



OneSite Patch Express

with Microsoft Defender

Table of Contents

Adaptiva Copyright and Legal Notices	1
Revision History	2
Getting Started with OneSite	3
Prerequisites	3
Supported Browsers	3
Logging	3
Customer Support	3
Adaptiva OneSite Admin Portal	4
Log in to the OneSite Admin Portal	4
Licensing Adaptiva Products	5
Add an OneSite License Key	6
Add a Licensed Product to a Collection Group	6
Adaptiva OneSite Patch Dashboard	8
Access the OneSite Patch Dashboard	8
OneSite Patch Express Setup Wizard	10
Welcome to OneSite Patch Express	10
Detection Integrations	11
Integrate a Partner Product	11
Use Copy From	14
Select a Remediation Schedule	16
Enable Vulnerability Detection	17
Enable Patch Pre-staging	18
Configure Deployment Notifications	19
Configure Deployment Approval	22
Configure Test Deployment	25
Configure Test Approval	28
Complete OneSite Patch Express Setup	30
Best Practices for Patch Express	32
Integrate Defender	33
Create a Microsoft Entra Application	33
Add Permissions to an Entra Application	34
Create a Shared Secret ID	37
Locate and Record the Microsoft Entra IDs	39
Integrate Defender with OneSite Patch	40
Administrators and Roles	41
Access Security Settings	41
View Administrators	42
Create a New Administrator	43
View Roles	45
Create a New Role	45
Menu Objects for OneSite Patch	50

Patching Analytics Dashboards	51
Using Search in OneSite Patch	51
Patching Analytics Overview	51
Products View	52
Patches View	55
Devices View	58
Flex Controls	61
Blacklisting	61
Blacklist Settings	62
Blacklisted Patches	64
Cycle Operations	70
Patching Cycles	71
Deployment Cycles	73
Rollout Cycles	75
Patching Exceptions	77
Using Patching Exceptions	77
Create a Patching Exception	77
Set Override Details for Patch Exception	78
Set Last Allowed Patch Versions	80
Add Target Business Units for Patch Exceptions	80
Global Pause	81
Stop All Patching Activity Immediately	82
Resume All Paused Patching Activity Immediately	83
Pause Patching for Specific Objects	85
Pause Deployment of a Specific Software Product	86
Pause Deployment of a Specific Patch	89
Pause Specific Cycles	91
Pause Deployment to a Business Unit	101
Rollbacks Overview	103
Rollback	103
Rollback to Version	121
Approval Requests	139
Approve or Reject a Patch Request	139
Auto Remediation	141
Access Auto Remediation and Deployment Settings	141
Using Auto Remediation Settings	142
Enable Auto Remediation	143
Vulnerability Detection Source Settings	145
Production Deployment Settings for Auto Remediation	145
Test Deployment Settings for Auto Remediation	146
Verify that Auto Remediation Works as Expected	147
Patching Preferences	148
Using Patching Preferences	148

Access Patching Preferences	148
Create a New Patching Preference	149
Add a Target Business Unit	149
Select a Server Maintenance Window	150
Select Server User Interaction Settings	152
Business Units	153
Understanding Business Units	153
Parent and Child Business Units	154
Managing Inheritance Settings	155
Enable Inheritance	156
Disable Inheritance	156
Organizing the Business Unit Hierarchy	156
Best Practices when Changing Priorities	157
Change the Order of the Hierarchy	157
Creating a Business Unit	158
Open and Save a Business Unit Template	159
Add Evaluation Schedules to a Business Unit	160
Configure Business Unit Scopes	161
Verify Business Unit Members	169
Create a Lab Business Unit	169
Create a Custom Lab Business Unit	171
Open and Save a Business Unit Template	159
Verify Business Unit Members	169
Create a Lab Business Unit	169
Test Deployment Settings for Auto Remediation	170
Create a Custom Lab Business Unit	171
Maintenance Windows	174
Open and Save a Maintenance Window Template	174
Add Dynamic Detection Workflow (Optional)	175
Apply to All Urgencies	175
Set Maintenance Windows by Urgency	175
Create a Maintenance Window	175
Set the All Urgencies Override Duration	176
Save and Deploy the Maintenance Window	176
User Interaction Settings	177
Understanding User Interaction Settings	177
Create User Interaction Settings	177
Open and Save a User Interaction Template	177
Edit or Create Urgency Settings	178
Set Deployment Notification Settings	179
Create System Reboot Notification Settings	180
Save and Deploy User Interaction Settings	182
Customized Products	183

Manage Settings for Customized Products	183
Open and Save a Customized Product Template	183
Add a Deployment Wave to a Customized Product Template	183
Add a Target Product	184
Configure Software Install Settings	185
Navigating the OneSite Patch Dashboard	187
Date Settings, Export, and Refresh	187
Set Dates for Status Views	187
Export Widget Data	188
Refresh the Status View	190
OneSite Patch Menus	190
Integration Menu	190
Platform Features Menu	191
OneSite Patch Dashboard and Performance Widgets	191
Patching Metrics	192
Patching Status	192
Overall Compliance	193
Risk Score	193
Patching Metadata	193
Patching System Health	194
Patching Activity	194
Top 5 Non-Compliant Products	195
Top 5 Missing Patches	195
Appendices	197
Software Products Library	197
Metadata Catalog	197
Endpoint Scans	197
Request a Scan	197

Adaptiva Copyright and Legal Notices

Copyright © 2023-2024 Adaptive Protocols, Inc. - All Rights Reserved

The information in these documents is proprietary and confidential to Adaptive Protocols, Inc. (Adaptiva®) and provided to customers for their internal use only. No part of this document may be reproduced or redistributed in any form without the prior written consent of Adaptiva.

All information supplied here is subject to change without notice. Contact Adaptiva to request the latest OneSite specifications and designs.

Adaptiva reserves the right to amend the product(s) or information disclosed herein at any time without notice. Adaptiva does not assume any responsibility or liability arising out of the application or use of any product or service described herein, except as expressly agreed to in writing by Adaptiva.

Any brand and/or product names mentioned may be trademarks of their respective companies.

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
October 30, 2024	v9.1.965.12	v1.1	Added full access to Flex Controls for Express users.
October 1, 2024	9.1.965.9	v1.0	First Release with Microsoft Defender integration.
August 27, 2024	9.1.965.4	EA Draft	EA Draft

Getting Started with OneSite

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.

Prerequisites

Before using any Adaptiva OneSite Products, you must set up your OneSite environment. See the *Adaptiva OneSite Platform Site Planning Guide* for details. The Adaptiva Server and Adaptiva Client software installations support all OneSite products. After you add license keys for your licensed products, you are ready to access the power of OneSite in your environment.

Supported Browsers


supports Google Chrome, Microsoft Edge and Chromium Edge, and most other browsers.



IMPORTANT

Do not use Microsoft Internet Explorer.

Logging

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

Access Adaptiva Client logs from the Adaptiva Client in `Program Files/Adaptiva/AdaptivaClient/Logs`.

Customer Support

Whenever you need information beyond what 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 Adaptiva OneSite Admin Portal and OneSite Patch dashboard to configure and manage OneSite Patch.

The OneSite Platform and all Adaptiva products use the OneSite Admin Portal to set up the Adaptiva environment, create policies, add administrators, and more. OneSite Admin Portal settings, such as groups, security, and administrators, are global settings and support all licensed Adaptiva products.

See the *Adaptiva OneSite Platform User Guide* for more information.

Log in to the OneSite Admin Portal

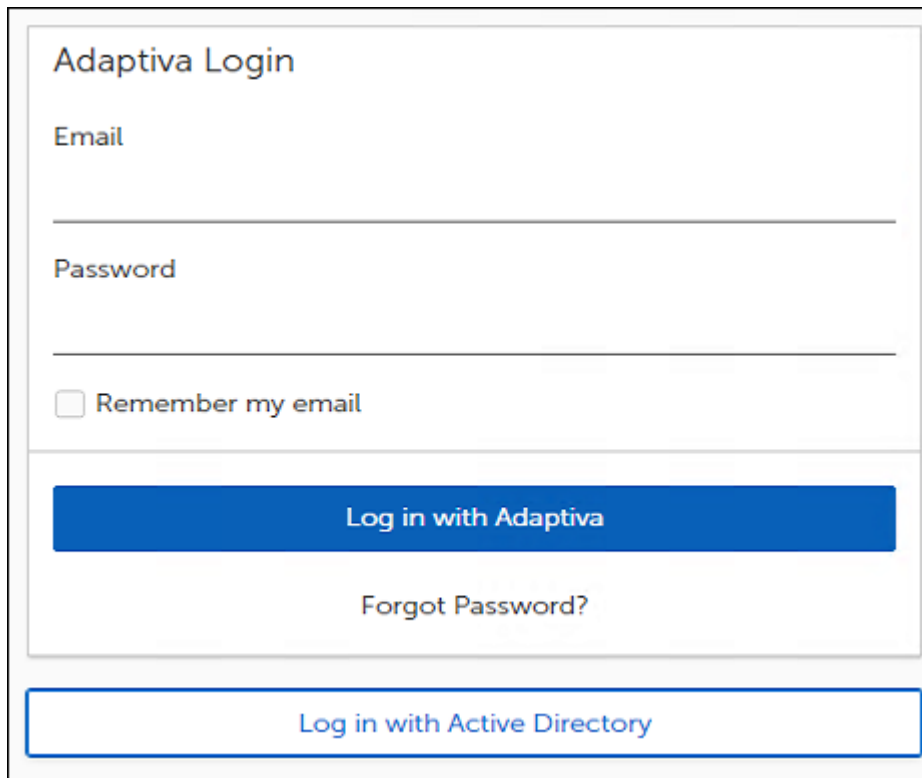
During the OneSite Product installation, the administrator creates a SuperAdmin account using either a native Adaptiva OneSite login or a Windows Active Directory account (recommended).

