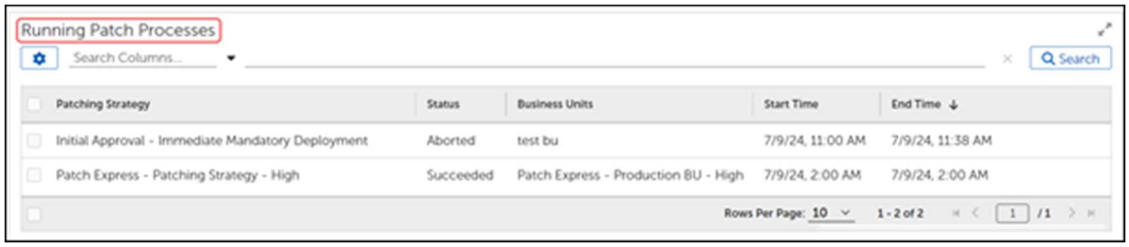


2. Select **History** on the upper left to change to the **History** tab:

    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**.



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

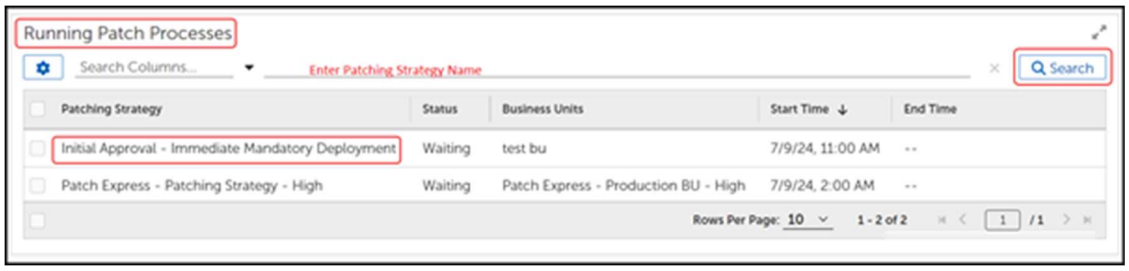
1. Mouse over or click **Flex Controls** in the **Home** menu, and then select **Cycle Operations > Deployment Cycles**.

    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**.



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

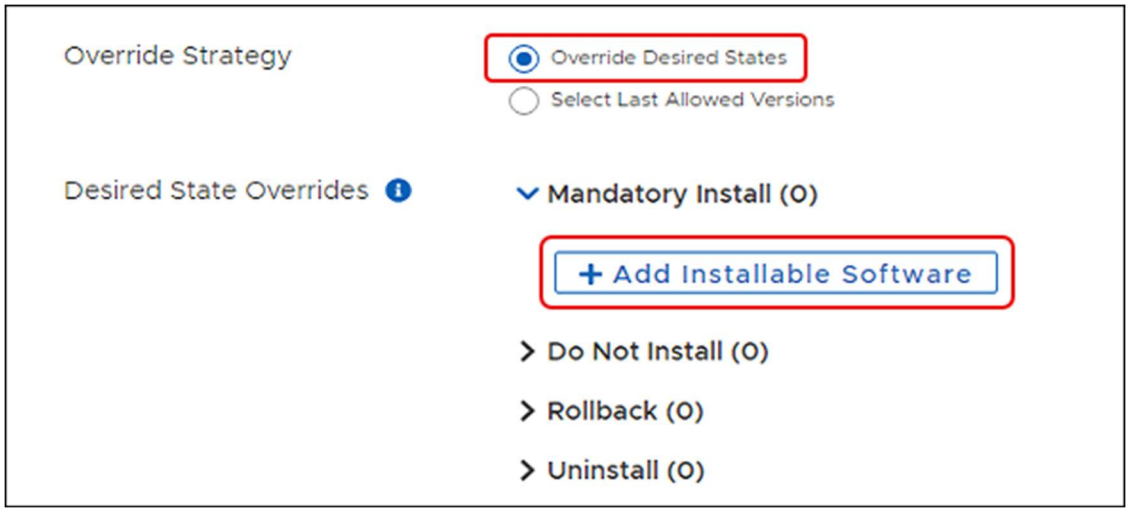
1. Select **Flex Controls** from the Home menu, and then select **Exceptions > Patches**.
2. Select **+ New** on the upper-right corner to open a Patching Exception template.
3. Name and describe the exception:
    a. Enter a descriptive Name for this exception in the **Name** field.
    b. Enter a detailed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



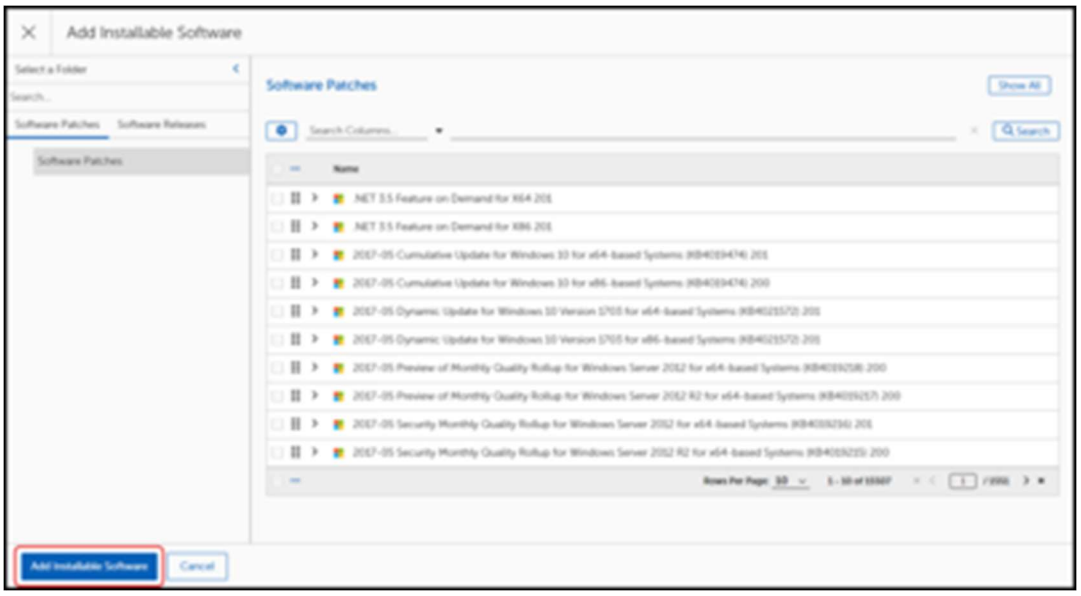
2. Select the type of **Desired State Override** , such as Mandatory Install, and then click **+Add Installable Software** for that state.

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.

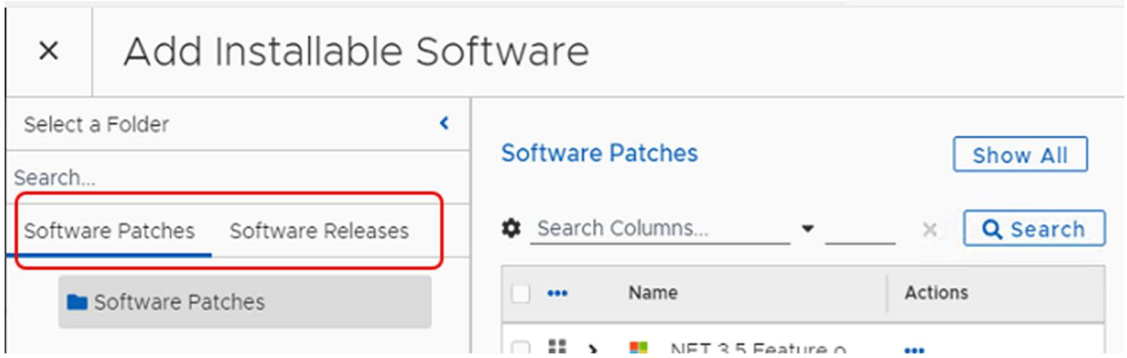
   b. Choose one of the methods below to search for a patch or release:



      - 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:

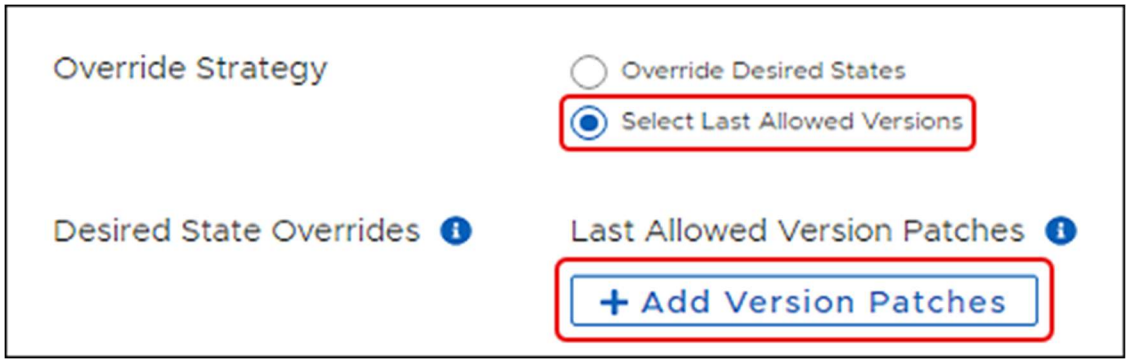
   a. Check the **Error View** and resolve any errors.

   b. Select **Save** again if you make any changes.

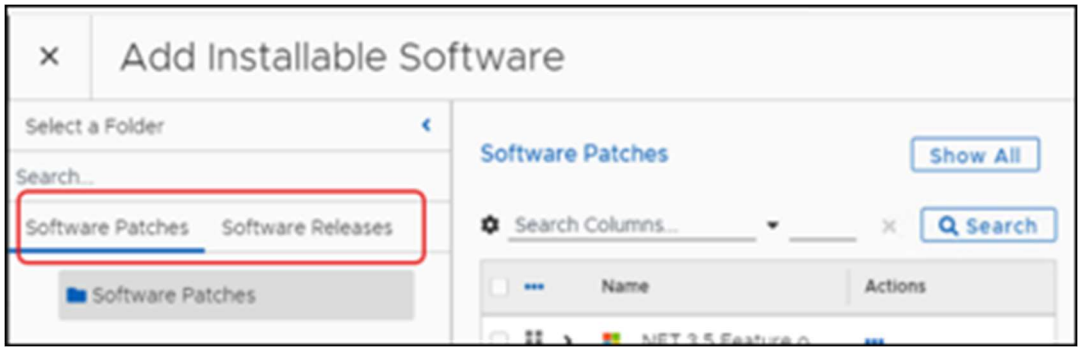
6. Continue to **Add Target Business Units**.

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.

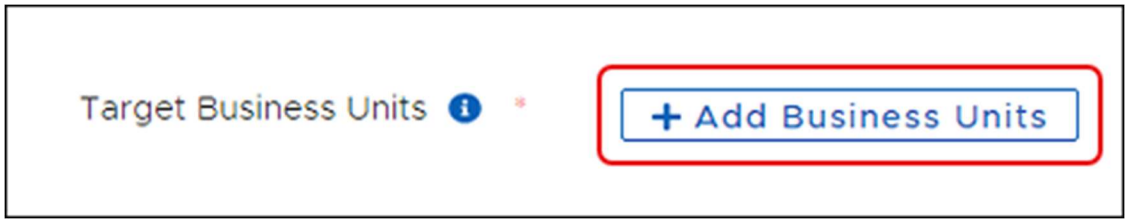


3. Select the **Search** field, and then enter the release name of the product you want to override:
    a. Select **Search**.
    b. Select one or more products for the patch exception. You may add items from both **Software Patches** and **Software Releases** tab.
    c. Select **Add Version Patches**.
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**.

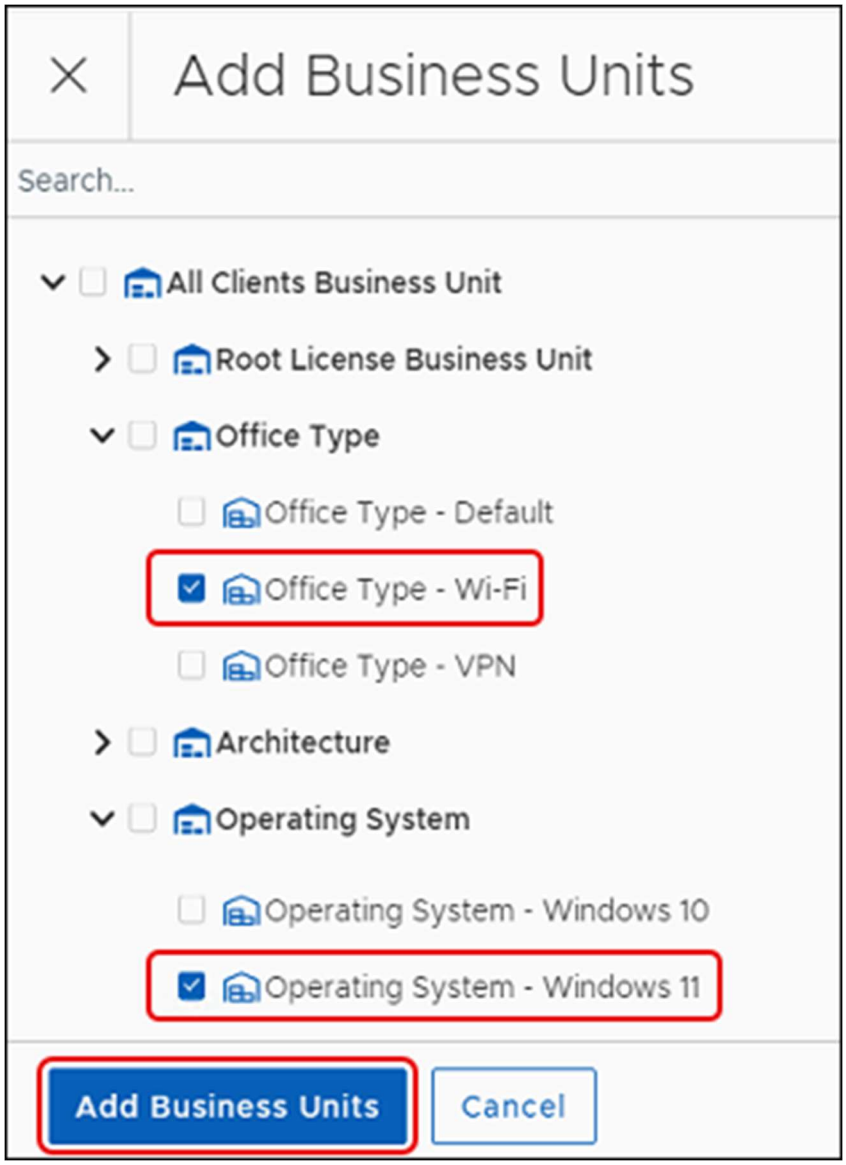
Add Target Business Units for Patch Exceptions

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.

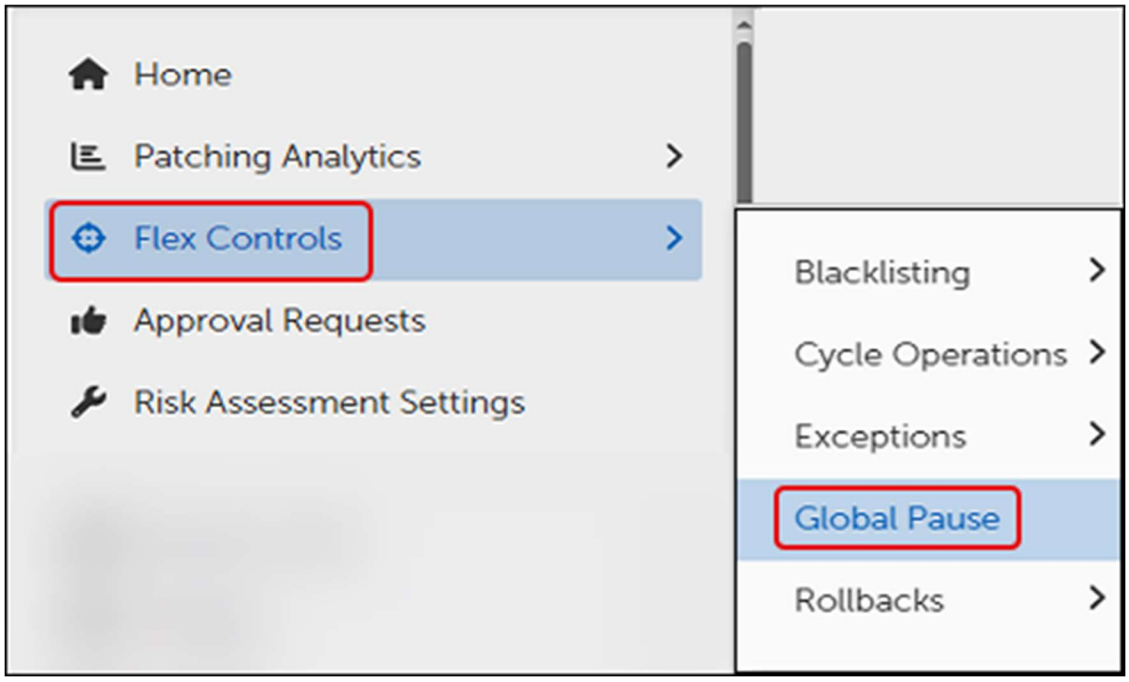
Paused Cycles: Pause Patching, Deployment, or Rollout Cycles either for specified Business Units or for the Business Units already targeted by the Cycle.

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

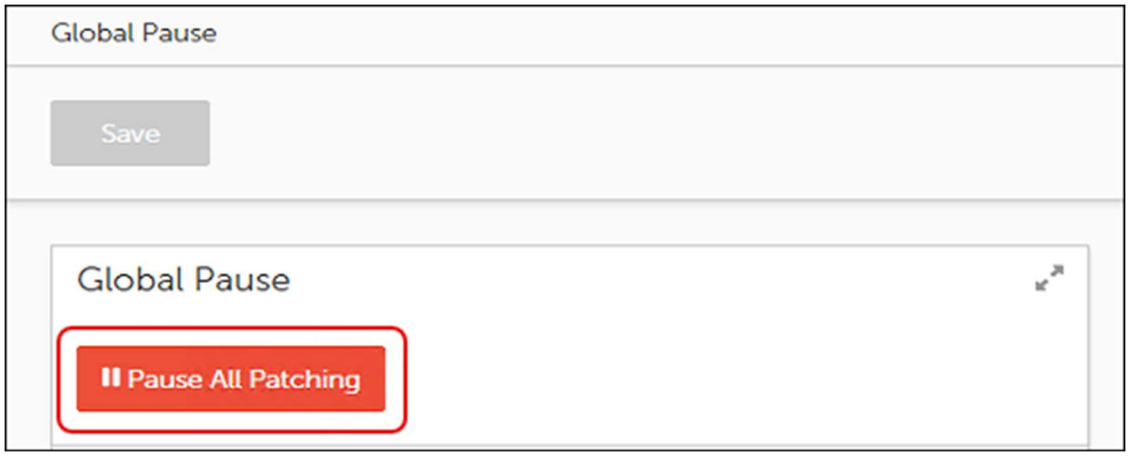
Stop All Patching Activity Immediately

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

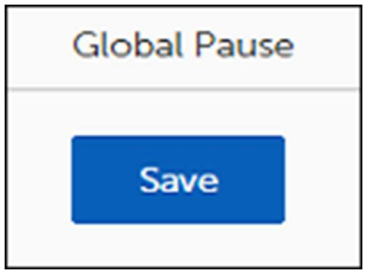
1. Select **Flex Controls** on the Home menu, and then select **Global Pause**.



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:

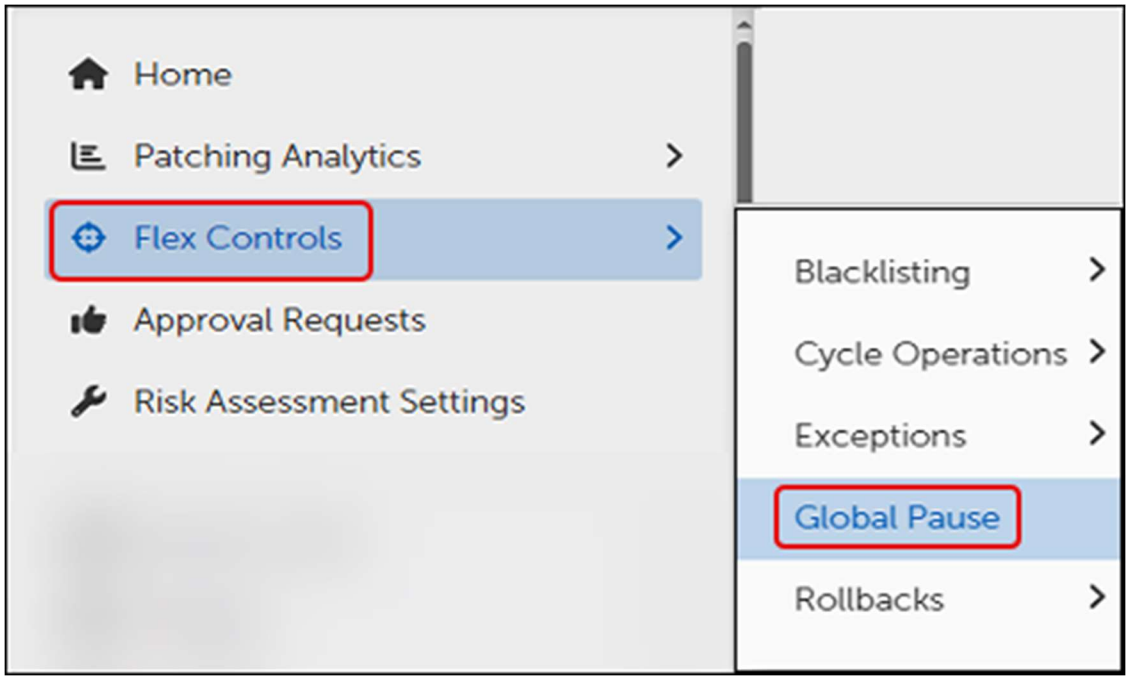
    c. All patch deployments in progress that have not reached an irreversible state are paused immediately.

    d. All newly initiated patch deployments are paused automatically.

Resume All Paused Patching Activity Immediately

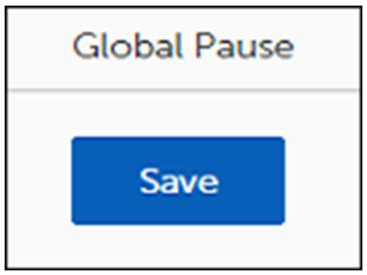
To resume all paused patching activity on all licensed clients, use the following steps to revoke a Global Pause.

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



This opens the **Global Pause** dialog:

2. Select **Resume Patching**.

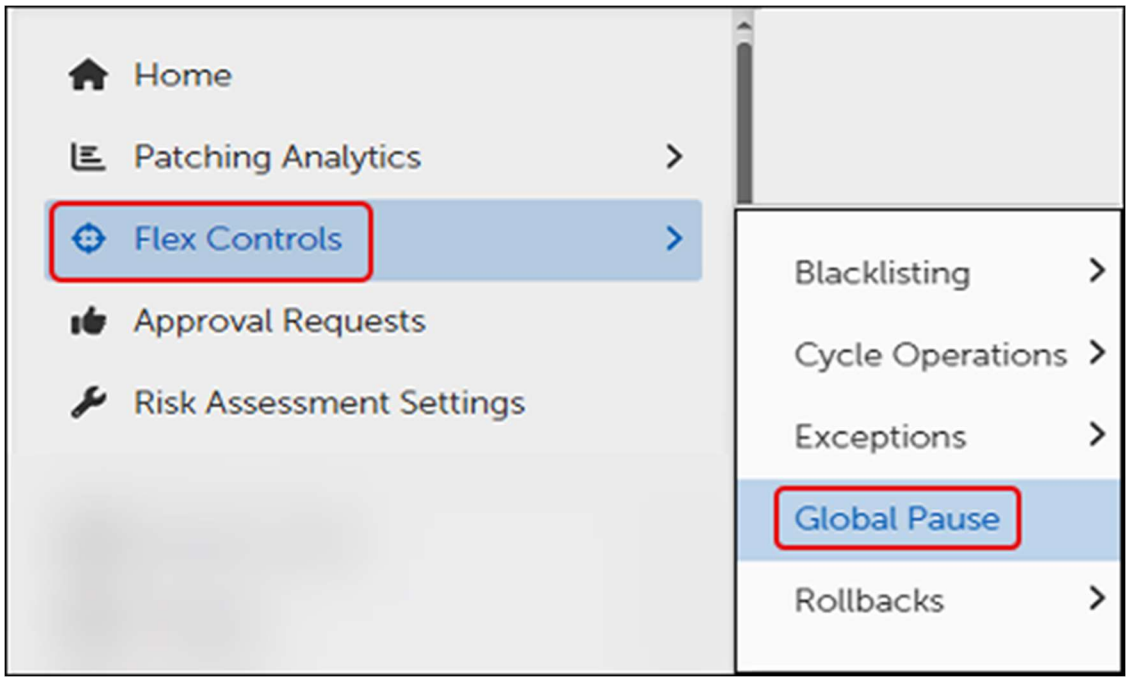


3. Select **Save** to revoke the Global Pause. This immediately revokes the Global Pause and allows patching activity to occur as configured.

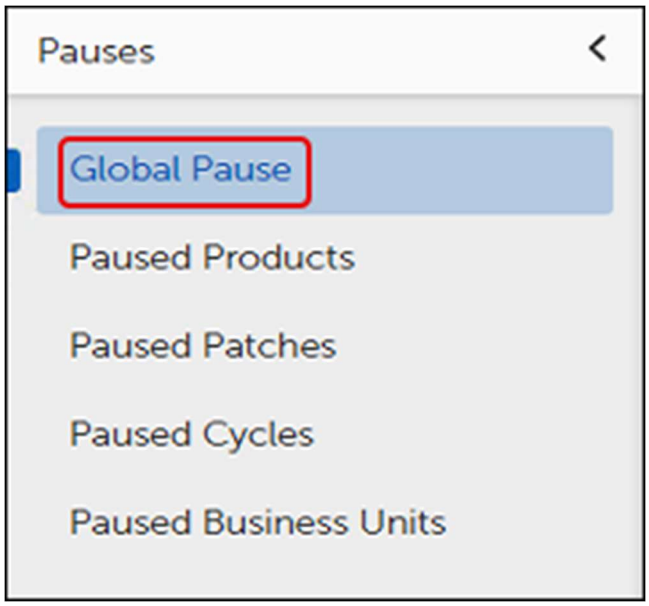
Pause Patching for Specific Objects

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.

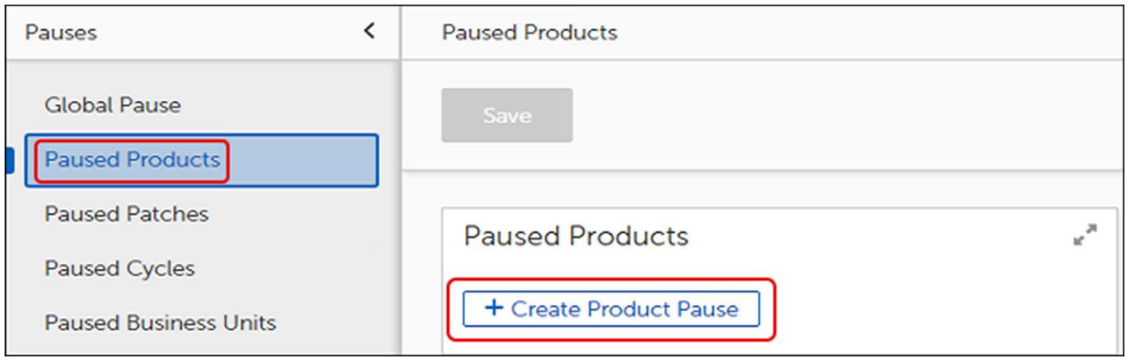
e. **Pause Business Units**: Pause patch deployments for one or more Business Units.

Pause Deployment of a Specific Software Product

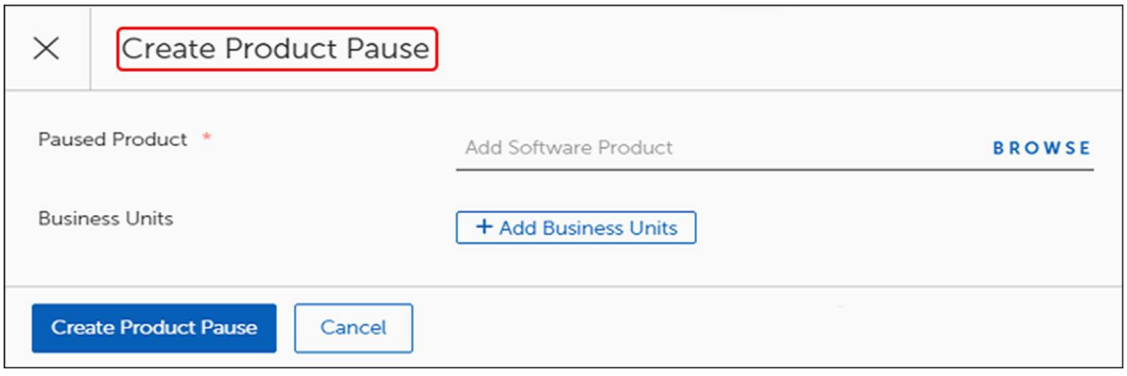
To stop patching activity for specific software products or patches, complete the following steps:

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

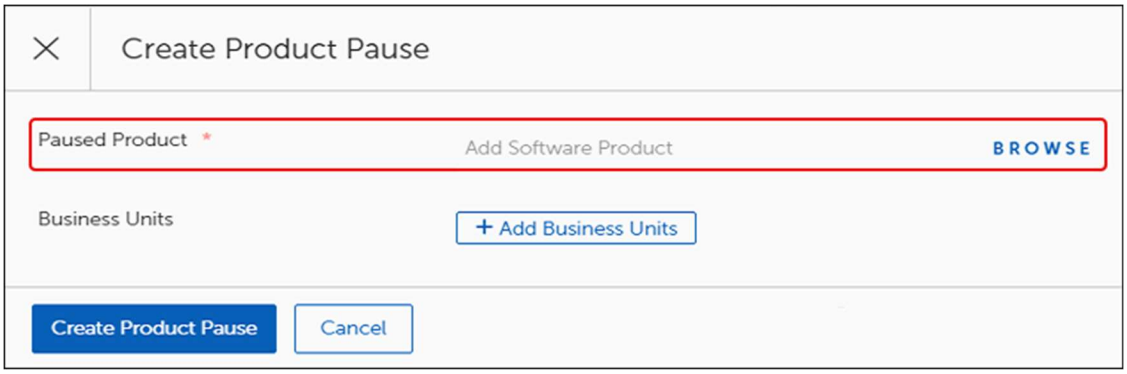
   This opens the Paused Products dialog:



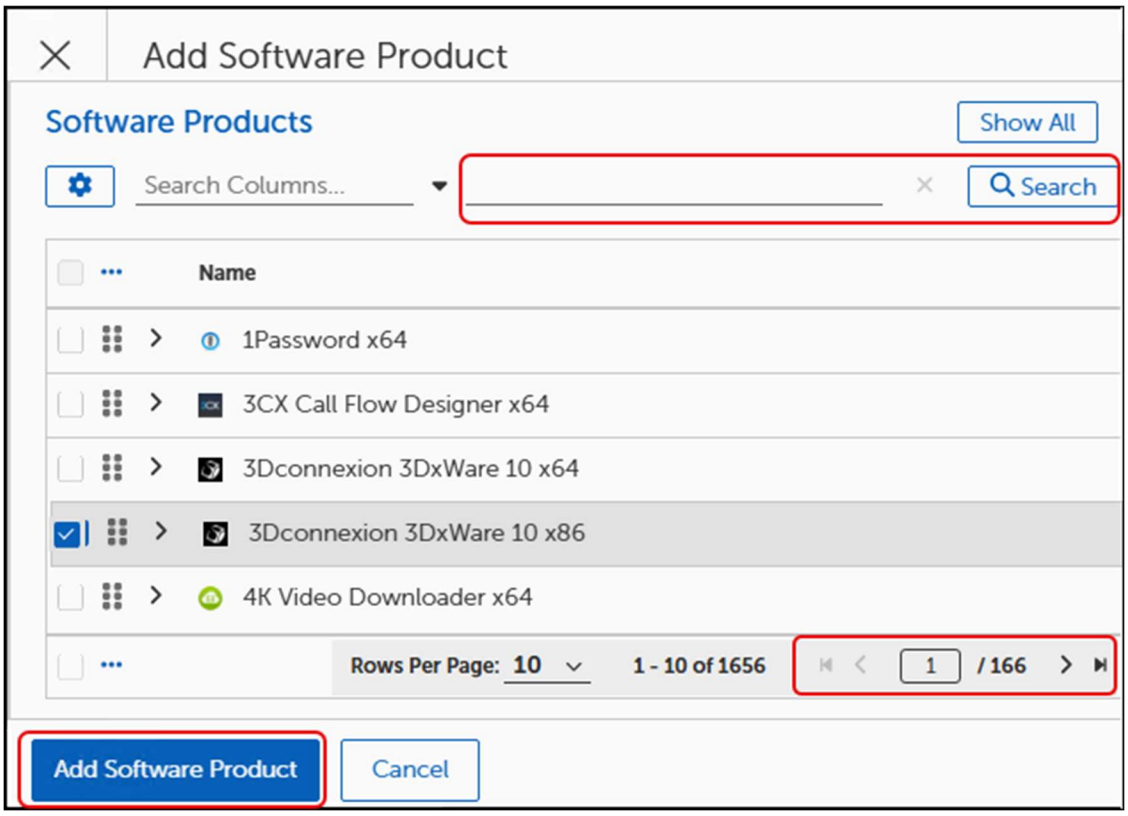
   a. Select **+Create Product Pause** to open the **Create Product Pause** dialog:



   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**.

