adaptiva

OneSite Patch Enterprise

with CrowdStrike

Table of Contents

Adaptiva Copyright

Legal Notice

Corporate Headquarters	E-mail	Website
Kirkland, WA +1 (425) 823-4500	<info@adaptiva.com>	www.adaptiva.com

Revision History

Date	Product Version	Document Version	Details
June 3, 2025	9.3.968.xx	v3.0	Added definitions for host groups, vulnerabilities, and user management.
April 2, 2025	9.2.967.xx	v2.0	• Cross-platform support for macOS third-party patching and Linux repository based patching. • Unified cross-platform visibility in Patch for customers with macOS, Linux, and Windows devices. • Platform-agnostic Peer to Peer (P2P) content distribution. • Allow users to specify a maintenance window for deployments and another for reboots when creating Business Units. • Allow users to suppress reboots using User Interaction Settings. • Updated content to improve usability and revised for clarity

New in this Release

Along with other improvements to usability and performance, the product for v9.2.967.xx includes the following new features:

- Cross-platform support for macOS third-party patching and Linux repository based patching.
- Unified cross-platform visibility in Patch for customers with macOS, Linux, and Windows devices
- Platform-agnostic Peer to Peer (P2P) content distribution

Getting Started with OneSite Patch

OneSite Patch 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.

OneSite Patch is powered by . is committed to providing the best tools for our customers to achieve their security outcomes.

Integrating CrowdStrike with OneSite Patch incorporates rich vulnerability insights from CrowdStrike, including real-time ExPRT Rating and Exploit Status. These products work together to determine patch priority, severity, and scheduling, ensuring all critical vulnerabilities receive the patches needed to protect organizations from potential threats.

Supported Operating Systems, Software, Drivers, and BIOS

- **Windows**
  - Windows 10 and newer
  - Windows Server 2012 and newer
  - Windows 365
  - Support for BIOS and Driver patching for the following third-party solutions:
    - DELL
    - Hewlett-Packard
    - Lenovo workstations and Servers

- **Linux**

  Automated OS package updates, libraries, and applications from official repositories for key Linux distributions (updates within the same distribution release within those repositories).
  - CentOS Stream 9
  - CentOS Stream 10
  - Debian 11
  - Debian 12
  - RHEL 8
  - RHEL 9
  - Ubuntu 18.04 LTS
  - Ubuntu 20.04 LTS
  - Ubuntu 22.04 LTS
  - Ubuntu 24.04 LTS

  TIP

  Support for repository-based library and application patching, including:

  - OS package updates (security, system services, libraries, and kernel).
  - Automated updates from the official repositories of each supported Linux distribution for each supported release.
  - Patch support for approximately 18,000+ products sourced from distribution-specific repositories.
  - Popular application support, such as Chromium, Firefox, Apache, OpenSSL, NGINX, and more.

  Some limitations apply. See Customer Facing FAQ Cross Platform 2025 for details.

- **Mac**

  Third-party patching only. Support for devices running the following macOS versions:
  - macOS 13 (Ventura)
  - macOS 14 (Sonoma)
  - macOS 15 (Sequoia)

NOTE
MacOS Patching is not supported at this time.

Supported Browsers

Adaptiva OneSite supports the following browsers:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Safari

IMPORTANT
Do not use Microsoft Internet Explorer.

Logs for Server

Access Server logs by navigating to > **Logs** in the Admin Portal, or by navigating to the following location:

`<path>\Adaptiva\Adaptiva Server\Logs`

NOTE
OneSite Patch - SaaS tenant logs can only be accessed by navigating to > **Logs** in the Admin Portal.

The following options are available on the **Logs** page:

- **Download All Server Logs:** Downloads all Server logs, including component and workflow logs.
- **Download Server Error Logs:** Downloads Adaptiva Server error logs.
- **Clear Web Logs:** Clears all Admin Portal runtime information and errors recorded by the browser session.
- **Download Web Logs:** Downloads all Admin Portal runtime information and errors recorded by the browser session.

Customer Support

When you need information beyond what this documentation or our Knowledge Base provides, enter a support ticket and request help from Adaptiva Customer Support (support account required).

Adaptiva OneSite Admin Portal

OneSite Patch uses the Admin Portal for configuration and management.

Use the Admin Portal to set up your environment, create policies, add administrators, and more. Global settings include groups, security, and administrators.

Log in to the Admin Portal

During the Adaptiva OneSite installation, the administrator creates a SuperAdmin account using either a native login, OIDC-enabled account, SAML-enabled account, or a Windows Active Directory account (recommended).

TIP

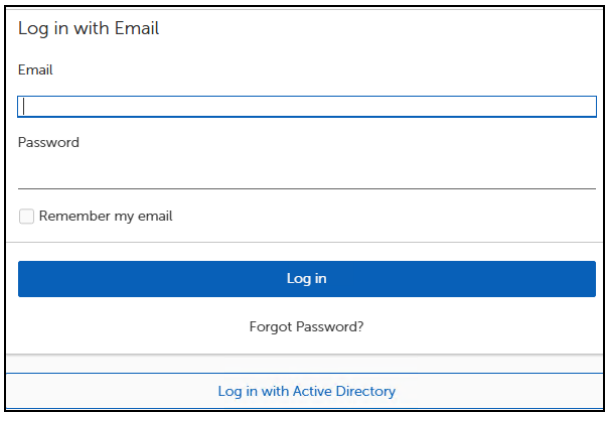
You can create an OIDC-enabled or SAML-enabled account after server activation and component configuration.

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

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

   If necessary, confirm the port details with the administrator who defined the port during the software installation. If the server is already using port 80, for example, the website may use port 9678.

2. Press **Enter**. The Admin Portal login dialog opens.



3. Log in using one of the following methods:

- Enter a native **Login ID** (email address) and password, and then select **Log in**.
- Select **Login with Active Directory** (recommended).
- Select **Login with <*OIDC Entry*>**. OIDC-enabled accounts can be configured after server activation and component configuration.
- Select **Login with <*SAML Entry*>**. SAML-enabled accounts can be configured after server activation and component configuration.

> **TIP**
> If you are using Mozilla Firefox, see Resolve the Mozilla Firefox Active Directory Login Issue KB article.

After successfully logging in, the Home page appears.

Licensing Products

Adaptiva OneSite Products requires a license for each active client. The license key contains the licensed company name and client count. The Adaptiva Server periodically counts all active, healthy, reporting clients as licensed clients.

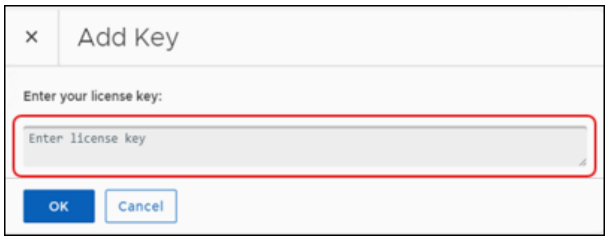
You may enter the license key when installing the Server, or enter the license key using the Admin Portal after completing the installation. If you are starting the Admin Portal for the first time or your key has expired, select **Manage Licenses** to add or replace the license.

To access CrowdStrike, obtain a license from CrowdStrike. You do not need to enter the CrowdStrike license in OneSite Patch.

Add a License Key

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

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



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

Target Collections for the Licensed Product

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

1. Select the OneSite Patch product name in the **Product Licensing** list.
2. Select **+ Browse** under **Target Collections**.
   This opens the **Select Group** dialog.
3. Select one or more Groups from the **All Groups** table.
4. Select **OK** on the lower-left corner to return to the **Product Licensing** workspace.

Dashboard

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

Access the Dashboard

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

- Select near the top of the page.
- Select **Go to** under **Licensed Products**.

Integrate Falcon Spotlight

CrowdStrike, part of CrowdStrike Falcon® Exposure Management, brings IT and Security teams together and improves visibility by combining CrowdStrike Expert Prediction Rating Artificial Intelligence (ExPRT) data with OneSite Patch deployment and management capabilities. Rather than exporting vulnerability data from CrowdStrike Falcon for patching, the integration includes ExPRT ratings from CrowdStrike directly in OneSite Patch, so you can prioritize patching preferences according to your organizations requirements and remediate vulnerabilities faster.

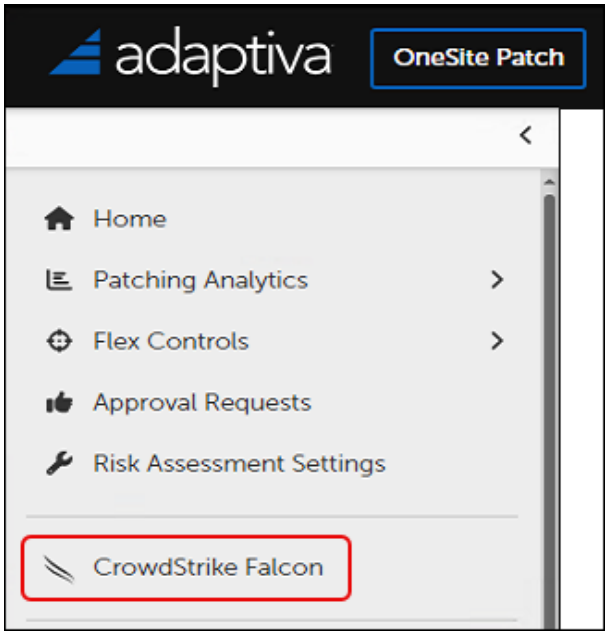
Using Falcon Spotlight in OneSite Patch

Adaptiva and CrowdStrike Falcon® Exposure Management have integrated CrowdStrike vulnerability metadata with Adaptiva Patch metadata to allow Patch Deployment Bots to deploy patches based on Spotlight vulnerability metadata.

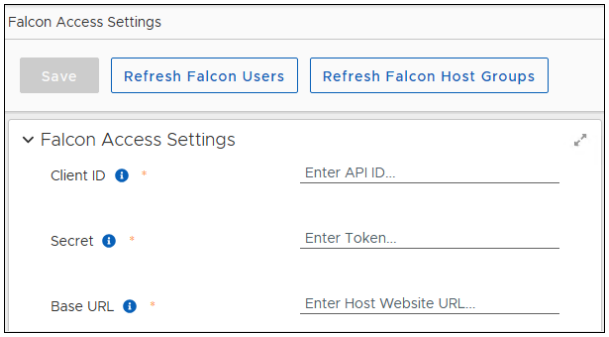
To access CrowdStrike from OneSite Patch, you must have a license from CrowdStrike that allows you to access CrowdStrike Falcon.

Access Falcon Spotlight

1. Select **Falcon Access Settings** in the left navigation menu of the OneSite Patch Dashboard.



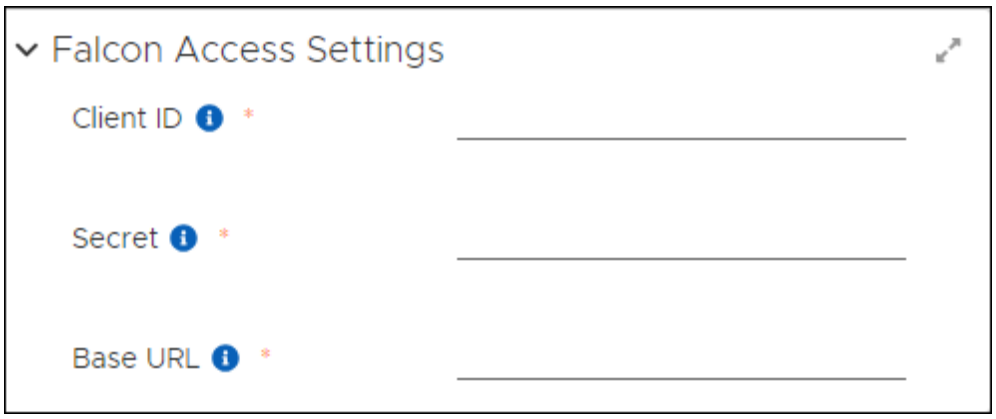
This opens the **Falcon Access Settings** dialog.



2. Enter the **Falcon Access Settings**. If you do not have these details, see Create a CrowdStrike API Client.

Enter the Falcon Access Setting Details

1. Enter the **Client ID**, **Secret**, and **Base URL** in the respective fields of the **Falcon Access Settings** dialog.

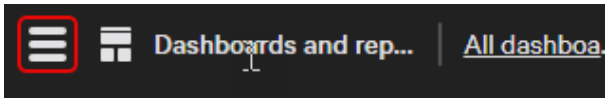


2. Select **Save** on the upper-left corner of the settings dialog. This populates Roles, Business Units, and vulnerability information in OneSite Patch related to the CrowdStrike Client ID.
3. Select **Business Units** in the left navigation pane of the OneSite Patch Dashboard to verify that your client Business Units and templates exist.

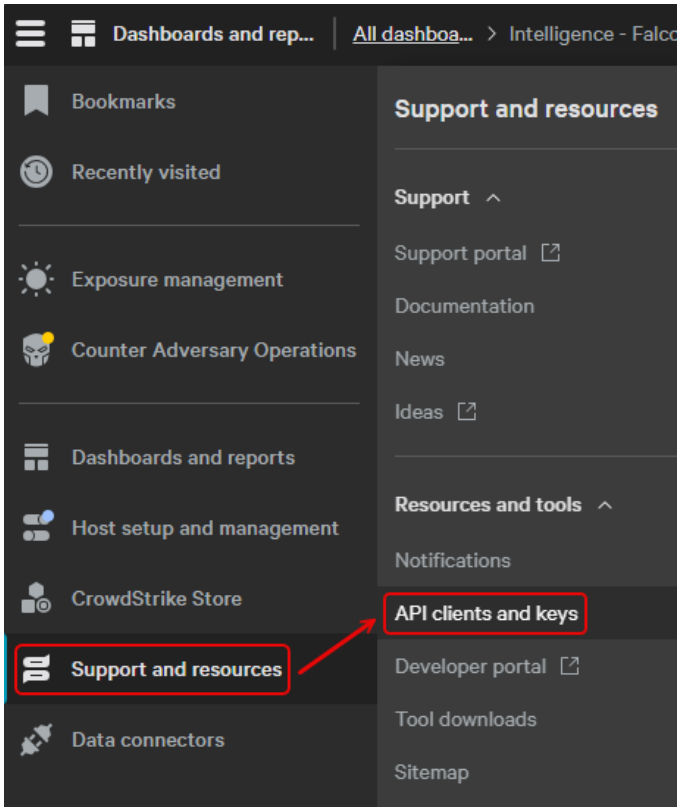
Create a CrowdStrike API Client

Create a CrowdStrike API Client to generate the client settings needed to access CrowdStrike.

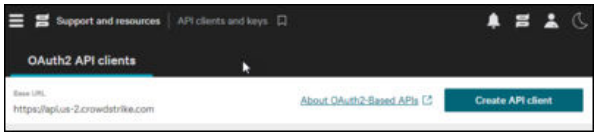
1. Log in to your **CrowdStrike Falcon Spotlight dashboard**.
2. Select the Stack icon on the upper-left of **Dashboards and reports**.



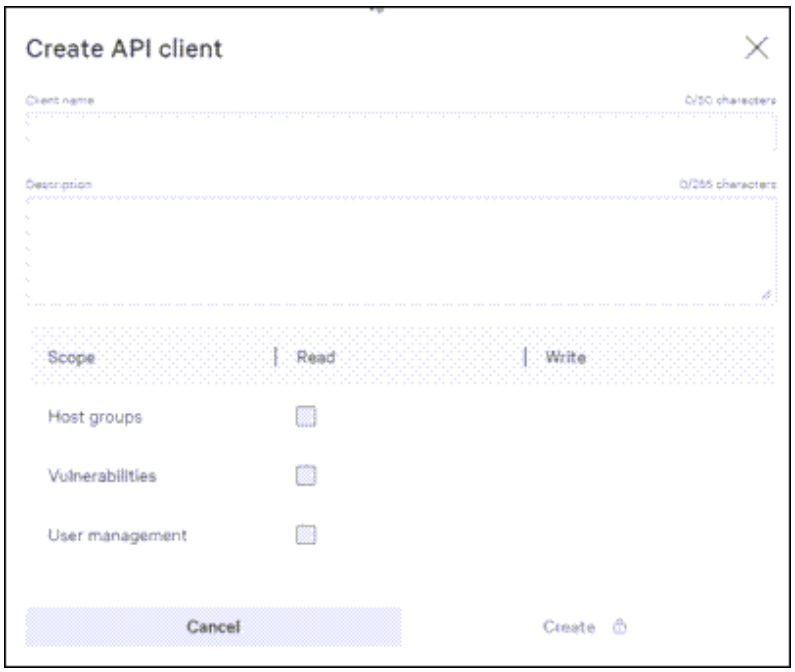
3. Select **Support and resources** in the left navigation pane, and then select **API clients and keys**.



4. Select **Create API Client** at the upper right.



This opens the **Create API Client** dialog.



Set Client Details

In the **CrowdStrike Falcon Spotlight Create API Client** dialog, complete the following steps:

1. Enter a **Client name**, and then enter a **Description** of the client.
2. Select **Read access** in the **Scope** column for each of the following items:
   - **Host Groups:** A collection of devices that Adaptiva retrieves from CrowdStrike and uses to create business units.
   - **Vulnerabilities:** A list of defined vulnerabilities (trigger properties) that Adaptiva retrieves from CrowdStrike. Adaptiva utilizes these properties to set automation, such as scheduling based on ExPRT.AI ratings.
   - **User Management:** The OneSite Platform retrieves and adds CrowdStrike users and roles to the platform. The system automatically adds all users to the read-only, **All Admins** role.

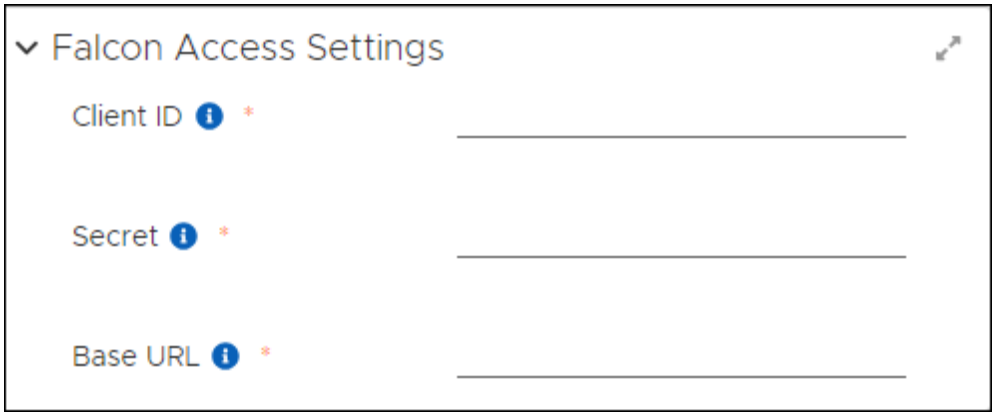
   > **IMPORTANT**
   > There is a built-in Approval Chain for the **All Admins** role, and users with this role will receive approval requests if this chain is assigned to a strategy.

3. Select **Create**. This opens the **API client created** response, which contains the details you must enter in the **Falcon Spotlight Access Settings**.

IMPORTANT

The details for the API client created screen show these details only once. Be sure to save this information in a safe location so you can access it later, if needed.

4. Copy and paste the **API client created** details directly into the fields of the **Falcon Spotlight Access Settings** dialog in the Adaptiva OneSite Admin Portal.



5. Select **Save** on the upper-left of the settings dialog. This populates Roles, Business Units, and vulnerability information in OneSite Patch related to the CrowdStrike Client ID.
6. Select **Business Units** in the left navigation pane of the OneSite Patch Dashboard to verify the availability of your Hosts.

Security

View, create, or modify Administrators and Roles, enable OIDC or SAML providers, and assign permissions to Roles. Changes made here affect all licensed OneSite products. How to assign Class Permissions to a role is coming soon.

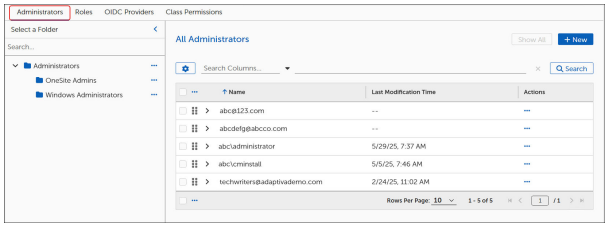
You can view your list of CrowdStrike users and their assigned roles.

Access Security Settings

1. Select ⚙ on the upper-right of the Admin Portal dashboard.
2. Open the **Settings** page with the **Administrators** tab selected to manage accounts, roles, OIDC Providers, SAML Providers, and Class Permissions.

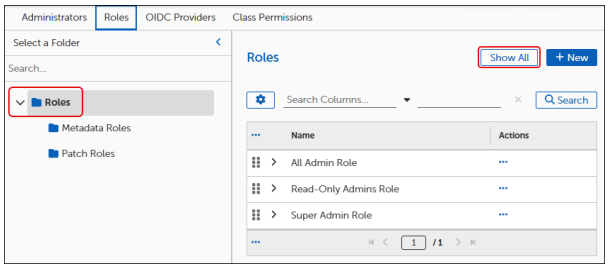
View Administrators

- Select the **Roles** tab of Security Settings.



View Roles

- Select the **Roles** tab of Access Security Settings to view the list of roles.



Introduction to Patching Strategies

Creating a Patching Strategy is a great way to start using . Start with a common scenario, and then build a Patching Strategy to distribute a patch to active clients.

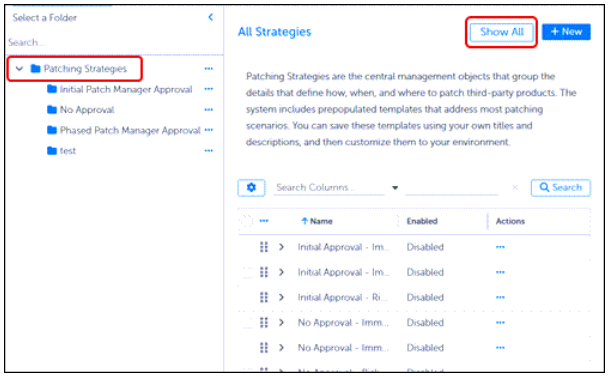
Patching Strategy Use Case

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 Falcon Host Group 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 select **Strategy** in the left navigation menu of the Dashboard, and then select **Patching Strategies**.
3. Select **Patching Strategies**, and then select **Show All** to see all available Patching Strategies.



   For descriptions of each template type, see Patching Strategy Templates.
4. Select the **Name** of a strategy to open it.
5. Select **More** in the upper left corner of the template, and then select **Save As**:
   a. Enter a unique name that reflects what the strategy does conceptually. For example, `ITS Immediate Daily Product Patching`.
   b. Select **Save as** on the bottom left corner of the dialog. 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 select **Save** on the upper-left of the dialog.

TIP

Remember to select **Save** on the upper-left to save your progress as you make changes. 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. Select **Browse** next to **Deployment Wave** in the **Deployment Settings** workspace of an open Patching Strategy template.

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

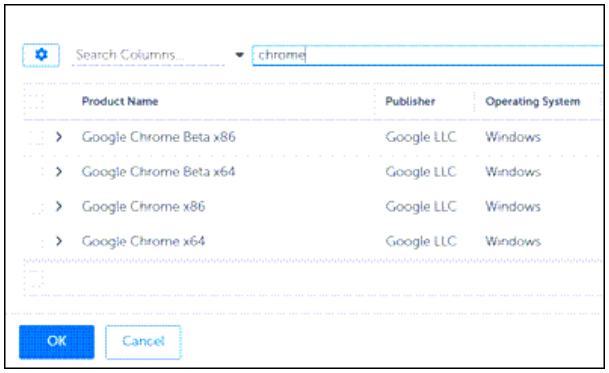
2. Select a **Deployment Wave** from the list.
   - Adaptiva provides a **Single Wave-All Clients** Deployment Wave, which includes a Business Unit called **All Clients Business Unit**.
   - If you are following the tasks in **Introduction to Patching Strategies**, choose **Single Wave-All Clients**.
3. Select **OK** on the bottom left of the dialog to return to the Patching Strategy.
4. Select **OK** to close the recommendation. The system returns you to the Patching Strategy at the Business Unit Addition Settings workspace:
   - If you are following the tasks in **Introduction to Patching Strategies**, skip to Add Software Products. There is no need to modify the Deployment Bot Runtime settings for purposes of this exercise.
   - If you are creating or modifying a Patching Strategy for ongoing use, continue with the next step.

Add Software Products

1. Select **+ Browse** in the **Products** workspace of an open Patching Strategy template. The following image shows the default settings for this dialog.

2. Select the **Include All Products** toggle to disable the inclusion of all products. This changes the next item to **Included Products**.

3. Select **Browse** to open the **Select Software Product** dialog.
4. Enter **Chrome** on the search line, and then select **Search**.
5. Select **Google Chrome x64**, and then select **OK** on the lower-left corner of the dialog.

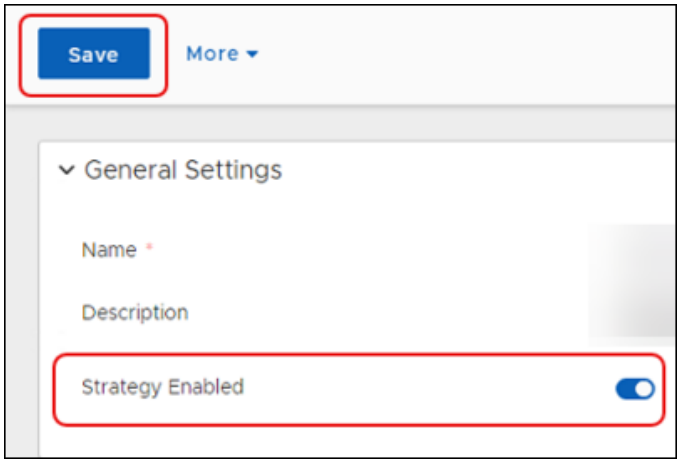


6. Scroll up to **General Settings** to enable the strategy.

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, select the **Strategy Enabled** toggle to enable the strategy and make it available for use.

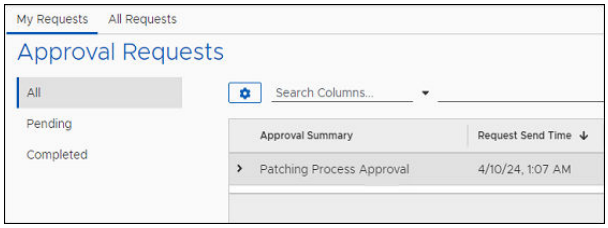


2. Select **Save** on the upper-left corner of the workflow to save the strategy:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** again if you make any changes.
3. Move the saved template to your folder.

View a Staged Patching Strategy

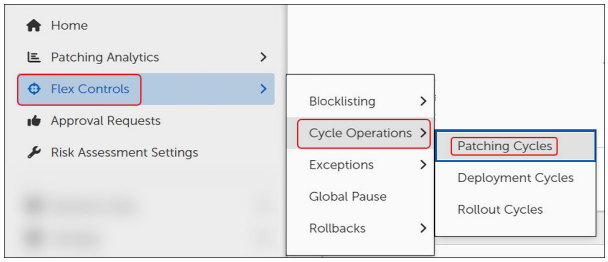
After you Enable the Patching Strategy, you can view the pending approval request.

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

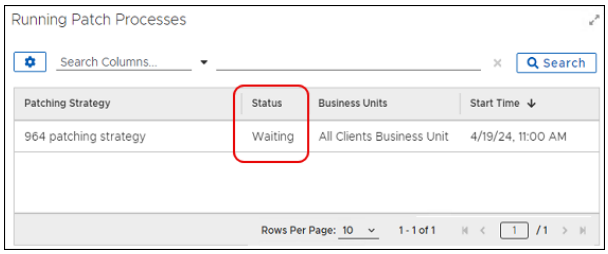


- The view defaults to **All** requests, which includes pending and completed.
- The Patching Strategy you just enabled appears in the **Approval Summary** table with a **Request Status** of **In Progress and Awaiting Response**.

2. Select **Flex Controls > Cycle Operations > Patching Cycles** from the left navigation menu of the 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 select the **Patching Strategy** in the table.
5. Select **Approve**, and then select **Back to Approval Requests**. You can wait until the patch time passes, or you can start the deployment manually.

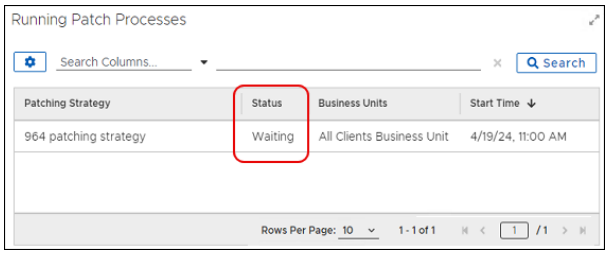
IMPORTANT

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

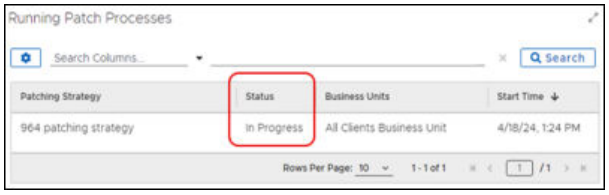
Start the Patching Strategy Manually

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 select the name of the Patching Strategy to open the **Cycle Information**.



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

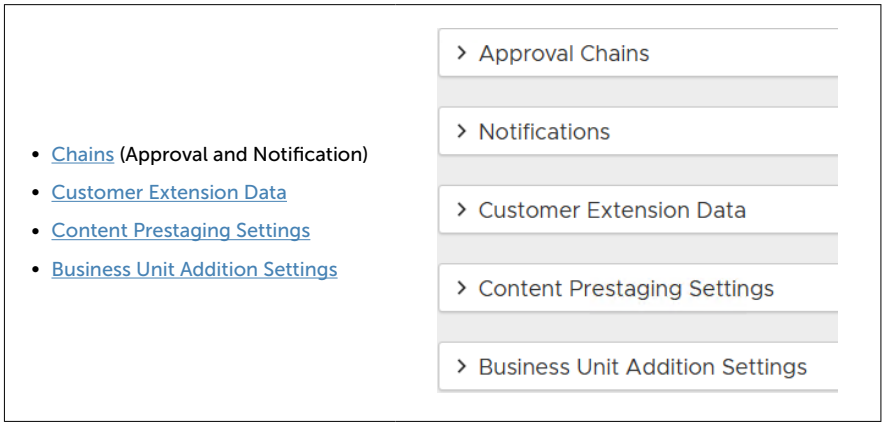


3. Select the **Patching Strategy** name to view details about the patching process.

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. Creating a Patching Strategy documents the configuration steps.



Organize New Patch Objects

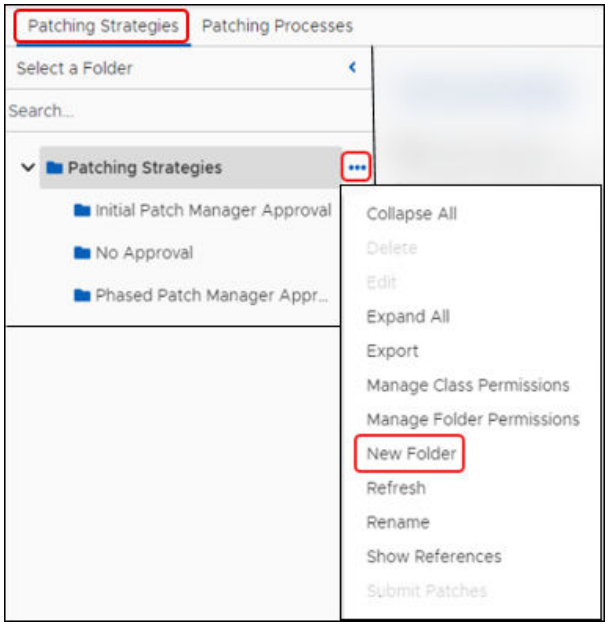
Throughout your patch management journey, you will customize object templates to meet the needs of your business environment.Adaptiva recommends setting up your own folder to hold object templates that you customize or create, to keep them separate from those provided by Adaptiva.

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 Adaptiva.

1. Select an object on the left navigation menu of the Adaptiva 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**.



   b. Enter a descriptive **Name** for the folder, and then select **OK** on the lower-left of the dialog.
      - This creates the new folder structure showing both your folder and the **Patching Strategies** folder.

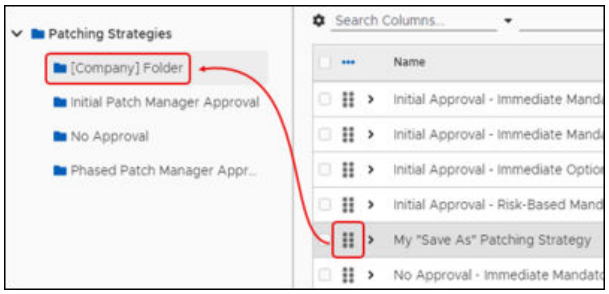
      - When you create new strategies or modify existing strategies, move them to your folder location (see Move an Object Template Between Folders).

Move an Object Template Between Folders

After creating 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**.

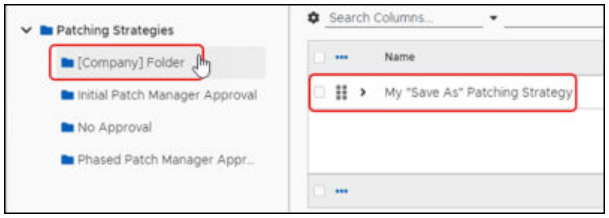
1. Select and hold the **stacked icon** next to the template you want to drag and drop to the new folder.

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 OneSite Patch

The menu on the left pane of the OneSite Patch 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 dashboard. For descriptions of each menu item, see Patch Menus.

Business Units and Rollout Processes

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

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

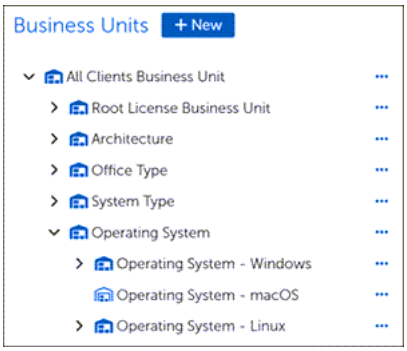
A Rollout Process runs at the Business Unit level to define and direct the rollout requirements of a Business Unit. This includes separating patch approvals, submitting them to a specified Business Unit, and sending a system request to begin the patch rollout for the Business Unit after receiving notification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

Additionally, children of Business Units inherit settings from their parent Business Units, thereby reducing the administrative burden of managing settings across multiple units. OneSite Patch includes a Parent Business Unit for All Clients and Child Business Units that address most device grouping scenarios.



Related business units, such as Child Business Units or Lab Business Units, provide an additional 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.

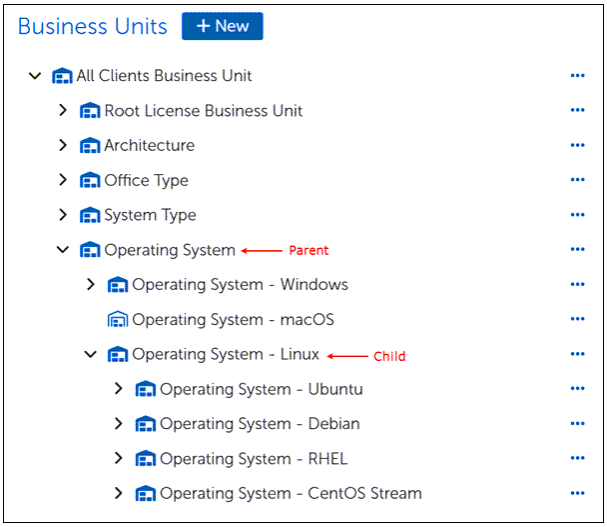
In addition to identifying the devices to include in a Business Unit, you can also specify various aspects of patching for endpoints, such as rollout processes, maintenance windows, approvals, and other relevant details.

Parent and Child Business Units

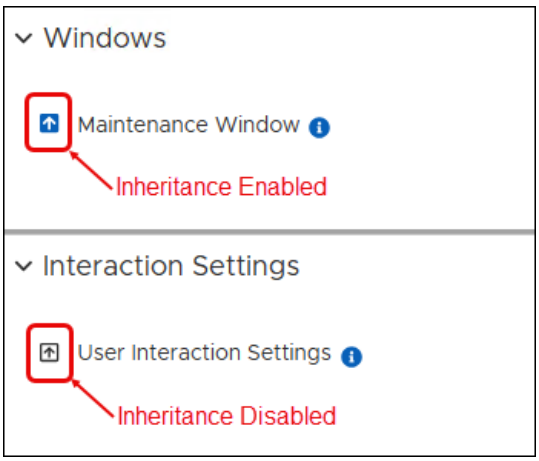
Business Unit objects use a parent-child hierarchy. A parent Business Unit may have multiple child Business Units, but a child Business Unit may have only one parent. The folder structure used in OneSite Patch shows the parent as the top-level folder and the child units as sub folders of a parent. This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

TIP

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.

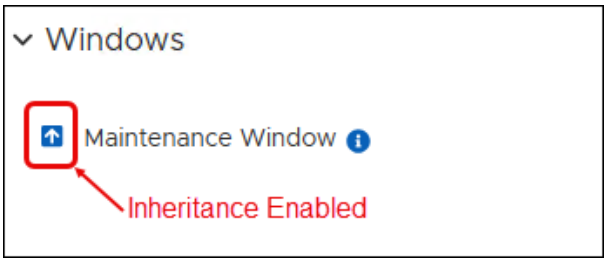


The hierarchical nature of Business Units allows a child Business Unit to inherit settings from its parent. An up-arrow with a blue background preceding a setting or process shows an inherited setting.

OneSite Patch 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 OneSite Patch inheritance defaults to Enabled.



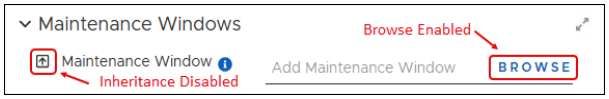
IMPORTANT

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.



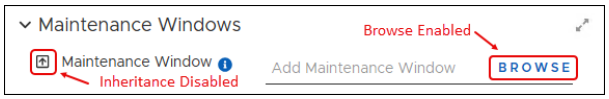
2. Select the up-arrow icon to enable inheritance

Disable Inheritance

A black up-arrow with a white background preceding a setting 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 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

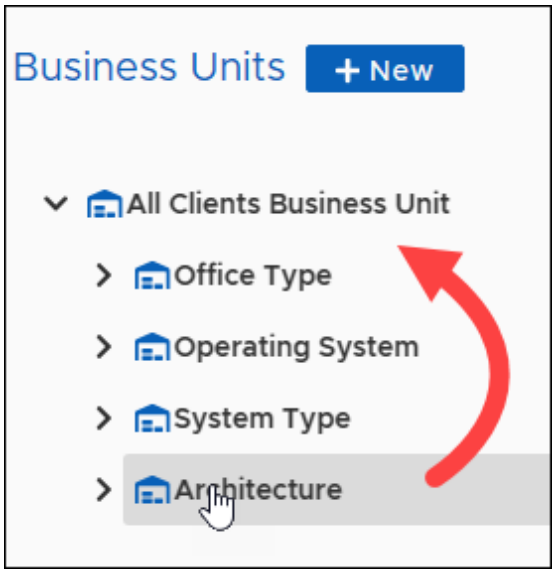
In the Business Unit hierarchy shown in the OneSite Patch dashboard, the Business Unit at the top of the list has the lowest priority. When changing the priority of a Business Unit in the hierarchy, consider the following items:

- **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?

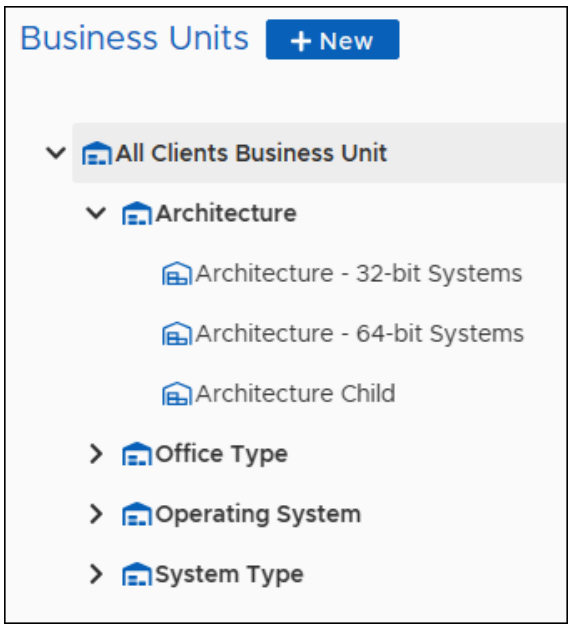
  Further, is the new parent, or any ancestors, included in a Wave Entry that includes descendants? If yes, do you want the new BU included in those deployments?

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

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

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

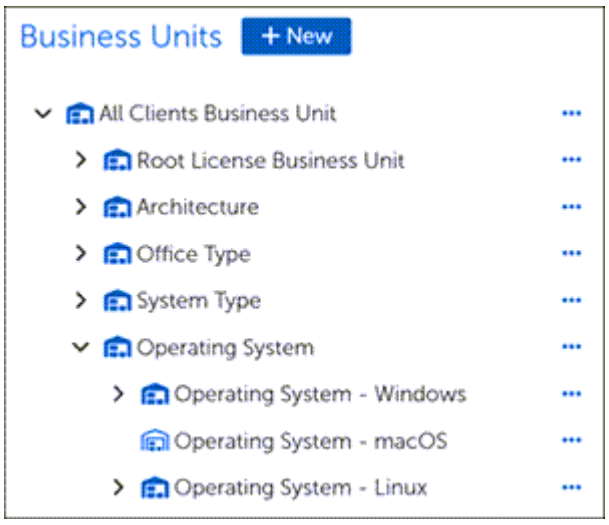
Open and Save a Business Unit Template

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

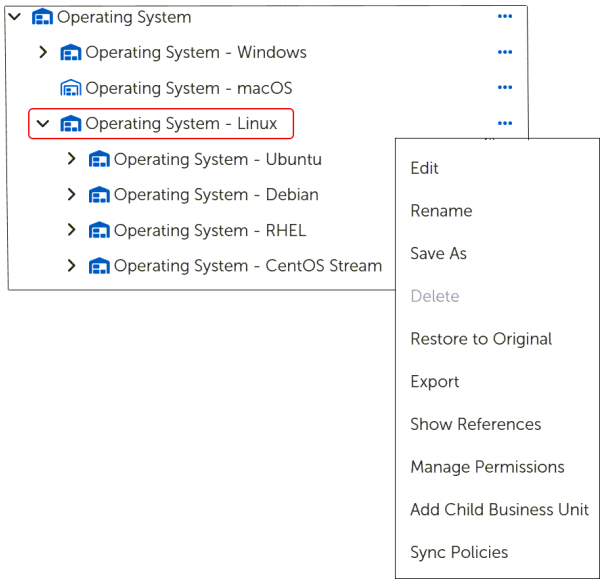
IMPORTANT

When creating a new Business Unit, and it is immediately scoped for membership (by default), it becomes the highest priority Business Unit. If you have not defined the Maintenance Window settings or the User Input Settings, this may override other settings in the hierarchy and cause unexpected software deployments or reboots.

1. Mouse over or select **Business Units** in the left pane of the Patch 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 **ellipses ...** next to the object you want to open, and then select Save As.



4. Save the template with a new title:
   a. Select **More** in the upper-left of the dialog, and then select **Save As**.
   b. Enter a new name for the template, and then select **Save as** on the lower-left of the dialog. This returns you to a copy of 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, and then select **Save** on the upper-left of the dialog.

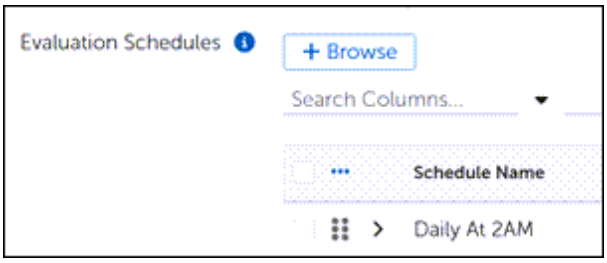
5. Select **Save**. When you have finished modifying your new template, you can drag and drop it onto the folder you created (see Patch Object Management).

Add Evaluation Schedules to a Business Unit

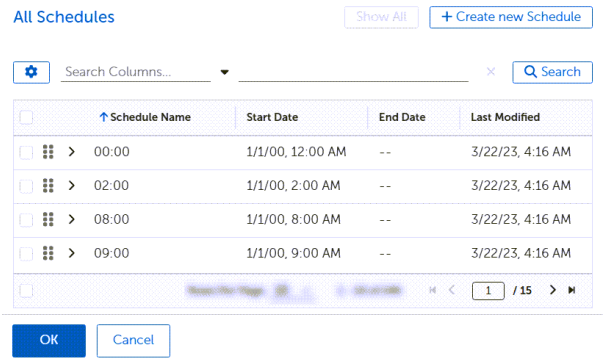
For Business Units with dynamic membership that may change over time, evaluation schedules determine when to check the membership of a Business Unit. Dynamic membership can occur based on Location or Sensor scopes, where a device moves between locations or Sensor results change over time.

The Evaluation Schedules added here trigger Group Membership evaluations for this Business Unit to regularly check for group membership changes.

1. From an open Business Unit, review the selected schedules (if any).
   - If you choose to use the existing schedules, skip to Configure Business Unit Scopes.
   - Otherwise, select **+Browse**, and then continue with the next step.



2. Select one or more schedules from the **All Schedules** table, and then select **OK** on the lower-left of the dialog.



3. Select **Save** on the upper-left 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.

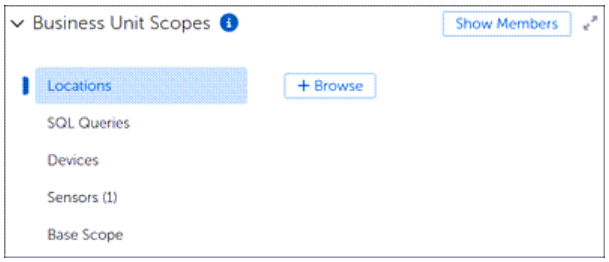
Configure Business Unit Scopes

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

TIP

If the scope type (Locations, and so on) has a number in parentheses 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 select 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.
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.

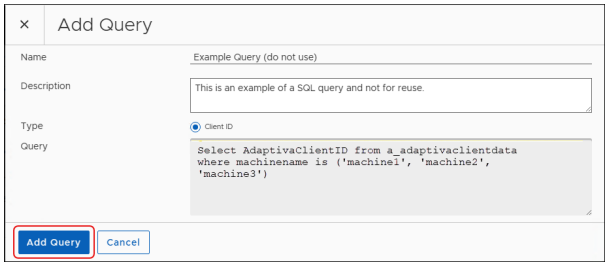
1. Select **Locations** from Business Unit Scopes, and then select **+Browse**.
2. Select one or more Location Names from the **Add Locations** table to assign them to the Business Unit. For information about managing available Location settings, see the *Adaptiva OneSite Platform Installation User Guide*.
3. Select **OK** on the lower-left of the dialog. This returns you to the Business Unit template and populates a table with the selected Locations.

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 select **+ Add Query**. This opens the **Add Query** dialog.

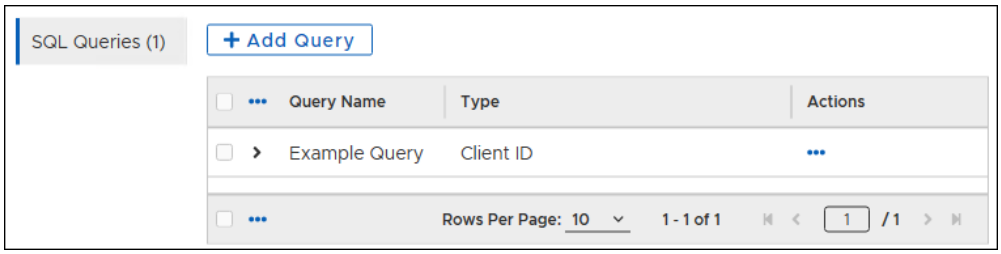
2. Enter a **Name** for the Query, and then add a detailed **Description**. The **Type** field defaults to **Client ID**, meaning that the software returns a list of Client IDs regardless of what the query might request.
3. Write your SQL query in the **Query** text box.



IMPORTANT

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

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



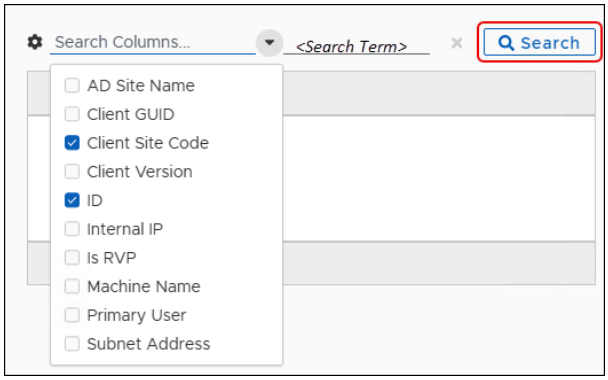
Add Devices

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

IMPORTANT

Device scoping is sensitive to the Client ID. If an administrator reinstalls a Client, the Client receives a fresh ID, and the Business Unit no longer scopes the new Client.

1. Select **Devices** from **Business Unit Scopes**, and then select **+Browse**.
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 select **Search**.



4. Select one or more devices to add to this Business Unit, and then select **OK** on the lower-left of the dialog.

Add Sensors

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

TIP

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

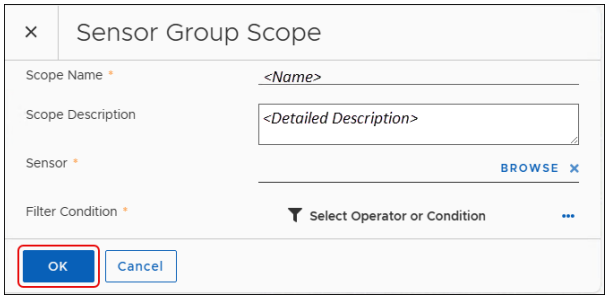
To include devices in this Business Unit based on sensor settings, complete the following steps:

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

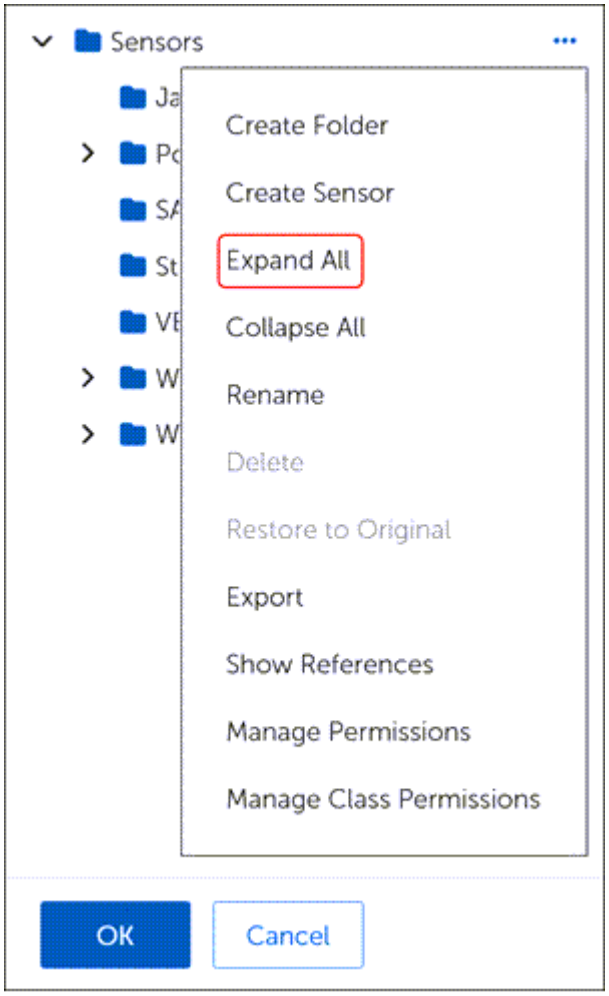
2. Enter a **Name** and a detailed **Description** of the Sensor Group in the **Sensor Group Scope** dialog.

NOTE

A red asterisk (*) indicates a required field.



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.

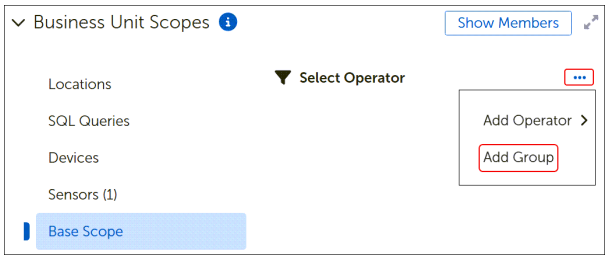


5. Select an item to use in your Sensor Group, and then select **Add Sensor**. This returns you to the **Sensor Group Scope** dialog. To add a Filter Condition, see Patch Filter Conditions
6. Select **OK** to return to the Business Unit template or change Base Scope settings.

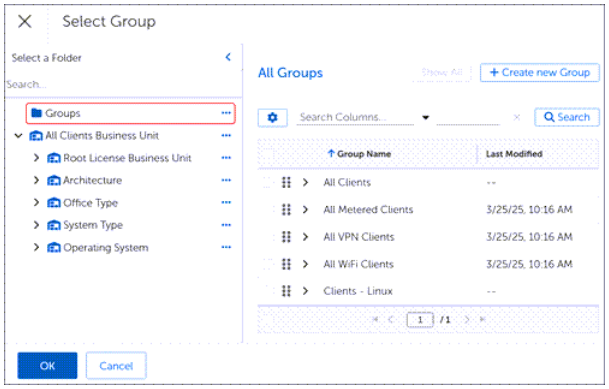
Set Base Scope

Use Base Scope settings to add or exclude devices in a Business Unit based groups, CM collections, or other business units. 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 select **Add Group**.



3. Select the container type you want to use.

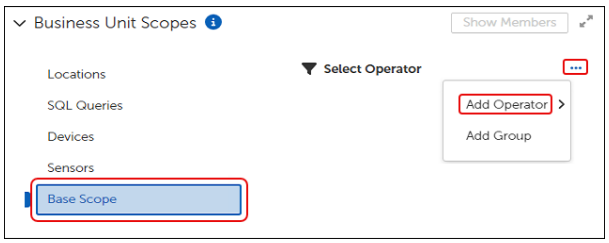


4. Select a **CM collection, Business Unit, or Group** to add to the **Base Scope**.
5. Select **OK** on the lower-left of the dialog. The entry under Business Unit Scopes shows the **AND** operator and the item you chose.

Add Multiple Groups or Business Units

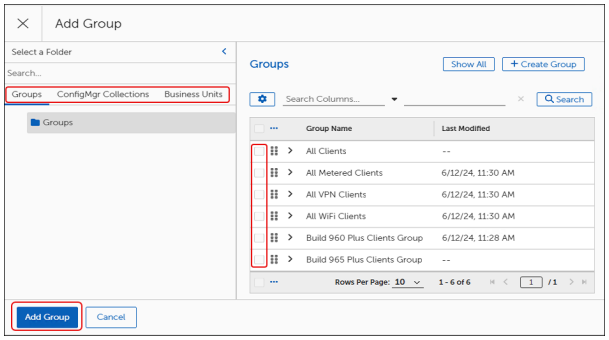
After setting the initial Base Scope, use this procedure to add additional Groups or Business Units to include in the Base Scope. You can add or exclude other Groups or Business Units or change Operators to customize your Base Scope depending on your needs.

1. In the **Business Unit Scopes** section of an object template, select **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 select **Add Group** on the lower-left of the dialog.



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

Remove Groups or Operators

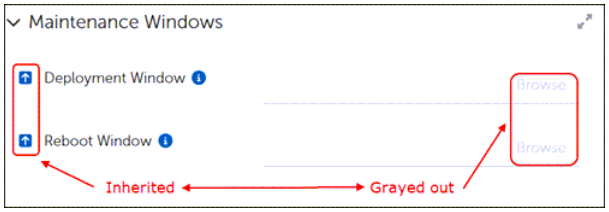
Select the **ellipsis (...)** to the right of an Operator or a Group, and then select **Remove**.

- 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.

Maintenance Windows in Business Units

Business Unit settings for Maintenance Windows allow you to set one maintenance window for deployments and another for reboots. Deployment Windows and Reboot Windows operate independently of each other. For example, if you specify a Deployment Window but not a Reboot Window, the installation occurs during the Maintenance Window you choose; however, if installation requires a reboot, the reboot may take place at any time. If the installation requires a reboot, you must set the Reboot Windows to occur during the Deployment Window.

1. Select **Browse** next to **Deployment Window** in an open Business Unit template.



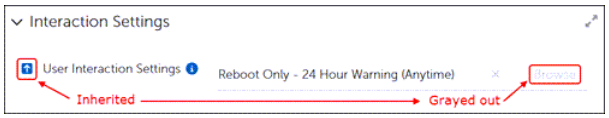
   If **Browse** is grayed out, the Business Unit you are editing inherits this setting (if any) from a parent. See Managing Inheritance Settings for details.

2. Select the **Maintenance Window** for this Business Unit. This setting indicates the time frame during which installations may occur on devices in the Business Unit.
3. Select **OK** to return to the Business Unit template.
4. Repeat these steps for the **Reboot Window** settings.