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]
```

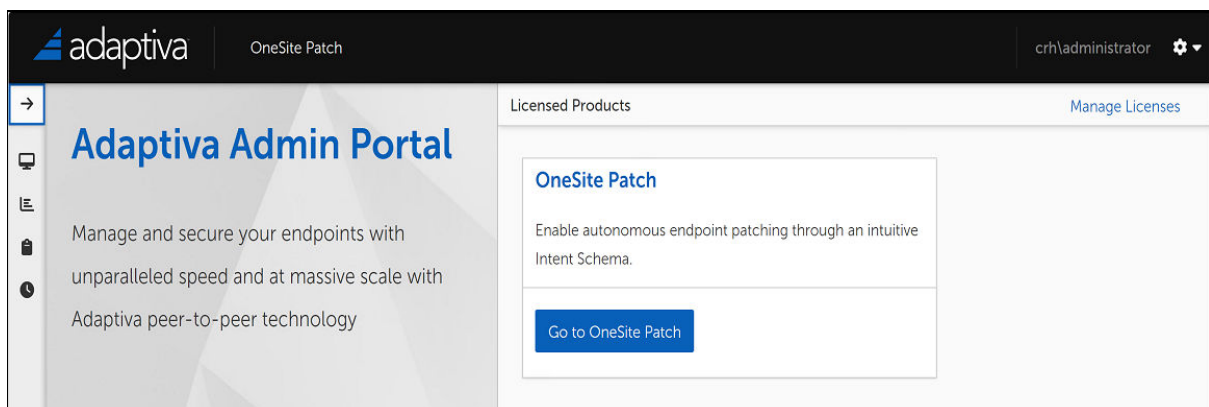
If necessary, confirm the port with the administrator who defined the port during software installation. If the server is already using port 80, for example, the web site might use port 9678.

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



The image shows a login form titled "Adaptiva Login". It contains two input fields for "Email" and "Password". Below these fields is a checkbox labeled "Remember my email". A prominent blue button labeled "Log in with Adaptiva" is centered below the form. Below the button is a link for "Forgot Password?". At the bottom of the form is a button labeled "Log in with Active Directory".

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



The image shows the OneSite Admin Portal dashboard. The top navigation bar includes the Adaptiva logo, "OneSite Patch", and the user "crh\administrator" with a settings icon. The main content area is split into two columns. The left column features the "Adaptiva Admin Portal" title and a description: "Manage and secure your endpoints with unparalleled speed and at massive scale with Adaptiva peer-to-peer technology". The right column is titled "Licensed Products" and contains a card for "OneSite Patch" with the text "Enable autonomous endpoint patching through an intuitive Intent Schema." and a "Go to OneSite Patch" button. A "Manage Licenses" link is visible in the top right of the right column.

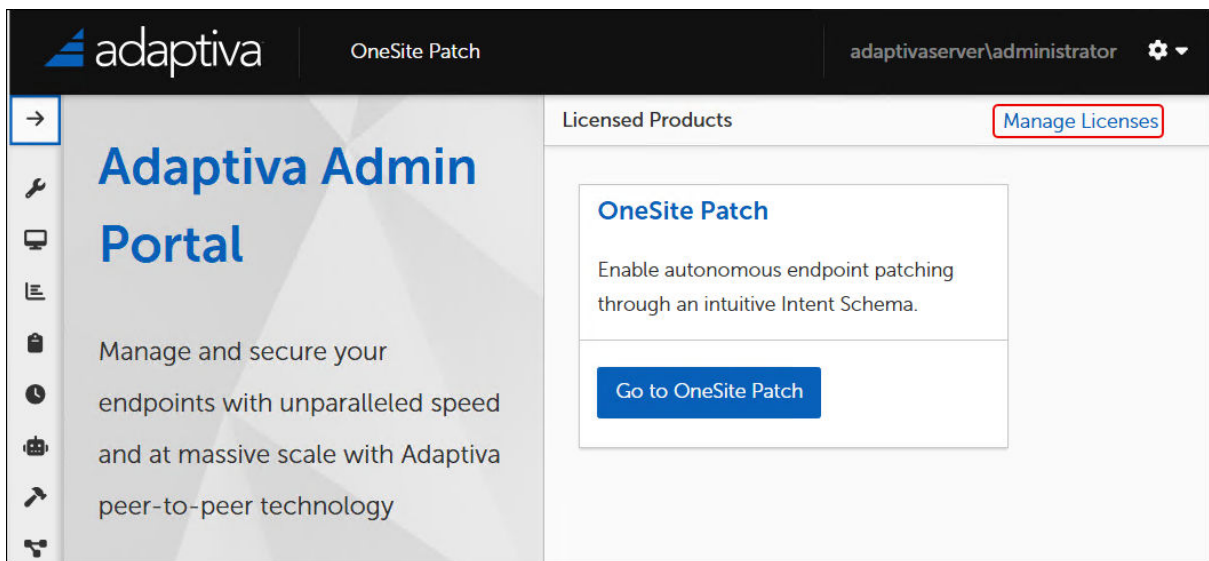
Licensing Adaptiva Products

Adaptiva OneSite Products require 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.

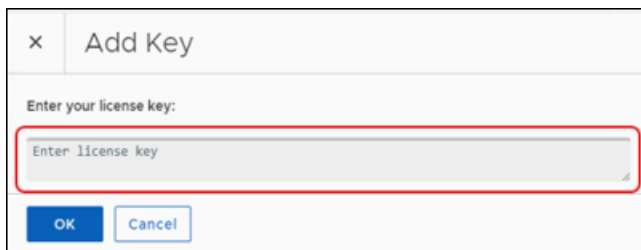
Enter the license key using the Adaptiva OneSite Admin Portal. If you are starting the OneSite Admin Portal for the first time or your key has expired, the software prompts you for a license key at login.

Add an OneSite License Key

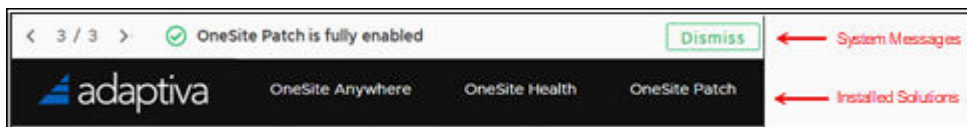
1. Click **Manage Licenses** at the upper-right of the Admin Portal dashboard.



2. Click **Add Key**, and enter your license key.



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



Add a Licensed Product to a Collection Group

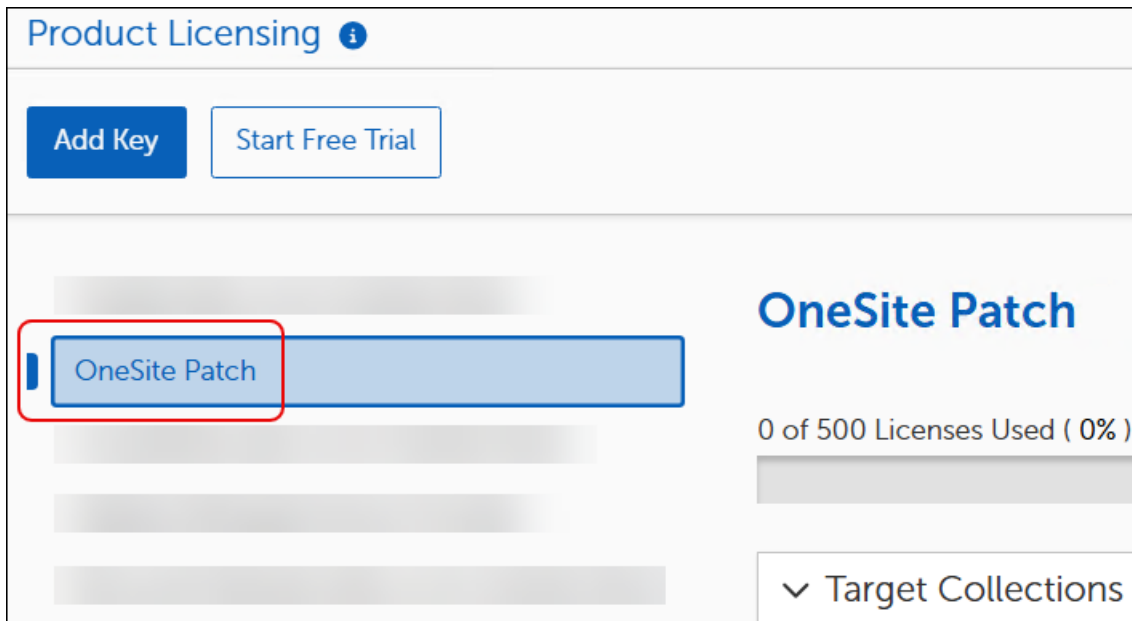
After entering a license key, select a Collection group for the licensed product.



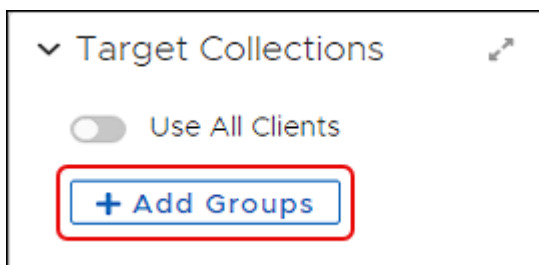
CAUTION

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

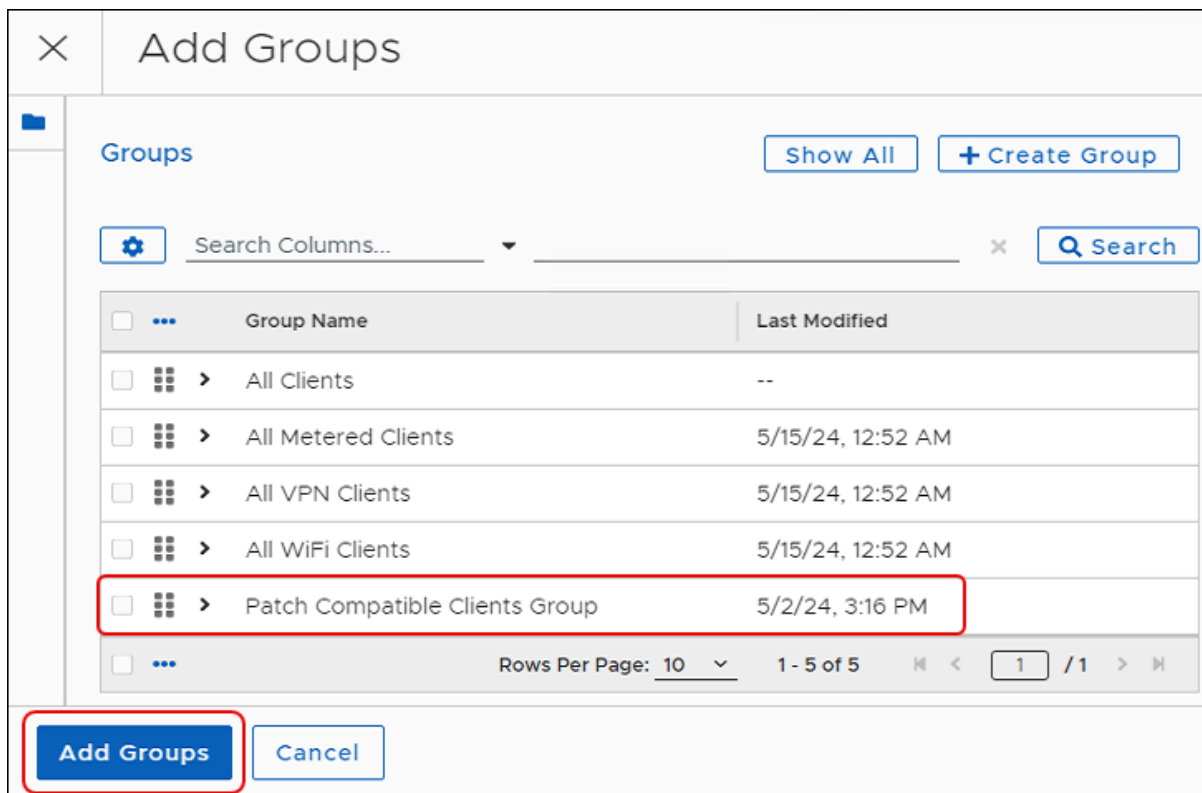
1. Select the OneSite Patch product name in the **Product Licensing** list.



2. Select **+ Add Groups** in the **Target Collections** section.



This opens the **Add Groups** dialog.



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

Adaptiva OneSite Patch Dashboard

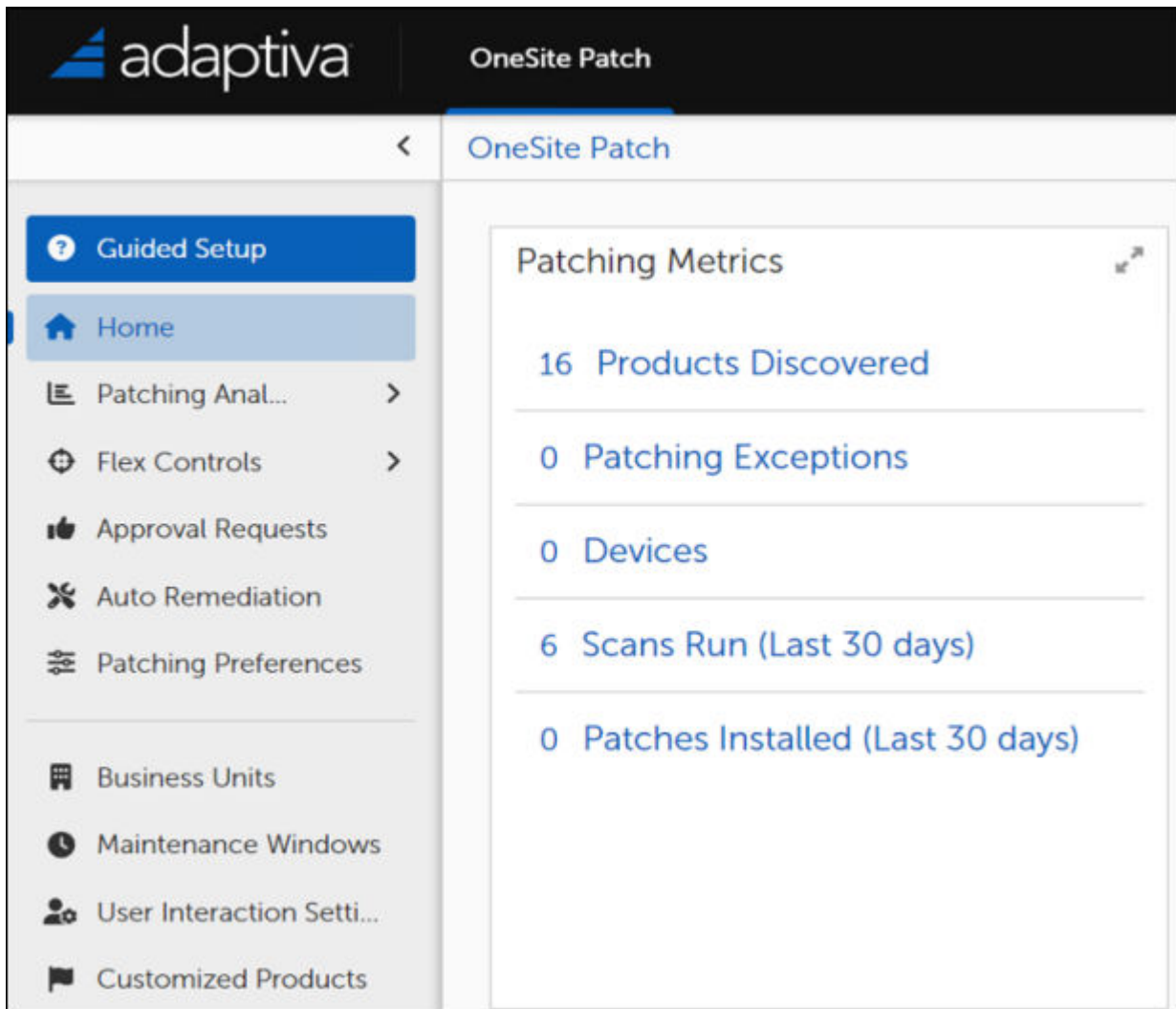
Use the OneSite Patch dashboard, available from the OneSite Admin Portal, to manage your patching strategies, review patching status, and more.

Access the OneSite Patch Dashboard

Open the OneSite Patch dashboard from the [OneSite Admin Portal](#) using one of the following methods:

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

This opens the OneSite Patch Dashboard.



OneSite Patch Express Setup Wizard

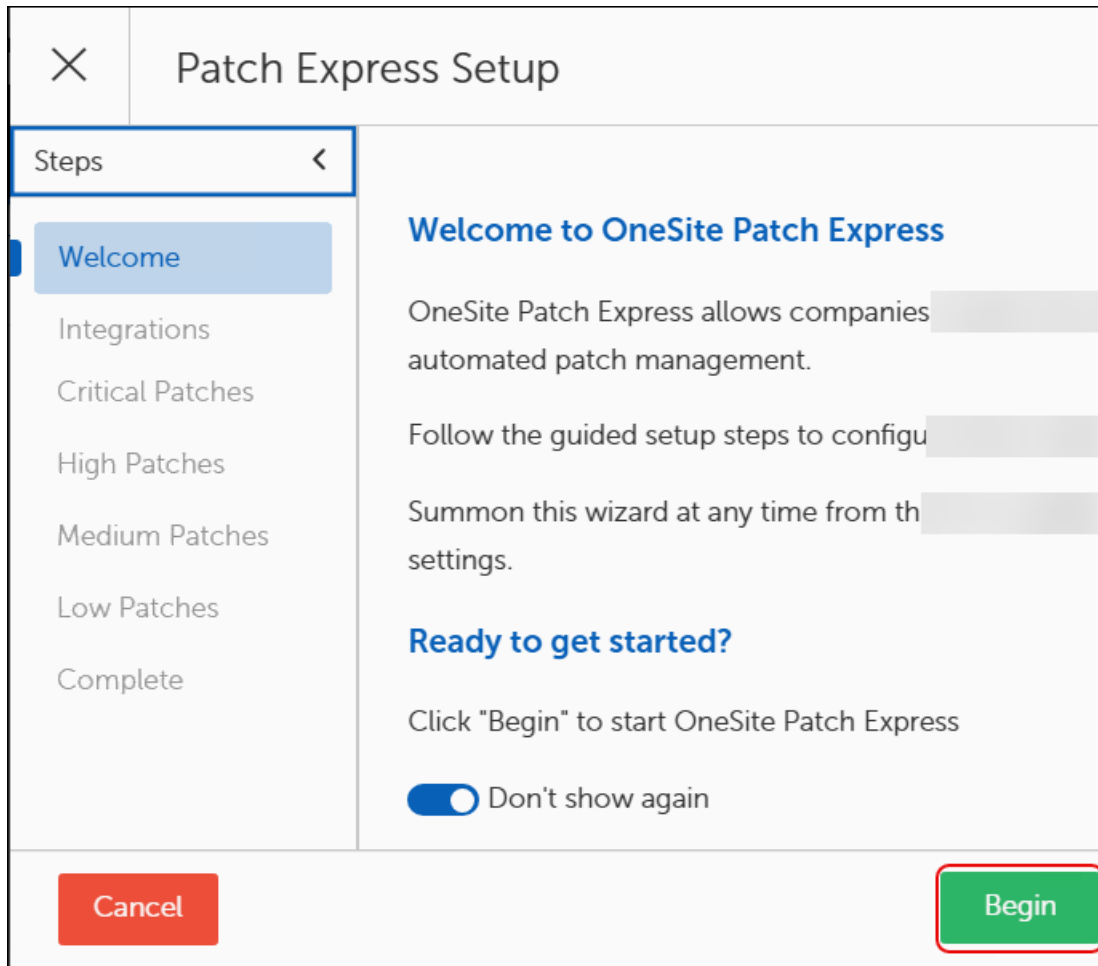
The OneSite Patch Express setup wizard provides step-by-step guidance for your first introduction to Patch Express. The wizard walks you through automatic deployment of patch remediation for each patch vulnerability level (Critical, High, Medium, and Low). You may use Patch Express on its own, or use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

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

Welcome to OneSite Patch Express

After you have completed the OneSite Express installation, the Guided Setup wizard starts automatically. You may choose to walk through it immediately to start and configure auto-remediation, or cancel the wizard and come back to it later. To prevent the wizard from starting automatically, see [Enable or Disable Guided Setup](#).

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



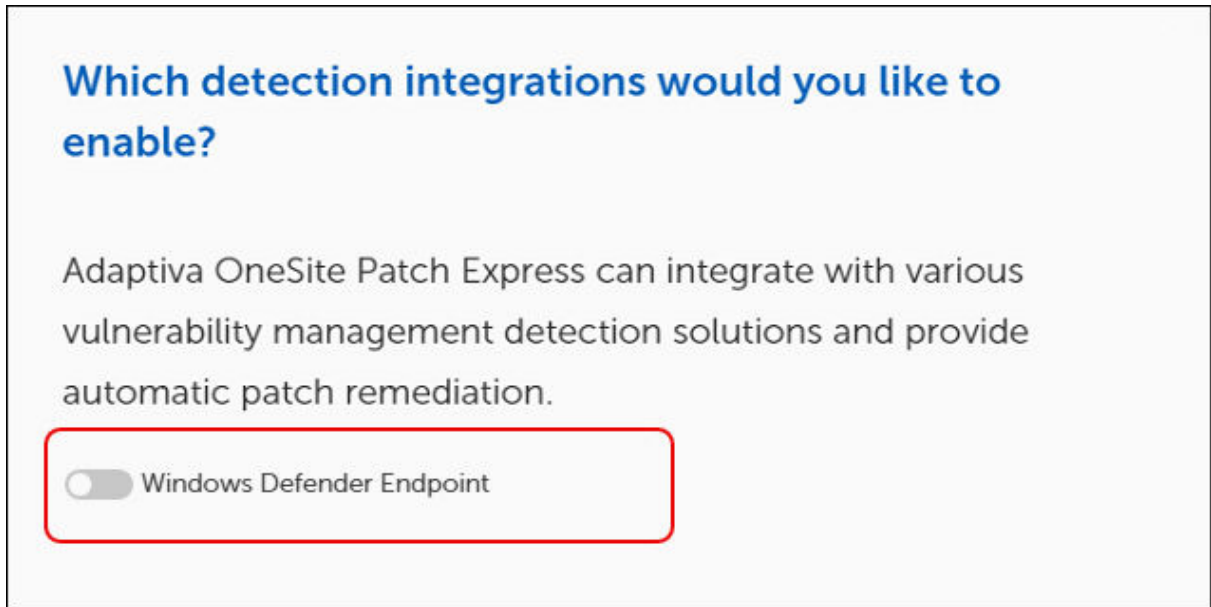
Detection Integrations

Detection integration means that OneSite Patch has detected a licensed partner product and wants to know whether to integrate it into OneSite Patch Express.

To integrate a partner product, you must have a valid OneSite license for the partner product. This is in addition to the base license for OneSite Express. Without a valid license installed, the integration pane has no options for integration. If you don't have a license for your partner product, contact [Adaptiva Customer Support](#).

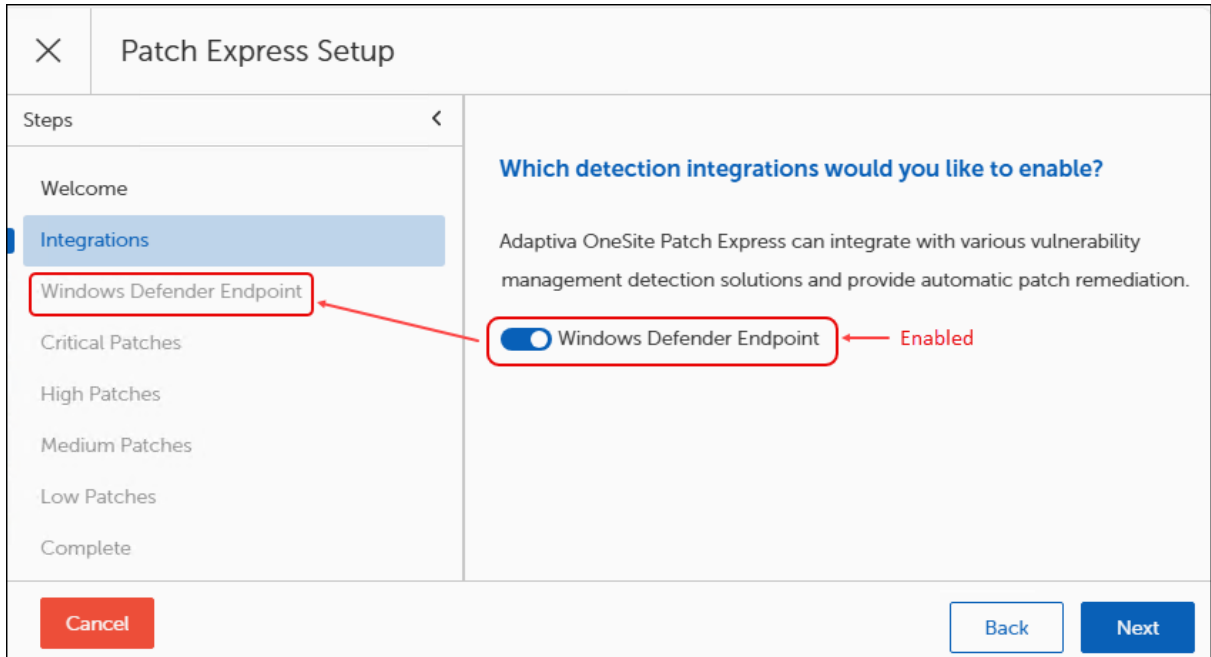
Integrate a Partner Product

1. Select **Begin** on the **Welcome** screen of the Patch Express Setup Wizard. This opens the Integrations pane.
 - If you have licensed a partner product in Patch Express, you will see it listed here. Continue to the next step.
 - If you do not use a partner product, skip to [Enablement](#).

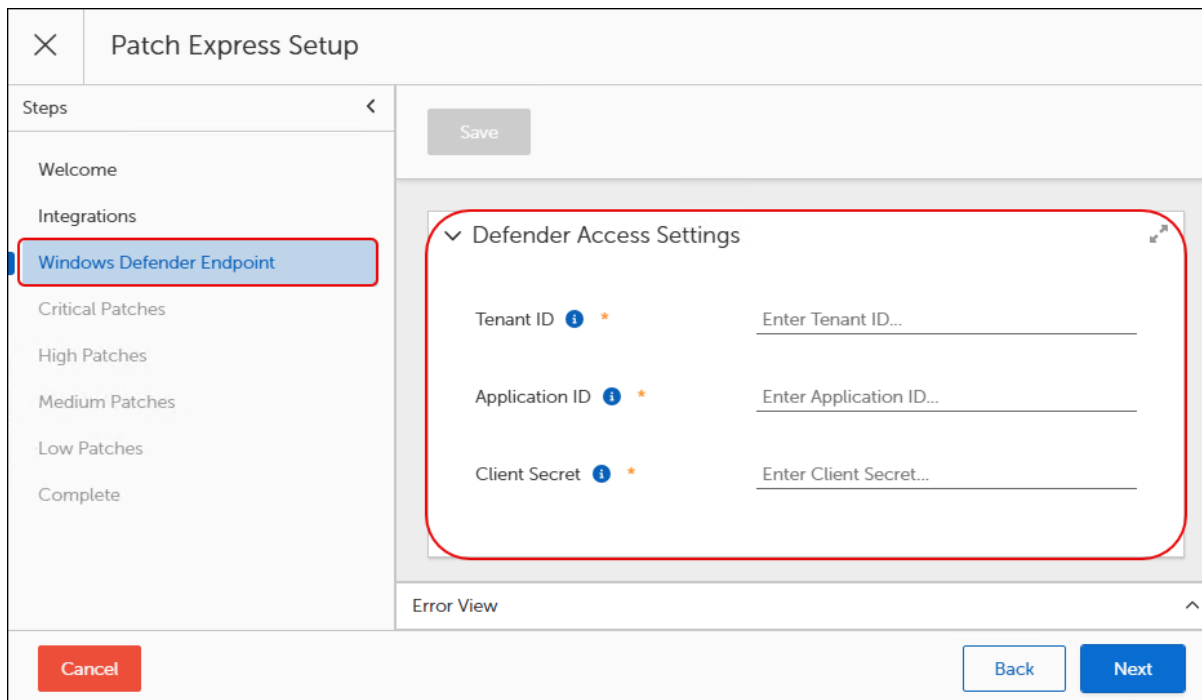


2. Select the **[Partner Product]** toggle to enable or disable (default) integration of your partner product.

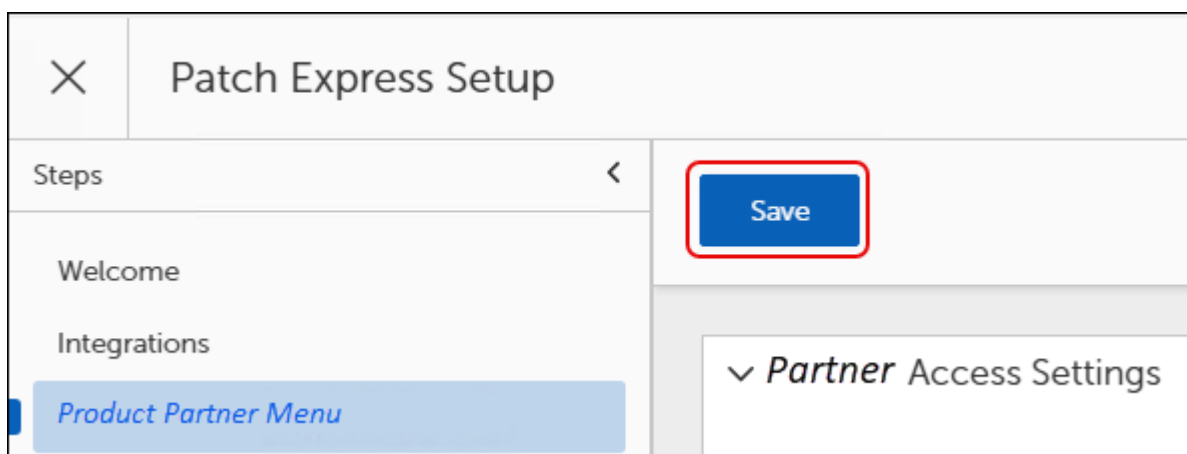
With the product enabled, the Steps of the left navigation menu include a new item related to product integration.



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



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



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



Use Copy From

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

The screenshot shows the 'Patch Express Setup' wizard interface. The title bar includes a close button (X) and the text 'Patch Express Setup'. Below the title bar is a 'Steps' navigation bar with tabs: 'Enablement...' (highlighted with a red box), 'Remedia...', 'Detectio...', 'Patch Pr...', and 'Deploym...'. On the left side, there is a vertical list of steps: 'Welcome', 'Integrations', 'Critical Patches', 'High Patches' (highlighted with a blue bar), 'Medium Patches', 'Low Patches', and 'Complete'. The main content area displays the question: 'Would you like to automatically remediate High level Patches?'. Below the question is explanatory text: 'If enabled, Adaptiva will automatically deploy patch remediations for all detected High level vulnerabilities.' At the bottom of the main area are three buttons: 'Yes' (blue), 'No' (orange), and 'Copy From' (blue with a dropdown arrow). At the very bottom of the wizard are three buttons: 'Cancel' (red), 'Back' (blue), and 'Next' (blue).

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

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

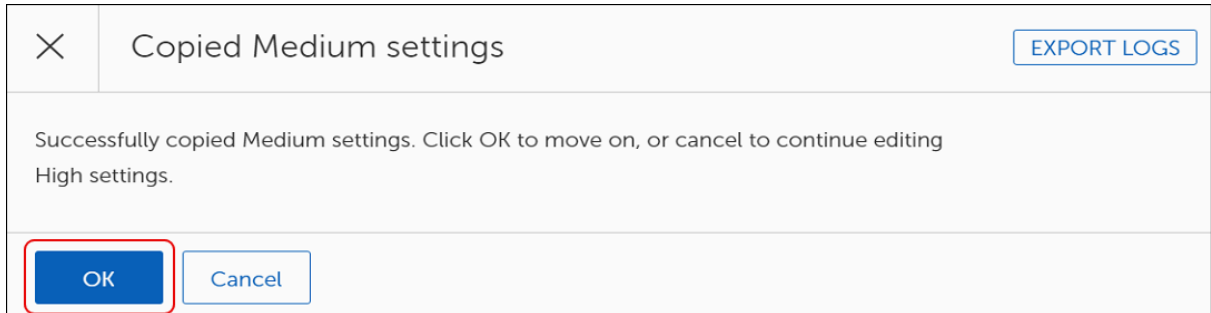
- If enabled, click the patch severity level from the Steps menu on the left navigation pane of the Patch Express Setup. The example uses High Patches
- Otherwise, click **No** to cycle to through the remaining patch severity levels.



TIP

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

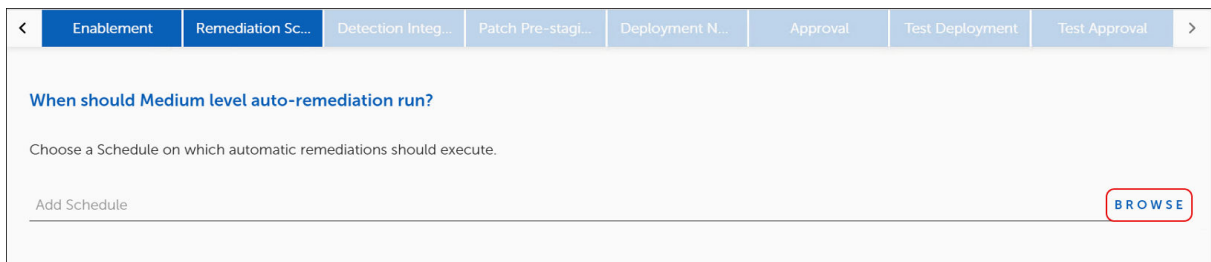
2. Select **Copy From**, and then select a **patch severity level** to copy. The example begins with High level patch remediation, so the available levels available to select are as follows:
 - **Copy Auto Remediation Level Low**
 - **Copy Auto Remediation Level Medium**
 - **Copy Auto Remediation Level Critical**
3. Select OK to return to the **Enablement** tab. The remediation level you started with now uses the same settings as the level you copied.



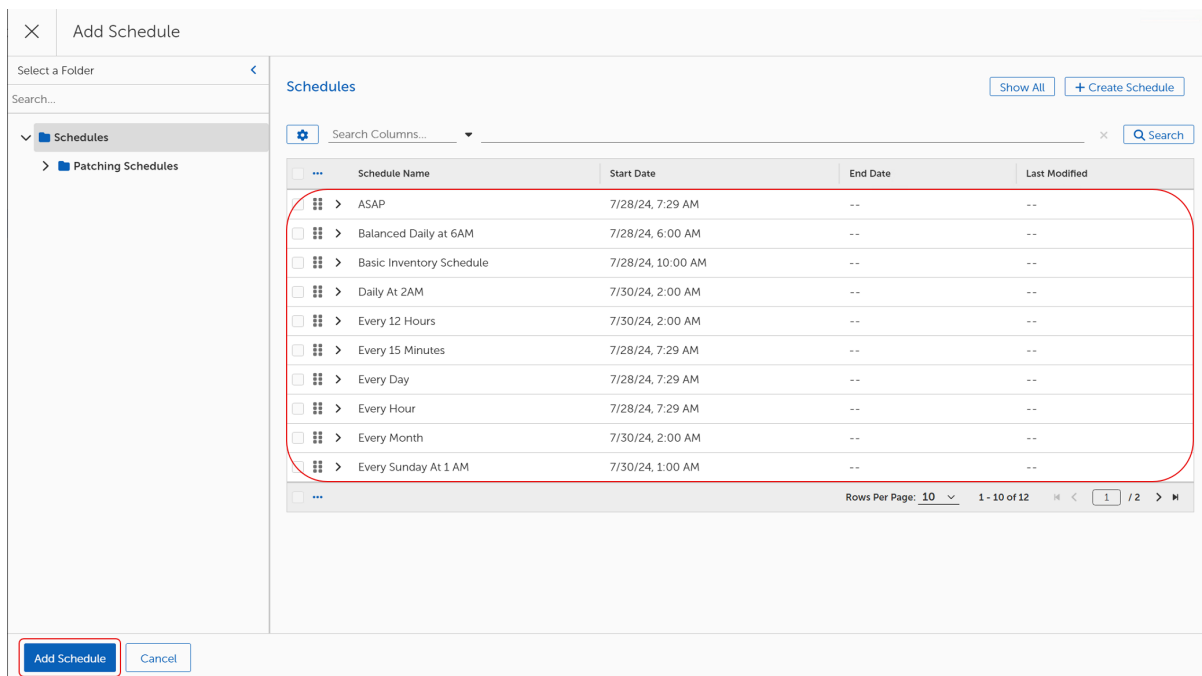
4. To make any changes to the applied settings, click **OK**, and then select the patch severity level you started with, in this case High Patches.
 - a. Select **Yes** to begin cycling through the applied settings.
 - b. Verify that the applied settings used the correct Remediation, Detection, Patch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

Select a Remediation Schedule

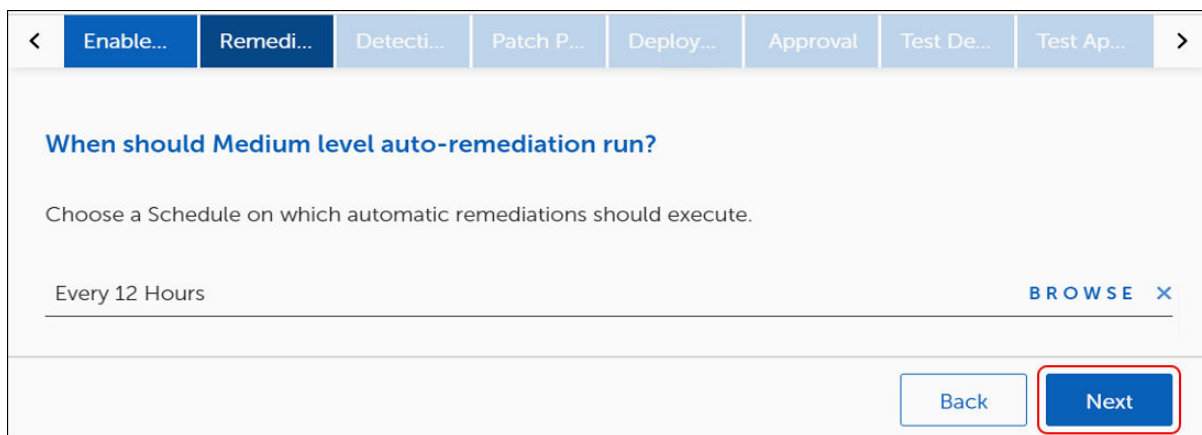
1. Select **Browse** to open the **Add Schedules** dialog.



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



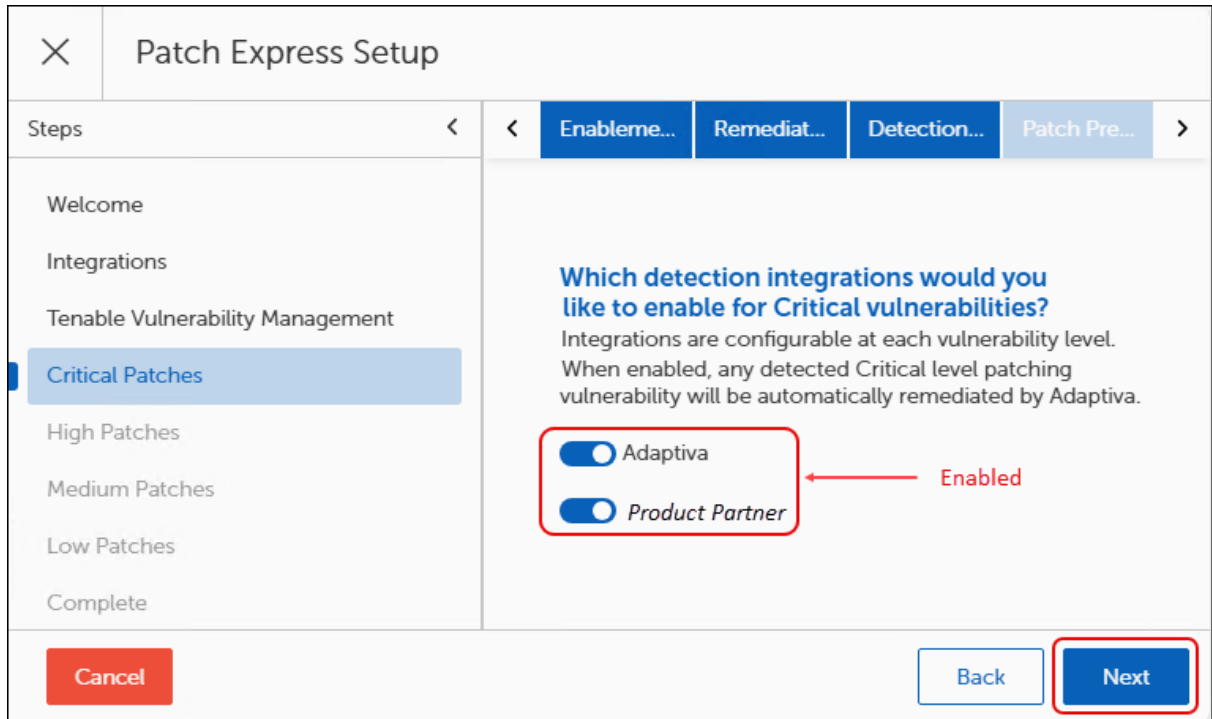
3. Select **Next** to go to the [Detection Integrations](#) step.



Enable Vulnerability Detection

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

1. Select the **Adaptiva** or **Product Partner** toggle to enable or disable one or more of the available Detection Integrations. You must enable at least one.



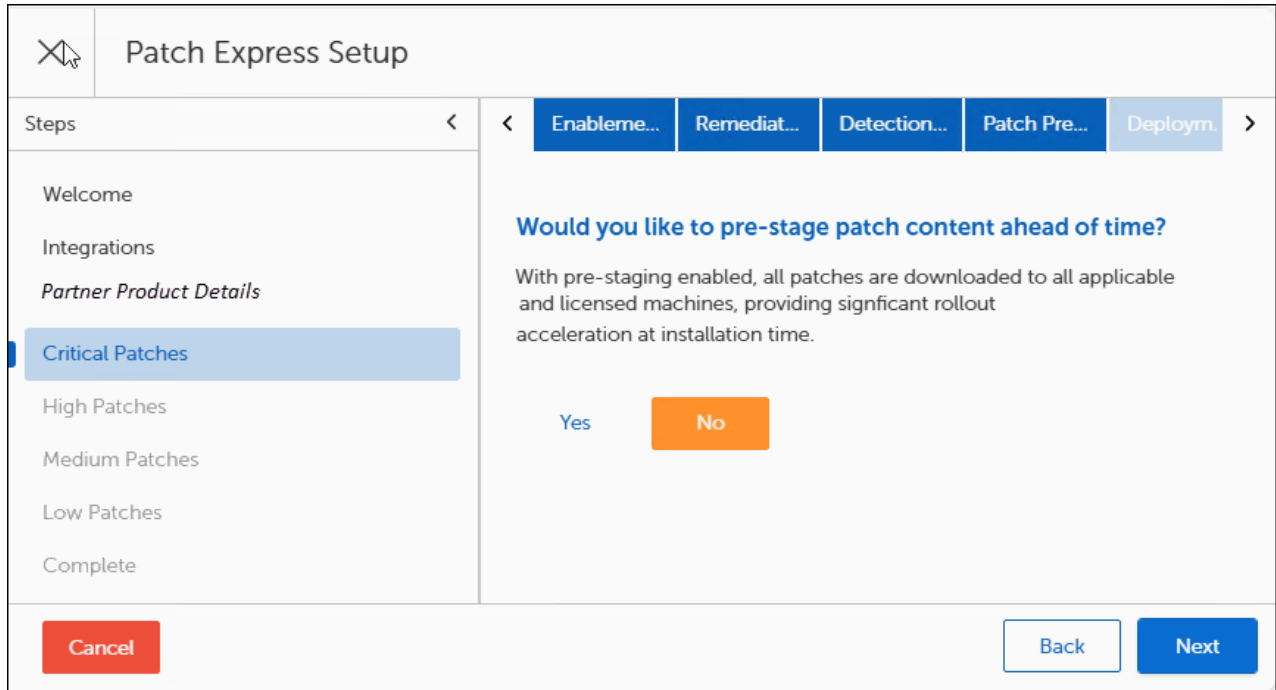
2. Select **Next** to [prestage patch content](#).

Enable Patch Pre-staging

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

Choose whether to pre-stage patches:

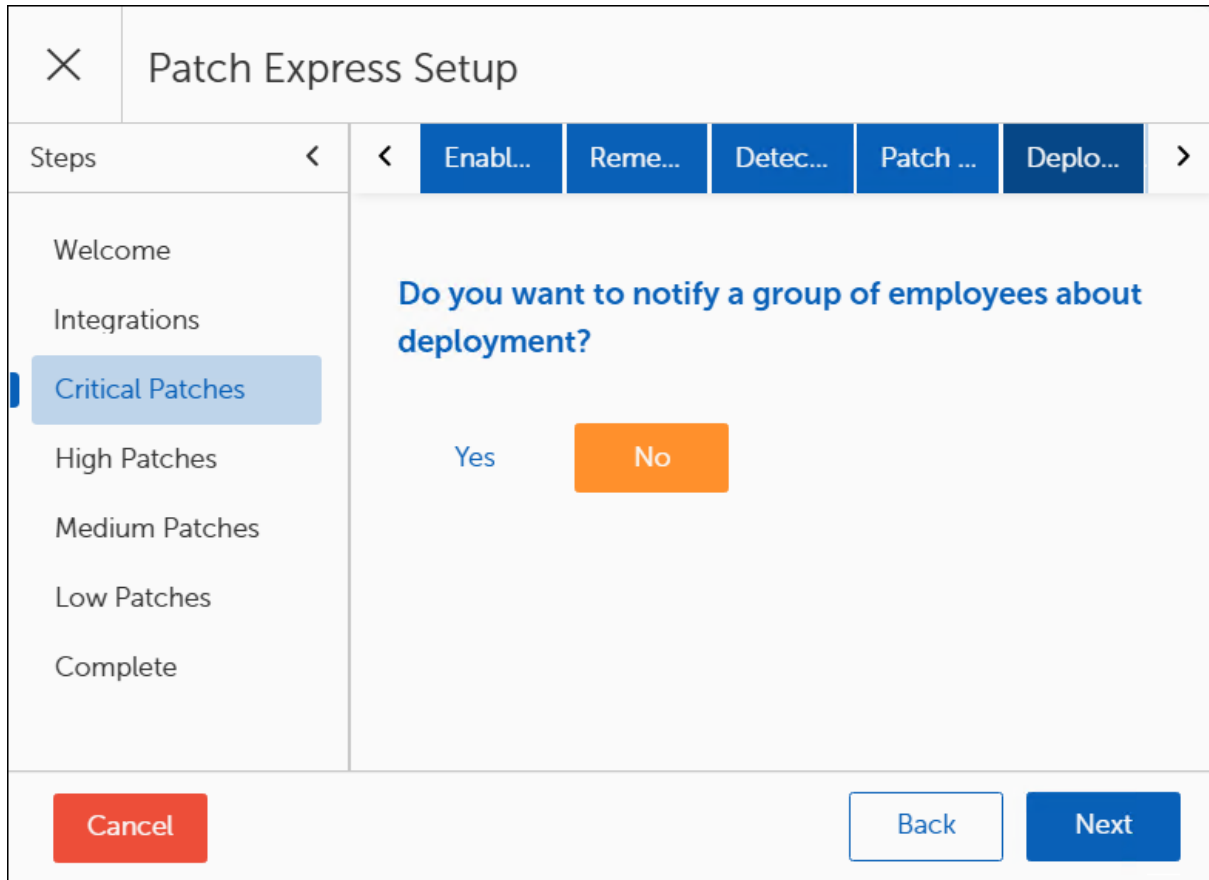
- Select **Yes** to enable patch pre-staging. This takes you to [Configure Deployment Notifications](#).
- Select **No** to skip patch pre-staging. This takes you to [patch approvals](#) (no deployment notification required).
- There is no need to click Next from this tab. If you do click Next, it takes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



Configure Deployment Notifications

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

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



2. Select **Browse** to open the **Add Role** dialog.

The screenshot shows the 'Patch Express Setup' wizard. The 'Steps' sidebar on the left includes: Welcome, Integrations, **Critical Patches** (highlighted), High Patches, Medium Patches, Low Patches, and Complete. The main content area is titled 'Do you want to seek approval before deploying Critical level' and features a 'Yes' button and a 'No' button. Below this is explanatory text: 'If specified, an Adaptiva production patch approval request will be sent to belong to the specified role. Any of the Administrators can approve the re patches to be deployed, then the approval request will not be sent.' At the bottom of this section is an 'Add Role' input field with a 'BROWSE' button to its right. The bottom navigation bar contains 'Cancel', 'Back', and 'Next' buttons.

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

The screenshot shows the 'Add Role' dialog box. On the left, a tree view shows 'Roles' expanded, with 'Metadata Roles' and 'Patch Roles' as sub-items. The main area is titled 'Roles' and contains a table with the following data:

	Name
<input type="checkbox"/>	All Admin Role
<input type="checkbox"/>	Read-Only Admins Role
<input type="checkbox"/>	Super Admin Role

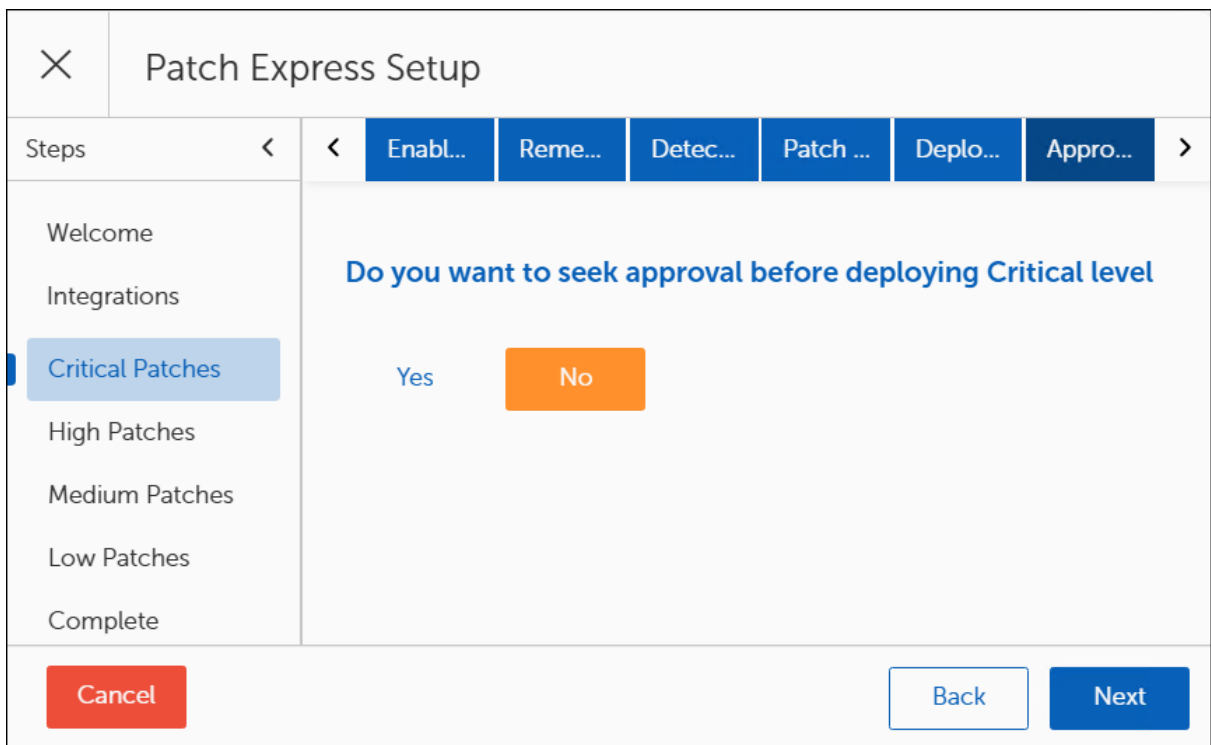
The 'All Admin Role' row is highlighted with a red box. At the bottom left, the 'Add Role' button is also highlighted with a red box. The bottom right of the dialog shows 'Rows Per Page: 10' and '1 - 3 of 3'.

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

Configure Deployment Approval

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

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



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

The screenshot shows the 'Patch Express Setup' wizard. The 'Steps' bar at the top includes 'Enabl...', 'Reme...', 'Detec...', 'Patch ...', 'Deplo...', and 'Appro...'. The left sidebar lists 'Welcome', 'Integrations', 'Critical Patches' (highlighted), 'High Patches', 'Medium Patches', 'Low Patches', and 'Complete'. The main content area asks: 'Do you want to seek approval before deploying Critical level' with 'Yes' and 'No' buttons. Below this, it states: 'If specified, an Adaptiva production patch approval request will be sent to belong to the specified role. Any of the Administrators can approve the re patches to be deployed, then the approval request will not be sent.' At the bottom of this section is an 'Add Role' input field with a 'BROWSE' button. The footer contains 'Cancel', 'Back', and 'Next' buttons.

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

The 'Add Role' dialog box shows a 'Select a Folder' sidebar with 'Roles' expanded, containing 'Metadata Roles' and 'Patch Roles'. The main area is titled 'Roles' and contains a table with the following data:

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

The 'All Admin Role' row is highlighted with a red box. Below the table, there is a 'Rows Per Page: 10' dropdown and '1 - 3 of 3' pagination. At the bottom of the dialog are 'Add Role' and 'Cancel' buttons.

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

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

Approval Timeout

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

0 Days 0 Hours 0 Minutes

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

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

Yes No

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

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

Approval Timeout

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

0 Days 0 Hours 0 Minutes

Back Next

- A non-zero value means deployment begins after the wait time passes, even if no one has approved.
- If you use a zero value, the deployment waits indefinitely for approval.

- (Optional) Enable and set a time frame for Load Leveling:

< **Enablen...** **Remedia...** **Detectio...** **Patch Pr...** **Deploym...** **Approval** >

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

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

Yes **No**

Load Leveling Window

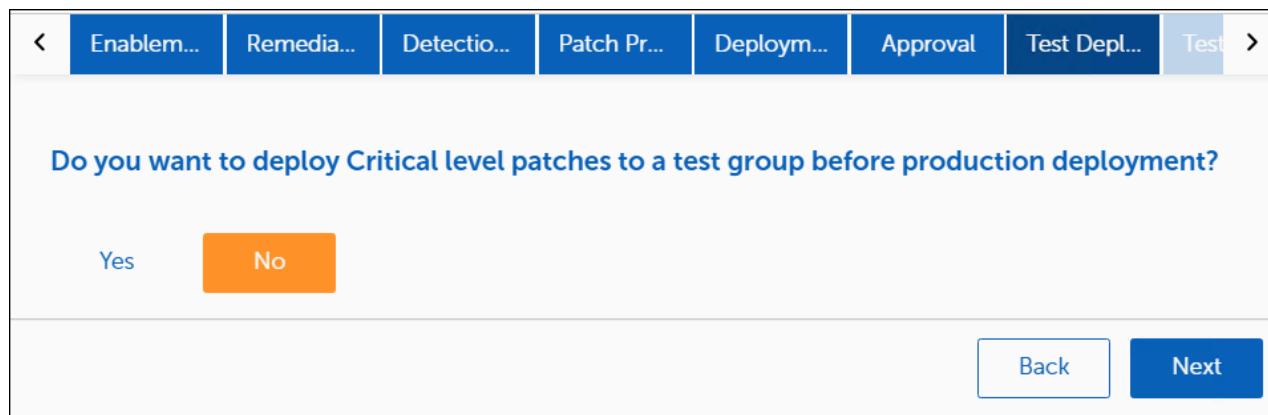
0 Days 0 Hours 0 Minutes

Back **Next**

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

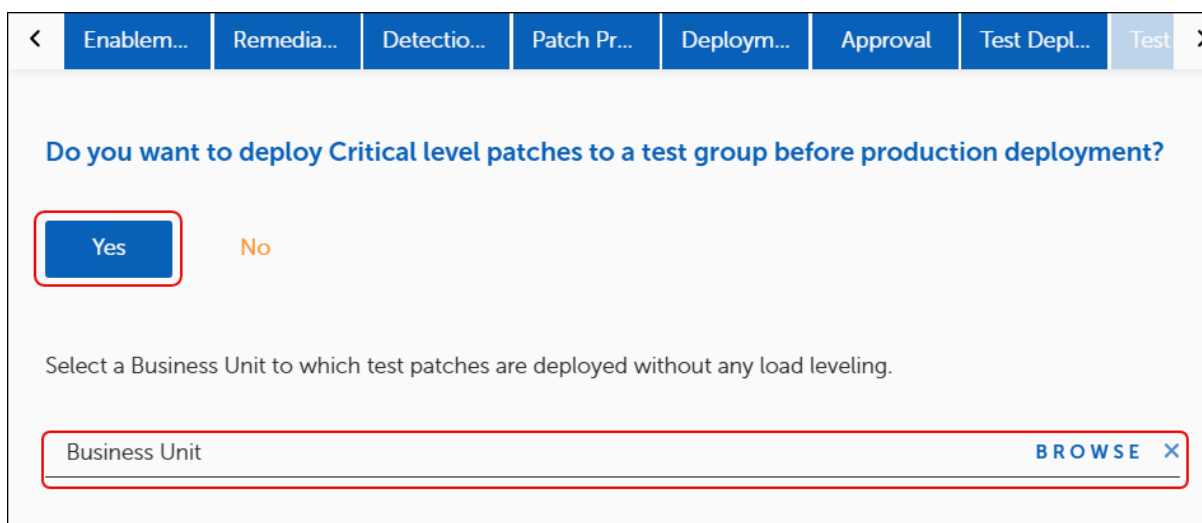
Configure Test Deployment

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



The screenshot shows a wizard interface with a navigation bar at the top containing tabs: < Enablem..., Remedia..., Detectio..., Patch Pr..., Deploym..., Approval, Test Depl..., and Test >. The main content area displays the question: "Do you want to deploy Critical level patches to a test group before production deployment?". Below the question are two buttons: "Yes" and "No". The "No" button is highlighted in orange. At the bottom right, there are "Back" and "Next" buttons.

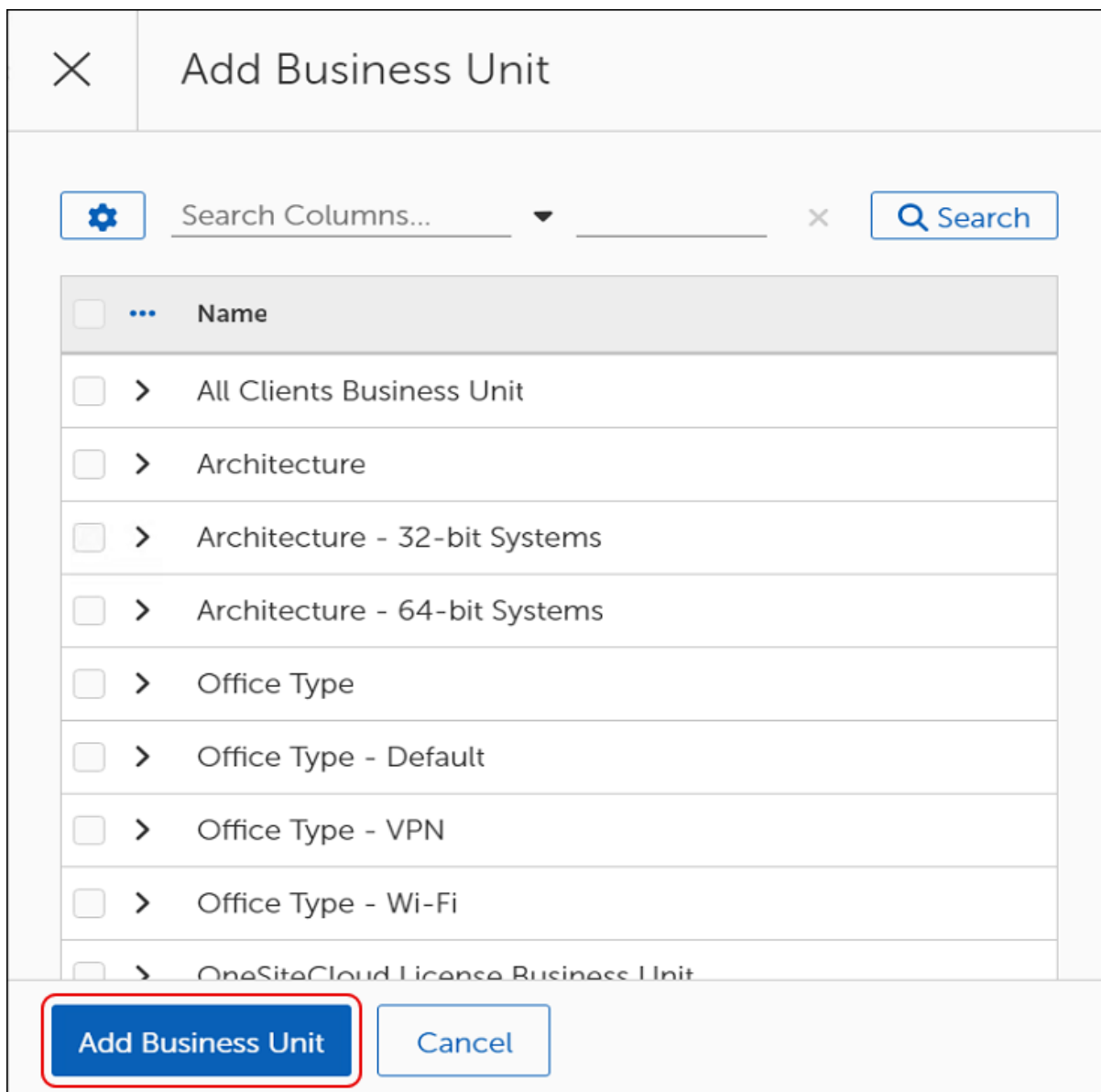
1. Decide whether to deploy the patch installation to a test group (recommended):
 - Select **Yes** to configure test group installation, and then continue with the next step.