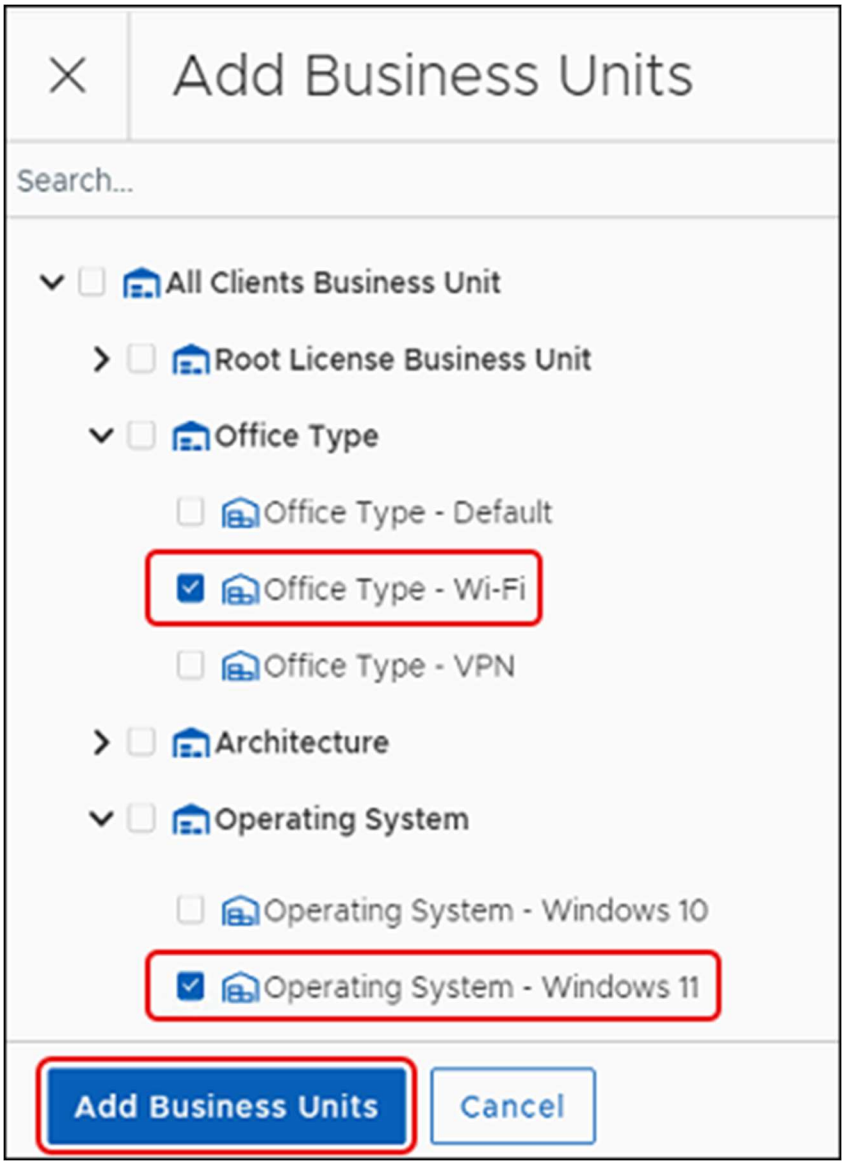
3. Add or remove **Business Units**:

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**.

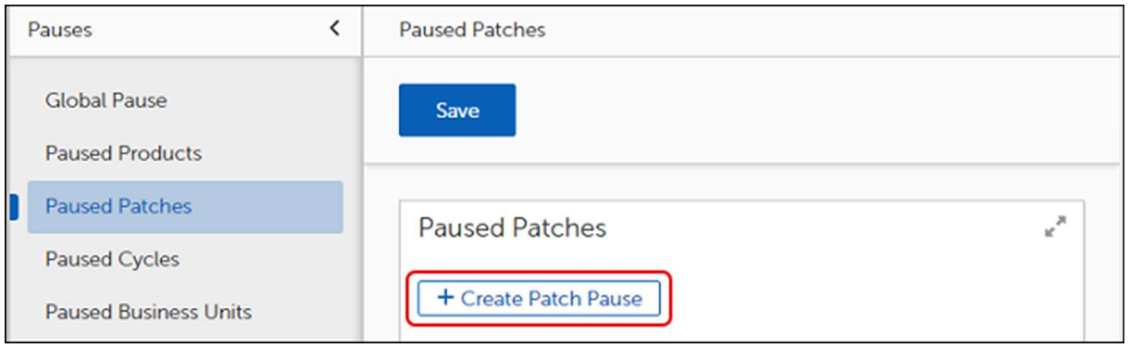
4. Select **Create Product Pause** and then click **Save** to create a global pause for the selected products.

Pause Deployment of a Specific Patch

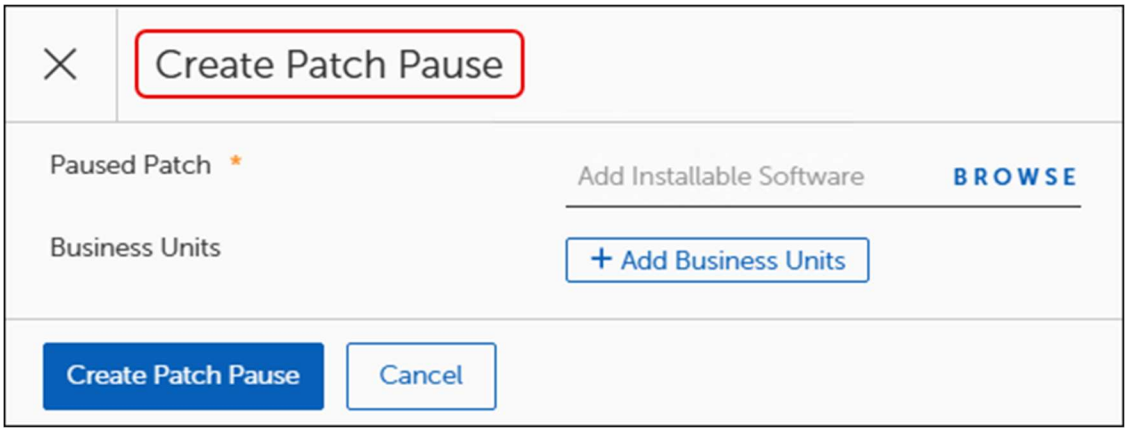
To stop patching activity for a specific patch, complete the following steps:

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

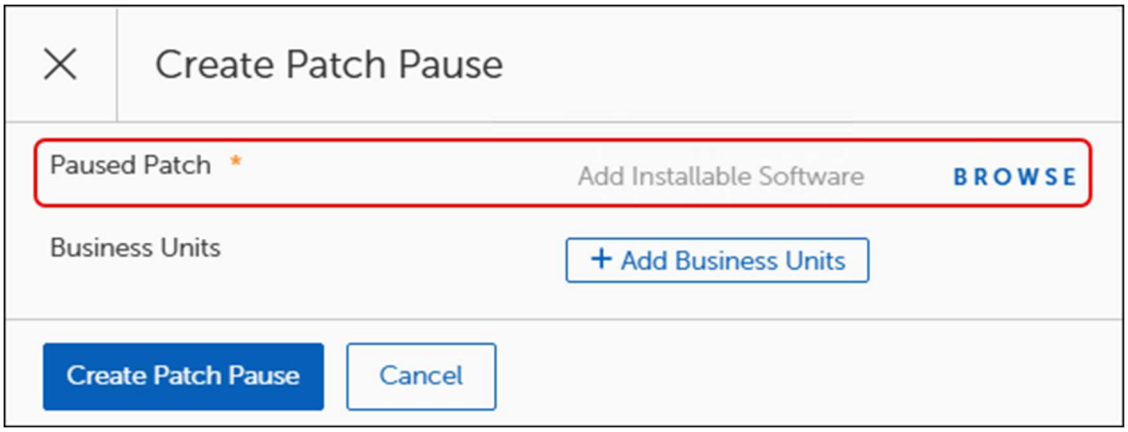
   This opens the Paused Patches dialog:



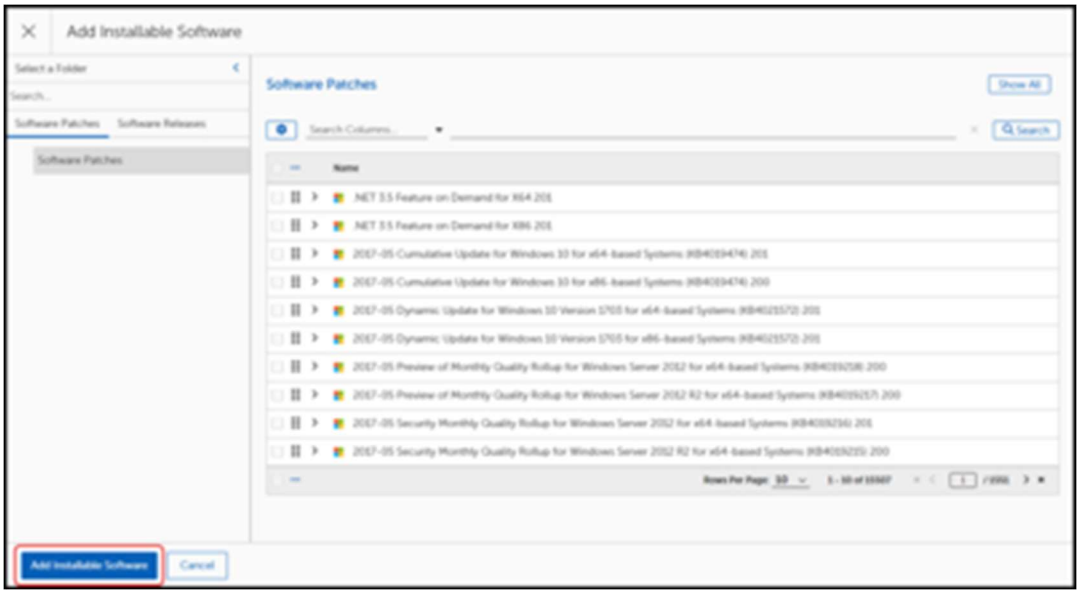
a. Select **+Create Patch Pause** to open the **Create Product Pause** dialog, and then select Browse to find the Software patch you want to pause:



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**.

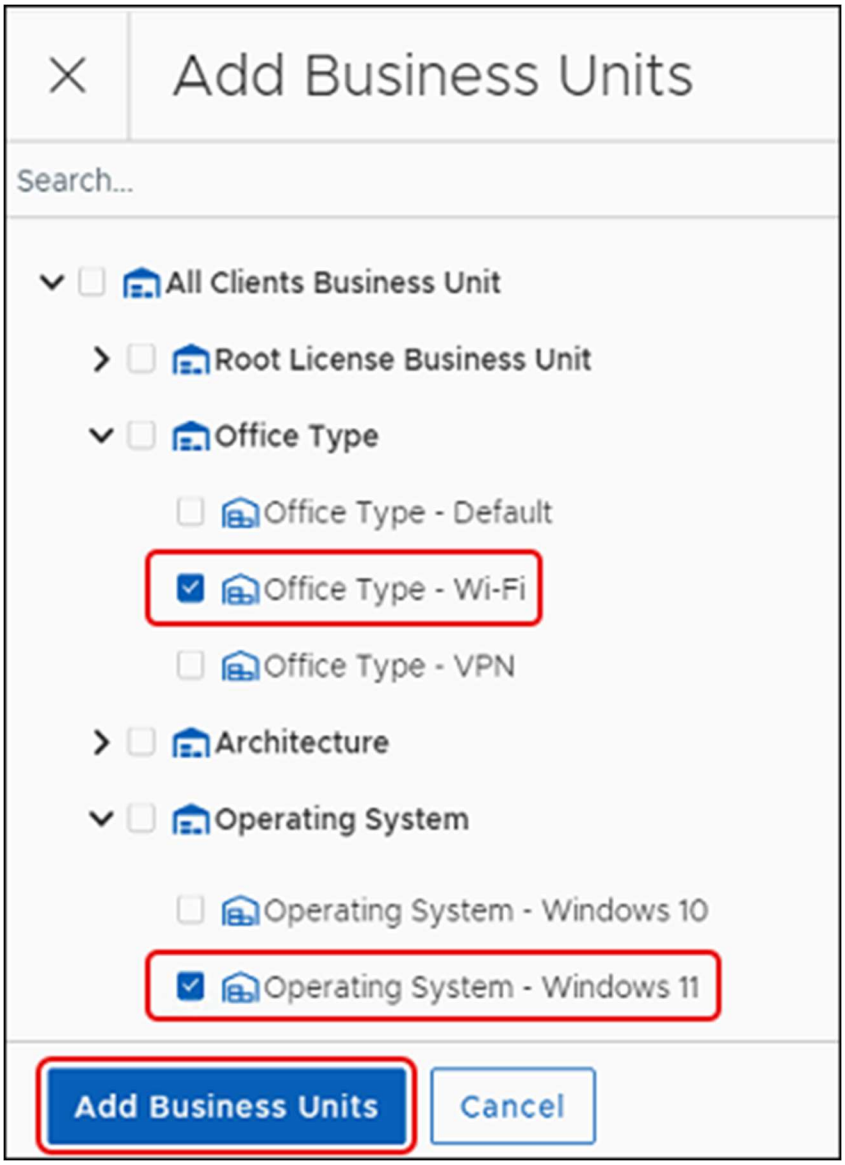
3. Add or remove **Business Units**:

    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

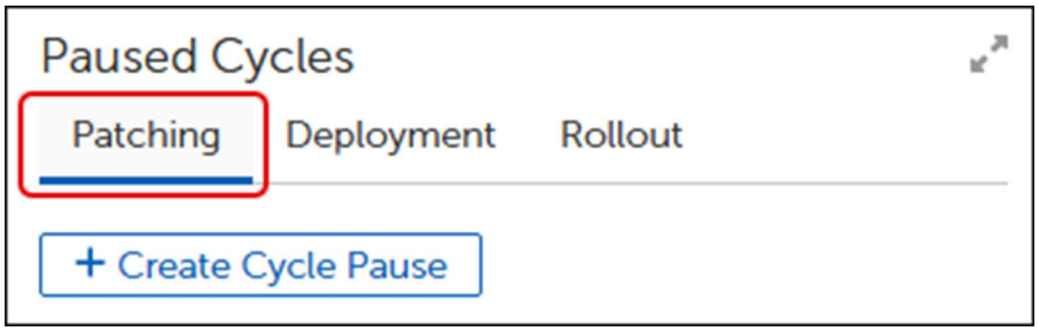
Pausing a cycle that is currently in a WAITING state (has not run yet), prevents that cycle from running until you remove the pause. This is the only server-side behavior related to pausing.

Pause a Patching Cycle

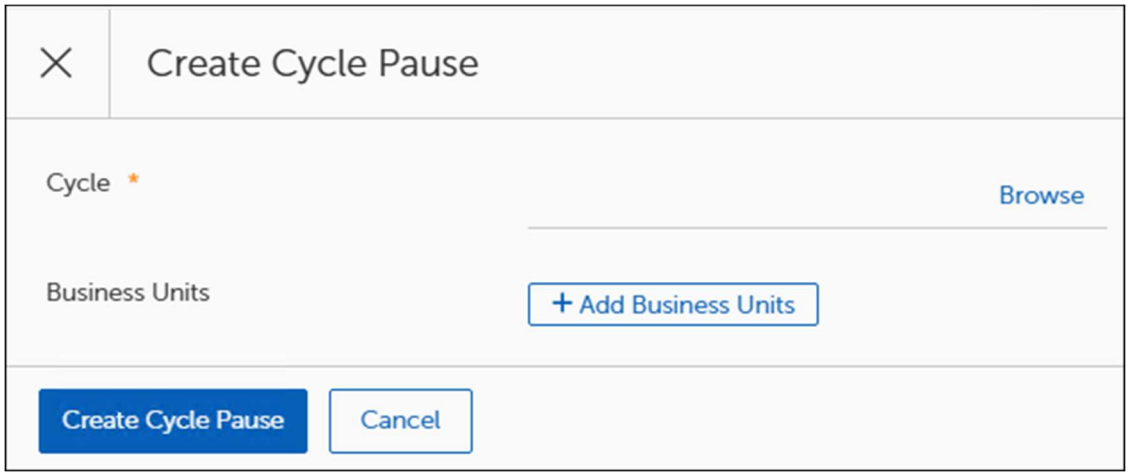
To stop patching activity for a specific patching cycle, complete the following steps:

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:



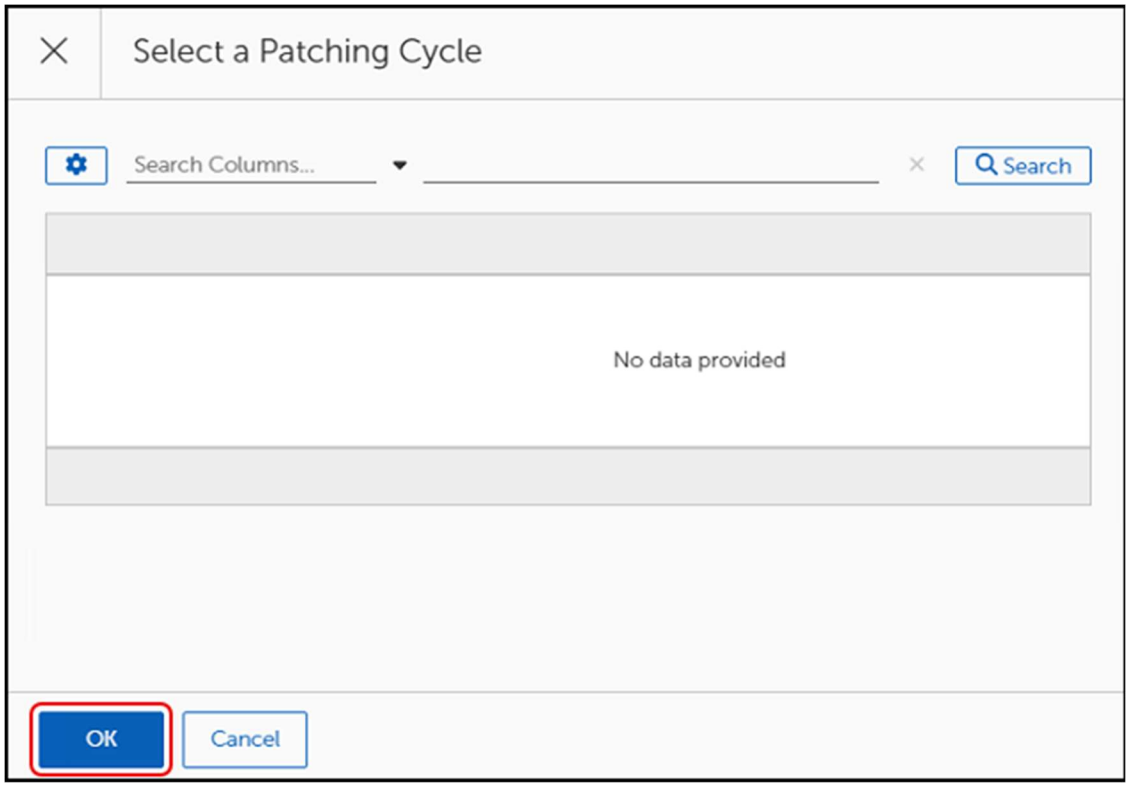
2. Select **+Create Cycle Pause** to open the **Create Cycle Pause** dialog, and then click **Browse**.



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.



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**.

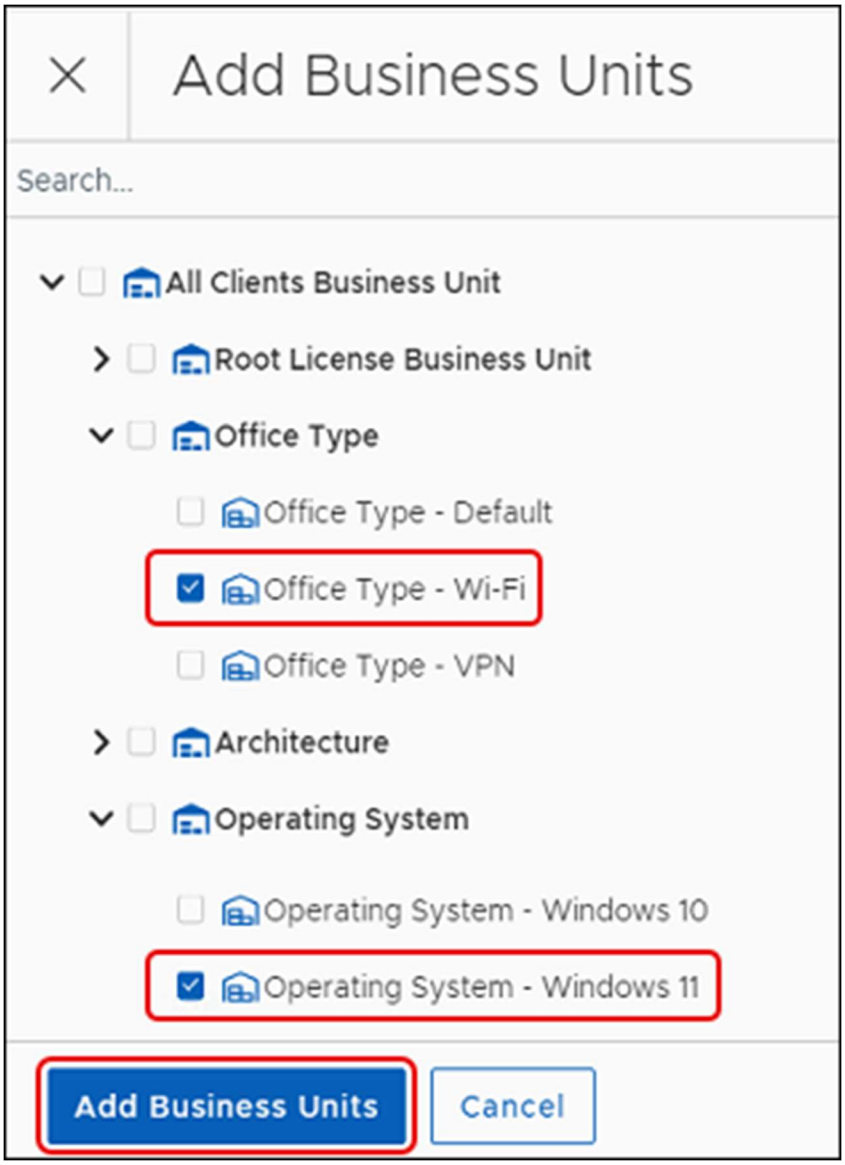
5. Add or remove **Business Units**:

   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.

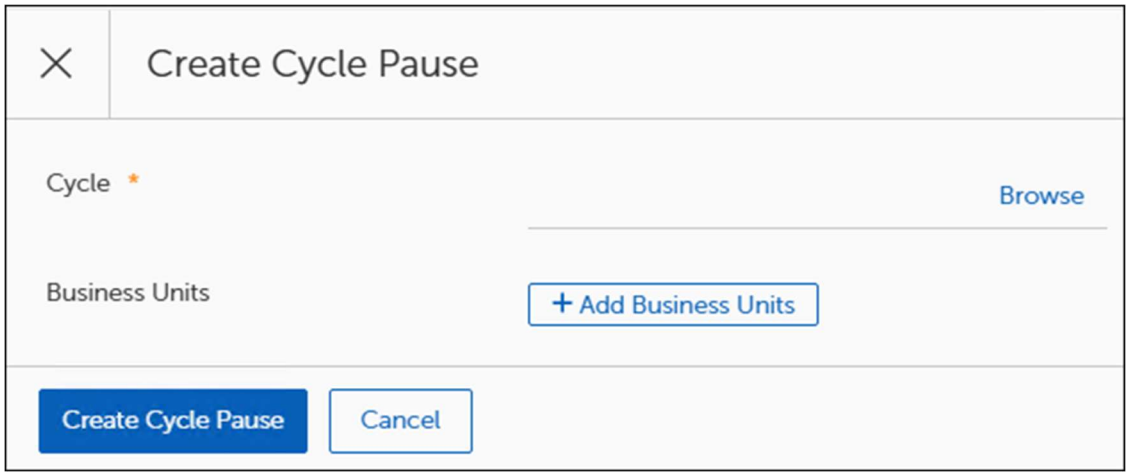
Pause a Deployment Cycle

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:

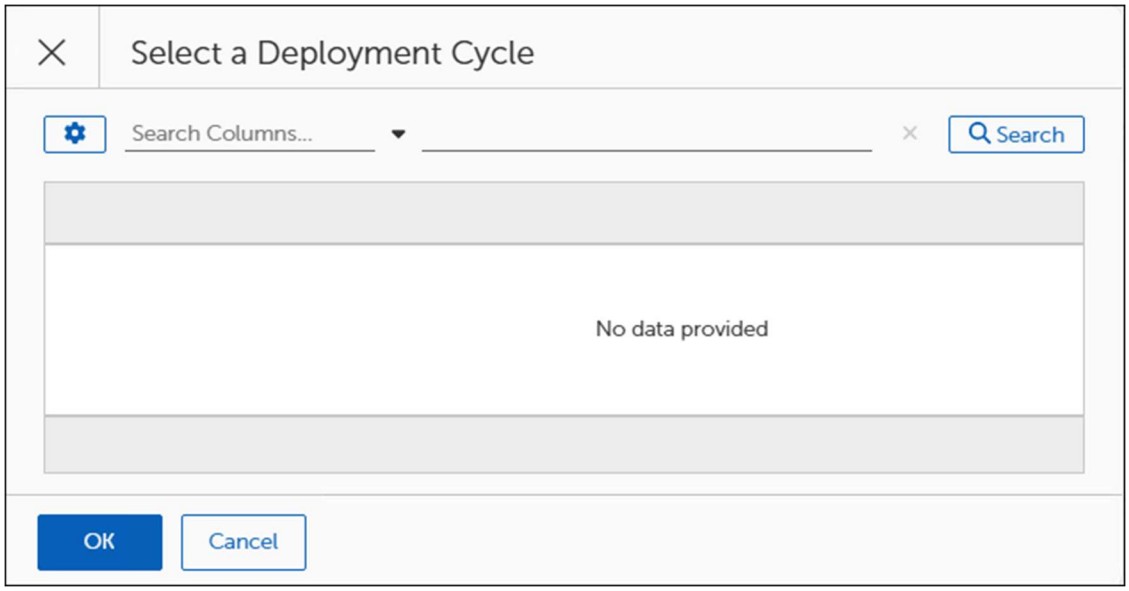
2. Select **+Create Cycle Pause**. This opens the **Create Cycle Pause** dialog:



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**.

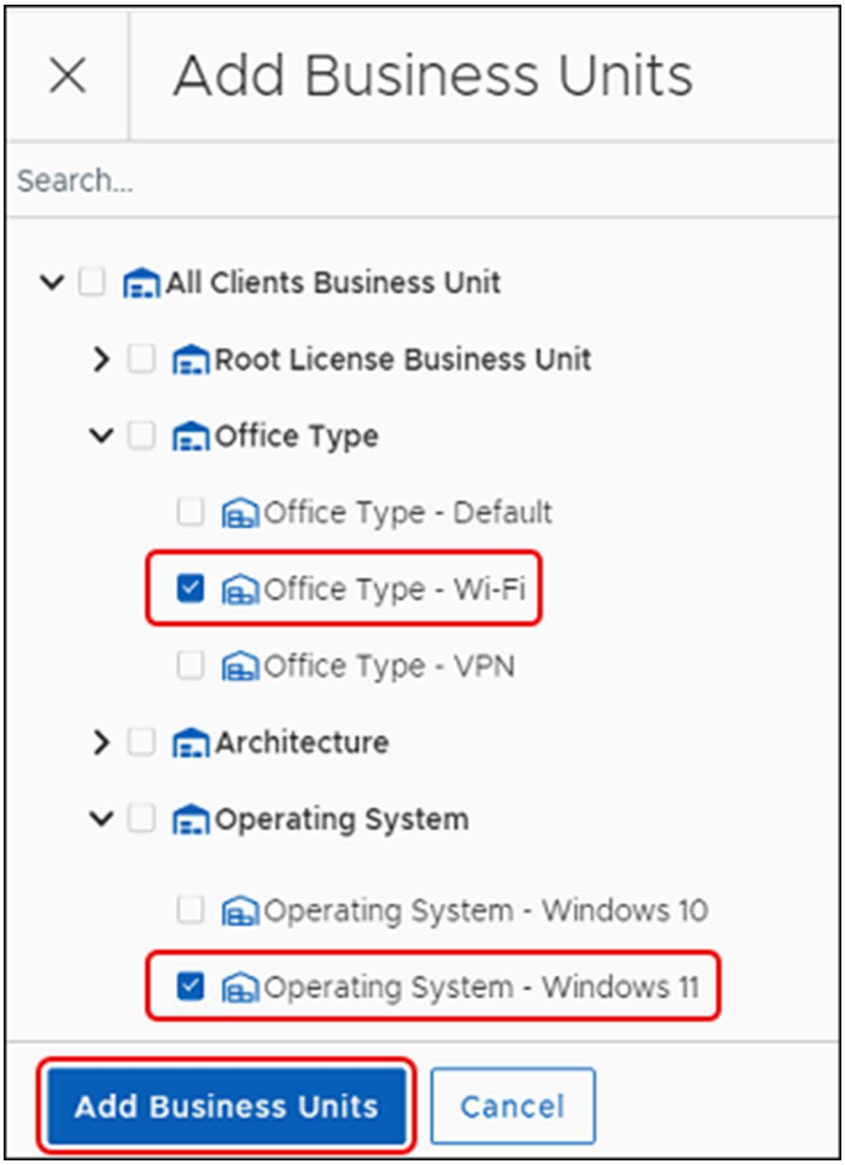
5. Add or remove **Business Units**:

   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**.

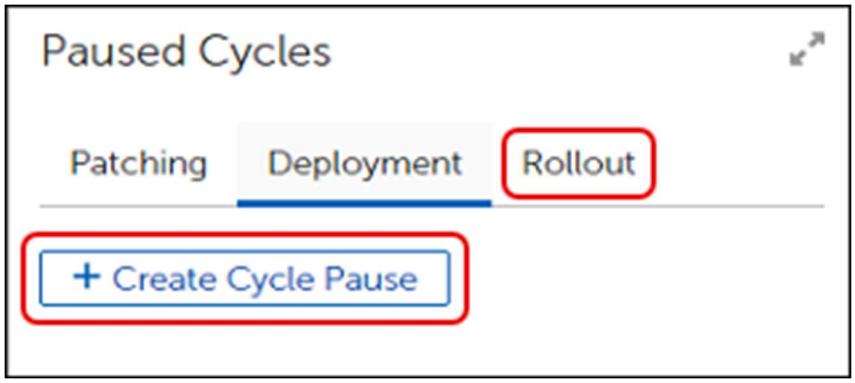
6. Select **Create Cycle Pause** and then click **Save** to create a pause for the selected cycle.