Add User Interaction Settings

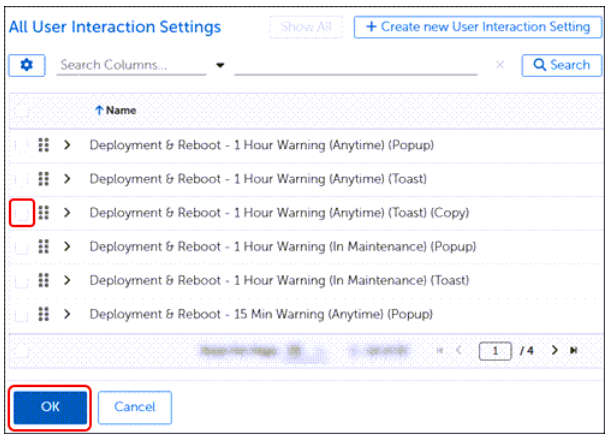
Choose a User Interaction Setting for the devices in this Business Unit. These settings control how end users are notified about upcoming installations and reboots. For more information about User Interaction Settings, see User Interaction Settings.

1. Select **Browse** next to **Interaction Setting**.



   - If the **Browse** button is grayed out, the Business Unit template you are editing inherits these settings (if any) from a parent.
   - See Managing Inheritance Settings for additional details.

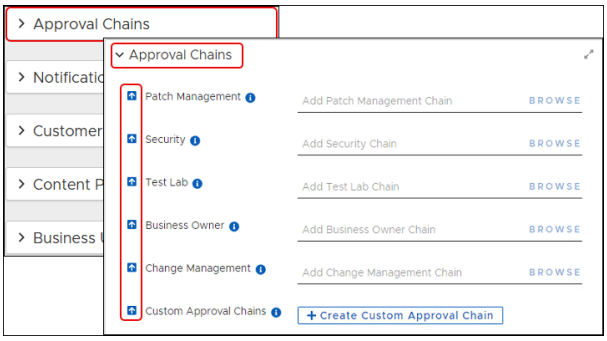
2. Select an **User Interaction Setting**, and then select **OK**.



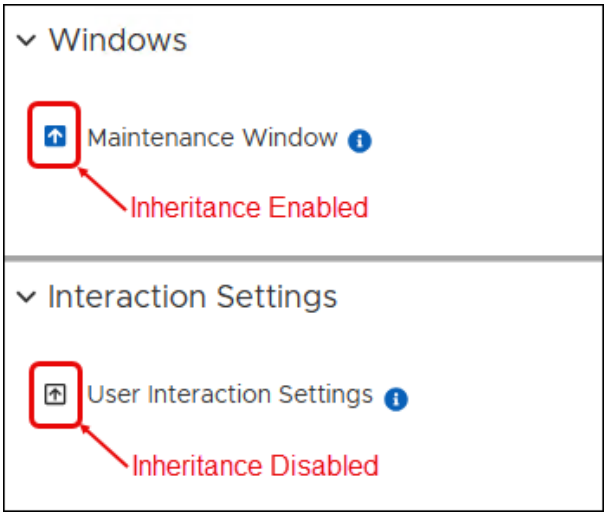
Add Approval Chains to a Business Unit

Adding Approval Chains to a Business Unit is an advanced feature. The **Approval Chains** fields allow advanced users to specify details for use in customized Patching Strategies, Deployment Chains, or Business Units when necessary to achieve different results.

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



   - Disable inheritance to enable Browse, and then 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.

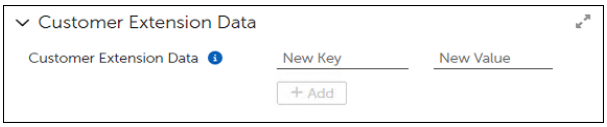
4. Select OK on the bottom left to return to the **Approval Chains** workspace.
5. Repeat Steps 2 through 4 for each of the groups listed in the **Approval Chains** workspace:

- Skip any groups that do not apply to your situation.
- 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.

Customer Extension Data

Customer Extension Data is an advanced feature of Adaptiva. 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.



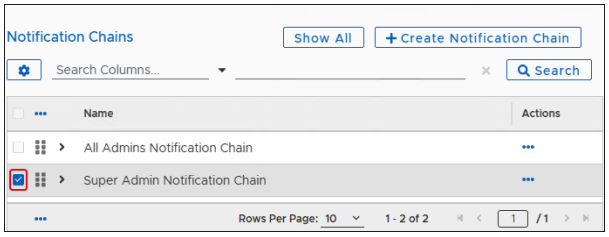
Customer Extension Data fields relate directly to fields in a customized template. If you do not have customized templates with key/value pairs you can modify, you do not need to configure or use this feature.

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

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 **Notification Chains**, and then 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 select **OK** (lower-left corner) to return to the template.

Content Prestaging Settings in Object Templates

The Content Prestaging feature deploys 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.

To configure these settings, see Content Prestaging Settings.

Verify Business Unit Members

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

IMPORTANT

Selecting Evaluate Now causes evaluation of the group membership rules to occur off schedule.

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 Adaptiva Client installed and are associated with a .
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.

Create a Custom Lab Business Unit

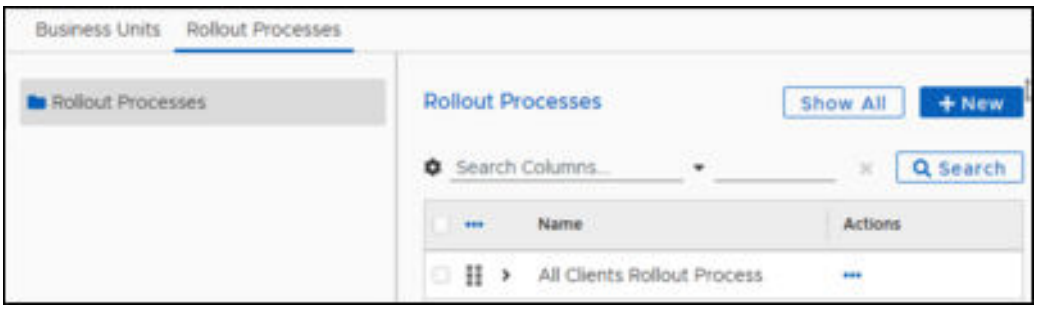
Designate Custom Business Units that a Lab Business Unit may use for testing purposes. If inherited from a parent Business Unit, values merge with the custom lab values of the parent and supersede the parent values when they conflict.

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, allowing 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 Process, enter a support ticket and request help from 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 Adaptiva because they group the details that define how, when, and where to update patches. Adaptiva 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 Adaptiva, you have a considerable number of products that require patching, and you prefer to review the progress of patching before fully automating the process.

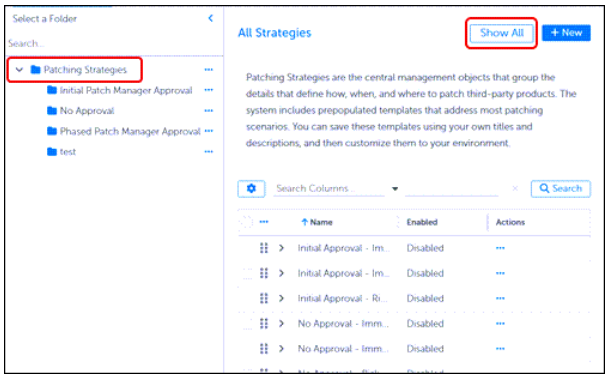
Reuse Intent Schema Objects

All objects in Adaptiva 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.

View built-in Patching Strategies

These built-in strategies are often enough to get an organization started with a patch deployment scenario.

1. Hover over or select the right-arrow next to **Strategy** in the left pane of the Adaptiva dashboard, and then select **Patching Strategies**.
2. Select any **Patching Strategy** to see the available templates associated with that strategy.



Patching Strategy Templates

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

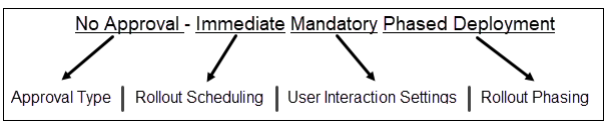
Recommended Use

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.

recommends creating a folder to hold all new or customized strategies. This separates them from the strategies provided with the product.

Patching Strategy Template Naming Conventions

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:
  - **No Approval:** Deploys at once.
  - **Initial Approval**: Requires approval prior to deploying.
  - **Phased Approval**: Requires approval between each wave in the Deployment Waves object.
- **Rollout Scheduling**: Defines the schedule and impact of a deployment.
  - **Immediate**: All product patches deploy at once.
  - **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.
  - **Mandatory**: Alerts the end user who can postpone depending on User Interaction Settings but cannot decline. All product patches deploy at once.
  - **Options**: Alerts the end user. Otherwise, functionality not available in this release.
- **Rollout Phasing**: Deploys in separate phases to allow a review before continuing.
  - 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.

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**

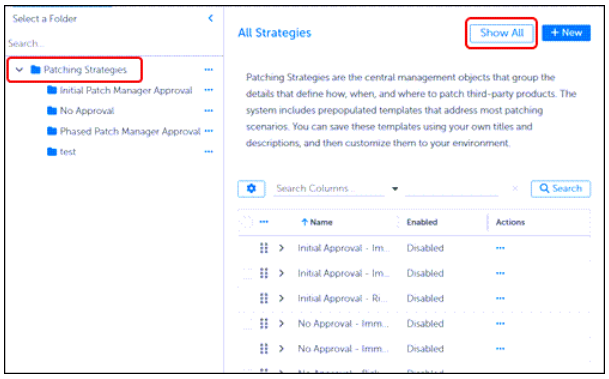
  Approval step required between each wave of the deployment, and then deploys the updates at once to all devices in the targeted business units based on risk levels. No user interaction.

Creating a Patching Strategy

A Patching Strategy template contains specific fields that you can configure to make a unique Patching Strategy for your environment. Adaptiva recommends opening an existing strategy that contains most of the configuration 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 select **Strategy** in the left navigation menu of the Dashboard, and then select **Patching Strategies**.
3. Select **Patching Strategies**, and then select **Show All** to see all available Patching Strategies.



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

4. Select the **Name** of a strategy to open it.
5. Select **More** in the upper left corner of the template, and then select **Save As**:
   a. Enter a unique name that reflects what the strategy does conceptually. For example, `ITS Immediate Daily Product Patching`.
   b. Select **Save as** on the bottom left corner of the dialog. 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 select **Save** on the upper-left of the dialog.

TIP

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

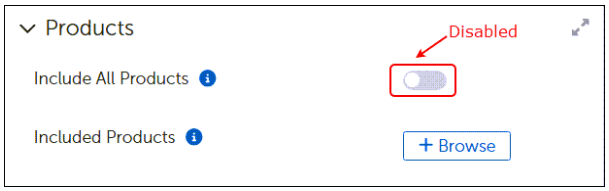
Managing Software Product Selections

In , configuration options provide several opportunities to select or exclude software products for a patching strategy. Options include include making product sections when creating a strategy, exempting products from business units, and more.

For more information about the products available with , see Software Products.

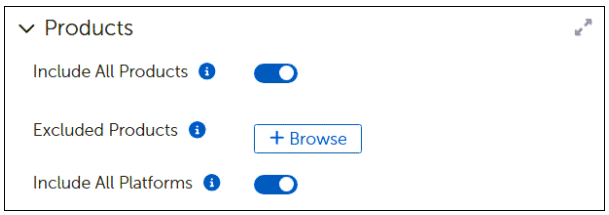
Include All Software Products

1. Scroll to the **Products** workspace in an open Patching Strategy template. The image below shows the default settings.



2. Select the **Include All Products** toggle to enable it.

   The following image shows the default settings and options when you select **Include All Products.**

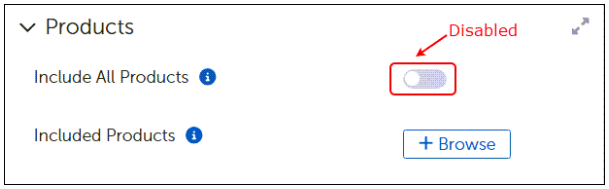


3. Select Save on the upper left corner of the strategy:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** again if you make any changes.

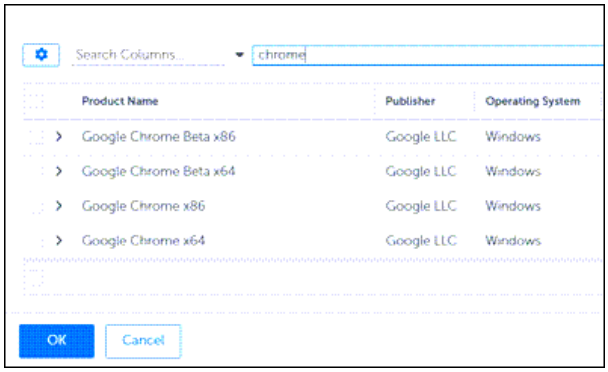
4. Choose one of the following options to continue managing products:
   - To exclude specific products for this strategy, see Exclude Products from a Patching Strategy
   - To include specific platforms, see Include or Exclude Platforms in a Patching Strategy

Include Specific Software Products

1. Scroll to the **Products** workspace in an open Patching Strategy template. The image below shows the default settings.



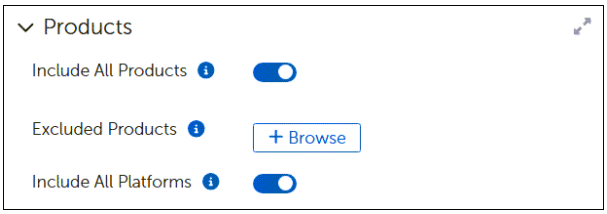
2. Select **+ Browse** to open the **Select Software Product** table:
   a. Enter a product name in the search line, and then select **Search**. This example uses Google Chrome.
   b. Select the product from the list, and then select **OK**.



3. Select **Save** on the upper right corner of the Patching Strategy:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** again if you make any changes.

Exclude Products from a Patching Strategy

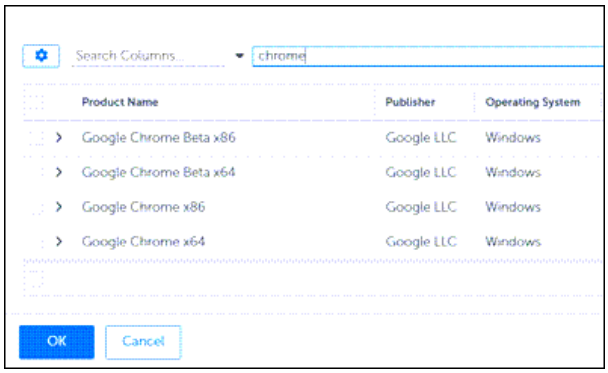
After enabling **Include All Products** from the Products workspace in an open Patching Strategy, you have the option to exclude individual products for the same Patching Strategy.



IMPORTANT

When you add Business Units to a Strategy, the Patching Exceptions set for the Business Unit take precedence over the Product settings in the Patching Strategy.

1. Select + **Browse** to open the **Select Software Product** table:
   a. Enter a product name in the search line, and then select **Search**. This example uses Google Chrome.
   b. Select the product from the list, and then select **OK**.

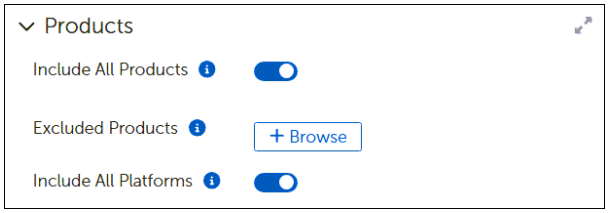


2. Select **Save** on the upper left of the strategy to keep your changes:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** again if you make any changes.

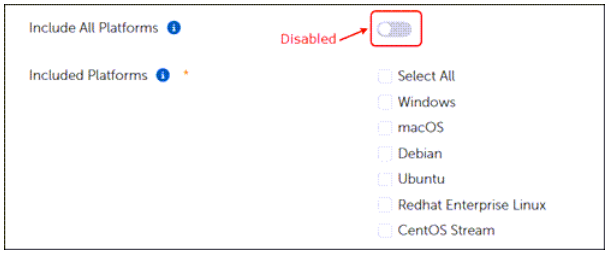
Include or Exclude Platforms in a Patching Strategy

When you enable **Include All Products** from the Products workspace in an open Patching Strategy, you also include all platforms by default.

1. Select + **Browse** to open the **Select Software Product** table:



2. Select the **Include All Platforms** toggle to disable it and view the available Platforms.



3. Decide which platforms to include:
   - To include all Platforms, either **Select All** or select the **Include All Platforms** toggle to enable it.
   - To include specific Platforms, select those you want to include.

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

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

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

Manage Trigger Metadata Properties

Adaptiva provides several Trigger Metadata Properties..

If a trigger metadata property changes in a given patch, and the patch meets each of the requirements below, the Patching process re-presents the patch to the Patching Strategy.

The changed patch must:

- Belong to a product in the strategy
- Be applicable on at least one device.
- Have been presented previously.

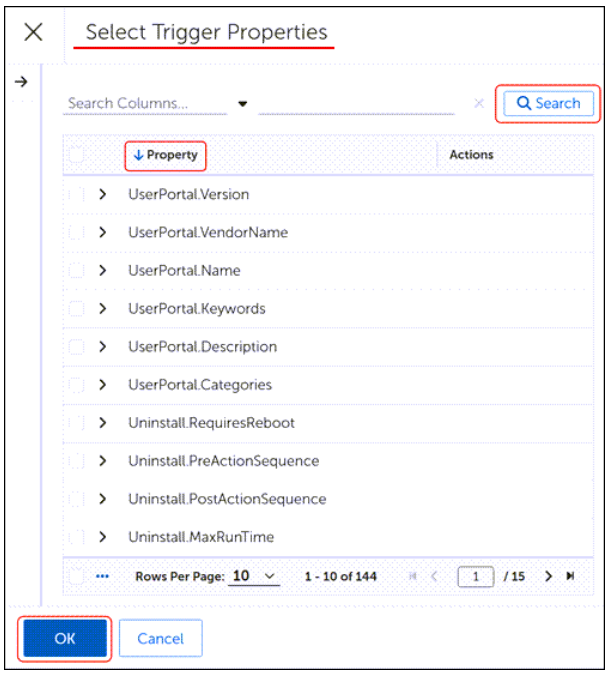
View All Trigger Metadata Properties

1. Scroll down to **Trigger Metadata Properties** in an open Patching Strategy template.
2. Select **+ Select** to open the **Select Trigger Properties** dialog.

Select from all Trigger Properties

The first table you see shows all available trigger properties.

1. In the **Select Trigger Properties** table of the **Trigger Metadata Properties** dialog, select one or more properties to use as triggers:
   - To find a specific trigger, enter a trigger name on the **Search** line, and then select **Search**.
   - To sort the list of Trigger Properties, click Property to reverse the alphabetical support order.
   - To page through the available trigger properties, use the navigation tools on the bottom-right of the dialog.

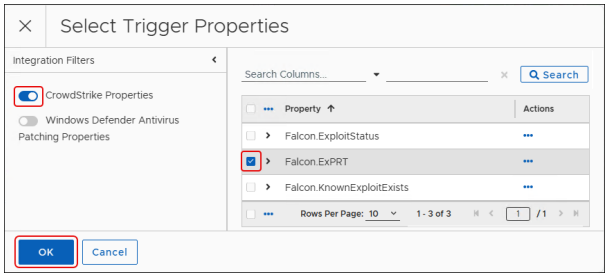


2. Select **OK** on the bottom-left corner of the dialog to save your selections and return to the Patching Strategy template.

Select Only CrowdStrike Falcon Trigger Properties

In the **Select Trigger Properties** table of the **Trigger Metadata Properties** dialog, enable a view of CrowdStrike Falcon properties only.

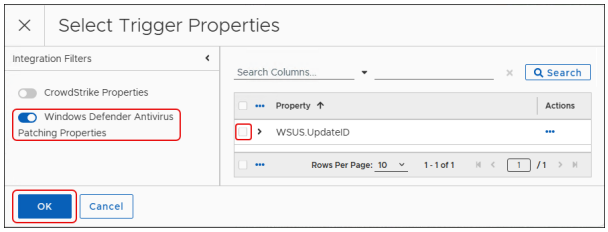
1. Select the **CrowdStrike Properties** toggle to enable or disable (default) a view of Falcon properties only.
2. Select one or more **Falcon** properties from the table.



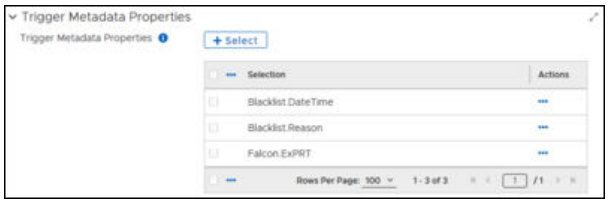
3. Select **OK** at the bottom left of the dialog to save your selections and return to the Patching Strategy template.

Select Only Windows Defender Antivirus Trigger Properties

1. Select the **Windows Defender Antivirus Patching Properties** toggle under **Integration Filters** in the **Select Trigger Properties** dialog.
2. Select a **Windows Defender** property from the table.

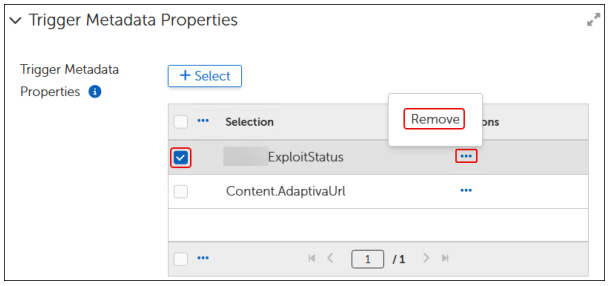


3. Select **OK** at the bottom left of the dialog to save your selections and return to the Patching Strategy template.



Remove Trigger Metadata Properties

1. Scroll down to **Trigger Metadata Properties** in an open Patching Strategy template. If the Patching Strategy includes Trigger Metadata Properties, the table under **+Select** lists those properties.
2. Select the **ellipsis (...)** under **Actions** for the trigger you want to remove, and then select **Remove**.



3. Select **Save** on the upper-left corner of the Patching Strategy to save your changes.

Deployment Settings

Deployment settings in a Patching Strategy include choosing a Deployment Wave, Creating a Deployment Bot Runtime configuration, and choosing whether to present each patch to the first matching Deployment bot only (defaults to disabled). 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 **Deployment Wave** in the **Deployment Settings** workspace of an open Patching Strategy template.

   This opens the **All Deployment Wave** dialog.
2. Select a **Deployment Wave** from the list.

- Adaptiva provides a **Single Wave-All Clients** Deployment Wave, which includes a Business Unit called **All Clients Business Unit**.
- If you are following the tasks in **Introduction to Patching Strategies**, choose **Single Wave-All Clients**.

3. Select **OK** on the bottom left of the dialog to return to the Patching Strategy.
4. Select **OK** to close the recommendation. The system returns you to the Patching Strategy at the Business Unit Addition Settings workspace:
   - If you are following the tasks in **Introduction to Patching Strategies**, skip to Add Software Products. There is no need to modify the Deployment Bot Runtime settings for purposes of this exercise.
   - If you are creating or modifying a Patching Strategy for ongoing use, continue with the next step.

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.

After adding a Deployment Wave to the Patching Strategy Deployment Settings, you can configure Deployment Bot Runtime scenarios. Follow these procedures for each Deployment Bot Runtime you need to create. If you need to create a Deployment Bot, see Creating Deployment Bots.

See also:

Bots – Patch Deployment and Notification Bots

Patching Processes

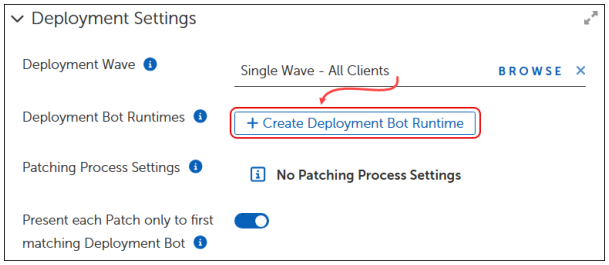
Deployment Channels and Deployment Channel Processes

Business Units and Rollout Processes

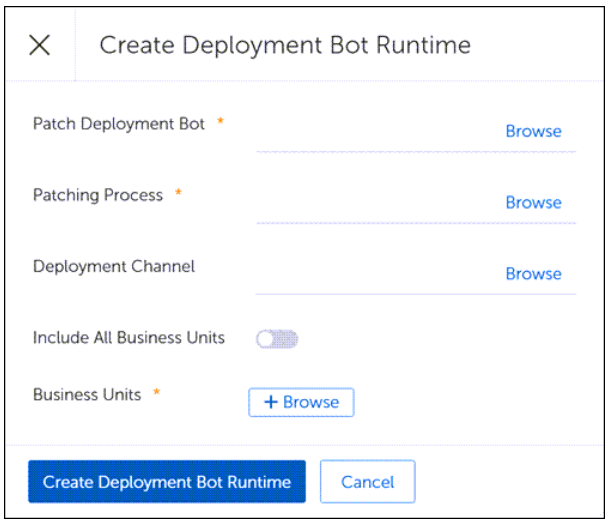
Create Deployment Bot Runtime Scenarios

Before creating a Deployment Bot Runtime, select a Deployment Wave to enable the **Create Deployment Bot Runtime** selection.

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



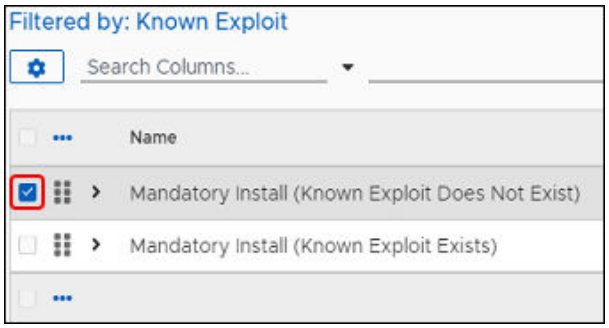
This opens the Create Deployment Bot Runtime dialog:



2. Begin by adding a Patch Deployment Bot.

Add a Patch Deployment Bot (Required)

1. Select **Browse** next to **Patch Deployment Bot** to open the **Select Patch Deployment Bot** dialog.
2. Choose a method for viewing Patch Deployment Bots:



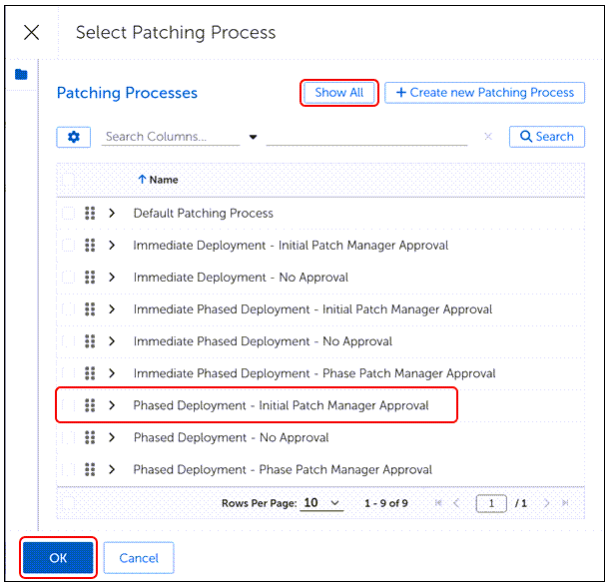
   - Select **Patch Deployment Bots**, and then select Show All to see the available choices.
   - Select a **Filtered by:** setting beneath **Patch Deployment Bots** to see only the items associated with that filter.

3. Select the template you want to use. For example, in **Filtered by: Known Exploit**, select **Mandatory Install (Known Exploit Exists)**.
4. Select **OK** on the bottom left of the dialog to return to the **Create Deployment Bot Runtime** template.

Add a Patching Process (Required)

1. Select **Browse** next to **Add Patching Process** in the Create Deployment Runtime dialog.
2. Select **Patching Processes**, and then 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 **OK** on the bottom left of the dialog.



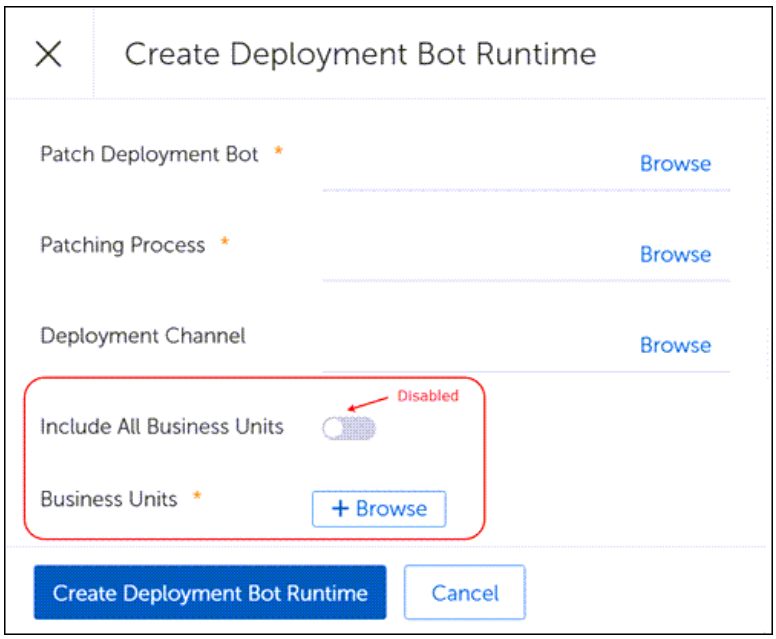
Add a Deployment Channel (Optional)

1. Select **Browse** next to **Add Deployment Channel**.
2. Select **Deployment Channels**, and then 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 OK on the bottom left of the dialog.

Add Business Units (Optional)

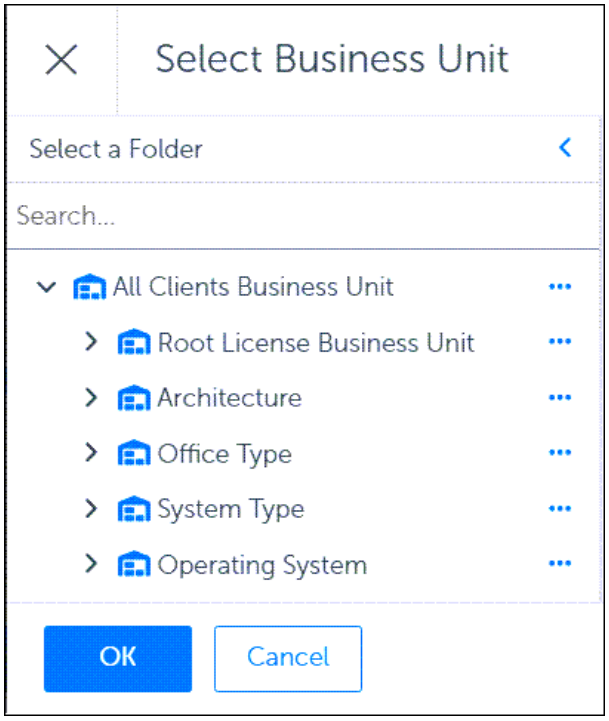
> **IMPORTANT**
> The Business Units you add here must be the same Business Units included in the Patching Strategy Deployment Wave. If you select other Business Units here or select All Business Units, the Patching Strategy will take no action on those that do not match the Deployment Wave settings.

1. Decide whether to include all Business Units in this Deployment Bot Runtime, or to add specific Business Units:
   - To include all Business Units, select the **Include All Business Units** toggle to enable running this configuration on all Business Units (defaults to disabled), and then skip to step 3.



- To choose specific Business Units for this Runtime, select **+ Browse**, 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**.



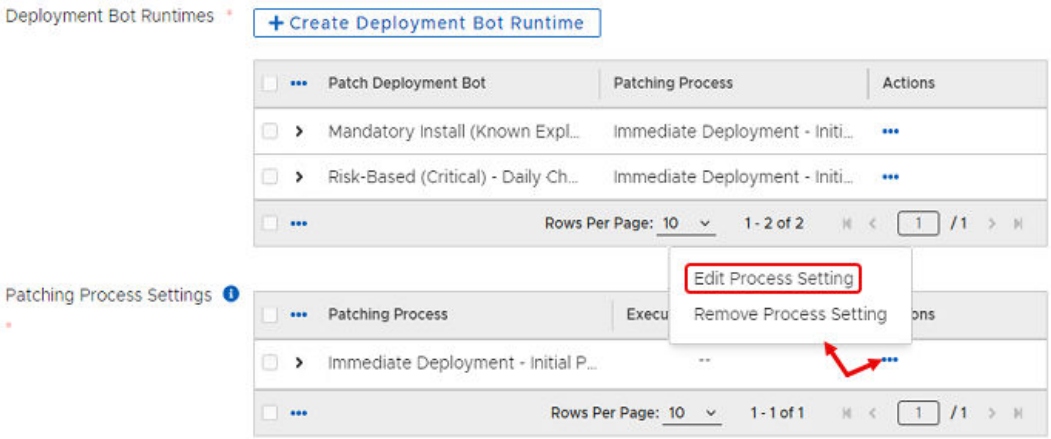
3. Select **OK** on the bottom left of the dialog to view the completed Runtime Bot.
4. Select **Create Deployment Bot Runtime** on the bottom-left corner of the dialog to return to the Patching Strategy.

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

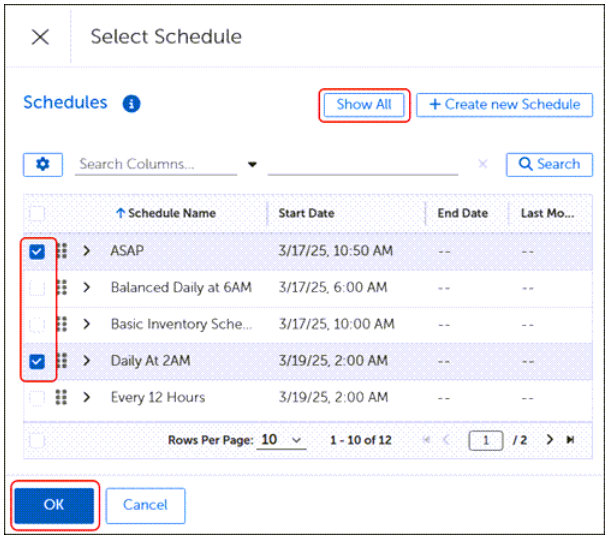
Set the Patching Process Runtime

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. Add one or more schedules for the process:
   a. Select **+ Browse** next to **Execution Schedules**.
   b. Select **Schedules**, and then select **Show All**.



   c. Select one or more schedules to use for the Process Setting runtime, and then select **OK** on the bottom left corner of the dialog.

      All Deployment Bot Runtime pairs that use the same Patching Process in this Patching Strategy run on the schedules you choose.

   d. Enter the number of **Hours**, **Minutes**, and **Seconds** that the patching process may run before timing out. Zero indicates no time limit.

3. Select **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.

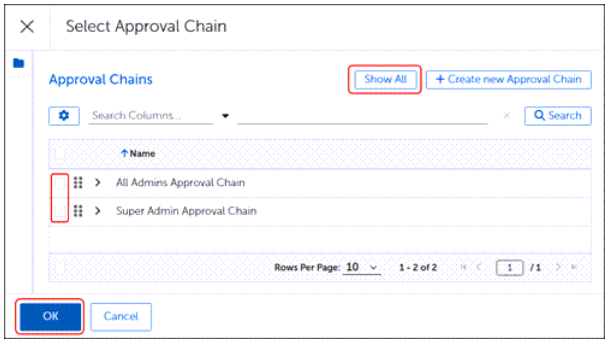
1. Scroll down to the bottom of the **Deployment Settings** workspace of an open Patching Strategy.

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.
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.



4. Select **OK** to return to the object template.
5. Repeat Steps 2 through 4 for each of the groups listed in the **Approval Chains** workspace:
   - Skip any groups that do not apply to your situation.
   - 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

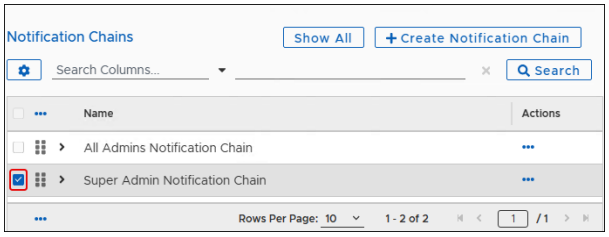
Patching Strategy, Deployment Channel, and Business Unit objects include a **Notifications** dialog where you can configure notification details. The configuration choices differ slightly for each object.

> **IMPORTANT**
> This configuration requires selecting a specific type of Notification Cycle template. Contact Adaptiva 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.



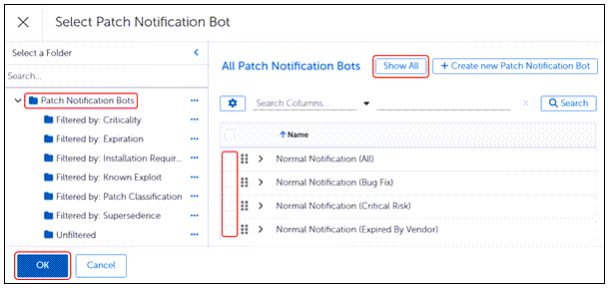
3. Select **Notification Chains**, and then select **Show All** to see the available templates.
4. Select a **Notification Chain** from the table. To edit or create Notification Chains, see Using Notification Chains.
5. Continue editing the **Notification** settings, or select **OK** (lower-left corner) 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 **+Browse** next to **Patch Notification Bots** in the **Notifications** workspace of the object template.

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



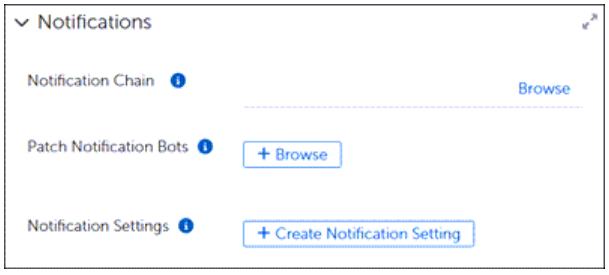
2. Select **Patch Notification Bots**, and then select **Show All** to list all available **Patch Notification Bots**, or select any **Filtered by:** folder to see the Bots associated with that filter.
3. Choose one or more **Notification Bots** to set requirements for this template. To create more Notification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

Create Notification Settings

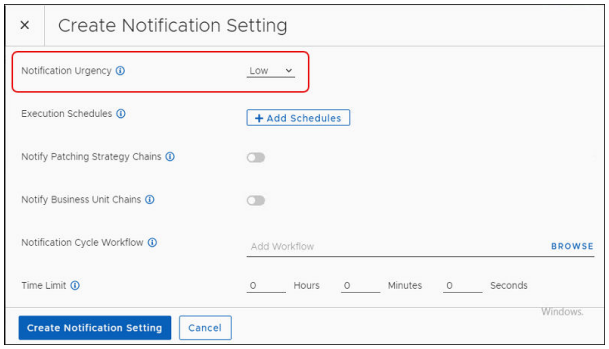
Set Notification Urgency

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** under **Notifications** 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.

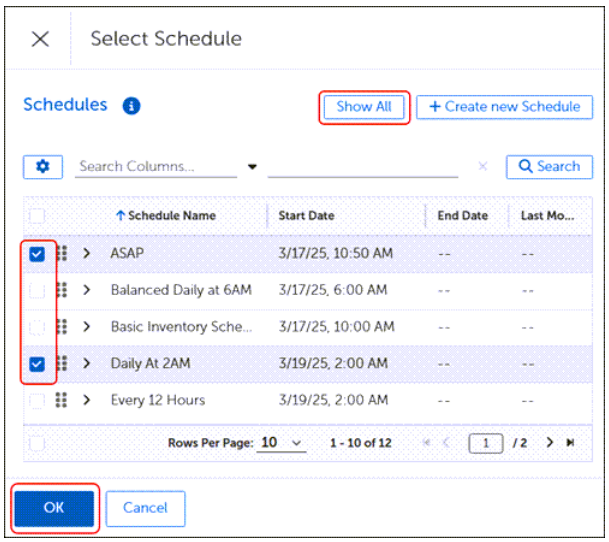


3. Continue editing the **Notification** settings or select Create Notification Settings to return to the template.

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 an object template.
2. Select **+Browse** next to **Execution Schedules** to display the available schedules.
3. Select one or more schedules from the **All Schedules** table, and then select **OK** on the lower-left of the dialog.



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

Enable Notifications for Patching Strategy and Business Unit Chains

When enabled, it 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:
   - 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.
   - 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 select Create Notification Settings to return to the template.

Choose a Notification Cycle Workflow

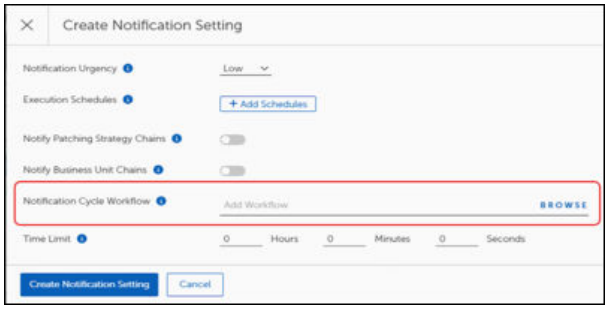
This setting names the Notification Cycle that processes the Notifications for the Patching Strategy or Deployment Channel. Notification Cycle workflows are customized for specific uses. Adaptiva does not provide sample Notification Cycle templates. These templates exist only if you create them for your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

IMPORTANT

Contact Adaptiva Customer Support for assistance with Notification Cycle templates.

1. Select **+Create Notification Setting** under **Notification** 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 select **Add Workflow** on the lower-left of the dialog.
4. Continue editing the **Notification** settings or select Create Notification Settings to return to the template.

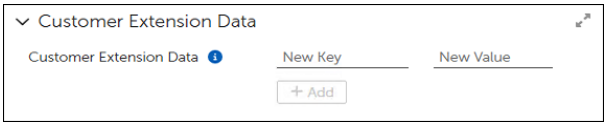
Set the Time Limit

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** under **Notification** 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 select Create Notification Settings to return to the template.

Customer Extension Data

Customer Extension Data is an advanced feature of Adaptiva. 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 Adaptiva Customer Support.

Content Prestaging Settings

The Content Prestaging feature deploys 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 Adaptiva pushes the content to the best-suited sources in all locations that require the content.Adaptiva 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 Adaptiva 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.

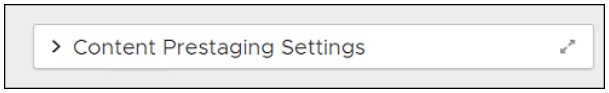
Pull Content

- **Not Enabled** -- Disables any prestaging as part of the Patching Process workflow or Patching Strategy.
- **Handled by System** – The Adaptiva 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.

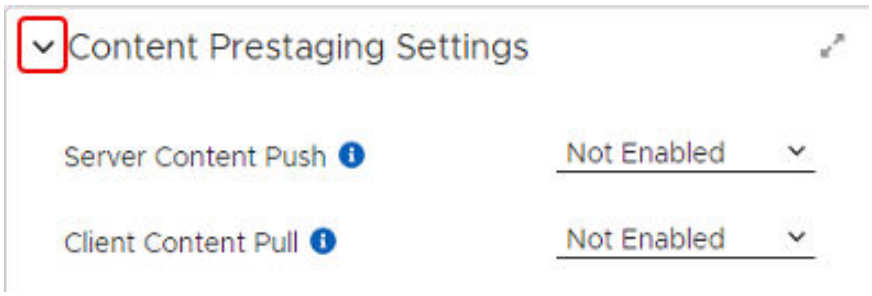
Set Content Prestaging Settings

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

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

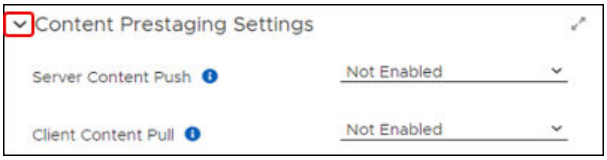


2. Expand the **Content Prestaging Settings** to view the available settings.

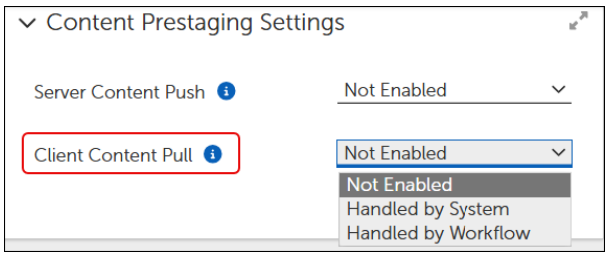


Enable Client Content Pull

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:



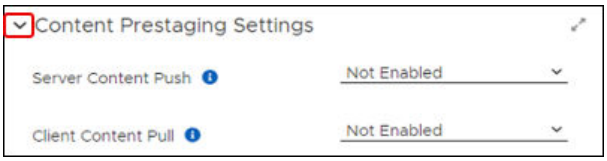
1. Select the arrow to the right of **Client Content Pull** to expand the menu of available options.



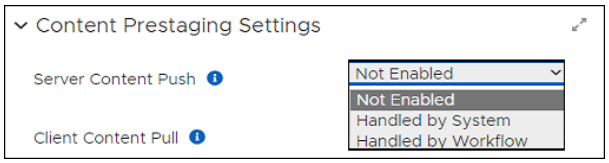
2. Select the option you need for the object template you are using. For definitions of push options, see Defining Content Prestaging Settings.
3. Select **Save** on the upper-left to save your changes:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** again if you make any 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 that has already completed the current patching cycle, you must use the **Business Unit Addition Settings** to add the parent Business Unit that contains the details, such as Patches, Patch Approval Settings, and any Business Unit added to the Strategy will inherit these details.

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 Patch Dashboard.
2. Scroll down to **Business Unit Addition Settings**, and then select the **right arrow** to expand the workspace.

Select a Business Unit

Specify the parent Business Unit for this strategy so that when new Business Units are added to the strategy after it has already run, the new 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 the **Business Unit** that has the parent settings for any future Business Units added to the Strategy.
3. Select **OK** to return to the 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.

> **IMPORTANT**
> If you came to this procedure while you were configuring Deployment Settings in a Patching Strategy, return to Deployment Settings to continue the Strategy configuration.

Select a Patching Process

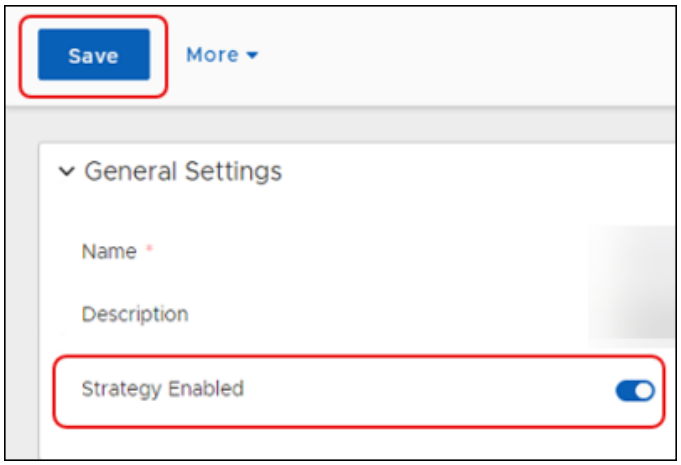
Identify the Patching Process that controls the approval and deployment logic for the existing Business Units in this strategy. This is the same Patching Process identified in the Deployment Bot Runtime, which is the only Patching Process you can choose here. This ensures that any Business Units added after the 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 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 select **OK**.
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, select the **Strategy Enabled** toggle to enable the strategy and make it available for use.

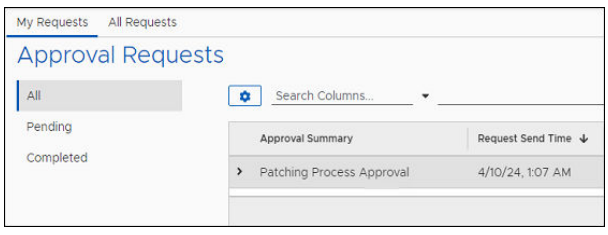


2. Select **Save** on the upper-left corner of the workflow to save the strategy:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** again if you make any changes.
3. Move the saved template to your folder.

View a Staged Patching Strategy

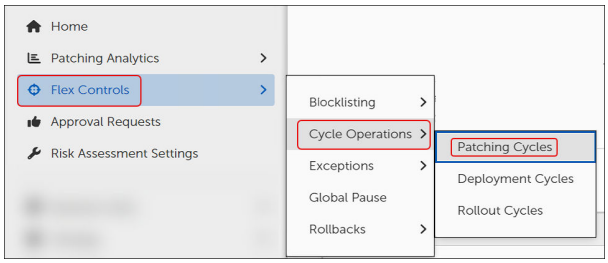
After you Enable the Patching Strategy, you can view the pending approval request.

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

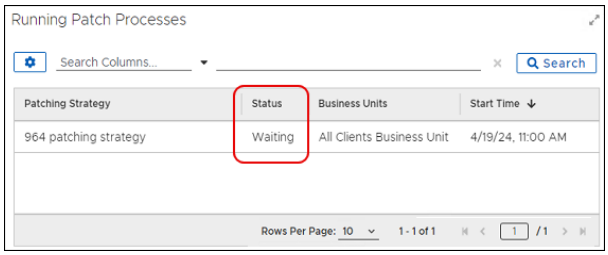


- The view defaults to **All** requests, which includes pending and completed.
- The Patching Strategy you just enabled appears in the **Approval Summary** table with a **Request Status** of **In Progress and Awaiting Response**.

2. Select **Flex Controls > Cycle Operations > Patching Cycles** from the left navigation menu of the 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 select the **Patching Strategy** in the table.
5. Select **Approve**, and then select **Back to Approval Requests**. You can wait until the patch time passes, or you can start the deployment manually.

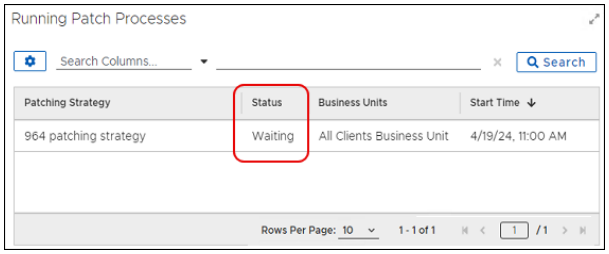
IMPORTANT

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

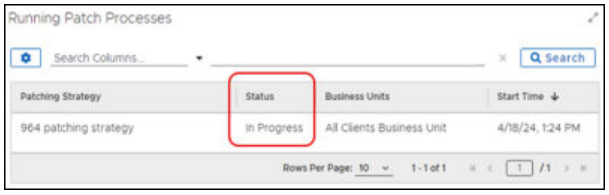
Start the Patching Strategy Manually

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 select the name of the Patching Strategy to open the **Cycle Information**.



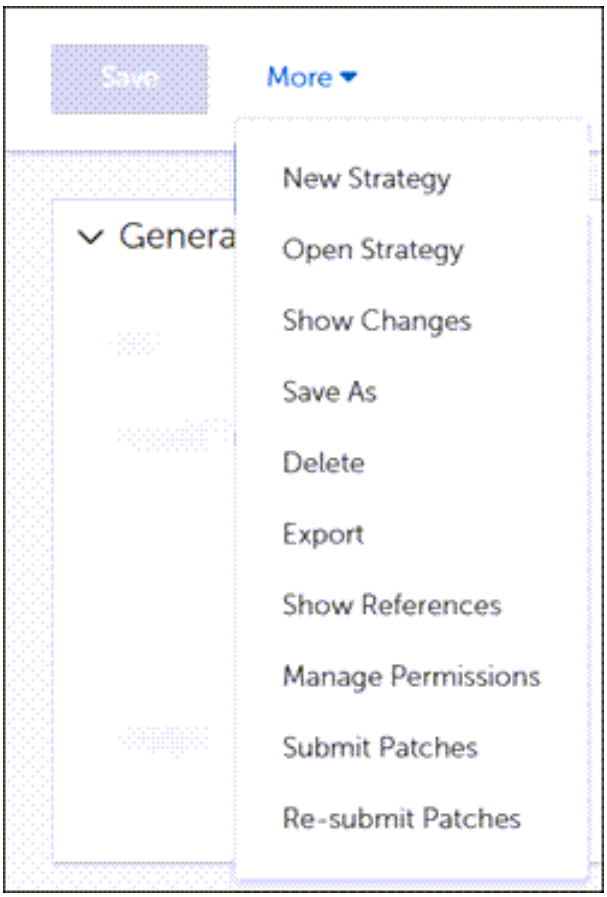
2. Select Play under **Cycle Information**, and then select **Close**. This returns you to the **Patching Cycles** workspace where you can view **Running Patch Processes**.



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

Managing Enabled Patching Strategies

OneSite Patch provides simplified processes to manage and modify Patching Strategies that you have already enabled. From an open, enabled Patching Strategies, the **More** menu contains the following options:

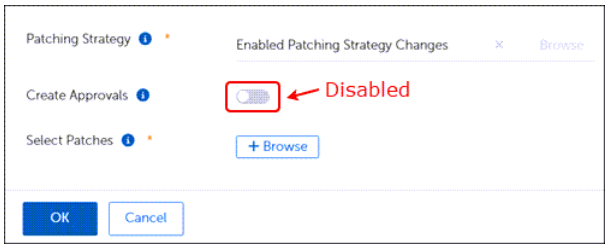


Delete an Enabled Patching Strategy

1. Select **Strategy > Patching Strategies** and navigate to the enabled strategy you want to delete.
2. Select the Strategy Name to open it.
3. Select **More**, and then select **Delete**. The system prompts you to verify the deletion.
4. Click **OK** to permanently delete the Patching Strategy.

Submit Patches to an Enabled Patching Strategy

1. Select **Strategy > Patching Strategies**, and then navigate to the enabled strategy you want to submit.
2. Select the strategy **Name** to open it.
3. Select **More**, and then select **Submit Patches**. This opens the dialog for the selected strategy.



4. Choose one of the following options:
   - To create approvals, select the **Create Approvals** toggle to enable Patch Approvals, and then select **+ Create Patch Approval**. See Approvals for Adding Patches.
   - To choose patches, select **+ Browse**, and then see Select Installable Software.

Approvals for Adding Patches

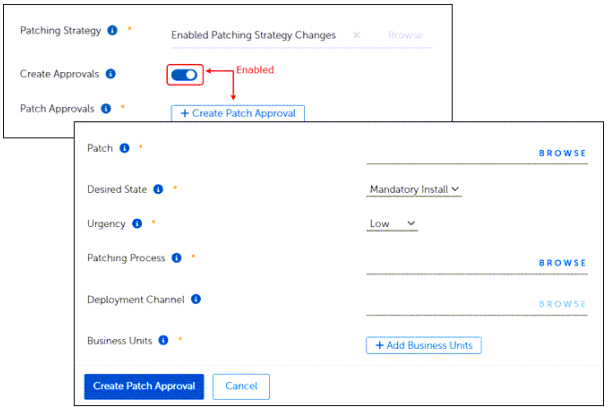
When you submit patches to an enabled strategy, you may also create approvals specific to the individual patch. Otherwise, the patching process and bots create the approvals automatically based on the process or bot settings.

The Create Approvals functionality requires at least one approval scenario. You must create separate approvals for each patch you choose to add to an enabled patch.

Approvals in this instance consist of the following, required settings:

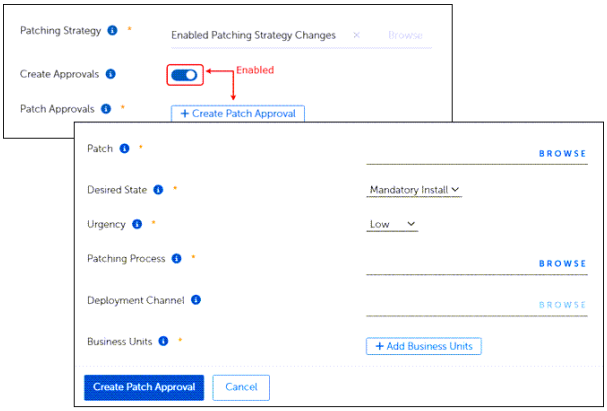
- Identify the patches or software that require approval.
- Set the state and urgency for the approval.
- Add a Patching Process
- Add Business Units

You may also add a Deployment Channel (optional).

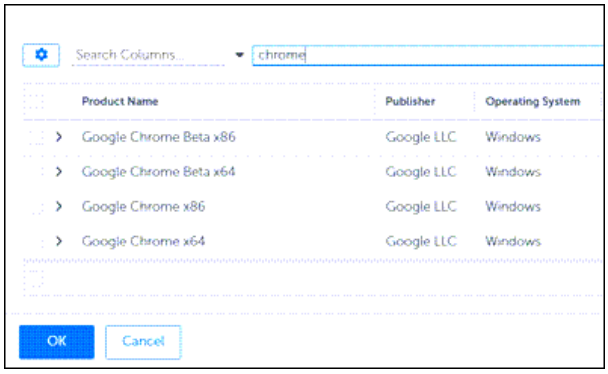


Create an Approval for an Added Patch

Complete the required fields in the **Create Patch Approval** dialog. The dialog already includes the name of the Patching Strategy you chose to modify.



1. Select **+ Browse** for **Patch** to select the patch to add. This opens a software selection table.
   a. Enter a product name in the search line, and then select **Search**. This example uses Google Chrome.
   b. Select the product from the list, and then select **OK**.



2. Select the **Desired State** for the patch approval, and then select the **Urgency** (Low, Normal, High, Critical):
   - **Mandatory Install:** Allows client devices to treat the product as mandatory for installation purposes.
   - **Do Not Install:** Allows client devices to block the installation of a particular product.
   - **Rollback:** Forces a rollback to a specific product version on a client device, when OneSite Patch detects a later product version than allowed.
   - **Uninstall:** Removes the product from client devices in the specified Business Unit.