 - Select **No** to skip setting up a test environment and have all vulnerability patch installations deploy to the production environment.
This takes you back to the [Enablement](#) tab where you can configure remediation for a different vulnerability level.
 - Select Next on the bottom right corner to skip setting up a test environment and go directly to test approvals.
2. Select **Browse** to show the available Business Units.



The screenshot shows the same wizard interface as above, but with the "Yes" button highlighted with a red box. Below the buttons, the text reads: "Select a Business Unit to which test patches are deployed without any load leveling." Below this text is a text input field with the placeholder "Business Unit" and a "BROWSE X" button on the right. The "BROWSE" button is highlighted with a red box.

3. Select the **Business Unit** to use as the test environment, and then click **Add Business Unit** on the bottom left corner of the dialog:
 - Patches deployed to a test environment do not use load leveling.

- If Patch Pre-staging is enabled, the patch is pre-staged to all target machines, and then the machines assigned to the business unit that you specified for the test deployment.



4. Choose whether to create preferences or test duration:

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

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

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

+ Create Preferences

Test Deployment Duration

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

0 Days 0 Hours 0 Minutes

Back Next

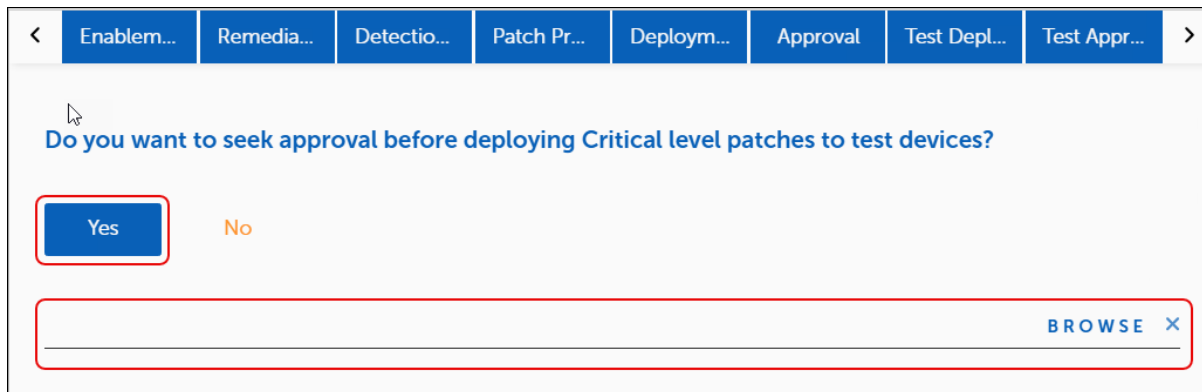
- To create preferences, click **+ Create Preferences** to control maintenance windows, user interaction settings, and reboots for the selected test environment. See [Patching Preferences](#) for configuration guidance.
- To create a test duration (Optional), set the number of **Days**, **Hours**, or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

5. Select **Next** to set test approval requirements.

Configure Test Approval

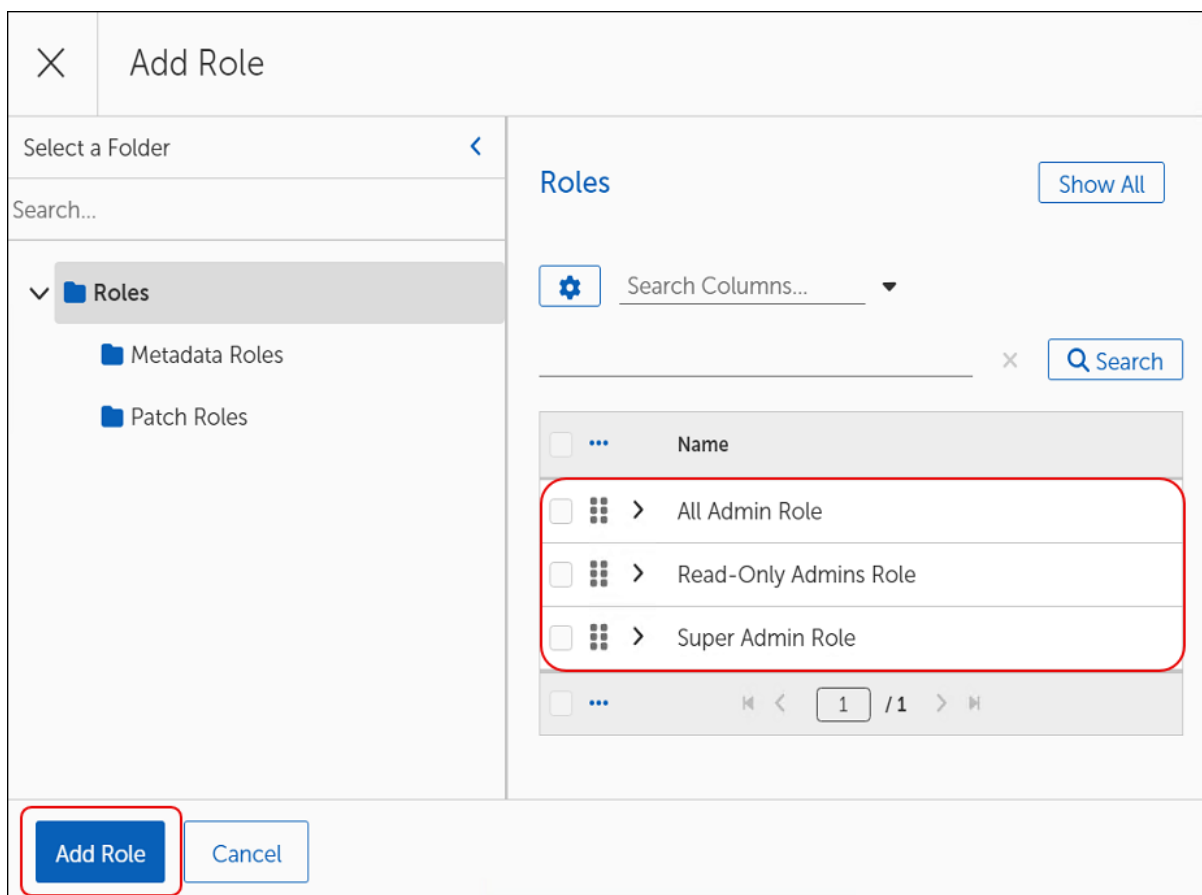
Decide whether to ask administrators to approve of deploying the patch installation to a test environment and select the type of administrators to approve based on Roles.

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



The screenshot shows a navigation bar with tabs: Enablem..., Remedia..., Detectio..., Patch Pr..., Deploym..., Approval, Test Depl..., and Test Appr... The main content area contains the question: "Do you want to seek approval before deploying Critical level patches to test devices?". There are two buttons: "Yes" (highlighted with a red box) and "No". Below the buttons is a text input field with a "BROWSE" button and a close icon (X).

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



The screenshot shows the "Add Role" dialog box. On the left, there is a "Select a Folder" section with a search bar and a tree view showing "Roles" expanded, with sub-items "Metadata Roles" and "Patch Roles". On the right, the "Roles" section has a "Show All" button, a "Search Columns..." dropdown, and a "Search" button. Below this is a table with a "Name" column and three rows: "All Admin Role", "Read-Only Admins Role", and "Super Admin Role". The table has a pagination bar at the bottom showing "1 / 1". At the bottom of the dialog, there are "Add Role" and "Cancel" buttons, with "Add Role" highlighted by a red box.

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

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

Approval Timeout

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

0 Days 0 Hours 0 Minutes

Back Next

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

Complete OneSite Patch Express Setup

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

✕ Patch Express Setup

Steps <

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

That's it. Ready to start patching?

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

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

Cancel **Back** **Finish**

Best Practices for Patch Express

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

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

Adaptiva recommends customizing a few administrative items before you begin.

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

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

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

Integrate Defender

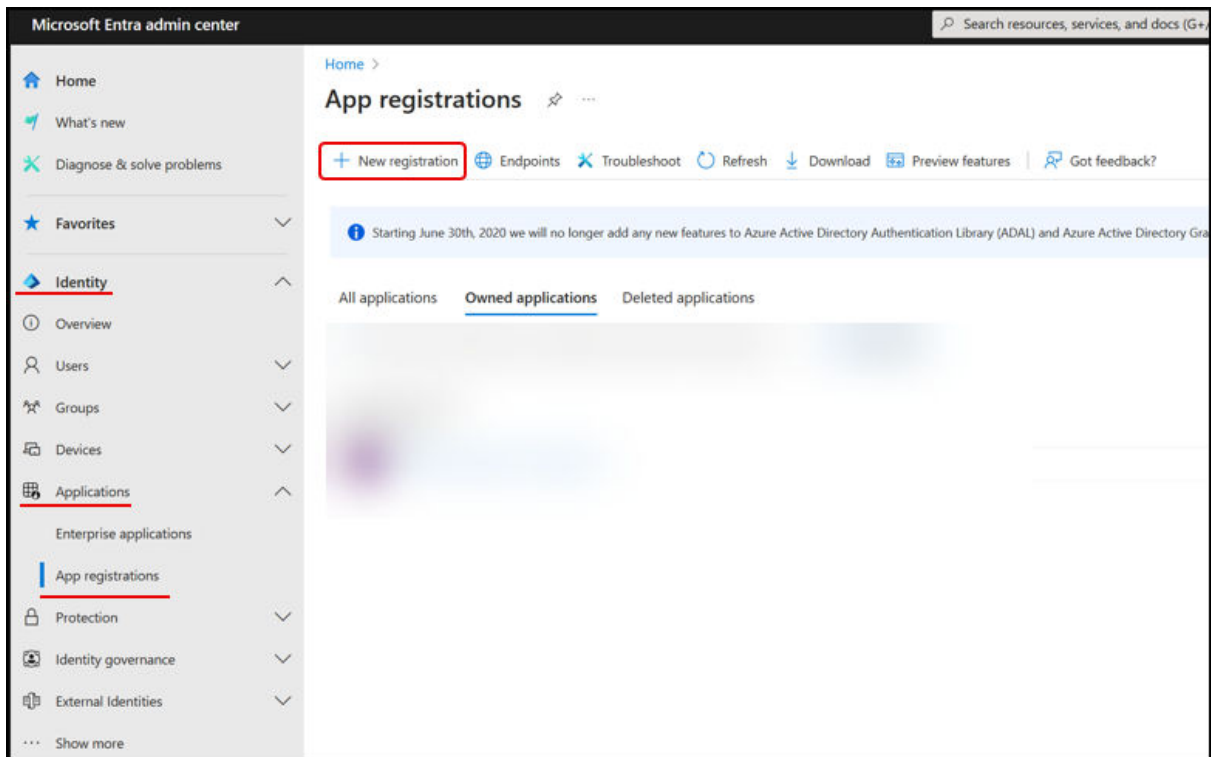
Integrating Microsoft Defender with requires the following Microsoft Entra ID information:

- Tenant ID (the existing Directory ID for the Entra customer).
- Application ID (a configured application Client ID for the Entra customer).
- Client Secret (a configured authentication for content sharing between OneSite Patch and Entra).

Create a Microsoft Entra Application

To integrate Microsoft Defender with , begin with registering an application with Microsoft Entra ID and creating a service principle.

1. Sign in to your **entra.microsoft.com** account as an administrator.
2. Browse to **Identity > Applications > App registrations**, and then select **New registration**.



3. Enter the following details into the form:

Home > App registrations > Register an application

Name

The user-facing display name for this application (this can be changed later).

Demonstration Application ✓

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (adaptivamatrixlab only - Single tenant)

Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform

By proceeding, you agree to the [Microsoft Platform Policies](#)

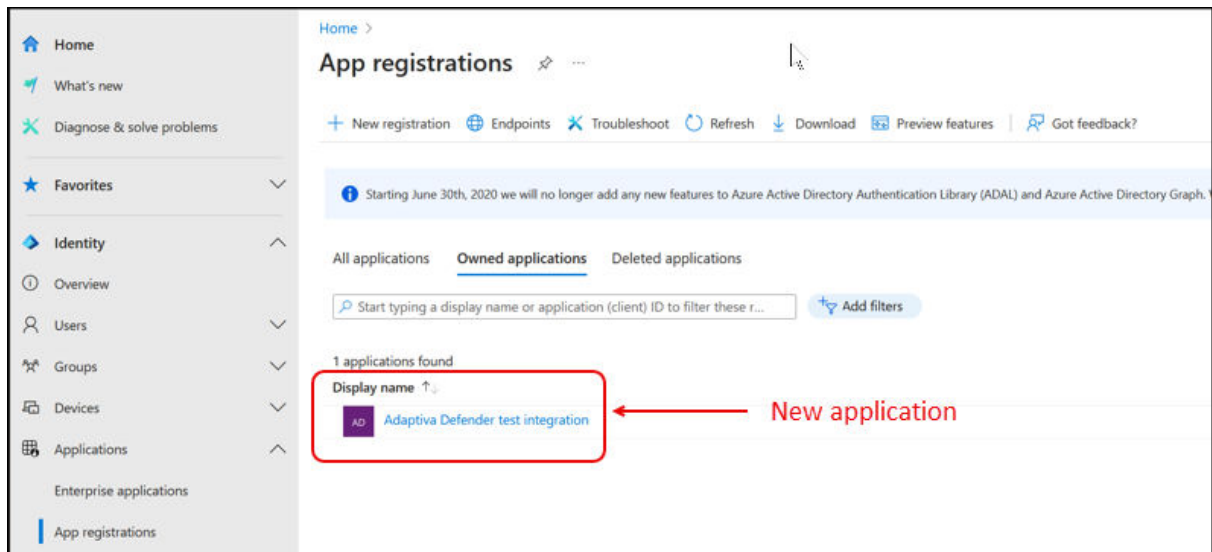
Register

- a. Enter a **Name** that identifies the Adapтива integration.
 - b. Select **Accounts in this organization directory only** under Supported account types.
 - c. Skip both **Redirect URI** and **Service Tree ID**. If you must enter something for the **Redirect URI**, select **Web**.
4. Select Register to create the application.
 5. [Add the necessary permissions](#).

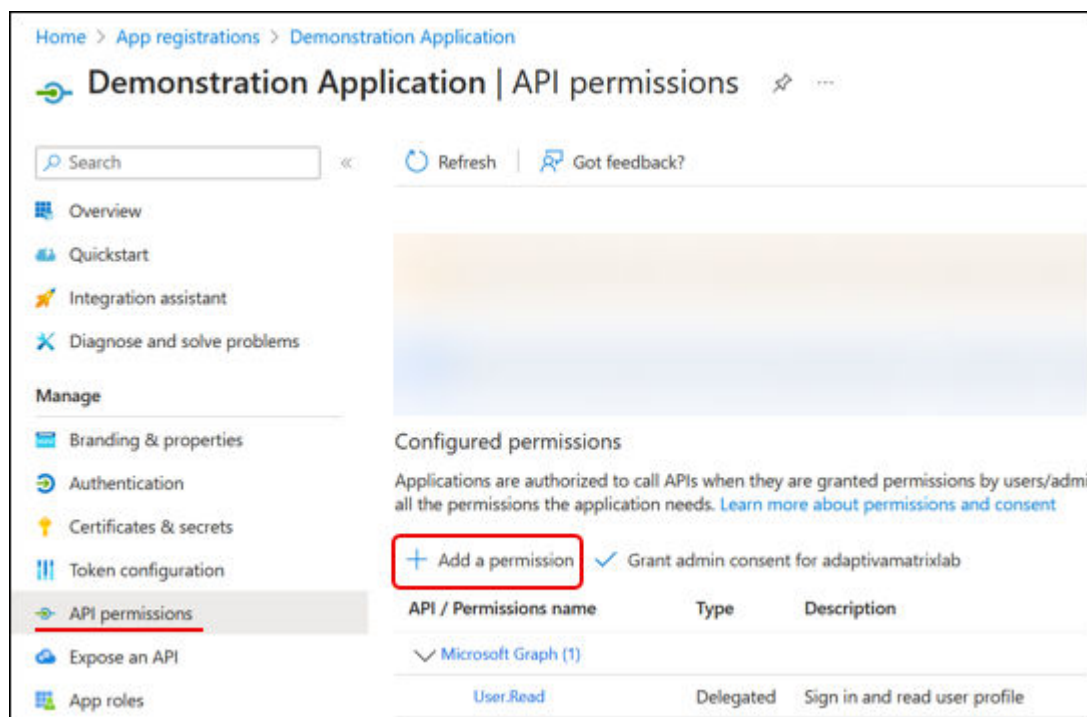
Add Permissions to an Entra Application

After [creating the new Entra application](#), use the following steps to add the `Vulnerability.Read.All` permission from **Add registrations**. Make sure you are logged in as an administrator.

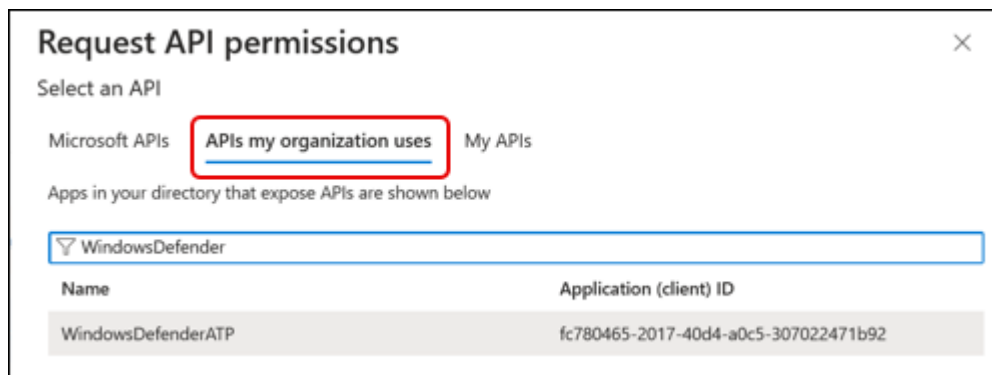
1. Access the API Permissions workspace from the App registrations page:



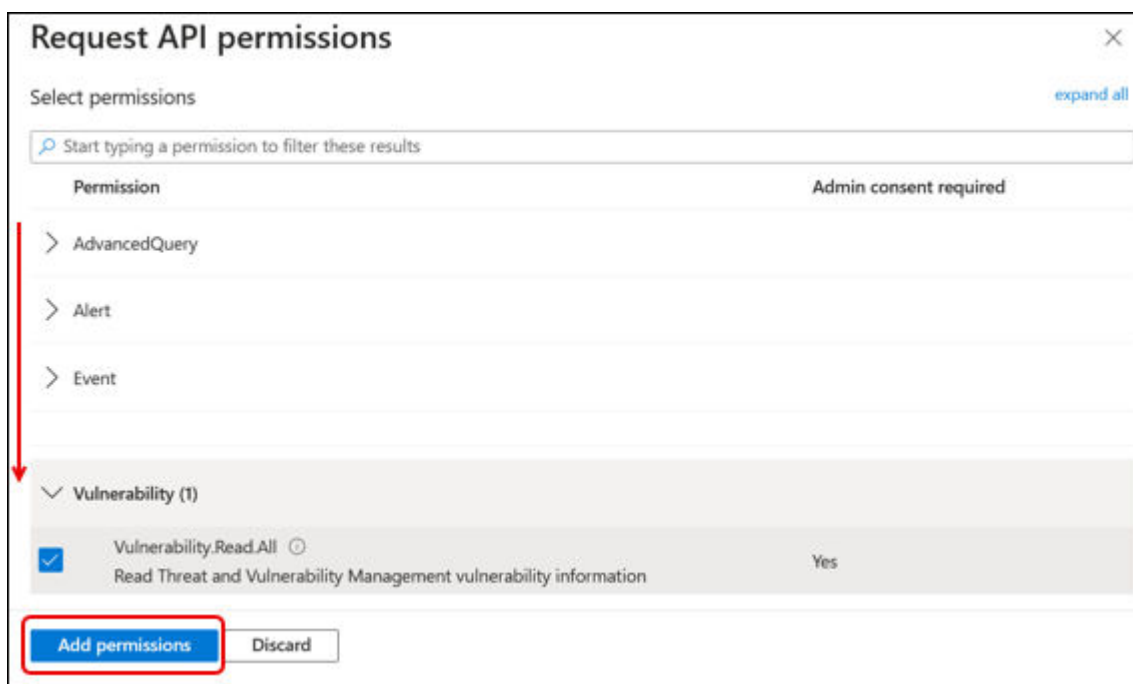
- Select the **Name** of the newly created application on the **App registrations** page. This opens the application and a new list of menu options.
- Select **API permissions** on the left navigation menu, and then click **Add a Permission**.



This opens the **Request API Permissions** workspace.



2. Select **APIs my organization uses**, and then locate **WindowsDefenderATP** in the list.
3. Select **WindowsDefenderATP**, and then select **Application permissions**.

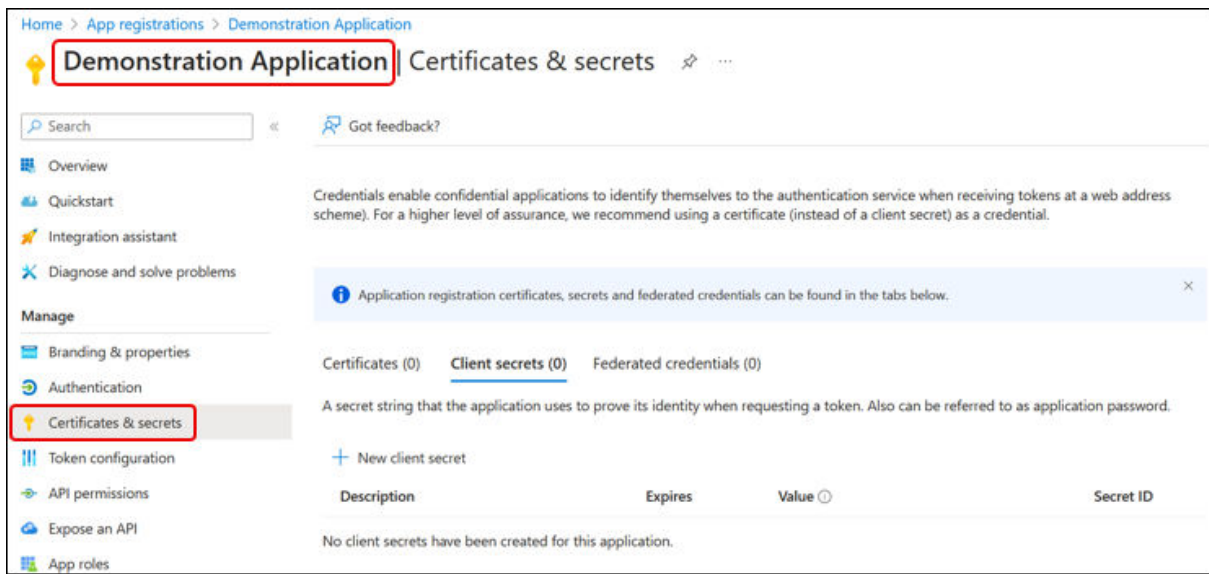


4. Scroll down to and expand **Vulnerability**, and then select **Vulnerability Read All**.
5. Select Add Permissions. If prompted, follow the required steps to provide administrator consent to make the change.