Pause a Rollout Cycle

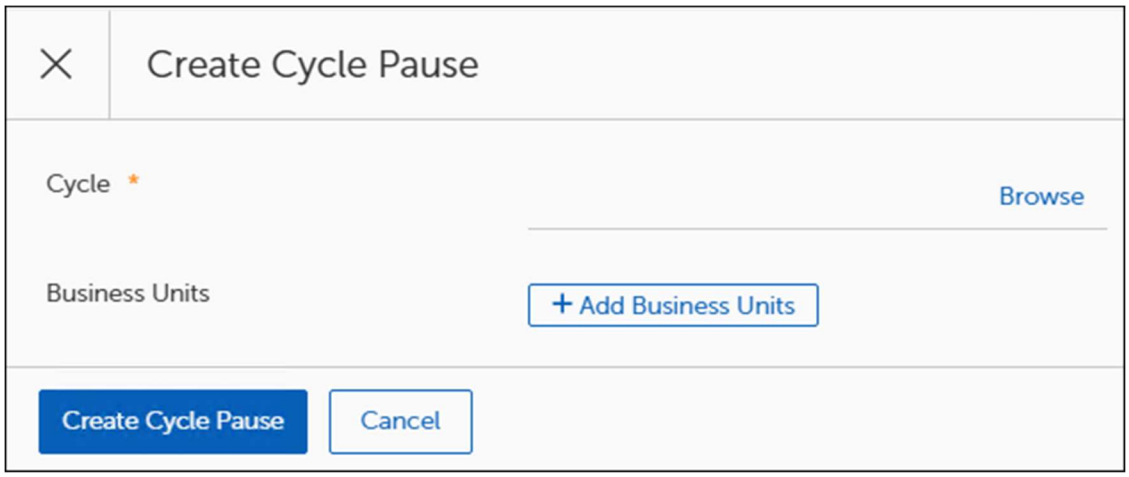
To stop all patching activity for a specific rollout cycle, complete the following steps:

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:



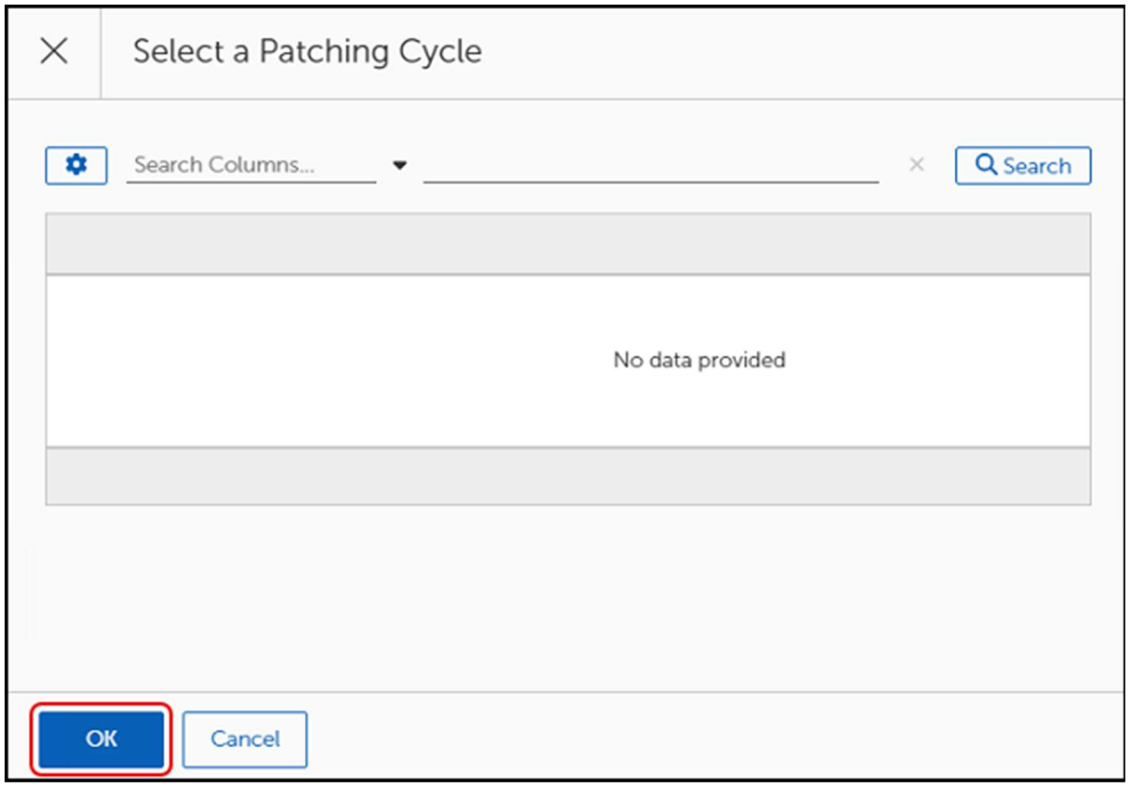
2. Select **+Create Cycle Pause**. This opens the **Create Cycle Pause** dialog:



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**.

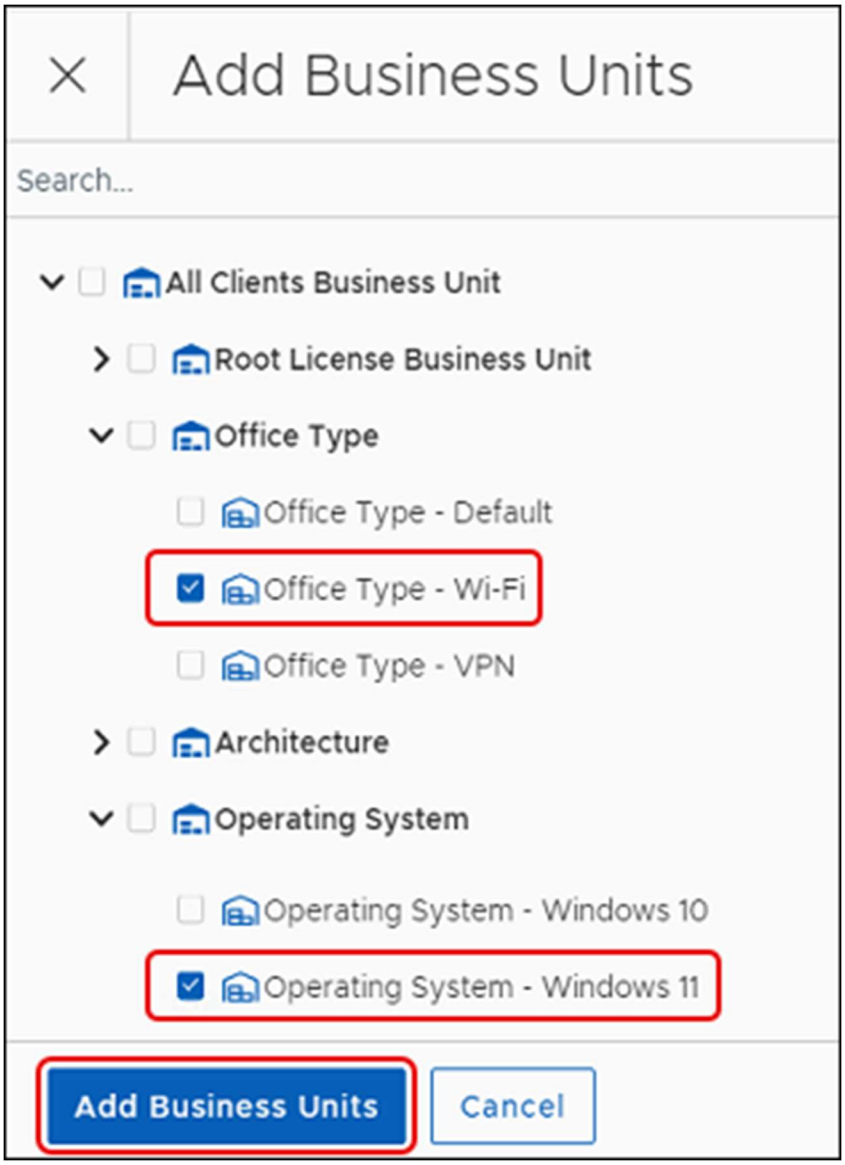
5. Add or remove **Business Units**:

   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**.

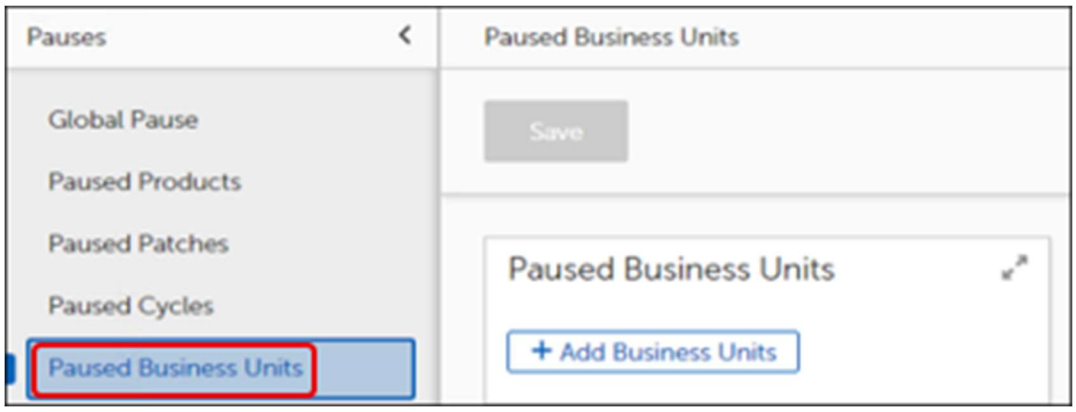
6. Select **Create Cycle Pause** and then click **Save** to create a pause for the selected rollout cycle.

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:



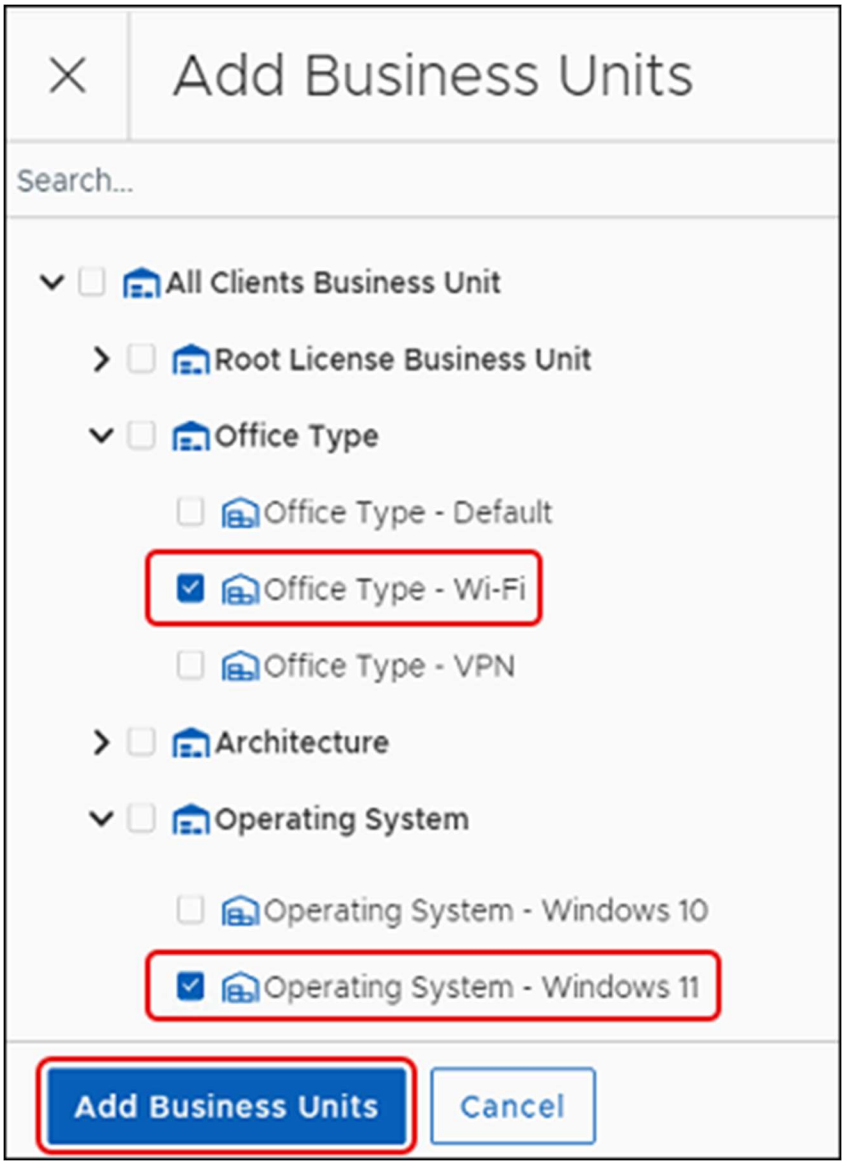
2. Add or remove **Business Units**:

   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.

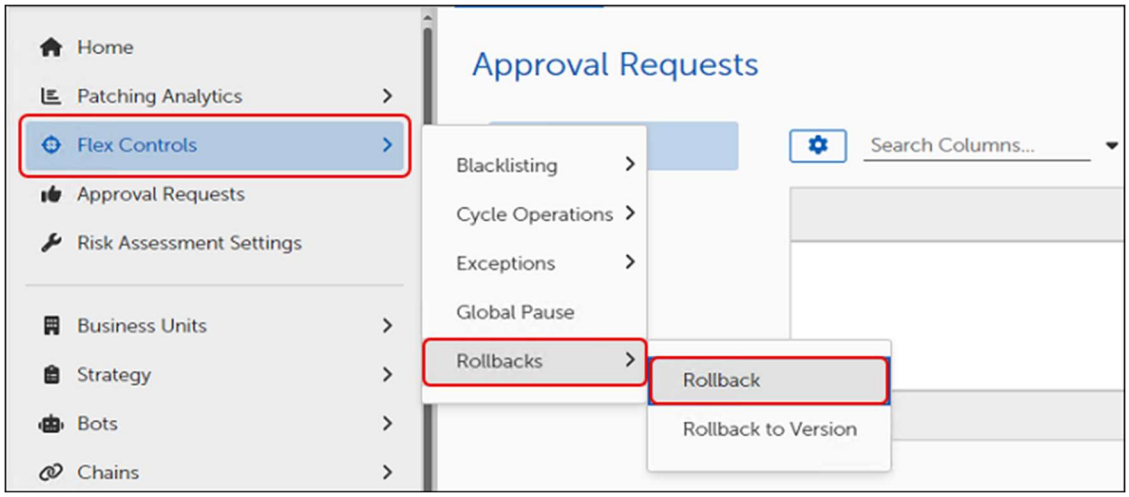
Rollback

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.

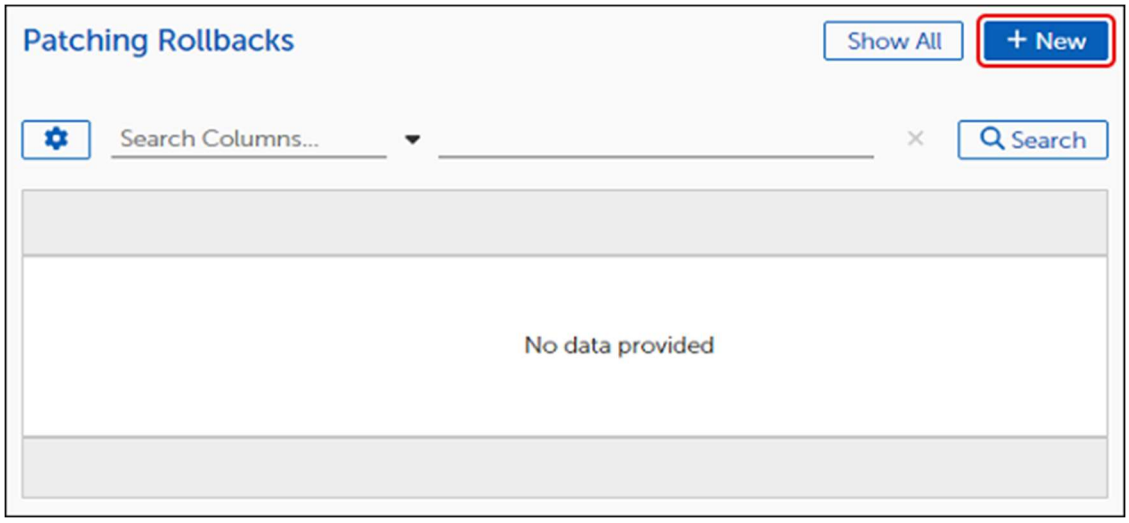
Create a Rollback

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**.



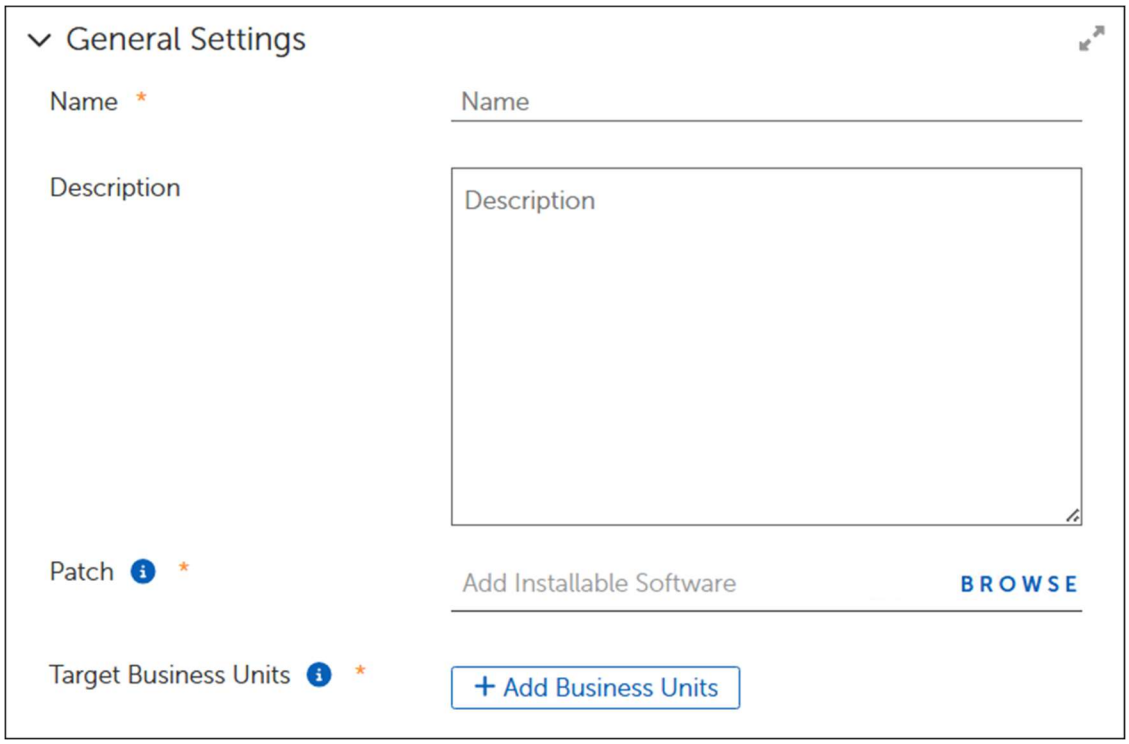
This opens the Patching Rollbacks table. Until you create a rollback, the table is empty.



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.



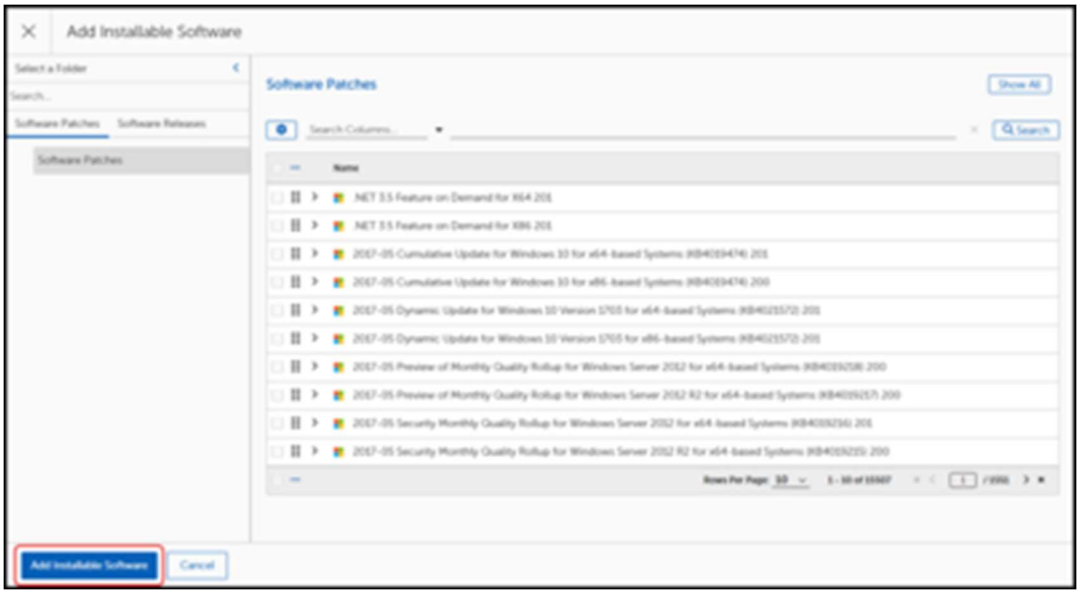
3. Locate the patch or release you want to roll back:

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:

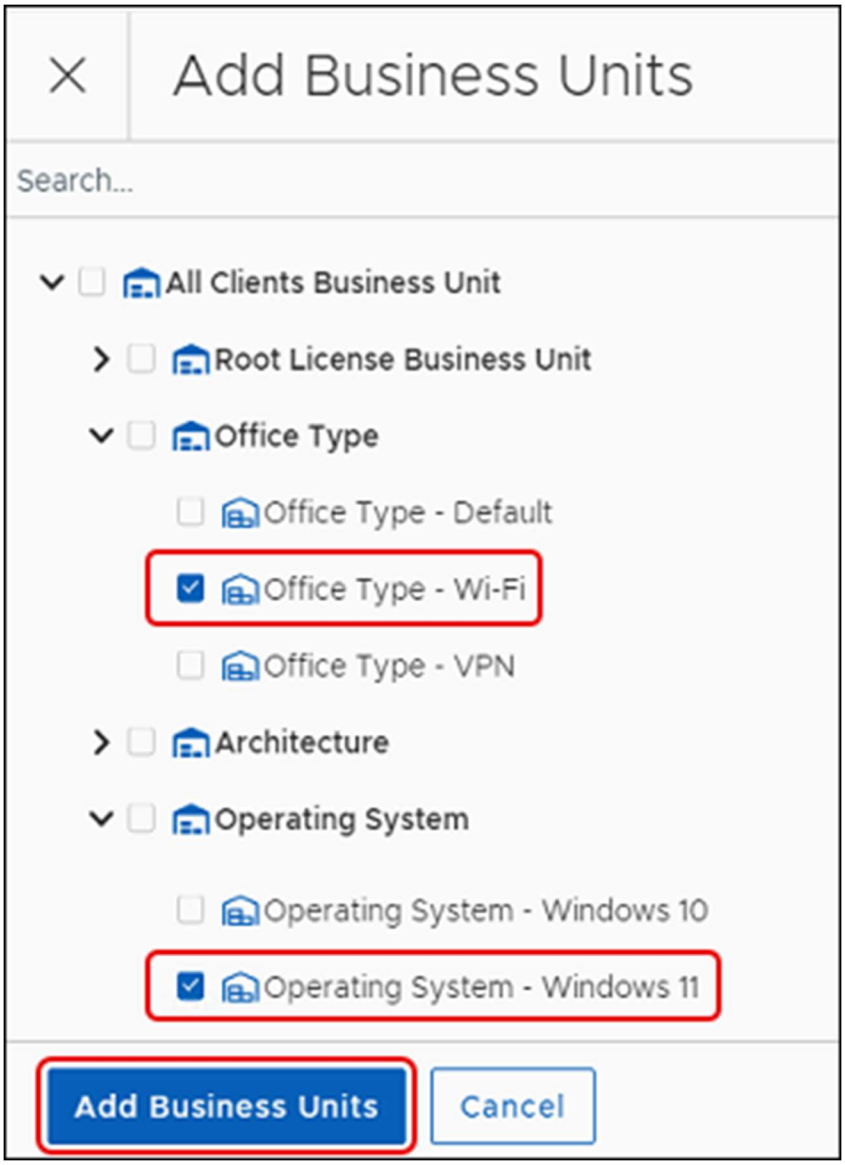


- Use the navigation tools on the bottom right to scroll through the pages to find and select a Software product or release.
- Enter a product name on the search line, and then click **Search** to find and select a specific product.

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.

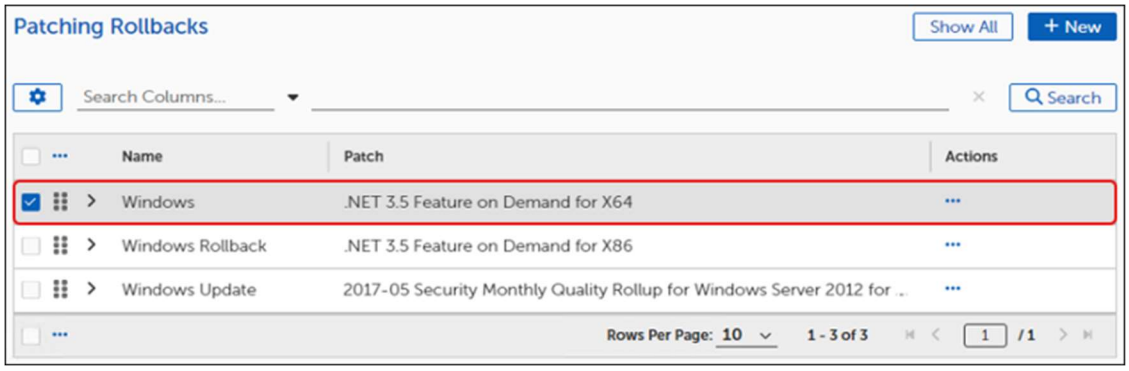


b. Select one or more **Business Units** to add, and then click **Add Business Units**.

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

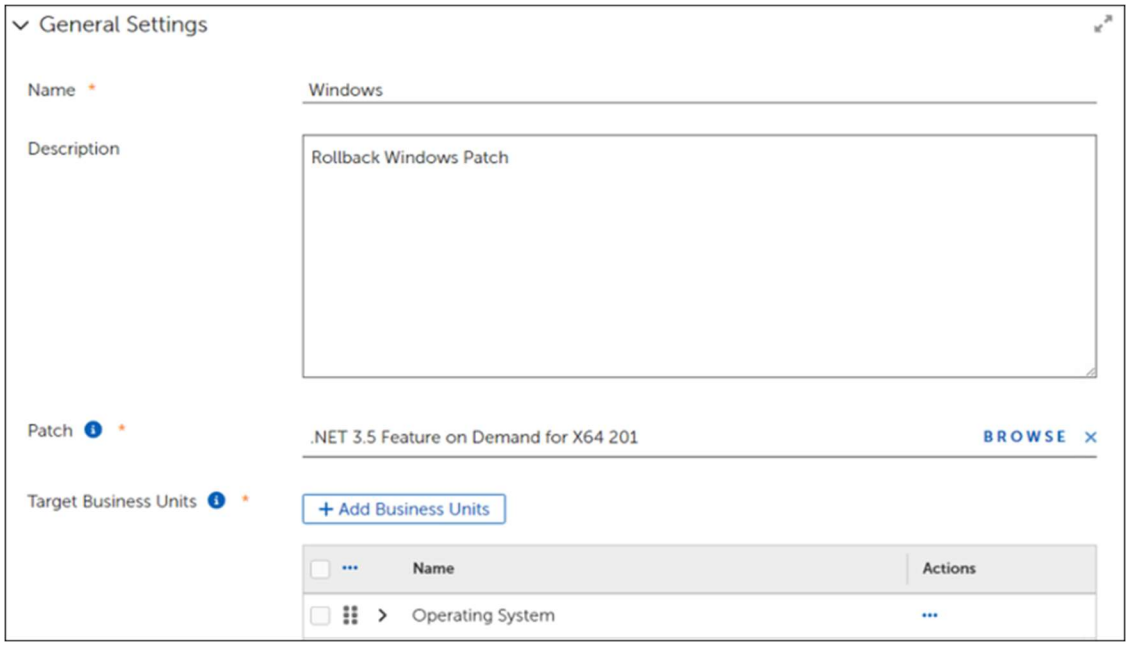
1. Select a **Rollback** template from the **Patching Rollbacks** table of an open Patching Rollbacks template.



This opens the template.

Note

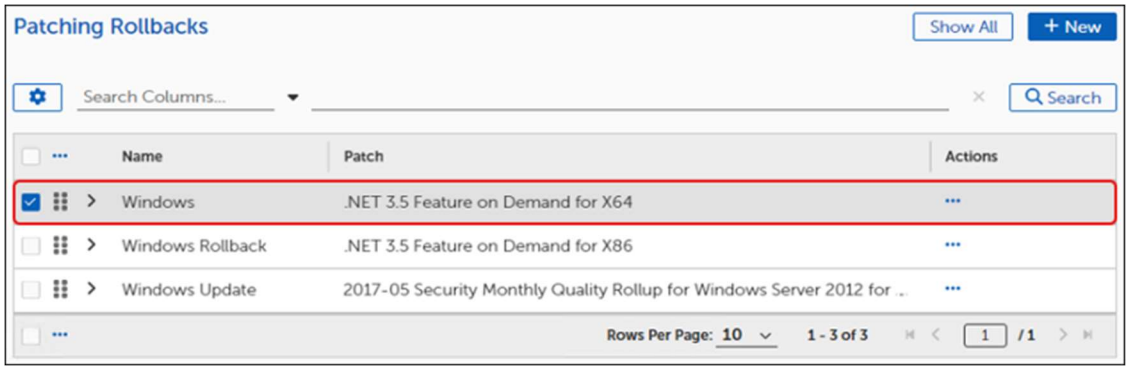
A red asterisk next to a field name indicates a required field.



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

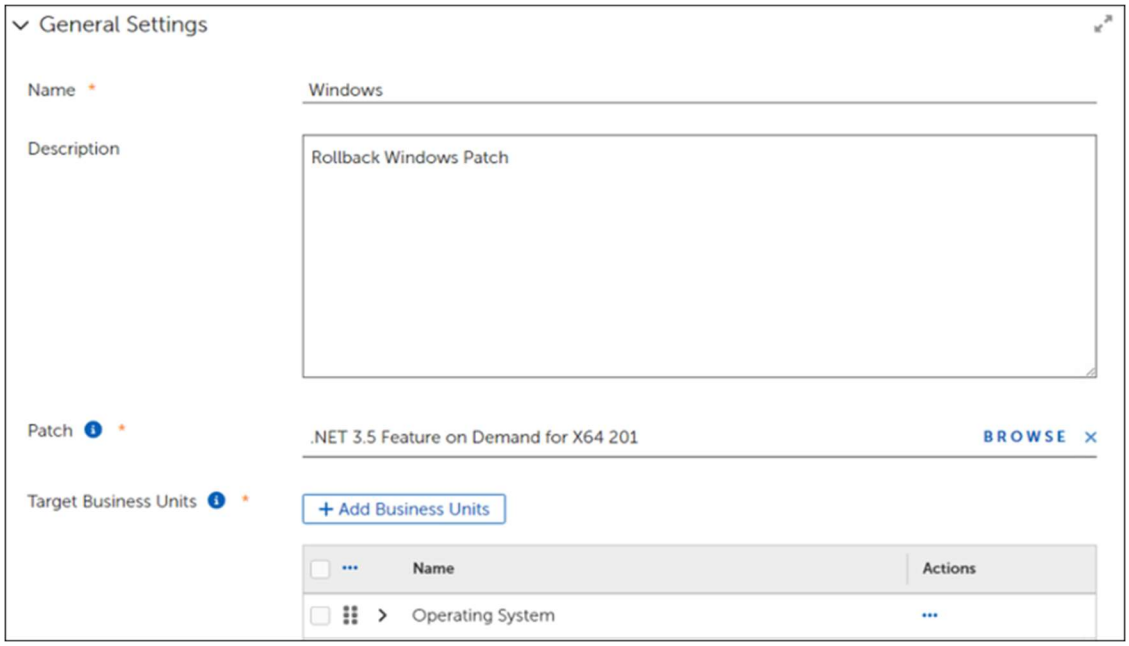
1. Select a **Rollback** template from the **Patching Rollbacks** table of an open Patching Rollbacks template.