3. Add a **Patching Process** (required) and a **Deployment Channel** (optional):

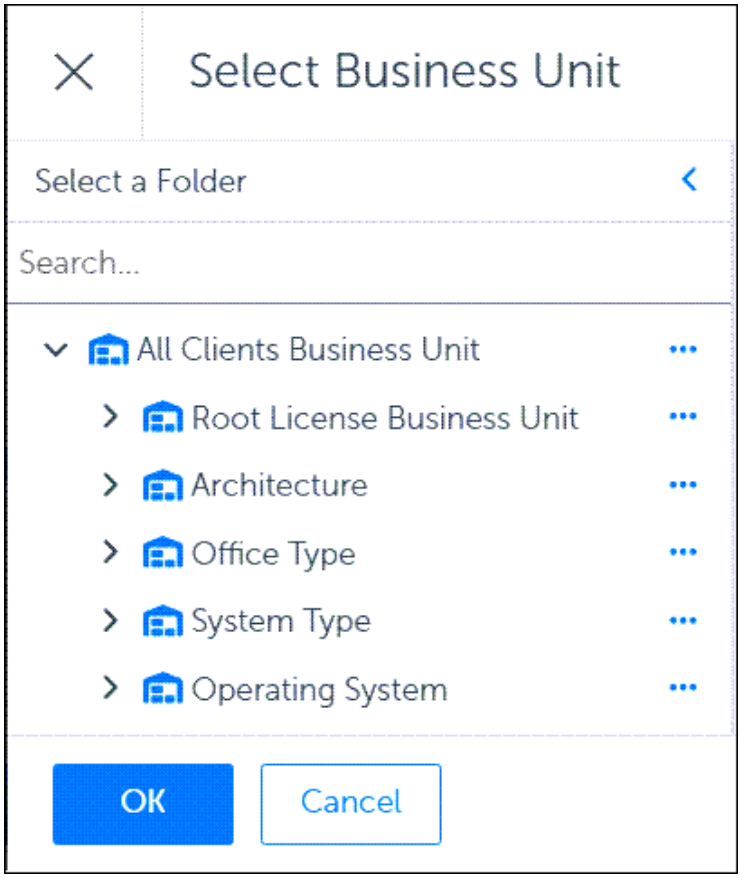
> **TIP**
>
> Add a Deployment Channel only when you have included it in the Deployment Bot Runtimes section of the Patching Strategy Deployment Settings.

   a. (Required) Select **Browse** next to **Patching Process**, and then select a process from the table.
   b. Select **OK** to return to the patch approval dialog.

c. (Optional) Select **Browse** next to **Add Deployment Channel**, and then select a channel from the table (see **Tip** above).

d. Select **OK** to continue creating the approval.

4. Select **+ Browse** next to **Business Units** to open the dialog.
   a. Select the Business Units.



   b. Select **OK**.

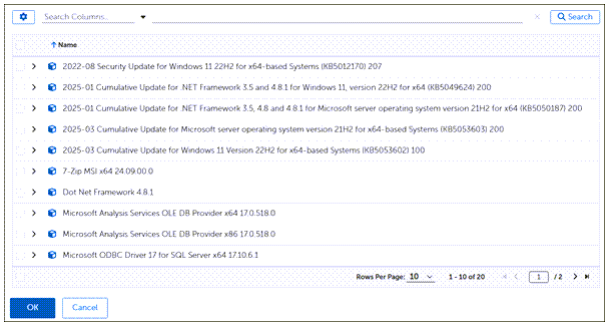
5. Complete the approval for the selected patch:
   a. Select **Create Patch Approval**. The patch submission now includes a table that lists the patch you selected.

   b. (Optional) Return to **Step 1** to create a patch approval for another patch.

   c. Select **OK** to return to the dialog.

Resubmit an Enabled Strategy

1. Select **Strategy > Patching Strategies**, and then navigate to the enabled strategy you want to resubmit.
2. Select the strategy name to open it.
3. Select **More**, and then select **Re-submit Patches**. This opens a table of applicable patches for the selected strategy.



4. Select the patches you want to resubmit with this strategy, and then click **OK**.
5. To verify the status of your Approval Request, see Approval Requests.

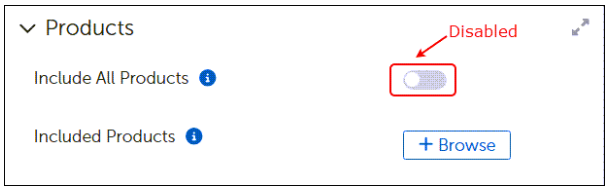
Managing Software Product Selections

In , configuration options provide several opportunities to select or exclude software products for a patching strategy. Options include include making product sections when creating a strategy, exempting products from business units, and more.

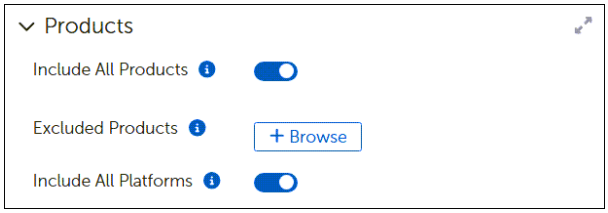
For more information about the products available with , see Software Products.

Include All Software Products

1. Scroll to the **Products** workspace in an open Patching Strategy template. The image below shows the default settings.



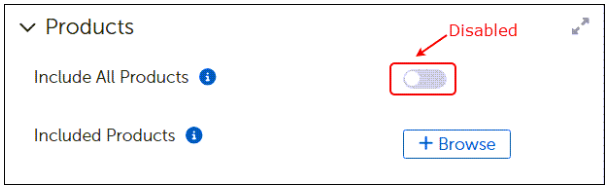
2. Select the **Include All Product**s toggle to enable it.
   The following image shows the default settings and options when you select **Include All Products.**



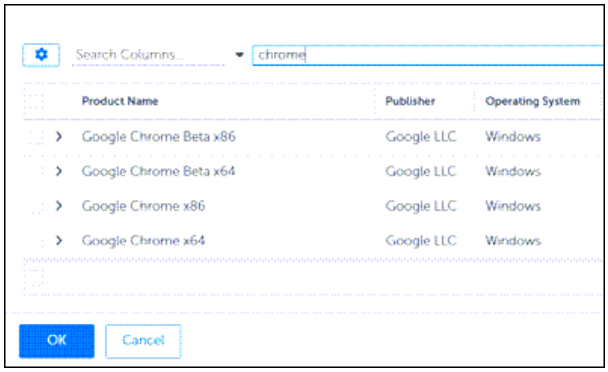
3. Select Save on the upper left corner of the strategy:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** again if you make any changes.
4. Choose one of the following options to continue managing products:
   - To exclude specific products for this strategy, see Exclude Products from a Patching Strategy
   - To include specific platforms, see Include or Exclude Platforms in a Patching Strategy

Include Specific Software Products

1. Scroll to the **Products** workspace in an open Patching Strategy template. The image below shows the default settings.



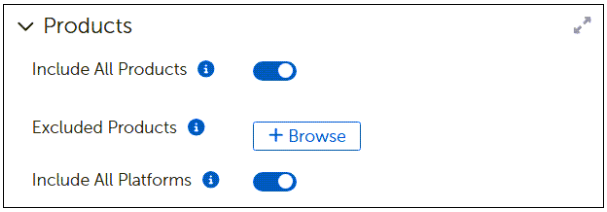
2. Select **+ Browse** to open the **Select Software Product** table:
   a. Enter a product name in the search line, and then select **Search**. This example uses Google Chrome.
   b. Select the product from the list, and then select **OK**.



3. Select **Save** on the upper right corner of the Patching Strategy:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** again if you make any changes.

Exclude Products from a Patching Strategy

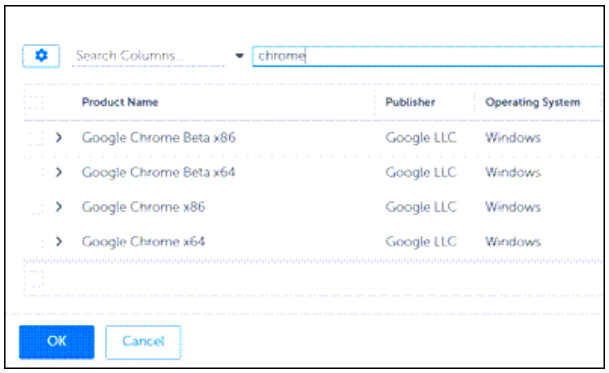
After enabling **Include All Products** from the Products workspace in an open Patching Strategy, you have the option to exclude individual products for the same Patching Strategy.



IMPORTANT

When you add Business Units to a Strategy, the Patching Exceptions set for the Business Unit take precedence over the Product settings in the Patching Strategy.

1. Select + **Browse** to open the **Select Software Product** table:
   a. Enter a product name in the search line, and then select **Search**. This example uses Google Chrome.
   b. Select the product from the list, and then select **OK**.

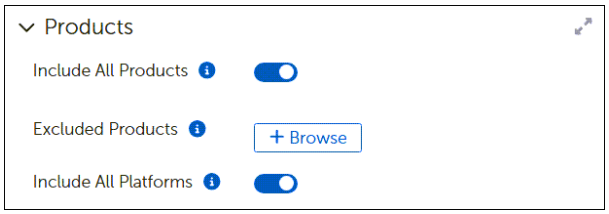


2. Select **Save** on the upper left of the strategy to keep your changes:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** again if you make any changes.

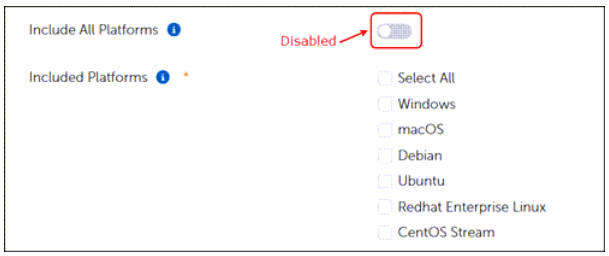
Include or Exclude Platforms in a Patching Strategy

When you enable **Include All Products** from the Products workspace in an open Patching Strategy, you also include all platforms by default.

1. Select + **Browse** to open the **Select Software Product** table:



2. Select the **Include All Platforms** toggle to disable it and view the available Platforms.



3. Decide which platforms to include:
   - To include all Platforms, either **Select All** or select the **Include All Platforms** toggle to enable it.
   - To include specific Platforms, select those you want to include.

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

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

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

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, OneSite Patch 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 Customer SupportAdaptiva 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.

Patching Strategy Templates

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

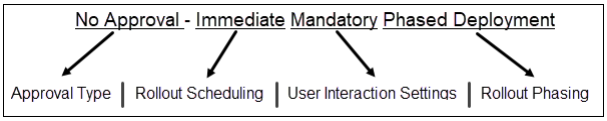
Recommended Use

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.

recommends creating a folder to hold all new or customized strategies. This separates them from the strategies provided with the product.

Patching Strategy Template Naming Conventions

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:
  - **No Approval:** Deploys at once.
  - **Initial Approval**: Requires approval prior to deploying.
  - **Phased Approval**: Requires approval between each wave in the Deployment Waves object.
- **Rollout Scheduling**: Defines the schedule and impact of a deployment.
  - **Immediate**: All product patches deploy at once.
  - **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.
  - **Mandatory**: Alerts the end user who can postpone depending on User Interaction Settings but cannot decline. All product patches deploy at once.
  - **Options**: Alerts the end user. Otherwise, functionality not available in this release.
- **Rollout Phasing**: Deploys in separate phases to allow a review before continuing.
  - 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.

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**

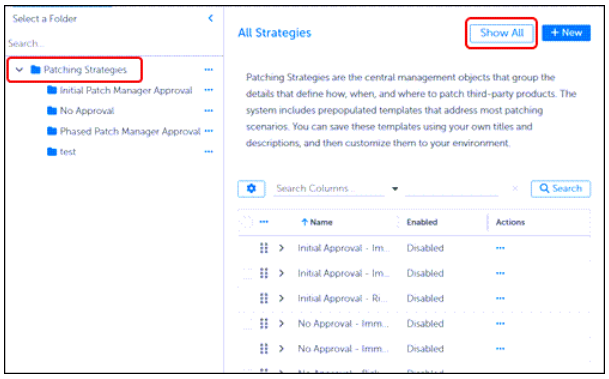
  Approval step required between each wave of the deployment, and then deploys the updates at once to all devices in the targeted business units based on risk levels. No user interaction.

Creating a Patching Strategy

A Patching Strategy template contains specific fields that you can configure to make a unique Patching Strategy for your environment. Adaptiva recommends opening an existing strategy that contains most of the configuration 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 select **Strategy** in the left navigation menu of the Dashboard, and then select **Patching Strategies**.
3. Select **Patching Strategies**, and then select **Show All** to see all available Patching Strategies.



   For descriptions of each template type, see Patching Strategy Templates.
4. Select the **Name** of a strategy to open it.
5. Select **More** in the upper left corner of the template, and then select **Save As**:
   a. Enter a unique name that reflects what the strategy does conceptually. For example, `ITS Immediate Daily Product Patching`.
   b. Select **Save as** on the bottom left corner of the dialog. 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 select **Save** on the upper-left of the dialog.

TIP

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

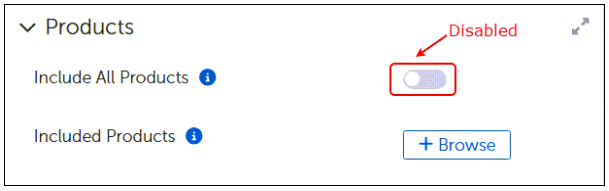
Managing Software Product Selections

In , configuration options provide several opportunities to select or exclude software products for a patching strategy. Options include include making product sections when creating a strategy, exempting products from business units, and more.

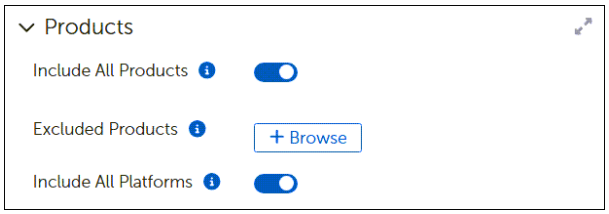
For more information about the products available with , see Software Products.

Include All Software Products

1. Scroll to the **Products** workspace in an open Patching Strategy template. The image below shows the default settings.



2. Select the **Include All Products** toggle to enable it.
   The following image shows the default settings and options when you select **Include All Products.**

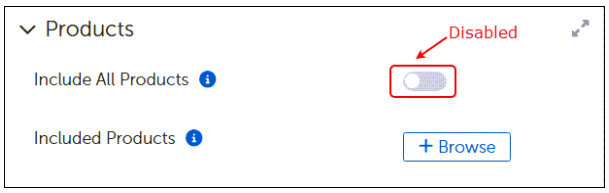


3. Select Save on the upper left corner of the strategy:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** again if you make any changes.

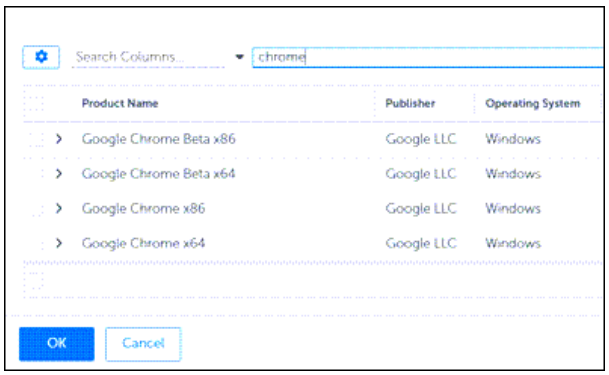
4. Choose one of the following options to continue managing products:
   - To exclude specific products for this strategy, see Exclude Products from a Patching Strategy
   - To include specific platforms, see Include or Exclude Platforms in a Patching Strategy

Include Specific Software Products

1. Scroll to the **Products** workspace in an open Patching Strategy template. The image below shows the default settings.



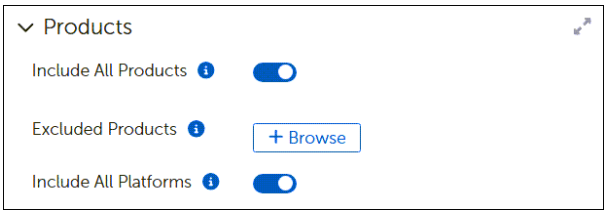
2. Select **+ Browse** to open the **Select Software Product** table:
   a. Enter a product name in the search line, and then select **Search**. This example uses Google Chrome.
   b. Select the product from the list, and then select **OK**.



3. Select **Save** on the upper right corner of the Patching Strategy:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** again if you make any changes.

Exclude Products from a Patching Strategy

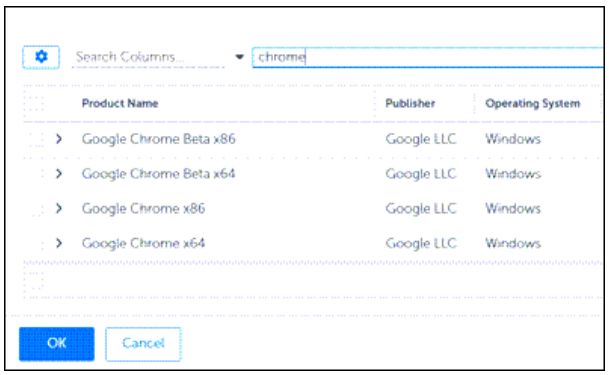
After enabling **Include All Products** from the Products workspace in an open Patching Strategy, you have the option to exclude individual products for the same Patching Strategy.



IMPORTANT

When you add Business Units to a Strategy, the Patching Exceptions set for the Business Unit take precedence over the Product settings in the Patching Strategy.

1. Select **+ Browse** to open the **Select Software Product** table:
   a. Enter a product name in the search line, and then select **Search**. This example uses Google Chrome.
   b. Select the product from the list, and then select **OK**.

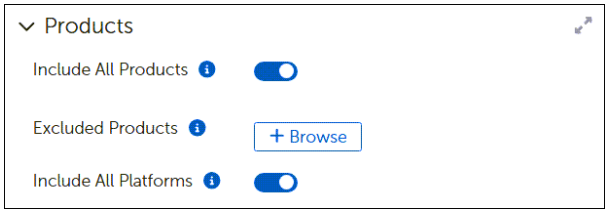


2. Select **Save** on the upper left of the strategy to keep your changes:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** again if you make any changes.

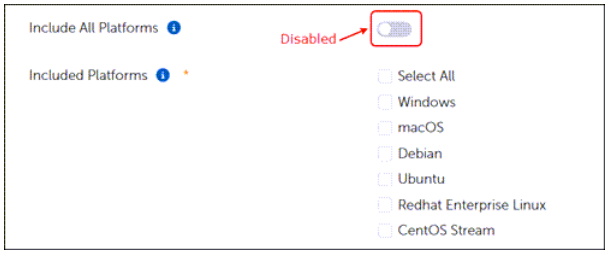
Include or Exclude Platforms in a Patching Strategy

When you enable **Include All Products** from the Products workspace in an open Patching Strategy, you also include all platforms by default.

1. Select **+ Browse** to open the **Select Software Product** table:



2. Select the **Include All Platforms** toggle to disable it and view the available Platforms.



3. Decide which platforms to include:
   - To include all Platforms, either **Select All** or select the **Include All Platforms** toggle to enable it.
   - To include specific Platforms, select those you want to include.

4. Select **Save** on the upper left corner to keep your changes:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** again if you make any changes.

Manage Trigger Metadata Properties

Adaptiva provides several Trigger Metadata Properties..

If a trigger metadata property changes in a given patch, and the patch meets each of the requirements below, the Patching process re-presents the patch to the Patching Strategy.

The changed patch must:

- Belong to a product in the strategy
- Be applicable on at least one device.
- Have been presented previously.

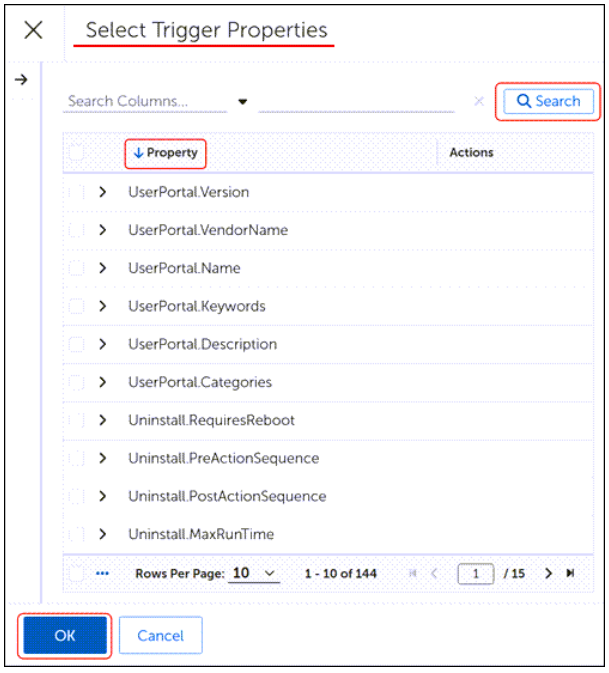
View All Trigger Metadata Properties

1. Scroll down to **Trigger Metadata Properties** in an open Patching Strategy template.
2. Select **+ Select** to open the **Select Trigger Properties** dialog.

Select from all Trigger Properties

The first table you see shows all available trigger properties.

1. In the **Select Trigger Properties** table of the **Trigger Metadata Properties** dialog, select one or more properties to use as triggers:
   - To find a specific trigger, enter a trigger name on the **Search** line, and then select **Search**.
   - To sort the list of Trigger Properties, click Property to reverse the alphabetical support order.
   - To page through the available trigger properties, use the navigation tools on the bottom-right of the dialog.

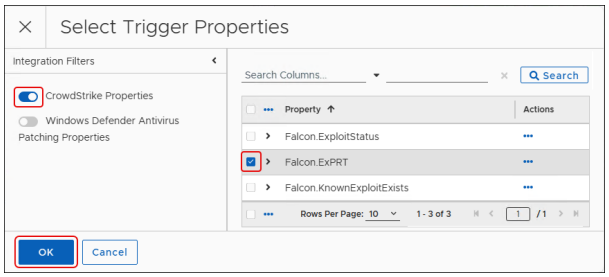


2. Select **OK** on the bottom-left corner of the dialog to save your selections and return to the Patching Strategy template.

Select Only CrowdStrike Falcon Trigger Properties

In the **Select Trigger Properties** table of the **Trigger Metadata Properties** dialog, enable a view of CrowdStrike Falcon properties only.

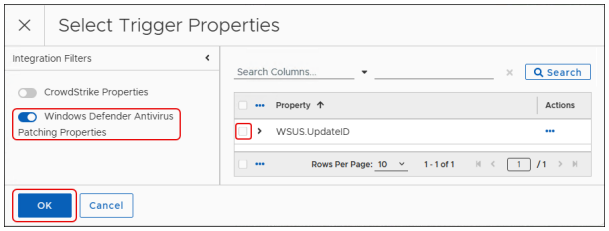
1. Select the **CrowdStrike Properties** toggle to enable or disable (default) a view of Falcon properties only.
2. Select one or more **Falcon** properties from the table.



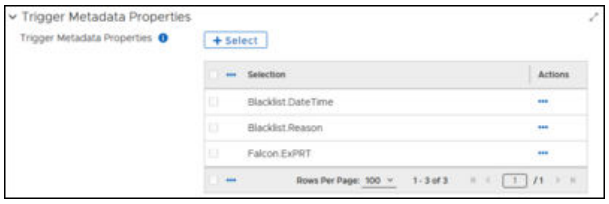
3. Select **OK** at the bottom left of the dialog to save your selections and return to the Patching Strategy template.

Select Only Windows Defender Antivirus Trigger Properties

1. Select the **Windows Defender Antivirus Patching Properties** toggle under **Integration Filters** in the **Select Trigger Properties** dialog.
2. Select a **Windows Defender** property from the table.



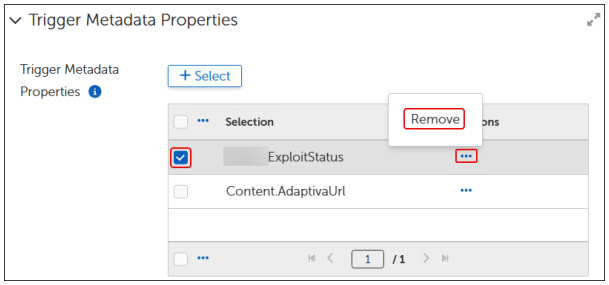
3. Select **OK** at the bottom left of the dialog to save your selections and return to the Patching Strategy template.



Remove Trigger Metadata Properties

1. Scroll down to **Trigger Metadata Properties** in an open Patching Strategy template. If the Patching Strategy includes Trigger Metadata Properties, the table under **+Select** lists those properties.

2. Select the **ellipsis (...)** under **Actions** for the trigger you want to remove, and then select **Remove**.



3. Select **Save** on the upper-left corner of the Patching Strategy to save your changes.

Deployment Settings

Deployment settings in a Patching Strategy include choosing a Deployment Wave, Creating a Deployment Bot Runtime configuration, and choosing whether to present each patch to the first matching Deployment bot only (defaults to disabled). 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 **Deployment Wave** in the **Deployment Settings** workspace of an open Patching Strategy template.

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

2. Select a **Deployment Wave** from the list.
   - Adaptiva provides a **Single Wave-All Clients** Deployment Wave, which includes a Business Unit called **All Clients Business Unit**.
   - If you are following the tasks in **Introduction to Patching Strategies**, choose **Single Wave-All Clients**.

3. Select **OK** on the bottom left of the dialog to return to the Patching Strategy.
4. Select **OK** to close the recommendation. The system returns you to the Patching Strategy at the Business Unit Addition Settings workspace:
   - If you are following the tasks in **Introduction to Patching Strategies**, skip to Add Software Products. There is no need to modify the Deployment Bot Runtime settings for purposes of this exercise.
   - If you are creating or modifying a Patching Strategy for ongoing use, continue with the next step.

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.

After adding a Deployment Wave to the Patching Strategy Deployment Settings, you can configure Deployment Bot Runtime scenarios. Follow these procedures for each Deployment Bot Runtime you need to create. If you need to create a Deployment Bot, see Creating Deployment Bots.

See also:

Bots – Patch Deployment and Notification Bots

Patching Processes

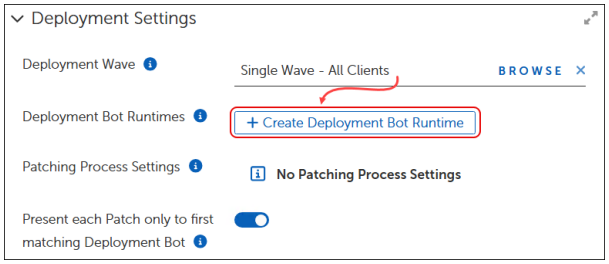
Deployment Channels and Deployment Channel Processes

Business Units and Rollout Processes

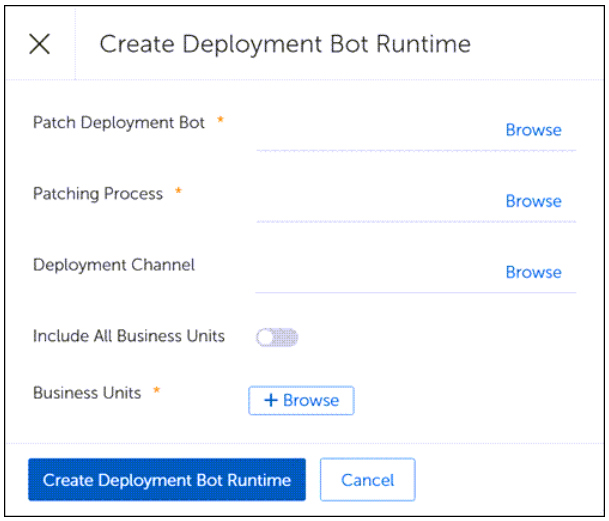
Create Deployment Bot Runtime Scenarios

Before creating a Deployment Bot Runtime, select a Deployment Wave to enable the **Create Deployment Bot Runtime** selection.

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



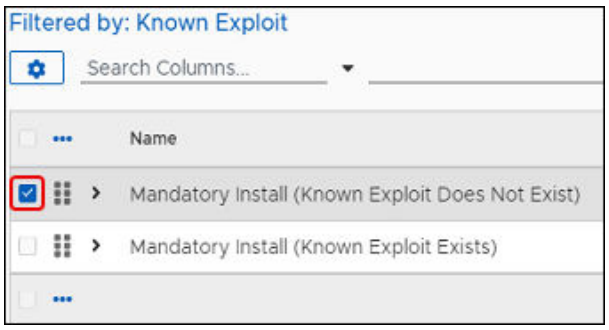
   This opens the Create Deployment Bot Runtime dialog:



2. Begin by adding a Patch Deployment Bot.

Add a Patch Deployment Bot (Required)

1. Select **Browse** next to **Patch Deployment Bot** to open the **Select Patch Deployment Bot** dialog.
2. Choose a method for viewing Patch Deployment Bots:

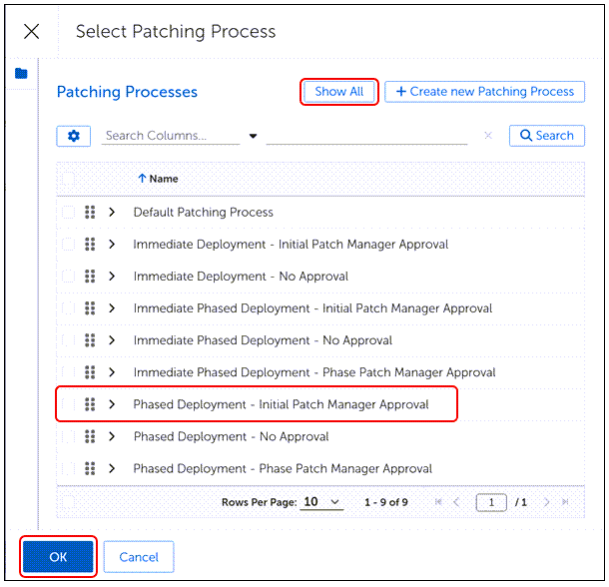


- Select **Patch Deployment Bots**, and then select Show All to see the available choices.
- Select a **Filtered by:** setting beneath **Patch Deployment Bots** to see only the items associated with that filter.

3. Select the template you want to use. For example, in **Filtered by: Known Exploit**, select **Mandatory Install (Known Exploit Exists)**.
4. Select **OK** on the bottom left of the dialog to return to the **Create Deployment Bot Runtime** template.

Add a Patching Process (Required)

1. Select **Browse** next to **Add Patching Process** in the Create Deployment Runtime dialog.
2. Select **Patching Processes**, and then 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 **OK** on the bottom left of the dialog.



Add a Deployment Channel (Optional)

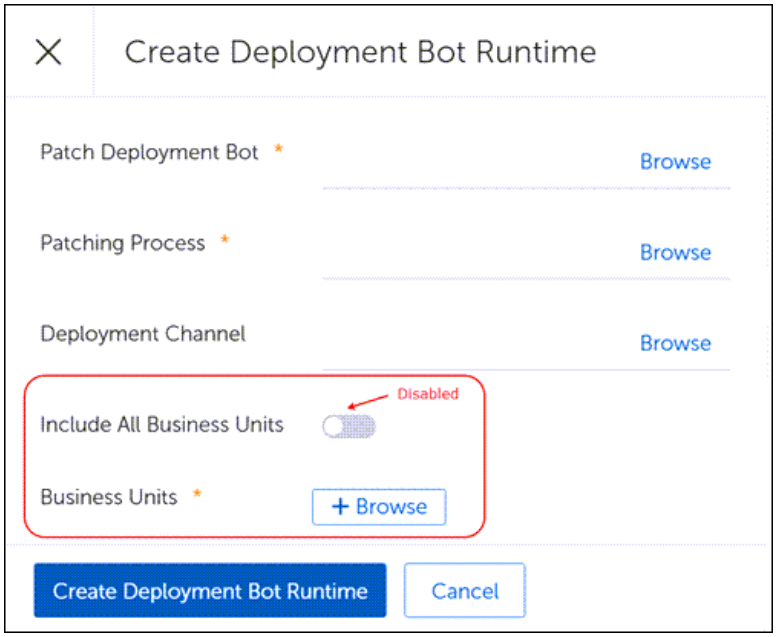
1. Select **Browse** next to **Add Deployment Channel**.

2. Select **Deployment Channels**, and then 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 OK on the bottom left of the dialog.

Add Business Units (Optional)

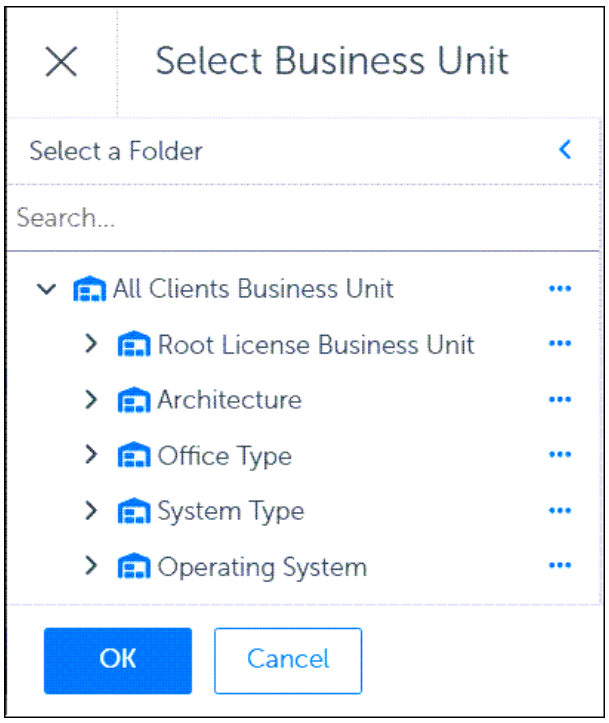
> **IMPORTANT**
>
> The Business Units you add here must be the same Business Units included in the Patching Strategy Deployment Wave. If you select other Business Units here or select All Business Units, the Patching Strategy will take no action on those that do not match the Deployment Wave settings.

1. Decide whether to include all Business Units in this Deployment Bot Runtime, or to add specific Business Units:
   - To include all Business Units, select the **Include All Business Units** toggle to enable running this configuration on all Business Units (defaults to disabled), and then skip to step 3.



   - To choose specific Business Units for this Runtime, select **+ Browse**, 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**.

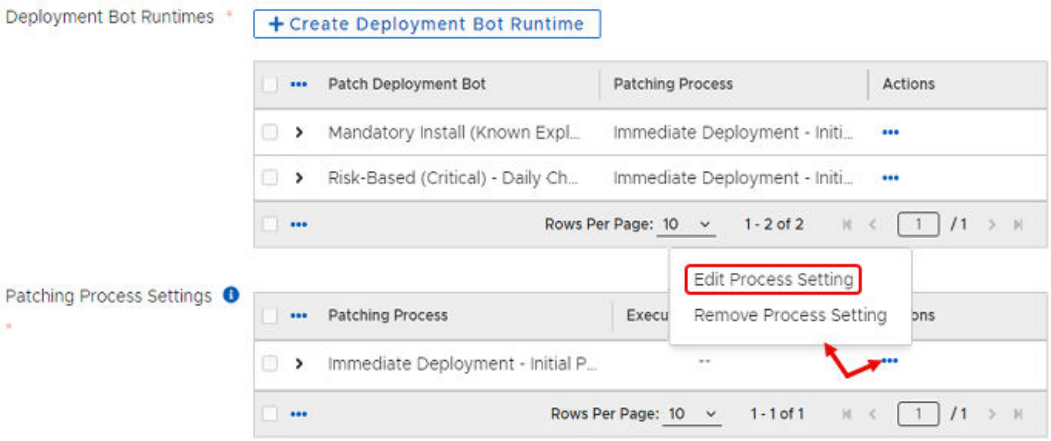


3. Select **OK** on the bottom left of the dialog to view the completed Runtime Bot.
4. Select **Create Deployment Bot Runtime** on the bottom-left corner of the dialog to return to the Patching Strategy.
5. Return to Create Deployment Bot Runtime Scenarios to add more Deployment Bot/Patching Process pairs to this Patching Strategy.

Set the Patching Process Runtime

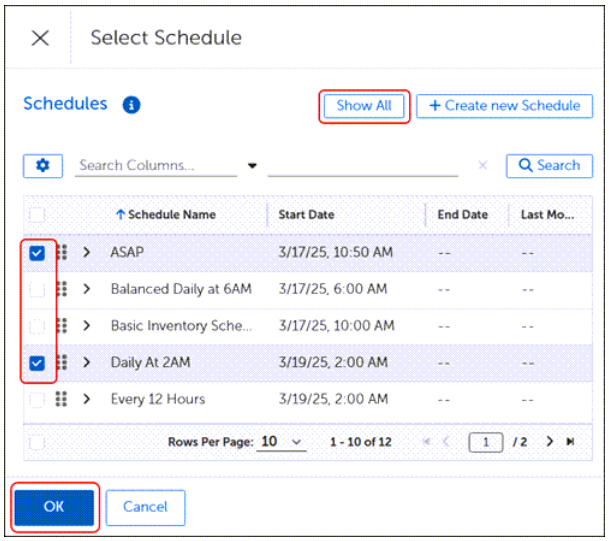
After creating a Deployment Bot Runtime, set the runtime schedule for each Patching Process.

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. Add one or more schedules for the process:
   a. Select **+ Browse** next to **Execution Schedules**.

b. Select **Schedules**, and then select **Show All**.



c. Select one or more schedules to use for the Process Setting runtime, and then select **OK** on the bottom left corner of the dialog.

   All Deployment Bot Runtime pairs that use the same Patching Process in this Patching Strategy run on the schedules you choose.

d. Enter the number of **Hours**, **Minutes**, and **Seconds** that the patching process may run before timing out. Zero indicates no time limit.

3. Select **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.

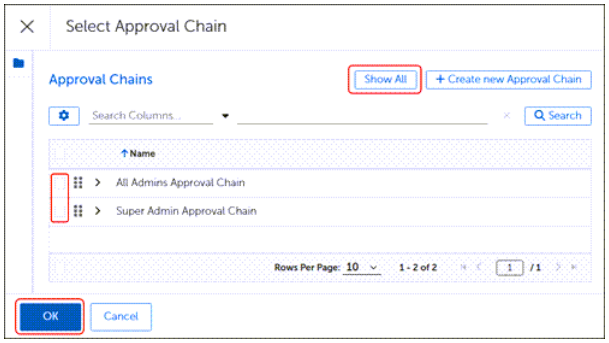
1. Scroll down to the bottom of the **Deployment Settings** workspace of an open Patching Strategy.

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.
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.



4. Select **OK** to return to the object template.
5. Repeat Steps 2 through 4 for each of the groups listed in the **Approval Chains** workspace:
   - Skip any groups that do not apply to your situation.
   - 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.

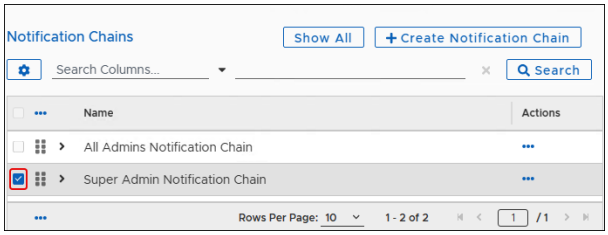
IMPORTANT

This configuration requires selecting a specific type of Notification Cycle template. Contact Adaptiva 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.



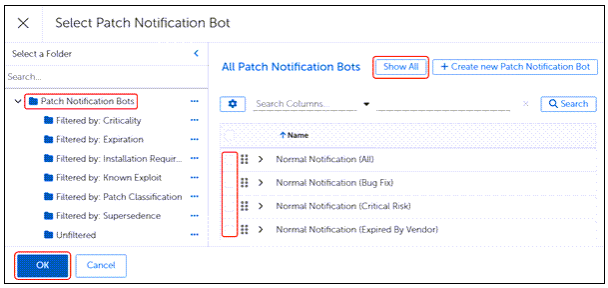
3. Select **Notification Chains**, and then select **Show All** to see the available templates.
4. Select a **Notification Chain** from the table. To edit or create Notification Chains, see Using Notification Chains.
5. Continue editing the **Notification** settings, or select **OK** (lower-left corner) 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 **+Browse** next to **Patch Notification Bots** in the **Notifications** workspace of the object template.

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



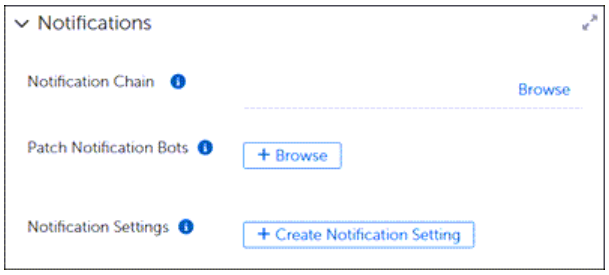
2. Select **Patch Notification Bots**, and then select **Show All** to list all available **Patch Notification Bots**, or select any **Filtered by:** folder to see the Bots associated with that filter.
3. Choose one or more **Notification Bots** to set requirements for this template. To create more Notification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

Create Notification Settings

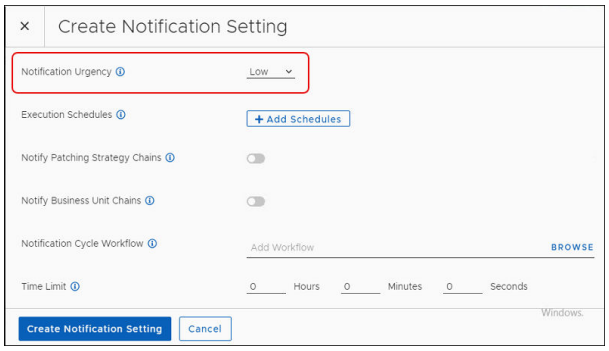
Set Notification Urgency

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** under **Notifications** 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.

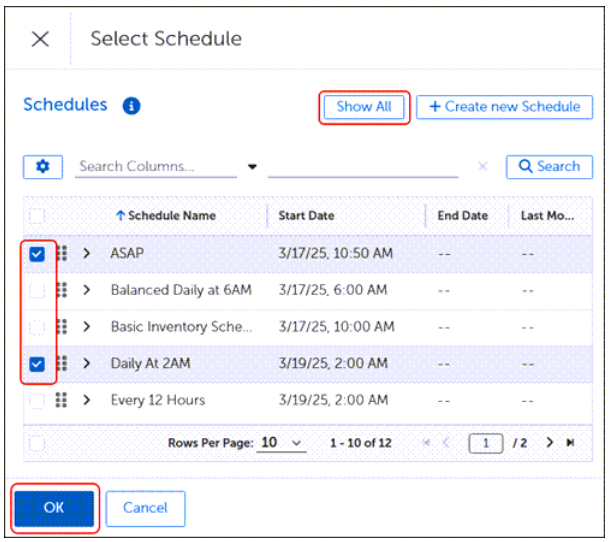


3. Continue editing the **Notification** settings or select Create Notification Settings to return to the template.

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 an object template.
2. Select **+Browse** next to **Execution Schedules** to display the available schedules.
3. Select one or more schedules from the **All Schedules** table, and then select **OK** on the lower-left of the dialog.



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

Enable Notifications for Patching Strategy and Business Unit Chains

When enabled, it 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:
   - 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.
   - 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 select Create Notification Settings to return to the template.

Choose a Notification Cycle Workflow

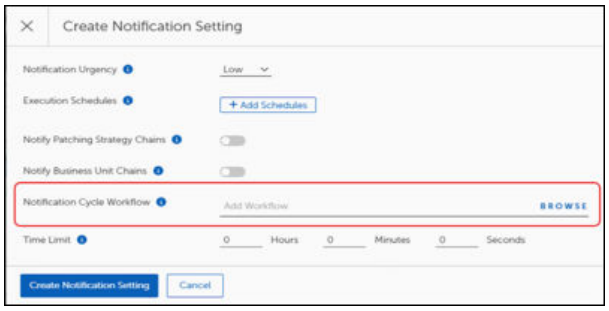
This setting names the Notification Cycle that processes the Notifications for the Patching Strategy or Deployment Channel. Notification Cycle workflows are customized for specific uses. Adaptiva does not provide sample Notification Cycle templates. These templates exist only if you create them for your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

IMPORTANT

Contact Adaptiva Customer Support for assistance with Notification Cycle templates.

1. Select **+Create Notification Setting** under **Notification** 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 select **Add Workflow** on the lower-left of the dialog.
4. Continue editing the **Notification** settings or select Create Notification Settings to return to the template.

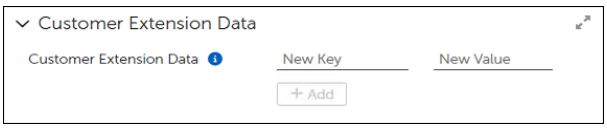
Set the Time Limit

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** under **Notification** 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 select Create Notification Settings to return to the template.

Customer Extension Data

Customer Extension Data is an advanced feature of Adaptiva. 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 Adaptiva Customer Support.

Content Prestaging Settings

The Content Prestaging feature deploys 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 Adaptiva pushes the content to the best-suited sources in all locations that require the content.Adaptiva 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 Adaptiva 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.

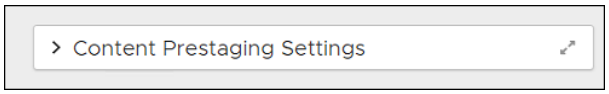
Pull Content

- **Not Enabled** -- Disables any prestaging as part of the Patching Process workflow or Patching Strategy.
- **Handled by System** – The Adaptiva 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.

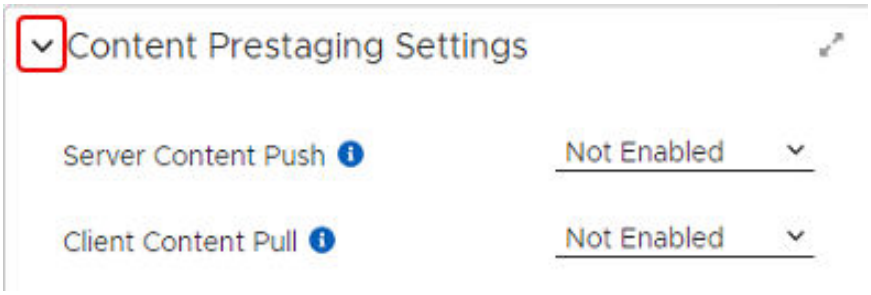
Set Content Prestaging Settings

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

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

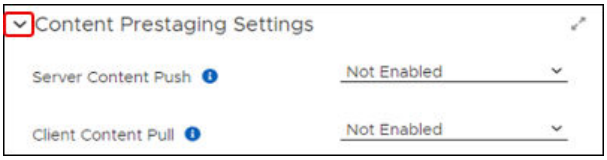


2. Expand the **Content Prestaging Settings** to view the available settings.

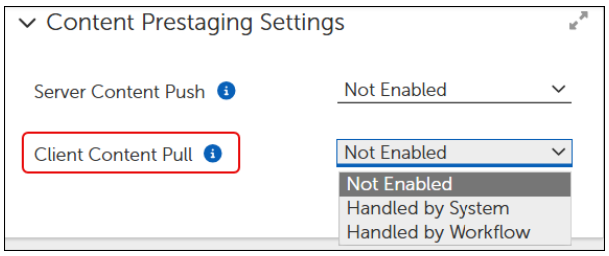


Enable Client Content Pull

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:



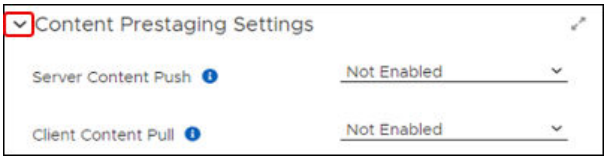
1. Select the arrow to the right of **Client Content Pull** to expand the menu of available options.



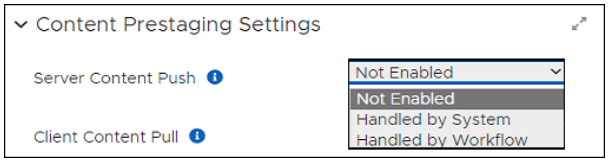
2. Select the option you need for the object template you are using. For definitions of push options, see Defining Content Prestaging Settings.
3. Select **Save** on the upper-left to save your changes:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** again if you make any 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 that has already completed the current patching cycle, you must use the **Business Unit Addition Settings** to add the parent Business Unit that contains the details, such as Patches, Patch Approval Settings, and any Business Unit added to the Strategy will inherit these details.

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 Patch Dashboard.
2. Scroll down to **Business Unit Addition Settings**, and then select the **right arrow** to expand the workspace.

Select a Business Unit

Specify the parent Business Unit for this strategy so that when new Business Units are added to the strategy after it has already run, the new 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 the **Business Unit** that has the parent settings for any future Business Units added to the Strategy.
3. Select **OK** to return to the 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.

> **IMPORTANT**
>
> If you came to this procedure while you were configuring Deployment Settings in a Patching Strategy, return to Deployment Settings to continue the Strategy configuration.

Select a Patching Process

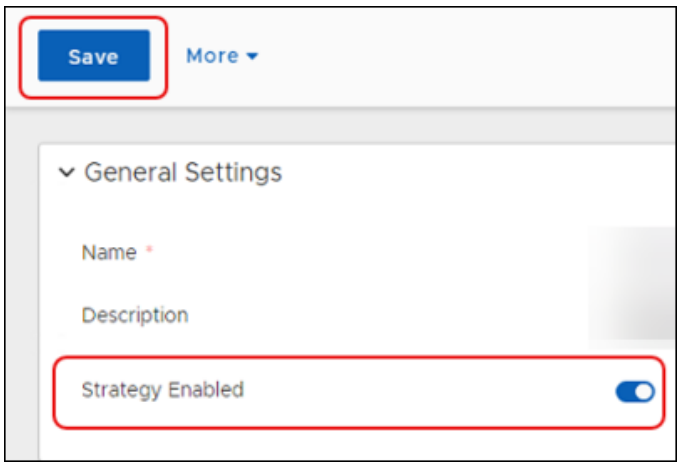
Identify the Patching Process that controls the approval and deployment logic for the existing Business Units in this strategy. This is the same Patching Process identified in the Deployment Bot Runtime, which is the only Patching Process you can choose here. This ensures that any Business Units added after the 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 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 select **OK**.
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, select the **Strategy Enabled** toggle to enable the strategy and make it available for use.

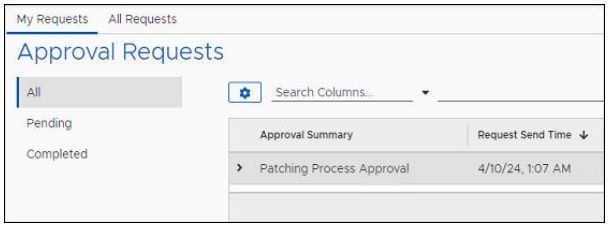


2. Select **Save** on the upper-left corner of the workflow to save the strategy:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** again if you make any changes.
3. Move the saved template to your folder.

View a Staged Patching Strategy

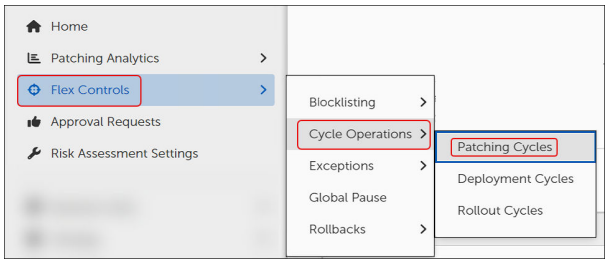
After you Enable the Patching Strategy, you can view the pending approval request.

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

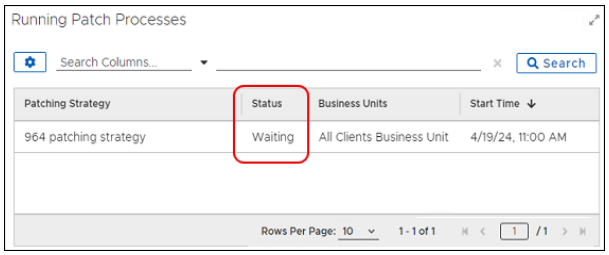


   - The view defaults to **All** requests, which includes pending and completed.
   - The Patching Strategy you just enabled appears in the **Approval Summary** table with a **Request Status** of **In Progress and Awaiting Response**.

2. Select **Flex Controls > Cycle Operations > Patching Cycles** from the left navigation menu of the 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 select the **Patching Strategy** in the table.
5. Select **Approve**, and then select **Back to Approval Requests**. You can wait until the patch time passes, or you can start the deployment manually.

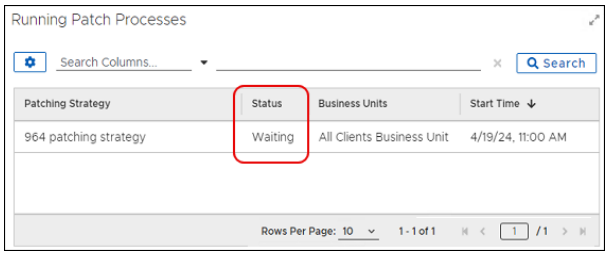
IMPORTANT

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

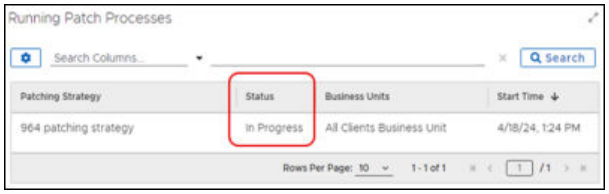
Start the Patching Strategy Manually

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 select the name of the Patching Strategy to open the **Cycle Information**.



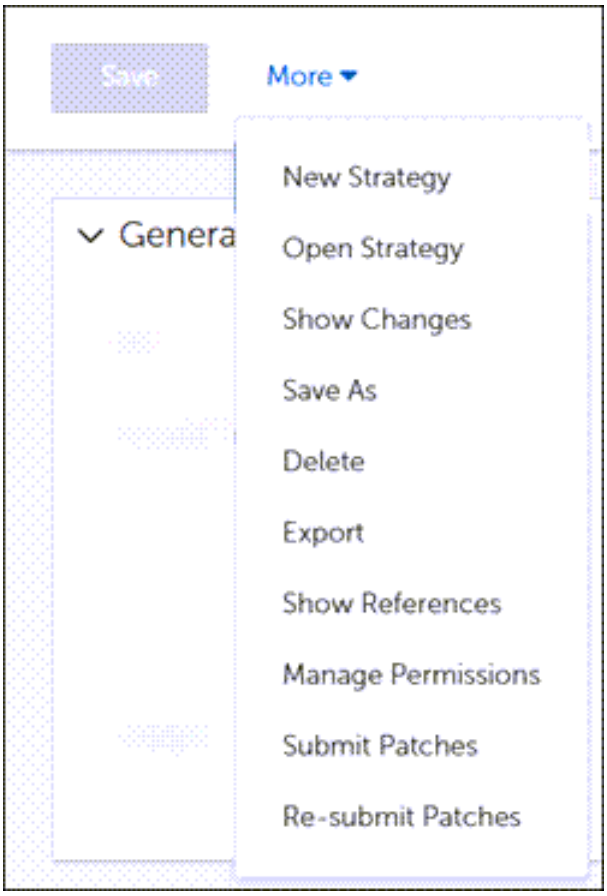
2. Select Play under **Cycle Information**, and then select **Close**. This returns you to the **Patching Cycles** workspace where you can view **Running Patch Processes**.



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

Managing Enabled Patching Strategies

OneSite Patch provides simplified processes to manage and modify Patching Strategies that you have already enabled. From an open, enabled Patching Strategies, the **More** menu contains the following options:



Delete an Enabled Patching Strategy

1. Select **Strategy > Patching Strategies** and navigate to the enabled strategy you want to delete.
2. Select the Strategy Name to open it.
3. Select **More**, and then select **Delete**. The system prompts you to verify the deletion.
4. Click **OK** to permanently delete the Patching Strategy.

Submit Patches to an Enabled Patching Strategy

1. Select **Strategy > Patching Strategies**, and then navigate to the enabled strategy you want to submit.
2. Select the strategy **Name** to open it.
3. Select **More**, and then select **Submit Patches**. This opens the dialog for the selected strategy.

4. Choose one of the following options:
   - To create approvals, select the **Create Approvals** toggle to enable Patch Approvals, and then select **+ Create Patch Approval**. See Approvals for Adding Patches.
   - To choose patches, select **+ Browse**, and then see Select Installable Software.

Approvals for Adding Patches

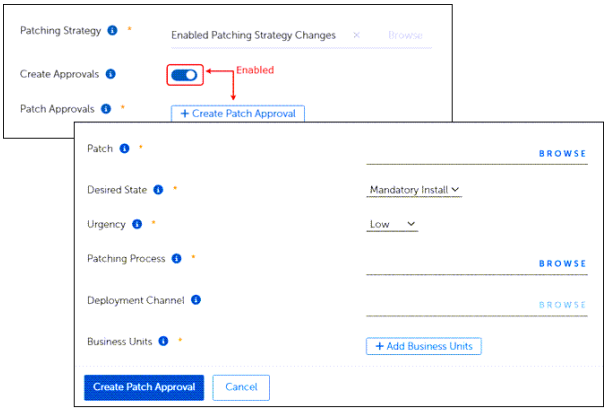
When you submit patches to an enabled strategy, you may also create approvals specific to the individual patch. Otherwise, the patching process and bots create the approvals automatically based on the process or bot settings.

The Create Approvals functionality requires at least one approval scenario. You must create separate approvals for each patch you choose to add to an enabled patch.