6. [Create a Client Secret ID](#) for the application.

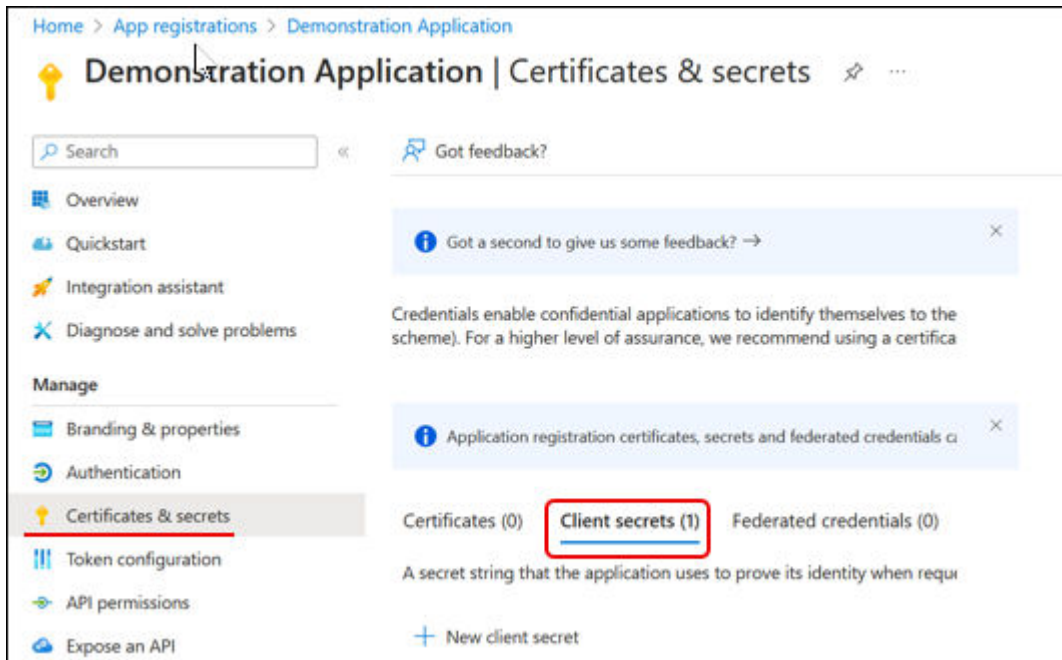
Create a Shared Secret ID

After creating an application and adding permissions, use the following steps to create a shared secret ID. The secret ID enables authentication between OneSite Patch and Windows Defender for the application you created.

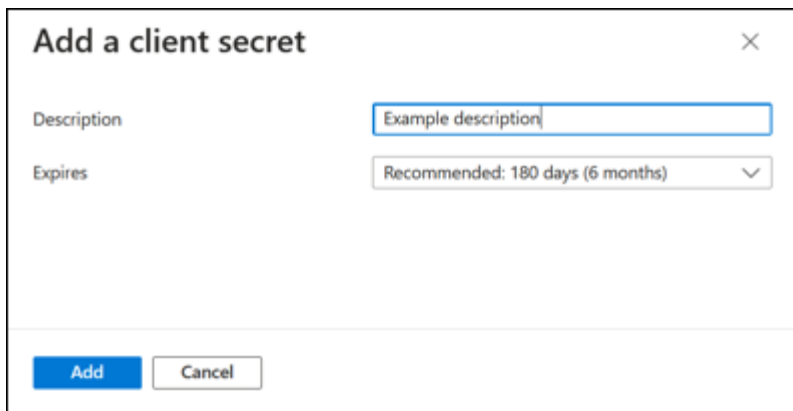
1. Select **Certificates & secrets** on the **Manage** menu for the open application.



2. Select **Client secrets**.



3. Select **+ New client secret**. This opens the **Add a client secret** dialog:



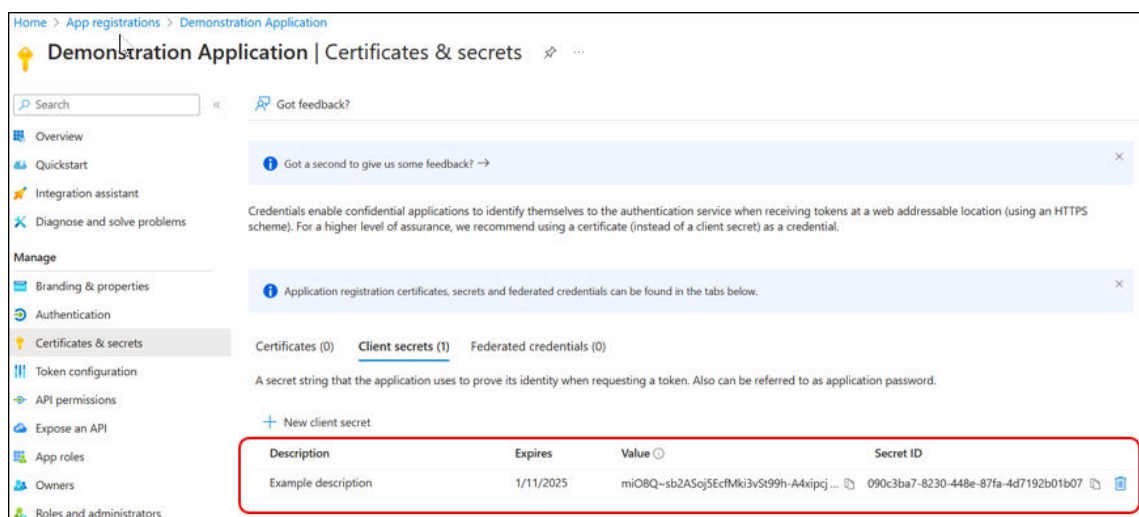
Add a client secret

Description: Example description

Expires: Recommended: 180 days (6 months)

Add Cancel

- Enter a Description of the secret.
- Select an Expires timeline.
- Select Add to save your changes and return to the Certificates & secrets workspace.



Home > App registrations > Demonstration Application

Demonstration Application | Certificates & secrets

Search Got feedback?

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems

Manage

- Branding & properties
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
Example description	1/11/2025	miOBQ-sb2ASoj5EcfMki3vS99h-A4xipcj ...	090c3ba7-8230-448e-87fa-4d7192b01b07

4. Copy and save the **Value** and **Secret ID** information.



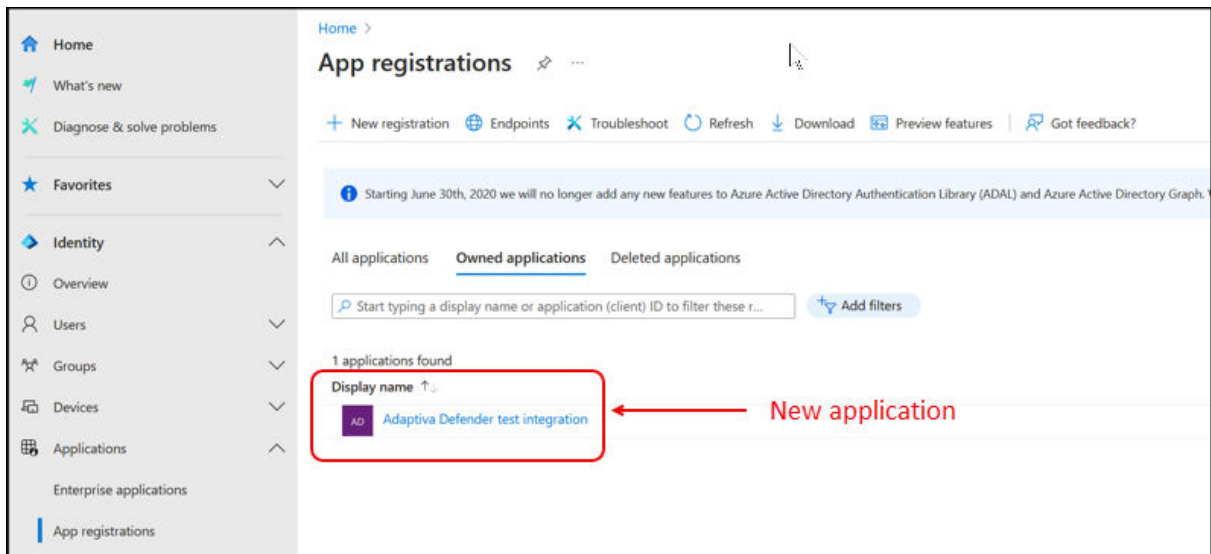
IMPORTANT

The system does not save this information when you leave this window. Be sure to record these numbers and save them to an accessible location for later use.

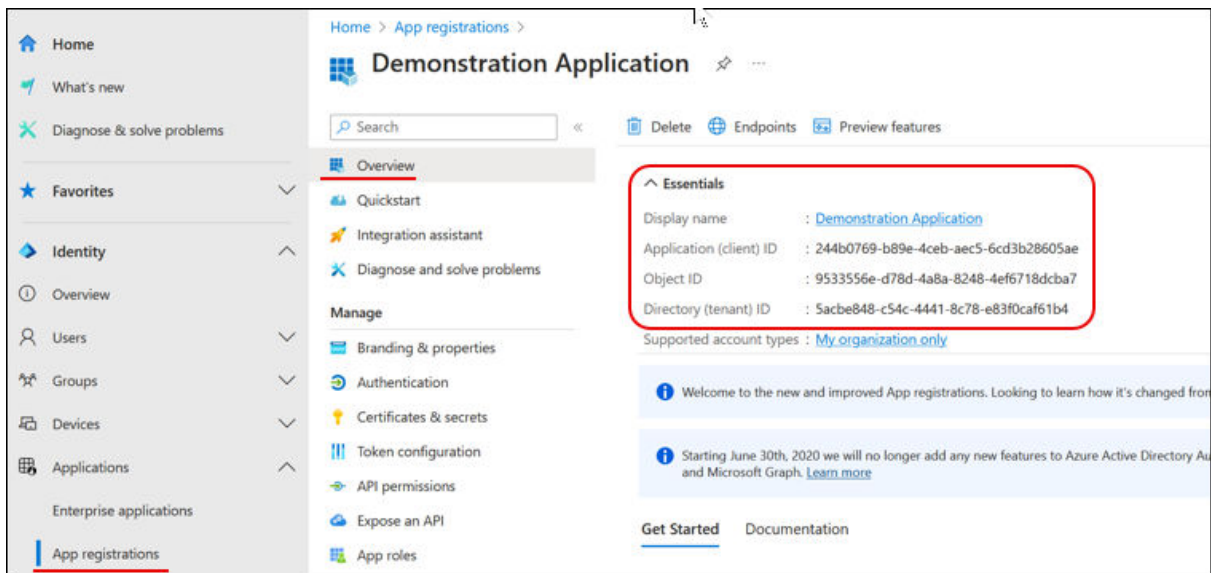
5. Gather the [integration details](#) you have created.

Locate and Record the Microsoft Entra IDs

1. Sign in to your entra.microsoft.com account as an administrator.
2. From the **Home** page, navigate to **Applications > App Registrations**, and then open the application you created for integration.



3. Select **Overview** on the left navigation of the application workspace, and then expand the **Essentials** section.



4. Record the following identification information:
 - Client ID
 - Tenant ID (Directory (tenant) ID)

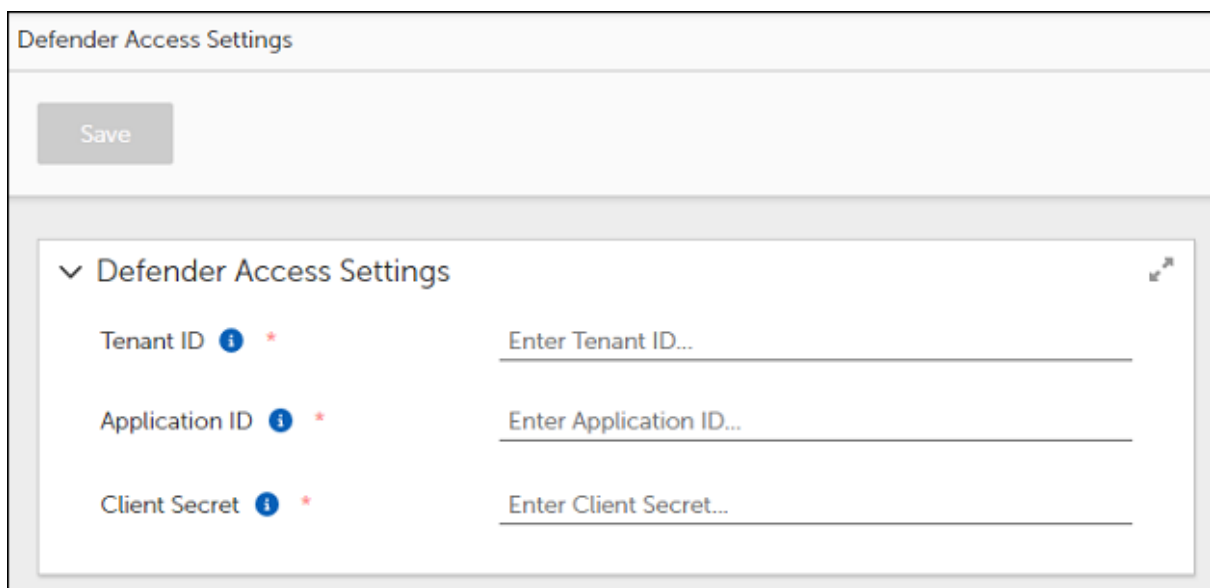
- Secret ID
5. Complete the [integration with AdapTiva OneSite Patch](#).

Integrate Defender with OneSite Patch

1. Select **Windows Defender Endpoint** on the left navigation menu of the OneSite Patch dashboard.



This opens the Defender Access Settings workspace.

A screenshot of the 'Defender Access Settings' workspace. At the top left is a 'Save' button. Below it is a section titled 'Defender Access Settings' with a dropdown arrow and a refresh icon. This section contains three rows of input fields. Each row has a label on the left, an information icon (i), and a red asterisk (*). The labels are 'Tenant ID', 'Application ID', and 'Client Secret'. The input fields contain placeholder text: 'Enter Tenant ID...', 'Enter Application ID...', and 'Enter Client Secret...'.

2. Enter the ID information gathered from [Microsoft Entra](#), and then click **Save** on the upper left.

Defender Access Settings

Save

▼ Defender Access Settings ↻

Tenant ID ⓘ * <Entra Tenant ID>

Application ID ⓘ * <Entra Application ID>

Client Secret ⓘ *

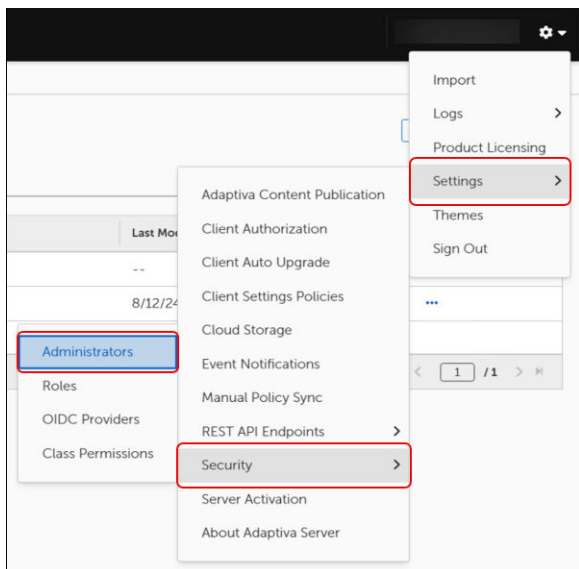
Administrators and Roles

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

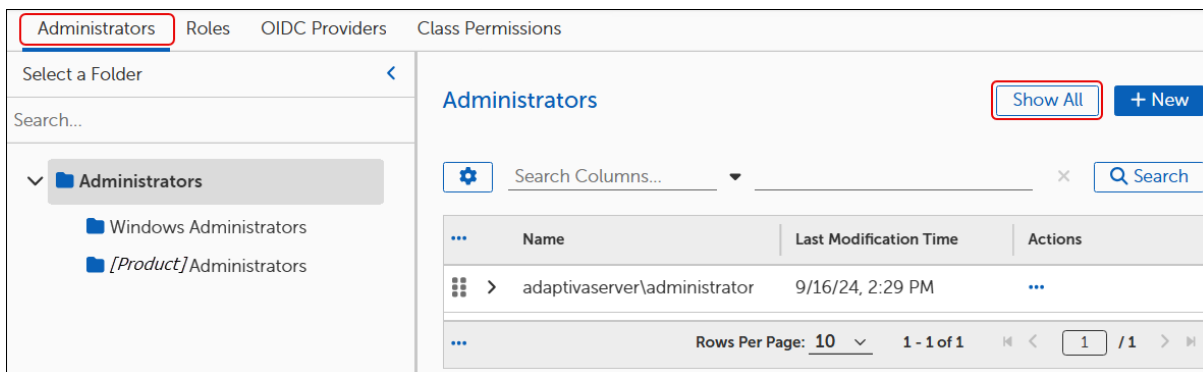
After integrating Defender with OneSite Patch, you can view your list of Microsoft Defender users and assigned roles for your integrated hosts. To make any changes to Administrators or Roles, you must use the Microsoft Defender product.

Access Security Settings

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

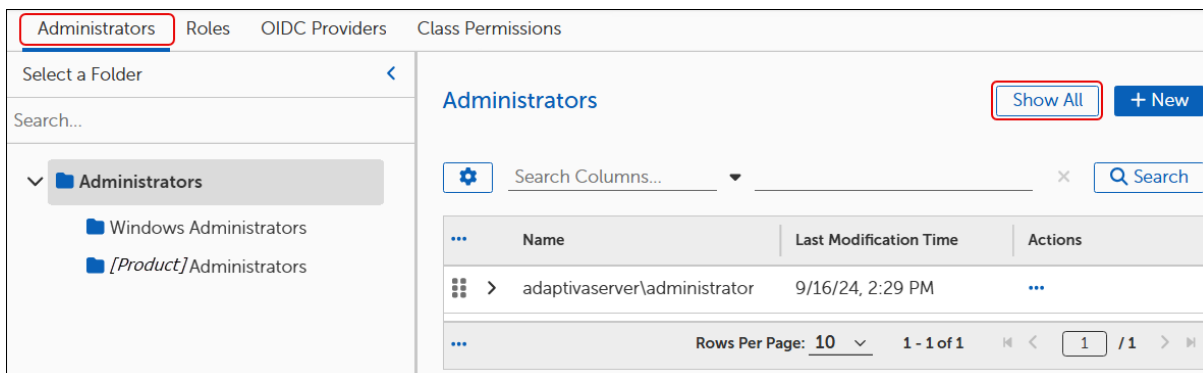


3. Select **Show All** to view existing administrators.



View Administrators

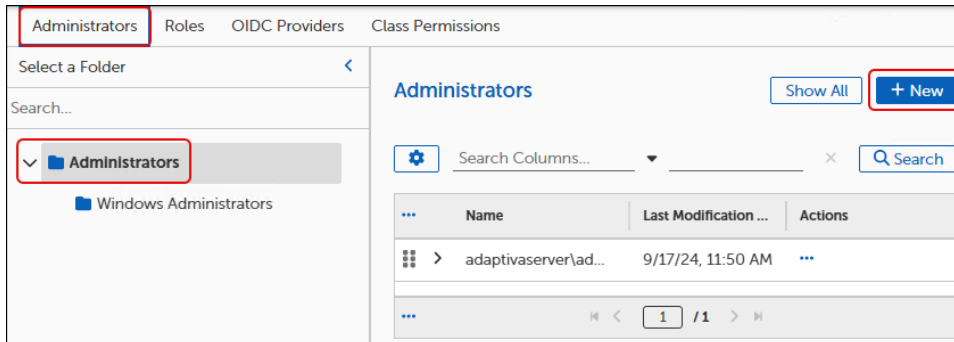
1. Select an **Administrators** folder from the Administrators tab of [Security Settings](#).



2. Select **Show All** to list all Administrators in the selected folder.
To make any changes to Administrators, you must use the Defender product.

Create a New Administrator

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



2. Enter the **Administrator Details**:
 - a. Select the **Admin Type** login from the list. Adaptilva recommends Windows Active Directory.

The screenshot shows the 'Administrator Details' form. It includes fields for 'Admin Type', 'Email Address *', 'Password *', and 'Confirm Password *'. The 'Admin Type' dropdown menu is open, displaying a list of options: 'Adaptiva', 'Adaptiva', 'Windows AD', and 'OpenID Connect'. The first 'Adaptiva' option is selected and highlighted with a red box. Below the dropdown are input fields for 'Password' and 'Confirm Password'.

- b. Enter the email address and login details for the new administrator.
3. Enter the **User Details**:
 - a. Add the **Name** and contact details for the new administrator.
 - b. Choose country codes from the drop-down lists for phone numbers.

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

4. Assign **Direct Roles**:

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

Direct Roles ⓘ
 Roles

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

- High level roles include **All Admin Role**, **Read-only Admin Role**, and **Super Admin Role**.

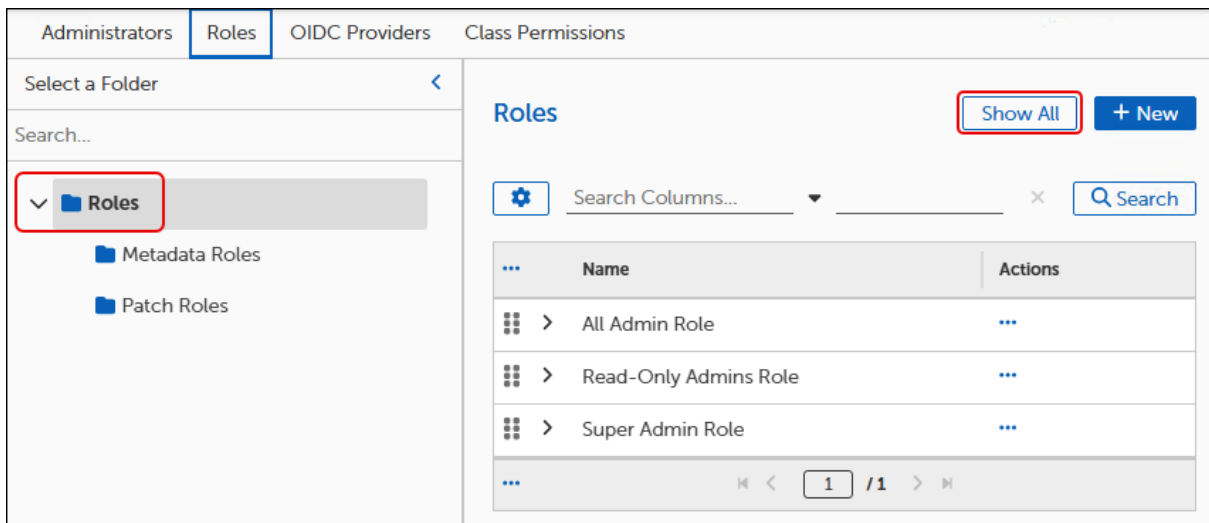
Manage Roles
 Select a Folder <
 Search...
 Roles
 Metadata Roles
 Patch Roles
 Roles
 Search Columns... Search
 Name
 All Admin Role
 Read-Only Admins Role
 Super Admin Role
 Rows Per Page: 10 1 - 3 of 3 1 / 1
 Manage Roles Cancel

- Patch Express roles include **Patch Express Administrator**.
- To create additional roles, you must use the Defender product.

- c. Select **Manage Roles** on the bottom-left corner of the dialog to return to the .
5. Select **Save** at the top left to save the new administrator.
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.

View Roles

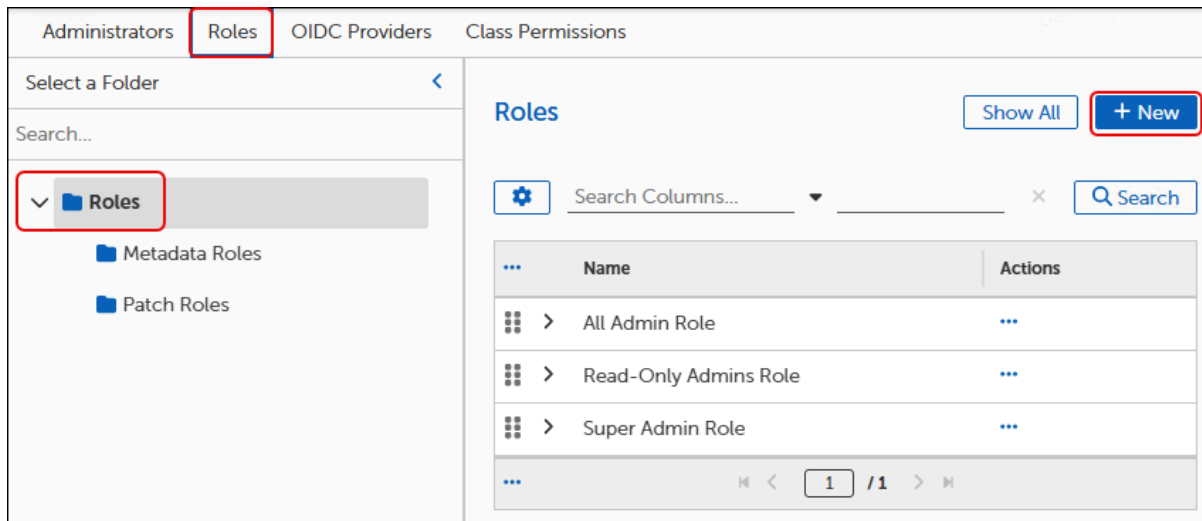
1. Select a **Roles** folder from the Roles tab of [Access Security Settings](#).



2. Select **Show All** to list all Roles in the selected folder.
To make any changes to Roles, you must use the Microsoft Defender product.

Create a New Role

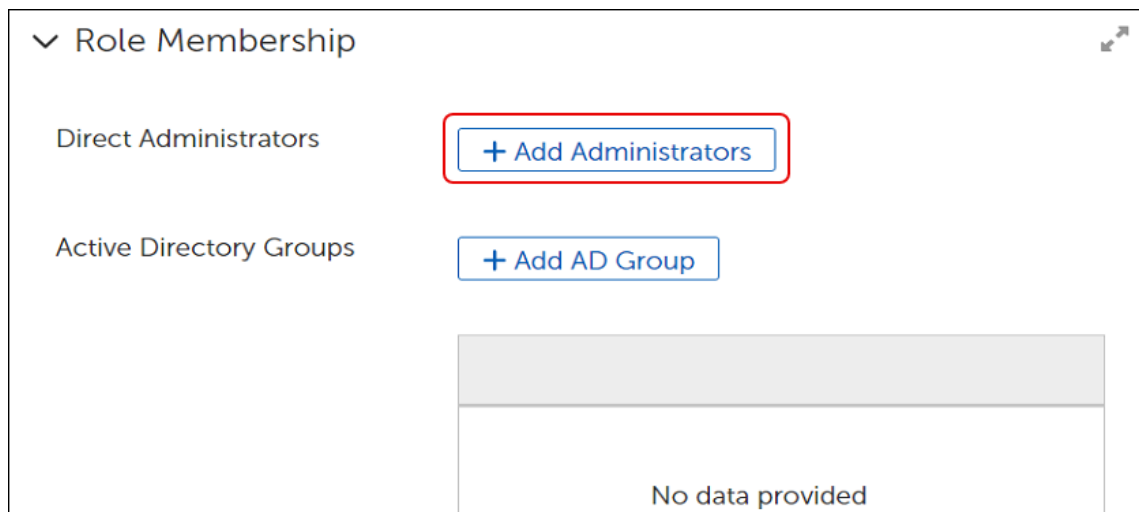
1. Select a **Roles** folder from the Roles tab of [Security Settings](#), and then select **+ NEW** to open a new Role template.



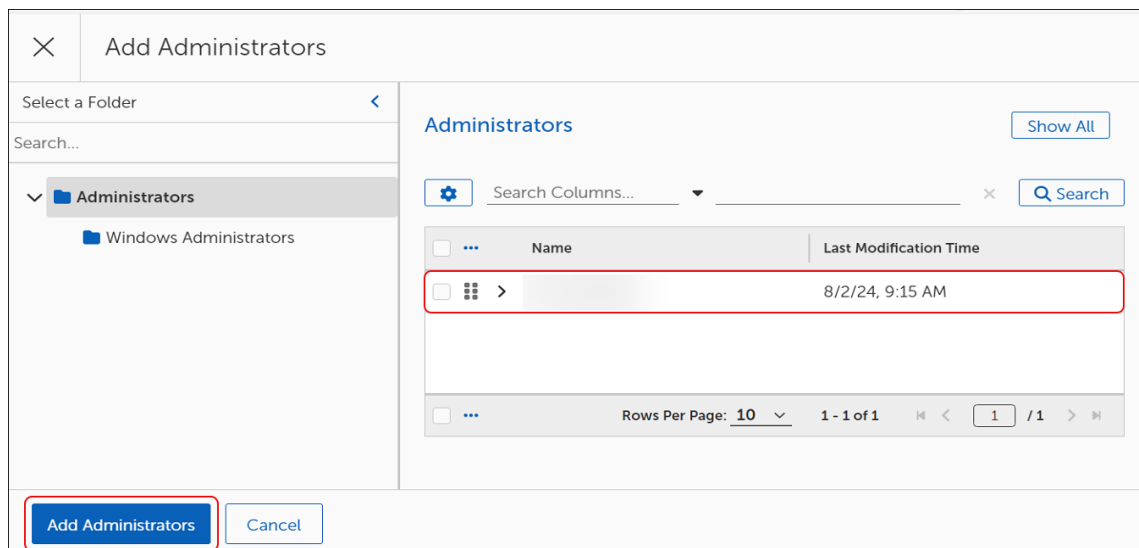
2. Enter a **Role Name** and a detailed **Role Description** in the **Role Properties** workspace.



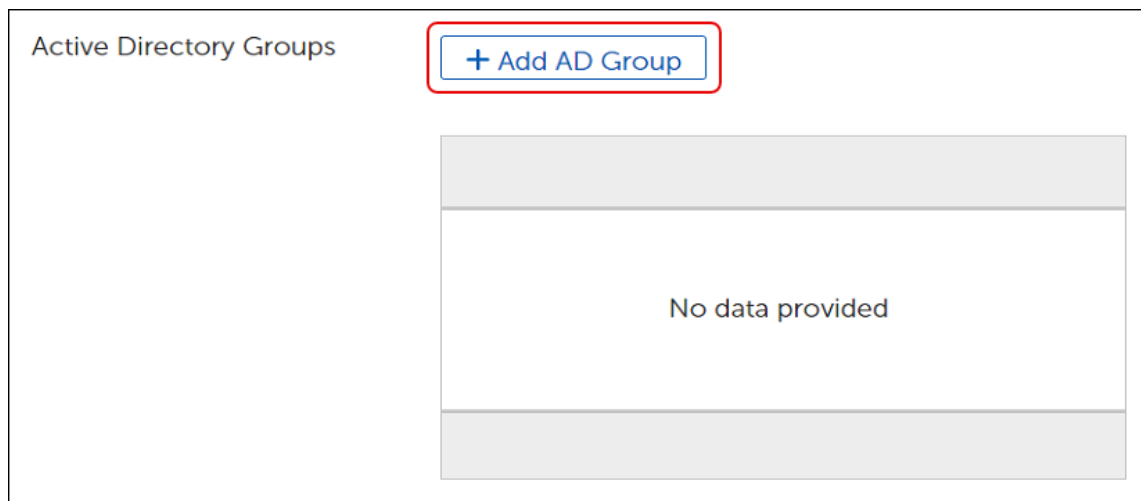
3. Add one or more **Direct Administrators** in the **Role Membership** section:
 - a. Select **Add Administrators** to open the **Add Administrators** dialog.



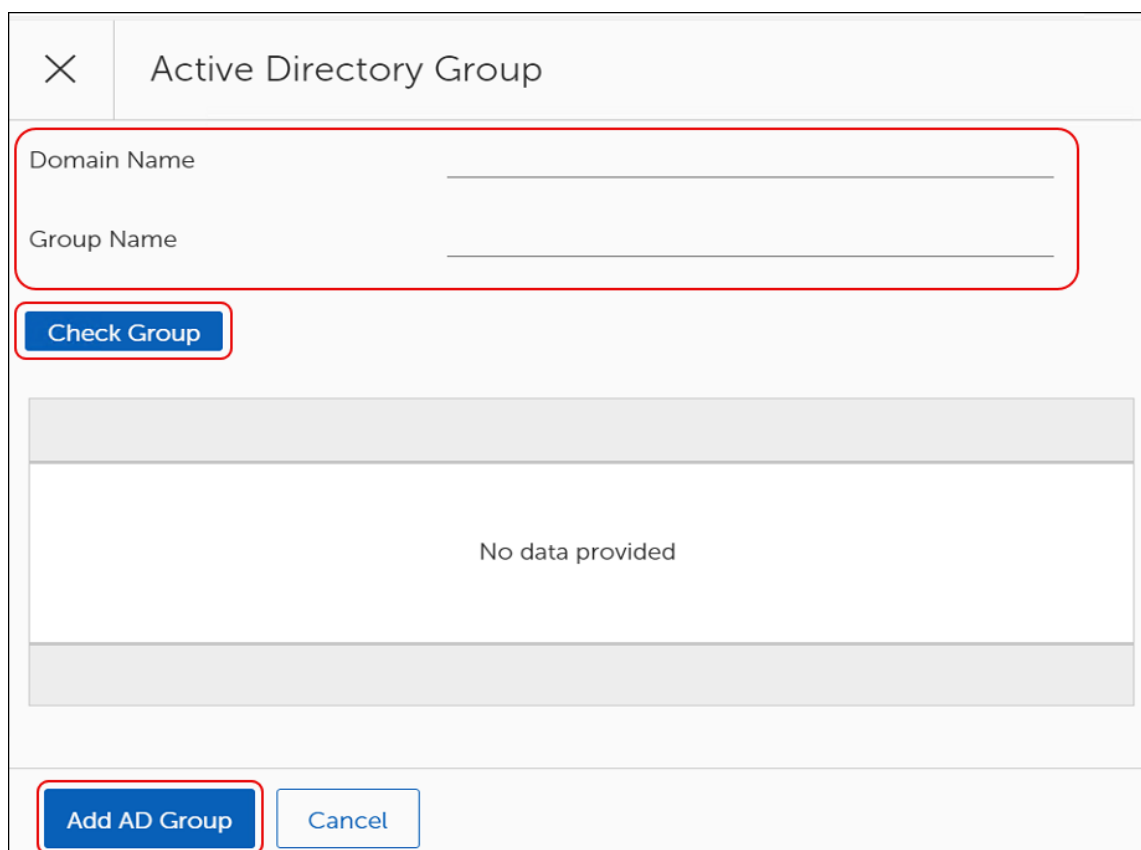
- b. Select one or more administrators from the table for the new role.



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



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



- c. Select **Add AD Group** to return to the Role template.
5. Select **Save** at the top left to save the new role:
- a. Check the **Error View** and resolve any errors.

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

Menu Objects for OneSite Patch

The OneSite Patch menu in 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 Integrations and Platform in the left navigation menu of the OneSite Patch dashboard. For descriptions of each menu item, see [OneSite Patch Menus](#).

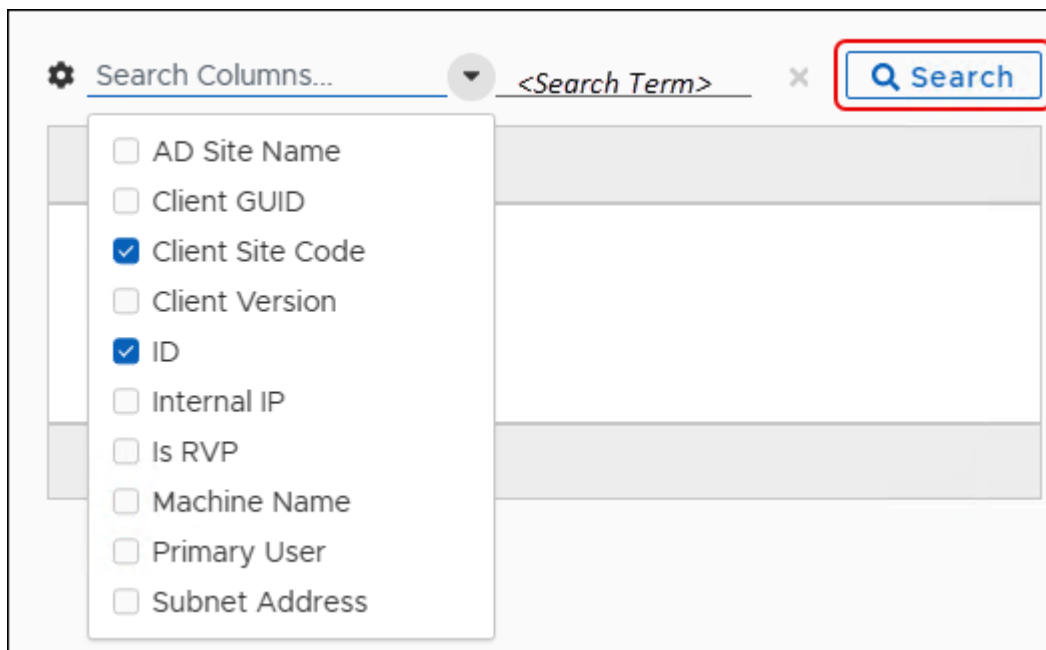
Patching Analytics Dashboards

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

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

Using Search in OneSite Patch

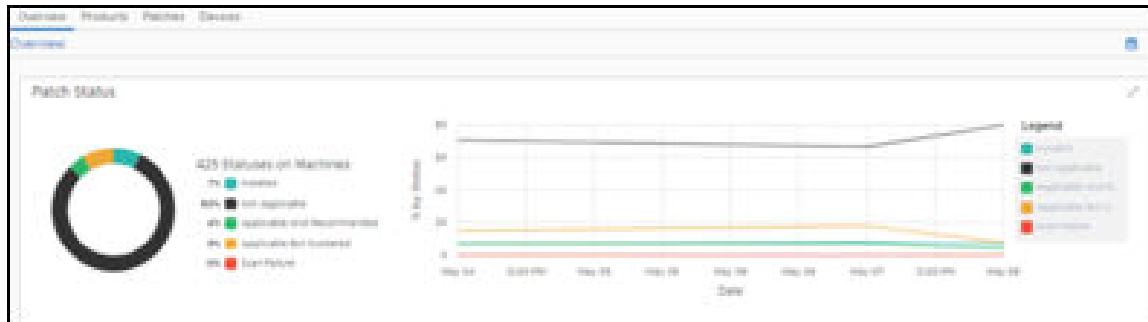
For tables in any dashboard view, the drop-down list next to **Search** allows you choose a column to search within. This provides several options for searching depending on the search term you have selected. Column choices change depending on the menu object.



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.

Product Status

Search Columns

Product Name	Product Name	Publisher	Patc...	Mach...	Devic...	Comp...	Risk ...	Actions
1Password v64	1Password ...	Ablebits Inc.	38	0	0	100%	0	→

ID 1000000270

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

Percentage Installed On

Strategies Including this Product 0

Average Risk Score 0

Risk Contribution 0

Criticality 50

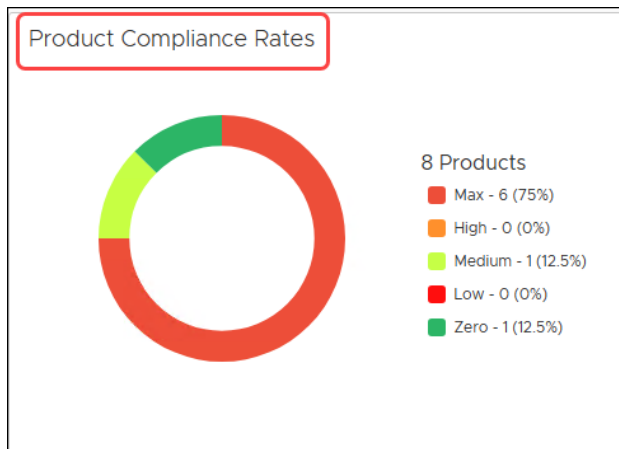
Products View

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

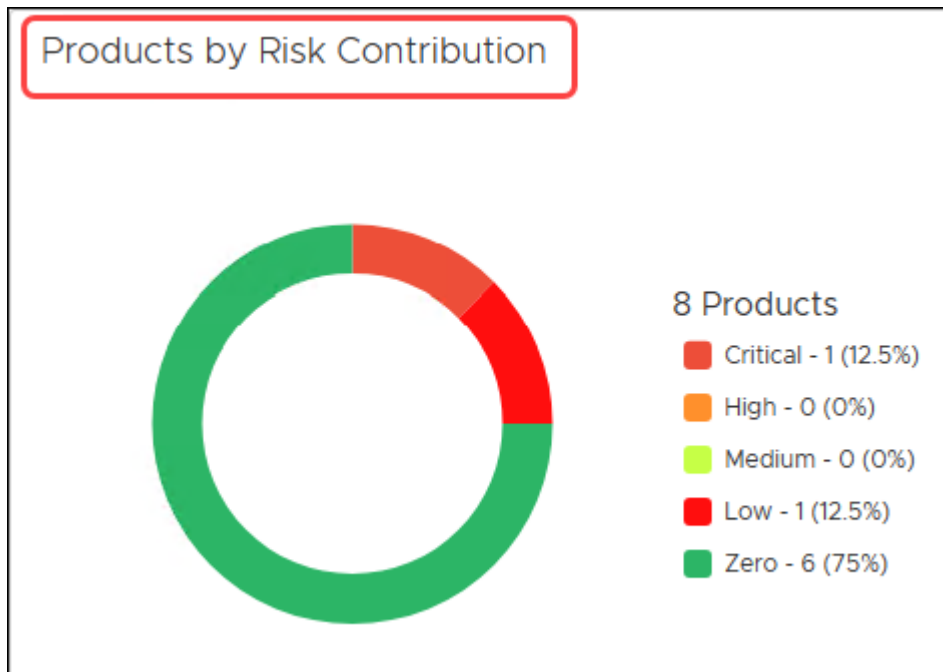
Product Metrics tracks supported products, detected products, and patching requirements, and provides a visual indication of product patching over time.



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



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

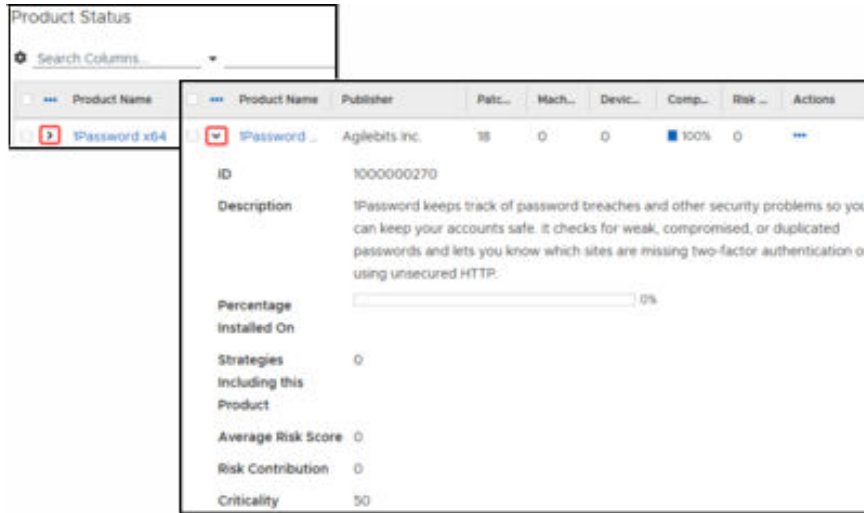


Active Product Deployments for products provides the number of products undergoing patch and the percentage of completion.



Product Status is a table that lists each product that 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.



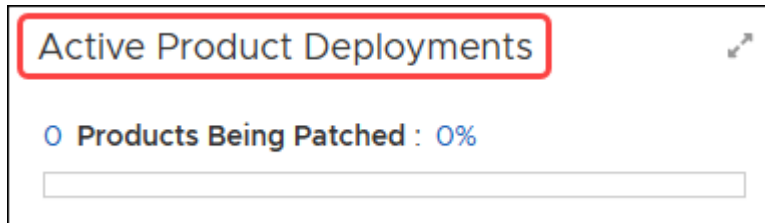
Patches View

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.



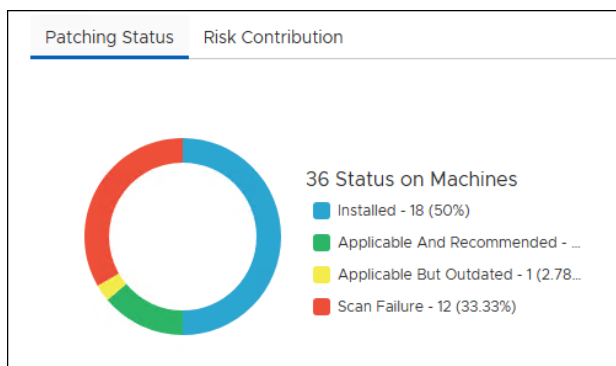
Active Product Deployments provides the number of patches undergoing installation and the percentage of completion.



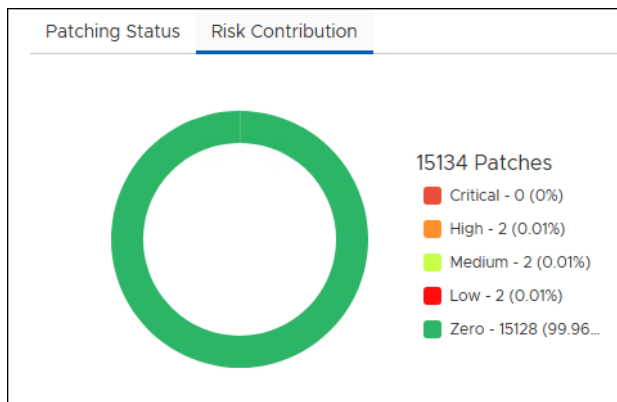
Patch Trends includes two tabs, one for Patching Status and one for Risk Contribution.



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.

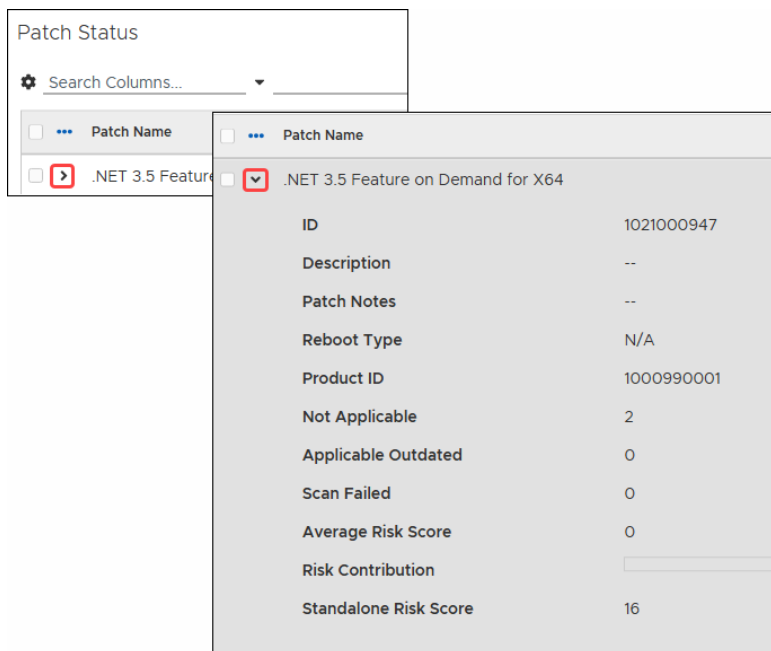


Top 10 Most Critical Patches tracks the risk contribution of the top ten most critical patches in the environment.

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

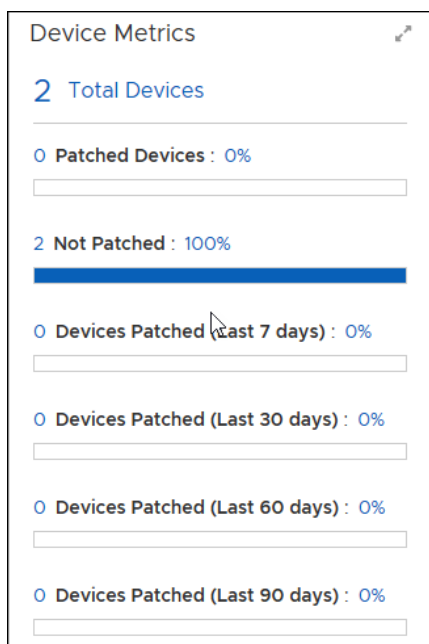
Patch Status is a table that lists each patch that OneSite Patch looks for during a scan, the installation/applicability status of each, and the status, compliance, and Risk Score for each.

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



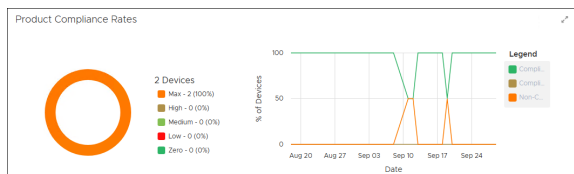
Devices View

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.

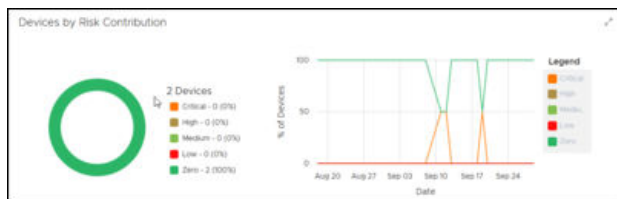


The **Product Compliance Rates** for Devices shows the rate of compliance for each device in the environment based on the latest device scan information. The graph

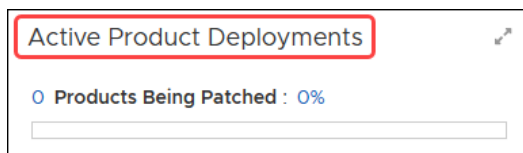
displays the percentage of devices that fall into each category of compliance (max, high, medium, low, and zero), and the line graph shows compliance trends over time.



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.

Device Status

Search Columns...

Device Name	Compliance	Risk Score	Risk Contribu...	Proc
adaptivaserver	67%	153	60%	6

adaptivaserver

- Device ID: 2
- Primary User: ADAPTIVASERVER\Administrator
- IP Address: [Redacted]
- Client Version: 9.0.963.2
- Last Check In: 11/29/23, 6:11 PM
- Operating System: Microsoft Windows Server 2022 Standard
- Location: No Office
- Compliant Products: 4
- Non-Compliant Products: 2
- Applicable Patches / Releases: 4

Flex Controls

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

Blacklisting	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 Blacklisting .
Cycle Operations	Includes access to Patching, Deployment, and Rollout Cycle details. Details include a graphical representation of any cycles in progress and a table that lists details for each cycle in progress. Also includes a graphical representation of previously completed cycles and a table that lists a each completed cycle. Select each completed cycle to review details. See Cycle Operations .
Exceptions	Allows administrators to exclude Business Units from specific updates on certain products or to use settings to maintain all endpoints at a specific version of a product. See Patching Exceptions .
Global Pause	Use Global Pause to pause or resume all patching activities for specified software products and patches. Affects all clients contained in one or more specified Business Units. See Global Pause .
Rollbacks	Create a Rollback object to rollback one or more patches to a system determined or specified version. See Rollbacks .

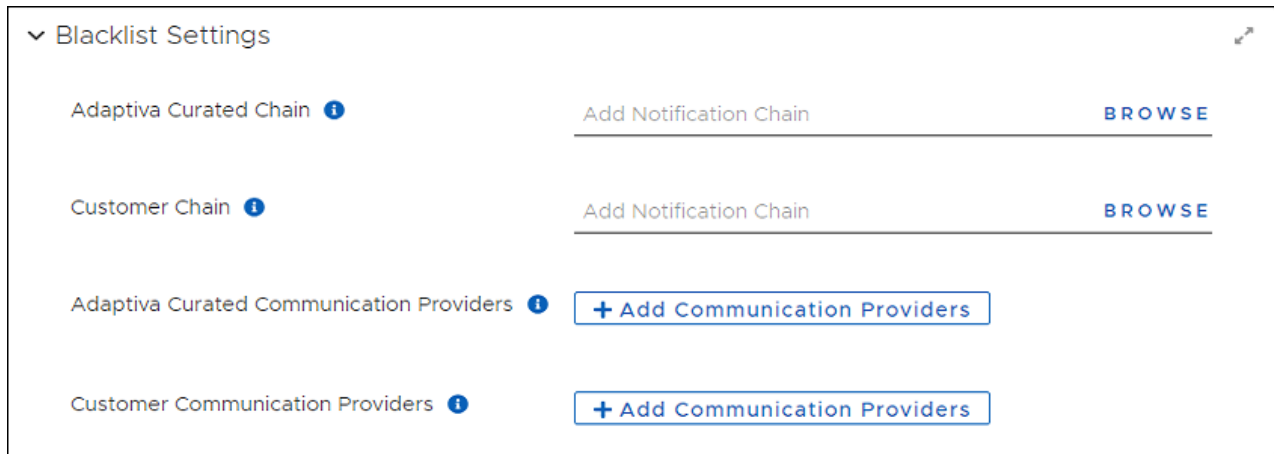
Blacklisting

includes an extra level of protection for customer devices and patching processes called Blacklisting. 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 team blacklists patches and products that have issues and automatically creates an exclusion for the patch on all clients. Blacklisting prevents the download and installation of potentially damaging content to customer devices.

Blacklist Settings

The Blacklist 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 blacklisted patches. See [Managing Blacklist Notification Settings](#).



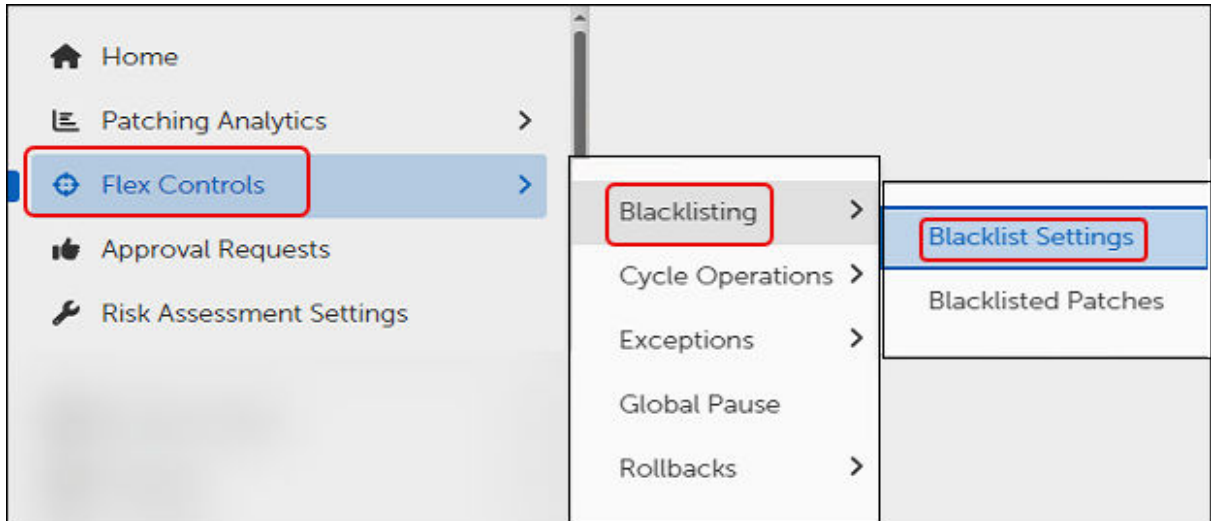
Managing Blacklist Notification Settings

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

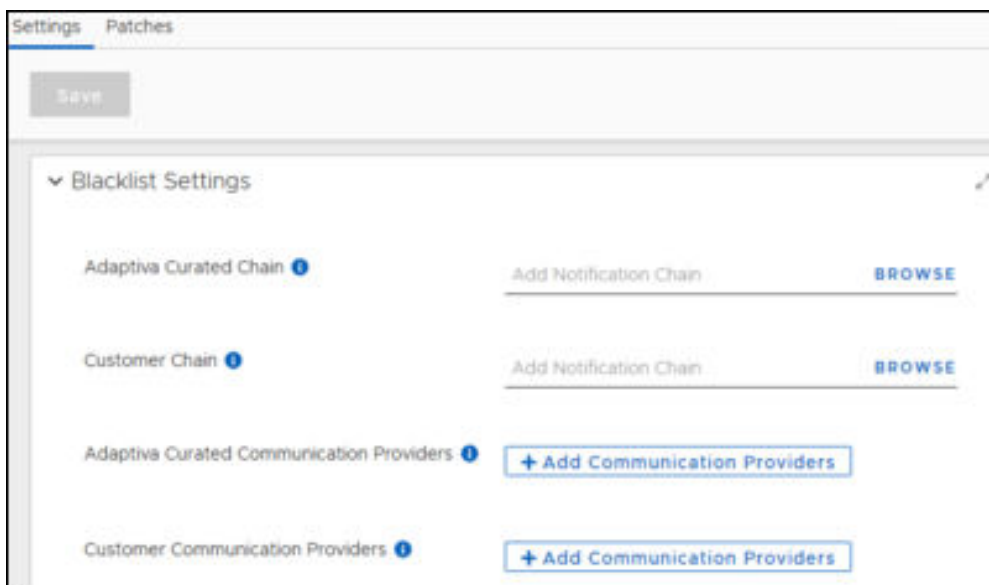
View Blacklist Settings

Blacklist Settings include notification details for blacklisted 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 click **Flex Controls** on the Home menu, and then select **Blacklisting > Blacklisted Patches**.



2. Select **Settings** to view the Blacklist Settings workspace.



Select a Notification Chain for Blacklisted Patches

1. Navigate to [Blacklist 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 bottom left of the dialog.

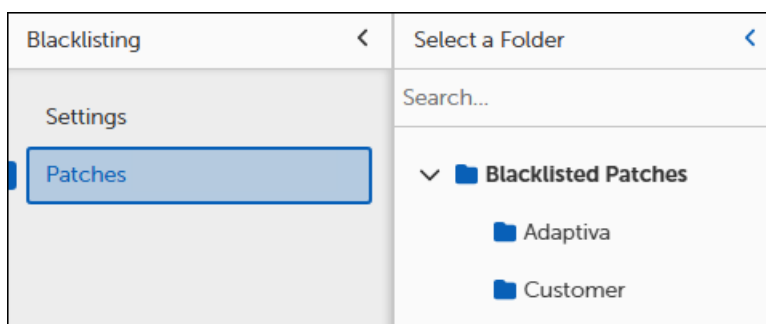
Choose Communication Providers for Notification Chains

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

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

Blacklisted Patches

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



Managing Blacklisted Patches

When a vendor issues a deficient or erroneous patch, Adaptiva blacklists the metadata and notifies customers automatically about the blacklisted patch. Blacklisting prevents inclusion of the patches in Patching Strategies and automatically creates an exclusion for the patch on all clients.

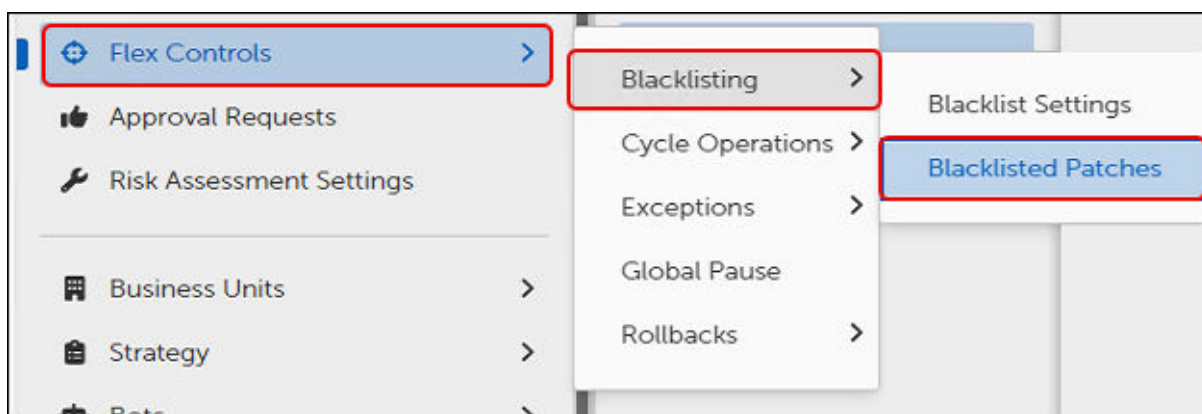
If Adaptiva determines that the vendor has fixed a blacklisted item, the metadata team can revoke the blacklisting. When the updated metadata arrives at the customer device, OneSite automatically removes the patch from the Blacklist, making it available for deployment.