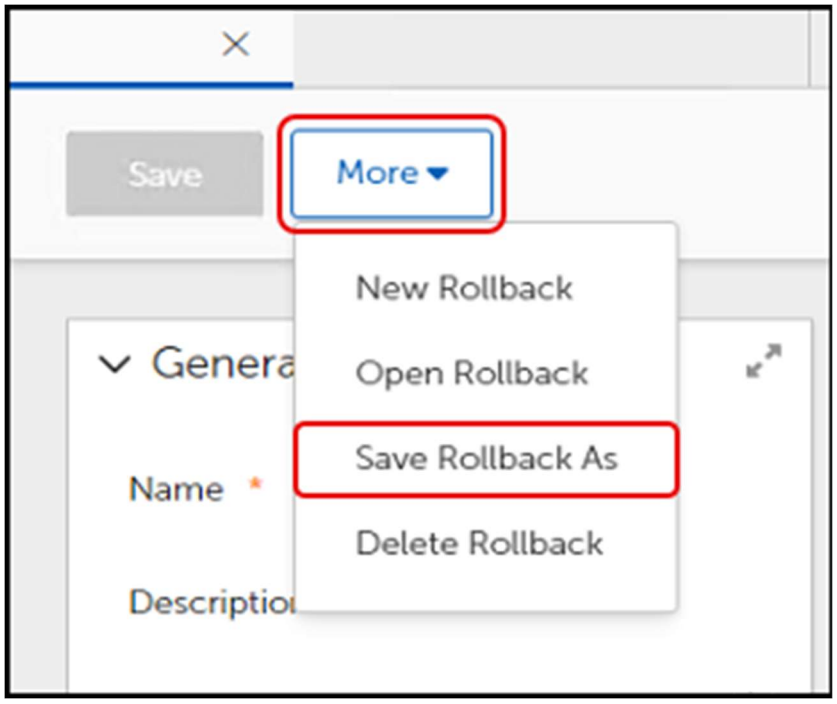
This opens the template.

Note

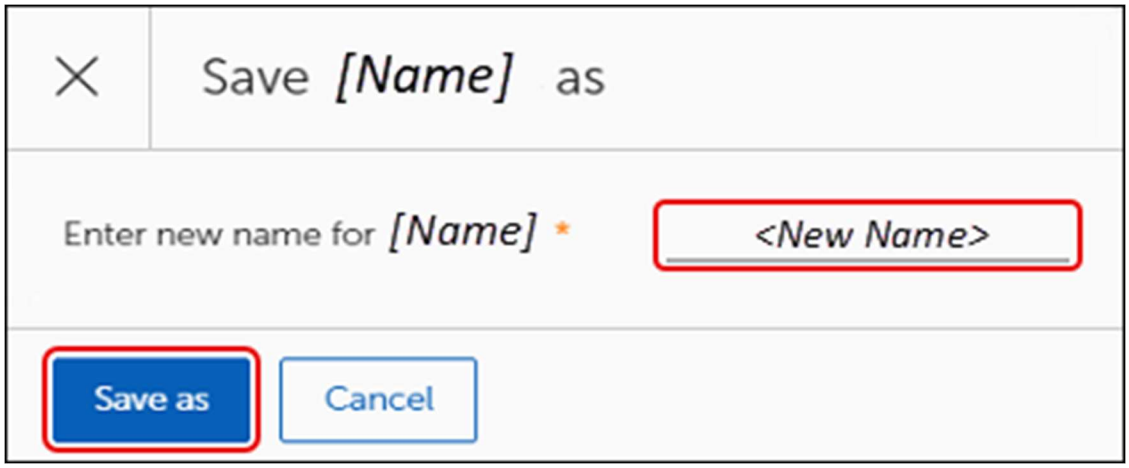
A red asterisk next to a field name indicates a required field.



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



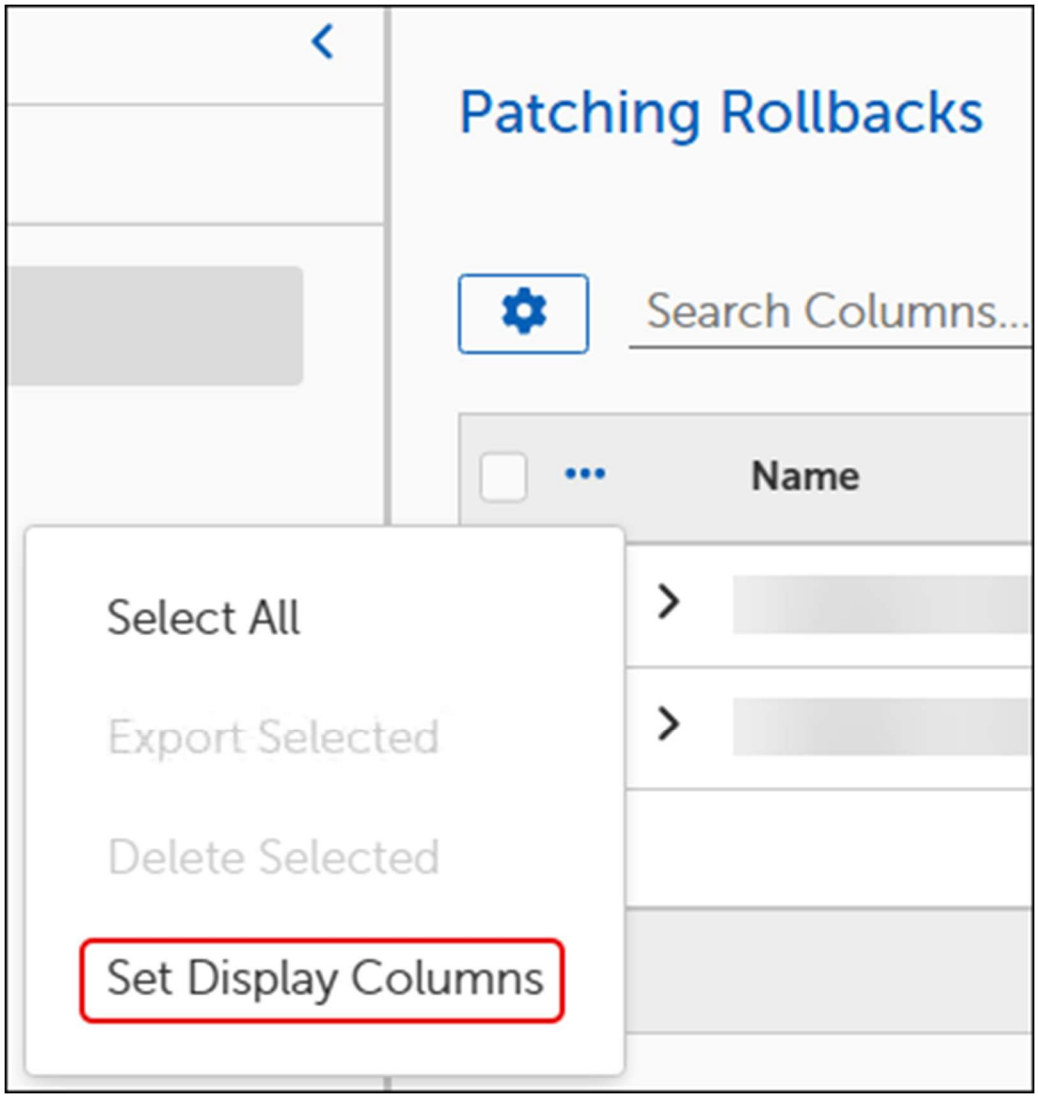
3. Enter a new **Name** for the template, and then click **Save as**.



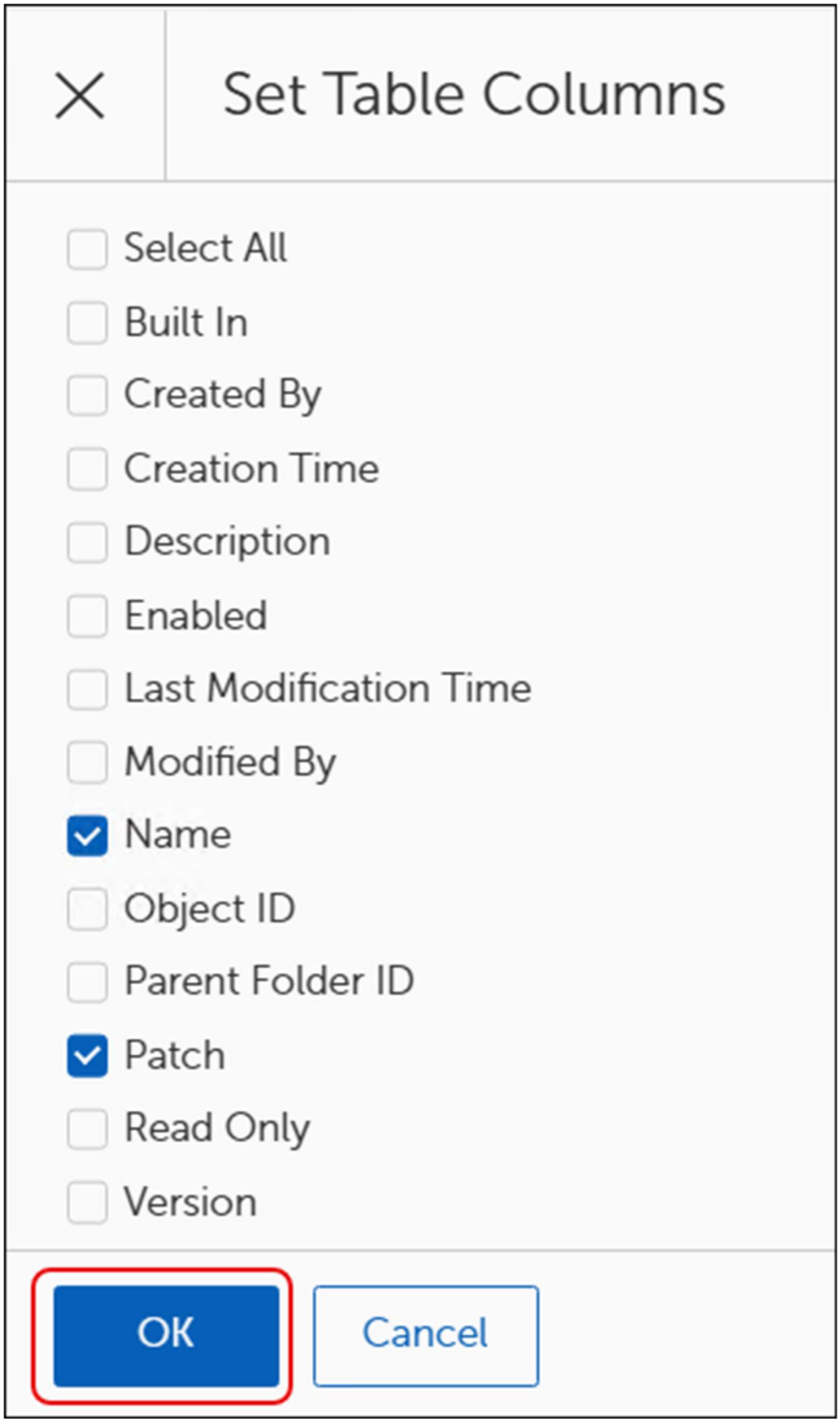
4. Revise the **Description** to reflect any changes needed for the copy, and then click **Save**.
5. Select **Back to Rollbacks** on the upper-left corner of the template to return to the **Rollbacks** table and view your changes.

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**.



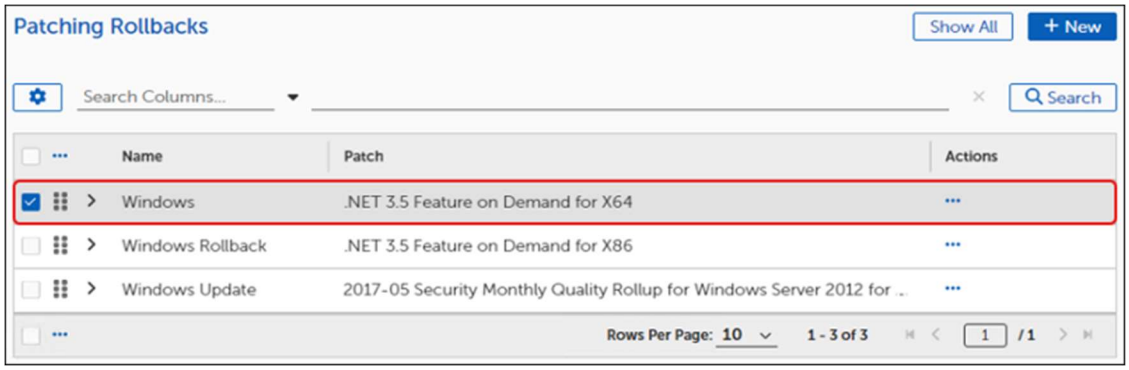
This opens the Set Table Columns dialog.



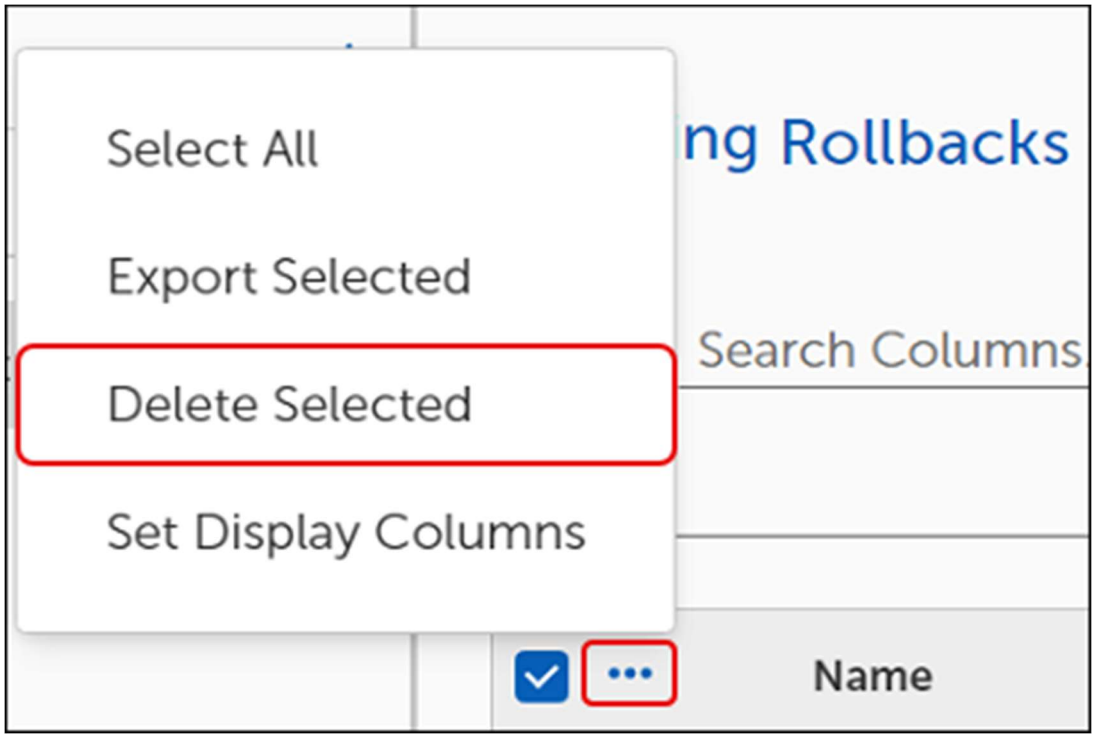
3. Select the **column names** you want the **Patching Rollbacks** table to display, and then click **OK**.

Delete a Rollback

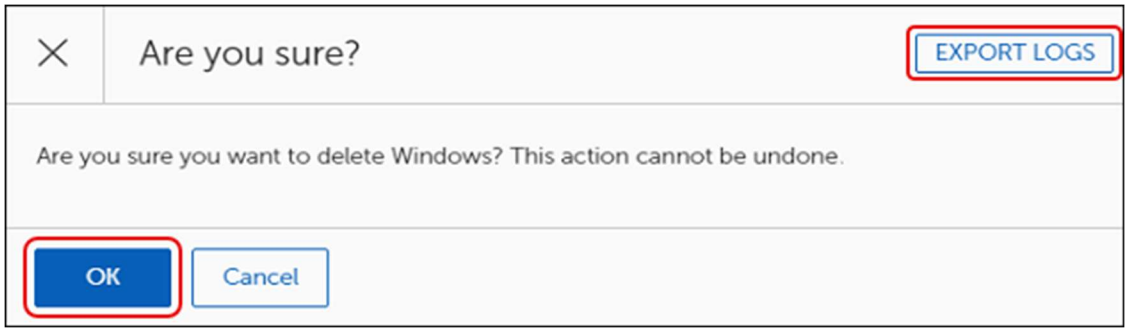
1. Select a **Rollback** template from the **Patching Rollbacks** table of an open Patching Rollbacks template.



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.

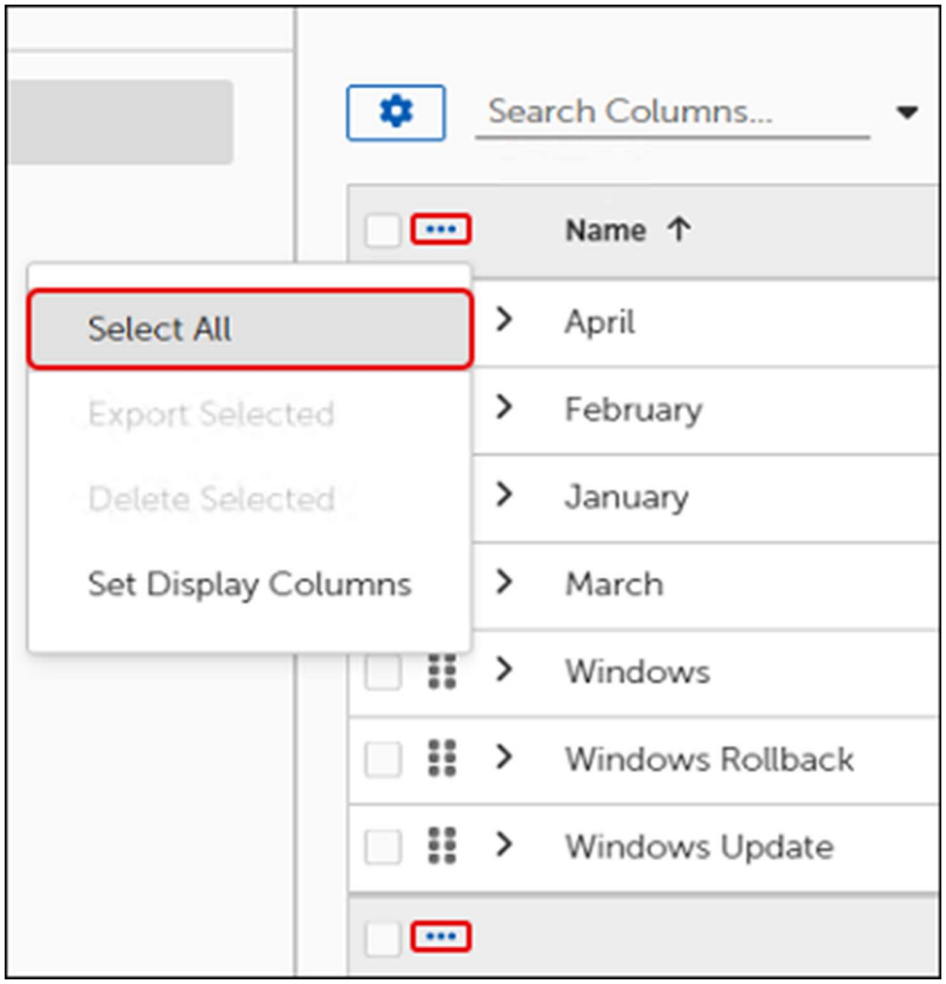
b. Select **OK** to delete the Rollback.

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.

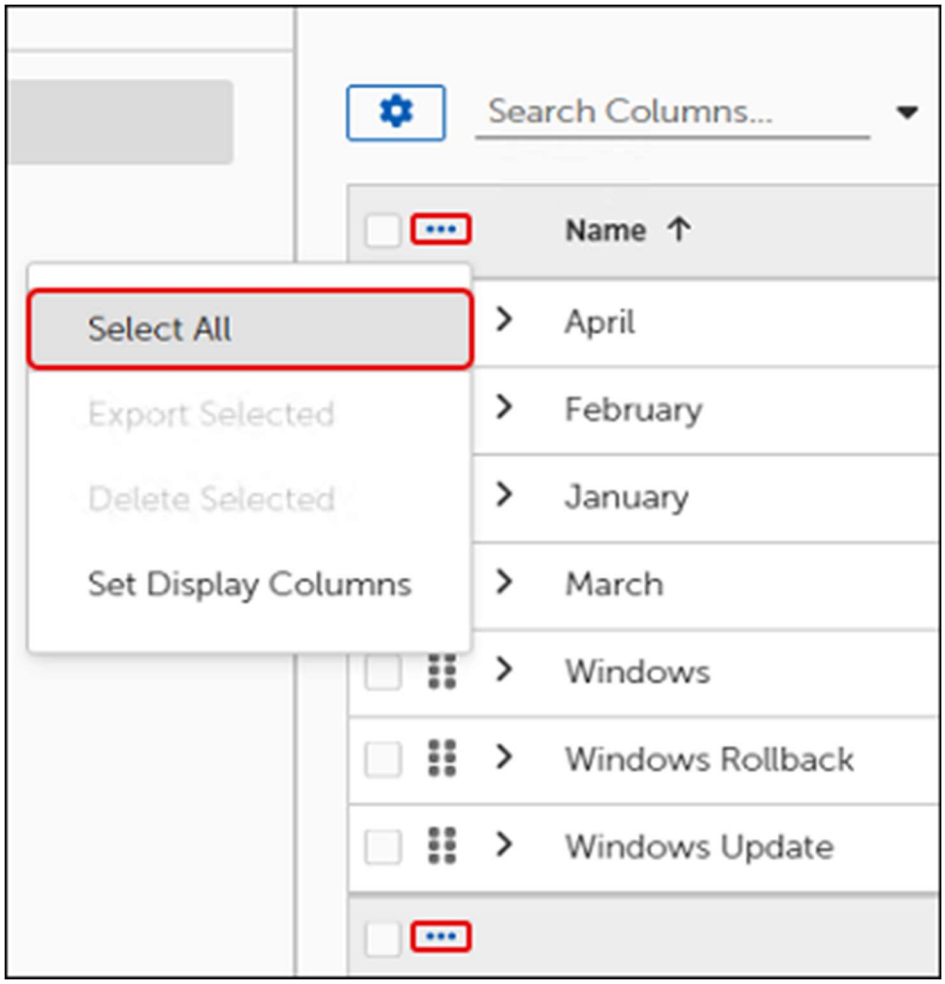
    b. To delete the Selected templates, see Bulk Delete Rollbacks.

    c. To customize the display columns of the Patching Rollbacks table, see Customize Patching Rollback Table Settings.

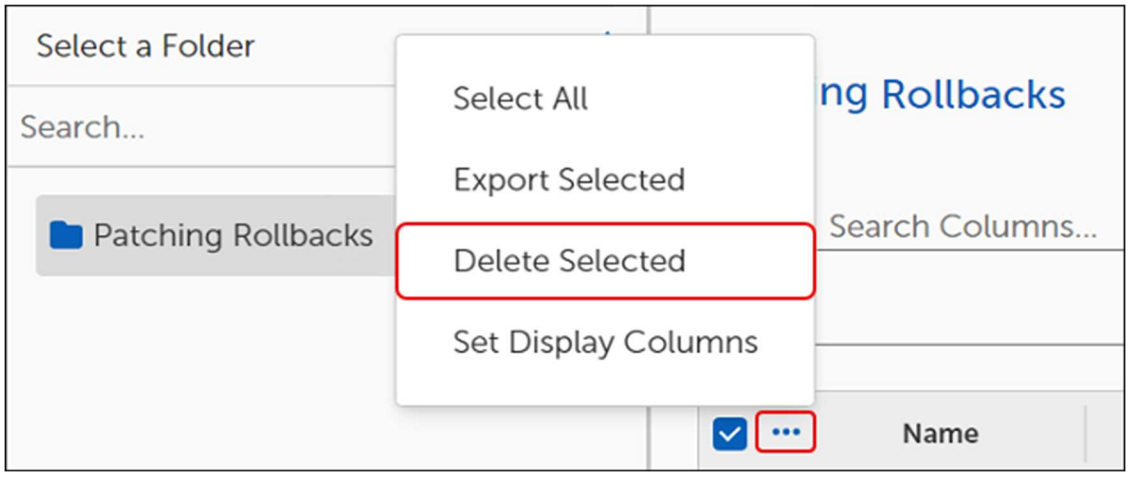
Bulk Delete Rollbacks

1. Open the **Patching Rollbacks** table (**Flex Controls > Rollbacks > Rollback**).

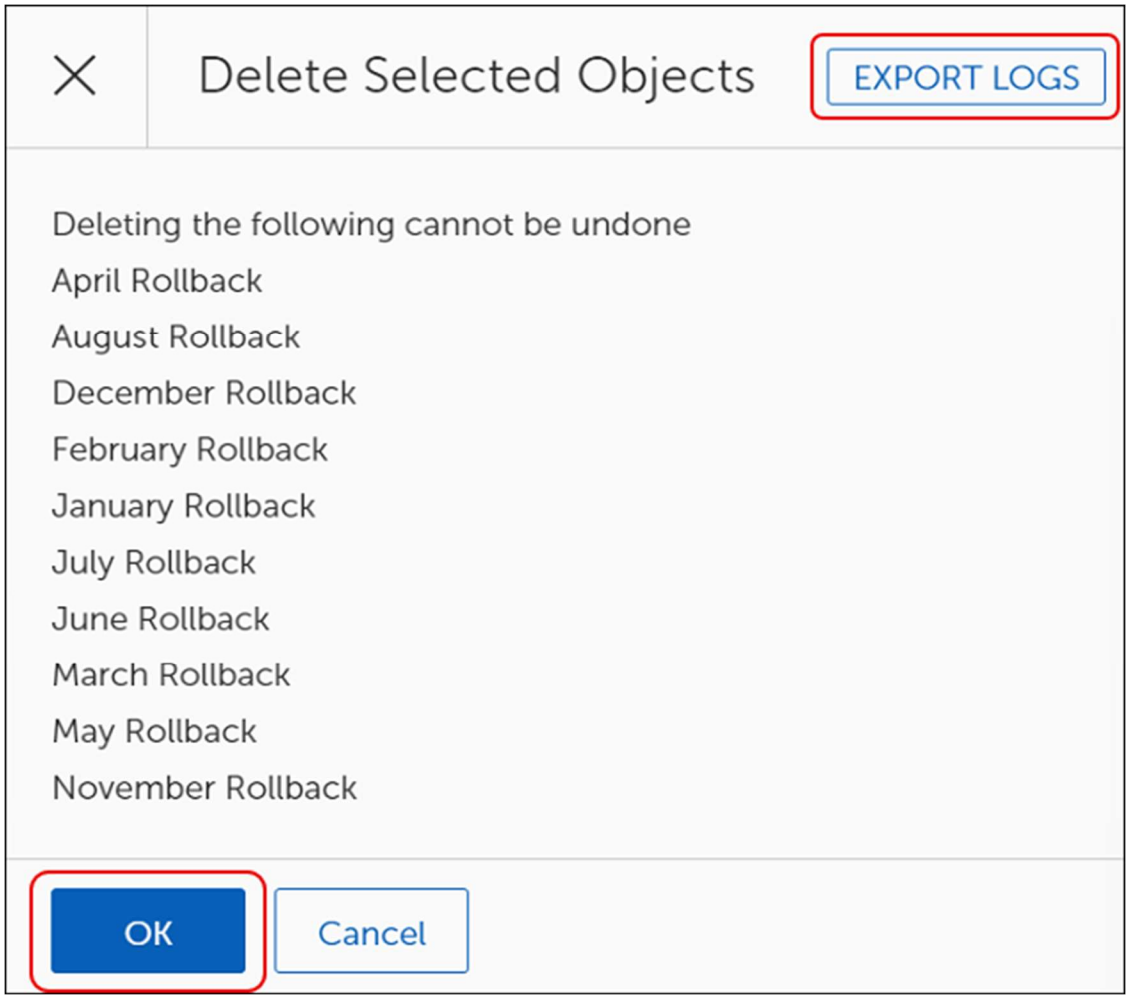
2. Select the **ellipsis (...)** next to Name, and then click **Select All**.



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



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



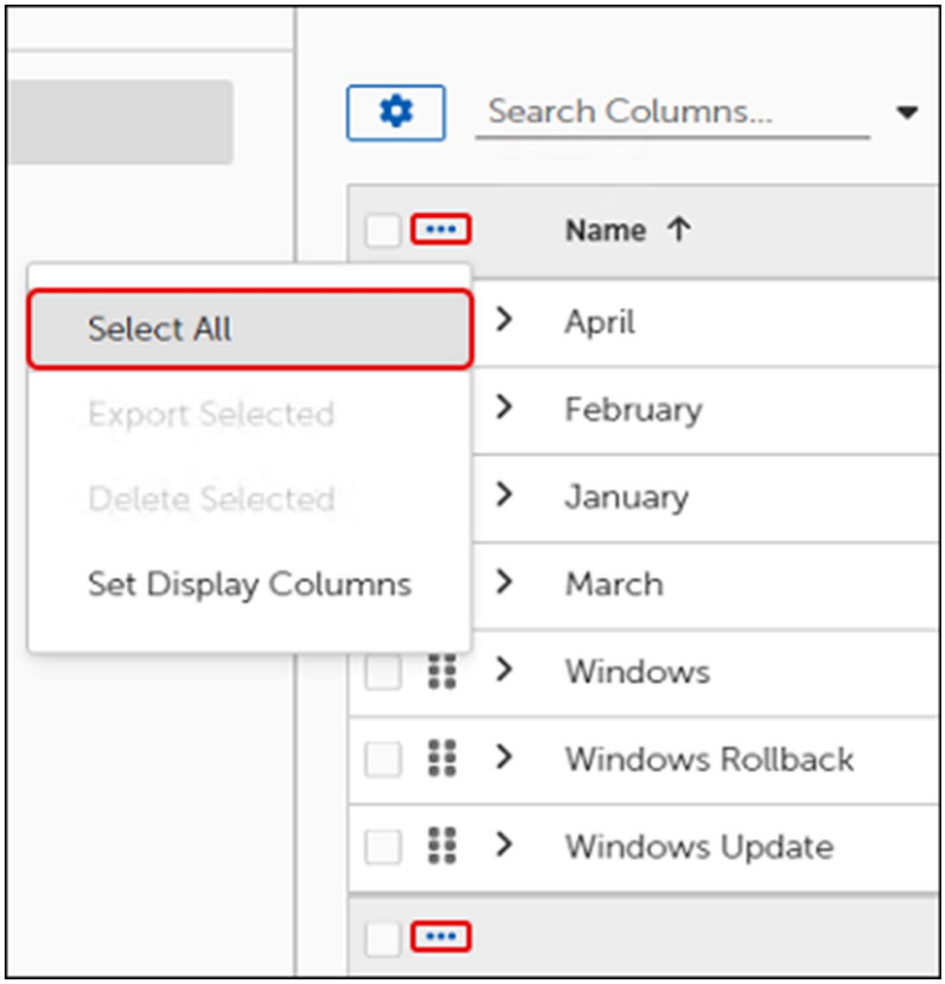
4. (Optional) Select **Export Logs** on the top-right corner of the **Delete Selected Objects** dialog to export trace logs. The trace logs download to your device as a file with a .log extension.

5. Select **OK** to delete the Rollbacks. This returns you to the **Patching Rollbacks to** table where the deleted Rollbacks no longer appear.