Approvals in this instance consist of the following, required settings:

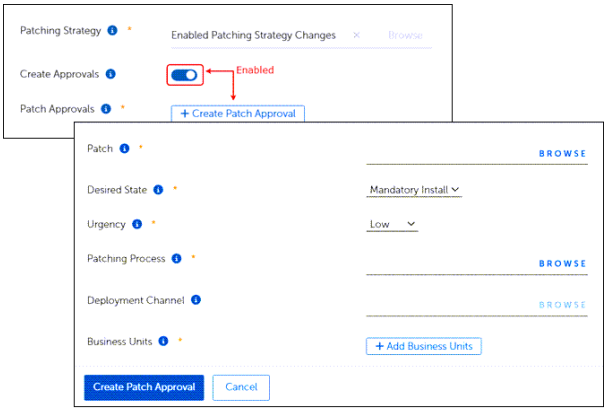
- Identify the patches or software that require approval.
- Set the state and urgency for the approval.
- Add a Patching Process
- Add Business Units

You may also add a Deployment Channel (optional).

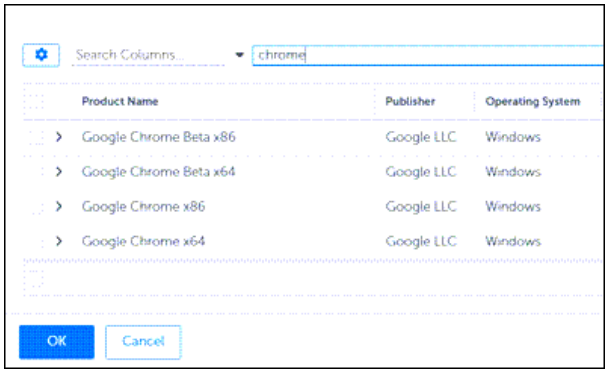


Create an Approval for an Added Patch

Complete the required fields in the **Create Patch Approval** dialog. The dialog already includes the name of the Patching Strategy you chose to modify.



1. Select **+ Browse** for **Patch** to select the patch to add. This opens a software selection table.
   a. Enter a product name in the search line, and then select **Search**. This example uses Google Chrome.
   b. Select the product from the list, and then select **OK**.



2. Select the **Desired State** for the patch approval, and then select the **Urgency** (Low, Normal, High, Critical):
   - **Mandatory Install:** Allows client devices to treat the product as mandatory for installation purposes.
   - **Do Not Install:** Allows client devices to block the installation of a particular product.
   - **Rollback:** Forces a rollback to a specific product version on a client device, when OneSite Patch detects a later product version than allowed.
   - **Uninstall:** Removes the product from client devices in the specified Business Unit.

3. Add a **Patching Process** (required) and a **Deployment Channel** (optional):

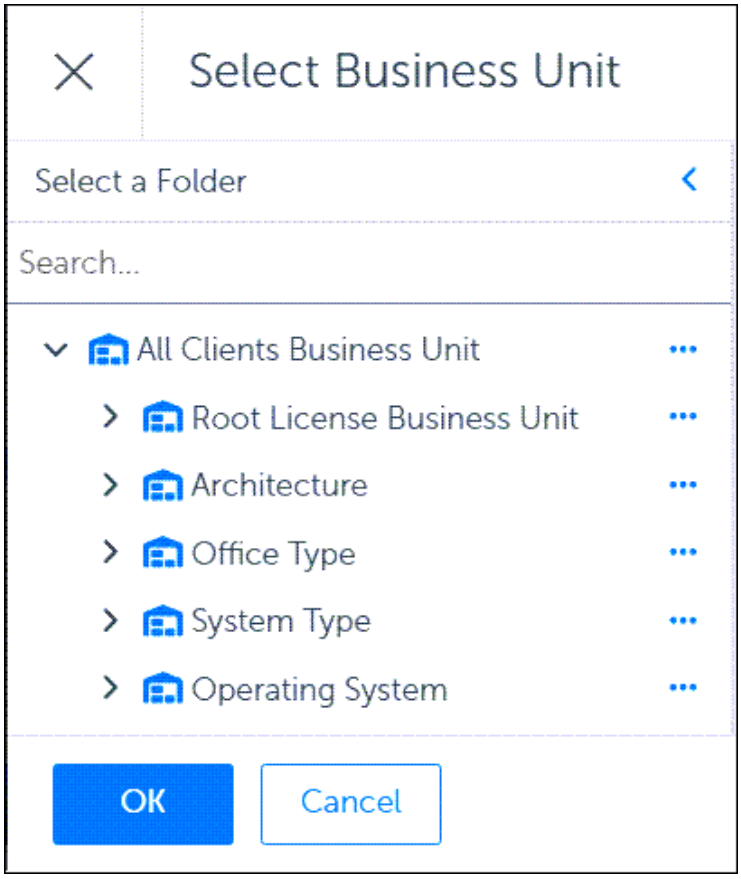
> **TIP**
>
> Add a Deployment Channel only when you have included it in the Deployment Bot Runtimes section of the Patching Strategy Deployment Settings.

   a. (Required) Select **Browse** next to **Patching Process**, and then select a process from the table.
   b. Select **OK** to return to the patch approval dialog.

c. (Optional) Select **Browse** next to **Add Deployment Channel**, and then select a channel from the table (see **Tip** above).

d. Select **OK** to continue creating the approval.

4. Select **+ Browse** next to **Business Units** to open the dialog.
   a. Select the Business Units.



   b. Select **OK**.

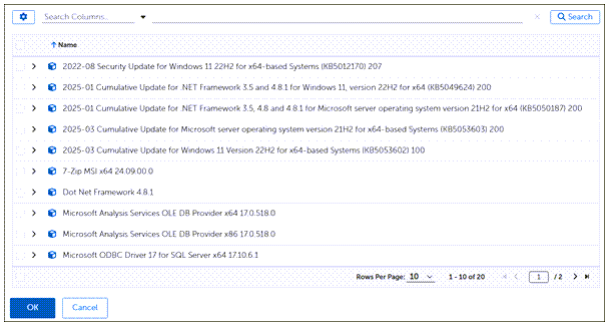
5. Complete the approval for the selected patch:
   a. Select **Create Patch Approval**. The patch submission now includes a table that lists the patch you selected.

   b. (Optional) Return to **Step 1** to create a patch approval for another patch.

   c. Select **OK** to return to the dialog.

Resubmit an Enabled Strategy

1. Select **Strategy > Patching Strategies**, and then navigate to the enabled strategy you want to resubmit.
2. Select the strategy name to open it.
3. Select **More**, and then select **Re-submit Patches**. This opens a table of applicable patches for the selected strategy.



4. Select the patches you want to resubmit with this strategy, and then click **OK**.
5. To verify the status of your Approval Request, see Approval Requests.

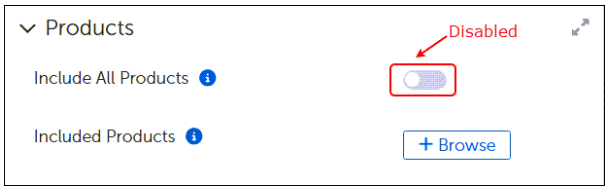
Managing Software Product Selections

In , configuration options provide several opportunities to select or exclude software products for a patching strategy. Options include include making product sections when creating a strategy, exempting products from business units, and more.

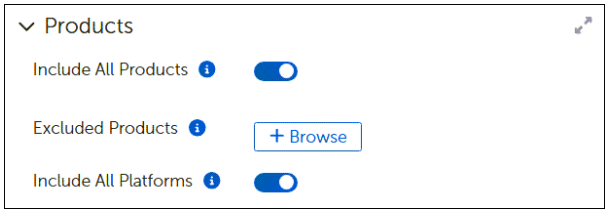
For more information about the products available with , see Software Products.

Include All Software Products

1. Scroll to the **Products** workspace in an open Patching Strategy template. The image below shows the default settings.



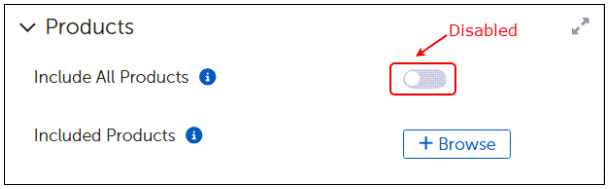
2. Select the **Include All Product**s toggle to enable it.
   The following image shows the default settings and options when you select **Include All Products.**



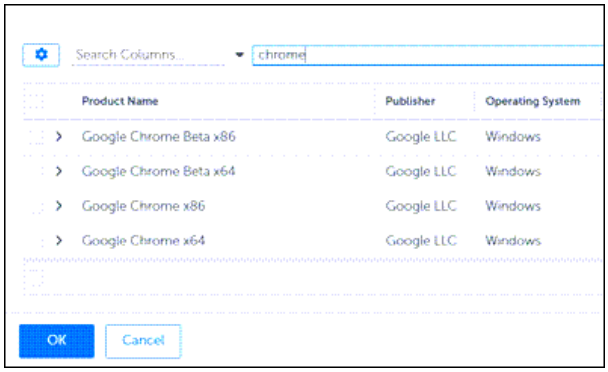
3. Select Save on the upper left corner of the strategy:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** again if you make any changes.
4. Choose one of the following options to continue managing products:
   - To exclude specific products for this strategy, see Exclude Products from a Patching Strategy
   - To include specific platforms, see Include or Exclude Platforms in a Patching Strategy

Include Specific Software Products

1. Scroll to the **Products** workspace in an open Patching Strategy template. The image below shows the default settings.



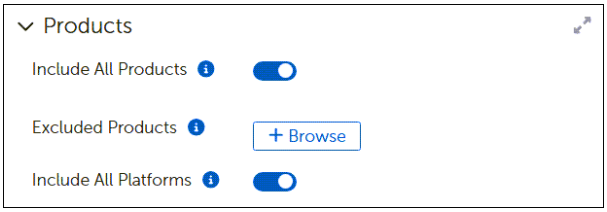
2. Select **+ Browse** to open the **Select Software Product** table:
   a. Enter a product name in the search line, and then select **Search**. This example uses Google Chrome.
   b. Select the product from the list, and then select **OK**.



3. Select **Save** on the upper right corner of the Patching Strategy:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** again if you make any changes.

Exclude Products from a Patching Strategy

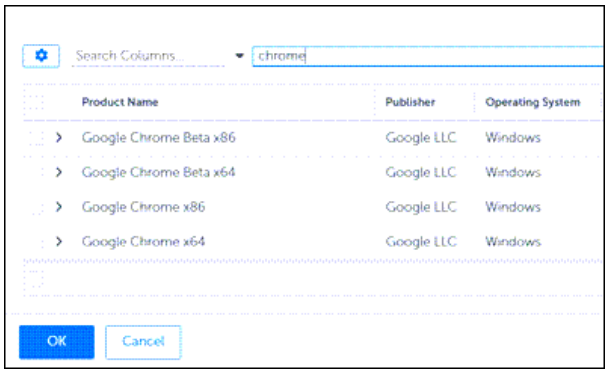
After enabling **Include All Products** from the Products workspace in an open Patching Strategy, you have the option to exclude individual products for the same Patching Strategy.



IMPORTANT

When you add Business Units to a Strategy, the Patching Exceptions set for the Business Unit take precedence over the Product settings in the Patching Strategy.

1. Select + **Browse** to open the **Select Software Product** table:
   a. Enter a product name in the search line, and then select **Search**. This example uses Google Chrome.
   b. Select the product from the list, and then select **OK**.

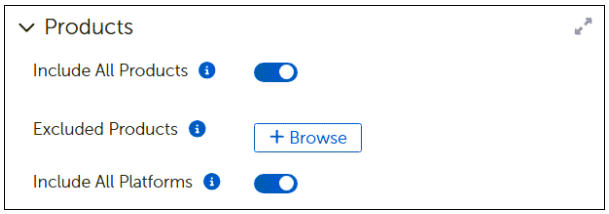


2. Select **Save** on the upper left of the strategy to keep your changes:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** again if you make any changes.

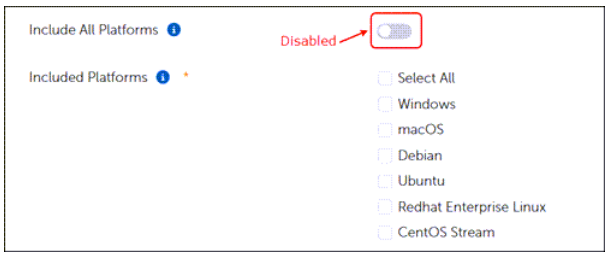
Include or Exclude Platforms in a Patching Strategy

When you enable **Include All Products** from the Products workspace in an open Patching Strategy, you also include all platforms by default.

1. Select + **Browse** to open the **Select Software Product** table:



2. Select the **Include All Platforms** toggle to disable it and view the available Platforms.



3. Decide which platforms to include:
   - To include all Platforms, either **Select All** or select the **Include All Platforms** toggle to enable it.
   - To include specific Platforms, select those you want to include.

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

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

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

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.

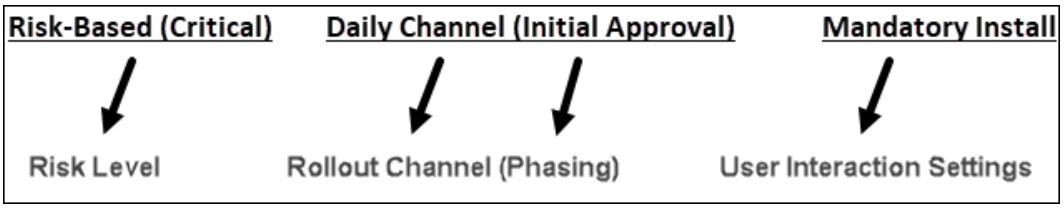
Deployment Bots

Patch Deployment Bot Template Naming Conventions

OneSite Patch 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

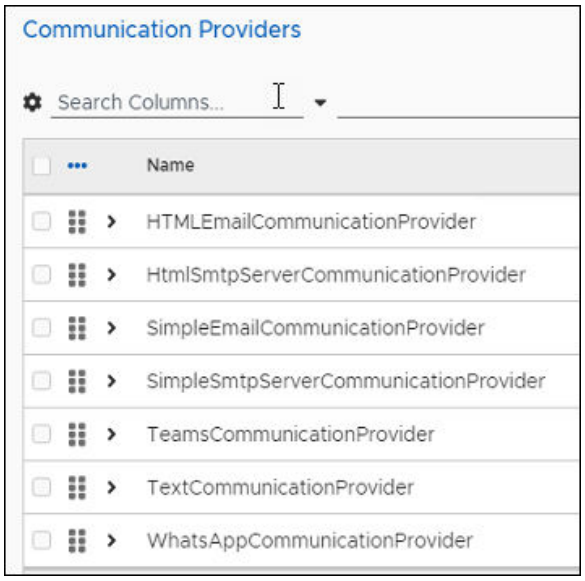
These templates filter specific categories of patches, including bug fixes, expired by vendor, known exploit, and so on. These bots filter based on category and then approve installation for all patches included in that category.

Descriptions of Bot Settings

The Bot templates provided by OneSite Patch 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, enter a support ticket and request help from Customer SupportAdaptiva 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:
  - **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 a notification.
- **Business Units:** Deployment Bots Only. Business Units are a fundamental organizational unit in OneSite Patch , 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**.

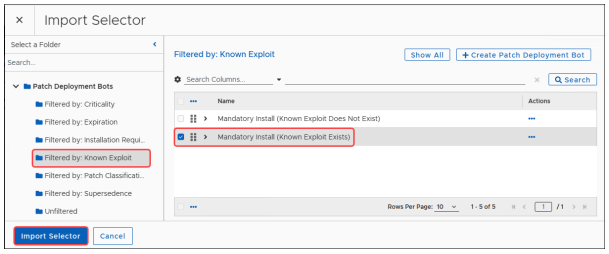


Open and Save a Patch Deployment Bot Template

OneSite Patch 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, Adaptiva recommends entering a support ticket and requesting assistance from Customer Support from Adaptiva Customer Support.

1. Follow the instructions in Create a New Folder for Objects.
2. Hover over or select **Bots** in the left navigation menu of the Adaptiva OneSite Admin Portal, and then select **Patch Deployment Bots**. The top folder lists the templates provided byAdaptiva
3. Select **Show All** to see the available templates or select **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**, select **Mandatory Install (Known Exploit Exists)**.



5. Save the template with a new title:
   a. Select **More** in the upper-left of the dialog, and then select **Save As**.
   b. Enter a new name for the template, and then select **Save as** on the lower-left of the dialog. This returns you to a copy of 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, and then select **Save** on the upper-left of the dialog.

Patch Filter Conditions

The OneSite PatchDeployment 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 assistance from Customer SupportAdaptiva Customer Support.

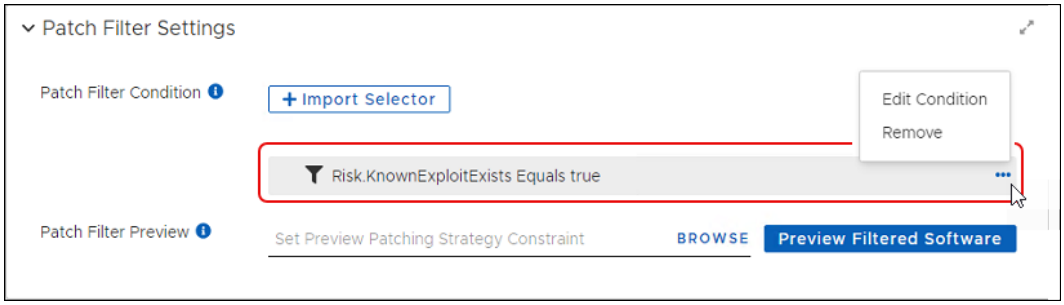
Used by both Deployment Bots and Notification Bots. New patches must meet the filter criteria before the Bot submits them to the Patching Cycle. After approving a patch that meets the Patch Filter Settings, the Bot forwards patch information to the Patching Process and the Deployment Wave associated 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, select the **ellipsis (...)**, and then select **Edit Condition**.
- If you want to remove a **Patch Filter Condition**, select the **ellipsis (...)**, and then select **Remove**.

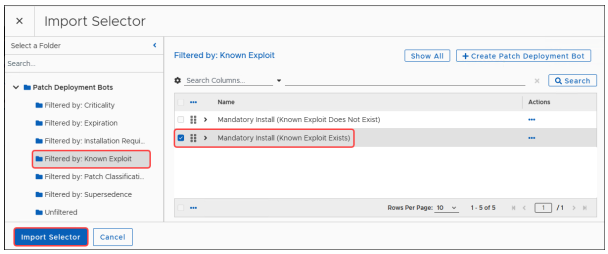


Add Patch Filter Conditions

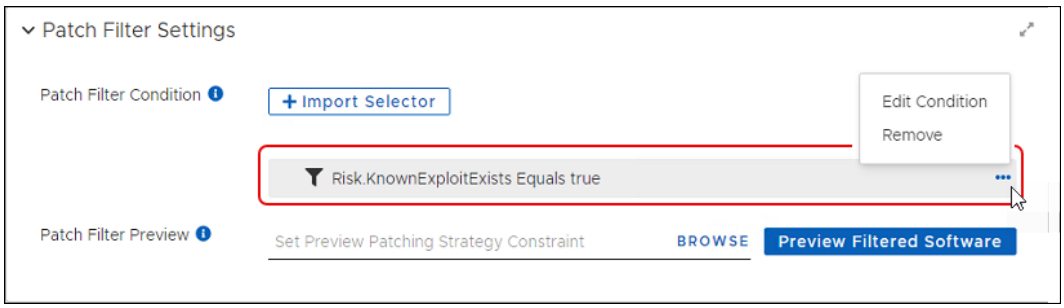
Allows you to select one or more, existing filter conditions to use for this Bot. If you want to add multiple conditions, see Set and Change Patch Filter Conditions. This example uses an existing Adaptiva patch filter that tells the Bot to include patches based on the imported filter settings.

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.

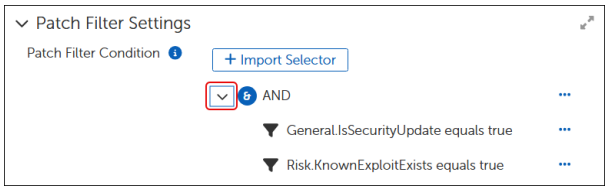
   For example, in **Filtered by: Known Exploit**, select **Mandatory Install (Known Exploit Exists)**.



3. Select **Import Selector** at the lower 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 choose more than one filter, the condition displays the **AND** operator and lists your selections:



Set and Change Patch Filter Conditions

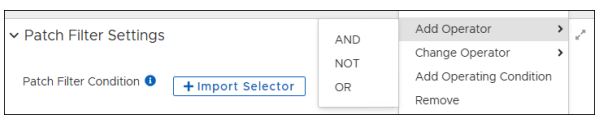
Use Operating Conditions and Operators to manually set multiple Patch Filter Conditions to use for this Bot. You must add the operator before you can add the condition. To add multiple conditions, repeat this section as needed.

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.
   - To **remove** an existing condition, select the **ellipsis (...)** to the right of the existing filter, and then select **Remove**.
   - To **add** the condition again as part of a string, record 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**.

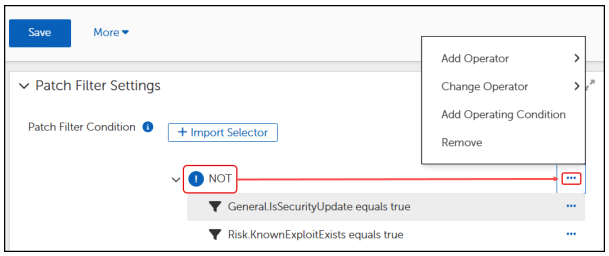


This returns you to the **Patch Filter Settings**, which displays the operator you selected.

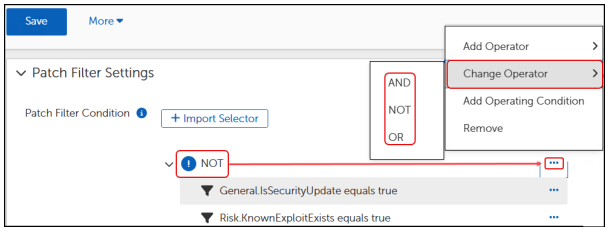
4. Continue to Add an Operating Condition.

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 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 WSUS.

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

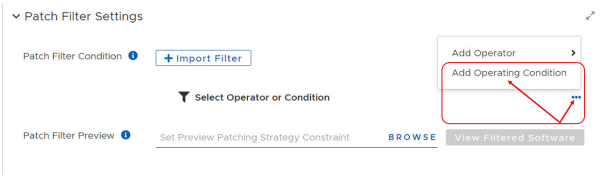
2. Expand the list next to **Data Column**, and then select the filter you want to use. For example, select **WSUS Classification**.
   - See Patch Filter Settings for a description of each available setting.
   - If you removed a Patch Filter Condition previously, you may add it back here.
3. Set the **Operating Condition** to **Equals**, and then choose one of the following for the **Value**:
   - **Updates:** Excludes Windows updates.
   - **Upgrades:** Excludes Windows upgrades.
   - **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.

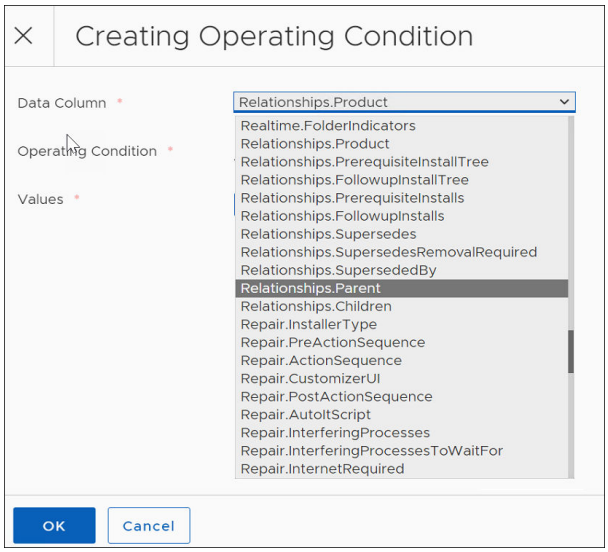
Filter Out Specific Patches by Product ID

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

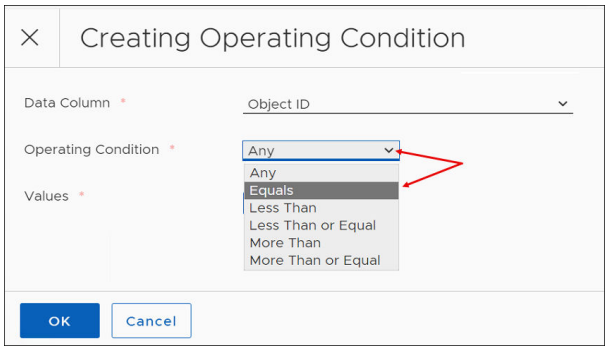
1. Contact Customer SupportAdaptiva Customer Support to obtain the Product ID for the vendor patches you want to filter.
2. Select **ellipsis (...)** to the right of **Select Operator or Condition**, and then select **Add Operating Condition**.



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



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



5. Enter the Product ID, and then select **OK**. This returns you to **Patch Filter Settings**, 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, using the steps below:

1. Select **Preview Filtered Software** on the lower-right 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

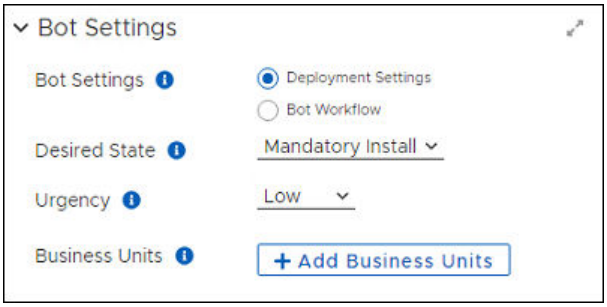
Using the Patch Filter Settings in a Deployment Bot template, you can preview the software filtered out by the Patch Filter Conditions you set. You can enhance these filter conditions by specifying a Patching Strategy to further constrain the preview results.

1. Select **Browse** next to **Patch Filter Preview** in the **Patch Filter Settings** of an open Deployment Bot template.
2. Select the Patching Strategy you want to preview, and then select **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.



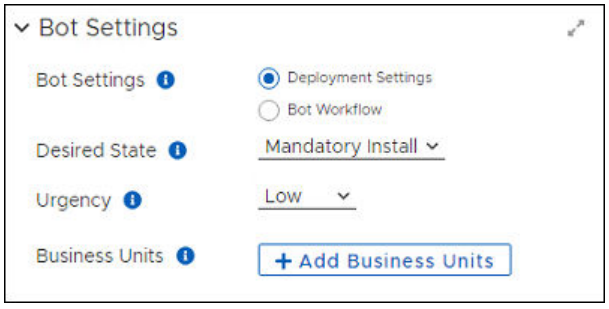
With **Deployment Settings** selected, complete the following steps:

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.

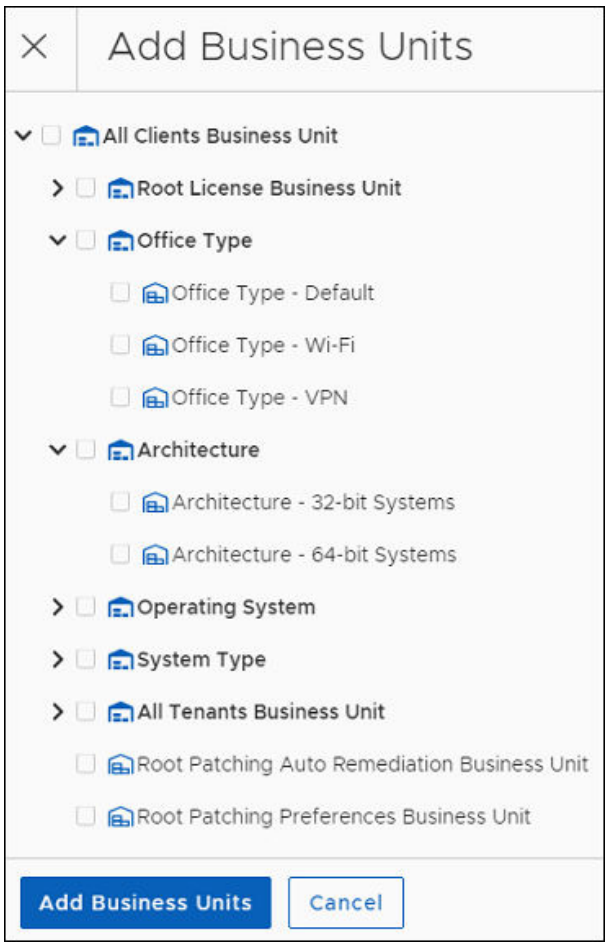
Business Units for Bot Deployment Settings

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

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



   - With no Business Units added to the Bot, the patching cycle patches the devices in all Business Units identified in the Patching Strategy.
   - 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.



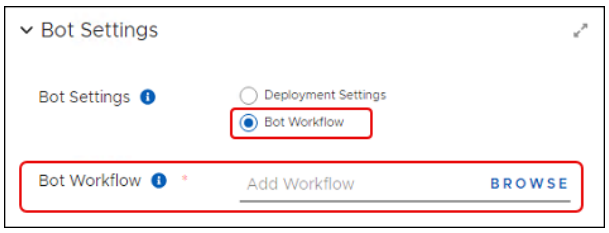
3. Select one or more **Business Units** to include in this Deployment Bot.
4. Select **Add Business Units** on the bottom left to return to the Deployment Bot template.
5. Select **Save** at the upper-left to save your progress:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** 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 Adaptiva 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 then 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 Adaptiva Customer Support to create a Deployment Bot Workflow for use with these settings.

3. Select the workflow **Name**, and then select **Add Workflow** on the lower-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.

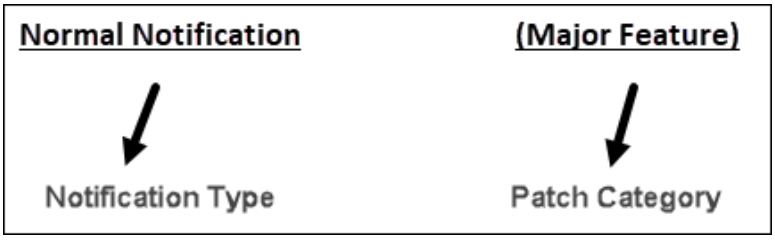
Notification Bots are optional components of Patching Strategy templates and Deployment Channel templates and exist only within these templates.

Patch Notification Bot Template Naming Conventions

Adaptiva Patch 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

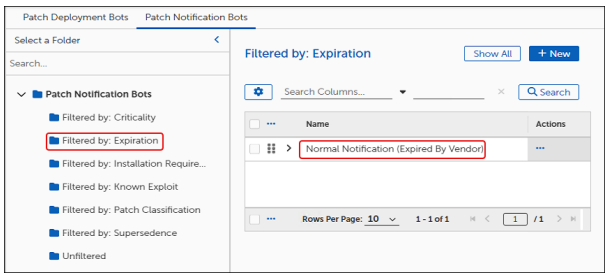
These templates filter several aspects of patches based on risk. They include different rollout schedules and approval levels, and all require mandatory installation.



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 select **Bots** in the left navigation menu of the Patch Dashboard, and then select **Patch Notification Bots**. The top folder lists the templates provided by OneSite Patch.
3. Select the **Show All** to see the available templates, or select **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**, select **Normal Notification (Expired by Vendor)**.



5. Save the template with a new title:
   a. Select **More** in the upper-left of the dialog, and then select **Save As**.
   b. Enter a new name for the template, and then select **Save as** on the lower-left of the dialog. This returns you to a copy of 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, and then select **Save** on the upper-left of the dialog.
6. Select **Save**. When you have finished modifying your new template, you can drag and drop it into the folder you created (see Patch 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.

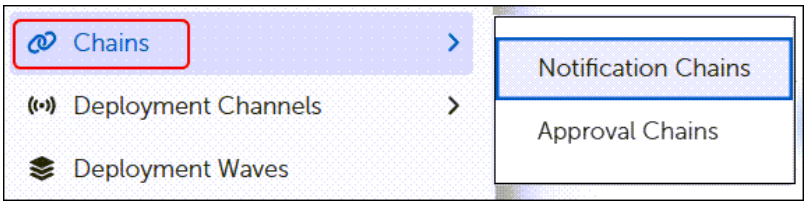
Configure Notification Bot Settings

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 select **+Add Communication Providers**.
   - Select one or more providers to use for notifications by this Bot.
   - 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** to resolve any errors.
4. Select **Save** again if you make any changes.

Chains

OneSite Patch 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 enable administrators to specify users who will receive patch approval requests for specific Patching Strategies or Business Units.

OneSite Patch 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

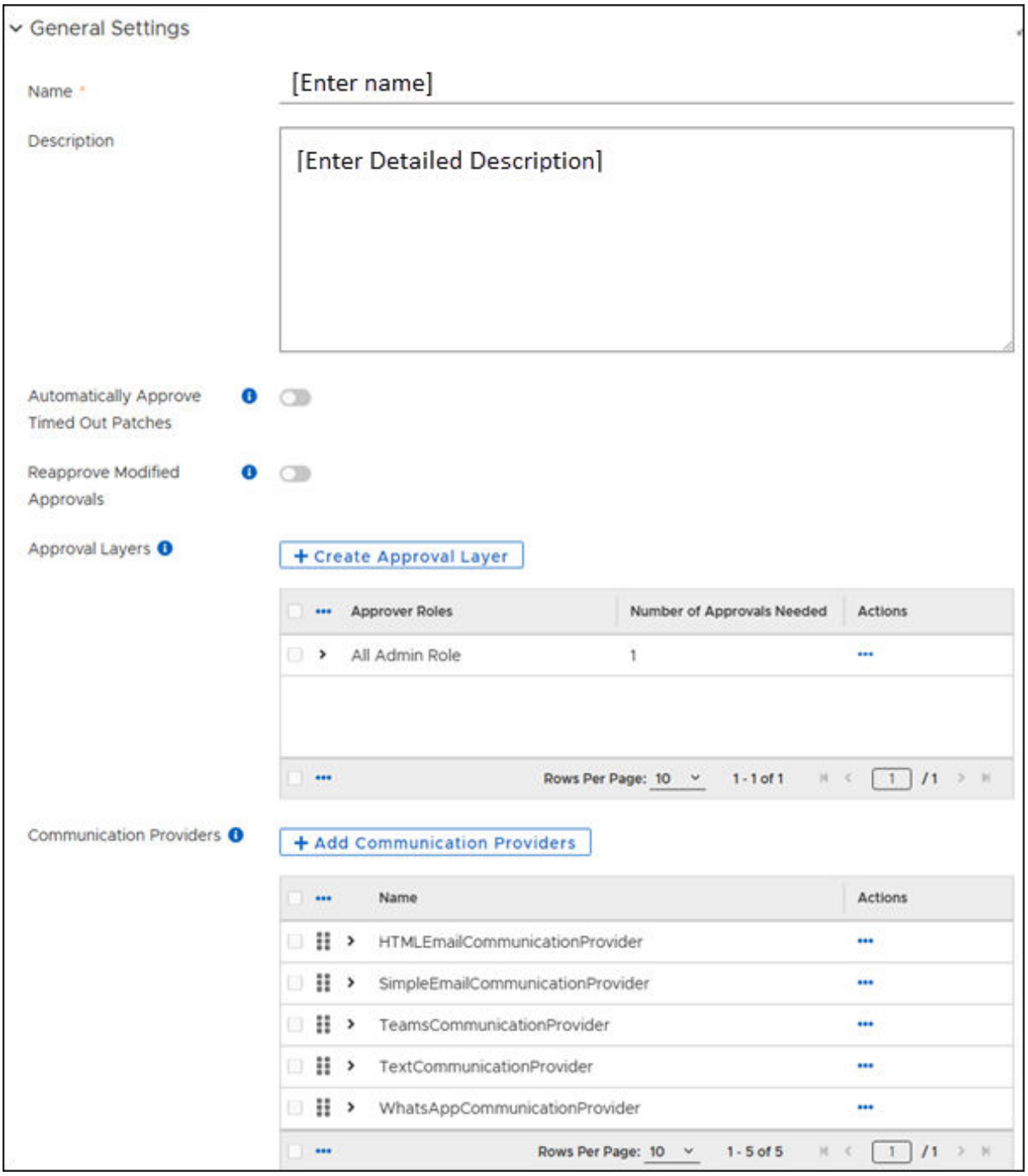
1. Mouse over or select **Chains** in the left navigation menu of the Dashboard, and then select **Approval Chains**.

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 of the dialog, and then select **Save As**.
   b. Enter a new name for the template, and then select **Save as** on the lower-left of the dialog. This returns you to a copy of 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, and then select **Save** on the upper-left of the dialog.

Managing Approval Chain Settings

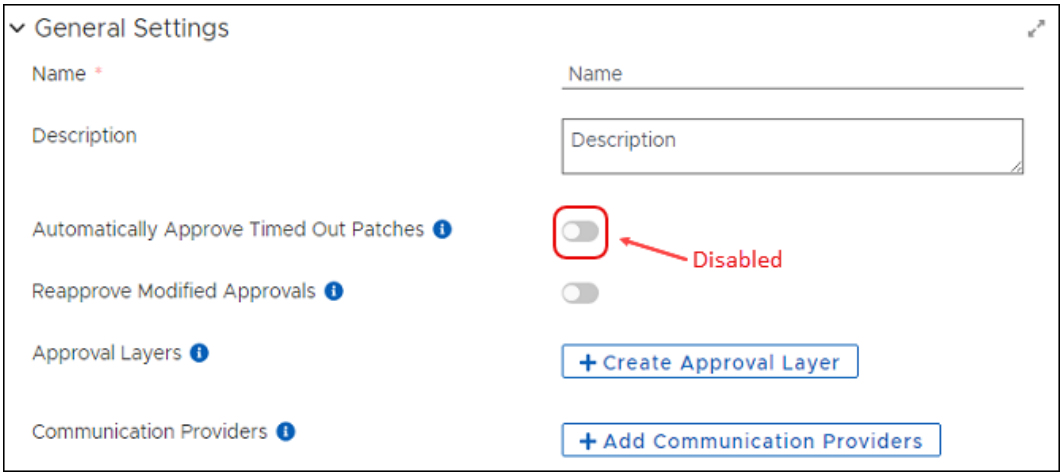
Approval Chain management choices include approval of timed out patches, reapproval of modified approvals, setting approval layers, and choosing communication providers.

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

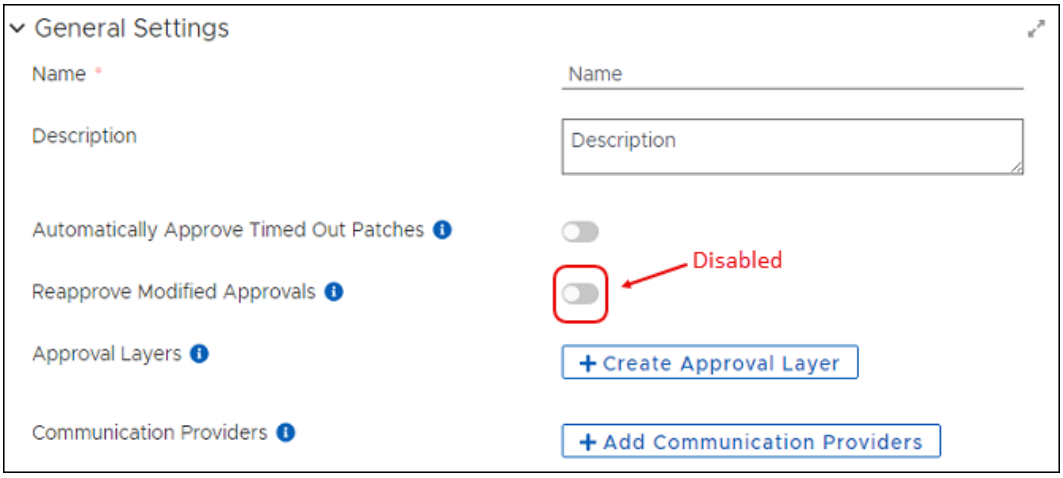
When enabled, this setting automatically approves patches when reviewers do not respond within the timeout duration specified in the Approval Layer.



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.

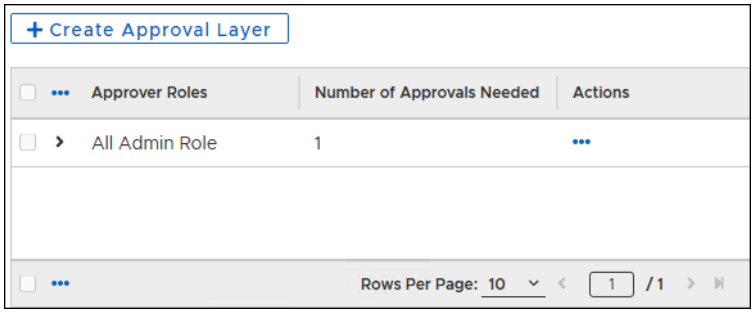


Select the **Reapprove Modified Approvals** toggle to enable or disable (default) this feature.

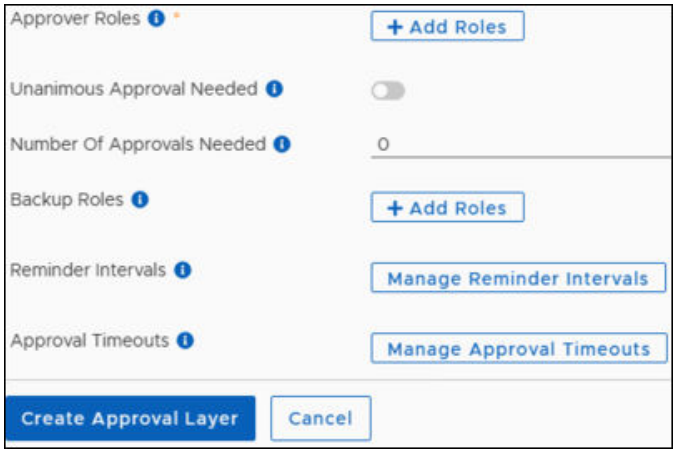
Create an Approval Layer

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.
   - For a new approval Layer, select **+Create Approval Layer**.
   - To change an existing Approval Layer, select the **ellipsis (...)** in the **Actions** column for the role you want to change, and then select **Edit Approval Layer**.



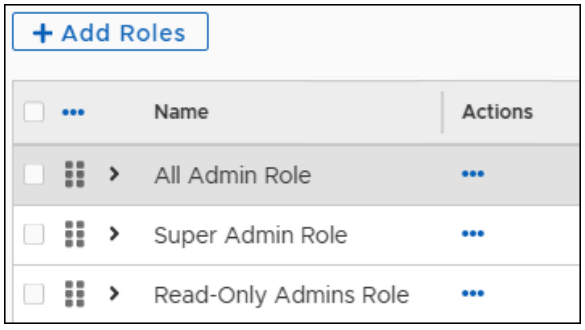
2. This opens the **Create Approval Layer** dialog.



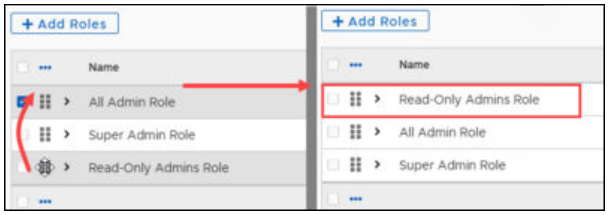
Add and Order Approval Roles

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 select **Add Roles** at the lower-left of the page. This returns you to the **Approval Layer** dialog.



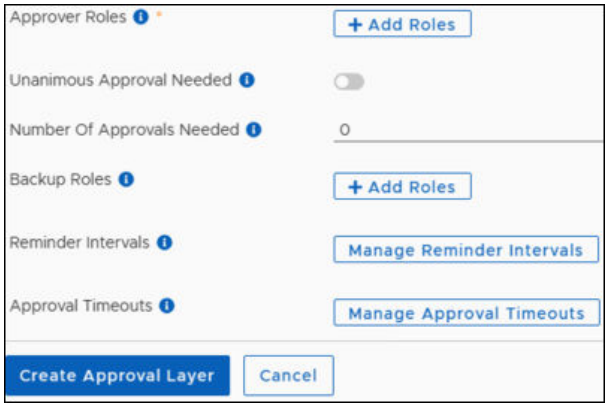
3. Reorder the roles to reflect the processing order you want the strategy to use:
   a. Select and hold the **stacked dots** for the role you want to move.
   b. Drag the **role** up or down to move it in the list.



Add Approval Roles to an Approval Layer

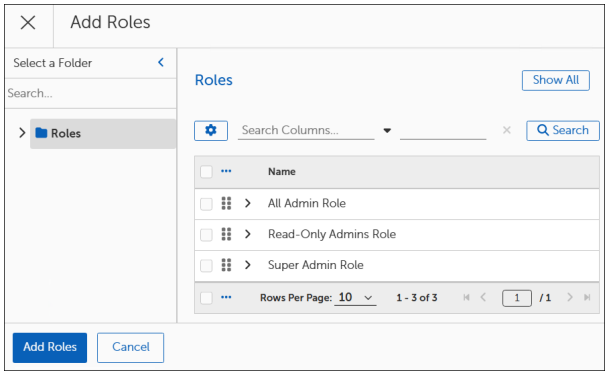
OneSite Patch includes templates for commonly required roles. You can add these existing roles to the Chains you create by creating approval layers.

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 lower-left of the page.

Set Unanimous Approval or Number of Approvals Needed

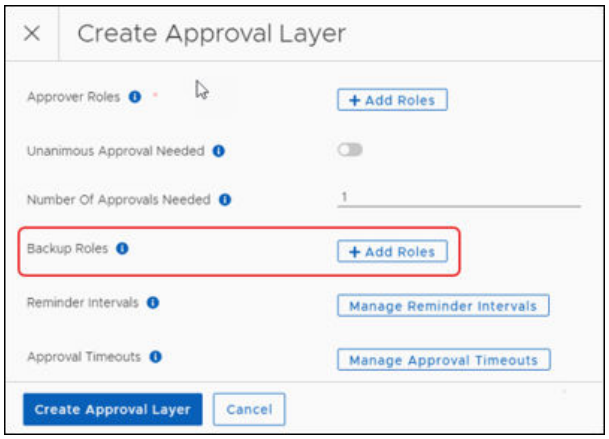
Choose the number of approvers who must approve patches to satisfy this Approval Layer:

- **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.

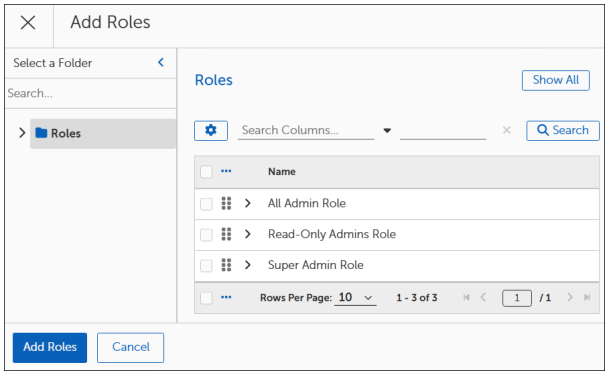
Add Backup Roles to an Approval Layer

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.

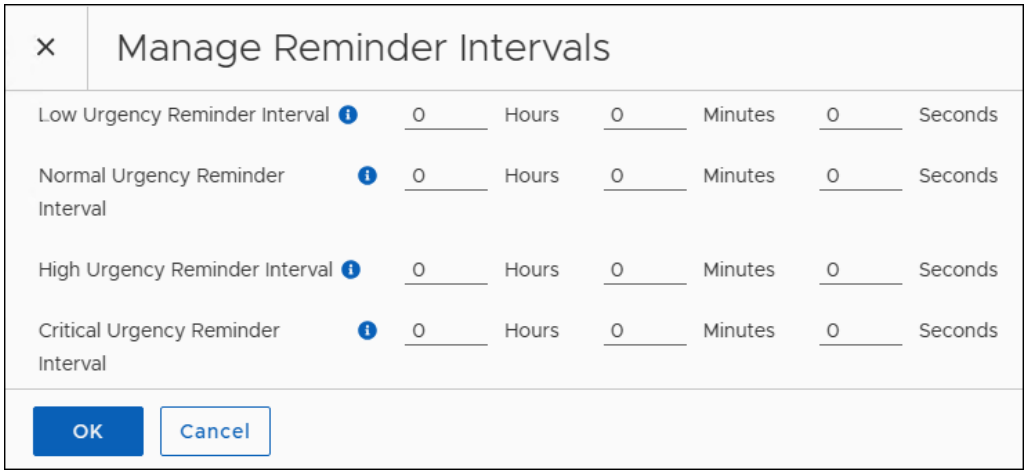


4. Select **Add Roles** at the lower-left of the page.

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 0 sends no reminders.

1. Select **Manage Reminder Intervals** under **Approver Roles**.
   The **Manage Reminder Intervals** dialog appears:

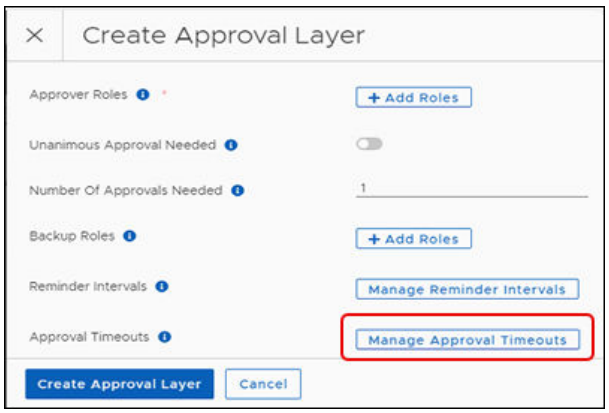


2. Enter a number for the **Urgency Reminder Interval** (**Low**, **Normal**, **High**, **Critical**).
   - At 0, the strategy sends no reminder.
   - When the request times out, the approval request fails.
3. Select **OK** at the lower-left of the page.

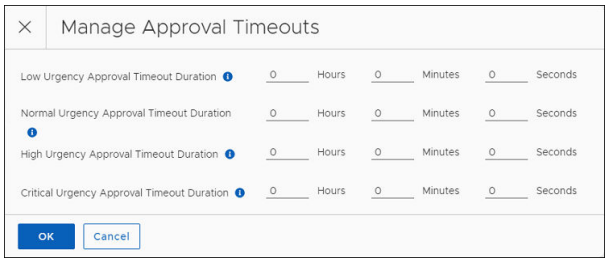
Set Approval Timeouts

These settings define the timeout variables for the approval request. You can specify different reminder intervals for each urgency level. A setting of 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:
   - At 0, the strategy sends no reminder.
   - If the request times out, the approval request fails.



3. Select OK on the lower-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

Adaptiva 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 lower-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

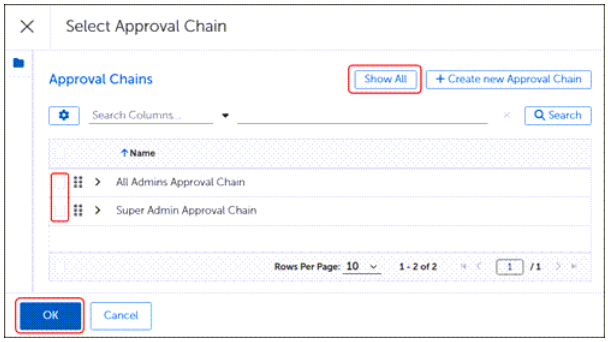
Patching Strategy and Business Unit object templates include an **Approval Chains** dialog so you can define administrative approval details as part of the object. To see links to other settings for Patching Strategies, see Optional Objects in Patching Strategy Templates.

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.
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.

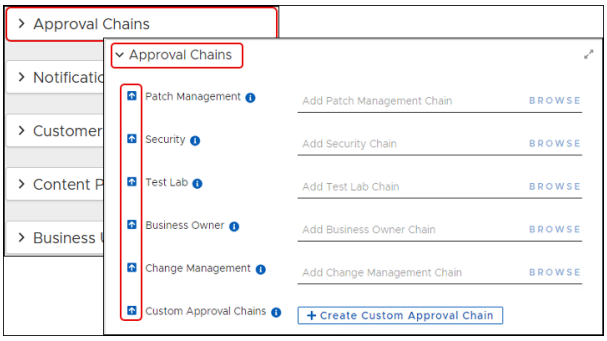


4. Select **OK** to return to the object template.
5. Repeat Steps 2 through 4 for each of the groups listed in the **Approval Chains** workspace:
   - Skip any groups that do not apply to your situation.
   - When each group from which you need an approval contains an approval chain, continue with the 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.

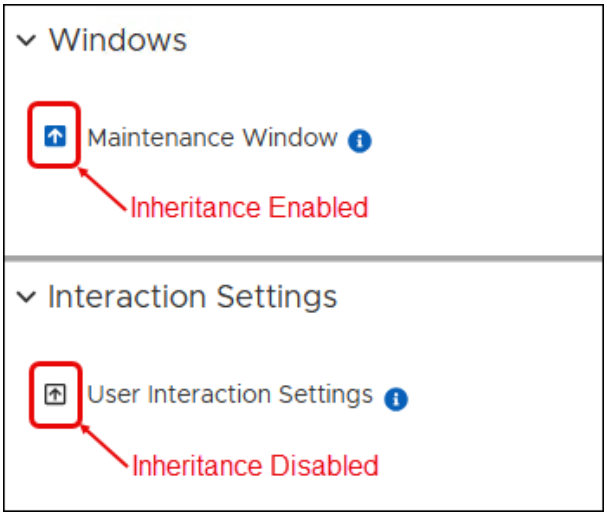
Add Approval Chains to a Business Unit

Adding Approval Chains to a Business Unit is an advanced feature. The **Approval Chains** fields allow advanced users to specify details for use in customized Patching Strategies, Deployment Chains, or Business Units when necessary to achieve different results.

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



   - Disable inheritance to enable Browse, and then 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.

4. Select OK on the bottom left to return to the **Approval Chains** workspace.
5. Repeat Steps 2 through 4 for each of the groups listed in the **Approval Chains** workspace:

- Skip any groups that do not apply to your situation.
- When each group from which you need an approval contains an approval chain, continue with the next step.

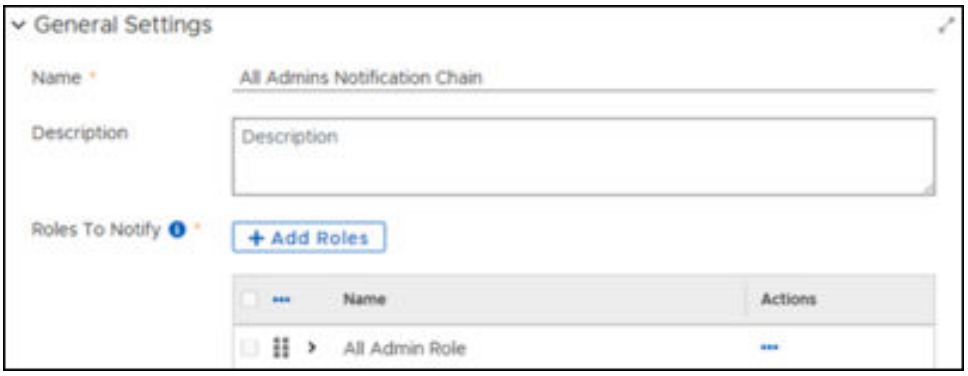
6. Select **Save** at the upper-left to save your progress:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** again if you make any changes.

Notification Chains

Using Notification Chains

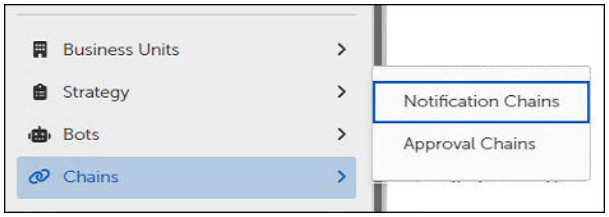
Notification Chains send notifications to the administrator roles you specify, informing them about pending deployments. In addition to creating Notifications Chains here, you can also view and create them in object templates for Patching Strategies and Business Units (see Managing Notification Settings,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

Notification Chains enable administrators to specify who will receive notifications about patches and deployments, as well as the method of delivery, including email, Teams, SMS text, or WhatsApp.



Open and Save a Notification Chain Template

1. Mouse over **Chains** or select the right arrow next to **Chains** in the left navigation menu of the Patch 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 of the dialog, and then select **Save As**.

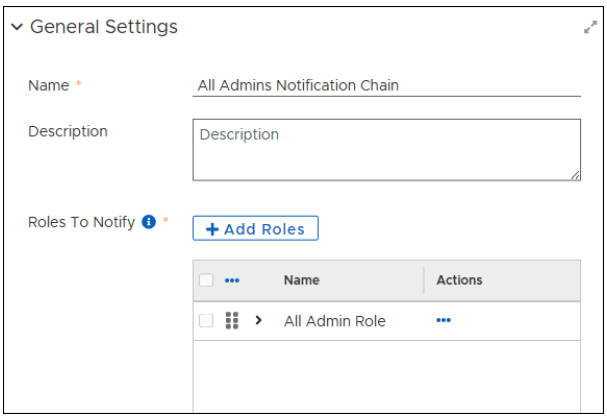
b. Enter a new name for the template, and then select **Save as** on the lower-left of the dialog. This returns you to a copy of the template with the new name.

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, and then select **Save** on the upper-left of the dialog.

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.

1. Scroll down to **Roles to Notify**. If a table appears, check to see whether the existing roles apply:
   - To remove a Role from the table, select the **ellipsis (...)** in the **Actions** column, and then select **Remove**.
   - To add Roles to the table, select **+Add Roles**, and then continue with the next step.
2. Select one or more **Roles** from the Roles table, and then select **Add Roles** at the upper-left of the dialog.
3. 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.