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

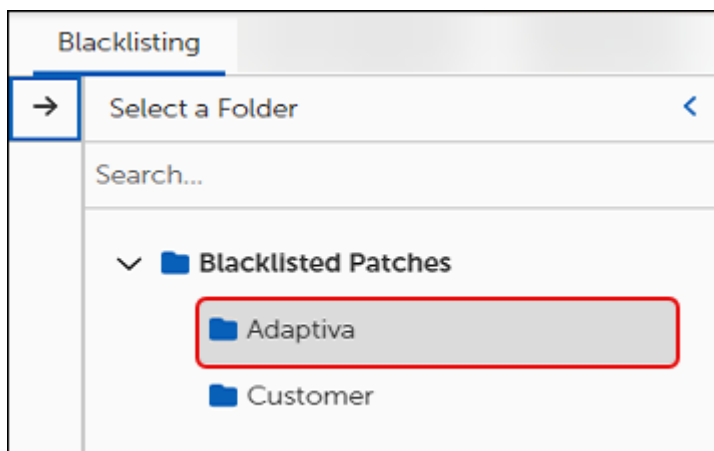
Customers may also create their own Blacklist for products they do not want deployed in their environment. Customers are responsible for managing their own blacklisted patches.

View Blacklisted Patches

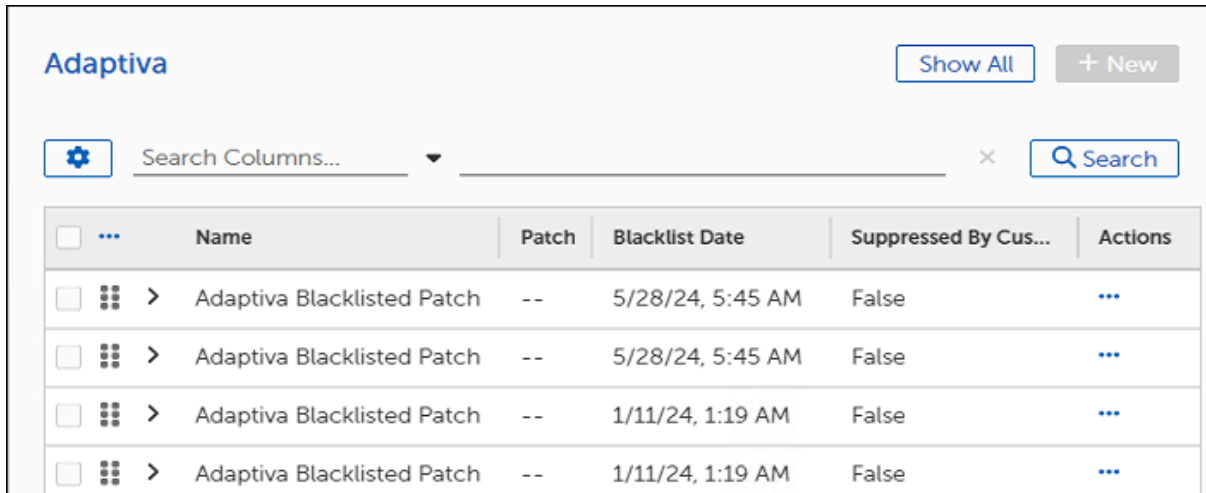
1. Mouse over or click **Flex Controls** on the Home menu, and then select **Blacklisting > Blacklisted Patches**.



2. Select **Blacklisted Patches**, and then select **Patches**.
3. Expand the **Blacklisted Patches** folder, and then select either the **Adaptiva** folder or the **Customer** folder to view blacklisted patches. This example uses the Adaptiva folder.



This displays the list of Adaptiva Blacklisted Patches.



<input type="checkbox"/>	...	Name	Patch	Blacklist Date	Suppressed By Cus...	Actions
<input type="checkbox"/>	☰ >	Adaptiva Blacklisted Patch	--	5/28/24, 5:45 AM	False	...
<input type="checkbox"/>	☰ >	Adaptiva Blacklisted Patch	--	5/28/24, 5:45 AM	False	...
<input type="checkbox"/>	☰ >	Adaptiva Blacklisted Patch	--	1/11/24, 1:19 AM	False	...
<input type="checkbox"/>	☰ >	Adaptiva Blacklisted Patch	--	1/11/24, 1:19 AM	False	...

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

Remove an Adaptiva Blacklisted Patch

When you enable **Removed from Blacklist** in an Adaptiva Blacklisted Patch template, you are expressly allowing clients in your environment to install a patch that Adaptiva has found deficient or erroneous.



CAUTION

Adaptiva does not recommend removing blacklisted patches.

1. Navigate to the table of Adaptiva Blacklisted Patches ([View Blacklisted Patches](#)), and then click the **Name** of the blacklisted patch you want to suppress. This opens to General Settings in the template.

General Settings

Name *

Description

Removed from Blacklist Disabled (default)

2. Select the **Removed from Blacklist** toggle to enable removal of this patch from the blacklist. Defaults to disabled.



CAUTION

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

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

Blacklisting

→ ← Back

Adaptiva Blacklisted Patch

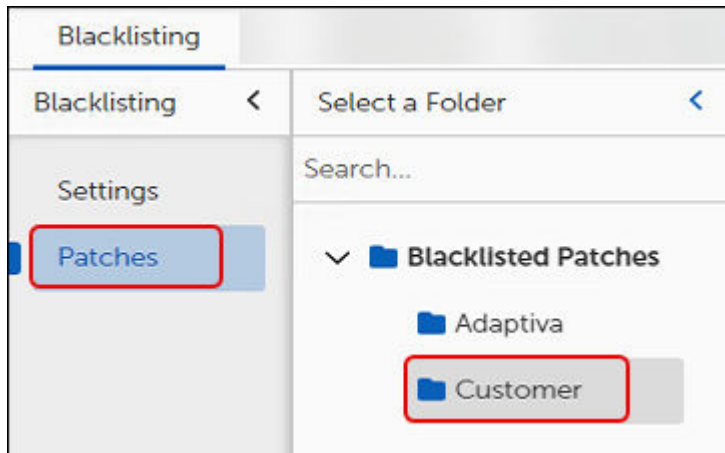
Save More ▾

Add a Patch to Customer Blacklisted Patches

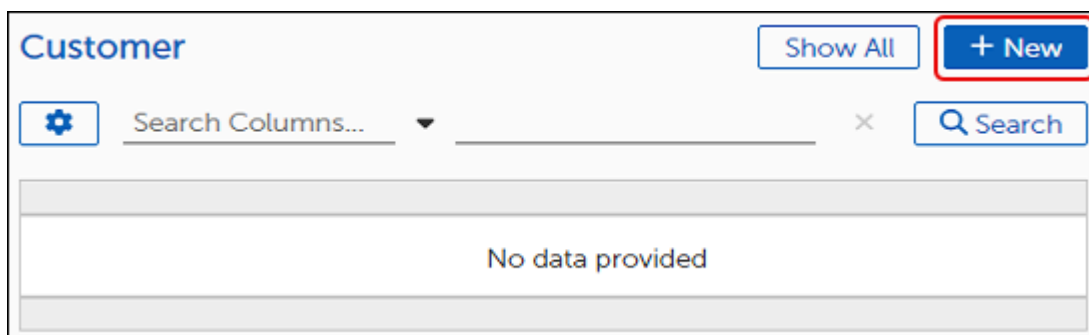
A Customer Blacklist is a customer created list of patch exceptions that applies globally to all customer devices. The red asterisk next to the field name indicates a required field.

1. Navigate to the table of blacklisted patches ([View Blacklisted Patches](#)).

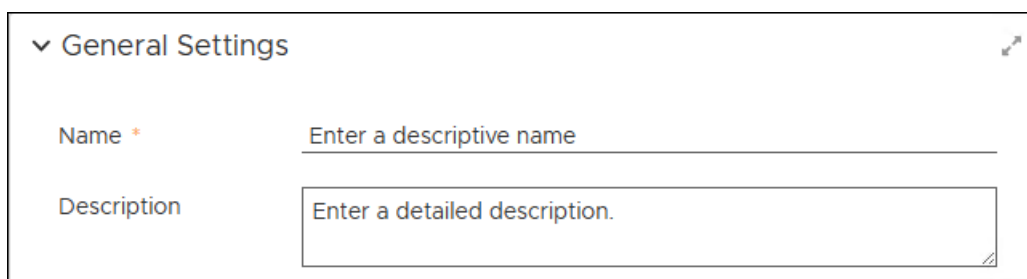
2. Select the **Customer** folder to view the table of patches blacklisted by the customer. Until you add patches, this table is blank.



3. Select **+ New** to add a patch to the blacklist table.

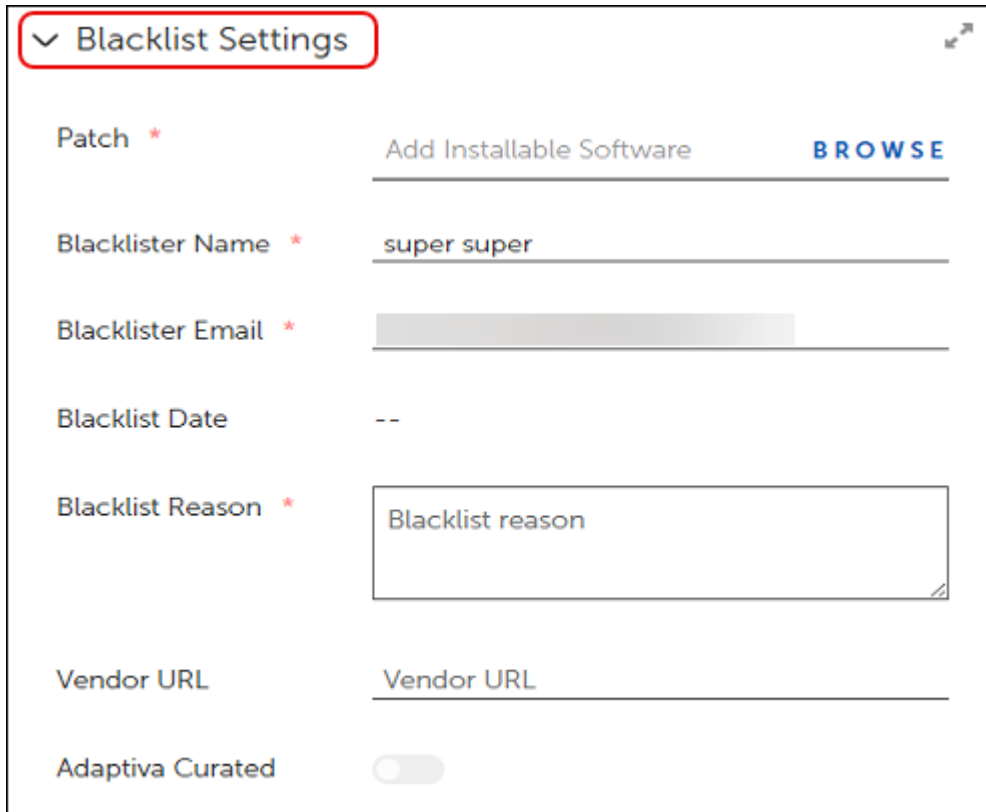


4. Enter a **Name** and **Description** for the patch you intend to blacklist.

A screenshot of the 'General Settings' form for a patch. It includes a 'Name' field with a red asterisk and a placeholder 'Enter a descriptive name', and a 'Description' field with a placeholder 'Enter a detailed description.'.

Configure Blacklist Settings

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



Blacklist Settings

Patch * Add Installable Software **BROWSE**

Blacklister Name * super super

Blacklister Email *

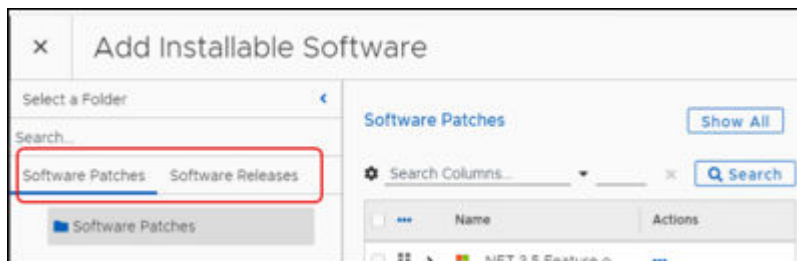
Blacklist Date --

Blacklist Reason * Blacklist reason

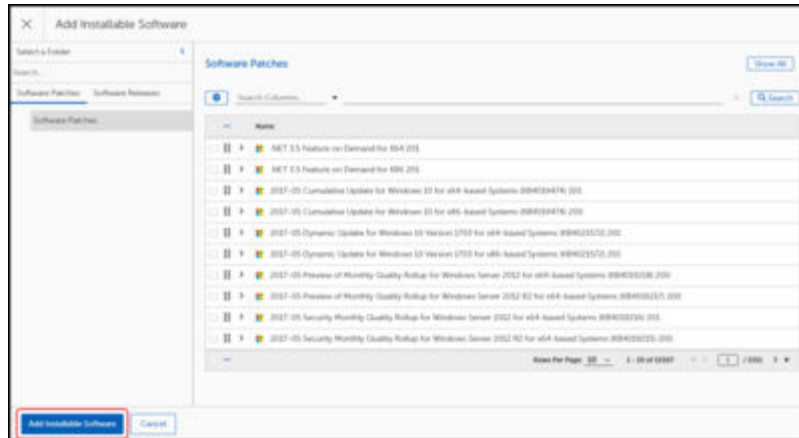
Vendor URL Vendor URL

Adaptiva Curated

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



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



- Use the navigation tools on the bottom right to scroll through the pages to find and select a Software product or release.
 - Enter a product name on the search line, and then click **Search** to find and select a specific product.
3. Select the **Name** of the patch to blacklist, and then click **Add Installable Software** at the bottom left of the dialog.
 4. Enter the following information:
 - Name of the person blacklisting this patch
 - Email of the person blacklisting this patch.
 - Describe the reason for the blacklisting of this patch.
 - Enter the vendor URL, if known (optional).

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

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

Cycle Operations

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

Details available for each cycle type include the following:

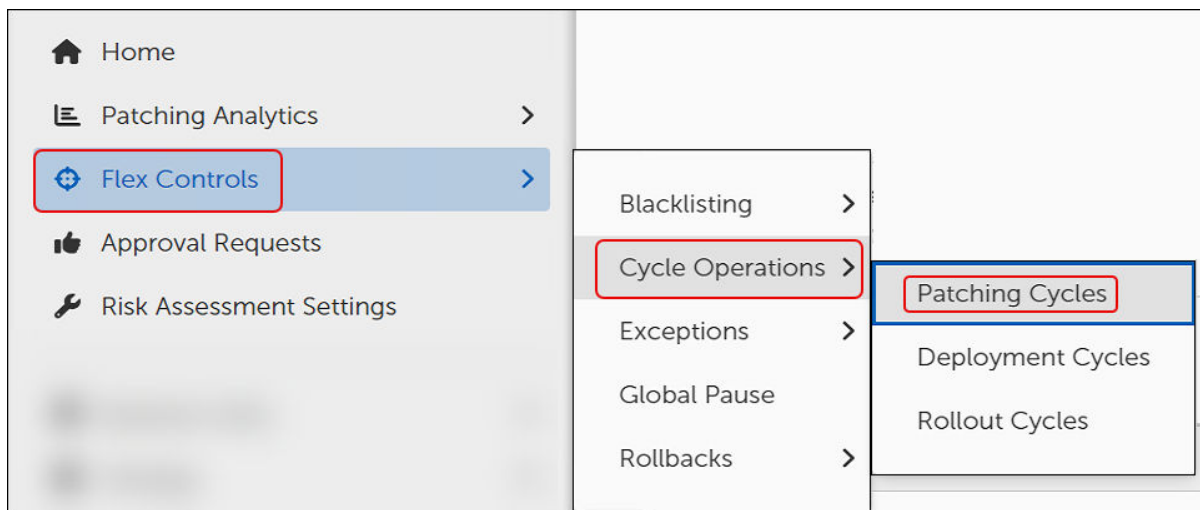
- **Cycle Information:** Provides general information about the Patch Process such as the Current State, the creation date and time, and the Patch Process schedule. This section also contains controls to manually start, stop, or delay a Patch Process.
- **Overall Metrics:** This section contains information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

Patching Cycles

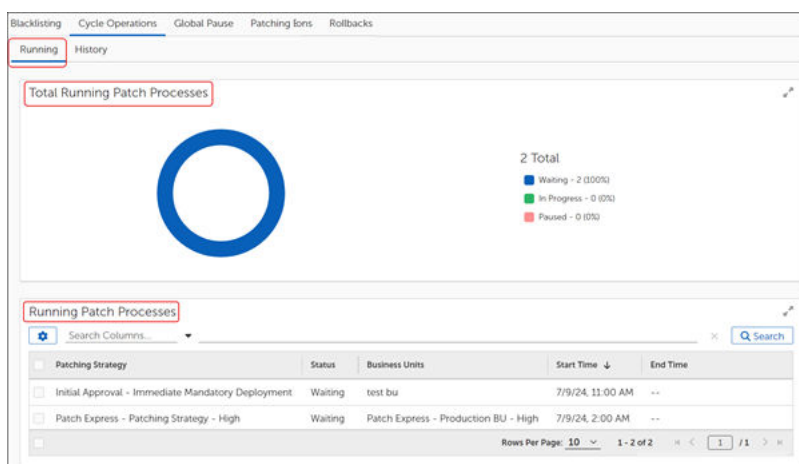
This dashboard shows information about the active Patch Processes in the environment. Patch Processes represent the workflow that models and performs the defined patching routine. As part of the overall Patching Strategy, Patch Deployment Bots use configured criteria to identify patches that apply to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

View the Running Patch Cycles

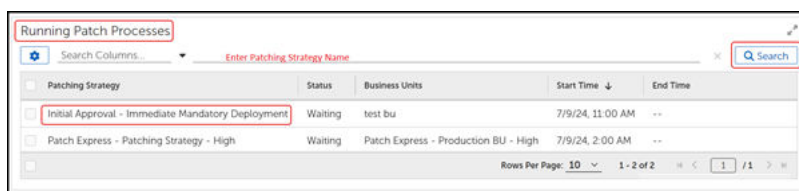
1. Mouse over or click **Flex Controls** on the **Home** menu, and then select **Cycle Operations > Patching Cycles**.



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



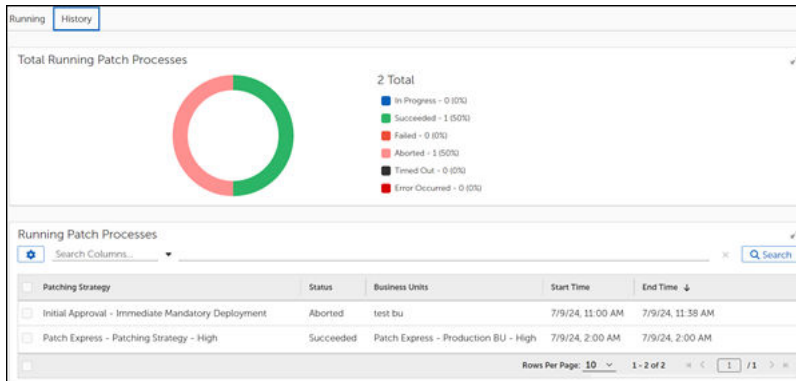
- The **Total Running Patch Processes** widget shows an aggregate summary of all patch processes and their corresponding states (Waiting, In Progress, or Paused).
 - The **Running Patch Processes** table lists the running Patching Strategies by name.
2. Enter a **Patching Strategy** name on the search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



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

View Patching Cycle History

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



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

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

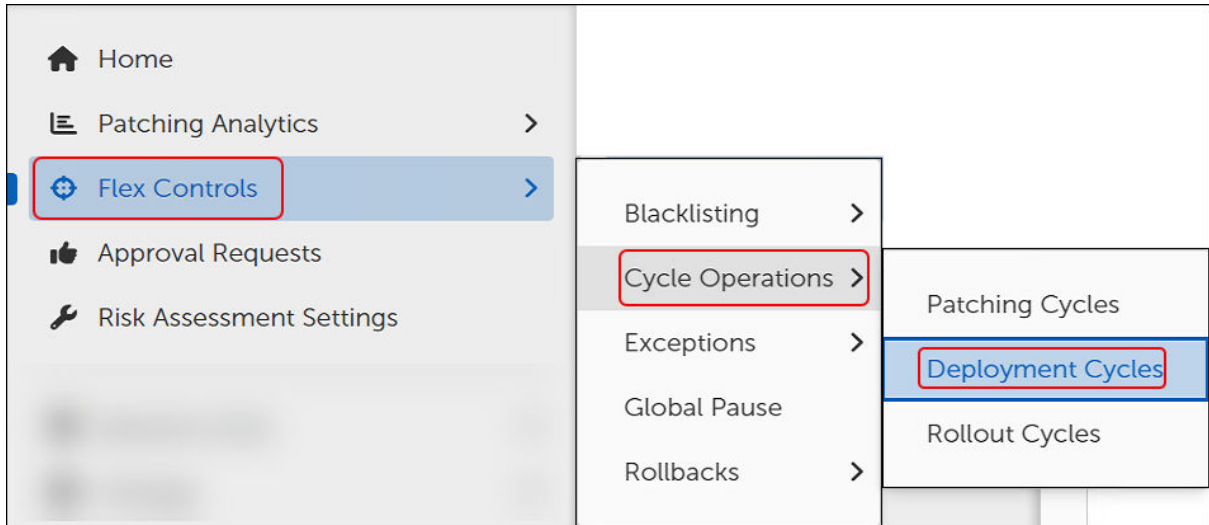
4. Select the **Patching Strategy** name in the **Running Patch Processes** table to see specific details about that process.

Deployment Cycles

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

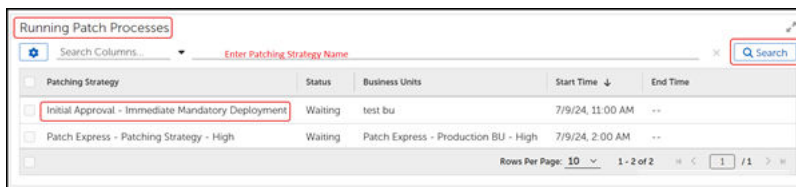
View the Running Deployment Cycles

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



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

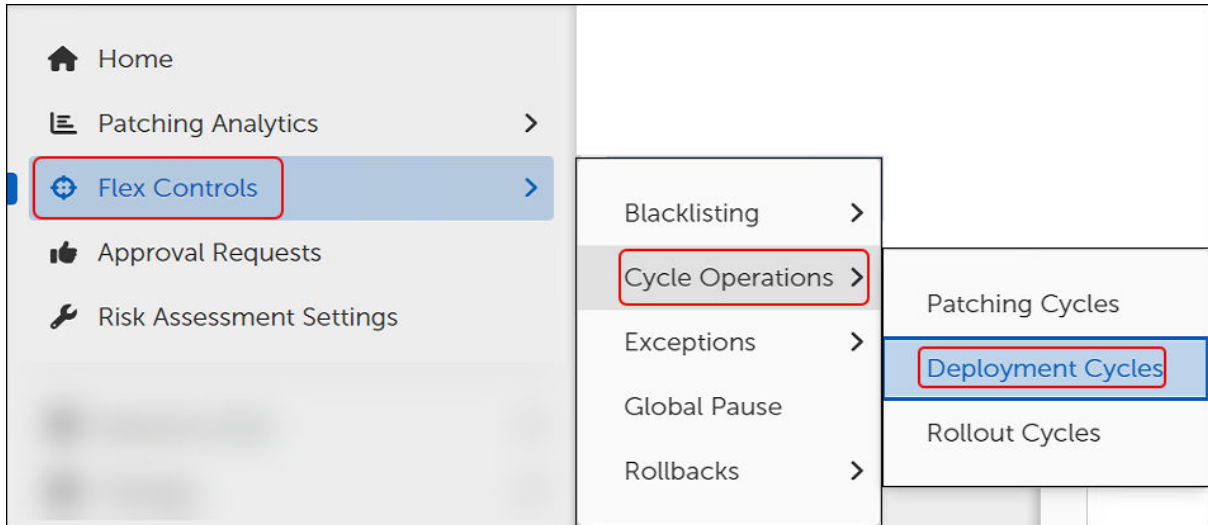
- The **Total Running Deployments** widget shows an aggregate summary of all patch processes and their corresponding states (Waiting, In Progress, or Paused).
 - The **Running Deployments** widget table lists the running Deployment Strategies by name.
2. Enter a **Deployment Strategy** name on the search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