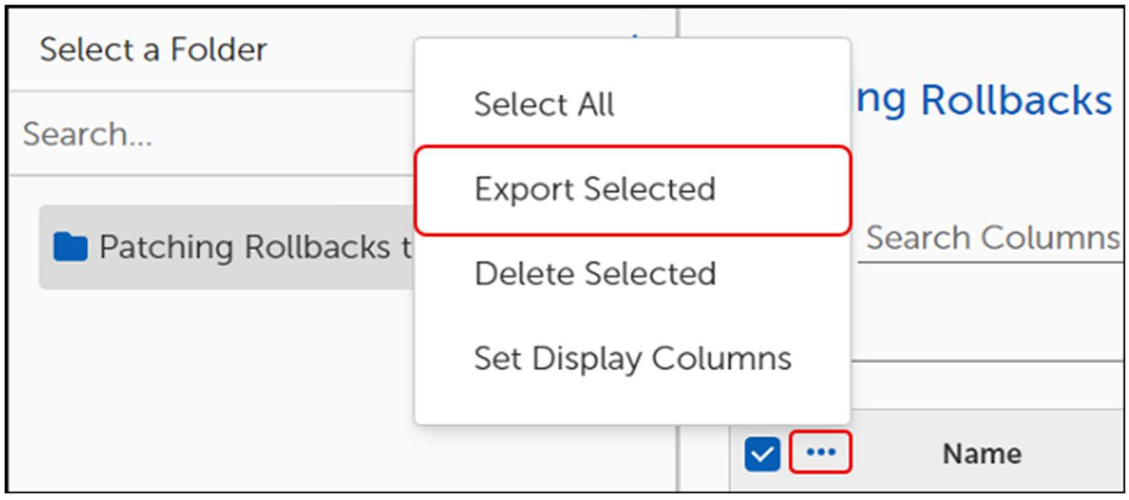
Export Rollbacks

1. Open the **Patching Rollbacks** table (Flex Controls > Rollbacks > Rollback).

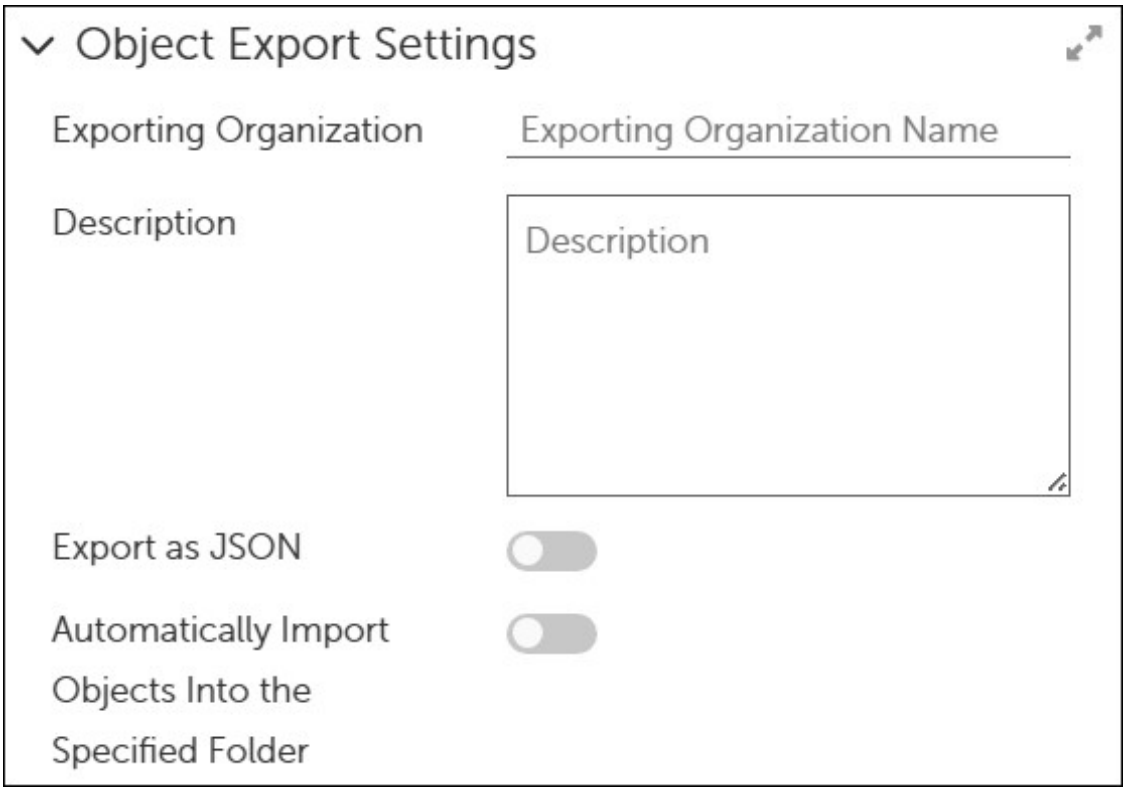
2. Select a single **Patching Rollback** from the table, or click the **ellipsis (...)** next to Name, and then click **Select All** to export all Rollbacks



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



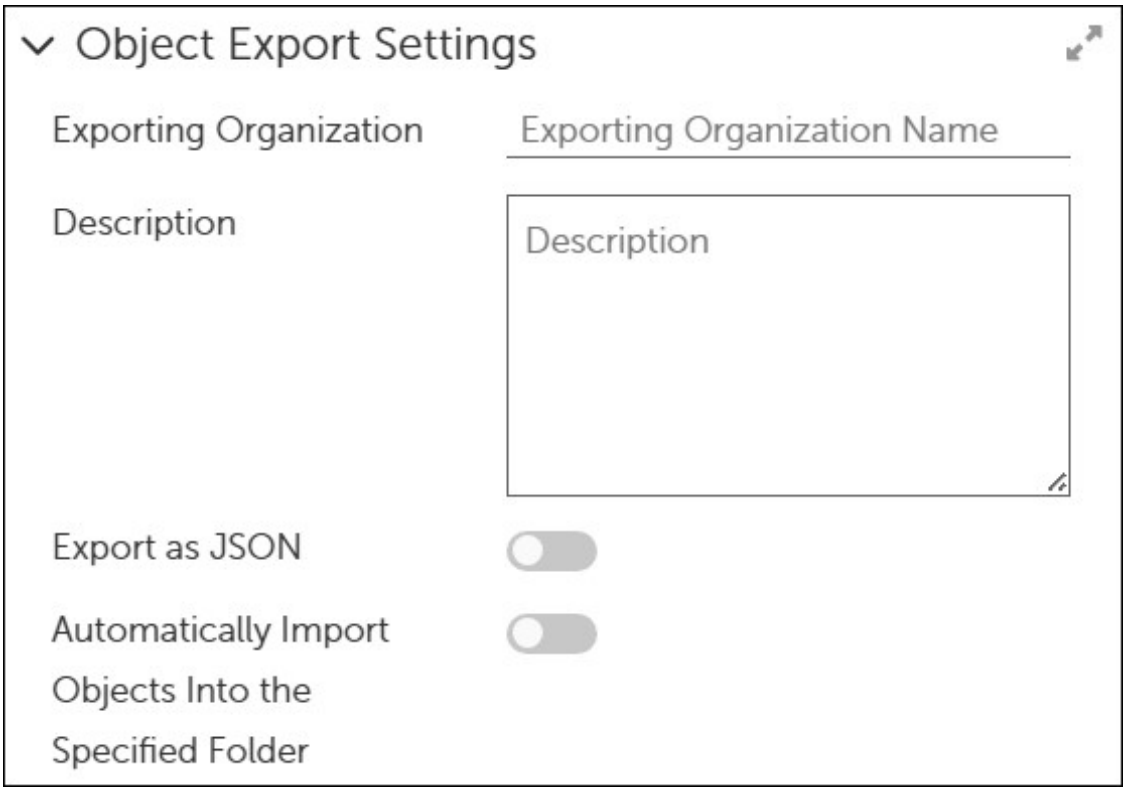
This opens the **Object Export Settings**:



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.



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.

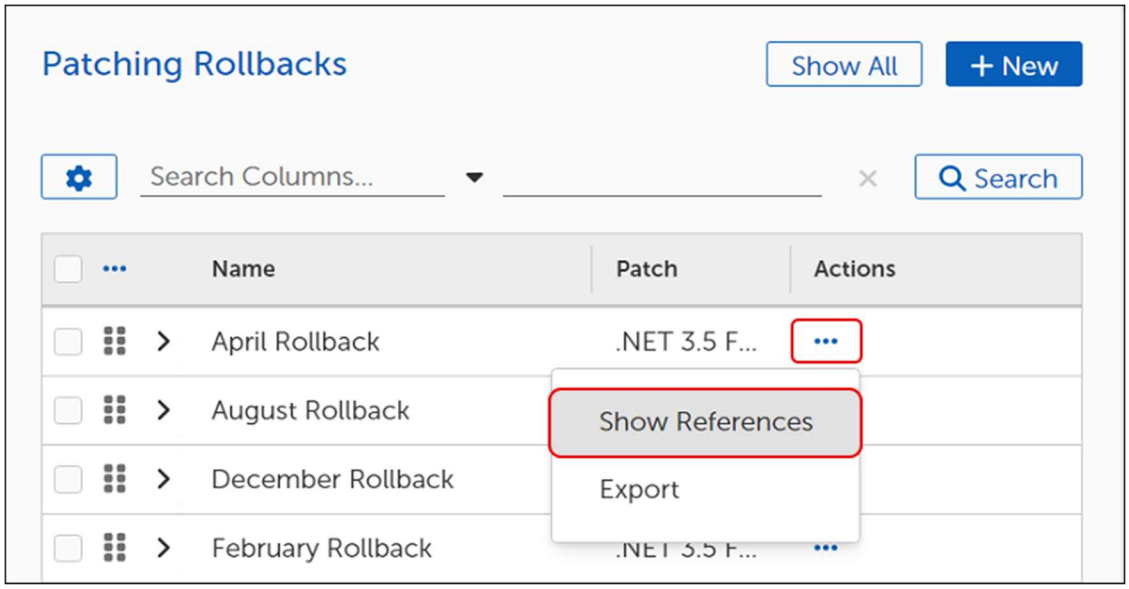
Important

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

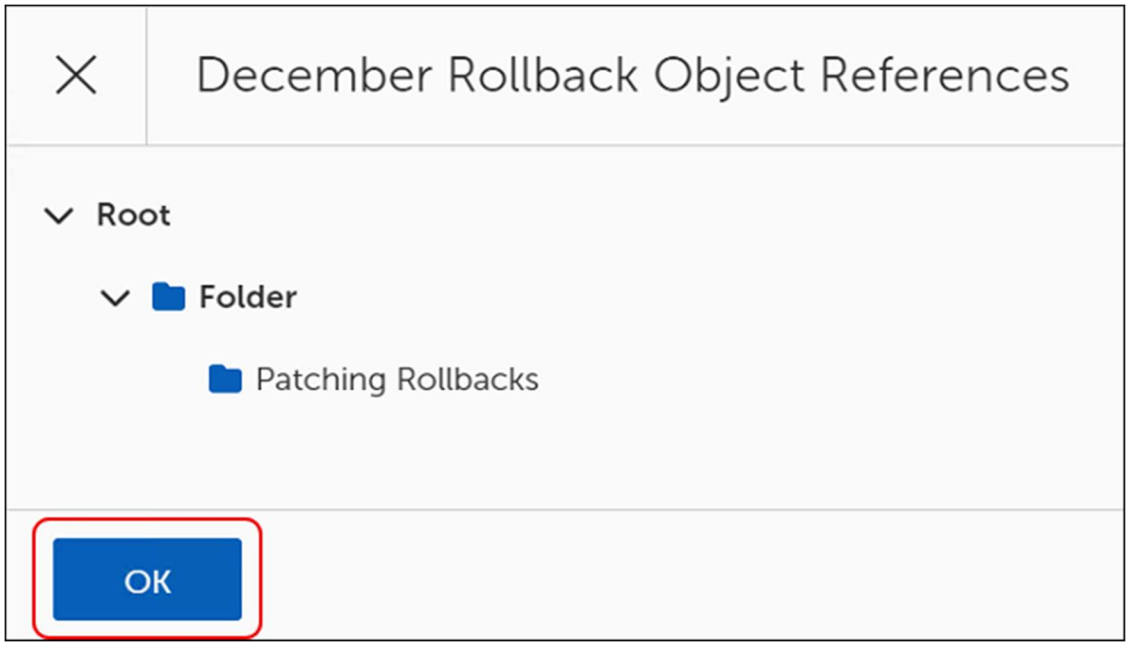
Show Rollback References

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**.



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



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.

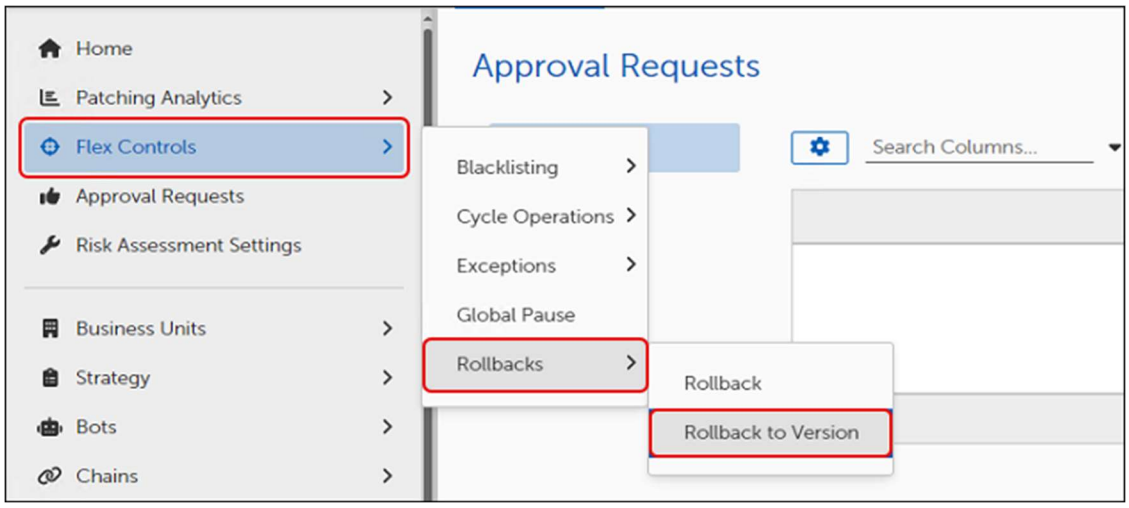
Rollback to Version

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.

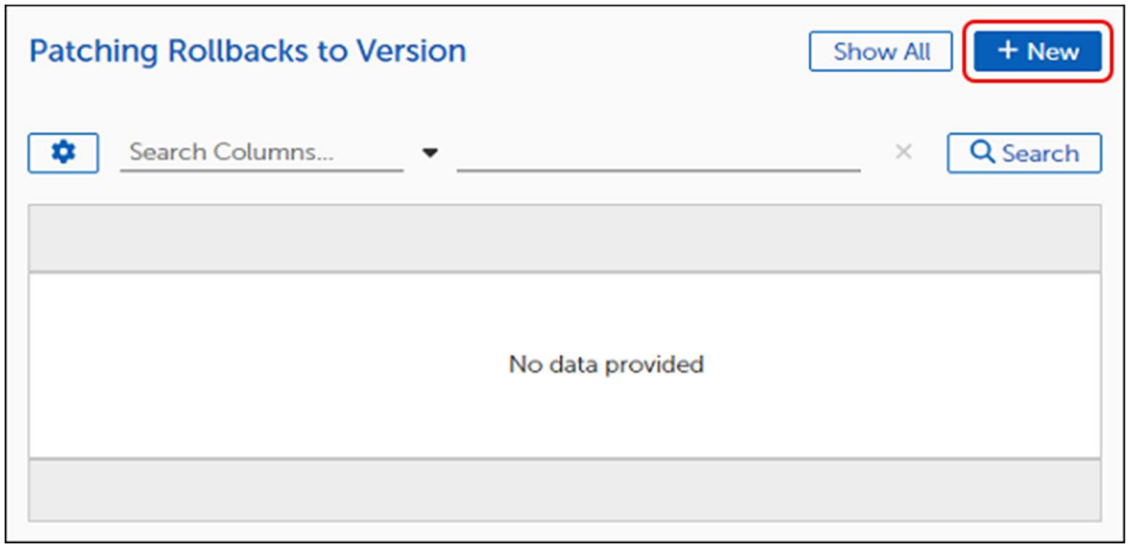
Create a Rollback to Version

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**.



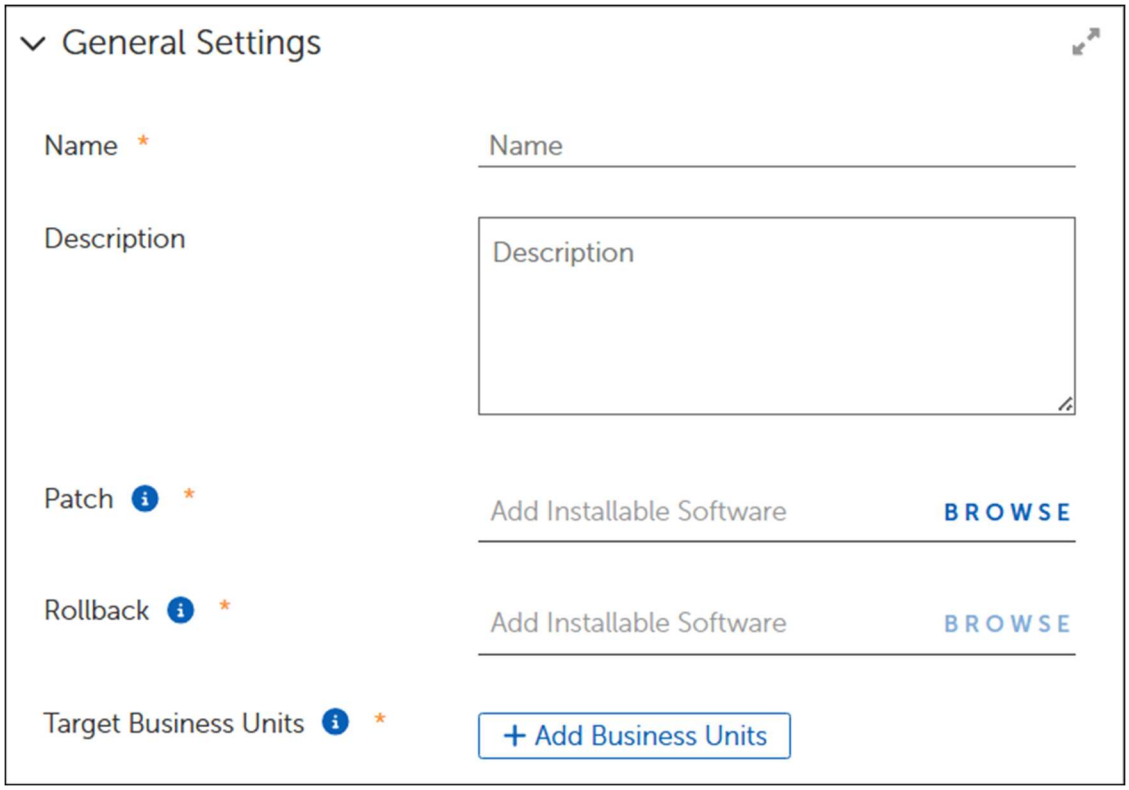
This opens the **Patching Rollbacks to Version** table. Until you create a rollback, the table is empty..



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.

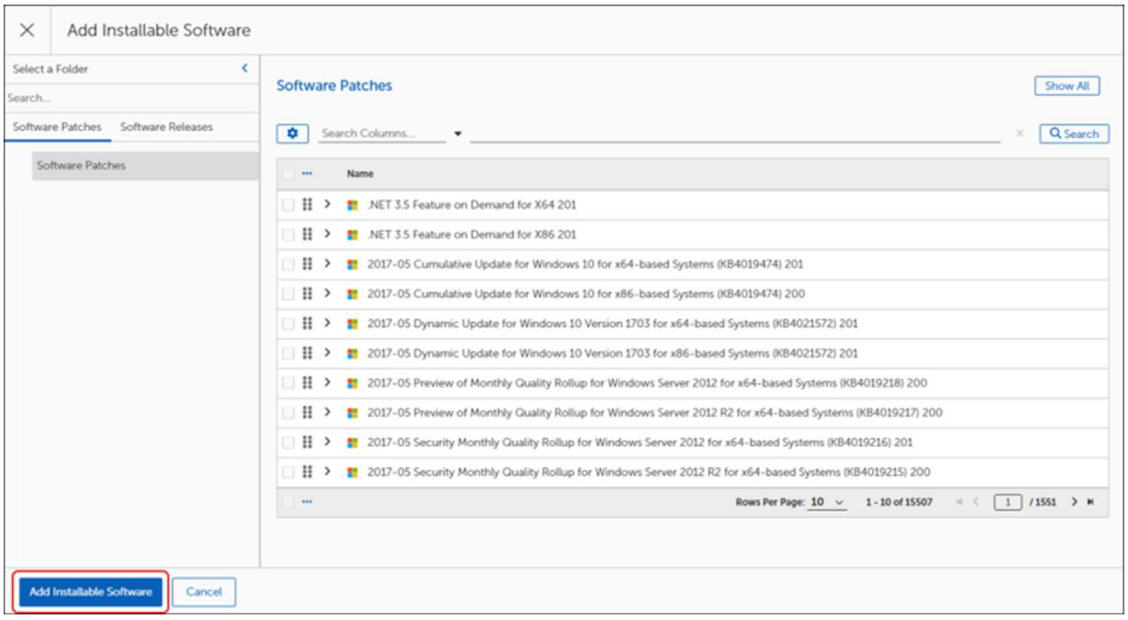


3. Enter a **Name** and a detailed **Description** of your Rollback to Version.
4. Add the patch or release to roll back from.

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.

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.



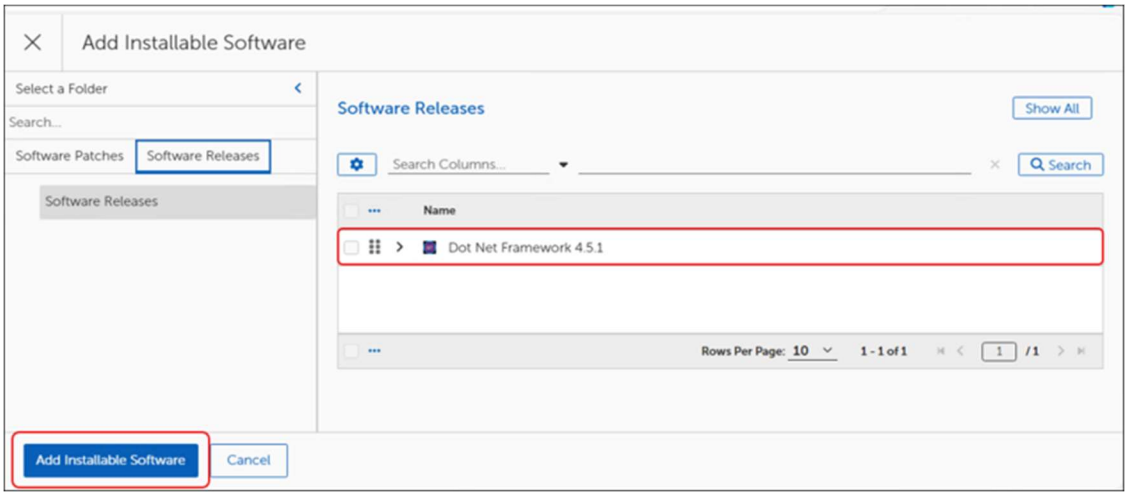
3. Select **Add Installable Software** to return to the Rollback to Version template.

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**.

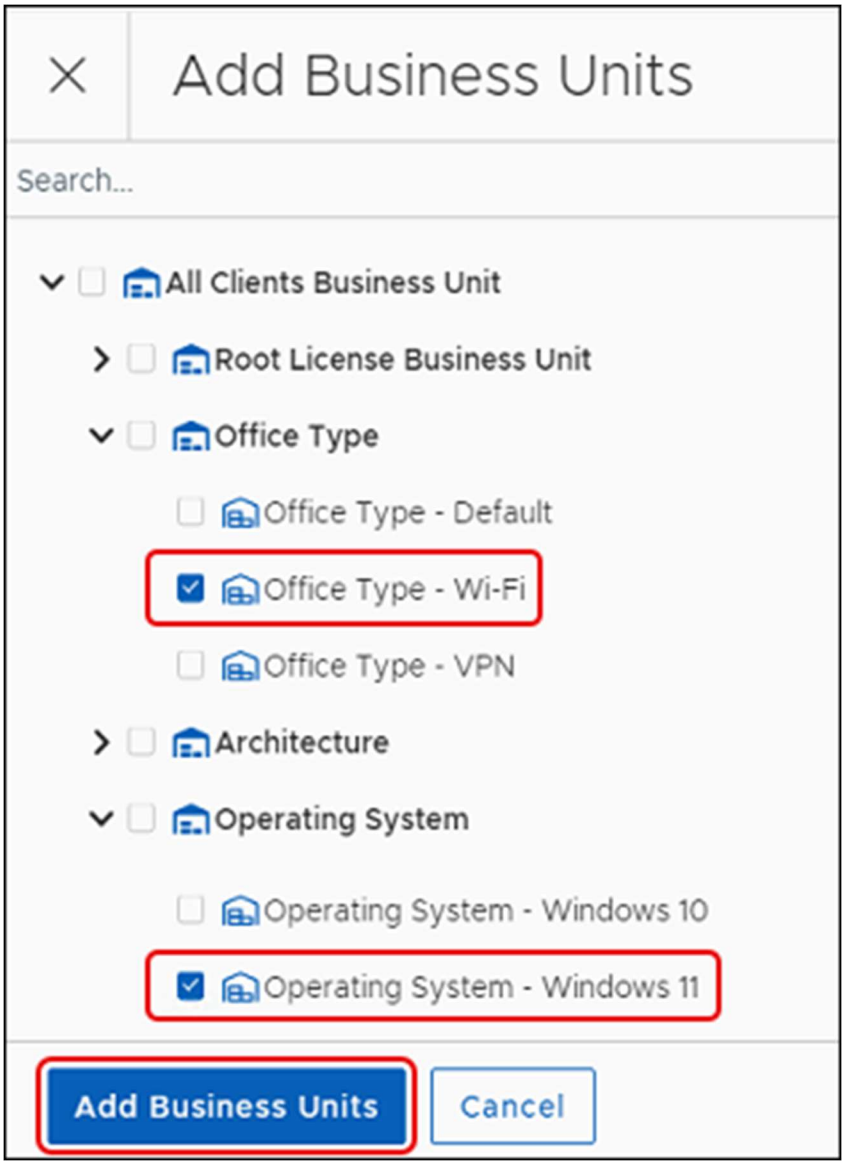
4. Add target Business Units for the Rollback to Version.

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.

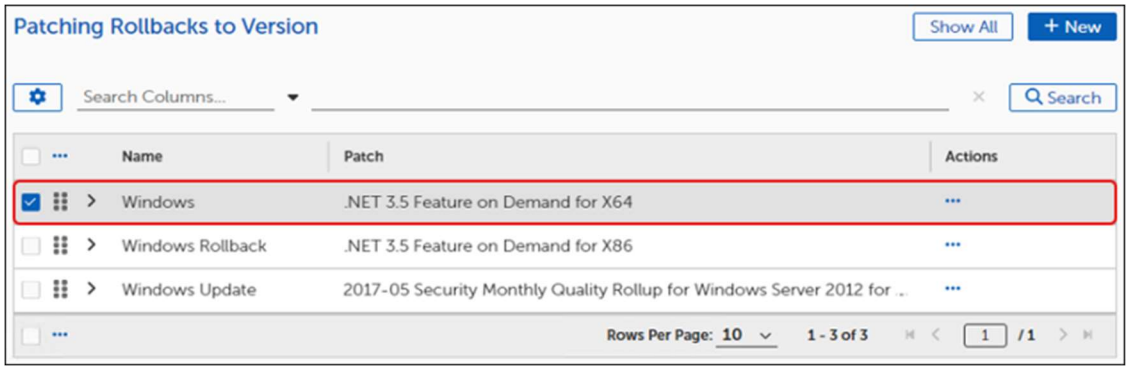


b. Select one or more **Business Units** to add, and then click **Add Business Units**.

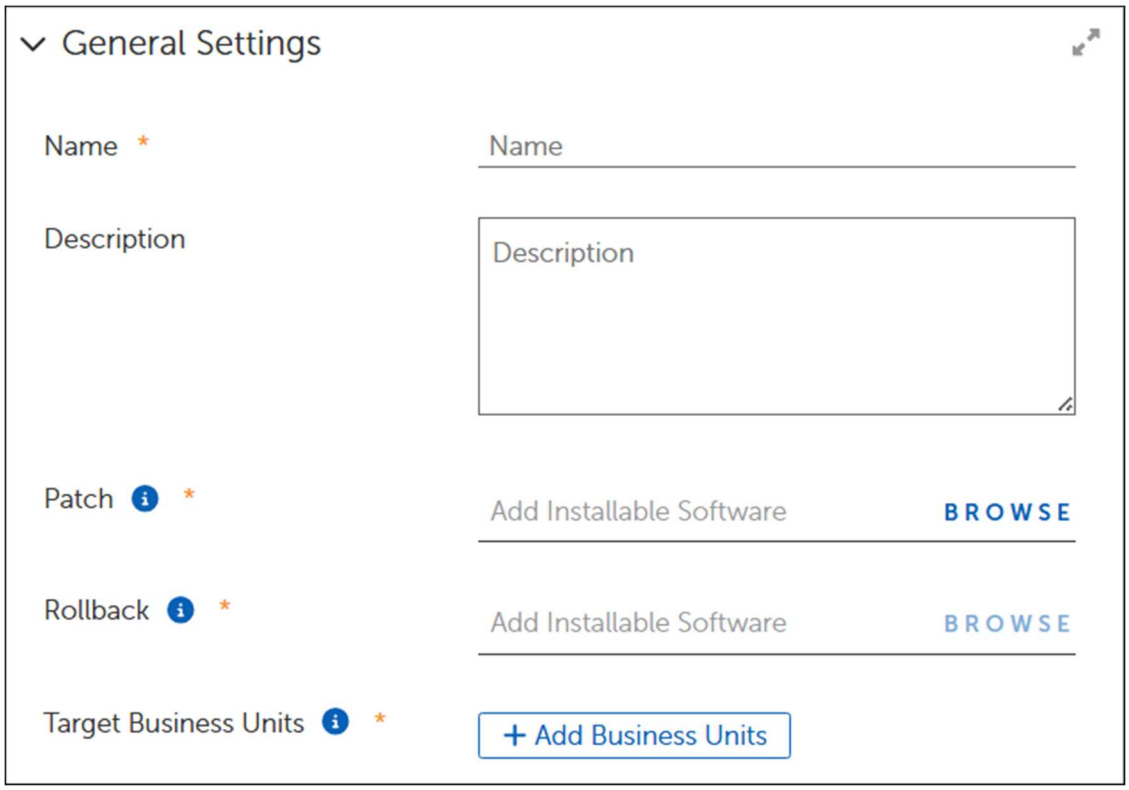
2. Select **Save** to rollback a patch to a prior version.

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.



This opens the template.



2. Modify the Rollback settings:

    a. Select **Browse** for Patch to choose a patch or release to roll back from.

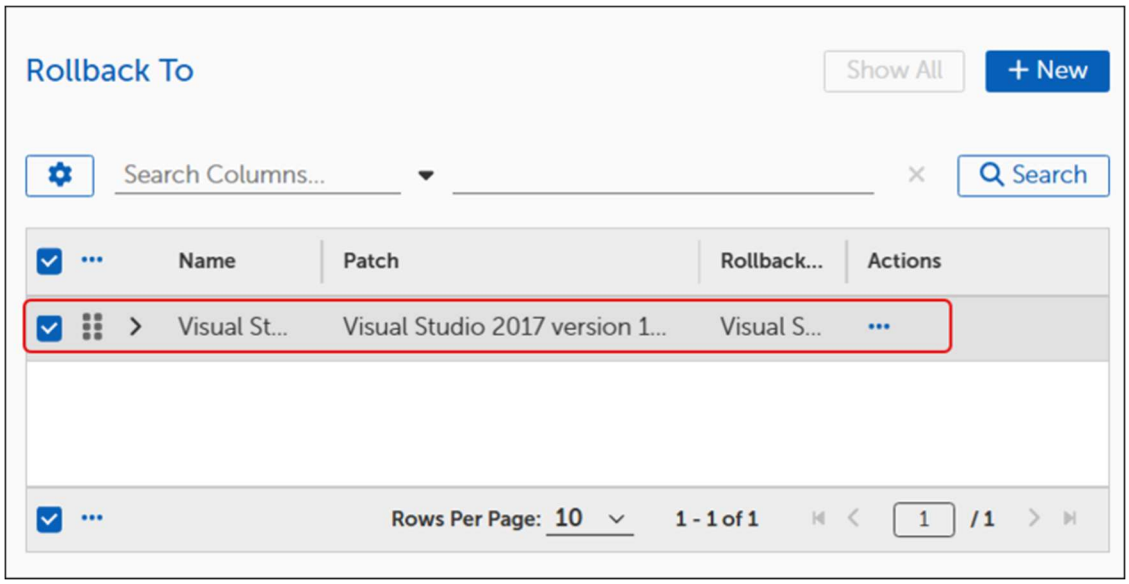
    b. Select **Browse** for Rollback to choose the version of the patch or release to roll back to.

    c. Select **+Add Business Units** to add or remove target devices.