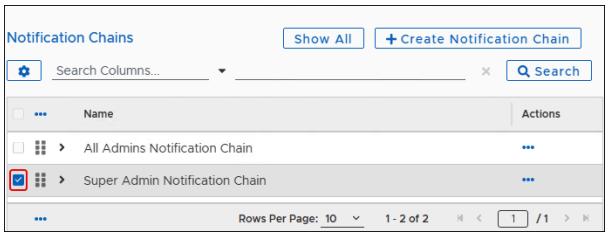
IMPORTANT

This configuration requires selecting a specific type of Notification Cycle template. Contact Adaptiva 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.



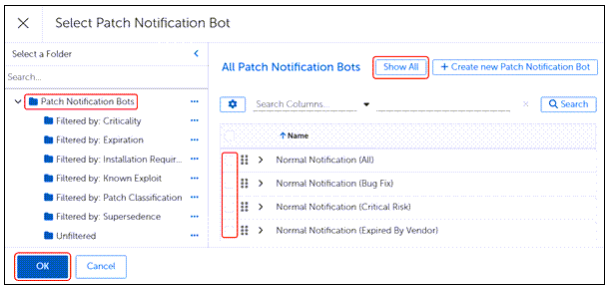
3. Select **Notification Chains**, and then select **Show All** to see the available templates.
4. Select a **Notification Chain** from the table. To edit or create Notification Chains, see Using Notification Chains.
5. Continue editing the **Notification** settings, or select **OK** (lower-left corner) 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 **+Browse** next to **Patch Notification Bots** in the **Notifications** workspace of the object template.

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



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

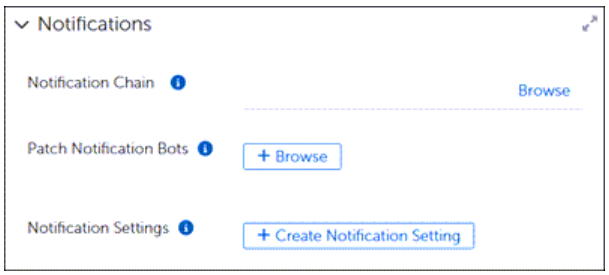
3. Choose one or more **Notification Bots** to set requirements for this template. To create more Notification Bots, see Creating Notification Bots.
4. Select **OK** on the lower-left of the dialog to return to the starting template.

Create Notification Settings

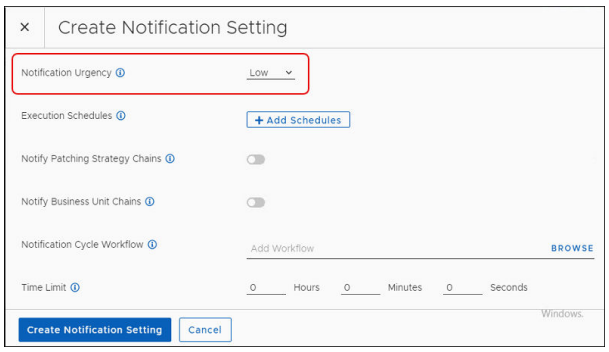
Set Notification Urgency

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** under **Notifications** 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.

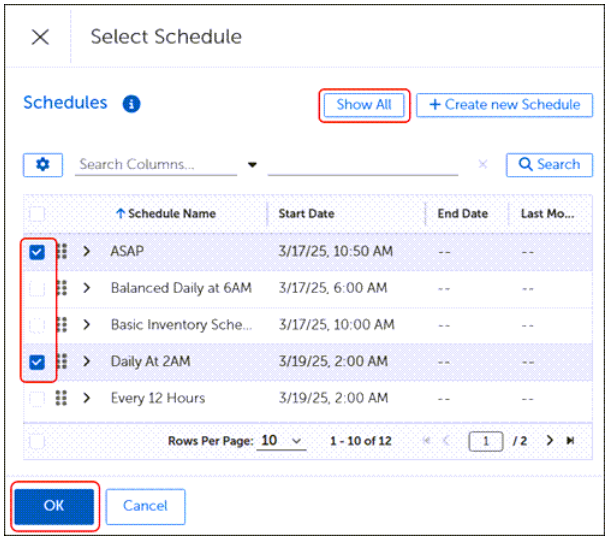


3. Continue editing the **Notification** settings or select Create Notification Settings to return to the template.

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 an object template.
2. Select **+Browse** next to **Execution Schedules** to display the available schedules.
3. Select one or more schedules from the **All Schedules** table, and then select **OK** on the lower-left of the dialog.



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

Enable Notifications for Patching Strategy and Business Unit Chains

When enabled, it 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:
   - 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.
   - 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 select Create Notification Settings to return to the template.

Choose a Notification Cycle Workflow

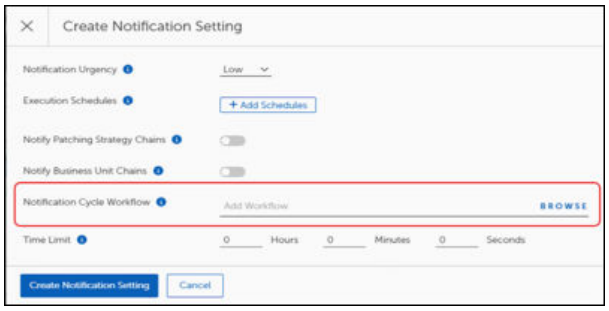
This setting names the Notification Cycle that processes the Notifications for the Patching Strategy or Deployment Channel. Notification Cycle workflows are customized for specific uses. Adaptiva does not provide sample Notification Cycle templates. These templates exist only if you create them for your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

IMPORTANT

Contact Adaptiva Customer Support for assistance with Notification Cycle templates.

1. Select **+Create Notification Setting** under **Notification** 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 select **Add Workflow** on the lower-left of the dialog.
4. Continue editing the **Notification** settings or select 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** under **Notification** 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 select 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, OneSite Patch 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. OneSite Patch 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 operating simultaneously. Therefore, 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, the Channel Merging Rules prevent multiple channels from executing simultaneously.

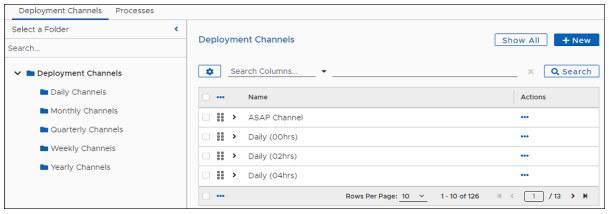
You can create multiple Channel Merging Rules for a Deployment Channel to address various potential scheduling issues. The Deployment Channel evaluates the rules according to the hierarchy; therefore, place higher-priority rules before lower-priority rules in the Channel Merging Rule dialog. The Deployment Channel evaluates each rule, and evaluation stops as soon as one rule matches. 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 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 of the dialog, and then select **Save As**.

b. Enter a new name for the template, and then select **Save as** on the lower-left of the dialog. This returns you to a copy of 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, and then select **Save** on the upper-left of the dialog.

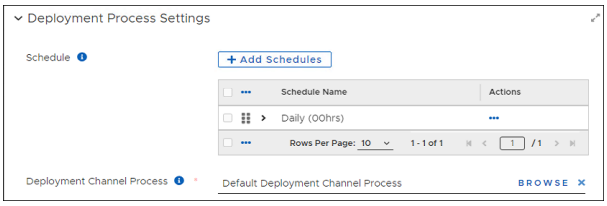
6. Move the new template to the folder you created, either now or after completing your changes.

Deployment Process Settings

To add Deployment Process Settings to a Deployment Channel template:

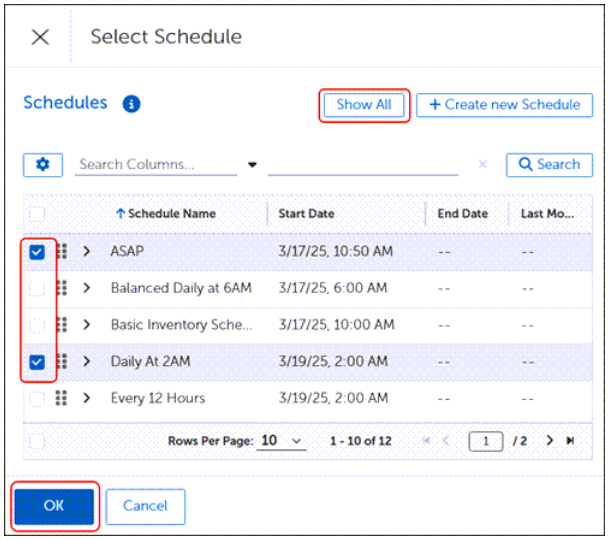
Open a Deployment Channel template, and then scroll down to **Deployment Process Settings** in an open Deployment Channel template.

This opens the Deployment Process workspace.



Add or Change a Deployment Process Schedule

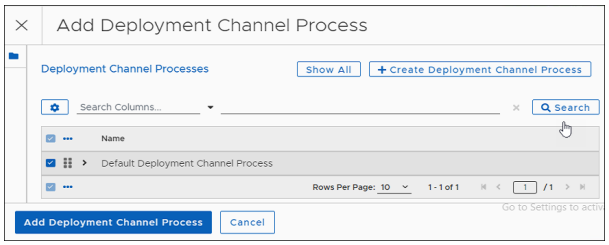
1. Select **+Add Schedules** from the **Deployment Process Settings** workspace of an open Deployment Channel template.
2. Select one or more schedules from the **All Schedules** table, and then select **OK** on the lower-left of the dialog.



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 then select the **Process** to use for this Deployment Channel.



3. Select **Add Deployment Channel Process** on the lower-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:

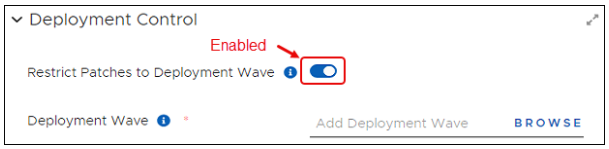
Open a Deployment Channel template, and then scroll down to the **Deployment Control** workspace.

Enable Deployment Control

The Deployment Control settings default 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 select Add Deployment Wave on the lower-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 the 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 upper-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

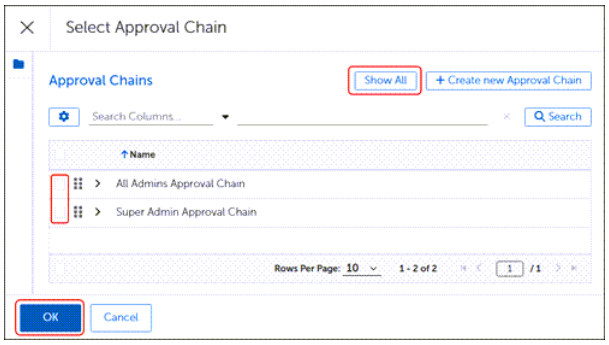
Approval Chains define and manage the approvals required before the Deployment Channel deploys patches to Business Units. Including an Approval Chain in a Deployment Channel template requires selecting an existing Approval Chain and saving it in the Deployment Channel template. For more information about 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 an open Deployment Channel template, scroll down to the **Approval Chain** workspace, and then select **Browse** next to **Add Approval Chain**.

   This opens the table of existing Approval Chains.



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

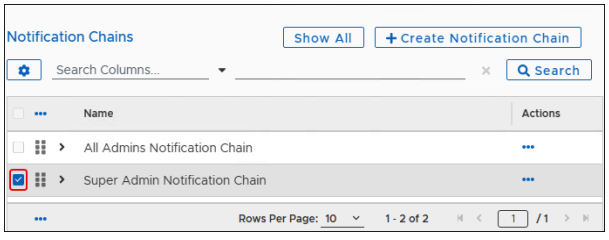
Notifications

Notification settings in the Deployment Channel template include adding a Notification Chain 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.



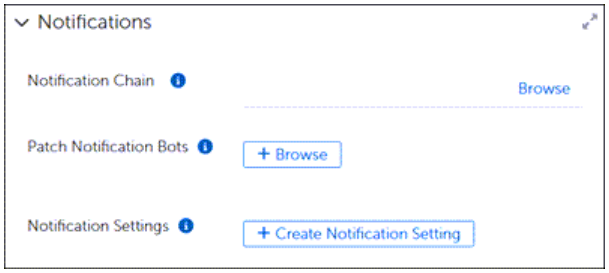
3. Select **Notification Chains**, and then select **Show All** to see the available templates.
4. Select a **Notification Chain** from the table. To edit or create Notification Chains, see Using Notification Chains.
5. Continue editing the **Notification** settings, or select **OK** (lower-left corner) to return to the template.

Create Notification Settings

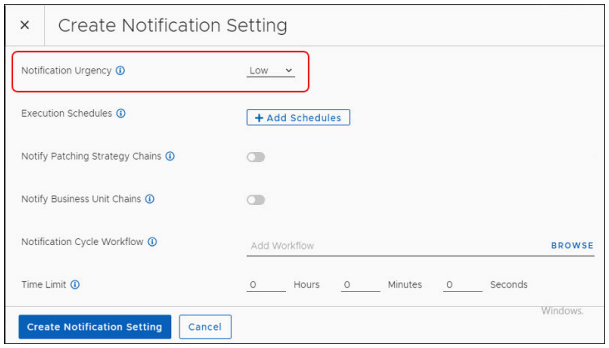
Set Notification Urgency

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** under **Notifications** 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.

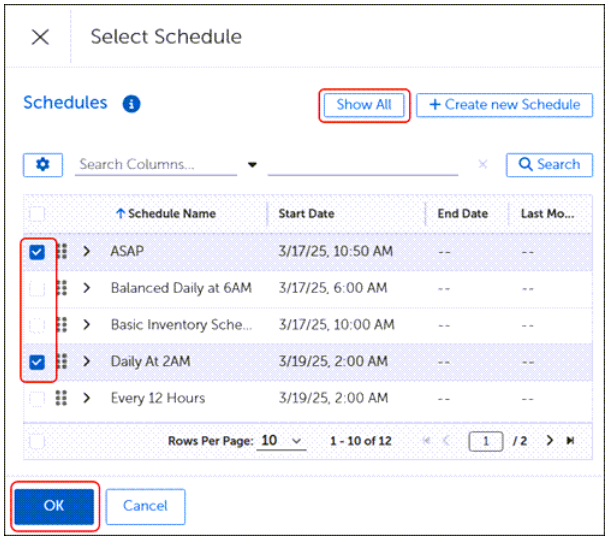


3. Continue editing the **Notification** settings or select Create Notification Settings to return to the template.

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 an object template.
2. Select **+Browse** next to **Execution Schedules** to display the available schedules.
3. Select one or more schedules from the **All Schedules** table, and then select **OK** on the lower-left of the dialog.



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

Enable Notifications for Patching Strategy and Business Unit Chains

When enabled, it 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:
   - 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.
   - 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 select Create Notification Settings to return to the template.

Choose a Notification Cycle Workflow

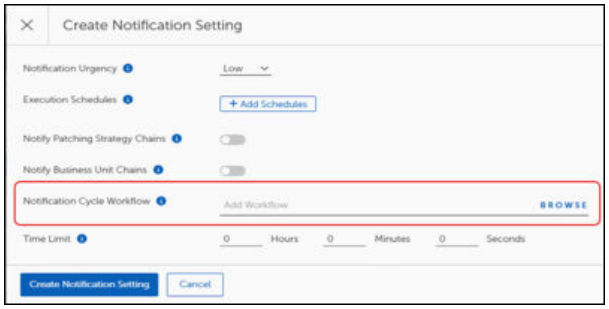
This setting names the Notification Cycle that processes the Notifications for the Patching Strategy or Deployment Channel. Notification Cycle workflows are customized for specific uses. Adaptiva does not provide sample Notification Cycle templates. These templates exist only if you create them for your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

IMPORTANT

Contact Adaptiva Customer Support for assistance with Notification Cycle templates.

1. Select **+Create Notification Setting** under **Notification** 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 select **Add Workflow** on the lower-left of the dialog.
4. Continue editing the **Notification** settings or select 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.

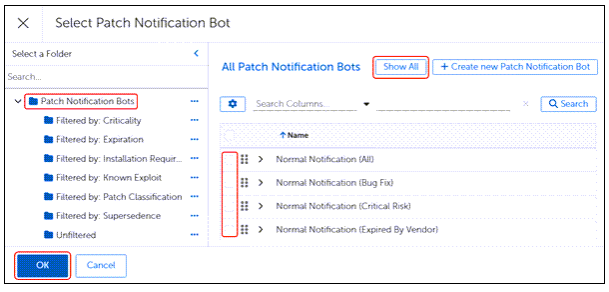
1. Select **+Create Notification Setting** under **Notification** of the object template.
2. Next to **Time Limit**, set the **Hours**, **Minutes**, or **Seconds** that the Notification Cycle will run, or leave the setting default at 0 for each item to allow the workflow to run indefinitely.
3. Continue editing the **Notification** settings, or select 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 **+Browse** next to **Patch Notification Bots** in the **Notifications** workspace of the object template.

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



2. Select **Patch Notification Bots**, and then select **Show All** to list all available **Patch Notification Bots**, or select 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 **OK** on the lower-left of the dialog to return to the starting template.

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 the Merge Duration. For more information, see Understanding Channel Merging Rules.

1. Select **Browse** next to **Add Deployment Channel**, and then select a **Deployment Channel**.
2. Select **+Create Channel Merging Rule** under **Notification** of a Deployment Channel template.
3. Select **Add Deployment Channel** at the lower-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.

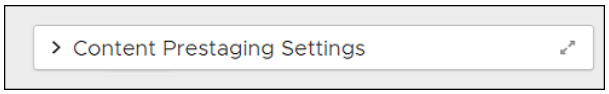
Content Prestaging Settings

The Content Prestaging feature deploys 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.

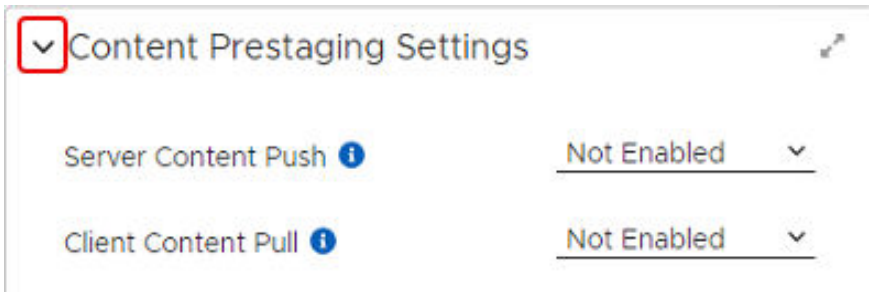
Set Content Prestaging Settings

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

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

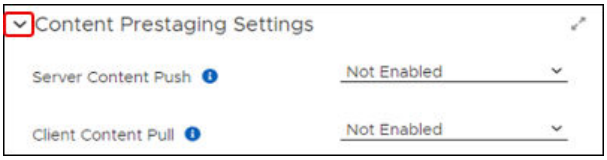


2. Expand the **Content Prestaging Settings** to view the available settings.

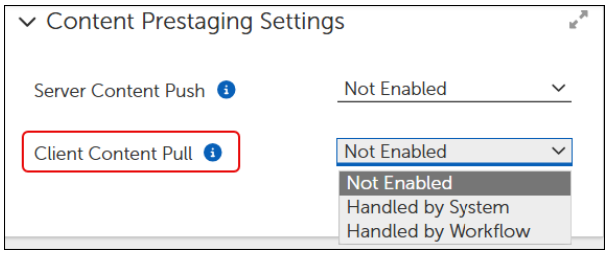


Enable Client Content Pull

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:



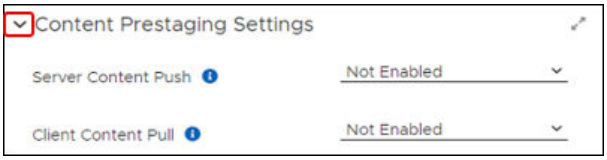
1. Select the arrow to the right of **Client Content Pull** to expand the menu of available options.



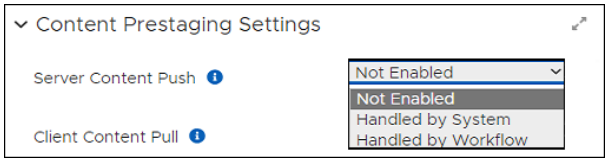
2. Select the option you need for the object template you are using. For definitions of push options, see Defining Content Prestaging Settings.
3. Select **Save** on the upper-left to save your changes:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** again if you make any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



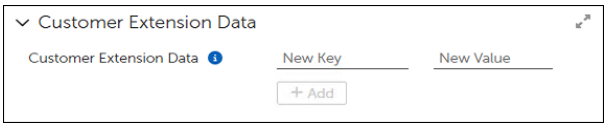
1. Select the arrow to the right of **Server Content Push** to expand the menu of available options.



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 Adaptiva. 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 Adaptiva 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 Adaptiva 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 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 of the dialog, and then select **Save As**.

b. Enter a new name for the template, and then select **Save as** on the lower-left of the dialog. This returns you to a copy of 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, and then select **Save** on the upper-left of the dialog.

Add a Deployment Wave Entry

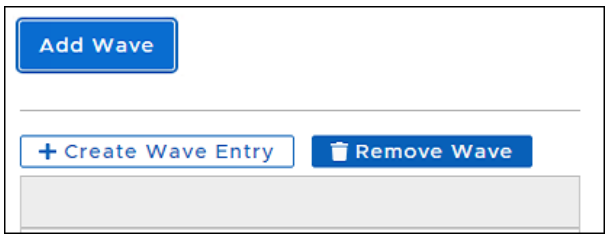
1. Scroll down to **Deployment Waves** in an open Deployment Wave template.
2. Select **Add Wave**. This creates a new table to hold another Wave in the template.

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

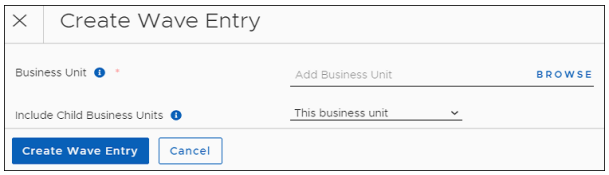
4. Select **Browse** next to **Add Business Unit**:
   a. Navigate to and select the Business Unit to which the Wave Entry applies.
   b. Expand the **Include Child Business Units** menu to include one or more child Business Units of the selected parent.
   c. Select the **item** that best describes 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.
   m. 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 Adaptiva 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:
   - To remove the Wave, select **Remove Wave Entry**.
   - 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. OneSite Patch 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 OneSite Patch 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.

OneSite Patch 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 Patch Dashboard.

> **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 **Show All** to display the available Maintenance Window settings. If Show All is grayed out, the table includes all available settings.
3. 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 of the dialog, and then select **Save As**.
   b. Enter a new name for the template, and then select **Save as** on the lower-left of the dialog. This returns you to a copy of 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, and then select **Save** on the upper-left of the dialog.

Dynamic Settings

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 Customer SupportAdaptiva Customer Support.

Add Dynamic Detection Workflow (Optional)

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 select **Add Workflow** in the lower-left corner.

Maintenance Windows by Urgency

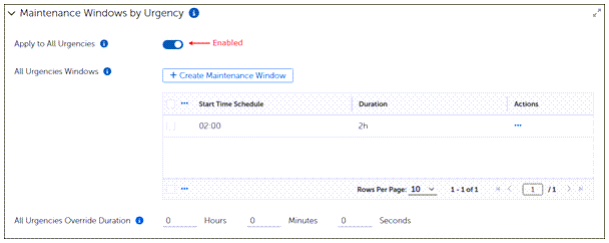
Create Maintenance Windows for use with different urgency settings (Low, normal, High, or Critical) or create a single Maintenance Window that applies to all Urgencies. Because urgency settings are cumulative, any settings specified at lower urgencies are inherited by higher urgency Maintenance Windows.

The urgency configuration settings use the same template whether creating a single maintenance window for all urgencies or creating individual maintenance windows for specific urgency levels.

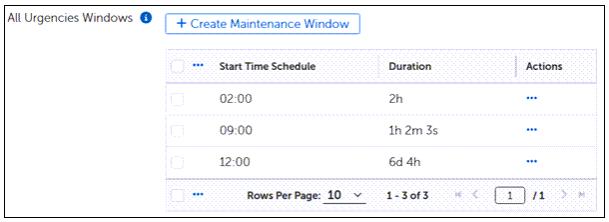
Apply a Maintenance Window to All Urgencies

Use the Maintenance Windows by Urgency workspace of an open Maintenance Window template to create an All Urgencies Maintenance Window. You may create multiple All Urgencies Maintenance Windows with different start times.

1. Select the toggle for **Apply to All Urgencies** to enable the All Urgencies options.



2. Configure the Maintenance Window schedule for patches of all urgencies:
   a. Select **+ Create Maintenance Window** to begin.
   b. Select **Browse** to open the list of all available start time schedules.
   c. Select the **schedule** you want to add, and then select **OK** to close the list of schedules.
   d. Enter the number of **Hours**, **Minutes**, or **Seconds** after the start time setting that the Maintenance Window remains open (required), and then select **Create Maintenance Window** on the bottom left corner to close the dialog.
   e. Repeat Step 2 to schedule additional Maintenance Windows for all urgencies.



3. Set an **All Urgencies Override Duration**.

   These settings override any non-zero duration values set inn the Maintenance Window when the Maintenance Window fails to open for urgency level updates.

4. Enter the number of **Hours**, **Minutes**, or **Seconds** to wait after the Maintenance Window fails to open to override the Maintenance Window duration settings.

Save and Deploy the Maintenance Window

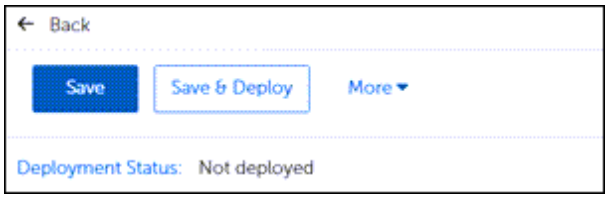
Deploy a Maintenance Window to make it available for use in a template. If you update a Maintenance Window template that was previously deployed, you must save and deploy it again for the changes to take effect.

1. Complete the Maintenance Window configuration (see Open and Save a Maintenance Window Template).

2. Save your changes:

   Select **Save & Deploy** to save and deploy your configuration:

   - Select **Save & Deploy** to save and deploy your changes.
   - Select **Save** to save your changes without deploying. Be sure to return and **Deploy** the changes to make them 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 OneSite Patch are HTML email, Simple email, HTML SMTP, Simple SMTP, SMS/Text, Microsoft Teams Notification, or WhatsApp notification.

Using Communication Providers

Adaptiva 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 the 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 of the dialog, and then select **Save As**.
   b. Enter a new name for the template, and then select **Save as** on the lower-left of the dialog. This returns you to a copy of 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, and then select **Save** on the upper-left of the dialog.

Set Communication Provider Properties

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

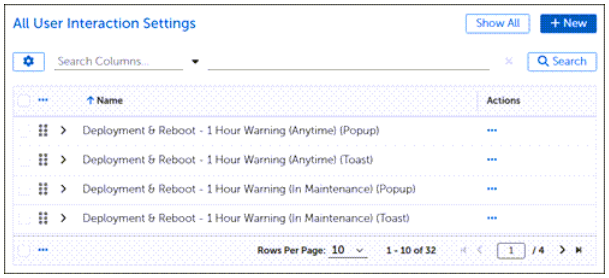
3. Select the **Supports Subject Line** toggle to enable or disable (default) whether this Communication Provider supports the ability to include a subject line with its messages.
4. Enter the **From Address** to use when utilizing the SMTP Server settings to communicate, if the Communication Provider 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).

Open and Save a User Interaction Template

1. Select **User Interaction Settings** in the left navigation menu of the Patch Dashboard, and then select **Show All**.

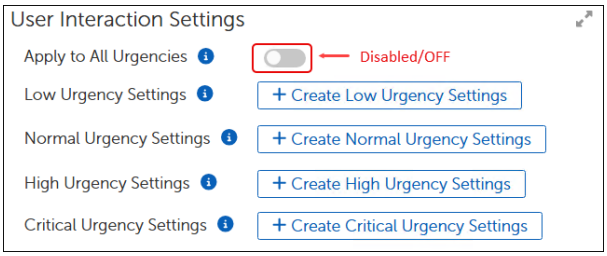


2. Select the Name of an existing template to open it. This example uses the Deployment & Reboot – 1 Hour Warning (Anytime)(Toast) template.
3. Save the template with a new name:
   a. Select **More** in the upper-left of the dialog, and then select **Save As**.
   b. Enter a new name for the template, and then select **Save as** on the lower-left of the dialog. This returns you to a copy of 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, and then select **Save** on the upper-left of the dialog.

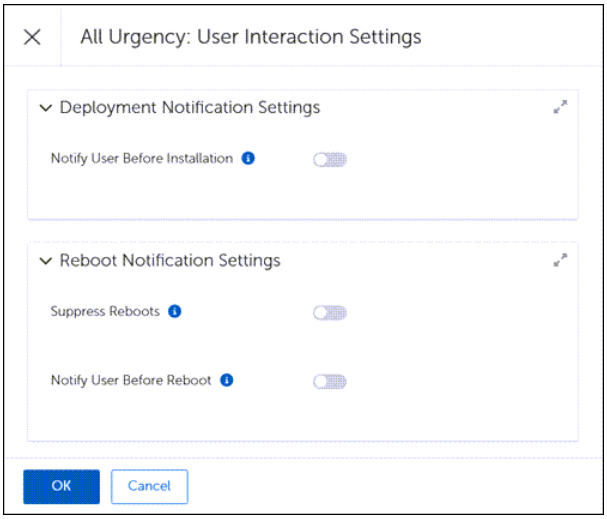
Choose Urgency Settings

1. Scroll down to **User Interaction Settings** in an open User Interaction Settings template:
   - 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).

   - 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 setting urgencies for all levels:
   - Each setting, including **Apply to All Urgencies**, uses the same template layout and fields.
   - This example uses the **Apply to All Urgencies** setting. The example below shows all settings disabled.



3. Configure deployment notification settings.

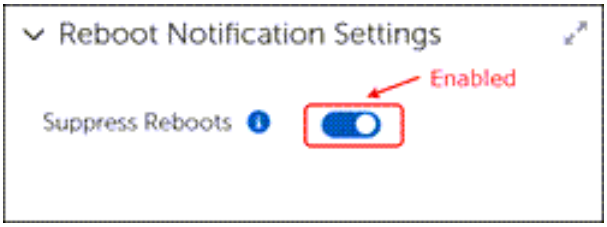
Configure Deployment Notification Settings

1. Select the toggle for **Notify User Before Installation** enable user notification when a deployment begins:
2. Set the **Notification Suppression Duration** to the number of Days, Hours, Minutes, or Seconds before the user receives another notification.
   - For example, if the user sees and chooses 5 minutes, the client waits 5 minutes before allowing another deployment notification to pop up.
   - When set to zero (0), the user does not receive any delay options.
3. Enter **Notification Text** in the text box. The user sees this text when the notification arrives on their device.
4. Next, see Reboot Notification Settings.

Reboot Notification Settings

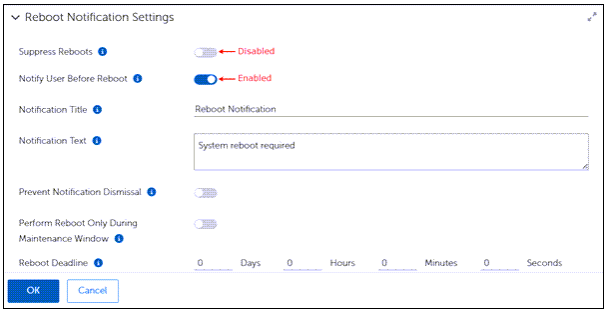
The Reboot Notification Settings in a User Interaction Settings dialog provides choices to Suppress Reboots and to Notify User Before Reboot.

Suppress Reboots: Enabling **Suppress Reboots** means that system automated reboots do not occur. Users must reboot their devices at their own discretion to complete patch deployments. Failure to reboot may prevent a deployment to that device. Use caution when suppressing reboots.



Notify User Before Reboot: Enabling **Notify User Before Reboot** allows you to customize user notifications when a deployment requires a device reboot. Configuration options for administrators include the following:

- Prevent users from dismissing notifications.
- Schedule reboot only during maintenance windows.
- Customize reboot deadline and postponement options (Days, Hour, Minutes, Seconds).
- Prevent or allow snooze duration and customization.



Configure Reboot Settings

With **Notify User Before Reboot** enabled, you may set other conditions related to the reboot. These include notification dismissal, rebooting during maintenance window, and reboot deadline.

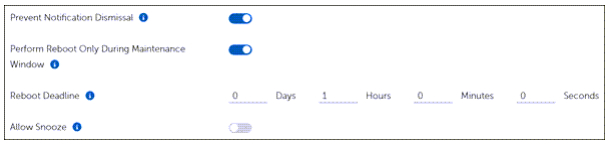
1. Select the **Perform Reboot Only During Maintenance Window** toggle to enable or disable reboot during the maintenance window established in the Business Unit that includes the device:
   - Enable to reboot only during the maintenance window.

   - Disable to allow reboot at any time.

2. Select the **Prevent Notification Dismissal** toggle to enable or disable whether the client device user may dismiss the notification:
   - Enable to prevent the user from dismissing the notification.

   - Disable to allow the user to dismiss the notification.

3. Enter the number of **Days, Hours, Minutes, or Seconds** to set the Reboot Deadline.



   - These entries define the amount of time that may pass before the system forces the reboot to occur.
   - If zero, OneSite Patch provides no warning to the user.

4. Configure snooze settings.

Managing Snooze Settings

When defining User Interaction Settings, OneSite Patch provides several configuration choices that define how a user interacts with reboot notifications and snooze settings. With Allow Snooze enabled, the user receives notification of a required reboot and may snooze the notification. This does not change the reboot deadline. Rather, it allows the user to snooze the notification for a set period of time that does not exceed the Reboot Deadline.

Administrators set the parameters of the user interaction by setting maximum snooze duration times, snooze reminders, and snooze durations. You may customize all snooze option settings to timing that meet your requirements.

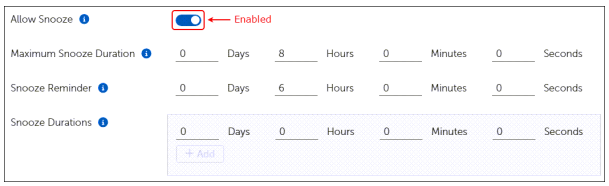
Snooze Duration settings default to the default settings shown below. If you do not specify a snooze duration (all settings 0), the default settings apply. The combination of default settings for Snooze Duration will not exceed the Maximum Snooze Duration setting. For example, setting the maximum duration to 30 minutes, limits the end user choices for snooze options to 5 minutes or 15 minutes.

- 4 hours
- 2 hours
- 1 hour
- 15 minutes
- 5 minutes

Configure Snooze Settings

Customize user interactions with reboot notifications by allowing snooze, and then setting snooze durations and snooze reminders. For details about default settings and limitations, see Managing Snooze Settings.

1. Select the toggle for **Allow Snooze** to enable or disable snooze options.



   - When enabled, you may define the timing of user interactions reboot notifications.
   - When disabled, the user receives no notification.

2. Define the Snooze settings:
   a. **Maximum Snooze Duration**: This is the maximum amount of time the user may snooze the reboot.

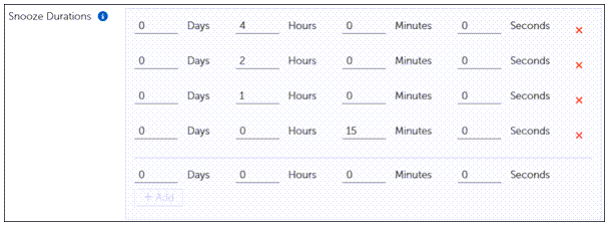
      Enter the **Days**, **Hours**, **Minutes** or **Seconds** that define the **Maximum Snooze Duration** (defaults to 8 hours).

   b. **Snooze Reminder** settings: Sets the amount of time between the notifications the user receives after the first snooze.

      Enter the **Days**, **Hours**, **Minutes** or **Seconds** that define the **Snooze Reminder** gap (defaults to 6 hours).

   c. **Snooze Duration**. Leave settings at zero (0) to use the default settings.

      Enter the **Days**, **Hours**, **Minutes** or **Seconds** that define the **Snooze Duration** (defaults to 4 hours, 2 hours, 1 hour, 15 minutes.



3. Select **+Add** to create additional **Snooze Duration** settings. You may add up to 5 additional lines.
4. Select **OK** on the bottom left corner to return to the User Interaction Settings workspace.

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. Complete the User Interaction configuration (see User Interaction Settings).
2. Save your changes:

   Select **Save & Deploy** to save and deploy your configuration:
   - Select **Save & Deploy** to save and deploy your changes.
   - Select **Save** to save your changes without deploying. Be sure to return and **Deploy** the changes to make them available for use.

Customized Products

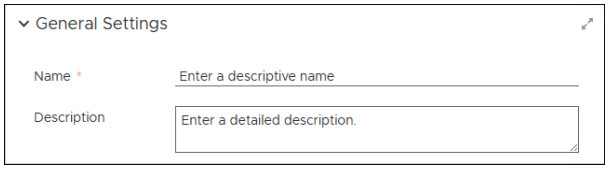
Software products and patches sometimes require user interaction when installing. Users enter details such as license information or request to show a menu at startup. Other default settings include auto update, or desktop shortcuts.

Adaptiva 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 Patch Dashboard.
2. Select **+ New** in the upper-right to open a new template:



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

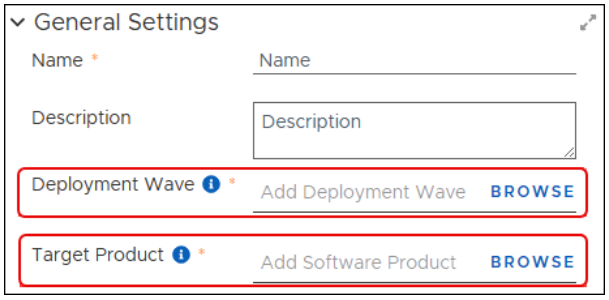
b. Enter a detailed **Description**, and then select **Save** on the upper-left of the dialog.

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.

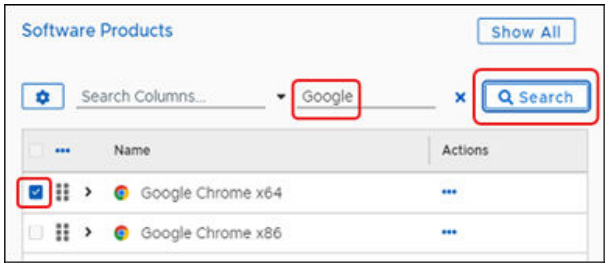
1. Select **Browse** next to **Add Deployment Wave** in an open Customized Product Template.



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 of the **Deployment Waves** dialog.
4. Select **Save** on the upper-left 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 select **Search**.

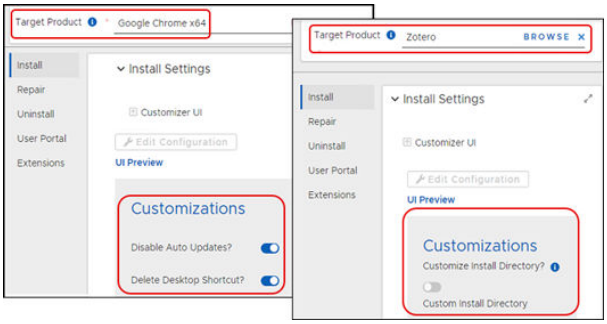


3. Select the **Software Product** you want to customize. You can target only one Software Product in each Customized Product entry.
4. Select **Add Software Product** to populate the configurable items in the static list of **Install Settings**. Settings change depending on the Target Product.

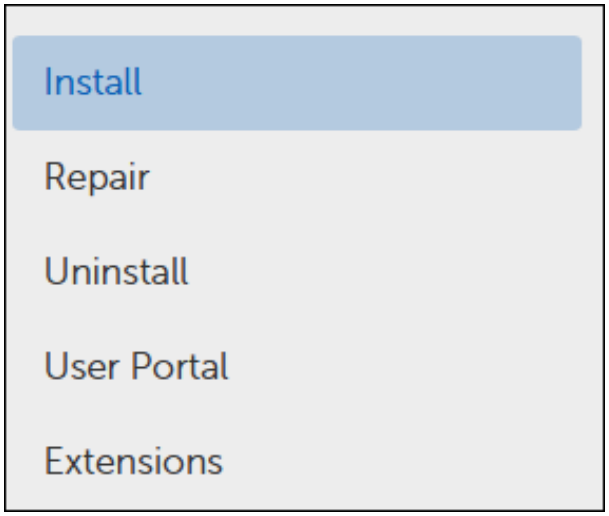
5. Select **Save** in the upper-left of the template to save your changes.
6. Continue with Configure Software Install Settings.

Configure Software Install Settings

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



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



3. Select **Save** on the upper-left 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.
4. Select **<-- Back to Customized Products** above **General Settings**. 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.

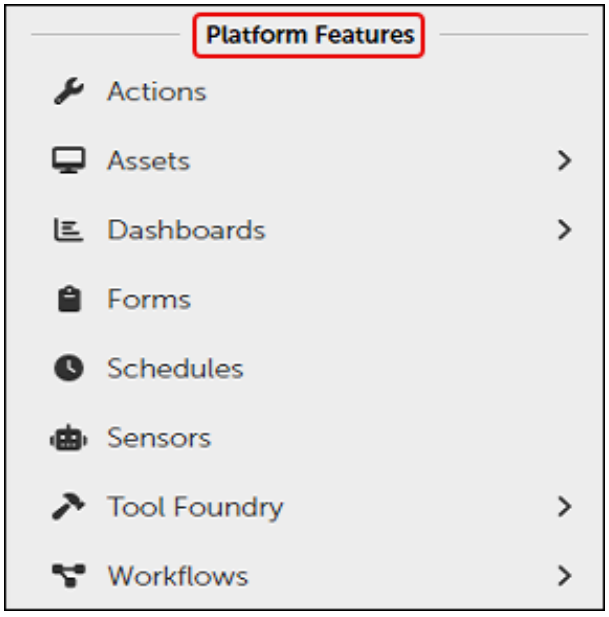
Select **Content Name** in the table to view the patch details. Information provided in the individual report includes Patch ID, Version, Content Size, Publication Status, and Content Details.

Schedules

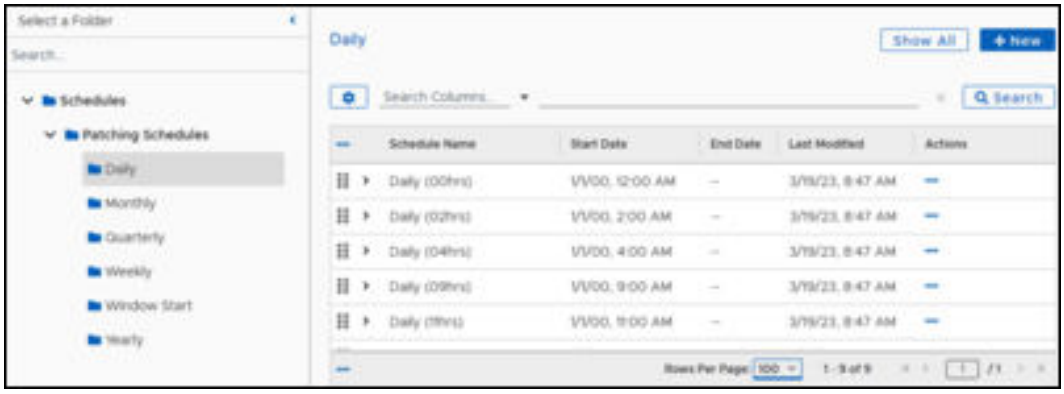
Adaptiva uses schedules throughout the product to automate patching processes that include content push, updating custom groups, setting maintenance windows, and more. Adaptiva provides several default schedules you can customize for your environment, or you can create new schedules. Schedules created in Adaptiva are available for use across all OneSite products.

View Available Schedules

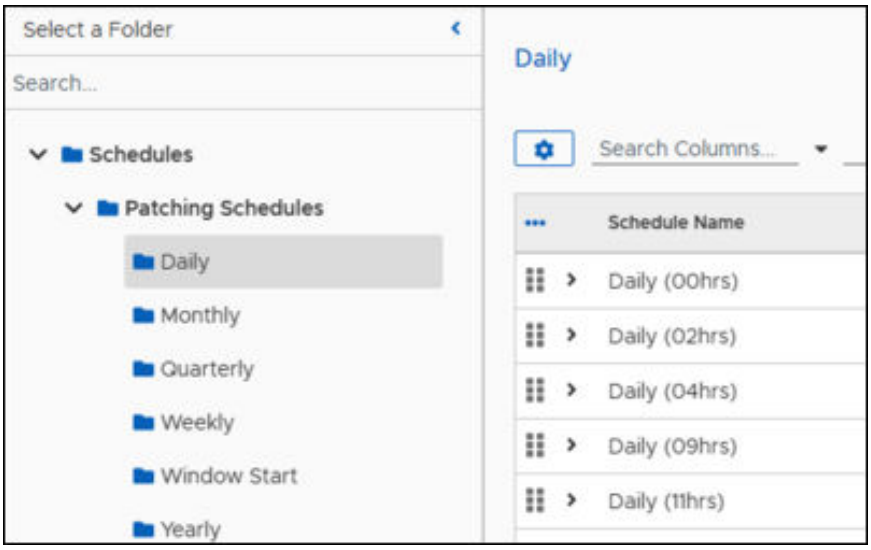
1. Select **Schedules** in the **Platform Features** menu of the *Dashboard*.



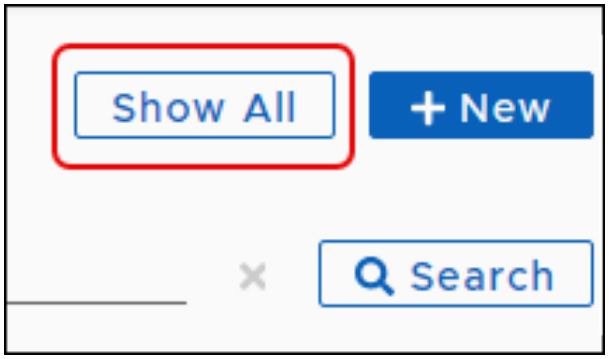
This opens the list of available schedules.



2. Choose how you want to view schedules:
   - Select one of the **Patching Schedule** folders listed in the left navigation pane. These choices list the available schedules for each category.
   - 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.

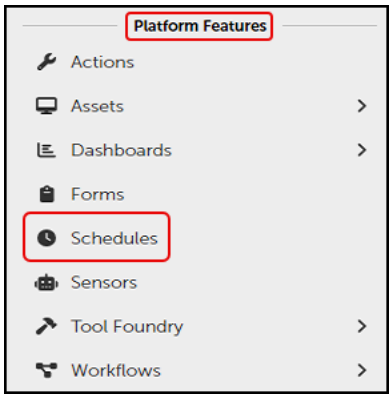


Create a Custom Schedule

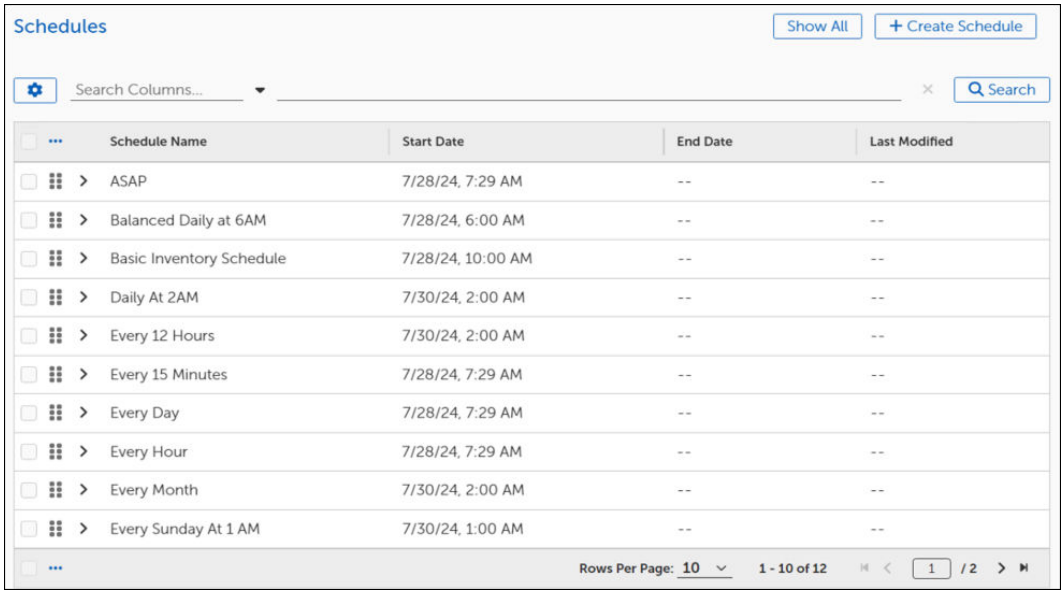
This example customizes an existing schedule template. You can also create a new schedule template under **+ New**. The template layout for either includes the same choices and fields.

Open and Save a Schedule Template

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



   This opens the list of available schedules.



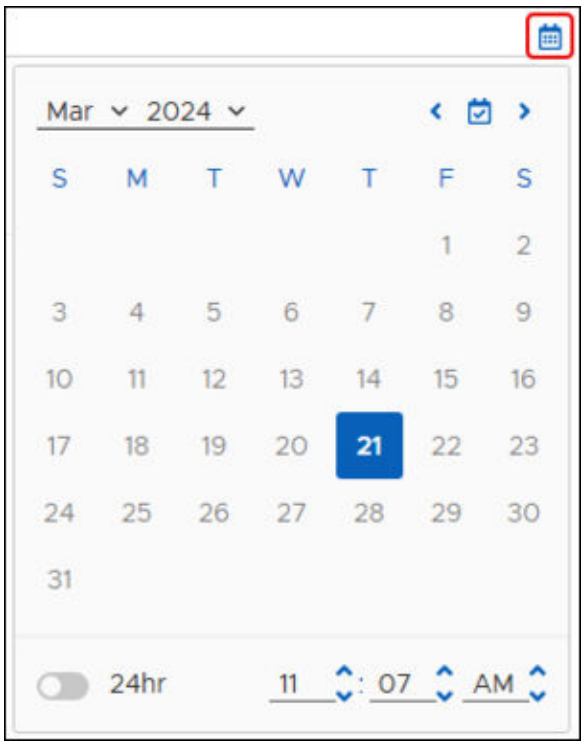
2. Select a **Schedule Name** from the table to open that scheduling template.
3. Save the template with a new **Name**:
   a. Select **More** in the upper-left of the dialog, and then select **Save As**.
   b. Enter a new name for the template, and then select **Save as** on the lower-left of the dialog. This returns you to a copy of 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, and then select **Save** on the upper-left of the dialog.

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 OneSite Patch 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.

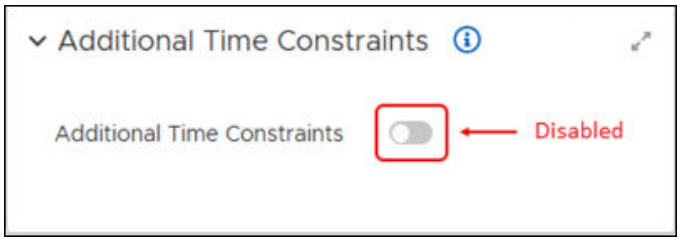
Recurring

- **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).

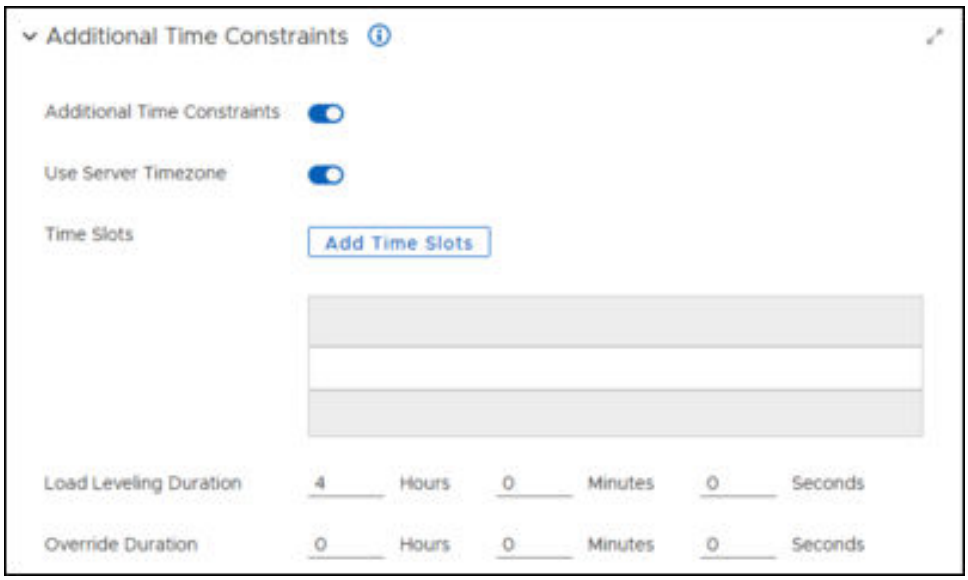
Set Additional Time Constraints

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 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. Adaptiva 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 Adaptiva.

1. Select **Schedules** in the **Platform Features** menu of the Patch Dashboard.
2. Set **Rows Per Page** at the upper-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 select **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, select **OK** to delete the schedule. You may not undo this action.

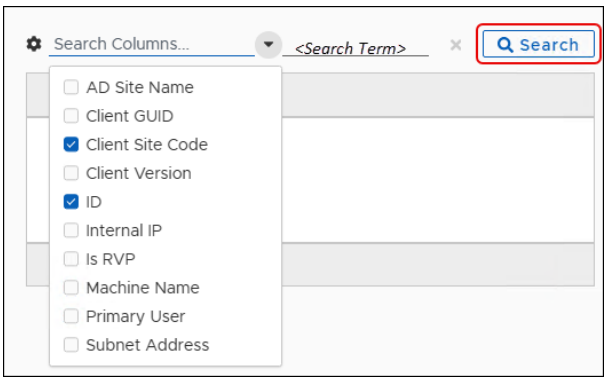
Patching Analytics Dashboards

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 OneSite Patch

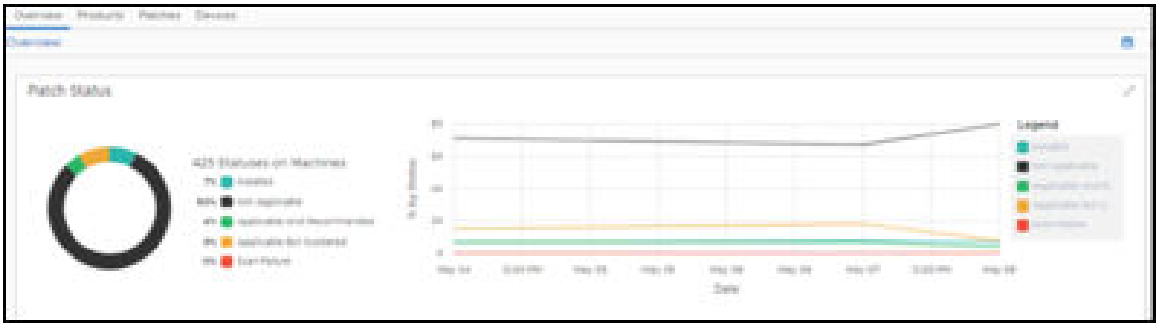
For tables in any dashboard view, the drop-down list next to **Search** allows you choose a column to search within. This provides several options for searching depending on the search term you have selected. Column choices change depending on the menu object.



Patching Analytics Overview

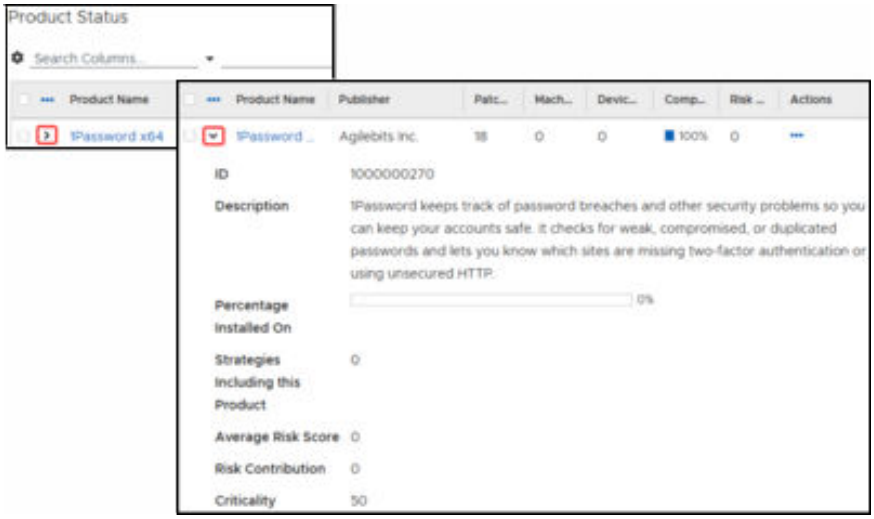
The **Overview** summarizes the state of all patches in the environment. This view includes **Patch Status** and **Product Status** widgets.

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 OneSite Patch 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.

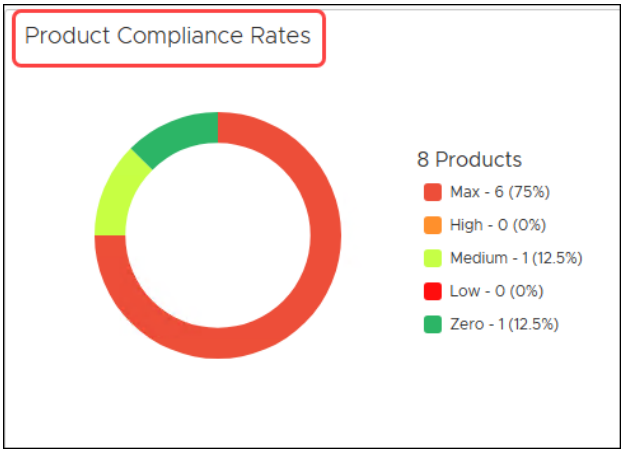


Products View

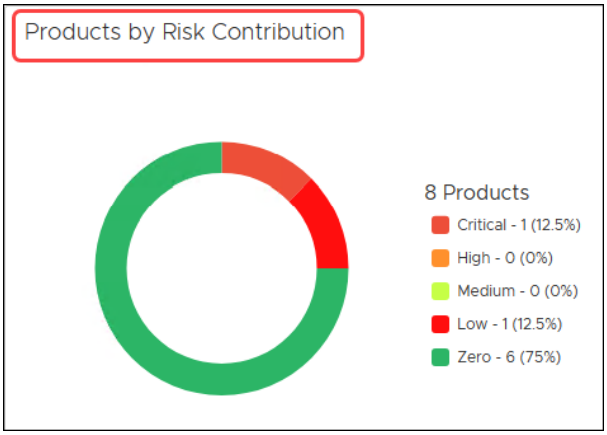
The **Products** view summarizes information from the product perspective.

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

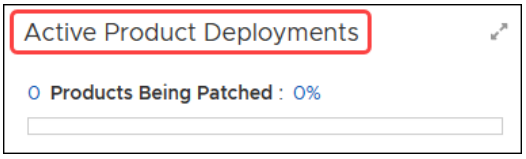
Product Compliance Rates show the number of products in the environment and the compliance rates by percentage. It also includes a chart that shows the level of compliance (**Compliant**, **Compliant by Exclusions**, and **Non-Compliant**) over time.



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.

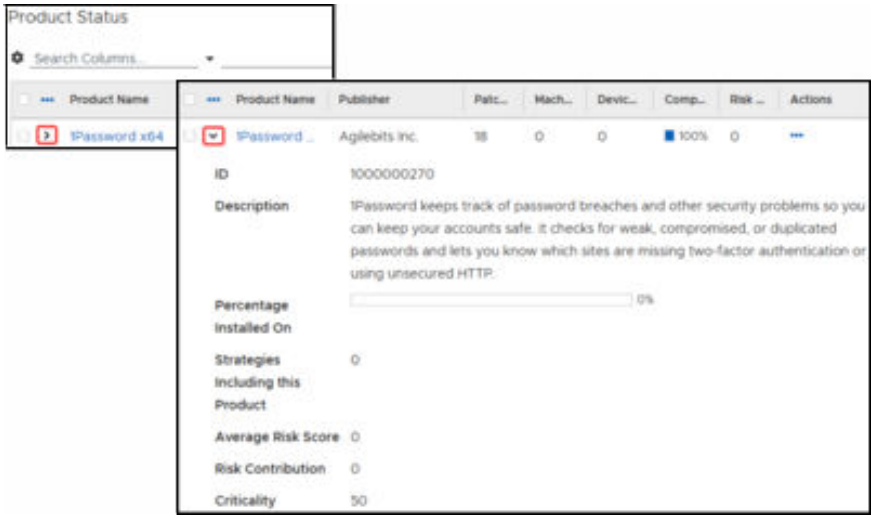


Active Product Deployments for products provides the number of products undergoing patching and the percentage of completion.



Product Status is a table that lists each product that OneSite Patch 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.



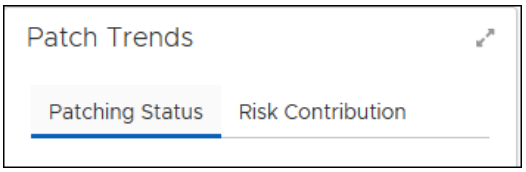
Patches View

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

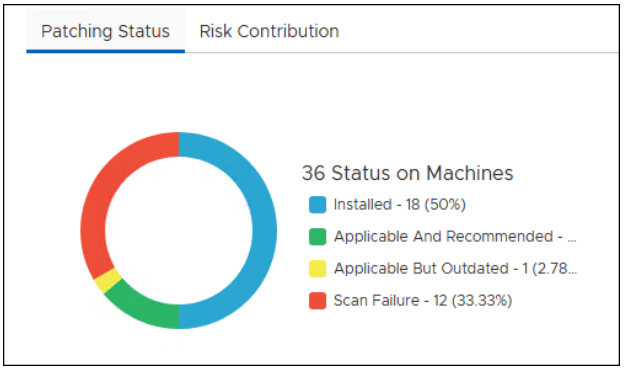
Patch Metrics tracks total patches, patches consumed, installed, or not required, and provides a visual indication of patch installation over time.

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

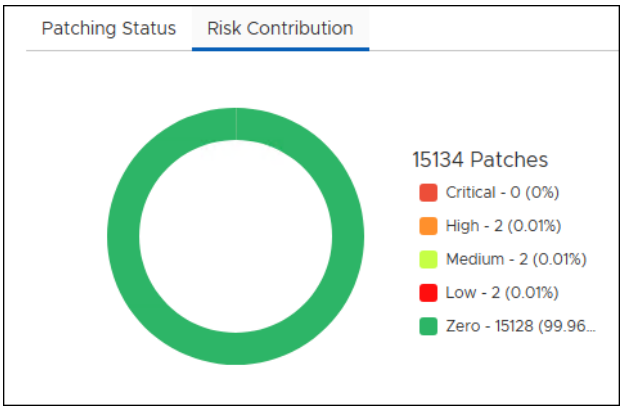
Patch Trends includes two tabs, one for **Patching Status** and one for **Risk Contribution**.



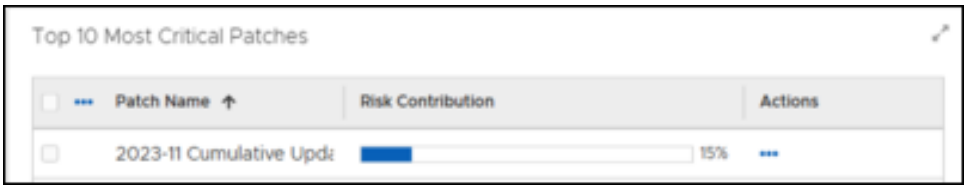
Patching Status shows the status of all patches, the number of machines tracked in the environment, and the number of patches in each status (**Installed**, **Applicable and Recommended**, **Applicable but Outdated**, **Scan Failure**) by percentage. The chart shows patching status over time.



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.

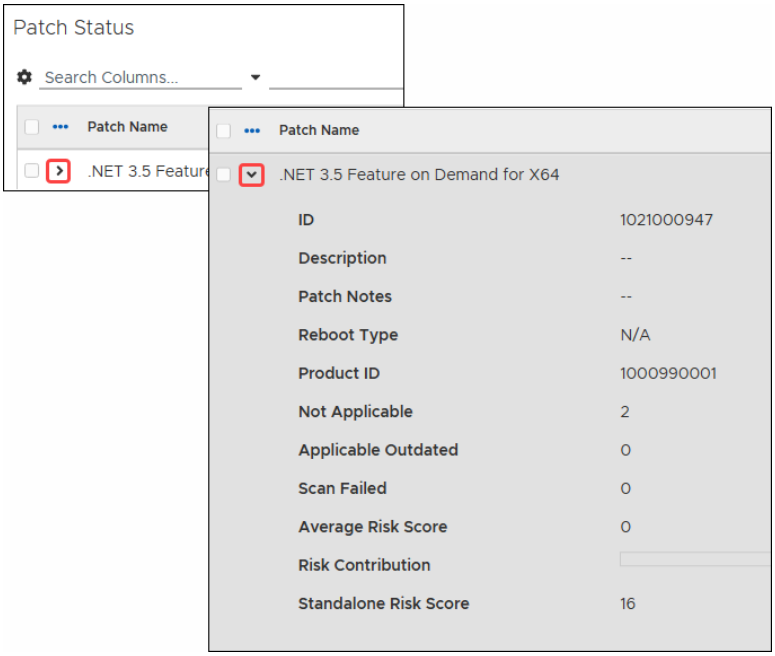


Top 10 Most Critical Patches tracks the risk contribution of the top ten most critical patches in the environment.



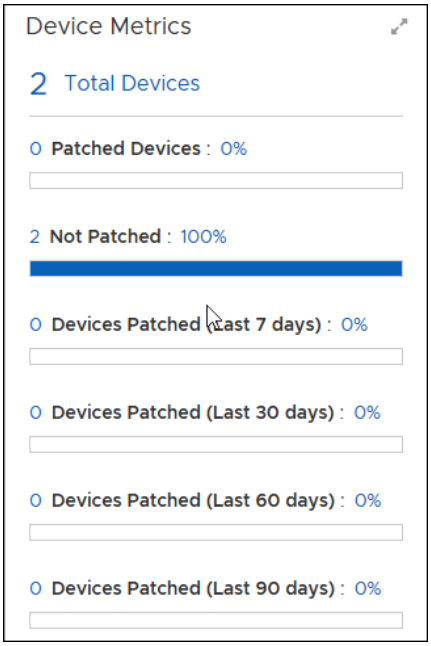
Patch Status is a table that lists each patch that OneSite Patch looks for during a scan, the installation/applicability status of each, and the status, compliance, and Risk Score for each.

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

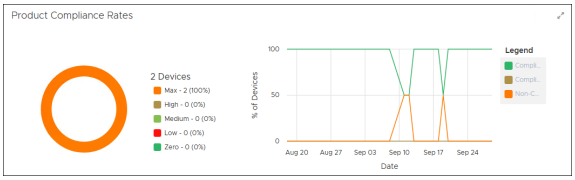


Devices View

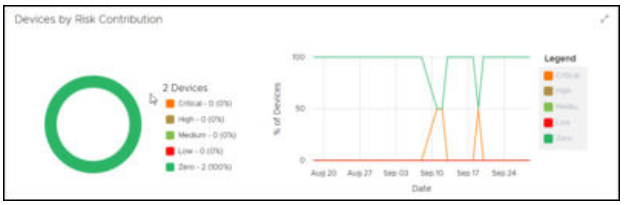
The **Device Metrics** widget shows the total number of devices in the environment, the percentage of patched and unpatched devices, and the percentage of devices patched in the last 7, 30, 60, and 90 days.



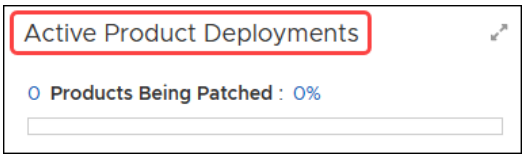
The **Product Compliance Rates** for Devices shows the rate of compliance for each device in the environment based on the latest device scan information. The graph displays the percentage of devices that fall into each category of compliance (max, high, medium, low, and zero), and the line graph shows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



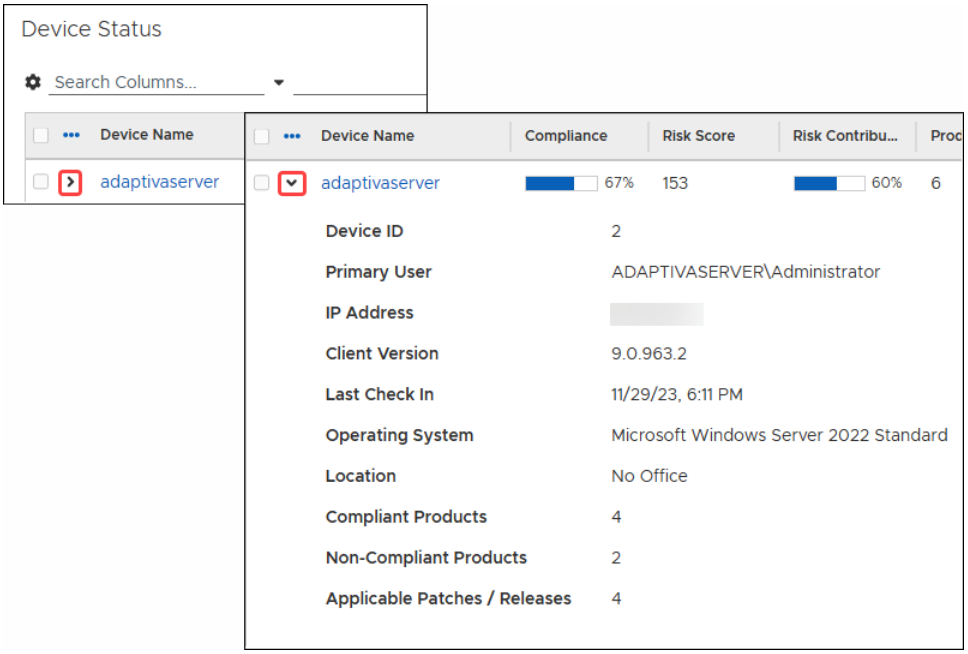
The **Risk Contribution** widget for Devices shows the total number of devices and the percentage that fall into each risk category (critical, high, medium, low, zero). The chart shows risk contribution trends over time.



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 a patch to a previous version. See Rollbacks.

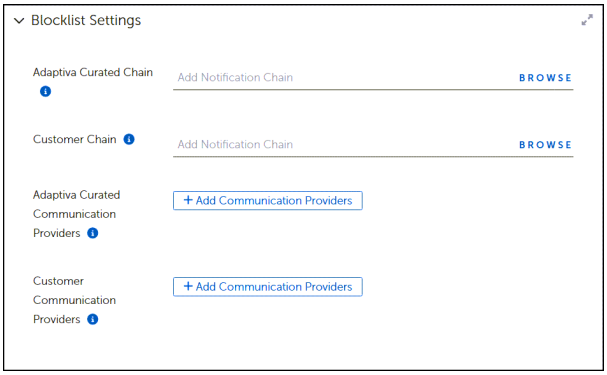
Blocklisting

Adaptiva includes an extra level of protection for customer devices and patching processes called Blocklisting. The Adaptiva 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 Adaptiva metadata team reviews the content and determines whether the patch has any issues that might cause unexpected behavior. The metadata team block lists 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.



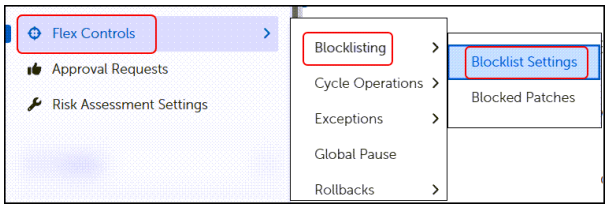
Managing Blocklist Notification Settings

Set categories of notification by selecting a Notification Chain to use when Adaptiva blocklists a patch/release. Select the same or a 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.

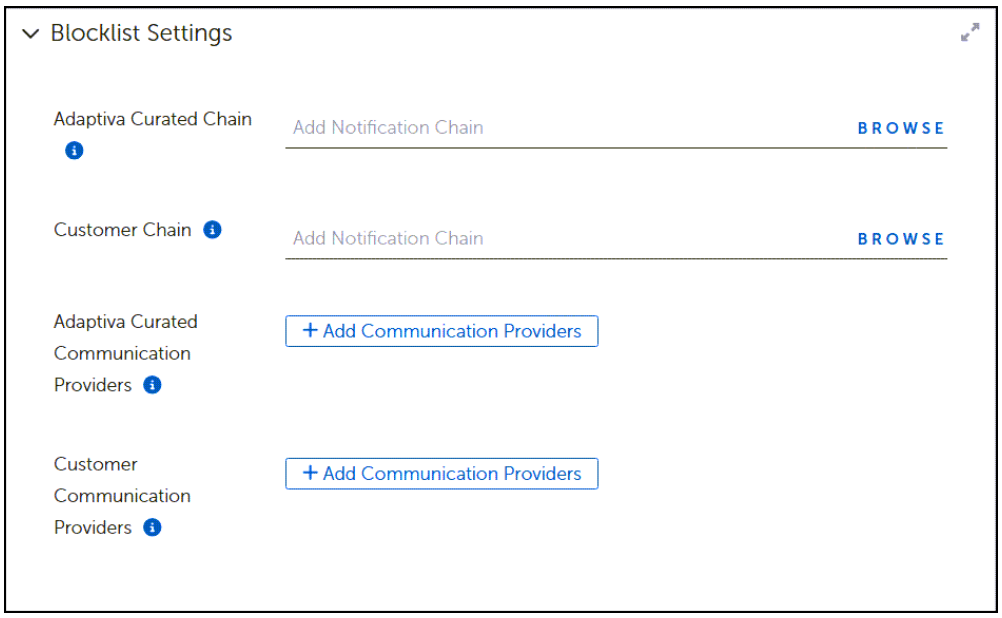
View Blocklist Settings

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

1. Mouse over or select **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 **Adaptiva 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 **Adaptiva Curated Chain** or the **Customer Chain**.
4. Select **Add Notification Chain** on the lower-left of the dialog.

Choose Communication Providers for Notification Chains

1. Navigate to Blocklist Settings.
2. Select **+ Add Communication Providers** for either or **Customer Communication Providers** from the **Blocklist Settings**.
3. Select one or more **Names** from the **Communications Provider** table, and then select **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.

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 each completed cycle. Select each completed cycle to review details.

Details available for each cycle type include the following:

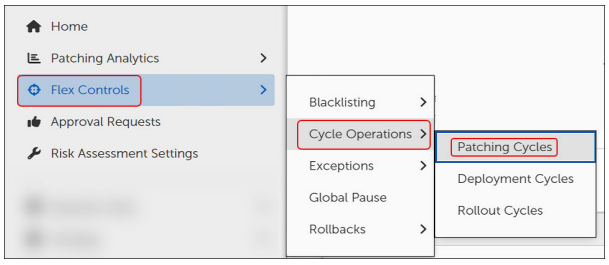
- **Cycle Information**: Provides general information about the Patch Process, such as the Current State, the creation date and time, and the Patch Process schedule. This section also contains controls to manually start, stop, or delay a Patch Process.
- **Overall Metrics**: This section contains information 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

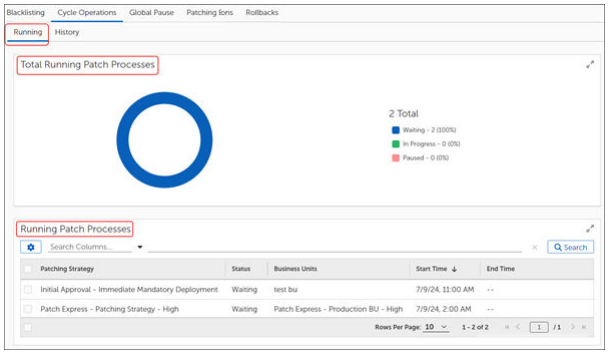
This dashboard shows information about the active Patch Processes in the environment. Patch Processes represent the workflow that models and performs the defined patching routine. As part of the overall Patching Strategy, Patch Deployment Bots use configured criteria to identify patches that apply to 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 select **Flex Controls** on the **Home** menu, and then select **Cycle Operations > Patching Cycles**.



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



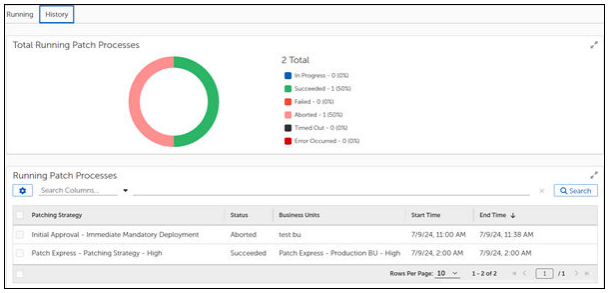
- The **Total Running Patch Processes** widget shows an aggregate summary of all patch processes and their corresponding states (**Waiting**, **In Progress**, or **Paused**).
- The **Running Patch Processes** table lists the running Patching Strategies by name.

2. Enter a **Patching Strategy** name in the search bar above the **Running Patch Processes** table, and then select **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 select **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:
   - 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).
   - 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 select **Search**.

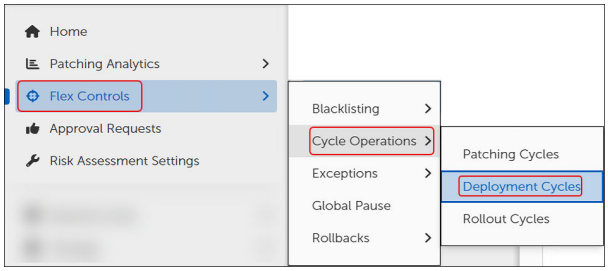
4. Select the **Patching Strategy** name in the **Running Patch Processes** table to see specific details about that process.

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

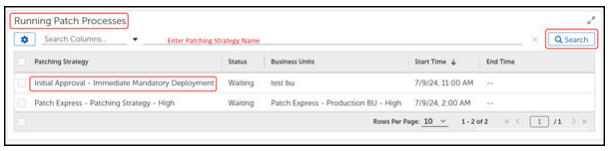
1. Mouse over or select **Flex Controls** in the **Home** menu, and then select **Cycle Operations > Deployment Cycles**.



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

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

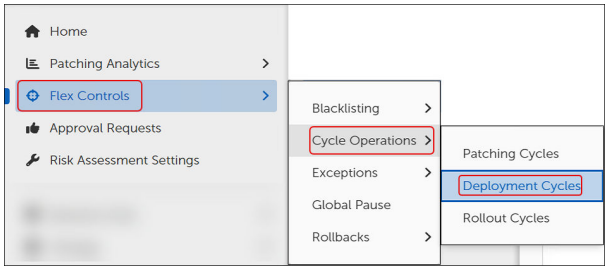
2. Enter a **Deployment Strategy** name in the search bar above the **Running Patch Processes** table, and then select **Search**.



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 select **Flex Controls** in the **Home** menu, and then select **Cycle Operations > Deployment Cycles**.



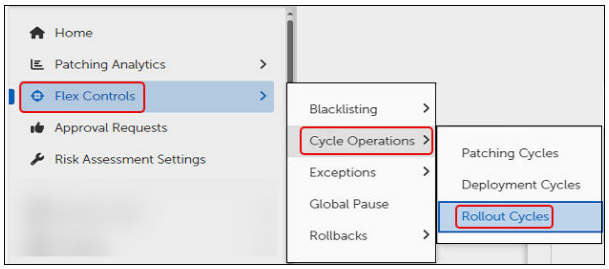
2. Select **History** on the upper left to change to the **History** tab:
   - The **Total Running Deployments** widget displays deployment processes and their corresponding states (Waiting, In Progress, or Paused).
   - The **Running Deployments** widget table lists the completed Deployment Strategies by name.
3. Enter a **Deployment Strategy** name in the search bar above the **Running Patch Processes** table, and then select **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 select **Flex Controls** on the **Home** menu, and then select **Cycle Operations > Rollout Cycles**.



   This opens to the **Running** tab of the **Rollout Cycles** workspace:
   - 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).
   - The **Running Rollout Cycles** table lists the completed patch processes by Rollout name.
2. Enter a **Rollout Cycle** name in the search bar above the **Running Rollout Processes** table, and then select **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 select **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:
   - The **Total Running Deployments** widget displays an aggregate summary of all deployment processes and their corresponding states (Waiting, In Progress, or Paused).
   - The **Running Deployments** widget table lists the completed Deployment Strategies by name.
3. Enter a **Rollout Cycle** name in the search bar above the **Running Rollout Cycles** table, and then select **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 must remain at a specific version of a product, Patching Exceptions provide a mechanism for creating and implementing the rules. Patching Exceptions provides version-level patch support, allowing administrators to exert granular control over patch deployment. For example, use Patching Exceptions to target and completely remove a product from an environment when the product is no longer required.

Patching Exceptions allow teams to define exceptions for specific business units or environments, create multiple exceptions under a single policy, and more. This means you can manage exceptions for several patches or products simultaneously.

Using Patching Exceptions

OneSite Patch includes two Patching Exception options: **Desired State Override** and **Last Allowed Version**. You may choose one option only per Patching Exception. For example, create one exception to use one or more Desired State Overrides, then create another to specify Last Allowed Versions. In either case, you may choose specific Business Units as the targets of the exception.

Desired State Override Options

- **Mandatory Install:** Allows client devices to treat the product as mandatory for installation purposes.
- **Do Not Install:** Allows client devices to block the installation of a particular product.
- **Rollback:** Forces a rollback to a specific product version on a client device, when OneSite Patch detects a later product version than allowed.
- **Uninstall:** Removes the product from client devices in the specified Business Unit.

Last Allowed Version

Specifies a product level to consider current and ignores all later releases. When specified, the **Last Allowed Version** sets the state for all products so that a later version than the one specified does not install.

Create a Patching Exception

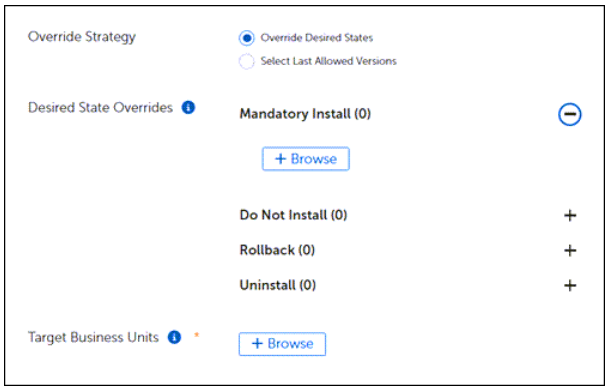
1. Select **Flex Controls** from the **Home** menu, and then select **Exceptions > Patches**.
2. Select **+New** on the upper-right to open a Patching Exception template.
3. Name and describe the exception:
   a. Enter a descriptive Name for this exception in the **Name** field.
   b. Enter a detailed **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:
   - If you choose **Override Desired States**, see Set Override Details for Patch Exception.
   - If you choose **Select Last Allowed Versions**, see Set Last Allowed Patch Versions.

Set Override Details for Patch Exceptions

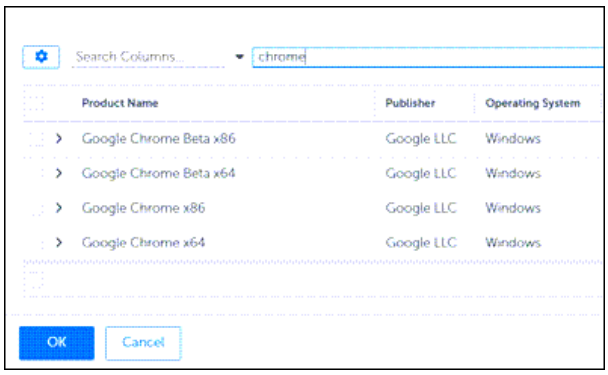
IMPORTANT

Choose only one software version per override exception.

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



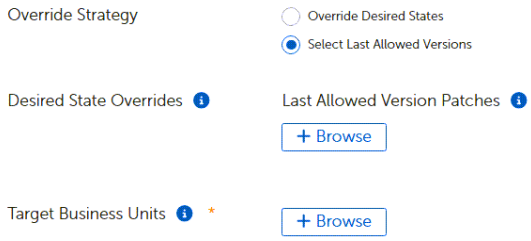
2. Select the + next to your choice for **Desired State Overrides**. The example uses **Mandatory Install**.
3. Select **+Browse** to open the table of available software:
4. a. Enter a product name in the search line, and then select **Search**. This example uses Google Chrome.
   b. Select the product from the list, and then select **OK**.



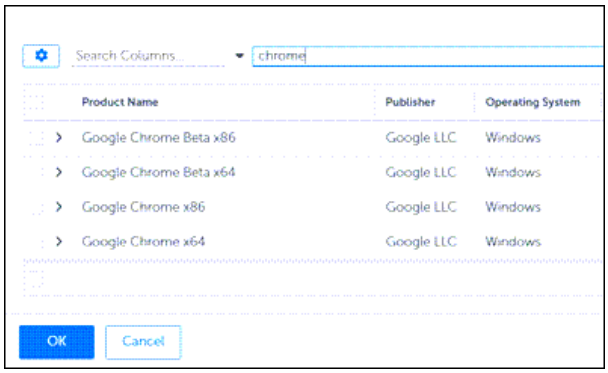
5. Select **Save** on the upper-left of the dialog to save your changes:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** again if you make any changes.
6. Continue to **Add Target Business Units**.

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 **+Browse** to select the **Last Allowed Version Patches**.
   a. Enter a product name in the search line, and then select **Search**. This example uses Google Chrome.
   b. Select the product from the list, and then select **OK**.

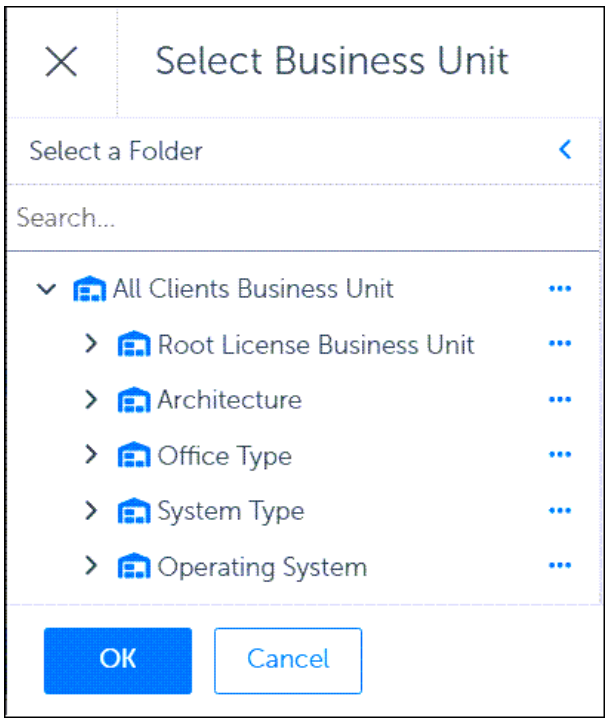


3. Select **Save** on the upper-left corner of the dialog to save your changes:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** again if you make any changes.
4. Continue to **Target Business Units**.

Add Target Business Units for Patch Exceptions

With **Select Last Allowed Versions** as your **Override Strategy** under Patching Exceptions, you may select one or more Business Units to which the patching exception applies. With no Business Units specified, the Patching Exception applies to all endpoints where the specified Patches apply.

1. Select **+Browse** next to **Target Business Units** in an open Patching Exception template.
2. Select one or more **Business Units** to include in the Patching Exception.



3. Select **OK** on the lower-left of the **Select Business Unit** dialog.
4. Select **Save** on the upper-left of the **Patching Exceptions** dialog 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 Adaptiva Server side, and the Adaptiva 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) OneSite Patch 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.

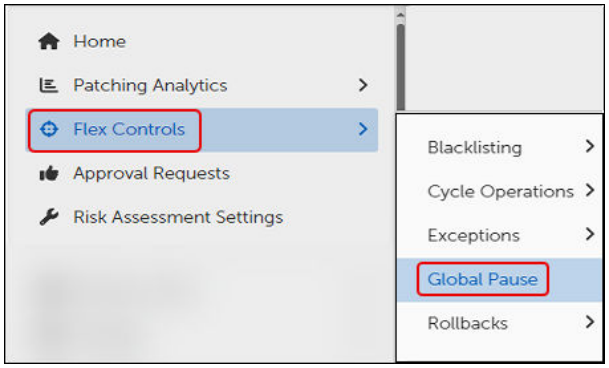
Paused Cycles: Pause Patching, Deployment, or Rollout Cycles either for specified Business Units or for the Business Units already targeted by the Cycle.

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

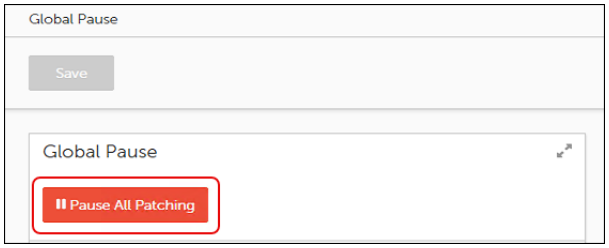
Stop All Patching Activity Immediately

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

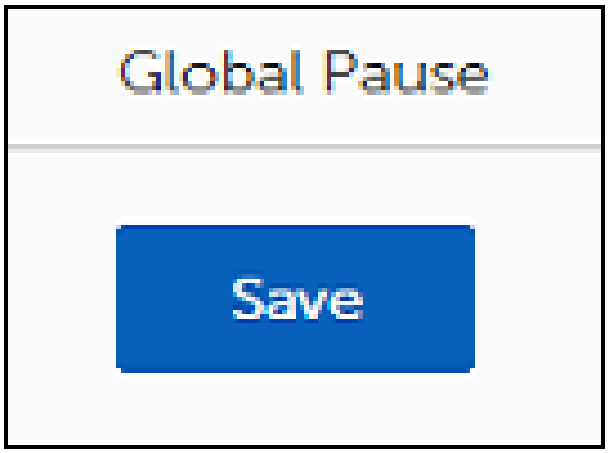
1. Select **Flex Controls** on the Home menu, and then select **Global Pause**.



This opens the **Global Pause** dialog:



2. Select **Pause All Patching**.

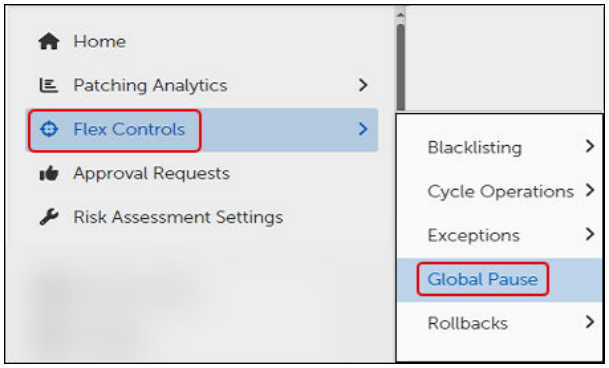


3. Select **Save** to activate Global Pause. This immediately stops all patch deployments across all licensed clients:
   - All patch deployments in progress that have not reached an irreversible state are paused immediately.
   - All newly initiated patch deployments are paused automatically.

Resume All Paused Patching Activity Immediately

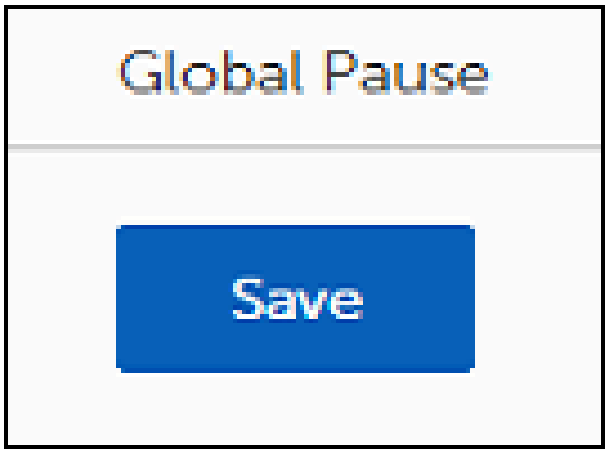
To resume all paused patching activity on all licensed clients, use the following steps to revoke a Global Pause.

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



This opens the **Global Pause** dialog:

2. Select **Resume Patching**.

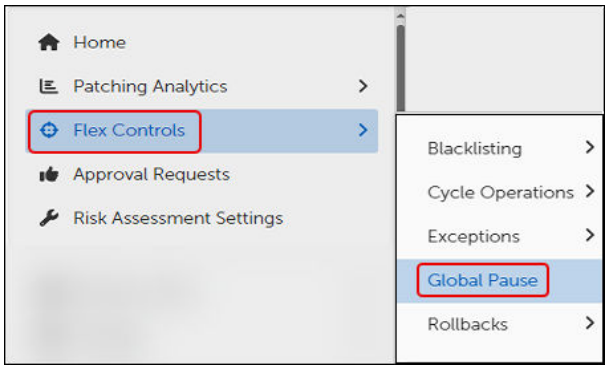


3. Select **Save** to revoke the Global Pause. This immediately revokes the Global Pause and allows patching activity to occur as configured.

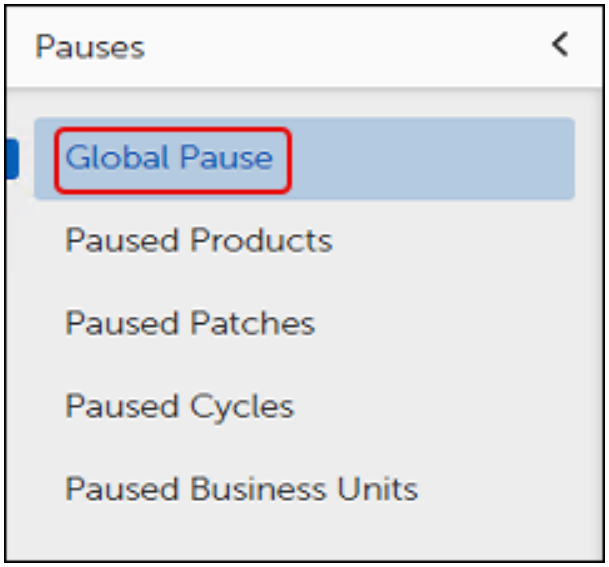
Pause Patching for Specific Objects

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:



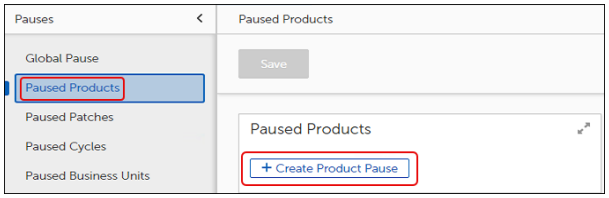
2. Select the pause you want to configure. You can configure multiple types of pauses, but you must configure them separately.
   - **Global Pause**: Pause all patching activity immediately (Stop All Patching Activity Immediately).
   - **Paused Products**: Pause patch deployments for one or more products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

Pause Deployment of a Specific Software Product

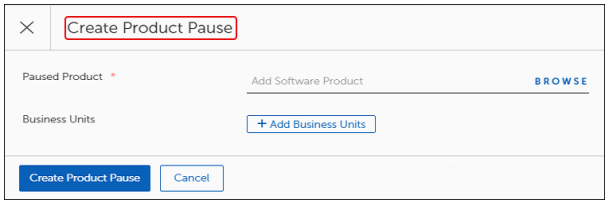
To stop patching activity for specific software products or patches, complete the following steps:

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

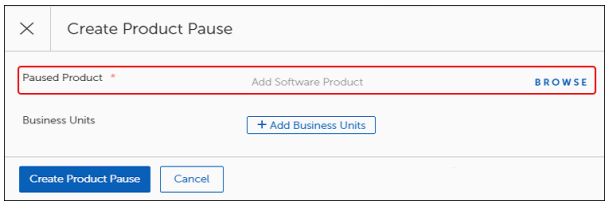
   This opens the Paused Products dialog:



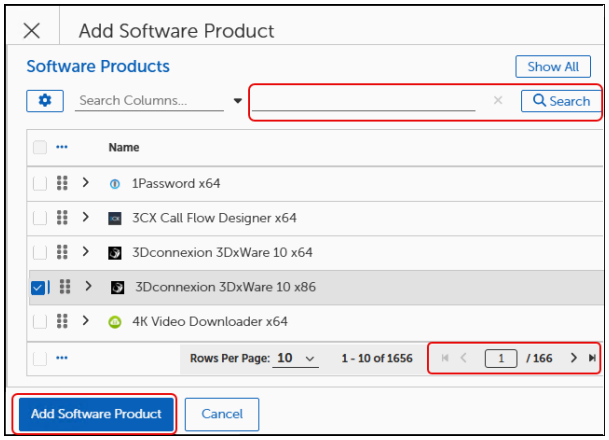
a. Select **+Create Product Pause** to open the **Create Product Pause** dialog:



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:

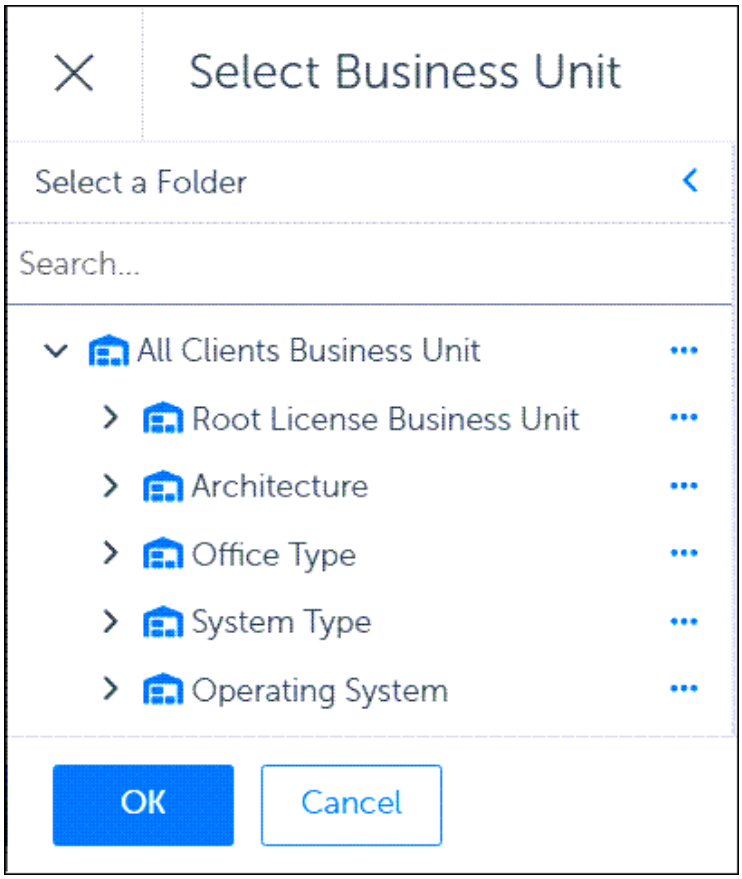


- Use the navigation tools on the bottom right to scroll through the pages and select one or more **Software Products** from the table.
- Enter a product name on the search line, and then select **Search** to find a specific product

2. Select **Add Software Product** to return to the **Create Product Pause** dialog, and then choose one of the following methods to proceed:
   - To create a **Global Pause** for the selected products, select **Create Product Pause**. This pauses the deployment of the selected software product on all devices in the estate.
   - To specify a pause for specific devices, continue with the next step to **Add Business Units**.

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

- To remove existing Business Units, select the **ellipsis (...)** under **Actions**, and then select **Remove Row**.
- To add Business Units, complete the following steps:
  a. Select the Business Units.



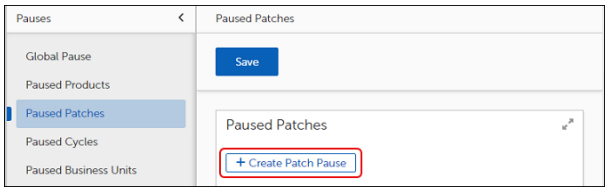
  b. Select **OK**.

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

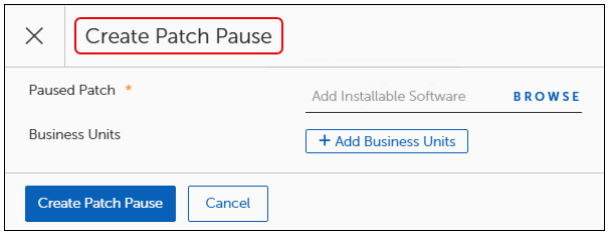
Pause Deployment of a Specific Patch

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

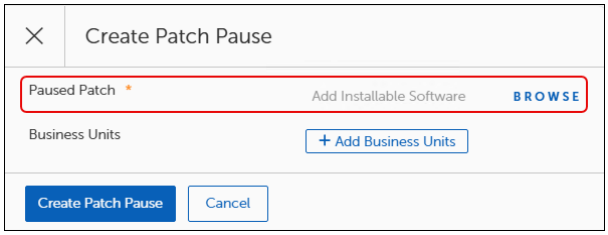
1. Navigate to the Pause menu (see Pause Patching for Specific Objects), and then select **Paused Patches**.
   This opens the Paused Patches dialog:



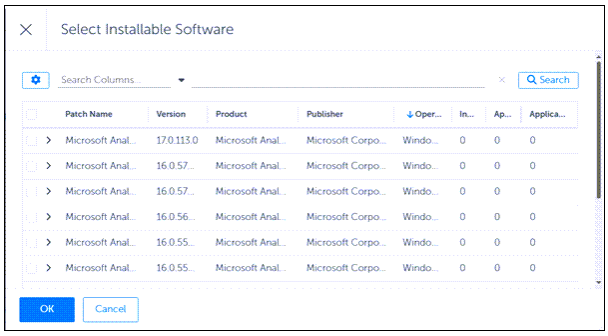
   a. Select **+Create Patch Pause** to open the **Create Product Pause** dialog, and then select **Browse** to find the Software patch you want to pause:



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

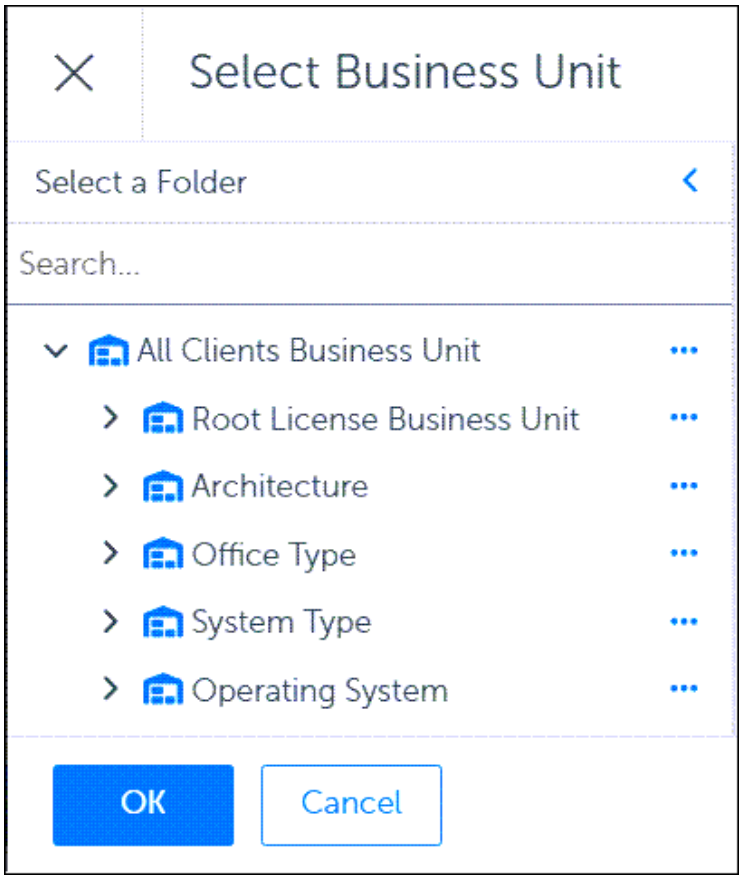


c. Select the patch you want to pause:



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

- To remove existing Business Units, select the **ellipsis (...)** under **Actions**, and then select **Remove Row**.
- To add Business Units, complete the following steps:
  a. Select the Business Units.



  b. Select **OK**.

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

Pause Specific Cycles

OneSite Patch 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

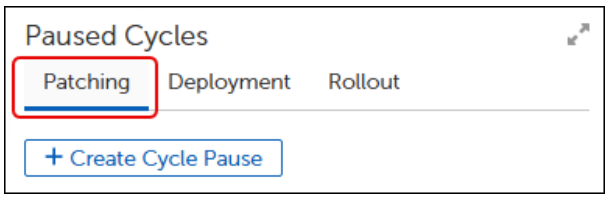
Pausing a cycle that is currently in a WAITING state (has not run yet), prevents that cycle from running until you remove the pause. This is the only server-side behavior related to pausing.

Pause a Patching Cycle

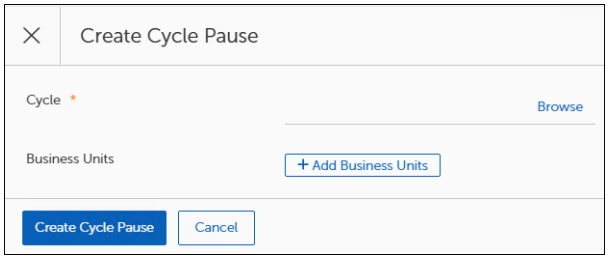
To stop patching activity for a specific patching cycle, complete the following steps:

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:



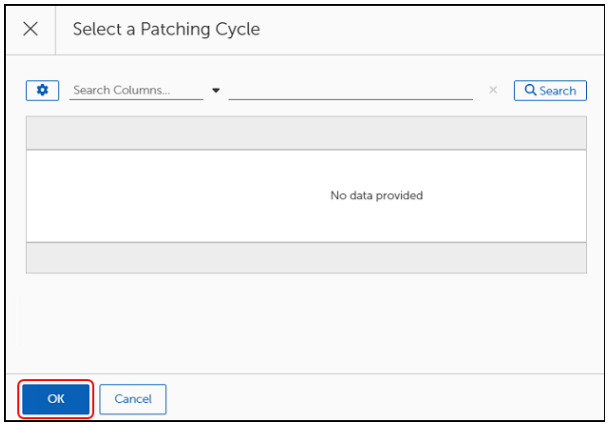
2. Select **+Create Cycle Pause** to open the **Create Cycle Pause** dialog, and then select **Browse**.



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

IMPORTANT

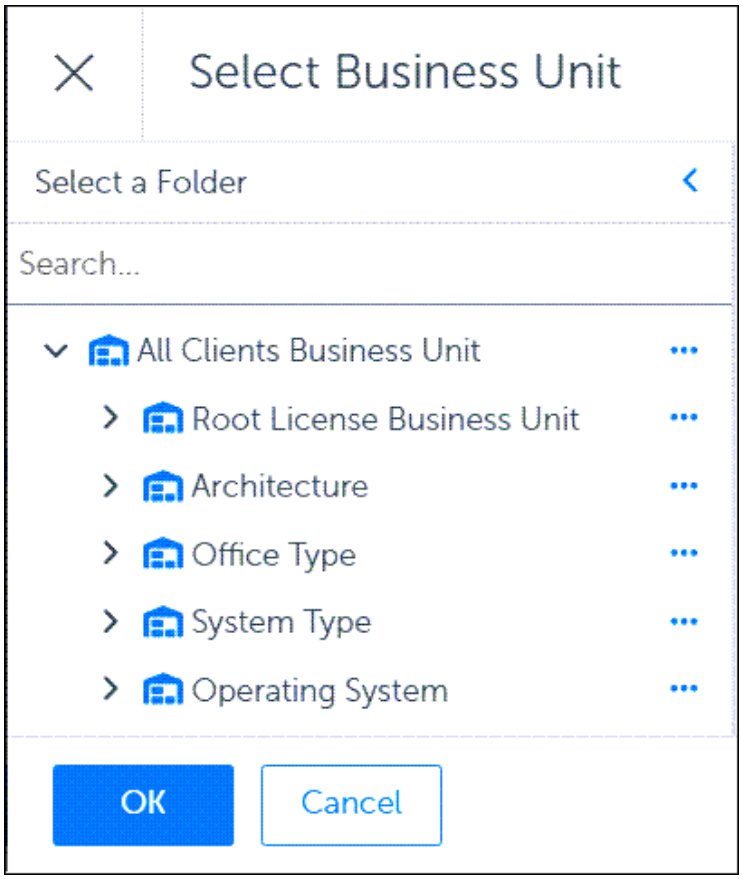
Cycles do not appear unless you have created them previously. If you do not have a cycle to stop, do not complete this section.



- Use the navigation tools on the bottom right to scroll through the pages to find and select a Patching Cycle from the table.
- Enter a cycle name in the search line, select **Search** to find, and then select a specific cycle.

4. Select **OK**, and then choose one of the following options to proceed:
   - 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.
   - To specify a pause for specific devices, continue with the next step to **Add Business Units**.
5. Add or remove **Business Units:**

- To remove existing Business Units, select the **ellipsis (...)** under **Actions**, and then select **Remove Row**.
- To add Business Units, complete the following steps:
  a. Select the Business Units.



  b. Select **OK**.

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

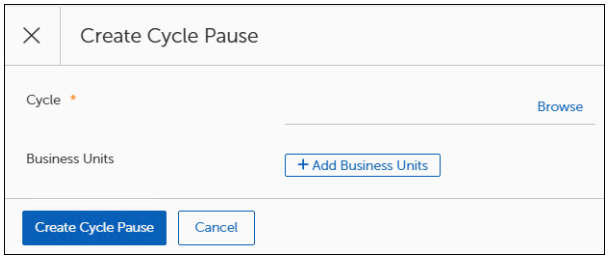
Pause a Deployment Cycle

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**.

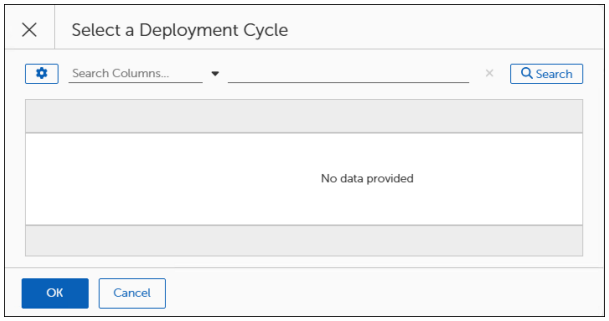
   This opens the **Paused Cycles** dialog to the **Deployment** tab:

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 choose 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.

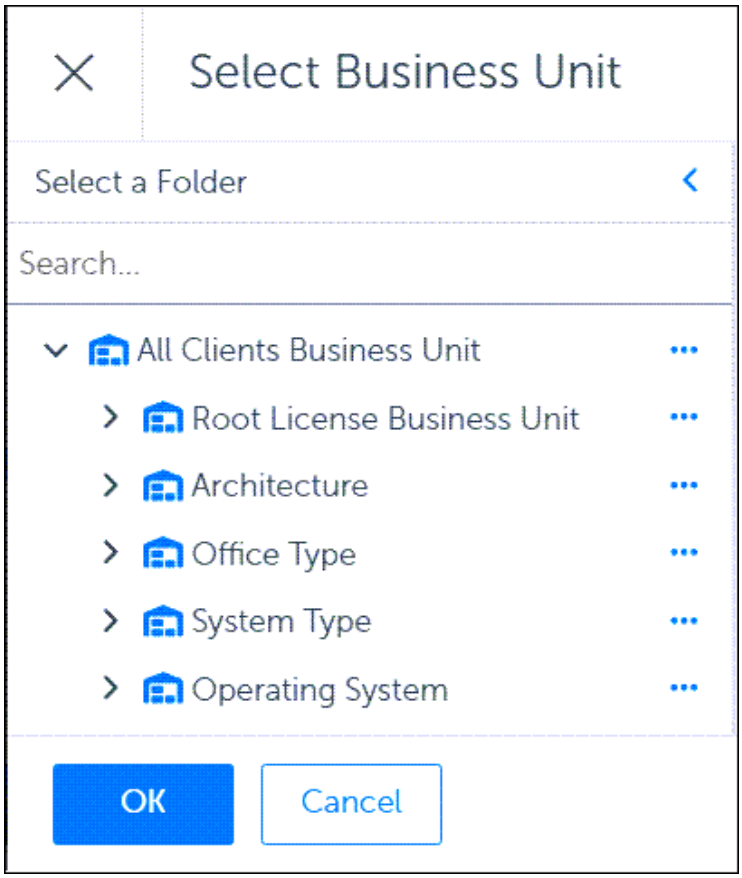


- Use the navigation tools on the lower-right to scroll through the pages to find and select a cycle from the table.
- Enter a cycle name in the search line, select **Search** to find, and then select a specific cycle

4. Select **OK** to save your entry, and then choose one of the following options to proceed:
   - 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.
   - To specify a pause for specific devices, continue with the next step to **Add Business Units**.

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

- To remove existing Business Units, select the **ellipsis (...)** under **Actions**, and then select **Remove Row**.
- To add Business Units, complete the following steps:
  a. Select the Business Units.



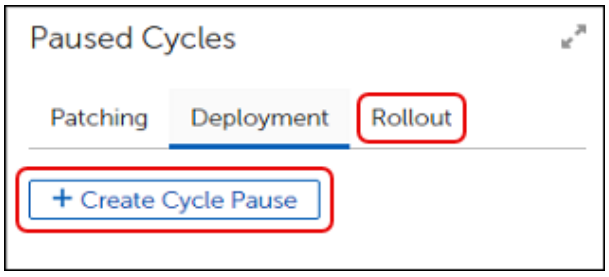
  b. Select **OK**.