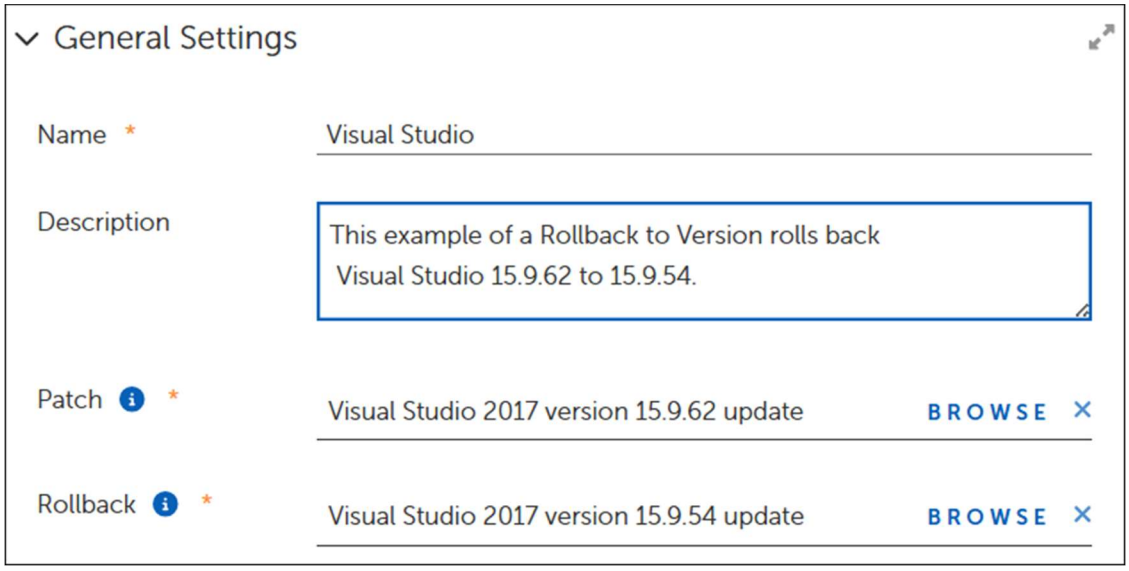
3. Select **Save** top-left corner of template to save the changes.

Copy a Rollback to Version Template

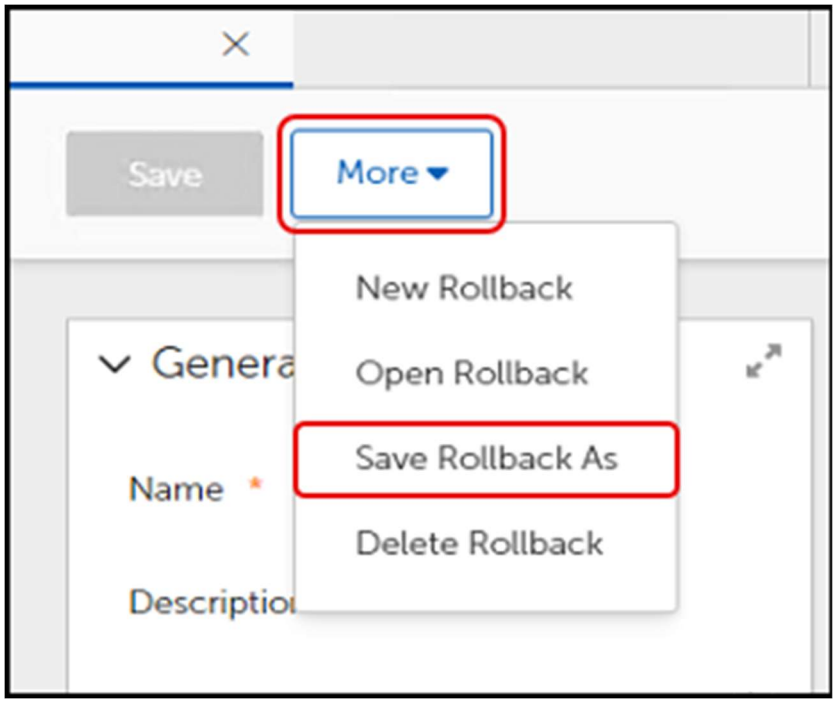
1. Select a **Rollback** template from the **Patching Rollbacks to Version** table of an open Patching Rollbacks template.



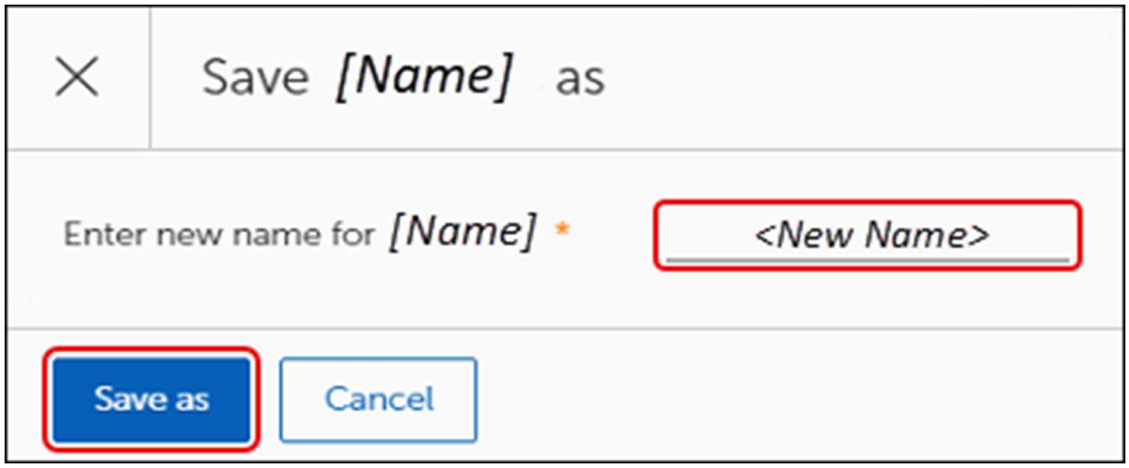
This opens the template.



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



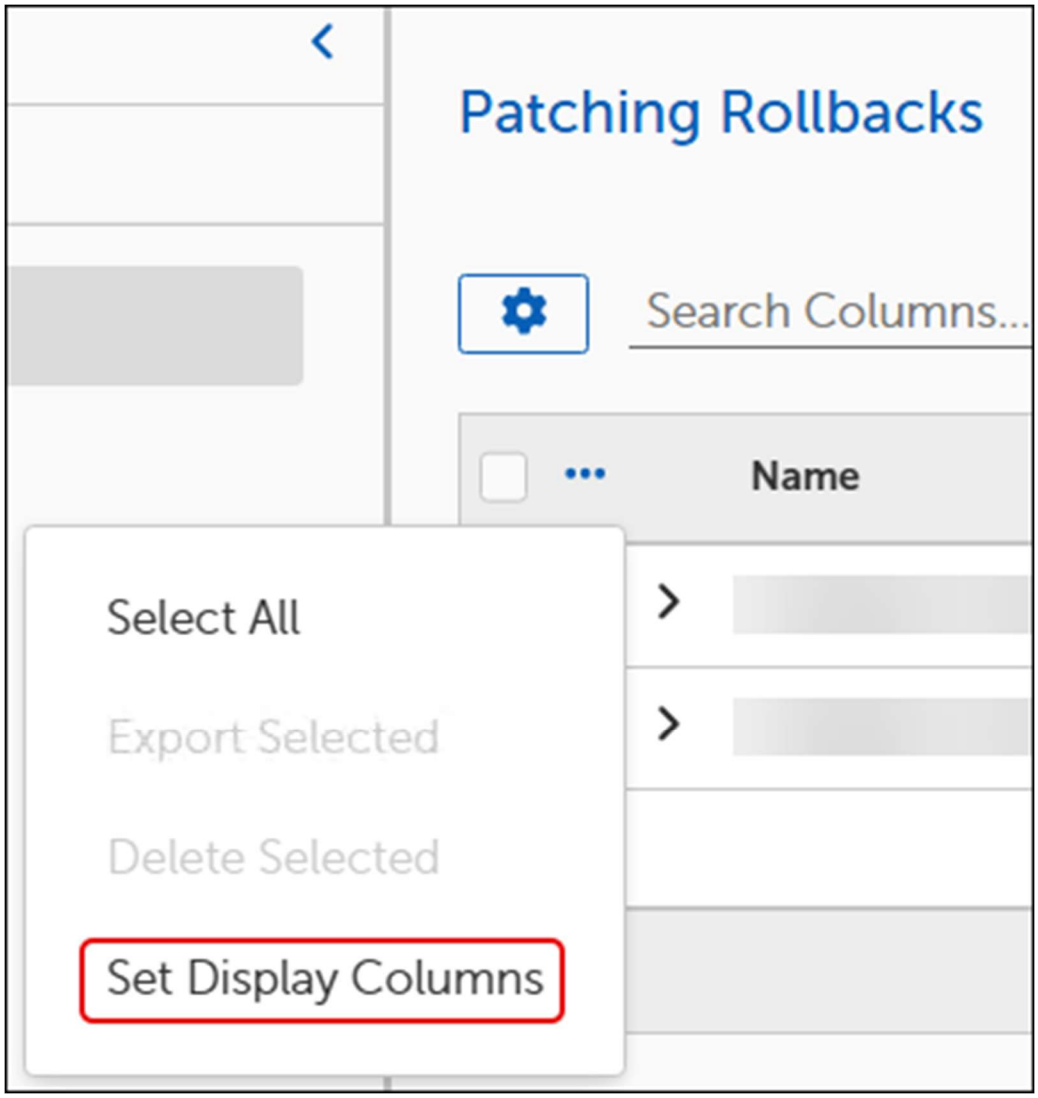
3. Enter a new **Name** for the template, and then click **Save as**.



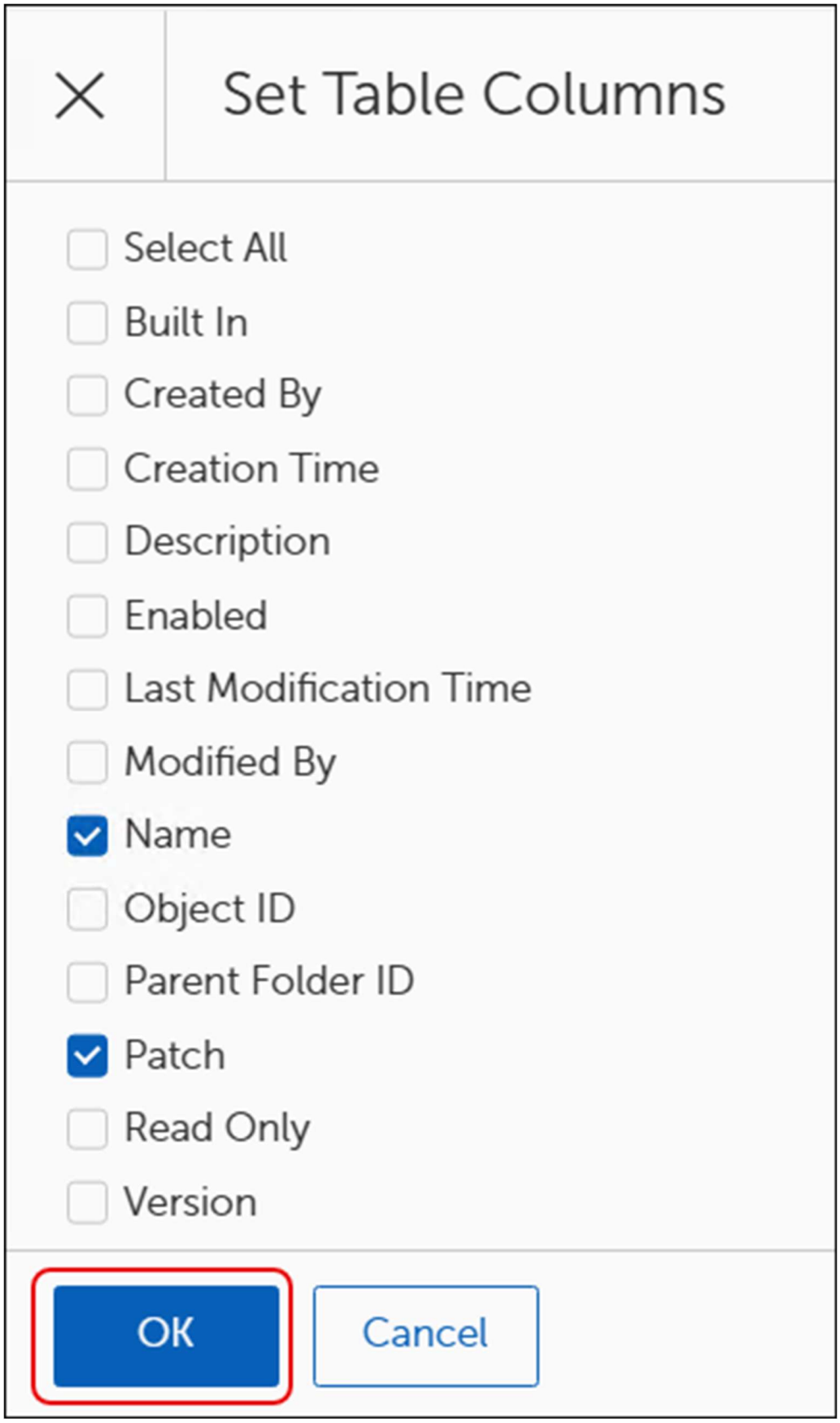
4. Revise the **Description** to reflect any changes needed for the copy, and then click **Save**.
5. Select **Back to Rollbacks** on the upper-left corner of the template to return to the **Rollbacks** table and view your changes.

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**.



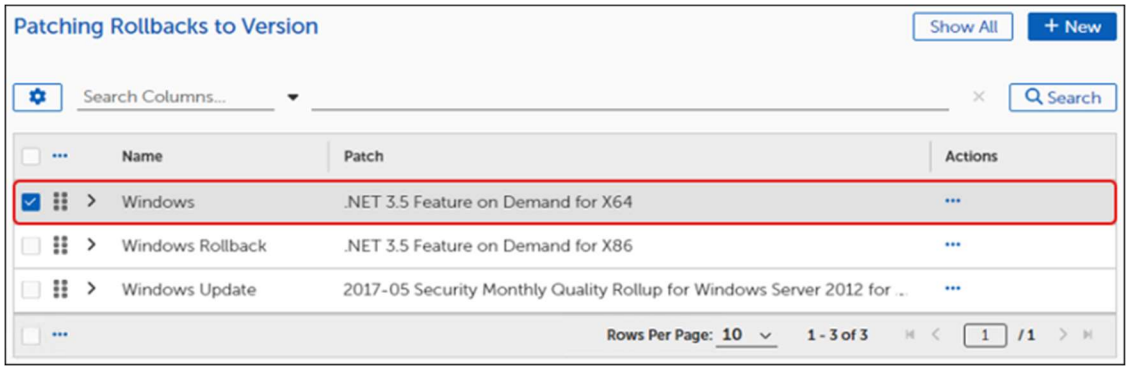
This opens the Set Table Columns dialog.



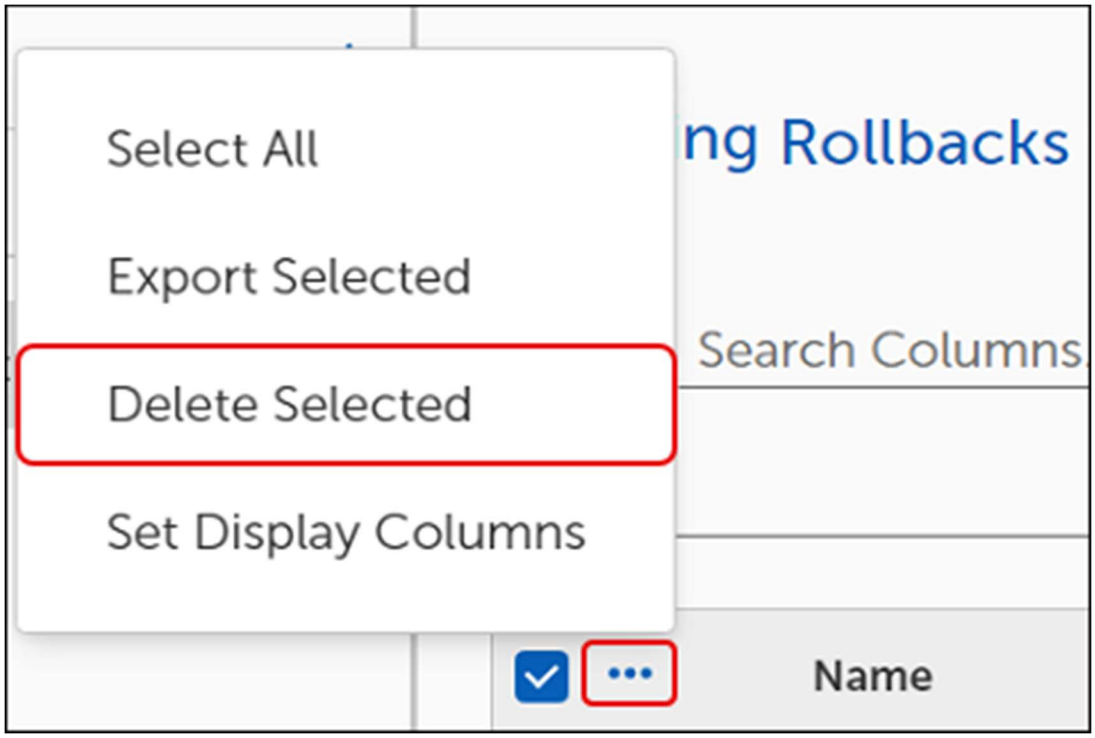
3. Select the **column names** you want the **Patching Rollbacks** table to display, and then click **OK**.

Delete a Rollback to Version

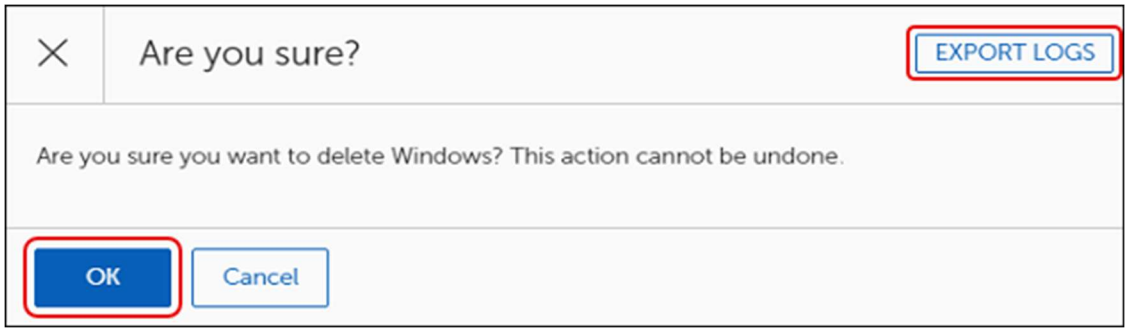
1. Select a **Rollback to Version** template from the **Patching Rollbacks to Version** table of an open Patching Rollbacks template.



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.

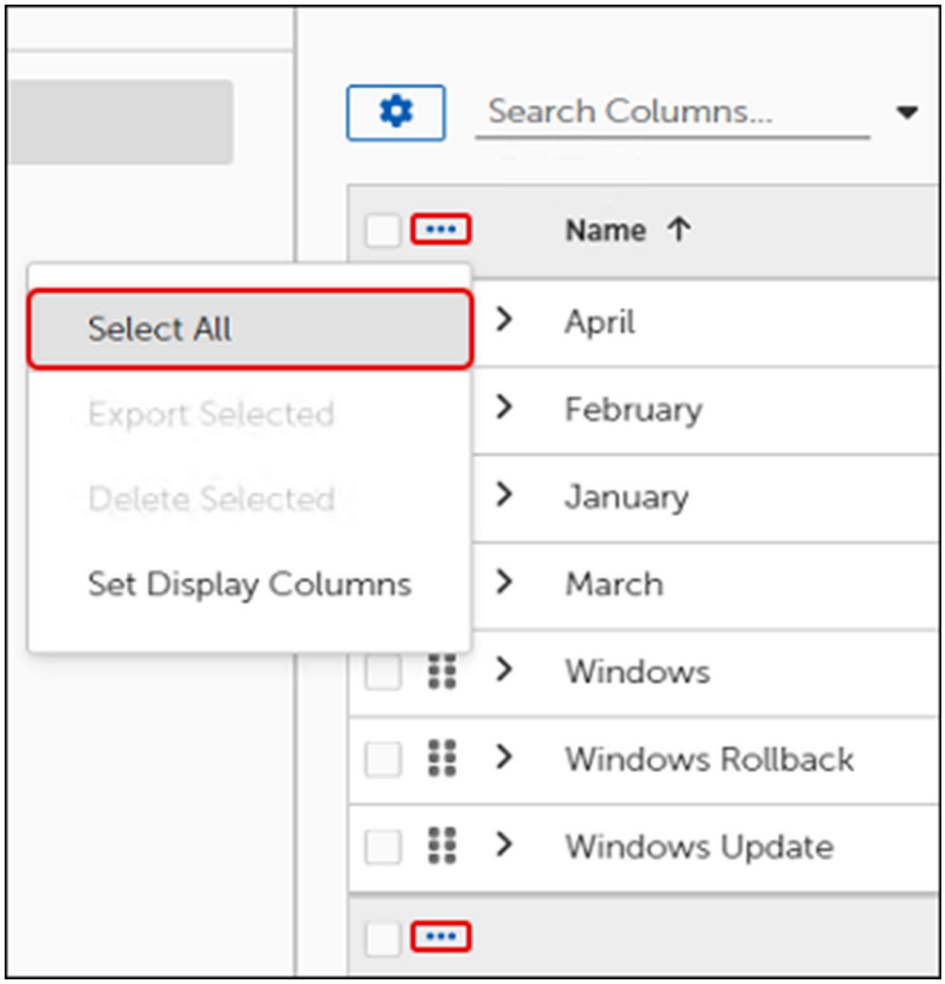
b. Select **OK** to delete the Rollback.

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.

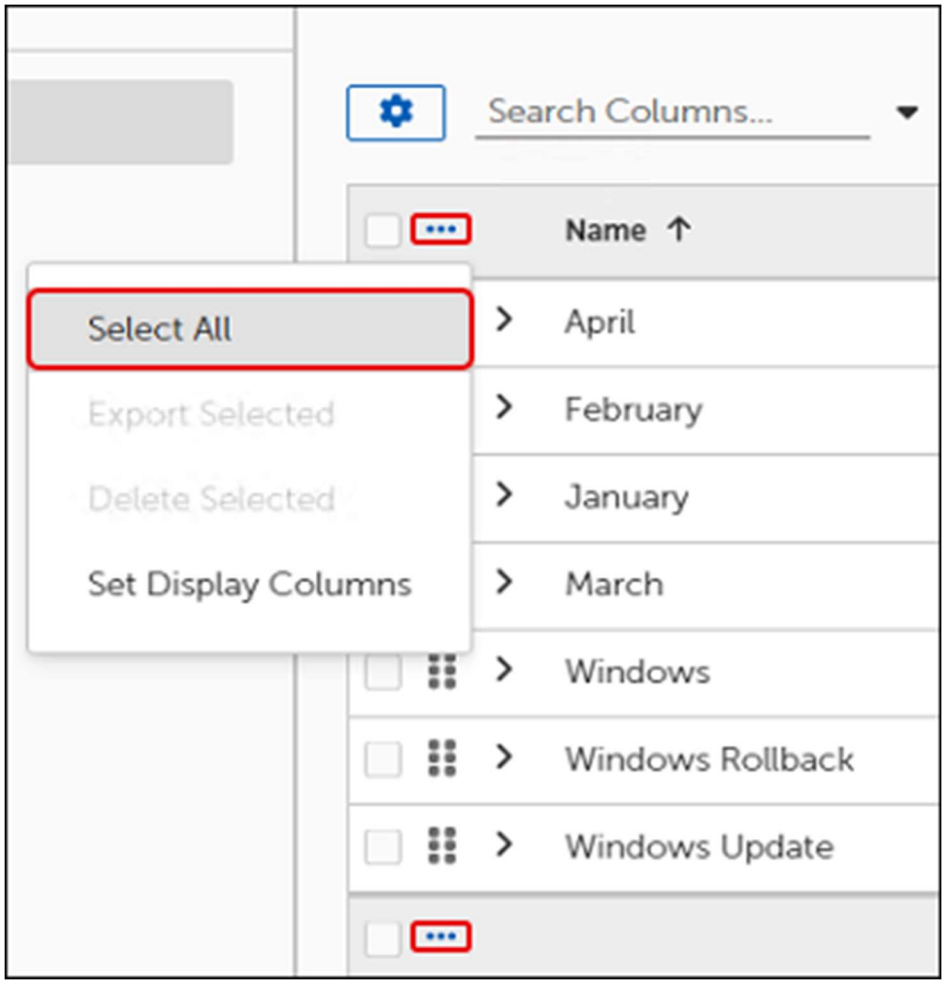
    b. To delete the Selected templates, see Bulk Delete Rollbacks.

    c. To customize the display columns of the Patching Rollbacks table, see Customize Patching Rollback Table Settings.

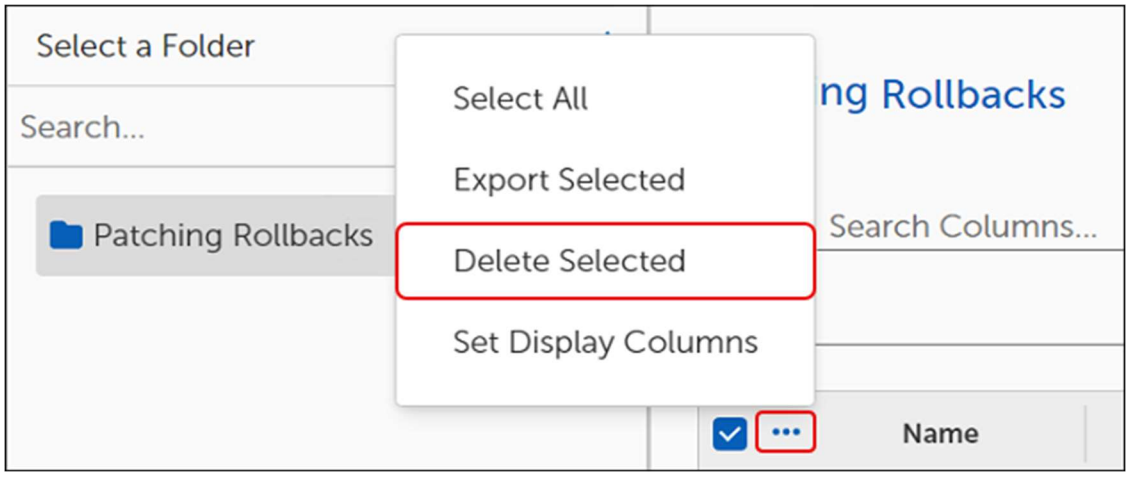
Bulk Delete Rollback to Version

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

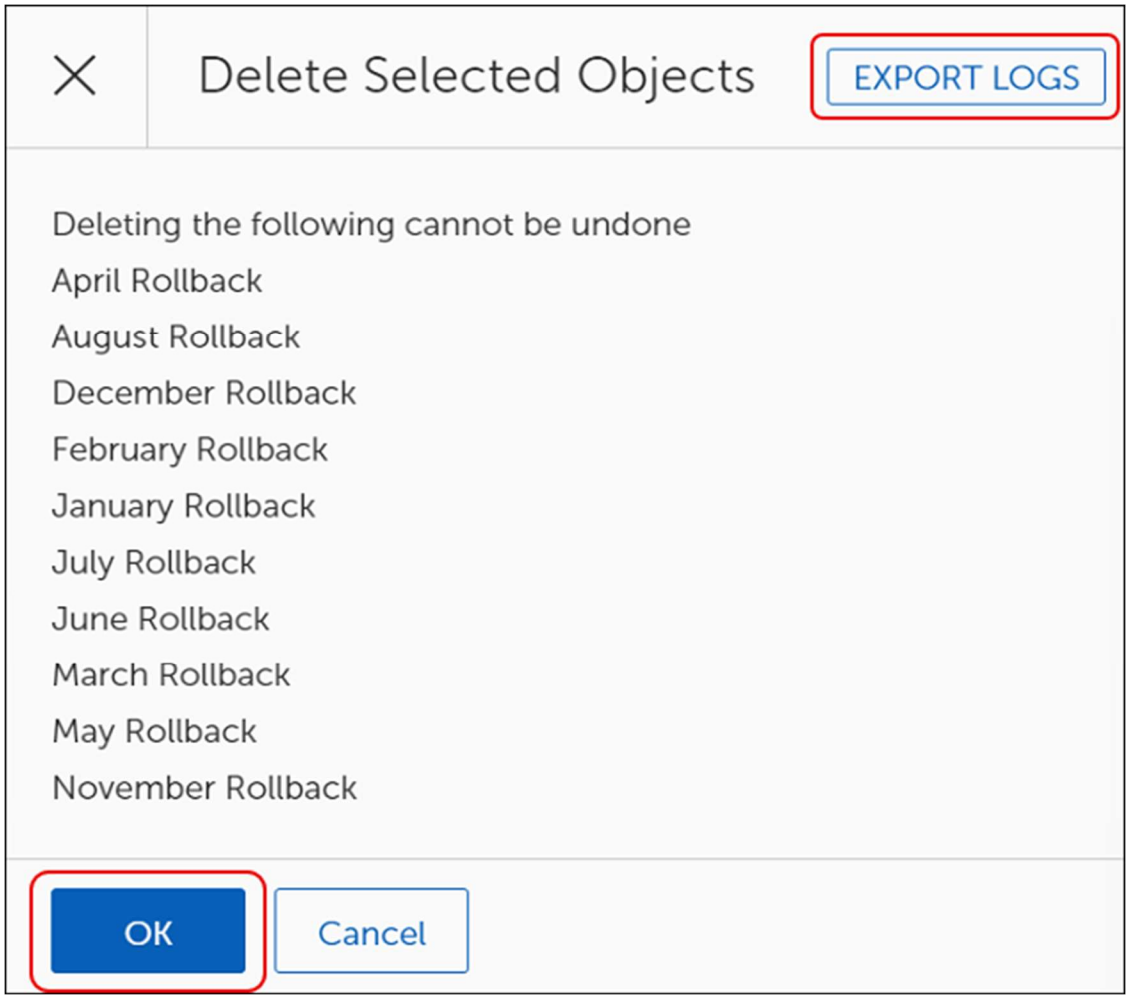
1. Open the **Patching Rollbacks** table (**Flex Controls > Rollbacks > Rollback to Version**).
2. Select the **ellipsis (...)** next to Name, and then click **Select All**.



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



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



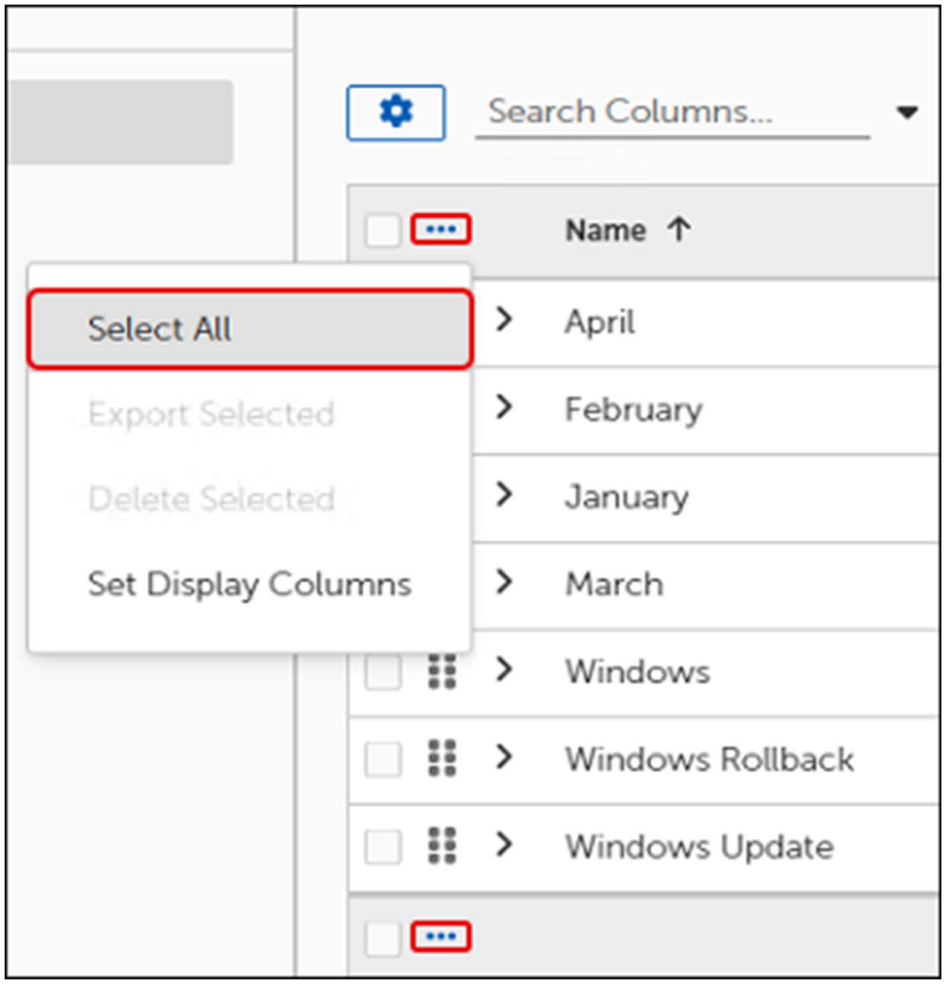
4. (Optional) Select **Export Logs** on the top-right corner of the **Delete Selected Objects** dialog to export trace logs. The trace logs download to your device as a file with a .log extension.

5. Select **OK** to delete the Rollbacks. This returns you to the **Patching Rollbacks to Version** table where the deleted Rollbacks no longer appear.

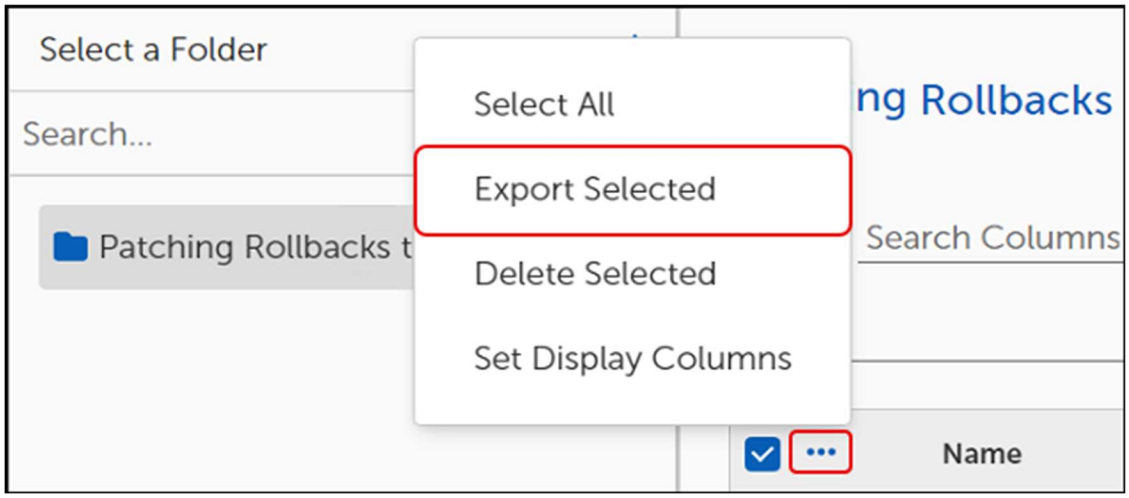
Export Rollback to Version

1. Open the **Patching Rollbacks** table (Flex Controls > Rollbacks > Rollback to Version).

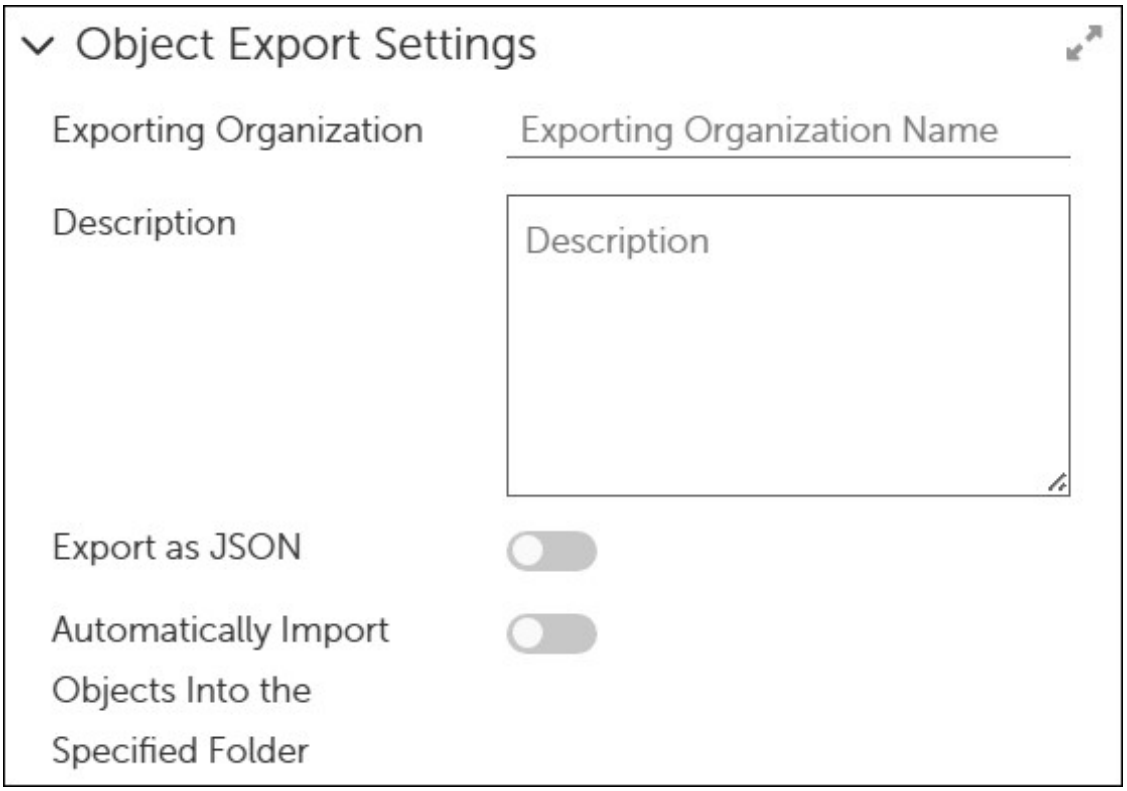
2. Select a single **Patching Rollback** from the table, or click the **ellipsis (...)** next to Name, and then click **Select All** to export all Rollbacks



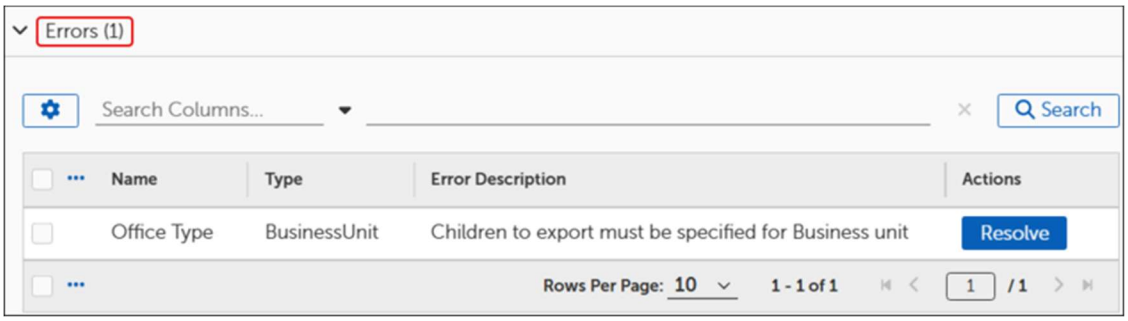
3. Select the **ellipsis (...)** next to Name again, and then click **Export Selected**.



This opens the **Object Export Settings**:



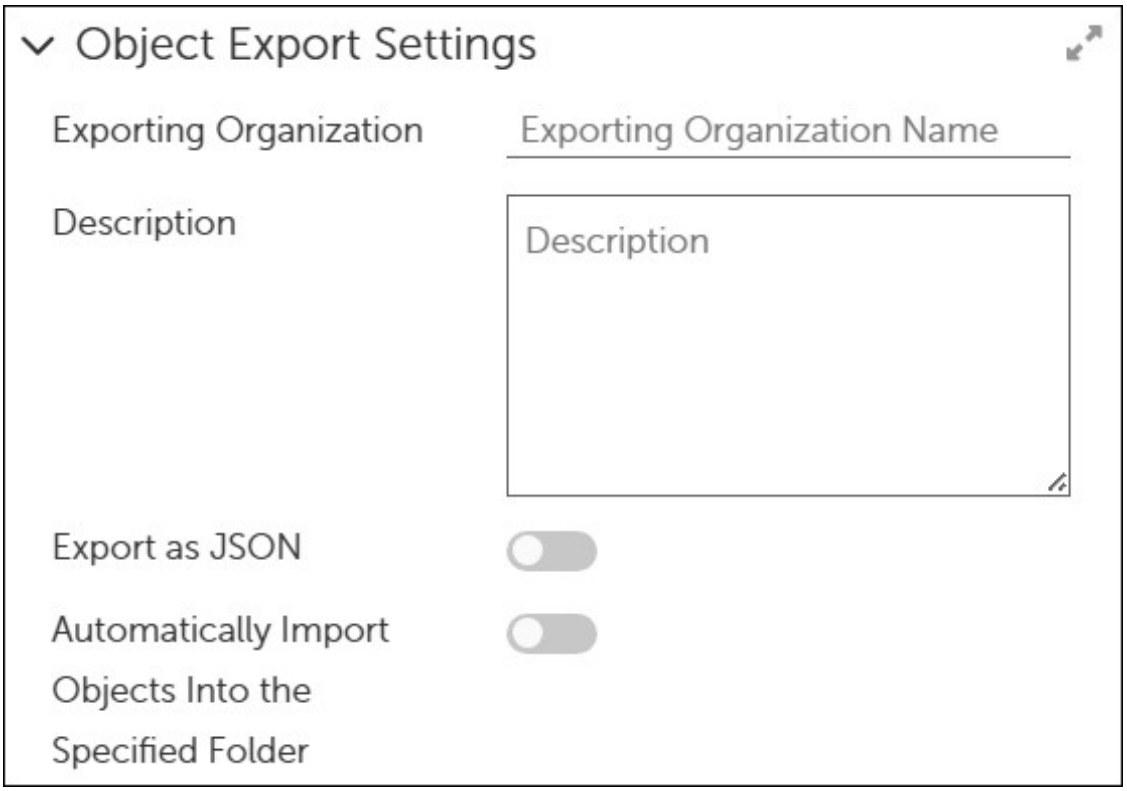
If Object Export Settings command returns an error similar to the following, see /document/preview/14345#UUID-8dd1ad08-6239-39ed-d91e-18e39741627c errors:



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.



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.

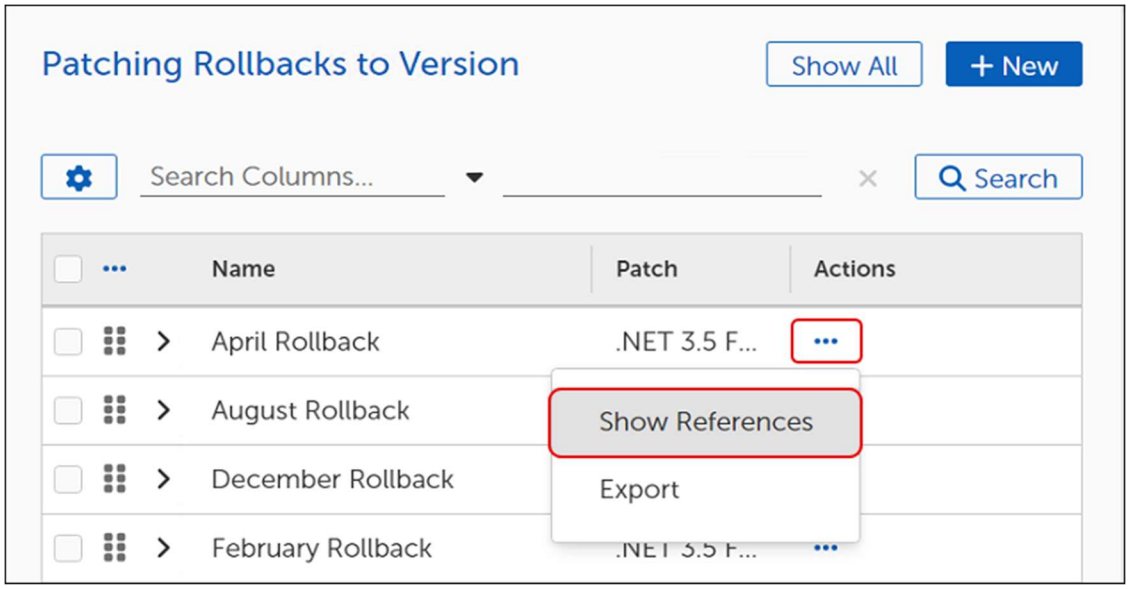
Important

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

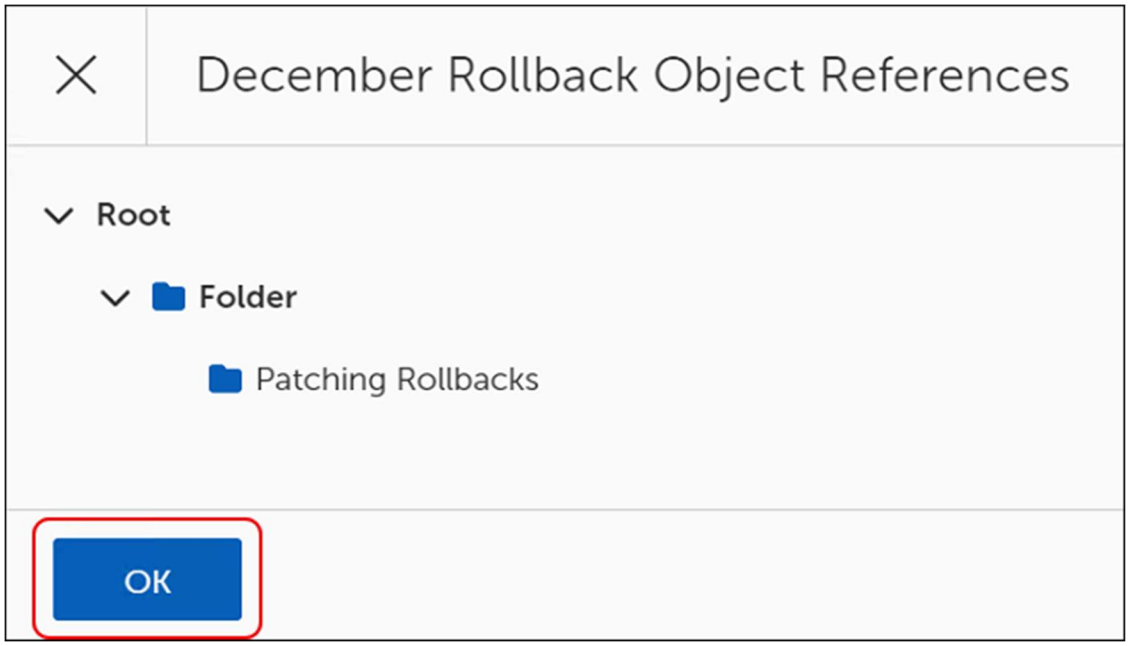
Show Rollback to Version References

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**.



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



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

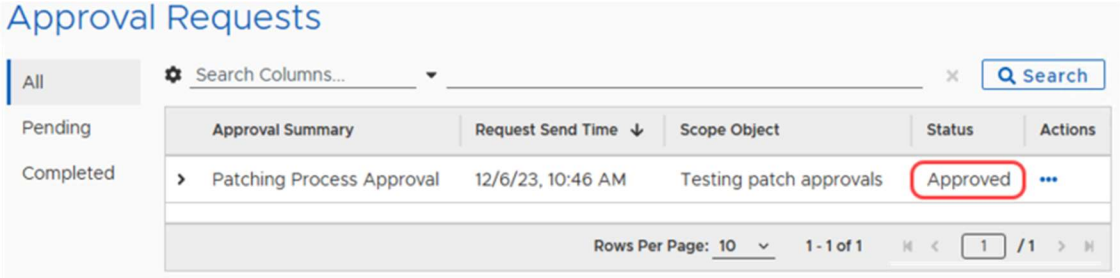
Some Patching Strategies require patch manager approval before beginning a patch cycle. The Patching Process looks for an Approval Chain to use when processing approvals and sends notification based on the communication process configured for each approver.

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

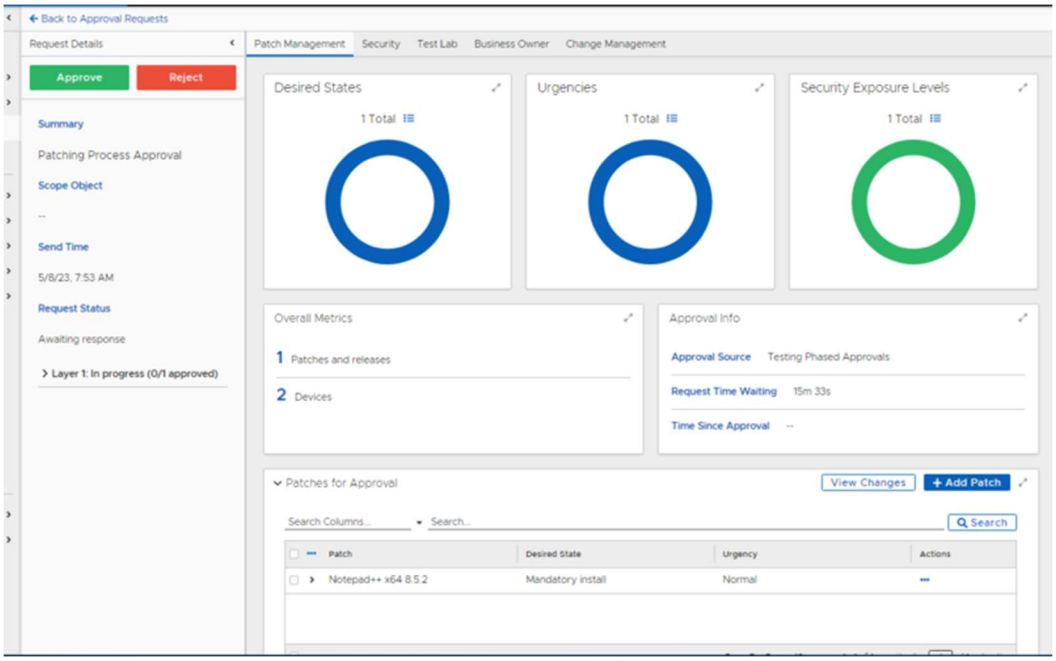
Administrators may see all pending and completed Approvals using the Tenable Patch Management dashboard.

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.

Risk Assessment Settings

Use Risk Assessment settings to customize risk calculations and display risks in other dashboards. The weight and formula information listed below is also available from the **Risk Assessment Settings** dialog under **Risk Assessment Info** in the upper right corner.

- Exposure Level Weight:
    a. Low = 0
    b. Medium = 33
    c. High = 66
    d. Critical = 100
- Exploit Exists Weight
    a. False = 0 (exploit does not exist)
    b. True = 100 (exploit exists)
- Product Criticality Rating Weight

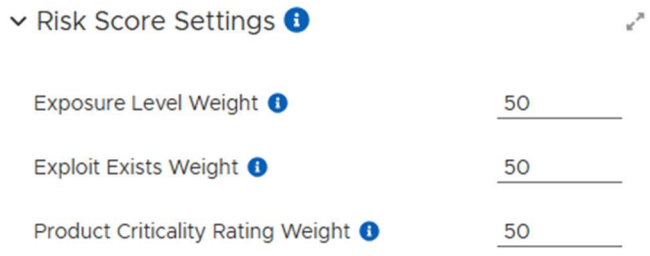
Use the default setting or set custom criticality by product. See *Custom Risk Settings*.

The Risk Assessment Score calculation uses the following formula:

((ExposureLevelValue * ExposureLevelWeight) + (ExploitExistsValue * ExploitExistsWeight) + (CriticalityValue * CriticalityWeight)) / (ExposureLevelWeight + ExploitExistsWeight + CriticalityWeight)

Risk Score Settings

The Risk Assessment Score calculation uses a weighted average of three aspects of software security listed below. Each uses an assigned weight between 0 – 100. The default value for each weight is 50.

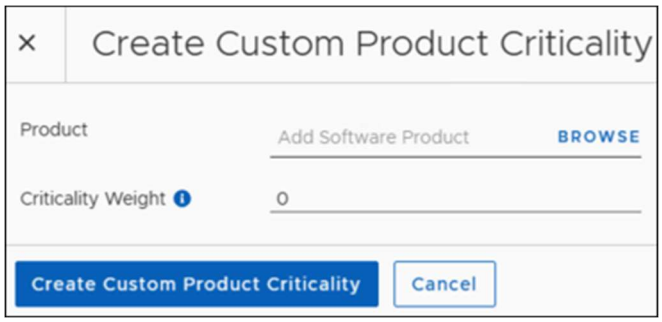


Custom Risk Settings

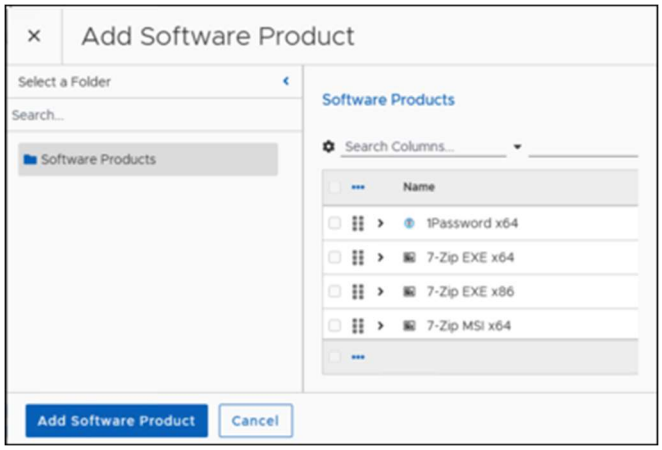
Use these settings to create settings that override the default settings defined in the metadata for Product Criticality settings or to create Custom Risk Scores.

Create Custom Product Criticalities

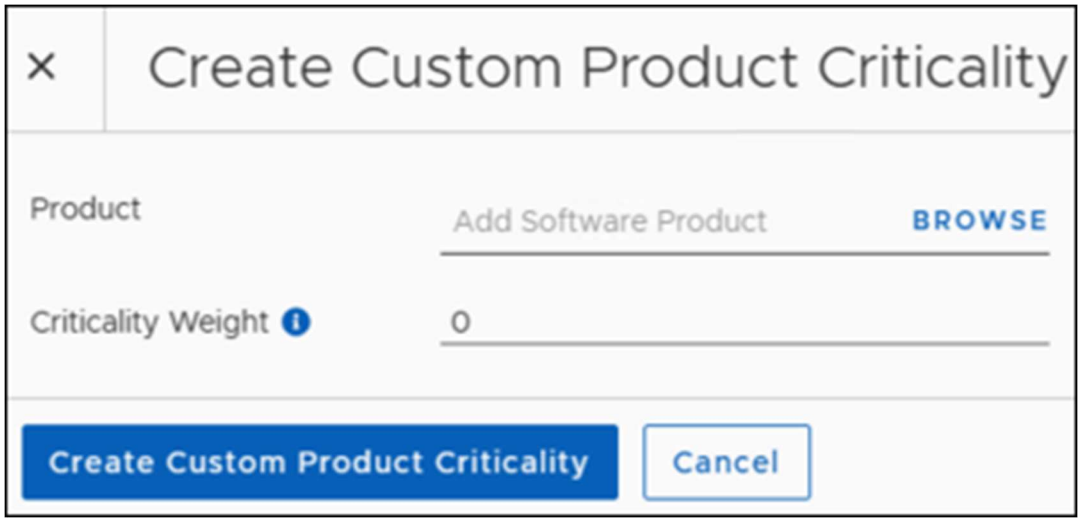
1. Select **+ Create Custom Product Criticality** in the **Custom Risk Settings** box. This opens the **Create Custom Product Criticality** dialog.



2. Select **Browse** to search for the product you want to customize.

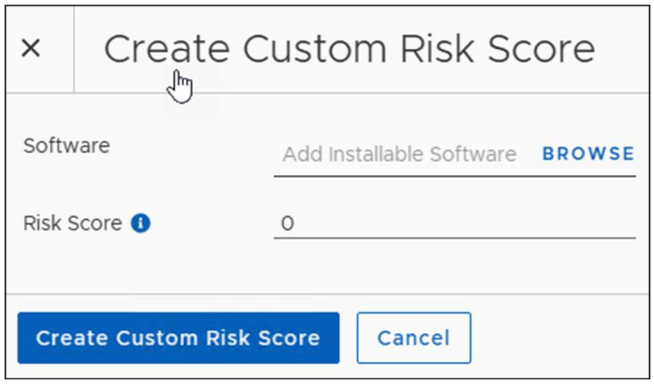


3. Select the product to modify, and then click **Add Software Product**.
    a. This adds a table to **Custom Product Criticalities**.
    b. Each time you add another product, the added information appears in this tabl
4. Enter the number that corresponds to the criticality weight you want to set for this product, and then click **Create Custom Product Criticality**.



Create Custom Risk Scores

1. Select **+ Create Custom Risk Score** in the **Custom Risk Settings** box of Risk Assessment Settings. This opens the **Create Custom Risk Score** dialog.

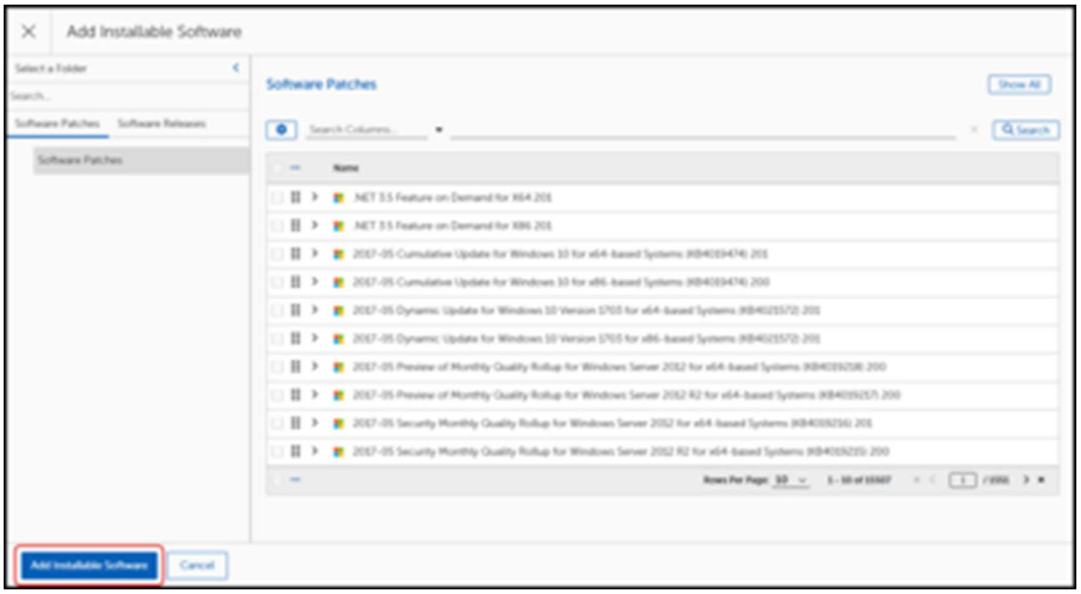


2. Select **Browse** to open the **Add Installable Software** dialog.

    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. Enter the number that corresponds to the risk score you want to set for this product, and then click **Create Custom Risk Score**.

    c. This adds a table to **Custom Risk Scores**.

    d. Each time you add another product, the added information appears in this table.

4. Select **Save Settings**.

Content Prestaging Settings

The Content Prestaging feature enables Tenable Patch Management to provide deployment content to devices ahead of the scheduled deployment, either pushing content to a location or allowing a client to pull content. Prestaging content makes the content available on the device locally when the deployment time arrives. This reduces the deployment time and minimizes the chances of missing service windows or having devices going offline before a content download finishes.

You can create Content Prestaging Settings within the Patching Strategy, Business Unit, or Deployment Channel templates.

Defining Content Prestaging Settings

The templates for Patching Strategies, Deployment Channels, and Business Units include the choice to set Content Prestaging settings. Settings default to **Not Enabled**.

Content Prestaging settings include two options:

- **Server Content Push (Recommended)** – The Tenable Server pushes the content to the best-suited sources in all locations that require the content. Tenable recommends this type of prestaging when the Deployment Strategy targets only a subset of devices. High-availability machines receive the content and function as local sources during discovery and deployment.
- **Client Content Pull** – This option enables any client that requires the content to download and cache it before deployment. Suitable when a Deployment Strategy targets all clients that need the updated content.

Push Content

- **Not Enabled** -- Disables any prestaging as part of the Patching Process workflow or Patching Strategy.
- **Handled by System** – The Tenable Patch Management system handles the prestaging automatically and pushes content to three automatically chosen devices within the office that require the content.

  This push occurs at once when the metadata updates include the latest content that meets patching requirements.
- **Handled by Workflow** – When enabled as part of a Patching Process, Deployment Channel, or Business Unit template, pushes the content upon deployment of the Patching Process.

Pull Content

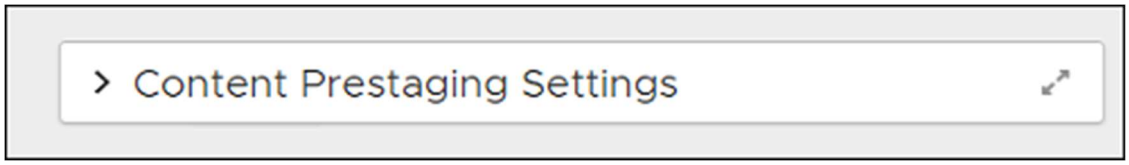
- **Not Enabled** -- Disables any prestaging as part of the Patching Process workflow or Patching Strategy.

- **Handled by System** – The Tenable Patch Management system handles the prestaging automatically. The Client pulls content from the Server and instructs all Clients that require the content to download and cache it ahead of any deployment.
- **Handled by Workflow** – When enabled as part of a Patching Process, Deployment Channel, or Business Unit template, the Client pulls the content upon deployment.

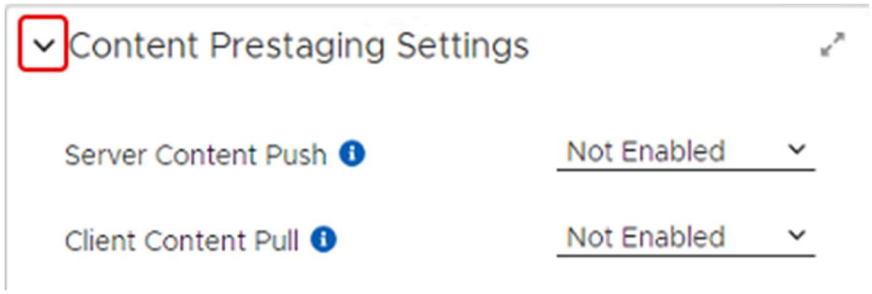
Set Content Prestaging Settings

Use this procedure to add or change Content Prestaging Settings in Patching Strategy, Business Unit, or Deployment Channel templates.