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

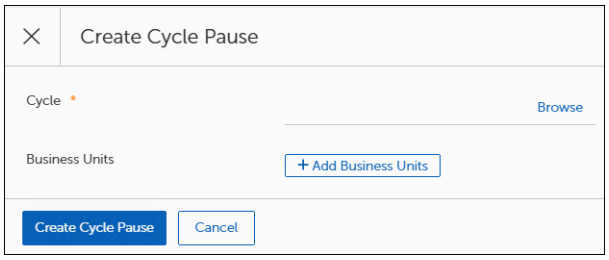
Pause a Rollout Cycle

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:

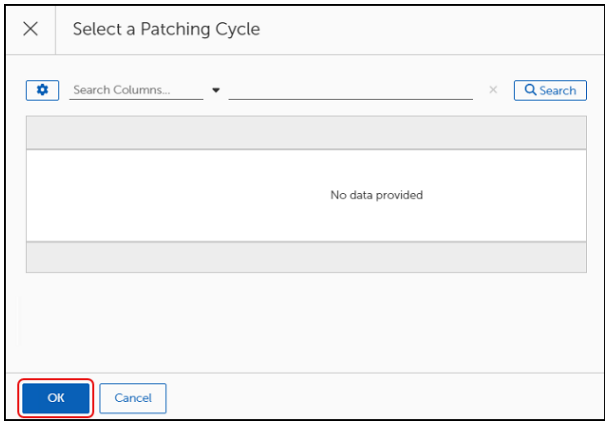


2. Select **+Create Cycle Pause**. This opens the **Create Cycle Pause** dialog:



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

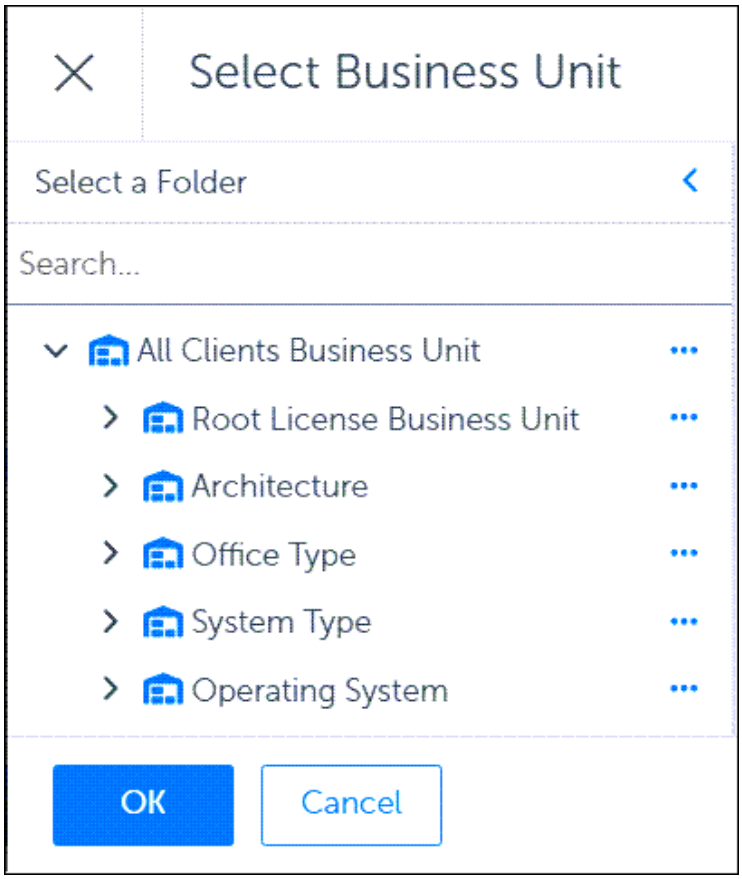
> **IMPORTANT**
> Cycles do not appear unless you have created them previously. If you do not have a cycle to stop, do not complete this section.



- Use the navigation tools on the lower-right to scroll through the pages to find and select a **Rollout Cycle** from the table.
- Enter a cycle name on the search line, and then select **Search** to find and select a specific cycle.

4. Select **OK** , and then choose one of the following options to proceed:
   - 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.
   - To specify a pause for specific devices, continue with the next step to **Add Business Units**.
5. Add or remove **Business Units:**

- To remove existing Business Units, select the **ellipsis (...)** under **Actions**, and then select **Remove Row**.
- To add Business Units, complete the following steps:
  a. Select the Business Units.



  b. Select **OK**.

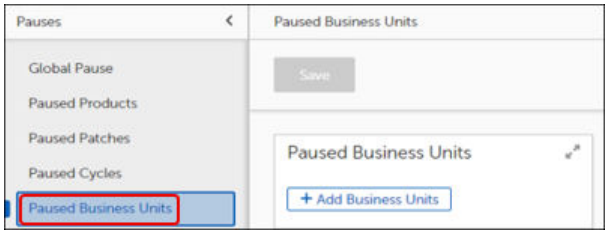
6. Select **Create Cycle Pause**, and then select **Save** to create a pause for the selected rollout cycle.

Pause Deployment to a Business Unit

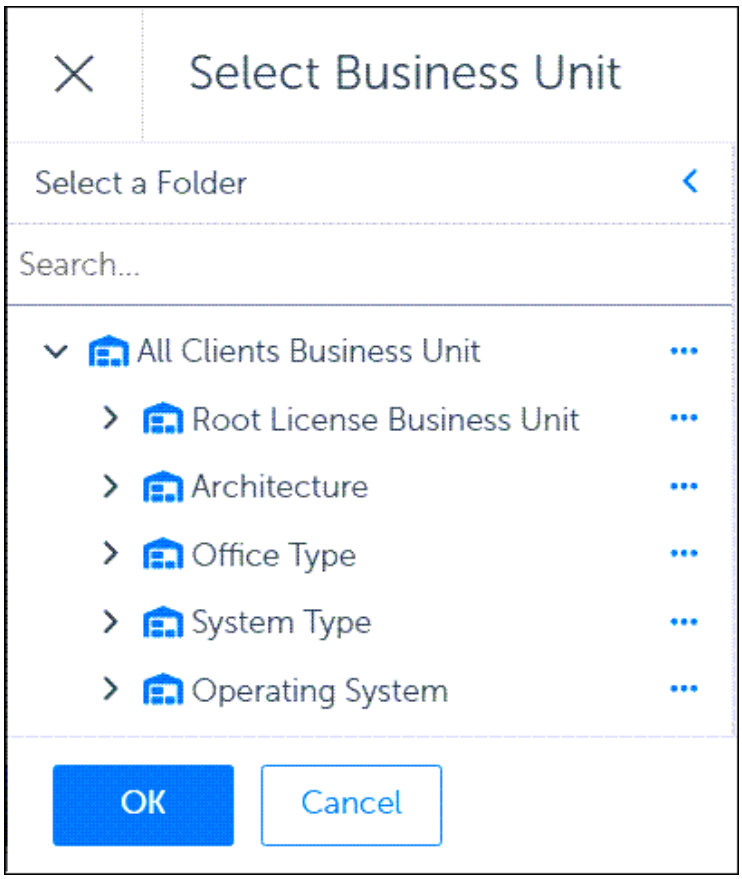
To stop patching deployment for specific business units, complete the following steps:

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:**
   - To remove existing Business Units, select the **ellipsis (...)** under **Actions**, and then select **Remove Row**.
   - To add Business Units, complete the following steps:
     a. Select the Business Units.



     b. Select **OK**.

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

Rollbacks Overview

The Rollbacks feature of OneSite Patch 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.

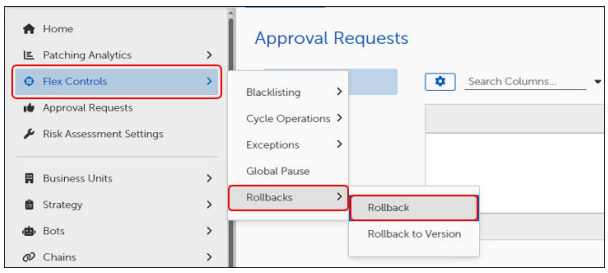
Rollback

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.

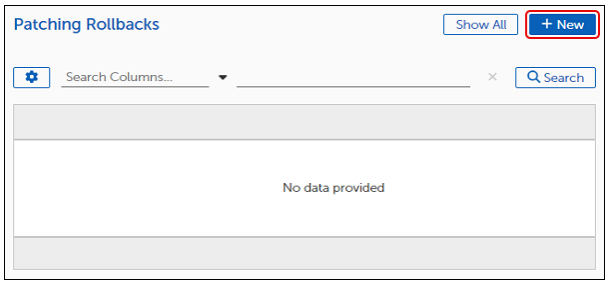
Create a Rollback

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 Patch Dashboard, and then select **Rollbacks > Rollback**.

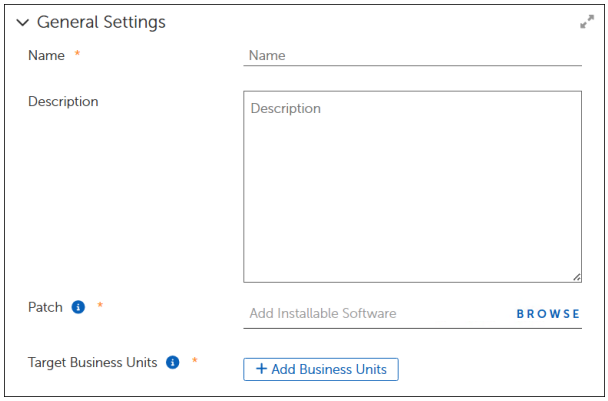


This opens the **Patching Rollbacks** table. Until you create a rollback, the table is empty.



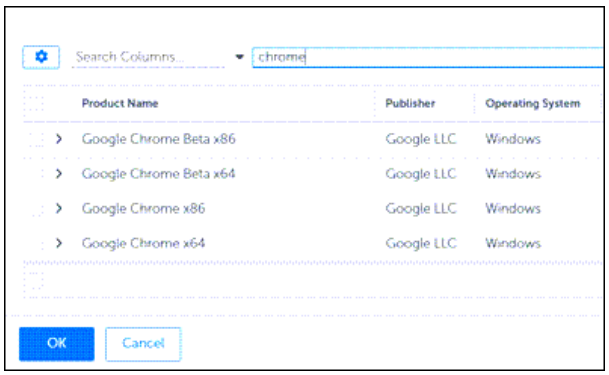
2. Select **+New** to open the Rollback template, and then enter a **Name** and a detailed **Description** of the rollback.

> **NOTICE**
> A red asterisk next to a field name indicates a required field.

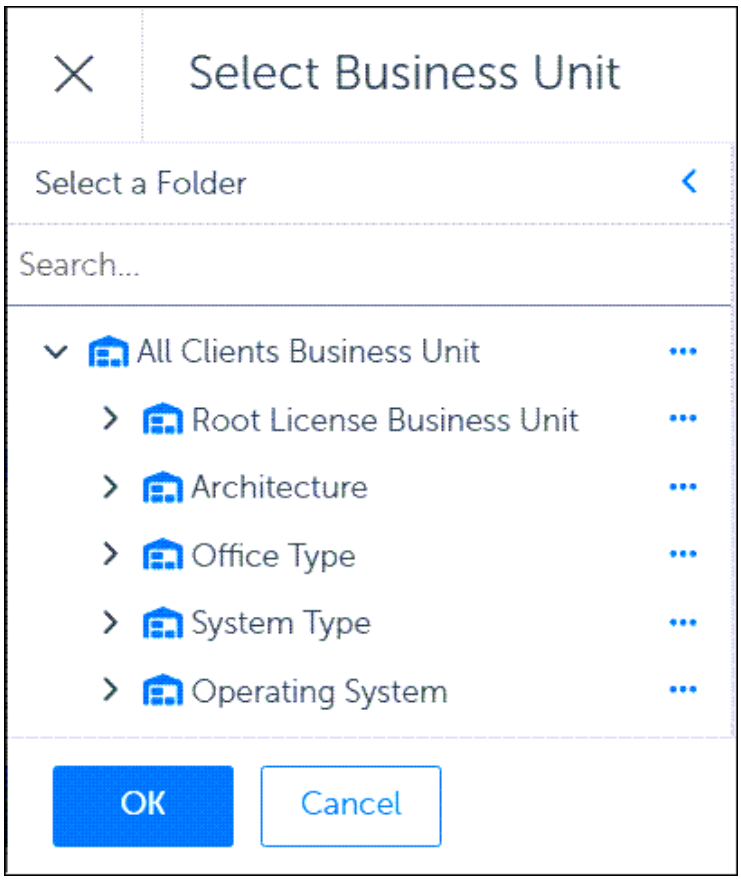


3. Locate the patch or release you want to roll back:

4. Select a Software patch or release:
   a. Enter a product name in the search line, and then select **Search**. This example uses Google Chrome.
   b. Select the product from the list, and then select **OK**.



5. Add one or more Business Units to specify the devices to rollback.
   a. Select the Business Units.

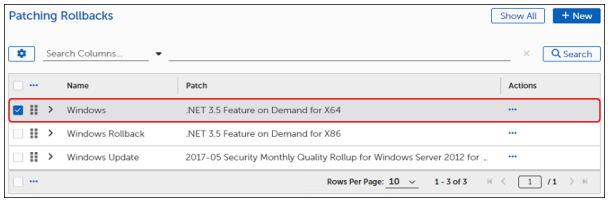


   b. Select **OK**.

6. Select **Save** to save the Rollback configuration. This returns you to the **Patching Rollbacks** table, which lists your new rollback.

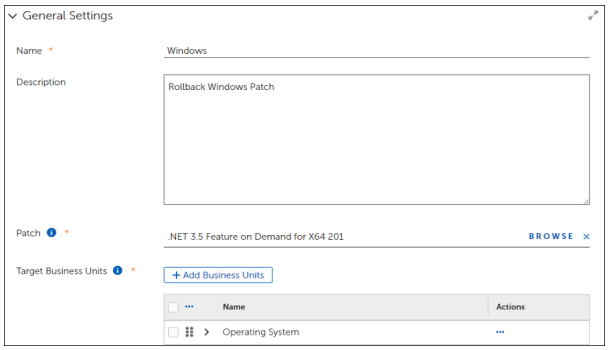
Edit a Rollback Template

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



This opens the template.

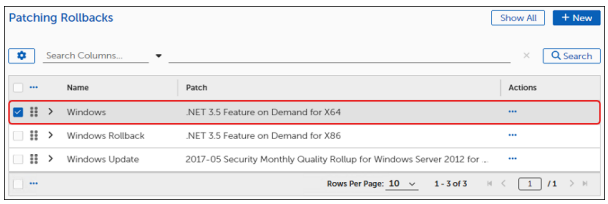
> **NOTE**
> A red asterisk next to a field name indicates a required field.



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 of the template to save the new settings.

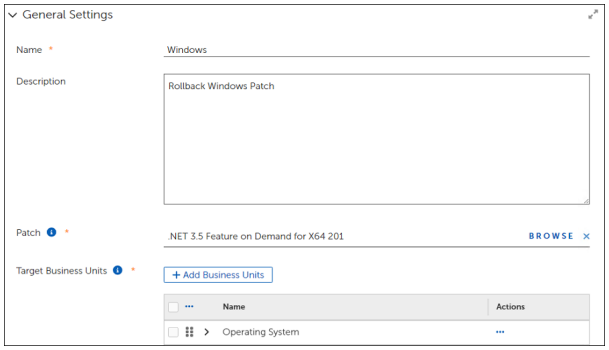
Copy a Rollback

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

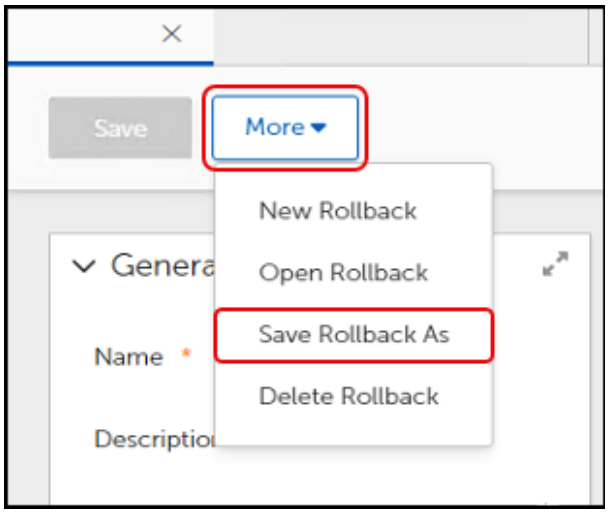


This opens the template.

> **NOTE**
> A red asterisk next to a field name indicates a required field.



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

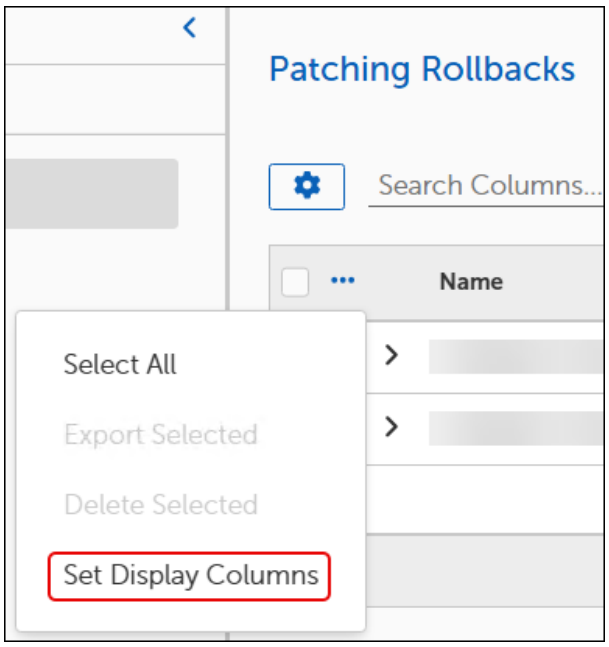


3. Enter a new **Name** for the template, and then select **Save as**.

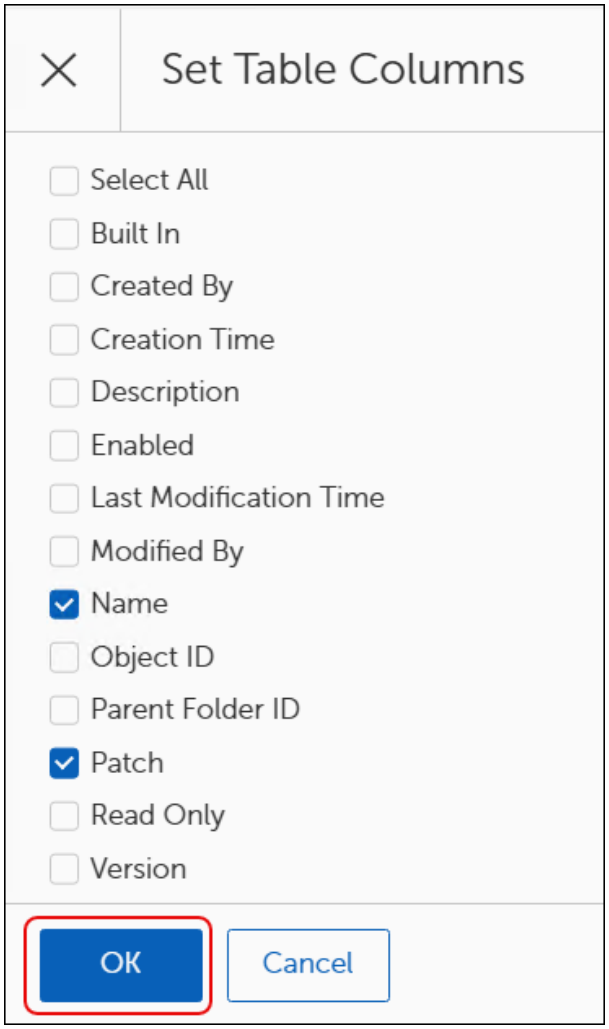
4. Revise the **Description** to reflect any changes needed for the copy, and then select **Save**.
5. Select **Back to Rollbacks** on the upper-left of the template to return to the **Rollbacks** table and view your changes.

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 select **Set Display Columns**.



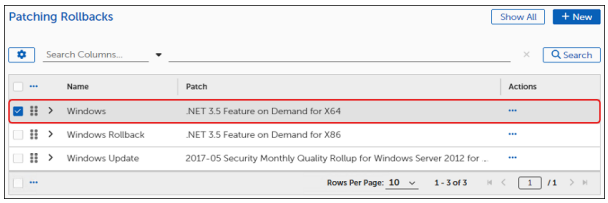
This opens the **Set Table Columns** dialog.



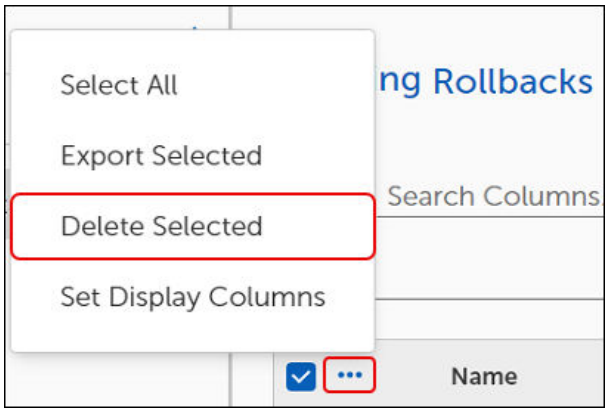
3. Select the **column names** you want the **Patching Rollbacks** table to display, and then select **OK**.

Delete a Rollback

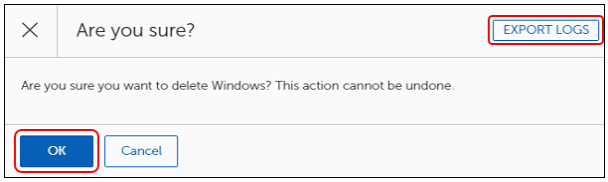
1. Select a **Rollback** template from the **Patching Rollbacks** table of an open Patching Rollbacks template.



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



3. Review the **Are you sure?** dialog:



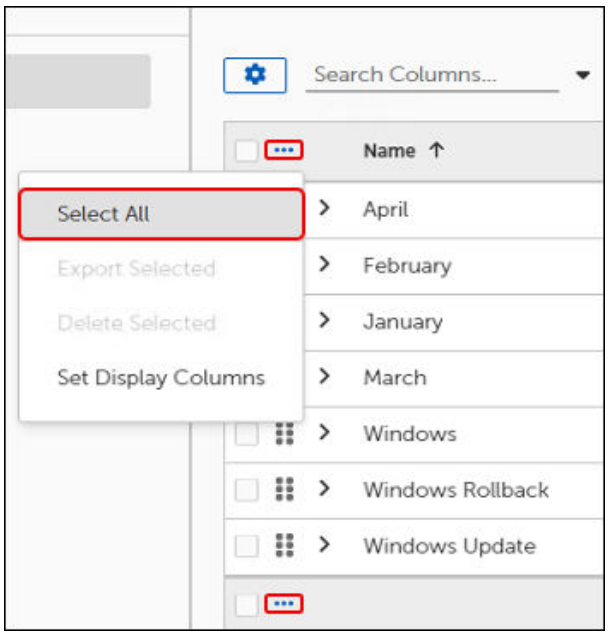
   a. Select **Export Logs** on the upper-right of the **Are you sure?** dialog to export trace logs. The trace logs download to your device as a file with a `.log` extension.

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

4. Select **Back to Rollbacks** on the upper-left of the template to return to the **Rollbacks** table and view your changes.

Select All Rollbacks

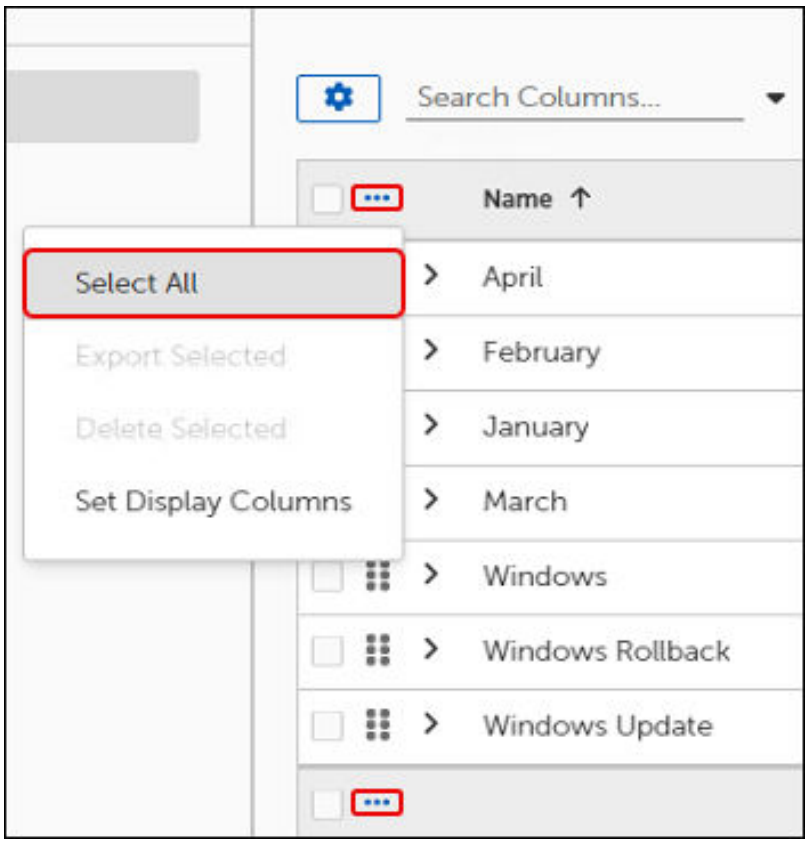
1. Open the **Patching Rollbacks** table (**Flex Controls > Rollbacks > Rollback**).
2. Select the **ellipsis (...)** next to **Name**, and then select **Select All**.



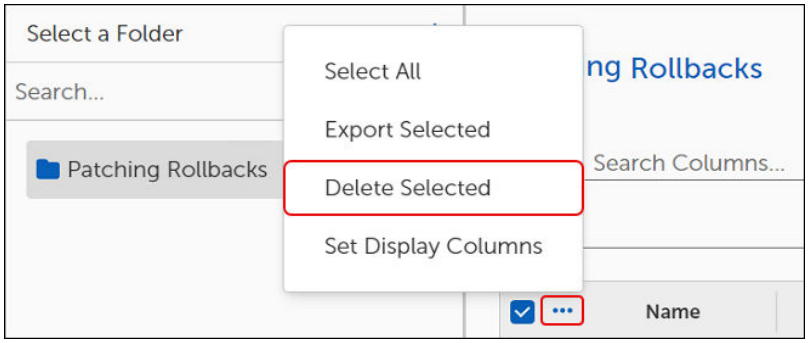
3. Select the ellipsis (...) again, and then choose what you want to do with the selected Rollbacks:
   - To export the selected Rollbacks, see Select All Rollback to Version Objects.
   - To delete the selected templates, see Bulk Delete Rollbacks.
   - To customize the display columns of the **Patching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

Bulk Delete Rollbacks

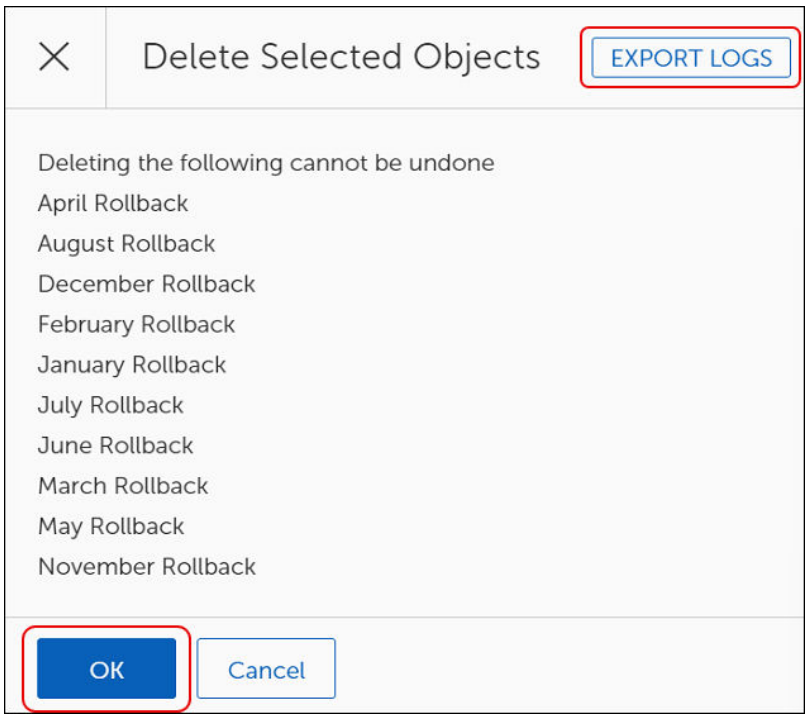
1. Open the **Patching Rollbacks** table (**Flex Controls > Rollbacks > Rollback**).
2. Select the **ellipsis (...)** next to **Name**, and then select **Select All**.



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



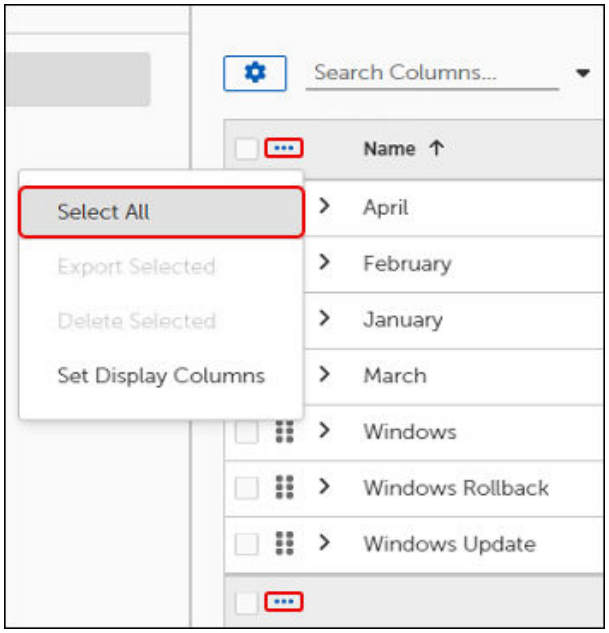
This opens the **Delete Selected Objects** dialog:



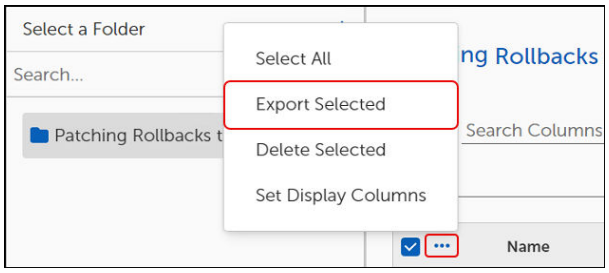
4. (Optional) Select **Export Logs** on the top-right corner of the **Delete Selected Objects** dialog to export trace logs. The trace logs download to your device as a file with a `.log` extension.
5. Select **OK** to delete the Rollbacks. This returns you to the **Patching Rollbacks** table where the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

Export Rollbacks

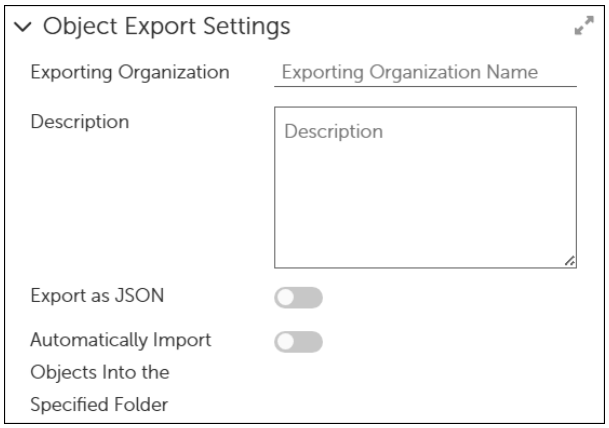
1. Open the **Patching Rollbacks** table (**Flex Controls > Rollbacks > Rollback**).
2. Select a single **Patching Rollback** from the table, or select the **ellipsis (...)** next to **Name**, and then select **Select All** to export all Rollbacks



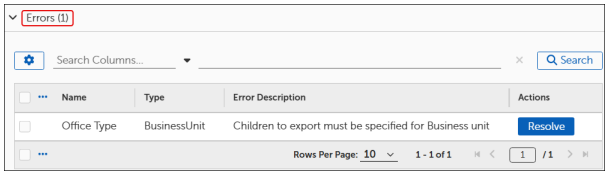
3. Select the **ellipsis (...)** next to **Name** again, and then select **Export Selected**.



This opens the **Object Export Settings**:



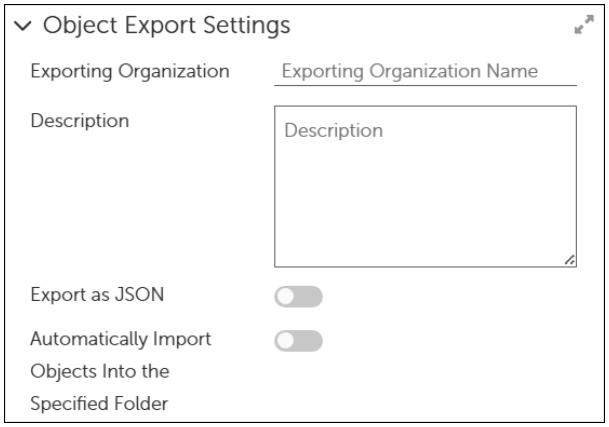
If the **Object Export Settings** command returns an error similar to the following, see Resolve Export Errors errors:



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.



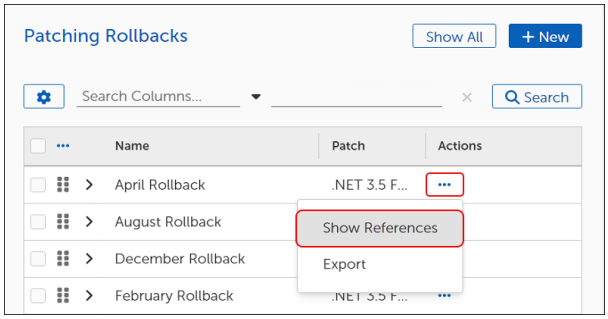
2. Enter an **Exporting Organization Name** and a **Description** of the settings you intend to create.
3. Toggle the **Export as JSON** switch to enable or disable (default) whether to export the settings as a JSON file.
4. Toggle the **Automatically Import ...** switch to enable or disable whether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

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

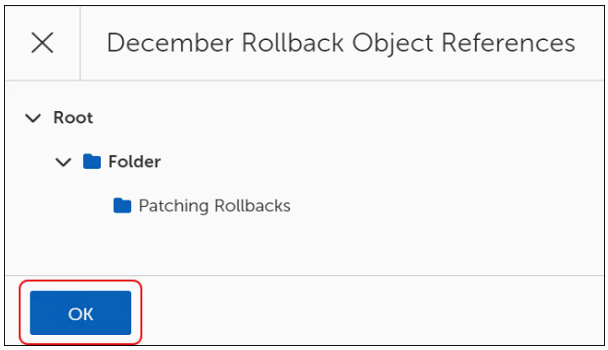
Show Rollback References

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.

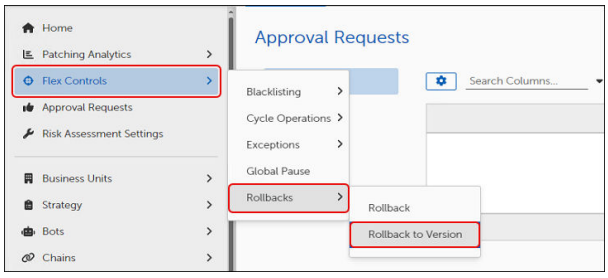
Rollback to Version

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.

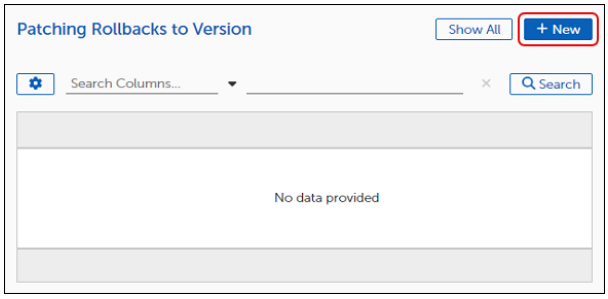
Create a Rollback to Version

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 Patch Dashboard, and then select **Rollbacks > Rollback to Version**.

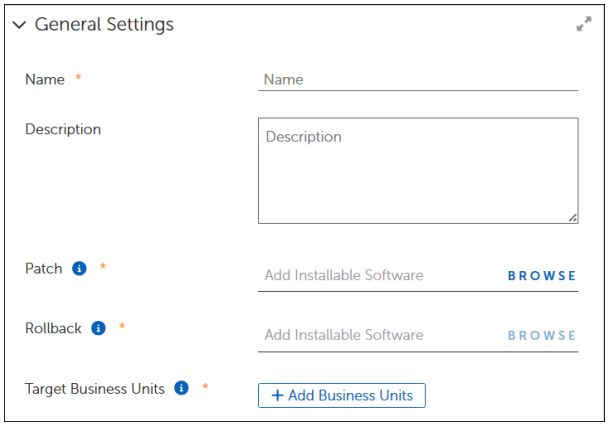


This opens the **Patching Rollbacks to Version** table. Until you create a rollback, the table is empty.



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

> **NOTICE**
> A red asterisk next to a field name indicates a required field.

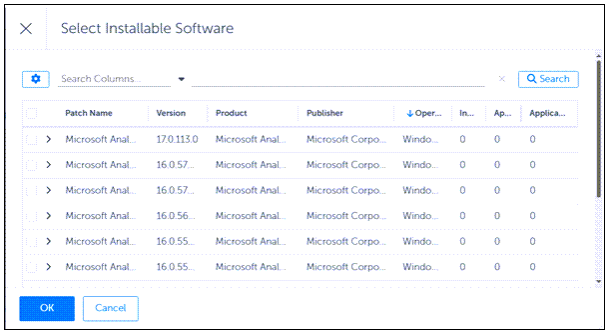


3. Enter a **Name** and a detailed **Description** of your Rollback to Version.
4. Add the patch or release to roll back from.

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.

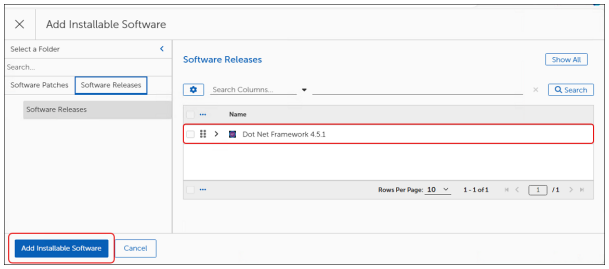


3. Select **Add Installable Software** to return to the Rollback to Version template.
4. Choose the software patch or release version to roll back to.

Choose the Software Patch or Release Version to Roll Back To

1. Select **Browse** next to **Rollback** in an open Rollback to Version template.

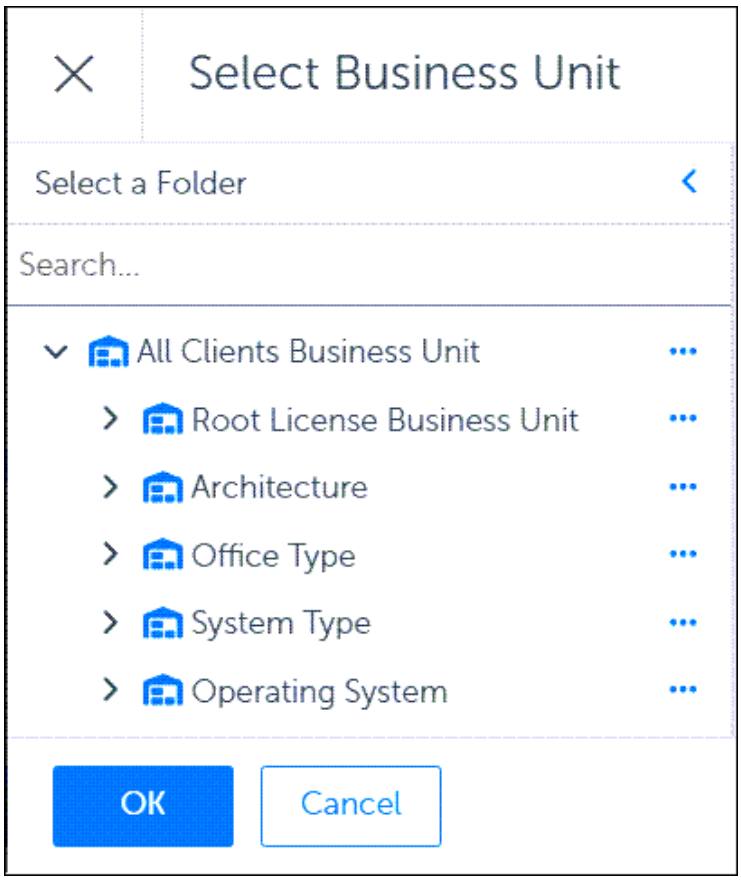
2. Select a **Patch** or **Release** version from the **Add Installable Software** table to roll back to. The only visible versions are those that match the item you selected for Patch. You can select only one Patch or Release to roll back to.



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 the Business Units.

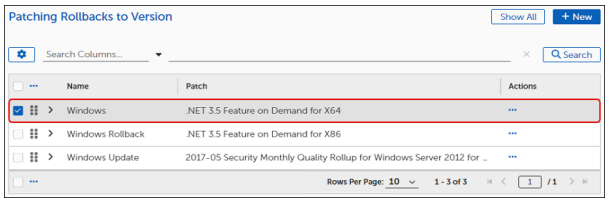


b. Select **OK**.

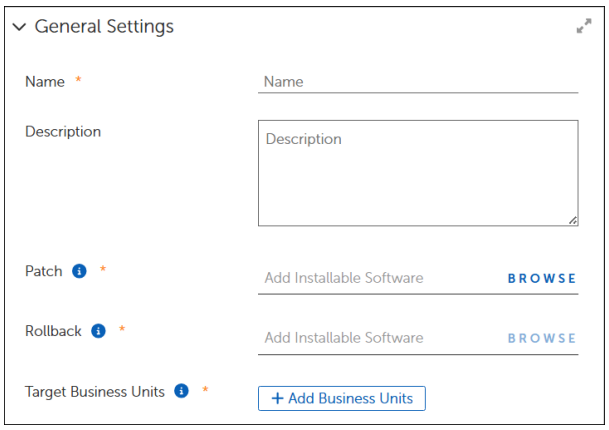
2. Select **Save** to rollback a patch to a prior version.

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.



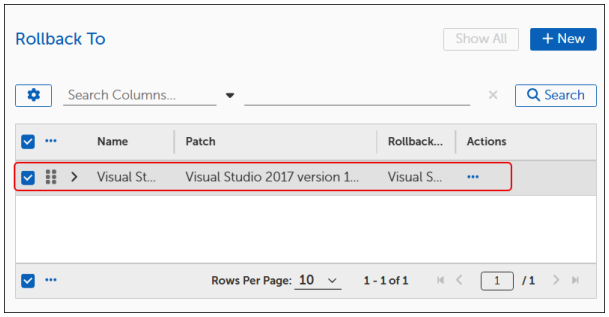
This opens the template.



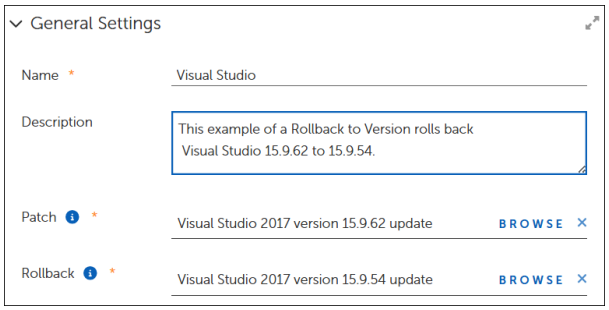
2. Modify the Rollback settings:
   a. Select **Browse** for Patch to choose a patch or release to roll back from.
   b. Select **Browse** for Rollback to choose the version of the patch or release to roll back to.
   c. Select **+Add Business Units** to add or remove target devices.
3. Select **Save**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

Copy a Rollback to Version Template

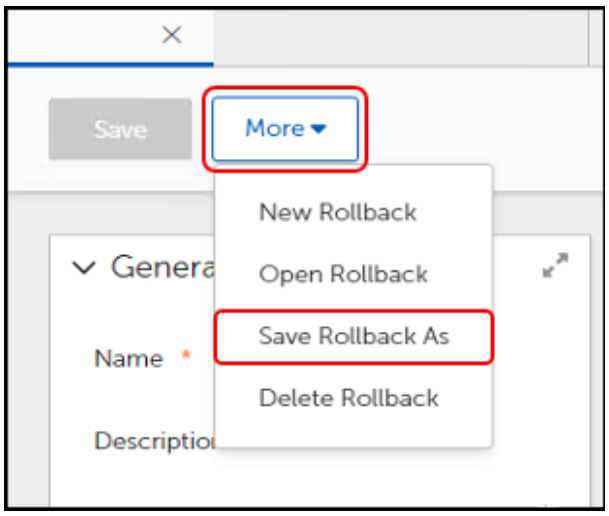
1. Select a **Rollback** template from the **Patching Rollbacks to Version** table of an open Patching Rollbacks template.



   This opens the template.



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

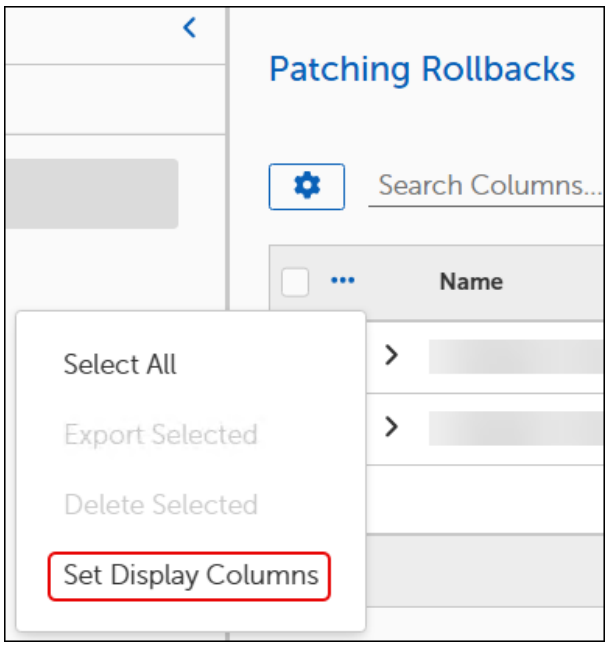


3. Enter a new **Name** for the template, and then select **Save as**.

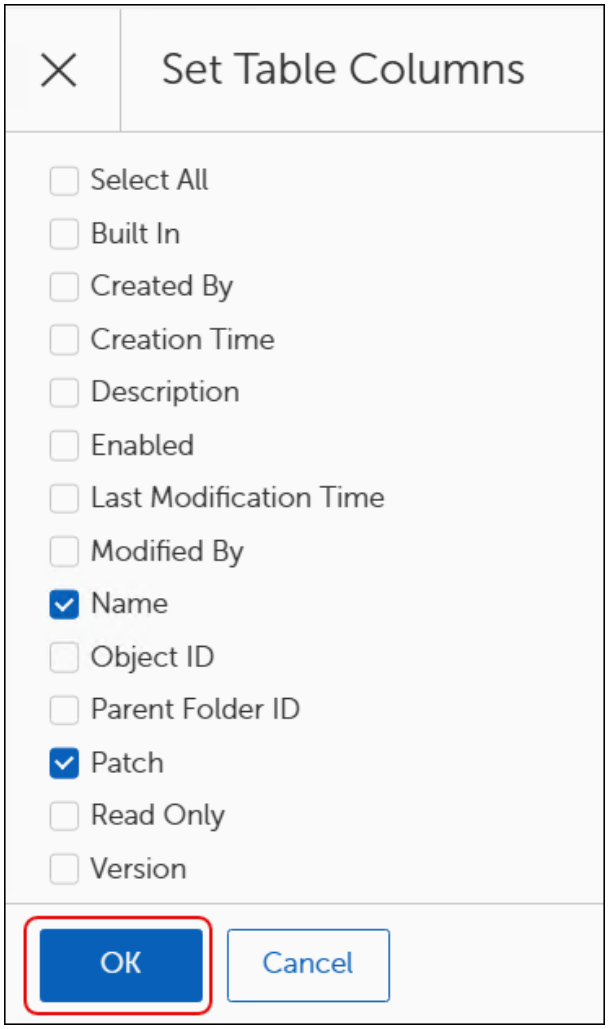
4. Revise the **Description** to reflect any changes needed for the copy, and then select **Save**.
5. Select **Back to Rollbacks** on the upper-left of the template to return to the **Rollbacks** table and view your changes.

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 select **Set Display Columns**.



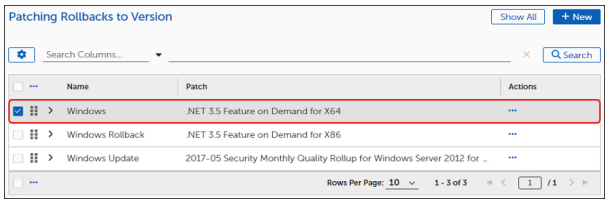
This opens the **Set Table Columns** dialog.



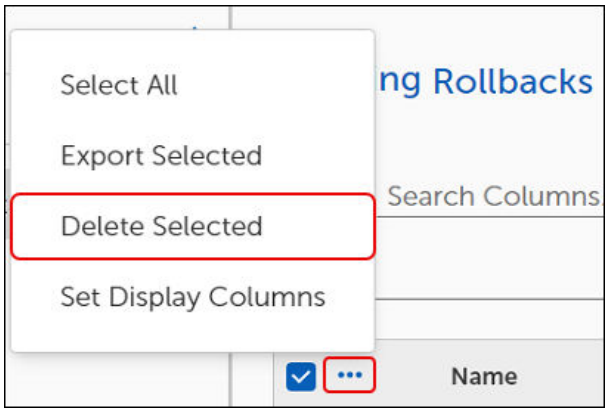
3. Select the **column names** you want the **Patching Rollbacks** table to display, and then select **OK**.

Delete a Rollback to Version

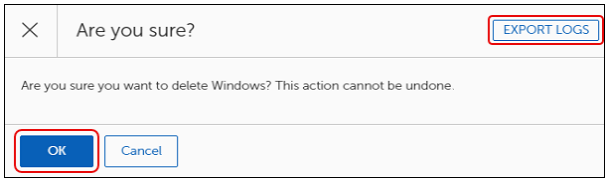
1. Select a **Rollback to Version** template from the **Patching Rollbacks to Version** table of an open Patching Rollbacks template.



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



3. Review the **Are you sure?** dialog:



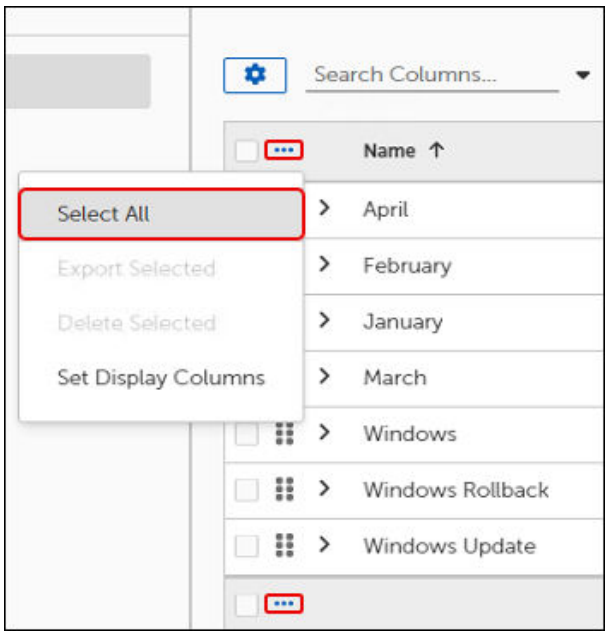
   a. Select **Export Logs** on the upper-right of the **Are you sure?** dialog to export trace logs. The trace logs download to your device as a file with a `.log` extension.

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

4. Select **Back to Rollbacks** on the upper-left 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 select **Select All**.

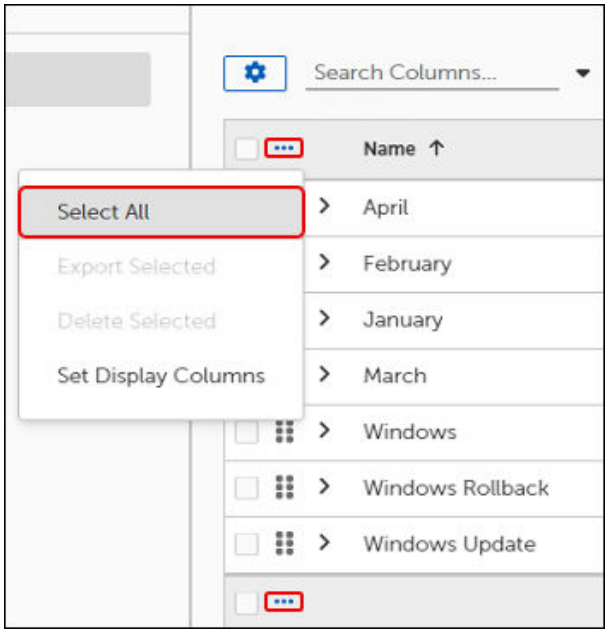


3. Select the ellipsis (...) again, and then choose what you want to do with the selected Rollbacks:
   - To export the selected Rollbacks, see Select All Rollback to Version Objects.
   - To delete the selected templates, see Bulk Delete Rollbacks.
   - To customize the display columns of the **Patching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

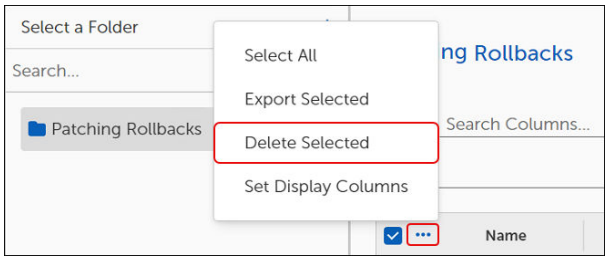
Bulk Delete Rollback to Version

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

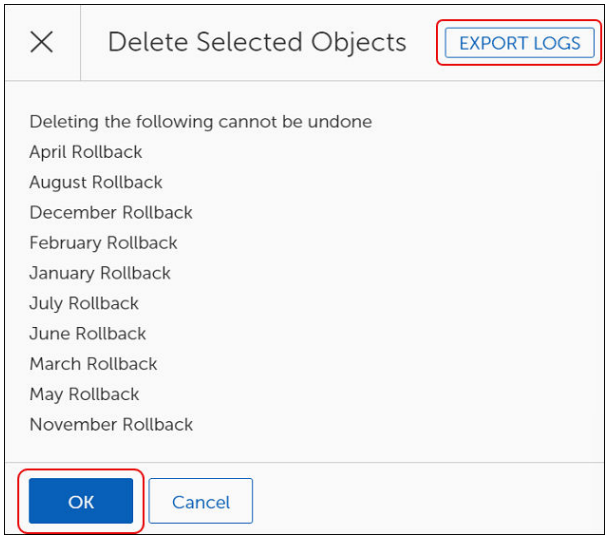
1. Open the **Patching Rollbacks** table (**Flex Controls > Rollbacks > Rollback to Version**).
2. Select the **ellipsis (...)** next to **Name**, and then select **Select All**.



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



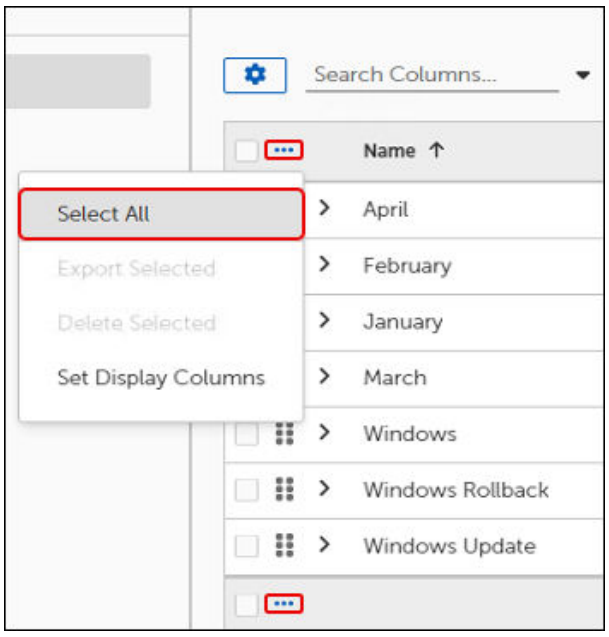
This opens the **Delete Selected Objects** dialog:



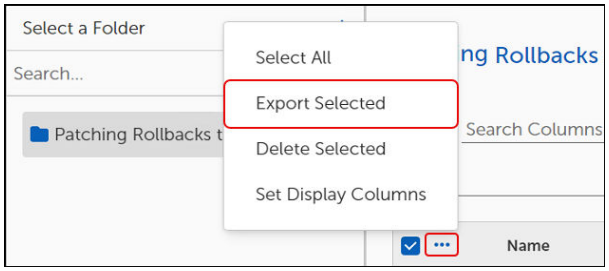
4. (Optional) Select **Export Logs** on the top-right corner of the **Delete Selected Objects** dialog to export trace logs. The trace logs download to your device as a file with a `.log` extension.
5. Select **OK** to delete the Rollbacks. This returns you to the **Patching Rollbacks to Version** table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

Export Rollback to Version

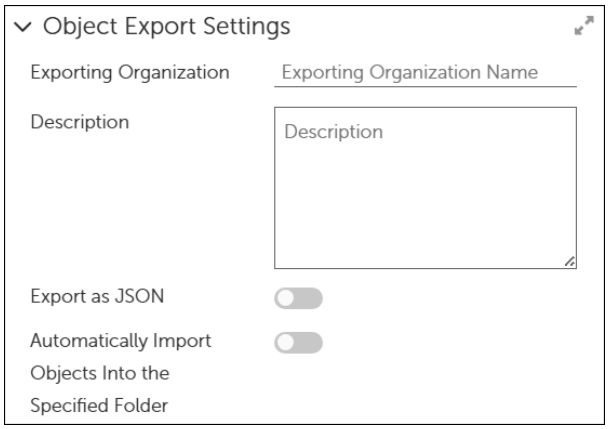
1. Open the **Patching Rollbacks** table (**Flex Controls > Rollbacks > Rollback to Version**).
2. Select a single **Patching Rollback** from the table, or select the **ellipsis (...)** next to **Name**, and then select **Select All** to export all Rollbacks



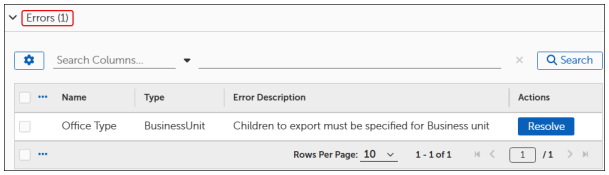
3. Select the **ellipsis (...)** next to **Name** again, and then select **Export Selected**.



This opens the **Object Export Settings**:



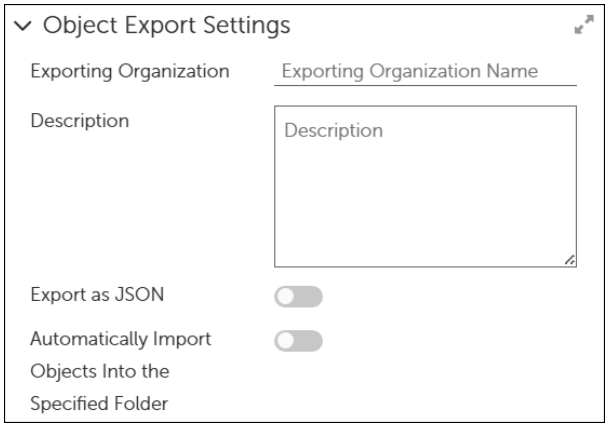
If the **Object Export Settings** command returns an error similar to the following, see Resolve Export Errors errors:



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.



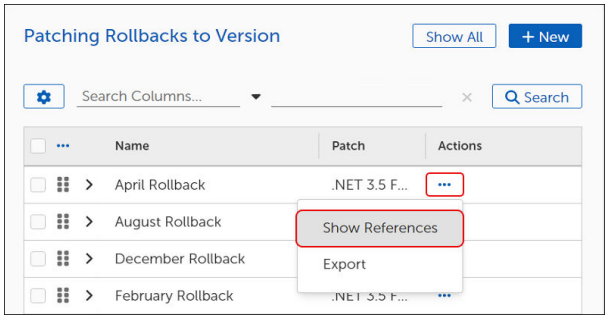
2. Enter an **Exporting Organization Name** and a **Description** of the settings you intend to create.
3. Toggle the **Export as JSON** switch to enable or disable (default) whether to export the settings as a JSON file.
4. Toggle the **Automatically Import ...** switch to enable or disable whether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

> **IMPORTANT**
>
> Adaptiva no longer supports the **Export to Linked Servers** functionality. Do not modify the default settings.

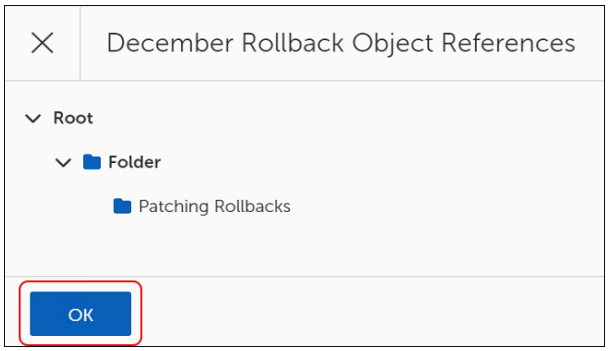
Show Rollback to Version References

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 a notification based on the communication process configured for each approver.

These approval communications include a link that directs the approver to the Admin Portal, prompting them to authenticate.

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

Approve or Reject a Patch Request

1. Select **Approval Requests** from the left navigation menu of the Patch dashboard, and then review All, Pending, or Completed approval requests.
   - The **All** view is read-only. You may view the Approval details, but you may not make any changes.
   - **Pending** lists the process awaiting approval. You may view and change processes with a status of pending. The Approval Request details for processes await approval in this list.
   - The **Completed** view is read-only. You may view the Approval Request details, but you may not make any changes.
2. Select the **ellipsis ...** in the **Action** column to view details of a specific request:

- Select **Approve** to approve a pending request.
- Select **Reject** to reject a pending request.
- Select **View** to view additional details about any request. For completed requests, View is your only option.

Risk Assessment Settings

Use the **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**.

- Exposure Level Weight:
  - Low = 0
  - Medium = 33
  - High = 66
  - Critical = 100
- Exploit Exists Weight
  - False = 0 (exploit does not exist)
  - True = 100 (exploit exists)
- Product Criticality Rating Weight

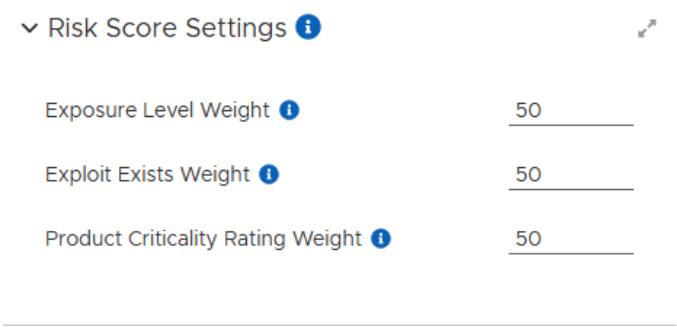
Use the default setting or set custom criticality by product. See Custom Risk Settings.

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.

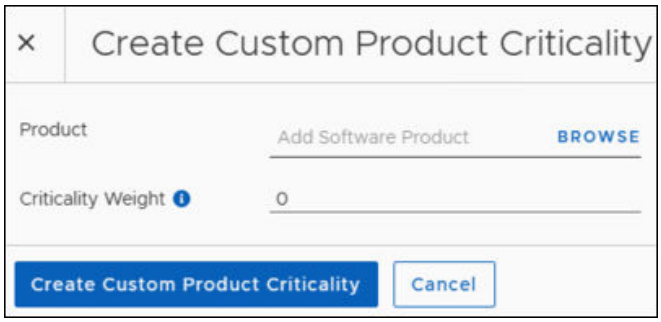


Custom Risk Settings

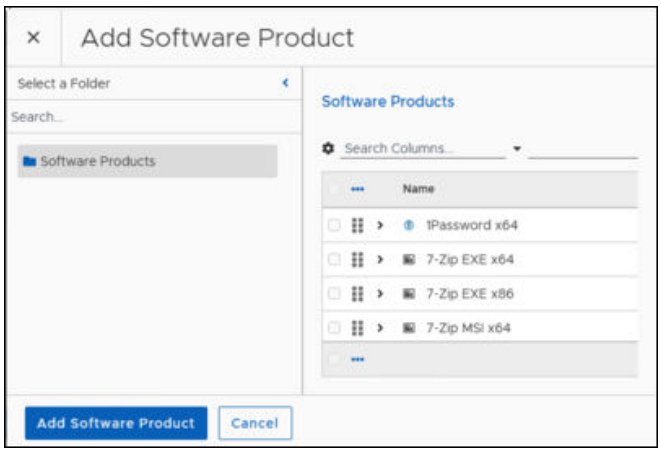
Use these settings to create settings that override the default settings defined in the metadata for Product Criticality settings or to create Custom Risk Scores.

Create Custom Product Criticalities

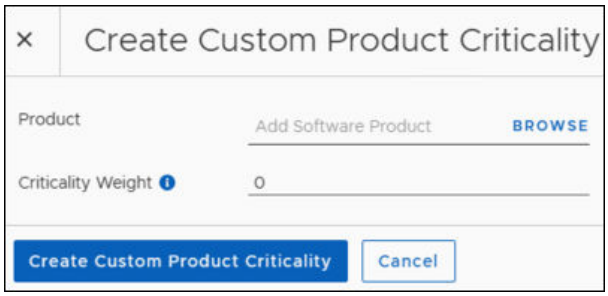
1. Select **+Create Custom Product Criticality** in the **Custom Risk Settings** workspace. This opens the **Create Custom Product Criticality** dialog.



2. Select **Browse** to search for the product you want to customize.

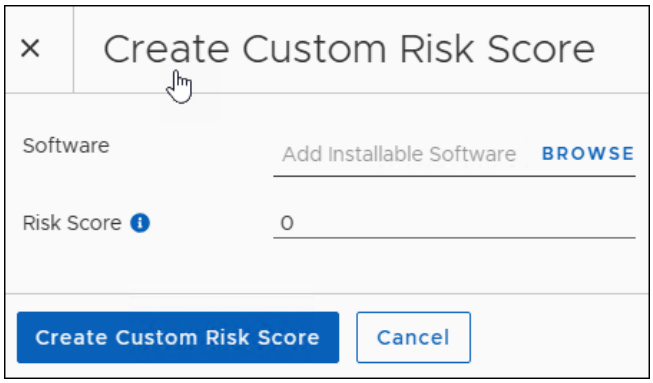


3. Select the product to modify, and then select **Add Software Product**.
   - This adds a table to **Custom Product Criticalities**.
   - Each time you add another product, the added information appears in this table.
4. Enter the number that corresponds to the criticality weight you want to set for this product, and then select **Create Custom Product Criticality**.



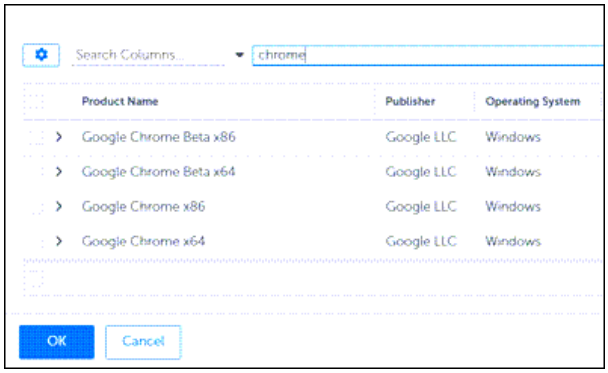
Create Custom Risk Scores

1. Select **+Create Custom Risk Score** in the **Custom Risk Settings** dialog. This opens the **Create Custom Risk Score** dialog.



2. Select **Browse** to open the **Add Installable Software** dialog.
3. a. Enter a product name in the search line, and then select **Search**. This example uses Google Chrome.

b. Select the product from the list, and then select **OK**.



4. Enter the number that corresponds to the risk score you want to set for this product, and then select **Create Custom Risk Score**.
   - This adds a table to **Custom Risk Scores**.
   - Each time you add another product, the added information appears in this table.
5. Select **Save Settings**.

Content Prestaging Settings

The Content Prestaging feature deploys 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 Adaptiva pushes the content to the best-suited sources in all locations that require the content.Adaptiva 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 Adaptiva 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.

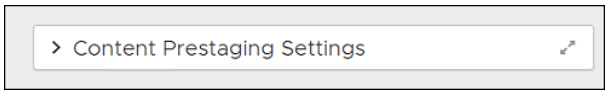
Pull Content

- **Not Enabled** -- Disables any prestaging as part of the Patching Process workflow or Patching Strategy.
- **Handled by System** – The Adaptiva 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.

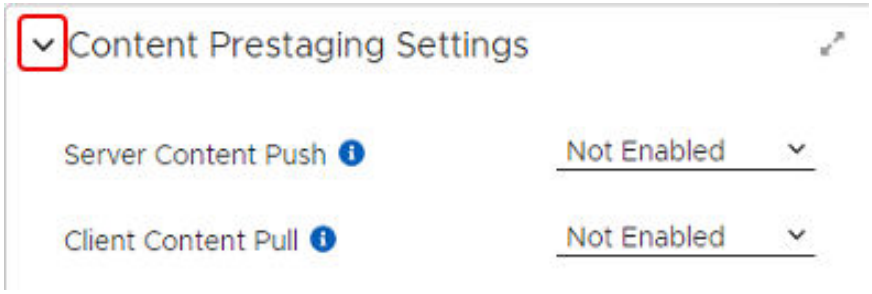
Set Content Prestaging Settings

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

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

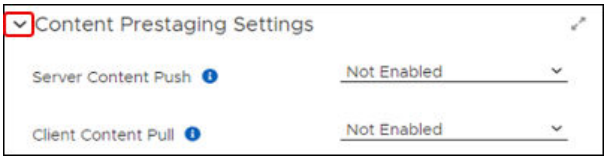


2. Expand the **Content Prestaging Settings** to view the available settings.

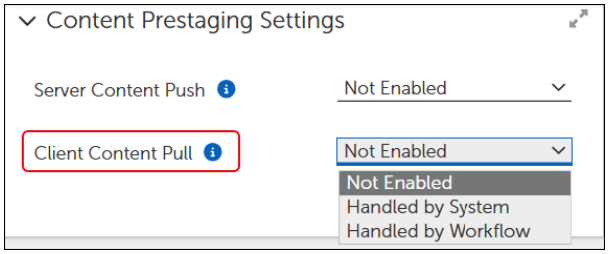


Enable Client Content Pull

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:



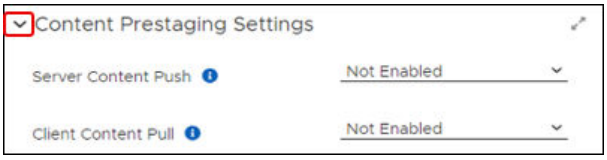
1. Select the arrow to the right of **Client Content Pull** to expand the menu of available options.



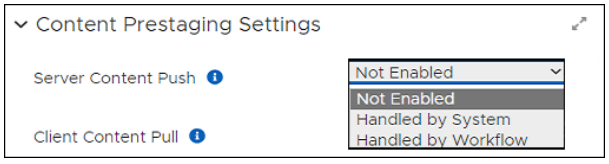
2. Select the option you need for the object template you are using. For definitions of push options, see Defining Content Prestaging Settings.
3. Select **Save** on the upper-left to save your changes:
   a. Check the **Error View** and resolve any errors.
   b. Select **Save** again if you make any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



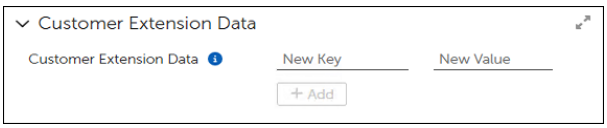
1. Select the arrow to the right of **Server Content Push** to expand the menu of available options.



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 Adaptiva. 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.



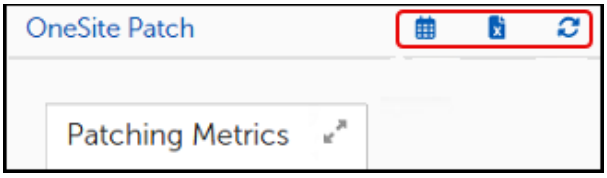
Customer Extension Data fields relate directly to fields in a customized template. If you do not have customized templates with key/value pairs you can modify, you do not need to configure or use this feature.

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

Navigating the OneSite Patch Dashboard

Date Settings, Export, and Refresh

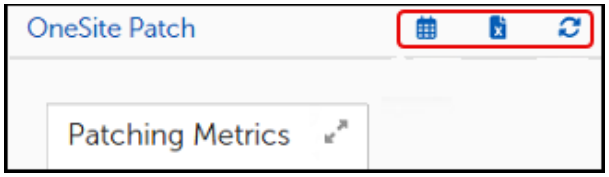
The three small icons (Calendar, Export and Refresh) on the upper right of the Home page and on any of the Patching Analytics pages (Overview, Products, Patches, or Devices) provide options to customize the date settings to a particular date range, choose some or all widgets on the page for exporting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



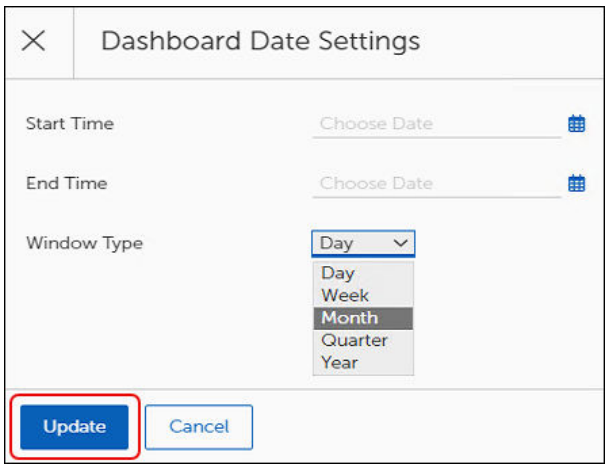
Set Dates for Status Views

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

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



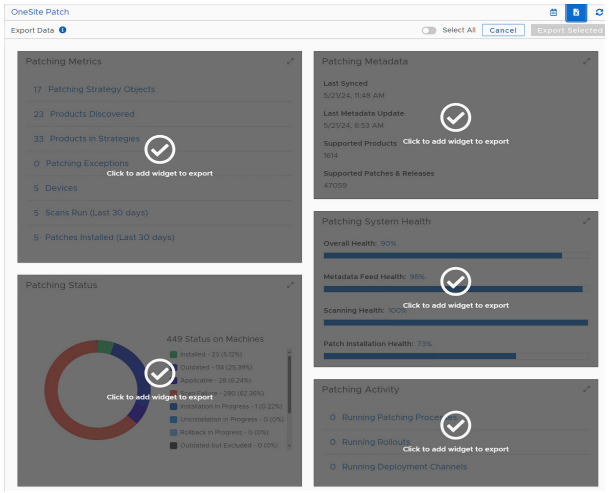
2. Enter the **starting and ending dates** for the range you want to view or use the calendar icon to the right of each date field to choose a date from the calendar.



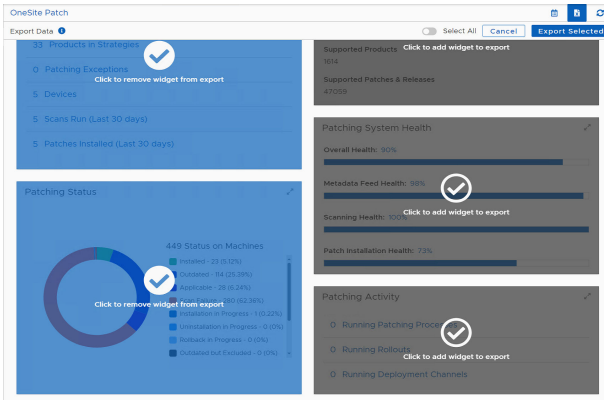
3. Select the **Window Type** setting, and then select whether to view data by **Day**, **Week**, **Month**, **Quarter**, or **Year** from the dropdown menu.
4. Select **Update** to save the settings. The view details update automatically for the date range you entered.

Export Widget Data

1. Select on the upper-right 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:
   - Select **Select All** at the top of the page to export all widgets.
   - Select an individual widget to export a single widget, or select multiple widgets to export.



3. Select **Export Selected** on the upper-right. 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.

Patch Menus

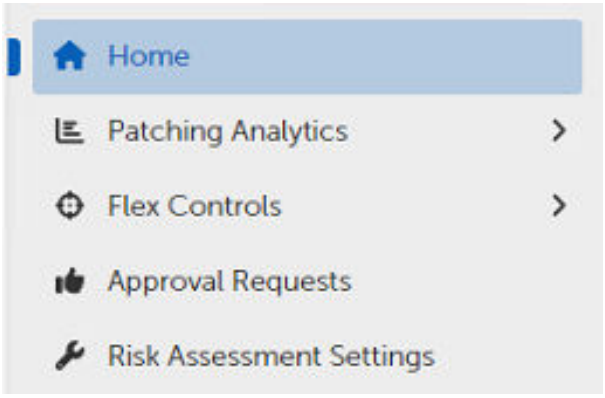
The left navigation menu lists the object available for configuring or monitoring in the OneSite Patch product. Those items with additional choices include a pop-out menu indicated by a right-angle bracket (>).

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

Home Menu

Home menu choices provide status information related to products, patches, devices, deployment, and approval requests, as well as access to settings for Risk Assessment and Flex Controls. Flex Controls contain tools that an administrator can use to monitor cycle operations, create patching exceptions, and pause or roll back patching strategies (see Home Menu Object Descriptions).

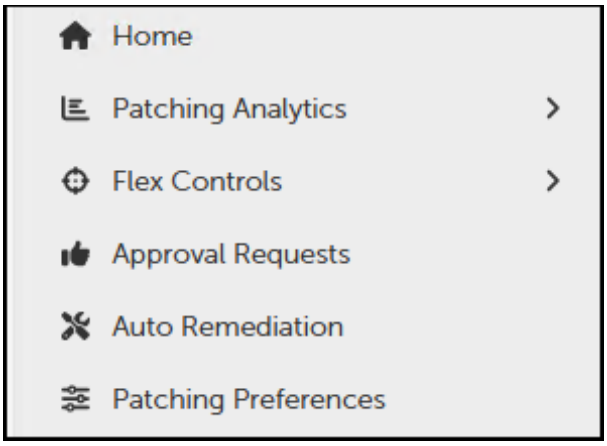
Administrators use this information to review performance and to help prioritize actions required to keep the environment updated, compliant, and risk free.



From any location within OneSite Patch, select **Home** to return to the Home page. For a description of Home page widgets, see Home dashboard and Performance Widgets.

Patch Express Home Menu

The Home menu provides access to the status and statistical information you can use to analyze the performance and activities occurring in the estate by products, patches and devices. **Flex Controls**, **Auto Remediation**, and **Patching Preferences** provide configuration workspaces where you may customize specific functionality.



From any location within , click **Home** to return to the **Home** page. For a description of **Home** page widgets, see Home Dashboard and Performance Widgets.

Home Menu Object Descriptions in Patch Express

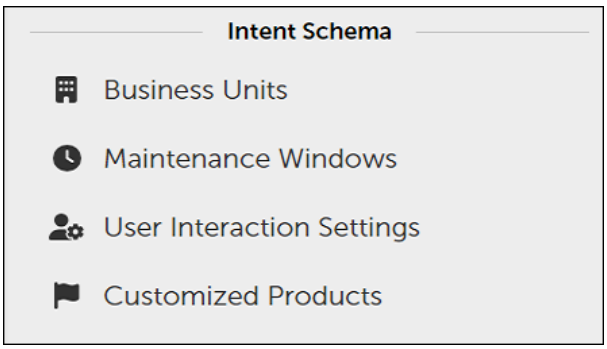
Object	Purpose
Home	Opens the **Home** page to view the overall status, metric, and compliance for patching in your environment. See Dashboard and Performance Widgets.
Patching Analytics	Shows the status of patches and products in the environment. Change tabs to view metrics for Products, Patches, or Devices. See Patching Analytics Dashboards. Sub menus include Overview, Products, Patches, and Devices.
Flex Controls	Review and manage settings for Blocklisting, Exceptions, Global Pause, and Rollbacks. Review Patching Cycle statistics (Cycle Operations), and view both running and historic cycles for Patching, Deployment, and Rollout. For details on each selection, see Flex Controls
Approval Requests	View all approval requests and check the status of pending and completed requests. See Approval Requests.
Auto Remediation	Use this menu to enable and configure Auto Remediation details for security issues based on level of criticality (Critical, High, Medium, Low). Configure and test production deployment settings.
Patching Preferences	Create patching preferences based on target Business Unit including assignment of a Maintenance Window and User Interaction settings.

Integration Menu

The Integrations menu provides access to available integrations based on licensing.

Intent Schema Menu

The **Intent Schema Menu** refers to the menu items administrators use to customize and manage patching policies for Business Units.

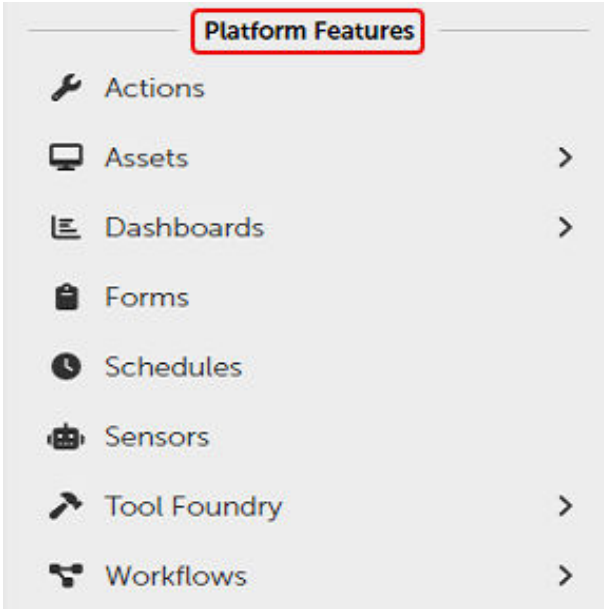


Intent Schema Object Descriptions

Object	Purpose
Business Units	Logically group and manage devices, settings, and other resources within a hierarchy. See Business Units
Maintenance Windows	Define maintenance and reboot windows. Primarily associated with Business Unit configurations. See Maintenance Windows.
User Interaction Settings	Control what the endpoint user sees and what options they have for interacting with patching notifications and required reboots. See User Interaction Settings.
Customized Products	Customization of installation for products with specific actions needed, such as license key entry or custom installation locations, before or after an installation. See Customized Products.

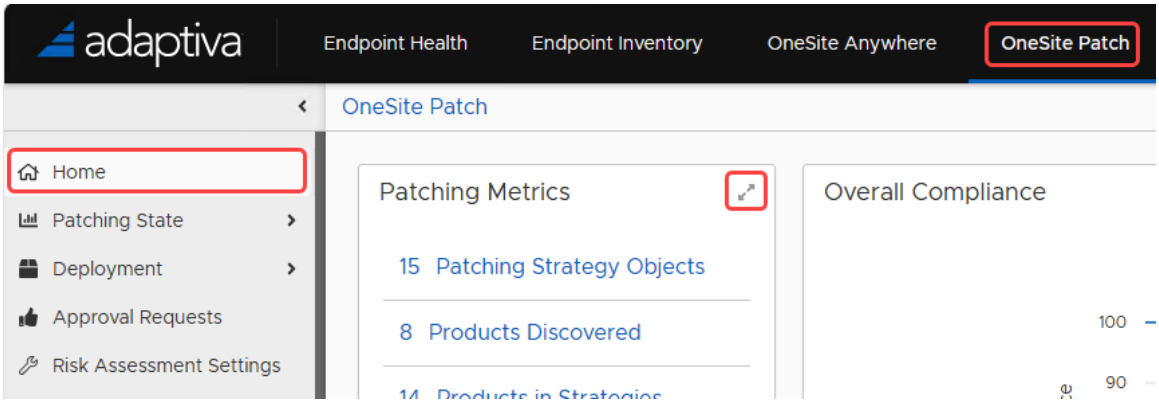
Platform Features Menu

These are common features available from every menu in . and across the full platform of OneSite products. For a description of the items in this menu, see the *Adaptiva OneSite Platform User Guide*.



Dashboard and Performance Widgets

The OneSite Patch 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.

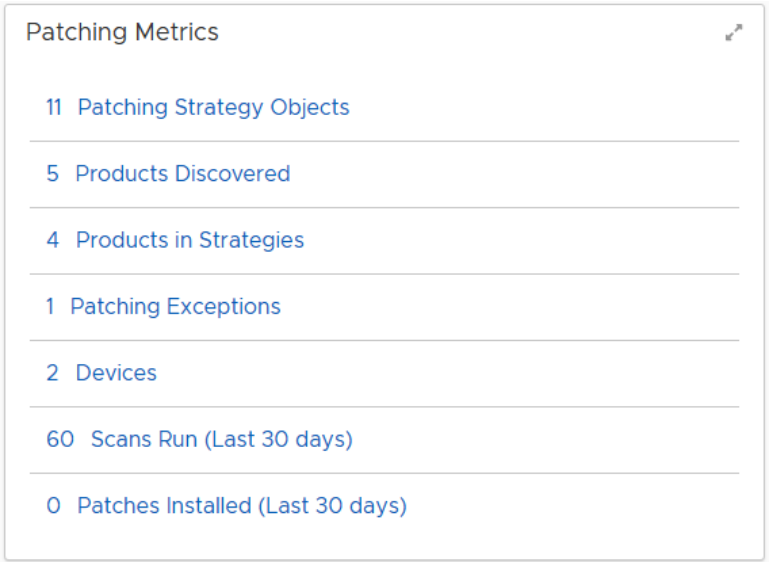


The layout of these widgets depends on the size of your computer monitor.

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

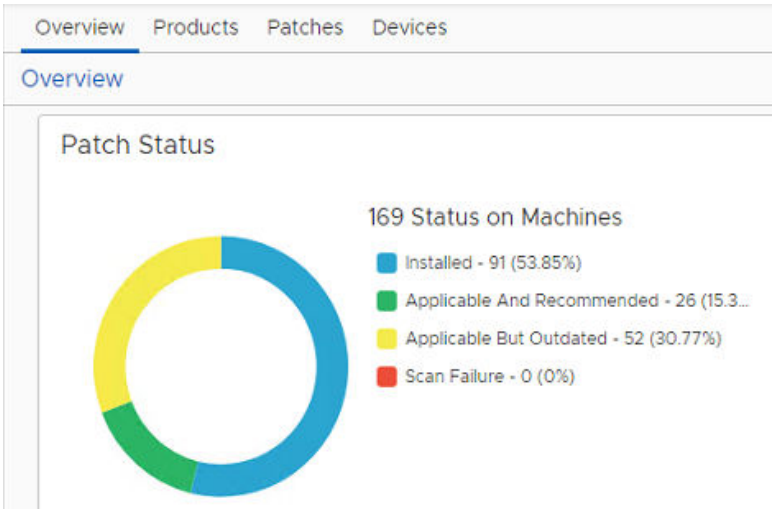
Patching Metrics

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**.



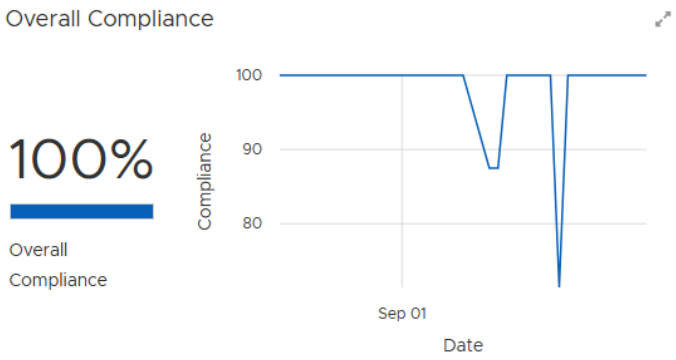
Patching Status

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



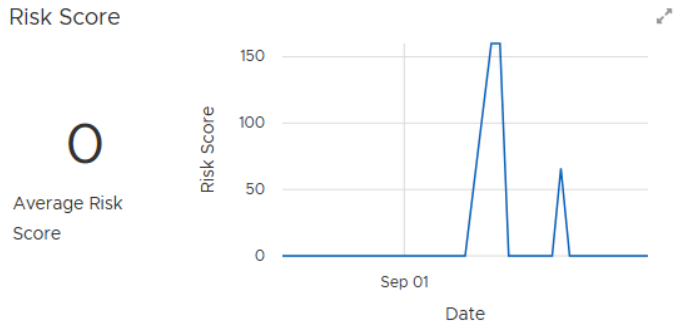
Overall Compliance

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



Risk Score

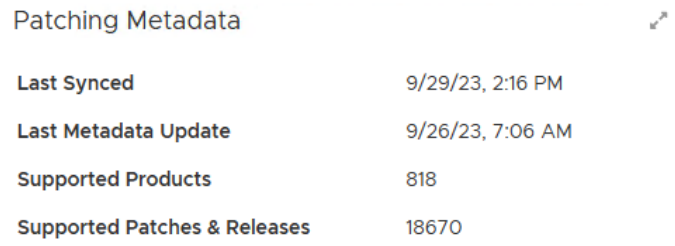
Returns the average risk score for all products identified in the metadata, and shows the average Risk Score. Depending on the dates chosen for the dashboard reporting, the administrator can see the changes in risk over time. See Date Settings for Status Views for more information.



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

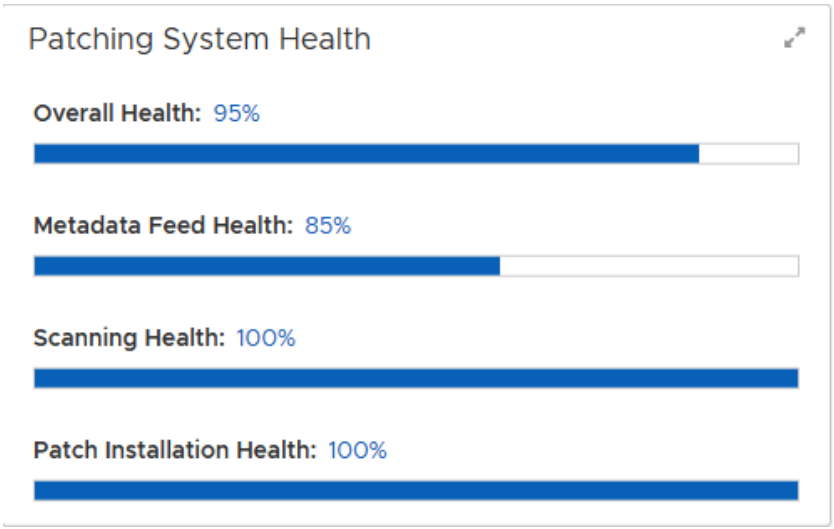
Summarizes the status of the latest endpoint scans and client product inventory updates. Metadata includes details about the products, patches, and updates approved by the company for installation. The **Patch Metadata** summary tells the administrator when the AdaptivaServer and AdaptivaClient last 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.



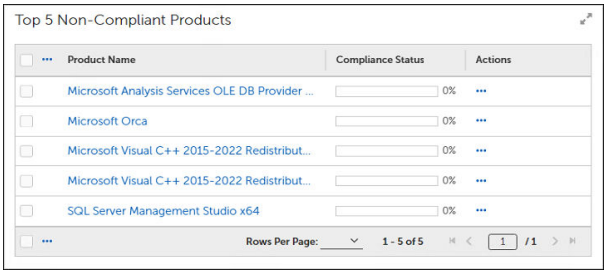
Patching Activity

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 the 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

OneSite Patch supports patching for multiple versions of products across licensed clients/endpoints. A dedicated team of metadata analysts constantly reviews and 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 an automatic notification within 24 hours of a release update. The team uses Virus Total to scan all downloaded content in an isolated and secure environment. The Virus Total score for the content must be zero (0) before Adaptiva publishes the content to the Adaptiva CDN. The Adaptiva CDN converts the update to our native content format and makes it accessible to licensed 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.

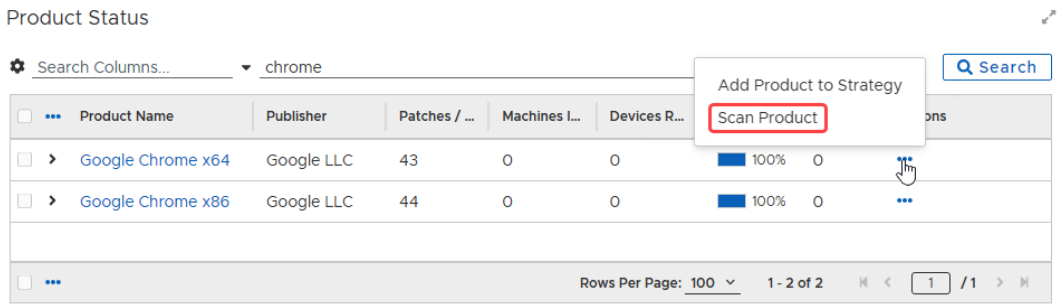
After confirming a successful update, the team creates, reviews, and approves the metadata before adding it to the metadata catalog. See OneSite Patch 3rd Party App Catalog (adaptiva.com) for more information.

Endpoint Scans

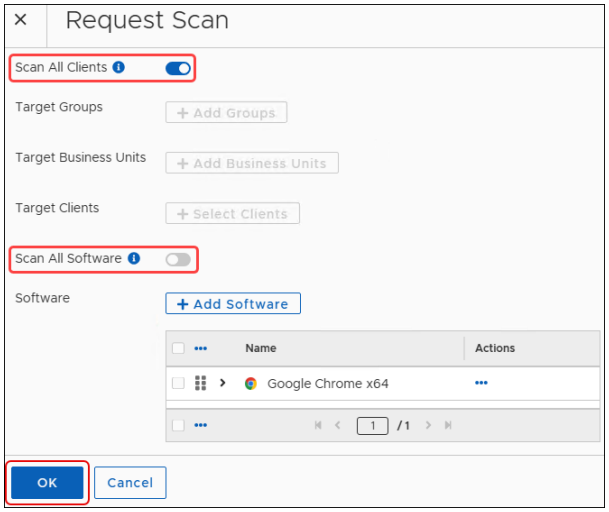
The endpoint scanning timeline for patch and product status defaults to once daily. Administrators can start and customize scans at any time using the **Request Scan** feature.

Request a Scan

1. From the Adaptiva 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:
   - **Overview** – **Product Status** table: Actions include Scan Product and Reset Deployment Failures for Product.
   - **Products** – **Product Status** table: Actions include Scan Product and Reset Deployment Failures for Product.
   - **Patches** – **Patch Status** table: Actions include Scan Patch and Reset Deployment Failures for Patch.
   - **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**.
   - This opens the **Request Scan** dialog and prepopulates the **Software** section with all the software available on the item you chose to scan.
   - **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`.

Patch Filter Settings

Display	Description
Object ID	
Version	
Name	
Description	
Product ID	
Parent ID	
Blocklist.On	Blocklisting state for this object. Values: true or false
Blocklist.Hidden	Hidden state for this blocklisting. Values: true or false
Blocklist.DateTime	The date and time the patch was added to the blocklist.
Blocklist.Reason	Detailed reason for blocklisting this patch.
Blocklist.VendorUrl	Vendor URL that describes problems leading to blocklisting.
Content.ContentId	Optional. If not specified, the content ID defaults to: `Adaptiva$MD$<Object ID of Object>`. Use the same format for a customer-provided ID to publish content files, or edit this property to insert a unique customer content ID.
Content.SourceType	Defines the content source using one of the built-in constants.
Content.VendorUrl	Required by the server to download the Object from the vendor download location. The Client uses the content ID to download content rather than the URL. Valid only if [SourceType] is the Vendor CDN or the Vendor CDN with Adaptiva CDN Backup.
Content.AdaptivaUrl	URL to use for Adaptiva CDN.
Content.FileName	The original file name of the file downloaded from the URL. Needed because some CDNs download the file with a junk name and we need to know the original filename to rename it, after download. Valid only if [ContentSourceType] is the Adaptiva CDN, Vendor CDN, or Vendor CDN with Adaptiva CDN Backup.
Content.Sha256Hash	Required by the server to download the Object from the vendor download location. The Client uses the content ID to download content rather than the URL. SHA256 secure hash for the Object file downloaded from the URL, used only by server for verifying and adding to content metadata. Not sent to clients as part of Object or software Object - clients receive it as part of content metadata.
Content.Size	Size of the content file.
ContentForRepair.ContentId	Optional. If not specified, the content ID is: `Adaptiva$MD$<Object ID of Object>`. Use the same format for a customer-provided ID to publish content files or edit this property to insert a unique customer content ID.
ContentForRepair.SourceType	The type of content source, using one of the built-in constants.
ContentForRepair.VendorUrl	Required by the server to download the Object from the vendor download location. The Client uses the content ID to download content rather than the URL. The external URL to download the Object from the vendor download location. Valid only if [SourceType] is Vendor CDN, or Vendor CDN with Adaptiva CDN Backup.
ContentForRepair.AdaptivaUrl	URL to use for Adaptiva CDN.

Display	Description
ContentForRepair.FileName	The original file name of the file downloaded from the URL. Needed because some CDNs download the file with a junk name. We need to know the original filename to rename it, after download. Valid only if [ContentSourceType] is the Adaptiva CDN, Vendor CDN, or Vendor CDN with Adaptiva CDN Backup.
ContentForRepair.Sha256Hash	Required by the server to download the Object from the vendor download location. The Client uses the content ID to download content rather than the URL. SHA256 secure hash for the Object file downloaded from the URL, used only by server for verifying and adding to content metadata. Not sent to clients as part of Object or software Object - clients receive it as part of content metadata.
ContentForRepair.Size	Size of the content file.
ContentForUninstallation.ContentId	Optional. If not specified, the content ID is: `Adaptiva$MD$<Object ID of Object>`. Use the same format for a customer-provided ID to publish content files or edit this property to insert a unique customer content ID.
ContentForUninstallation.SourceType	The content source type, using one of the built-in constants.
ContentForUninstallation.VendorUrl	Required by the server to download the Object from the vendor download location. The Client uses the content ID to download content rather than the URL. Valid only if [SourceType] is the Vendor CDN or the Vendor CDN with Adaptiva CDN Backup.
ContentForUninstallation.AdaptivaUrl	URL to use for Adaptiva CDN.
ContentForUninstallation.FileName	The original file name of the file downloaded from the URL. Needed because some CDNs download the file with a junk name, and we need to know the original filename to rename it after download. Valid only if [ContentSourceType] is the Adaptiva CDN, Vendor CDN, or Vendor CDN with Adaptiva CDN Backup.
ContentForUninstallation.Sha256Hash	Required by the server to download the Object from the vendor download location. The Client uses the content ID to download content rather than the URL. SHA256 secure hash for the Object file downloaded from the URL, used only by server for verifying and adding to content metadata. Not sent to clients as part of Object or software Object - clients receive it as part of content metadata.
ContentForUninstallation.Size	Size of the content file.
Extensions.PreInstallationActionSequence	Action sequence to execute before Adaptiva installation actions. Fails install if any action fails.
Extensions.PostInstallationActionSequence	Action sequence to execute after Adaptiva installation actions.
Extensions.PreRepairActionSequence	Action sequence to execute before Adaptiva uninstallation actions. Fails uninstall if any action fails.
Extensions.PostRepairActionSequence	Action sequence to execute after Adaptiva uninstallation actions.
Extensions.PreUninstallationActionSequence	Action sequence to execute before Adaptiva repair actions. Fails repair if any action fails.
Extensions.PostUninstallationActionSequence	Action sequence to execute after Adaptiva repair actions.
Falcon.ExPRT	The highest ExPRT rating of CVEs referenced by the metadata object in Risk.CveIds and all its superseded objects.
Falcon.ExploitStatus	The highest exploit status of all CVEs referenced by the metadata object in Risk.CveIds and all its superseded objects.
Falcon.KnownExploitExists	If Falcon.ExploitStatus = Available, Easily Accessible, or Actively used, then true. Otherwise, false.
General.Schema	The schema version number for this object, starting with 1.
General.ExpiredByVendor	Specifies that the vendor expired the software represented by this object. Recommend that clients no longer use this version.

Display	Description
General.Name	Required. The user-readable name of this Object. Use the same name that the vendor specified, so that customers can see the same name they see on the Internet.
General.ShortName	Required. A vendor Object name for this that follows a consistent format for each vendor Object. For example, Microsoft Objects use a KB number, such as KB4474419. Adobe uses a Bulletin ID, such as APSB21-85. Use whatever is appropriate for each third-party and be consistent across all Objects for that vendor.
General.Description	A description of the Object, readable to users. If the software vendor has published a description for the Object, reuse that description without changes. Otherwise, Adaptiva generates an appropriate description, based on the available details. If empty, no description.
General.VendorVersion	The version of the software as specified by the vendor. This is a non-standard format, so not reliable for comparison of one Object version with another. For that comparison, use the **ReleaseDate** property. Unless otherwise stated by vendor, Objects with an earlier **ReleaseDate** are a lower version than an Object with a later **ReleaseDate**.
General.VendorName	The name of the vendor that published this Object. Vendor name should be consistent for all Objects published by the same vendor.
General.ReleaseDate	The date and time of the first release of the Object.
General.ReleaseNotes	The release notes for this Object, from the vendor, unedited. If empty, no release notes.
General.AdditionalInformationUrl	A URL containing additional information published by the vendor of the Object. If empty, no URL is available.
General.MsiGuid	The MSI GUID of the application, if it is an MSI used for detection rules and uninstallation.
General.IsSecurityUpdate	If this update contains security fixes.
General.IsUpdateRollup	If this update contains a rollup update.
General.IsMinorFeature	--
General.IsMajorFeature	--
General.IsServicepack	--
General.IsBugfix	--
General.TargetType	Specifies the type of software targeted by the Object, using one of the built-in constants. Required.
General.WhoAmI	Specifies the origin and business use of the metadata object.
Icon.IconID	Object ID of the Icon Object for this software.
Icon.CompressedData	compressed base64 of the .ico file, used only in Icon objects.
Install.InstallerType	Specifies the type of installer using one of the following built-in constants: MSI, MSIX, MSIX Bundle, Silent EXE, non silent EXE, PowerShell script, VB script, Batch file.
Install.PreActionSequence	Action sequence to execute before installation of this software. The expressions may use macros, contain multiple actions, ignore errors for some actions, or fail in case of others. Installation takes place only if the expression succeeds.
Install.ActionSequence	Action sequence to execute to install this software. The expressions may use macros, contain multiple actions, written to ignore errors for some actions, or fail in case of others.
Install.CustomizerUI	Optional. User Form JSON containing UI for the customizer that lets the administrator select installation options.
	Defaults to no customizer is available.
Install.PostActionSequence	An action sequence that executes only after successful installation of this software. The expressions may use macros, contain multiple actions, written to ignore errors for some actions, or fail in case of others.

Display	Description
Install.AutoItScript	If present, this autoIT script performs a silent install of this software. The script is a sensor expression, which contains liberal doses of literal strings containing OneSite Patch AutoIT commands and scripts, peppered with Adaptiva macros and sensor expressions. At runtime, evaluates this sensor expression, and the resulting string contains a fully valid and executable AutoIT script. The system automatically writes this resulting script to the Adaptiva.AU3 file in the unpacking folder. The AutoITScriptPath runtime property contains the absolute path of this script file that, when passed as a parameter to the AutoIT action, executes the AutoIT script.
Install.InterferingProcesses	Optional. A list of process names known to interfere with installation of this Object that require ending before installation begins so they do not interfere. Specify each process using the full name of the executable. For example, excel.exe. Defaults to none.
Install.InterferingProcessesToWaitFor	Optional. A list of process names known to interfere with installation of this Object must run to completion before the installation begins. These processes must end naturally prior to installation. Specify each process name using the full name of the executable. For example, excel.exe. Defaults to none.
Install.InternetRequired	Defines whether the installation requires an Internet connection to install the Object properly.
Install.LoggedOnUser	Uses one of the built-in constants below to determine whether a logged-on user affects this installation. Constants are: Required, Prohibited, or Don't care. Defaults to Don't care.
Install.RequiresReboot	Uses one of the built-in constants below to determine whether the installation requires reboot using one of the following built-in constants: Required, Prohibited, or Don't care. Default: Do not care.
Install.DiskSpaceRequired	The amount of disk space required for uninstallation. Defaults to 2x content size.
Install.MaxRunTime	The maximum amount of time required for uninstallation, after the uninstaller begins executing. Defaults to 4:00:00 (4 hours). If uninstallation fails to complete during this time, the uninstaller process ends and fails the uninstall.
InstallTime.ObjectID	--
InstallTime.UnpackingFolder	Absolute path of the folder into which the installation unpacks content for this product.
InstallTime.AutoITScriptPath	Absolute path of the file that contains the runtime version of the AutoIT script.
Media.FileNamePattern	Use when the media consists of a single file, such as 7z2106-x64.exe, or a regular expression that matches the single file. Conclusive detection of this media occurs by matching the single file against this pattern.
Media.KeyFileName	--
Media.MediaDetectionSensorExpression	--
Realtime.RegistryIndicators	Specifies one or more registry keys to watch for real time detection of any install/uninstall activity for this software.
Realtime.FolderIndicators	Specifies one or more files or folders to watch for real time detection of any install/uninstall activity for this software. May contain environment variables in the standard %NAME% format.
Relationships.Product	The objectID of the product to which this object belongs.
Relationships.PrerequisiteInstalls	Object IDs of one or more software products/software release groups/releases/patches that require installation prior to installing this software (all the dependencies of this software). For software release groups, the installation uses the release group rules to scan for and use the latest release group. For products, the installation uses the latest release of the latest release group. The installation aborts if it detects an error.

Display	Description
Relationships.FollowupInstalls	Object IDs of one or more software products/software release groups/releases/patches that require installation after installing this software, such as any follow-ons of this software for software release groups, the installation uses the release group rules to scan for and use the latest release group.
	For products, the installation uses the latest release of the latest release group.
	The installation continues even if it detects an error.
Relationships.Supersedes	Object IDs of all software releases and patches which this software supersedes, including all the software contained in [SupersedesRemovalRequired]. Includes patches and releases superseded by one or more of these objects by reference only.
Relationships.SupersedesRemovalRequired	Object IDs of all software releases and patches that this software supersedes, and that require uninstalling before installing this software. Subset of the IDs specified in [Supersedes]. Includes patches and releases superseded by one or more of these objects by reference only.
Relationships.SupersededBy	Object IDs of any software releases or patches which supersede this software, if any. Includes patches and releases superseded by one or more of these objects by reference only. Superseded whenever an existing software has metadata published by Adaptiva.
Relationships.Parent	Object ID of the parent of this object.
Relationships.Children	Object IDs of the children of this object.
Repair.InstallerType	Specifies the type of this installer, using one of the following built-in constants: MSI, MSIX, MSIX Bundle, Silent EXE, Non silent EXE, PowerShell script, VB script, Batch file.
Repair.PreActionSequence	Action sequence to execute before installation of this software. The expressions may use macros if needed. It may contain multiple actions. You may write it to ignore errors for some actions, or to fail in others. Installation takes place only if this expression succeeds.
Repair.ActionSequence	Action sequence to execute to install this software. The expressions may use macros if needed. It may contain multiple actions. Write this to ignore errors for some actions or to fail in others.
Repair.CustomizerUI	Optional. User Form JSON containing UI for the customizer that will let the admin select installation options. Default: no customizer is available.
Repair.PostActionSequence	Action sequence to execute only after successful installation of this software. The expressions may use macros if needed. It may contain multiple actions. Write it to ignore errors for some actions or to fail in others.
Repair.AutoItScript	If present, this is the autoIT script for performing silent install of this software. It is a sensor expression which contains liberal doses of literal strings containing AutoIT commands and script, peppered with Adaptiva macros and sensor expressions. At runtime, we will evaluate this sensor expression, and the resulting string will contain a fully valid and executable AutoIT script. The system will automatically write this resulting script to the Adaptiva.AU3 file in the unpacking folder. The AutoITScriptPath runtime property contains the absolute path of this script file, which can be passed as a parameter to the AutoIT action, which will execute the AutoIT script.
Repair.InterferingProcesses	Optional. A list of process names known to interfere with installation of this Object, and the process shuts them down before installing the patch. Specifies each process name using the full name of the executable, such as excel.exe. Default: none.

Display	Description
Repair.InterferingProcessesToWaitFor	Optional. A list of process names known to interfere with installation of this Object but must end naturally so they do not run during installation. Specify each process name using the full name of the executable, such as excel.exe. Default: none.
Repair.InternetRequired	Whether or not installing the Object properly requires Internet.
Repair.LoggedOnUser	Whether a logged-on user affects this installation, using one of the following built-in constants: Required, Prohibited, or Don't care. Default: Do not care.
Repair.RequiresReboot	Whether this installation requires reboot: using one of the following built-in constants: Required, Prohibited, or Don't care. Default: Do not care.
Repair.DiskSpaceRequired	The amount of disk space required for uninstallation. if missing, 2x content size is used by default.
Repair.MaxRunTime	The maximum amount of time required for uninstallation, after the uninstaller has started executing. If missing, 4:00:00 (4 hours) is used by default. If uninstallation has not completed in time, the process shuts down the uninstaller and the uninstall fails.
Risk.CveIds	The IDs of any CVEs resolved by this Object. If empty, there are no CVE IDs.
Risk.CvssScores	All the CVSS scores for vulnerabilities fixed by this patch or release.
Risk.SecurityExposureLevel	Vendor's indication of how critical the security exposure for this Object is, using one of the built-in constants. Id a patch fixes multiple CVEs with different CVSS scores, the highest of those scores are reflected in this property
Risk.KnownExploitExists	Whether or not a known exploit exists for the vulnerability that this Object fixes.
Risk.Criticality	This value is the default that is used to calculate the risk assessment score for releases/patches. Customers may override it. Represents the importance of a product in a customer environment. Rate minor tools like text editors low, and rate involved and data-sensitive software high.
Rules.InstalledAuthoringRuleObject	JSON representation of the MetadataAuthoringRule object that detects installation of this Software Product/Release Group/Software Release/Software Patch is the client machine. Returns a boolean response. This property is removed from the Feed view and replaced with the InstalledRuleId property.
Rules.InstallableAuthoringRuleObject	JSON representation of the MetadataAuthoringRule object that detects whether this Software Release/Software Patch is currently Installable on the client machine. The rule returns a boolean value. This removes the property from the Feed view and replaces it with the InstallableRuleId property. 1) Install this release or patch on this machine, using only the pre-requisites defined in the object metadata.
Rules.ApplicableAuthoringRuleObject	JSON representation of the MetadataAuthoringRule object that detects whether this Software Release/Software Patch is currently applicable on the client machine. The rule returns a boolean response. This removes this property from the Feed view and replaces it with the ApplicableRuleId property. Applicability is defined as: 1) A previous version of this software is currently installed on this machine, AND 2) You may install this release, or patch, on this machine using only the pre-requisites defined in the object metadata, AND 3) installation of this object would replace the previous version if performed using the pre/post/installation steps defined in the object metadata
Rules.InstallPathSensorExpression	An optional sensor expression that returns the absolute installation path of the installed software.
Rules.InstalledVersion	An optional sensor expression that returns the version of the installed product.
Tracking.Method	The method used for tracking releases of this software.

Display	Description
Tracking.WebScrapeURL	The URL for the website to monitor for this software.
Tracking.WebScrapeDescription	A description of the monitor to use for administrative purposes.
Tracking.WebScrapeInterval	The interval (in hours) on which to check for changes.
Tracking.WebScrapeScanDate	The last time the scan ran. Used to determine when to run the next scan.
Tracking.WebScrapeIdentificationAttributes	The html attributes to identify the element for checking for changes.
Tracking.WebScrapeMonitoringAttributes	The html attributes to compare for changes.
Uninstall.InstallerType	Specifies the type of this installer, using one of the following built-in constants: MSI, MSIX, MSIX Bundle, Silent EXE, Non silent EXE, PowerShell script, VB script, Batch file.
Uninstall.PreActionSequence	Action sequence to execute before installation of this software. The expressions may use macros if needed. It may contain multiple actions. You may write it to ignore errors from some actions or fail in case of others. Installation takes place only if this expression succeeds.
Uninstall.ActionSequence	Action sequence to execute to install this software. The expressions may use macros if needed. It may contain multiple actions. You may write it to ignore errors for some actions or fail in case of others.
Uninstall.CustomizerUI	Optional. User Form JSON containing UI for the customizer that will let the admin select installation options. Default: no customizer is available.
Uninstall.PostActionSequence	Action sequence executed only after successful installation of this software. The expressions may use macros if needed. It may contain multiple actions. You may write it to ignore errors for some actions or fail in case of others.
Uninstall.AutoItScript	If present, this is the autoIT script for performing silent install of this software. It is a sensor expression which contains liberal doses of literal strings containing AutoIT commands and script, peppered with Adaptiva macros and sensor expressions. At runtime, we will evaluate this sensor expression, and the resulting string will contain a fully valid and executable AutoIT script. The system will automatically write this resulting script to the Adaptiva.AU3 file in the unpacking folder. The AutoITScriptPath runtime property will contain the absolute path of this script file, passed as a parameter to the AutoIT action, which will execute the AutoIT script.
Uninstall.InterferingProcesses	Optional. A list of process names known to interfere with installation of this Object. Shut down these processes before installing the patch. Specify each process name using the full name of the executable, such as. excel.exe. Default: none.
Uninstall.InterferingProcessesToWaitFor	Optional. A list of process names known to interfere with installation of this Object and must end to end naturally. These processes should not be running during installation. Each process name is specified using the full name of the executable, such as excel.exe. Default: none.
Uninstall.InternetRequired	Whether the installation requires Internet to install the Object properly.
Uninstall.LoggedOnUser	Whether a logged-on user affects this installation, using one of the following built-in constants: Required, Prohibited, or Don't care. Default: Do not care.
Uninstall.RequiresReboot	Whether this installation requires reboot: using one of the following built-in constants: Required, Prohibited, or Don't care. Default: Do not care.
Uninstall.DiskSpaceRequired	The amount of disk space required for uninstallation. if missing, 2x content size is used by default.

Display	Description
Uninstall.MaxRunTime	The maximum amount of time required for uninstallation, after the uninstaller has started executing. If missing, 4:00:00 (4 hours) is used by default. If uninstallation has not completed in time, the process shuts down the uninstaller and the uninstall fails.
UserPortal.Name	Optional. Used for overriding the same property in the [General] section, else the value from the [General] section is displayed.
UserPortal.Description	Optional. Used for overriding the same property in the [General] section, else the value from the [General] section is displayed.
UserPortal.Version	Optional. Used for overriding the same property in the [General] section, else the value from the [General] section is displayed.
UserPortal.VendorName	Optional. Used for overriding the same property in the [General] section, else the value from the [General] section is displayed.
UserPortal.Categories	Any categories within the user catalog to which this software belongs.
UserPortal.Keywords	Any keywords the software should be associated with within the user catalog.
WSUS.UpdateID	Specifies the WSUS update ID for this patch.
WSUS.CAB	Specifies the base CAB file name for this patch. For Windows patches, set to W + <4-digit year of creation>. CAB name schema defined in future for other Microsoft products.
WSUS.FileNames	Contains all file names for this WSUS update.
WSUS.FileURLs	Contains the Microsoft URLs corresponding to each of the file names for this wsus update.
WSUS.UninstallSupported	If set to true, the process may uninstall this WSUS update.
WSUS.Classification	Specifies the WSUS classification to which this update belongs, such as Security updates, Upgrades, Critical updates, and so on.
WSUS.Products	Specifies one or more WSUS products to which this update belongs, such as Windows 10, Windows 11, Windows 10 LTSB, and so on.
WSUS.KBs	Specifies one or more KB article numbers with which this update is associated, such as KB7354748.