1. Expand the **Notifications** box in an open object template, and then scroll down to the Content Prestaging Settings.



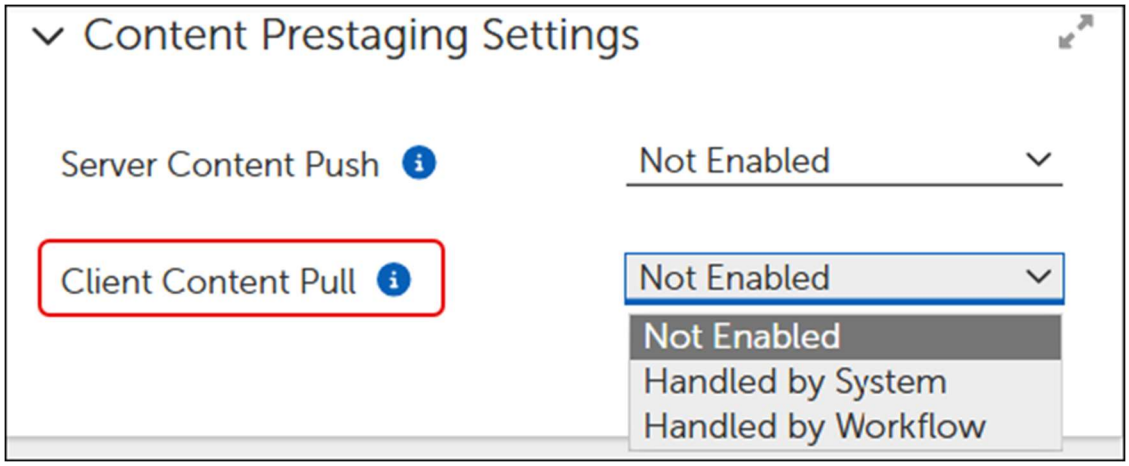
2. Expand the Content Prestaging Settings box to view the available settings.



Enable Client Content Pull

Client Content Pull defaults to Not Enabled. To enable pull settings, complete the following steps in the Content Prestaging Settings of a Patching Strategy, Business Unit, or Deployment Channel template:

1. Select the arrow to the right of **Client Content Pull** to expand the menu of available options.



2. Select the option you need for the object template you are using. For definitions of push options, see Defining Content Prestaging Settings.

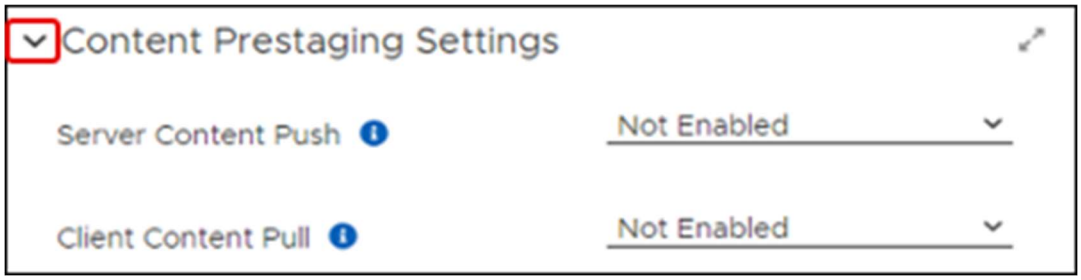
3. Select **Save** on the upper left to save your changes:

    a. Check the **Error View** and resolve any errors.

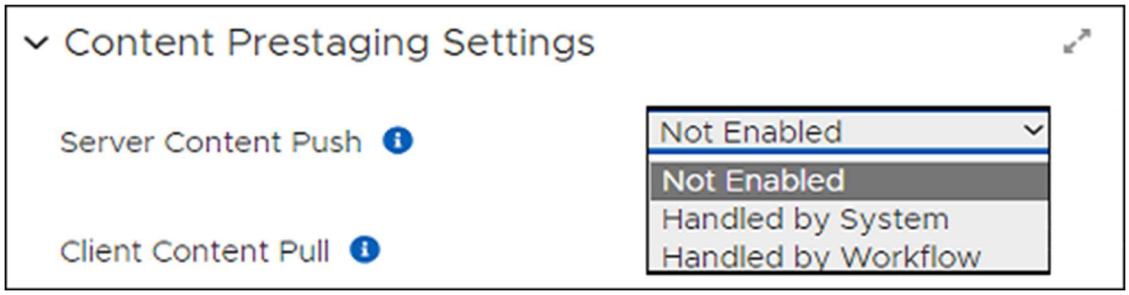
    b. Select **Save** again if you make any changes.

Enable Server Content Push

Server Content Push defaults to Not Enabled. To enable push settings, complete the following steps in the Content Prestaging Settings of a Patching Strategy, Business Unit, or Deployment Channel template, complete the following steps:



1. Select the arrow to the right of **Server Content Push** to expand the menu of available options.



2. Select the option you need for the object template you are using. For definitions of push options, see Defining Content Prestaging Settings.

3. Select **Save** on the upper left to save your changes:

    a. Check the **Error View** and resolve any errors.

    b. Select **Save** again if you make any changes.

Customer Extension Data

Customer Extension Data is an advanced feature of Tenable Patch Management. The Customer Extension Data fields allow advanced users to specify different key/value pairs for use in customized Patching Strategies, Deployment Chains, or Business Units when necessary to achieve different results.

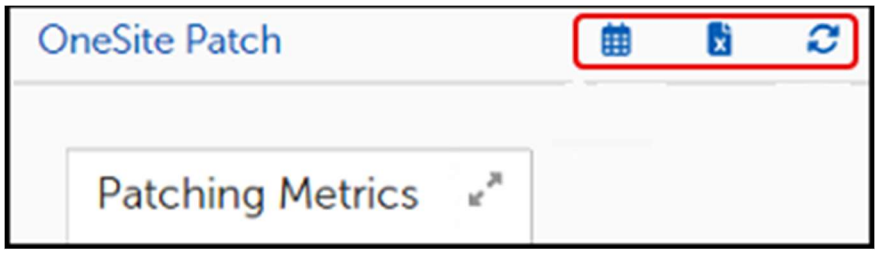
Customer Extension Data fields relate directly to fields in a customized template. If you do not have customized templates with key/value pairs you can modify, you do not need to configure or use this feature.

If you want to create customized templates that use key/value pairs for some settings, contact Tenable Customer Support.

Navigating the Tenable Patch Management Dashboard

Date Settings, Export, and Refresh

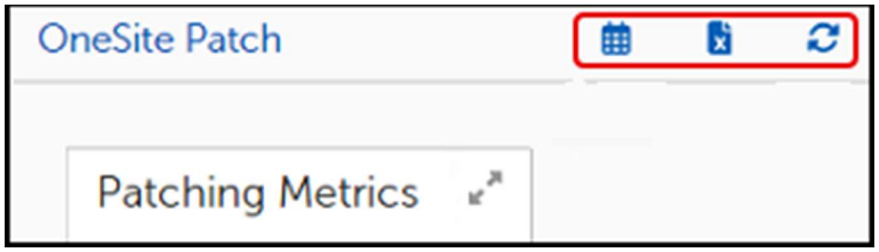
The three small icons (Calendar, Export and Refresh) on the upper right of the Tenable Patch Management Home page and on any of the Patching Analytics pages (Overview, Products, Patches, or Devices) provide options to customize the date settings to a particular date range, choose some or all widgets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



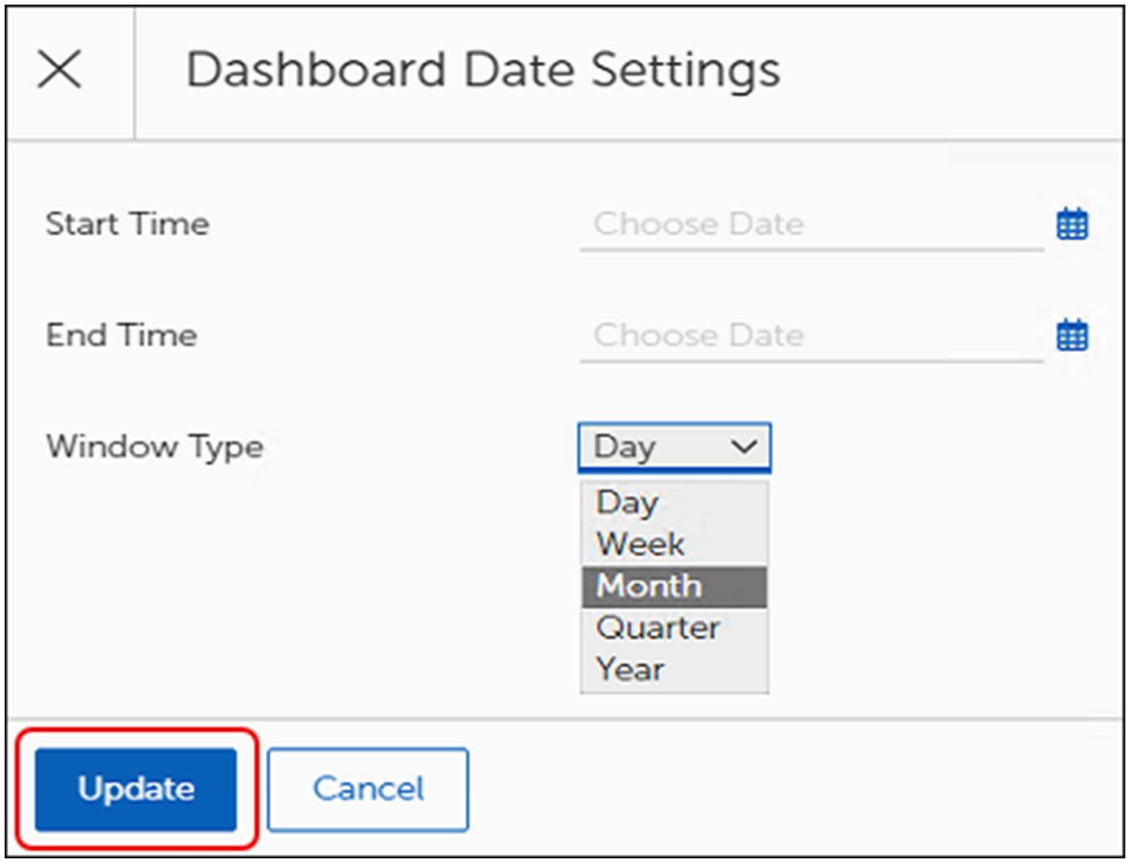
Set Dates for Status Views

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.

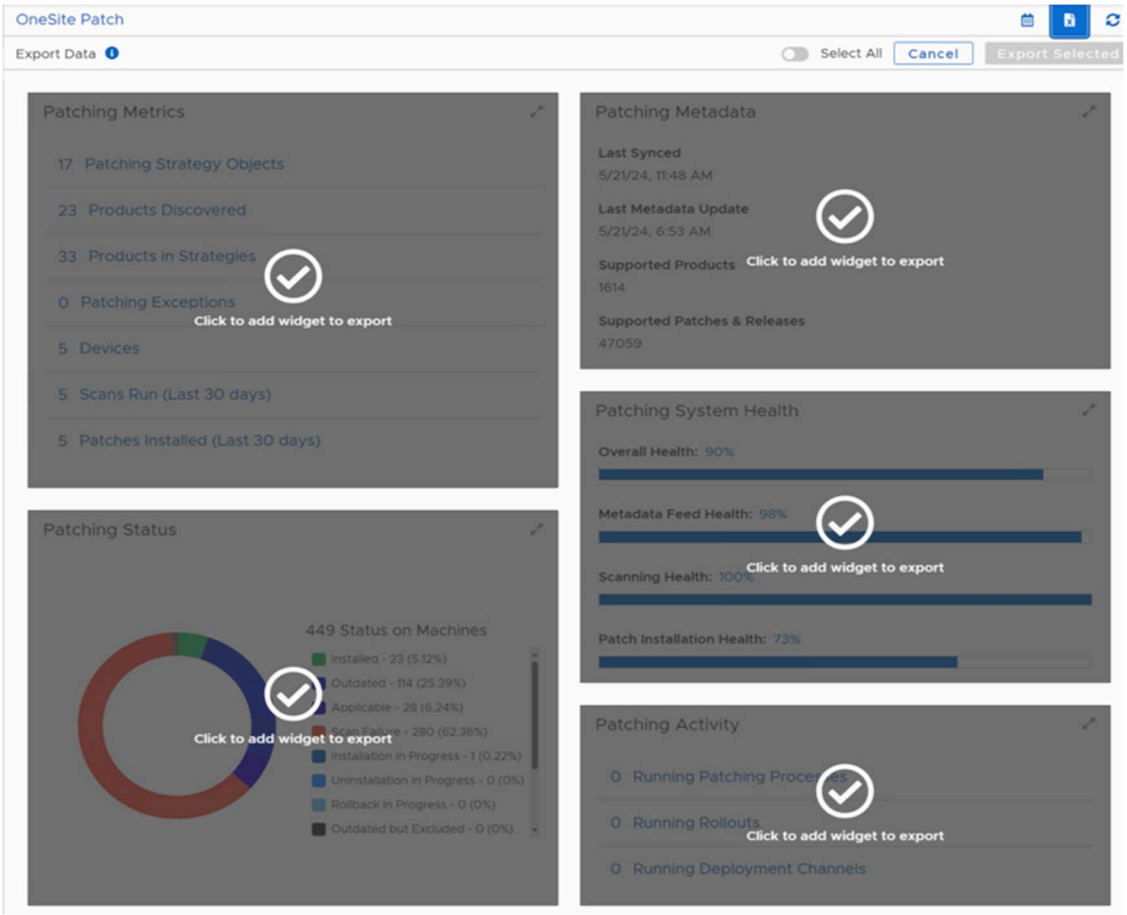


3. Select the **Window Type** setting, and then select whether to view data by **Day**, **Week**, **Month**, **Quarter**, or **Year** from the dropdown menu.

4. Select **Update** to save the settings. The view details update automatically for the date range you entered.

Export Widget Data

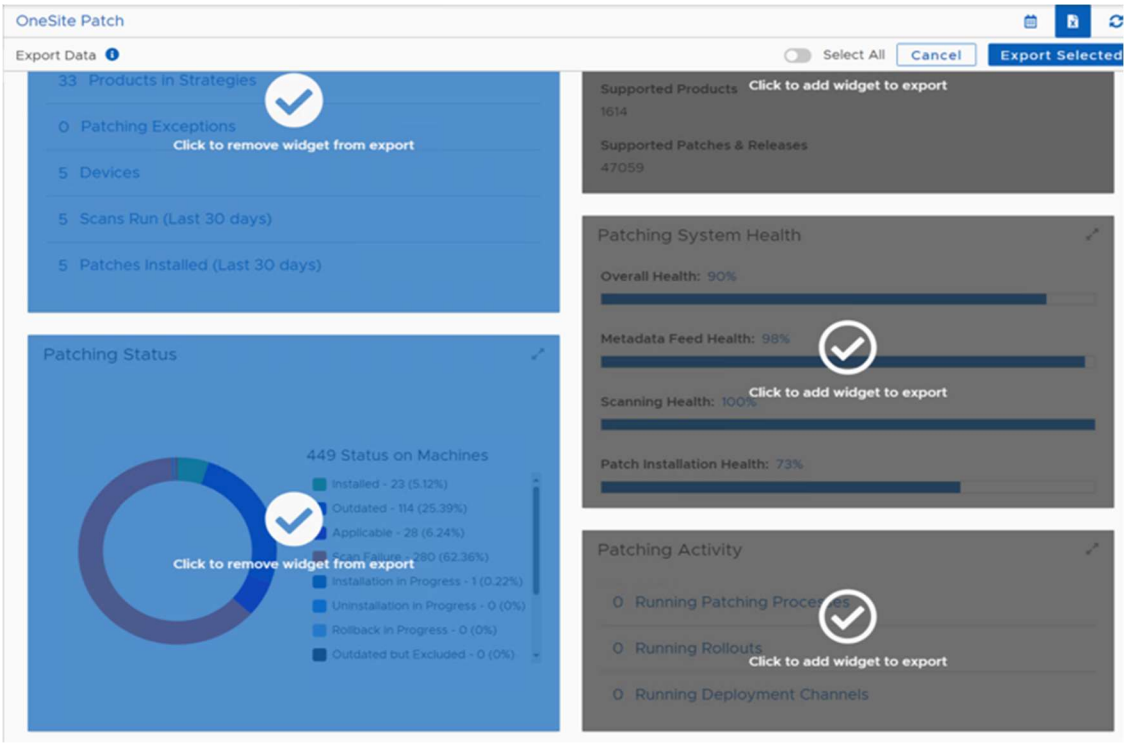
1. Select the Export icon on the upper-right corner of the **Home** page or on any **Patching Analytics** page. This changes the view to an **Export Data** page, which highlights in gray the widgets you can export.



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.

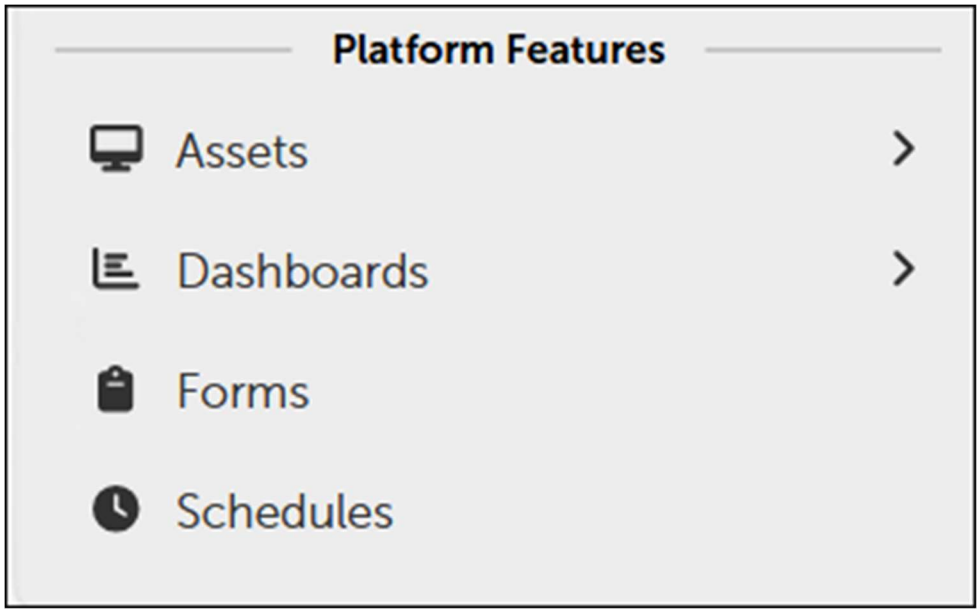
Tenable Patch Management Menus

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.

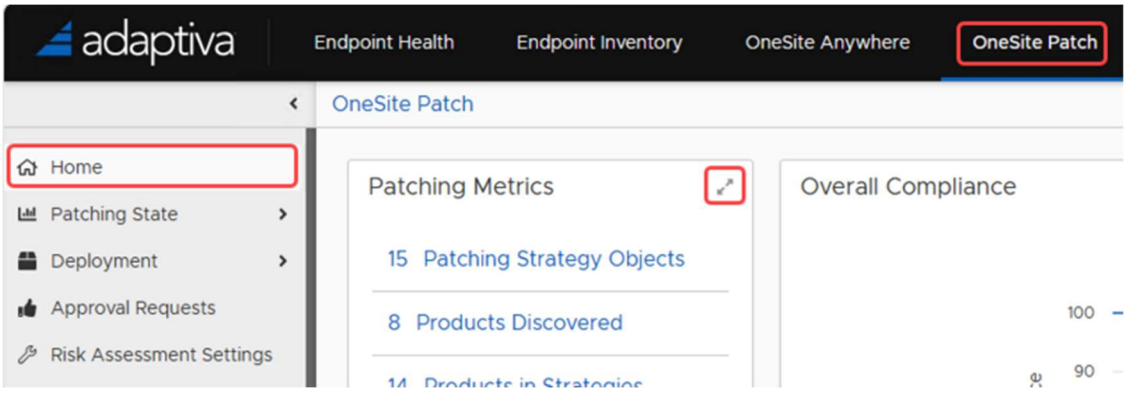
Platform Features Menu

These are common features available from every menu in Tenable Patch Management.



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.



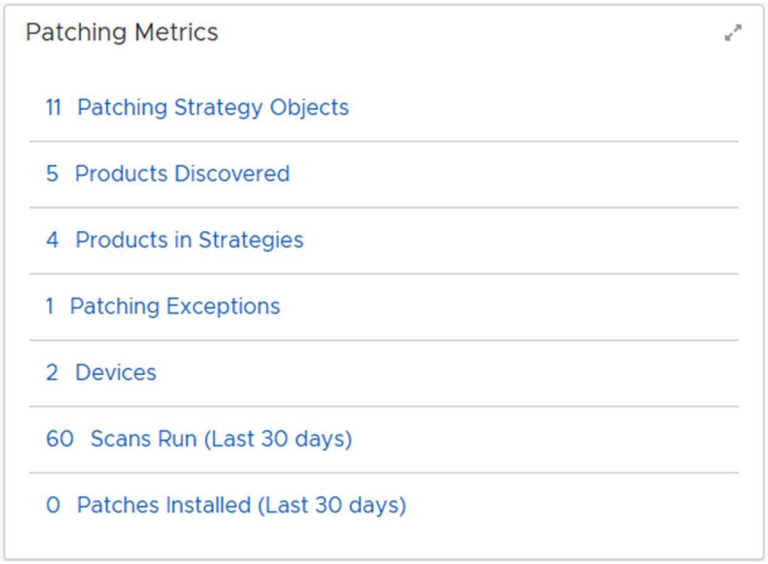
The layout of these widgets depends on the size of your computer monitor.

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

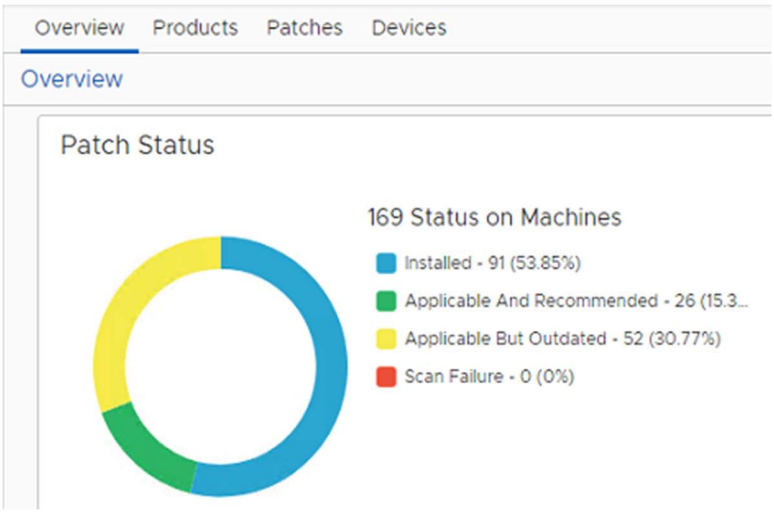
Accessed from the **Home** screen, **Patching Metrics** show basic patch related information specific to your environment based on scanning requirements. Details include a quantitative summary of

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**.



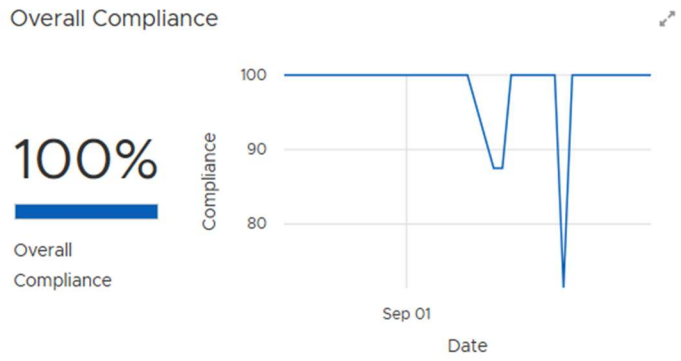
Patching Status

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.



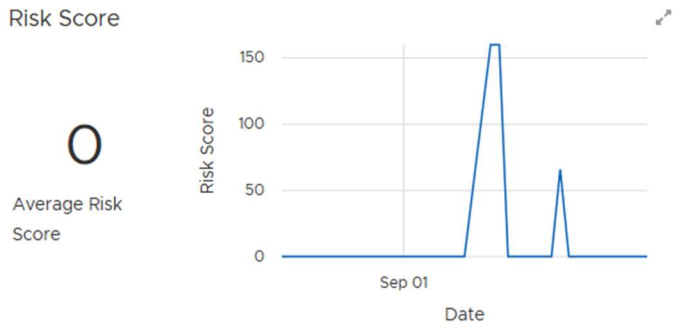
Overall Compliance

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



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.



The average number reported here reflects a customized risk assessment for each product based on patch status, applicability, and weight of risk. See Risk Assessment Settings for more information.

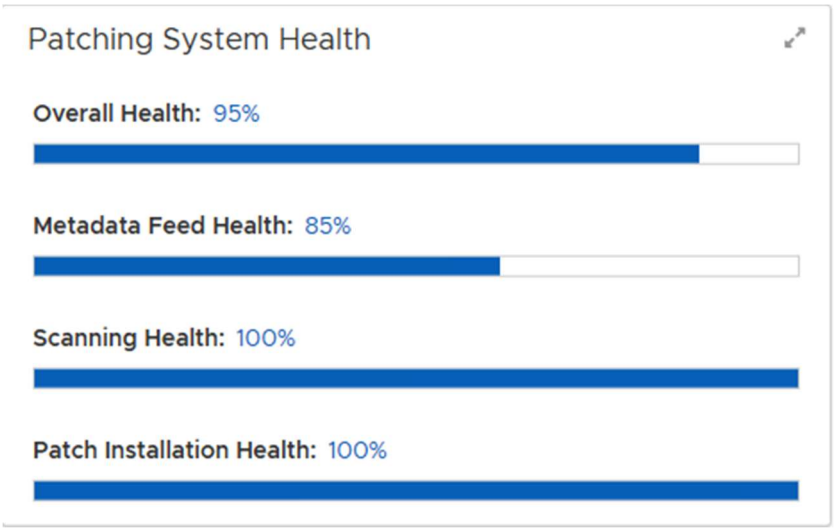
Patching Metadata

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.

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.



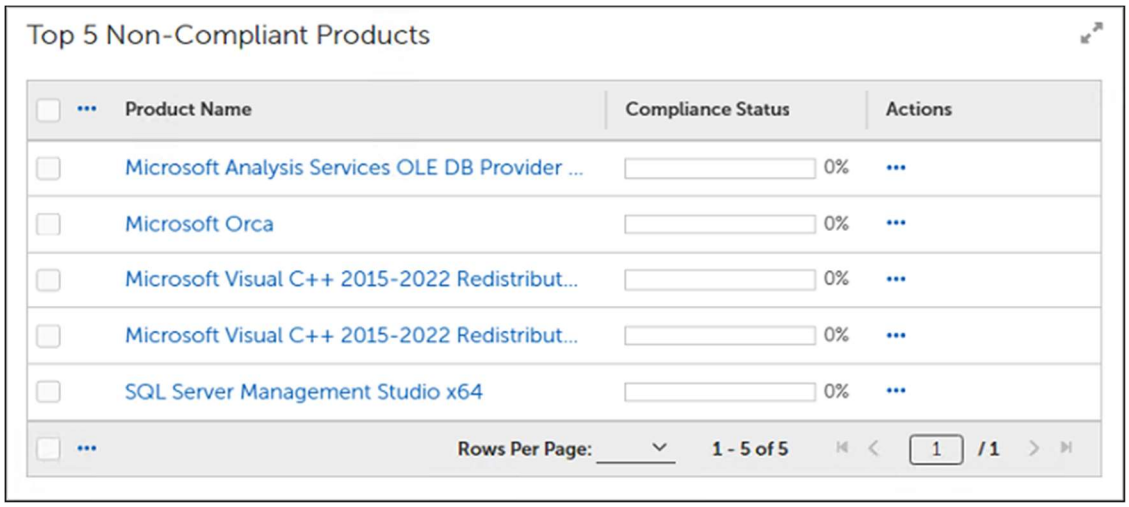
Patching Activity

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 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.

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 Adaptiva. 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

Adaptiva 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 Adaptiva 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:

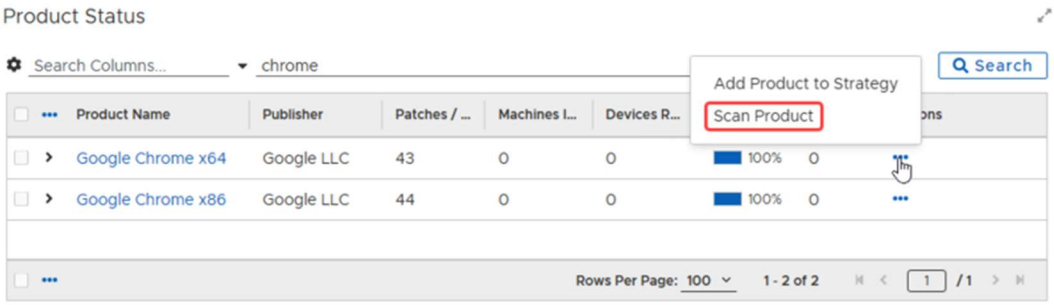
    a. **Overview** – **Product Status** table; Actions include Scan Product and Reset Deployment Failures for Product.

    b. **Products** – **Product Status** table; Actions include Scan Product and Reset Deployment Failures for Product.

c. **Patches** – **Patch Status** table. Actions include Scan Patch and Reset Deployment Failures for Patch.

d. **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.

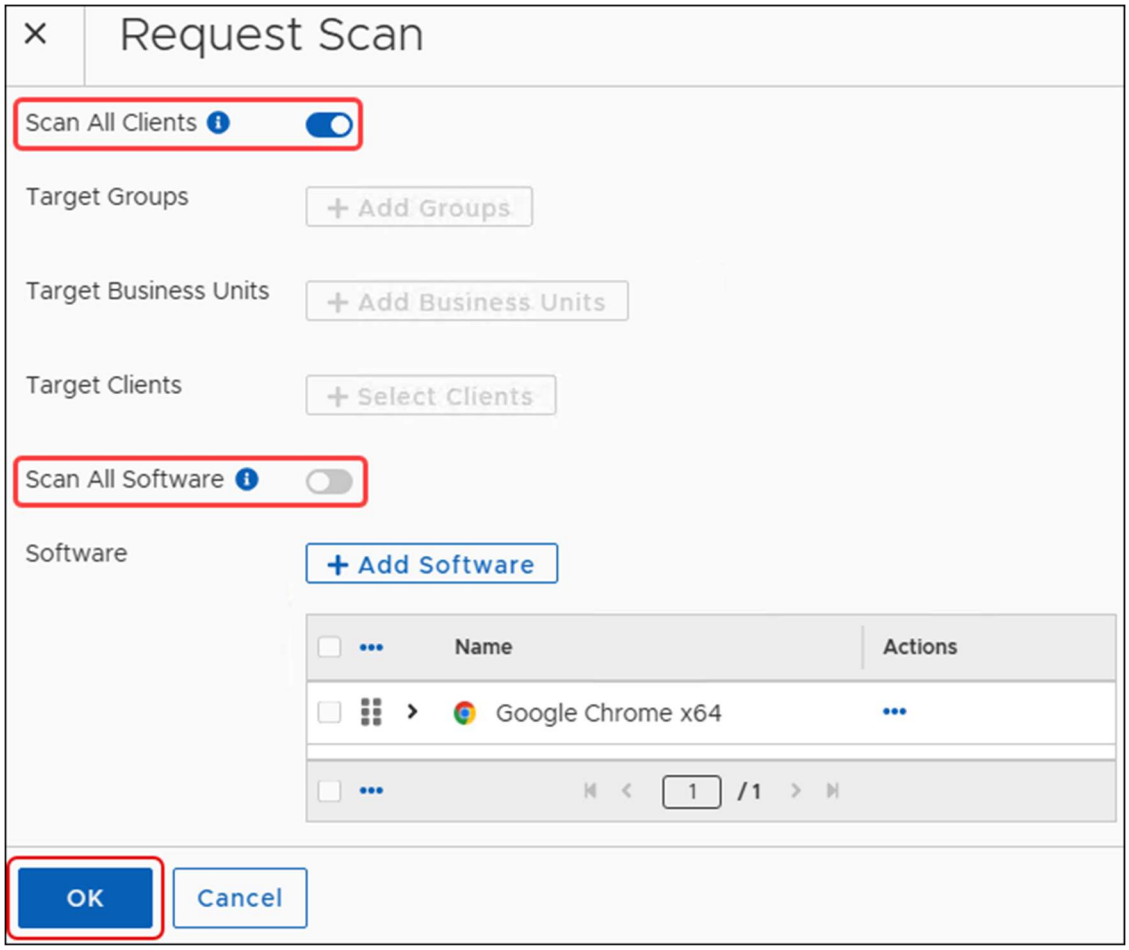


4. Select **Scan Product**.

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.