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

View Deployment Cycle History

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



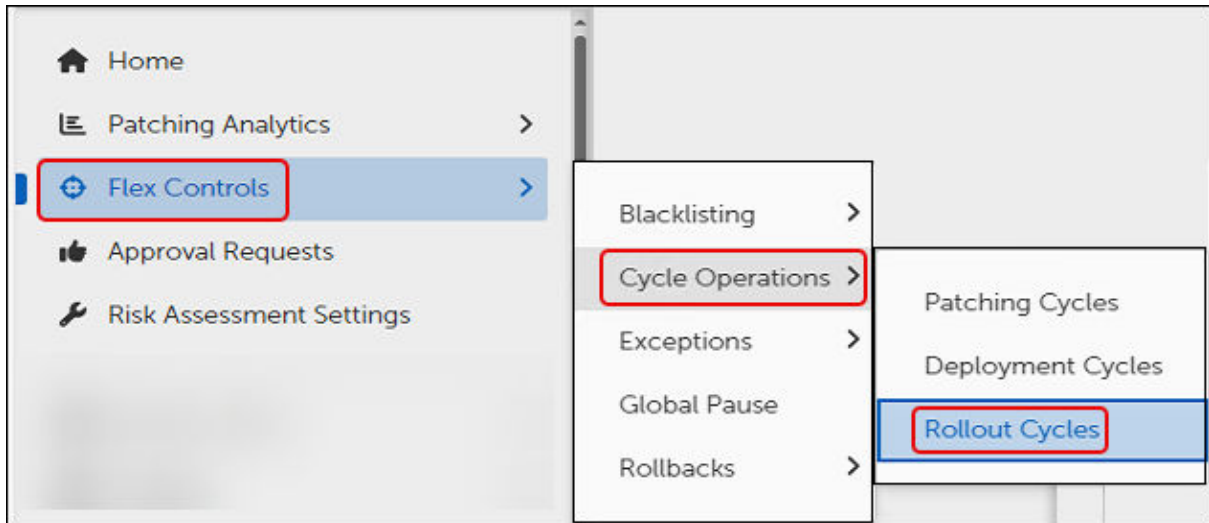
2. Select **History** on the upper left to change to the **History** tab:
 - The **Total Running Deployments** widget shows an aggregate summary of all deployment processes and their corresponding states (Waiting, In Progress, or Paused).
 - The **Running Deployments** widget table lists the completed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

Rollout Cycles

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

View the Running Rollout Cycles

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



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

- 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 on the search bar above the **Running Rollout Processes** table, and then click **Search**.
 3. Select the **Rollout Cycle** name in the **Running Rollout Processes** table to see specific details about that process.

View Rollout Cycle History

1. Mouse over or click **Flex Controls** on the **Home** menu, and then select **Cycle Operations > Rollout Cycles**.
2. Select **History** on the upper left to change to the **History** tab:
 - The **Total Running Deployments** widget shows 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 on the search bar above the **Running Rollout Cycles** table, and then click **Search**.

4. Select the **Rollout Cycle** name in the **Finished Cycles** table to see specific details about that process.

Patching Exceptions

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

Using Patching Exceptions

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

Desired State Override Options

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

Last Allowed Version

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

Create a Patching Exception

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

- b. Select **Save** again if you make any changes.
5. Choose an Override Strategy:
 - 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](#).

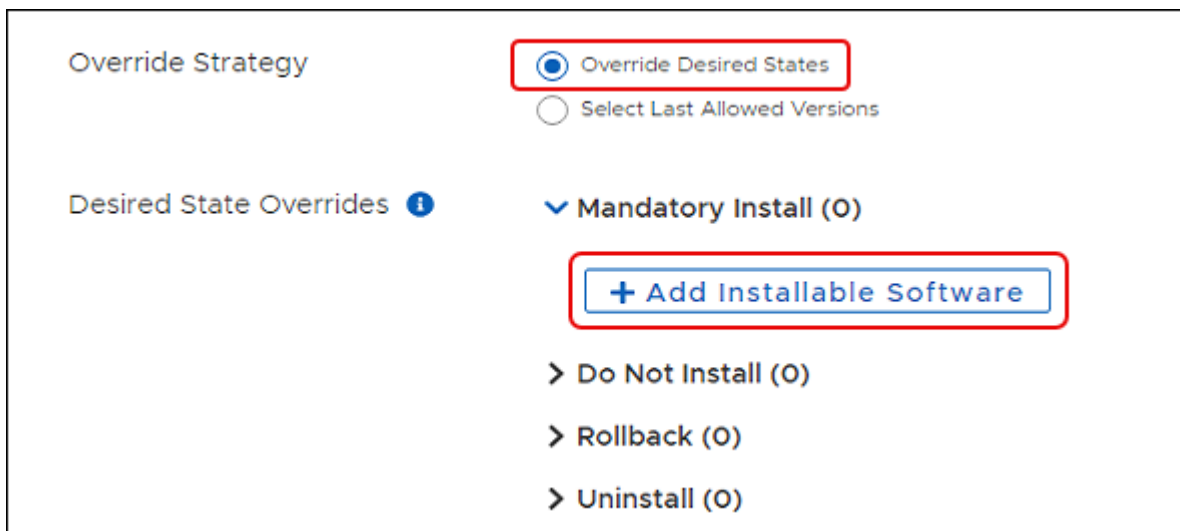
Set Override Details for Patch Exception



IMPORTANT

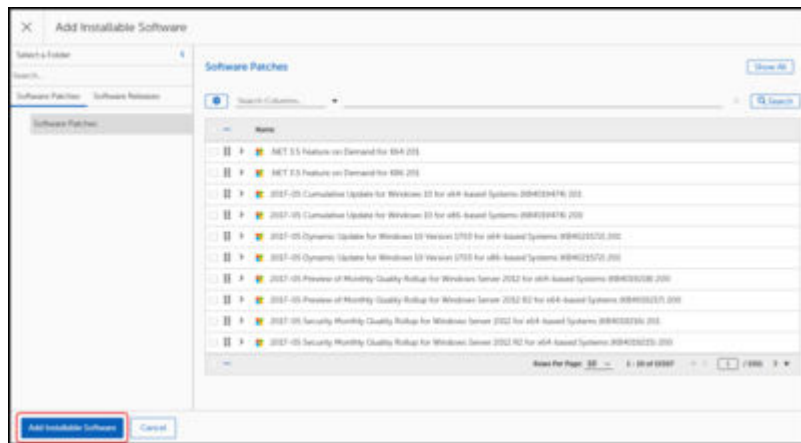
Choose only one software version per override exception.

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

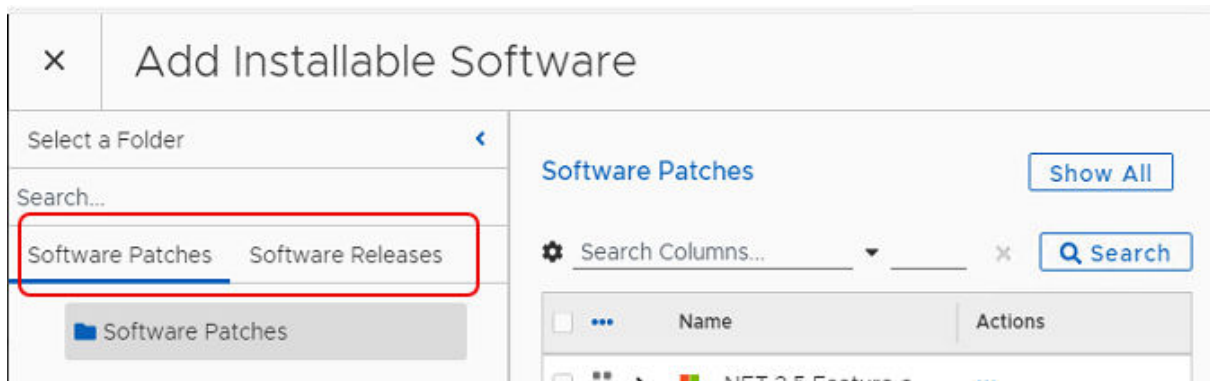


2. Select the type of **Desired State Override**, such as Mandatory Install, and then click **+Add Installable Software** for that state.
3.
 - a. Select one of the following tabs from the left-side column of the **Add Installable Software** dialog box:
 - Select the Software Patches tab to choose a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

- Select the Software Releases tab to choose a product release.
- b. Choose one of the methods below to search for a patch or release:



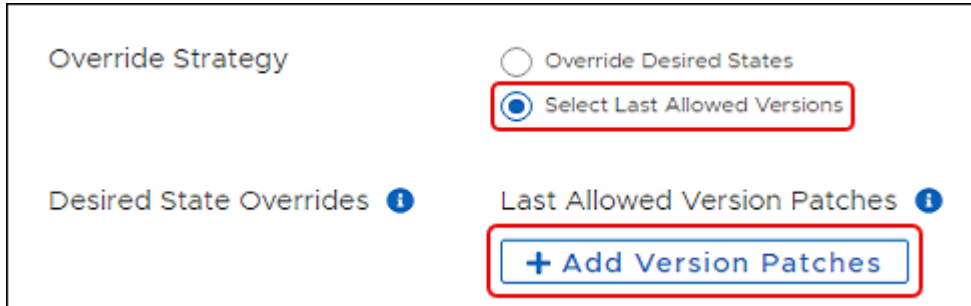
- Use the navigation tools on the bottom right to scroll through the pages to find and select a Software product or release.
 - Enter a product name on the search line, and then click **Search** to find and select a specific product.
4. Select the tab for either **Software Patches** (default) or **Software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



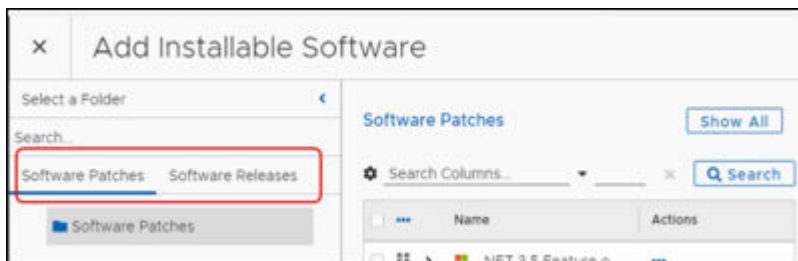
5. Select **Save** on the upper-left corner of the dialog to save your changes:
- a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.
6. Continue to **Add Target Business Units**.

Set Last Allowed Patch Versions

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



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



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

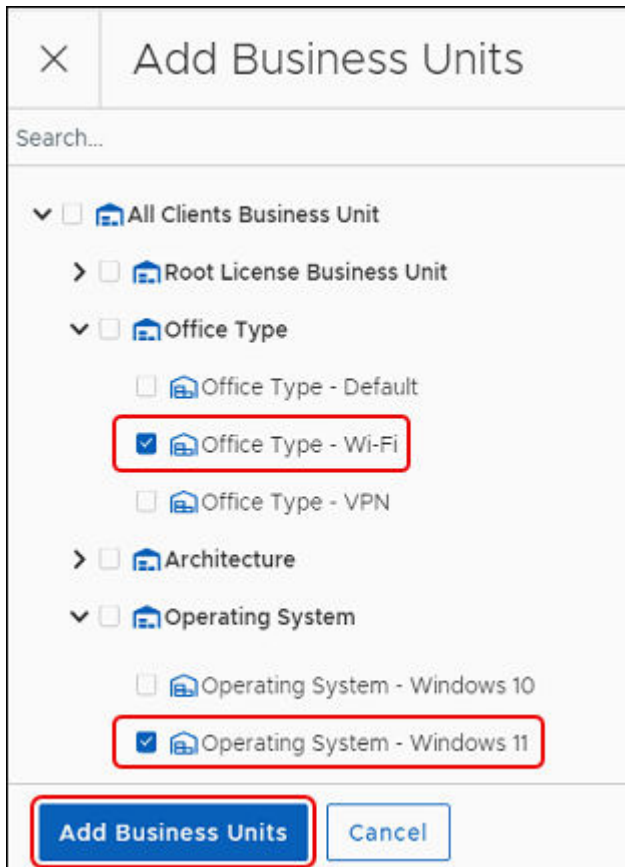
Add Target Business Units for Patch Exceptions

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

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



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



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

Global Pause

Global Pause settings take effect immediately on the clients you identify either globally or within the selected Business Units. Patch cycles continue to run as configured on

the 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.

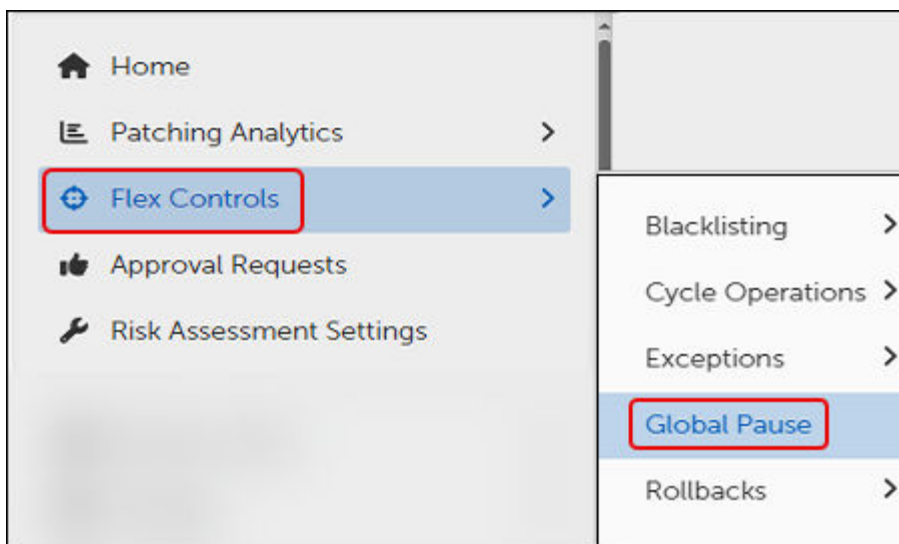
Paused Cycles: Pause Patching, Deployment, or Rollout Cycles either for specified Business Units or for the Business Units already targeted by the Cycle.

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

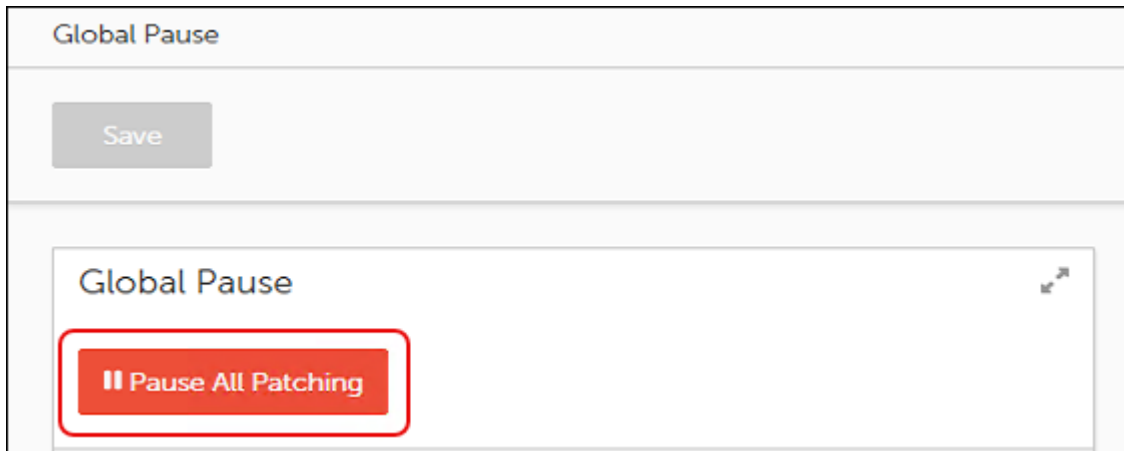
Stop All Patching Activity Immediately

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

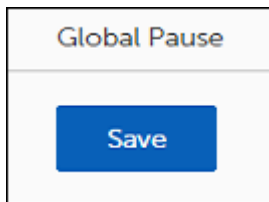
1. Select **Flex Controls** on the Home menu, and then select **Global Pause**.



This opens the **Global Pause** dialog:



2. Select **Pause All Patching**.

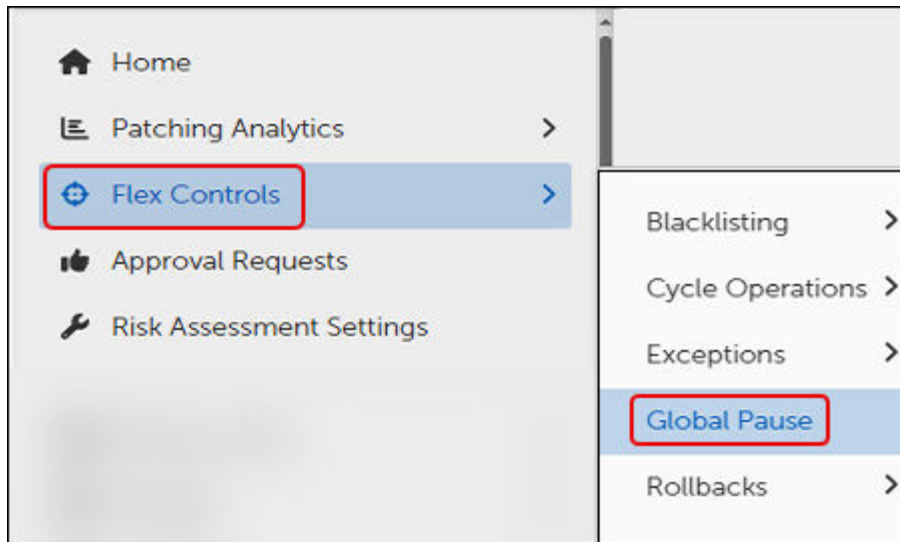


3. Select **Save** to activate Global Pause. This immediately stops all patch deployments across all licensed clients:
 - All patch deployments in progress that have not reached an irreversible state are paused immediately.
 - All newly initiated patch deployments are paused automatically.

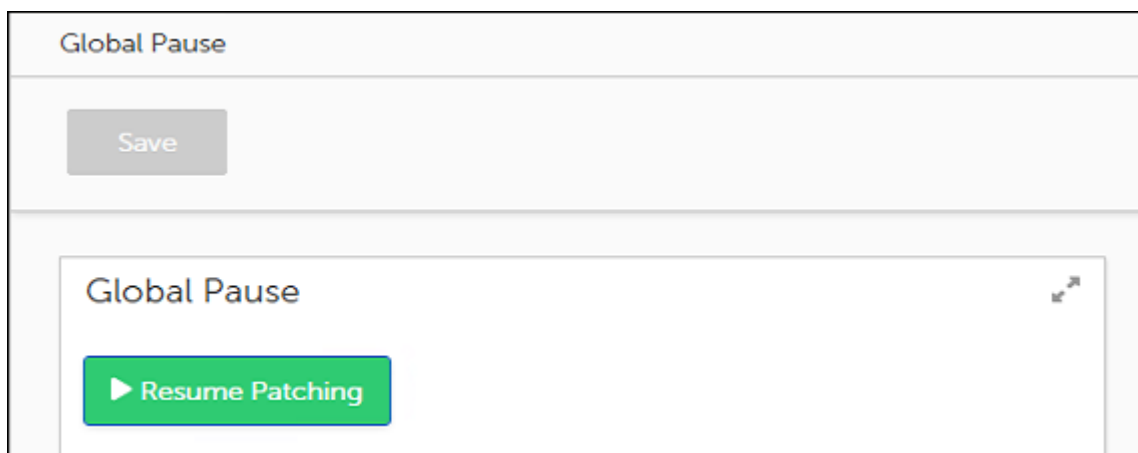
Resume All Paused Patching Activity Immediately

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

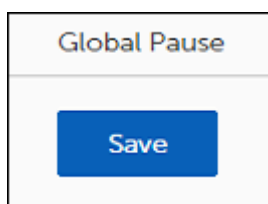
1. Select **Flex Controls** on the Home menu, and then select **Global Pause**.



This opens the **Global Pause** dialog:



2. Select **Resume Patching**.

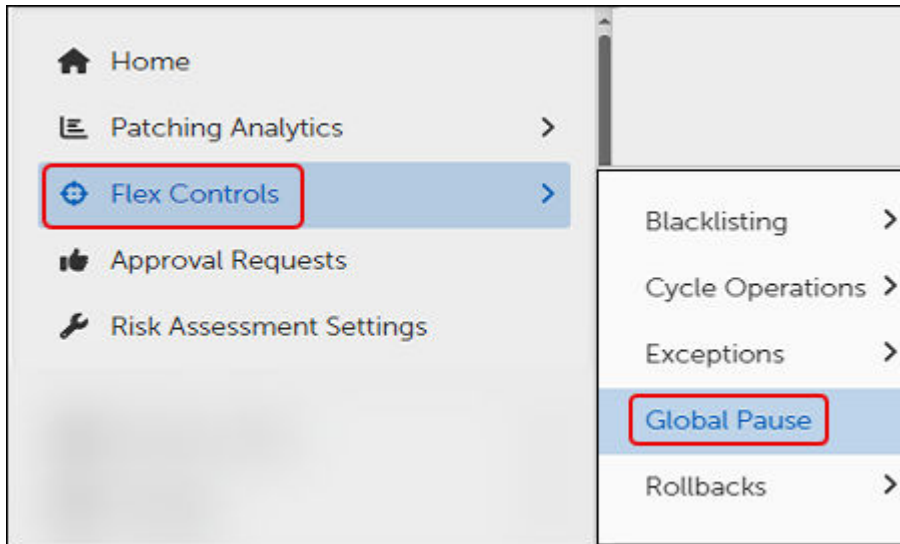


3. Select **Save** to revoke the Global Pause. This immediately revokes the Global Pause and allows patching activity to occur as configured.

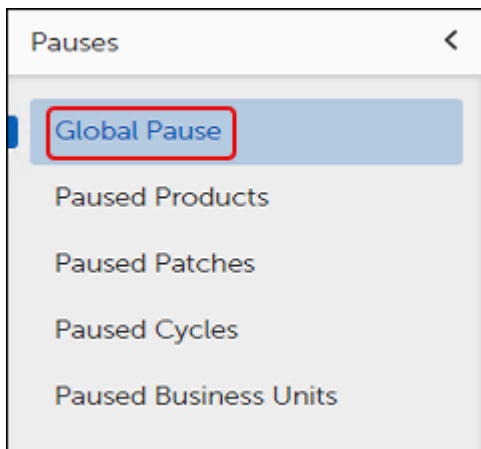
Pause Patching for Specific Objects

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](#)).

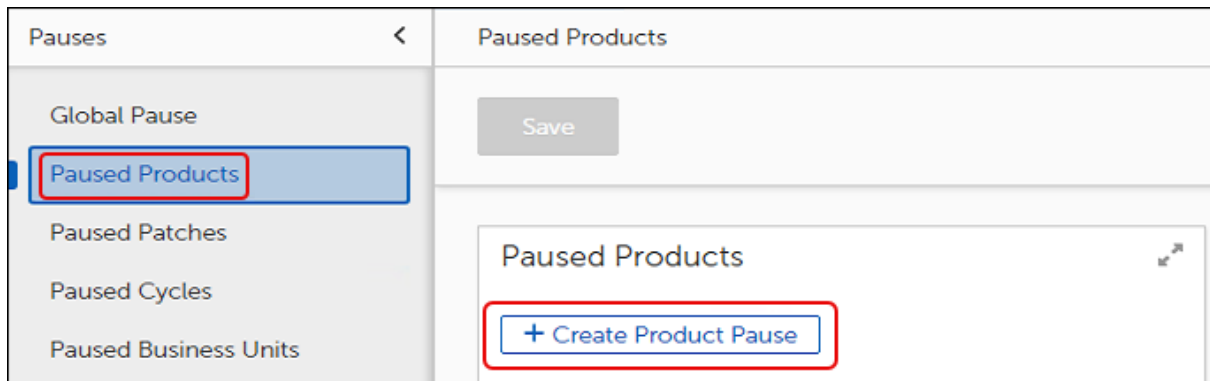
- **Pause Patches:** Pause deployment of a software patch or release for one or more products ([Paused Patches](#)).
- **Paused Cycles:** Specify a [Patching](#), [Deployment](#), or [Rollout](#) cycle to pause for one or more products.
- **Pause Business Units:** Pause patch deployments for one or more [Business Units](#).

Pause Deployment of a Specific Software Product

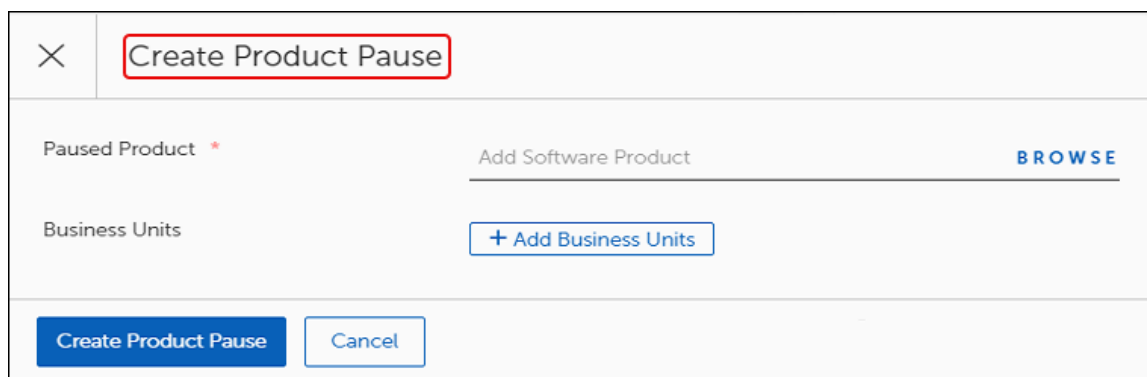
To stop patching activity for specific software products or patches, complete the following steps:

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.

×

Create Product Pause

Paused Product * Add Software Product [BROWSE](#)

Business Units [+ Add Business Units](#)

[Create Product Pause](#) [Cancel](#)

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

×

Add Software Product

Software Products [Show All](#)

[Settings](#) Search Columns... [Search](#)

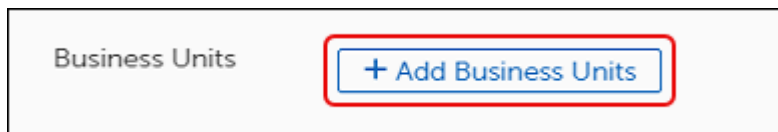
<input type="checkbox"/>	...	Name
<input type="checkbox"/>	>	1Password x64
<input type="checkbox"/>	>	3CX Call Flow Designer x64
<input type="checkbox"/>	>	3Dconnexion 3DxWare 10 x64
<input checked="" type="checkbox"/>	>	3Dconnexion 3DxWare 10 x86
<input type="checkbox"/>	>	4K Video Downloader x64

Rows Per Page: **10** 1 - 10 of 1656 1 / 166

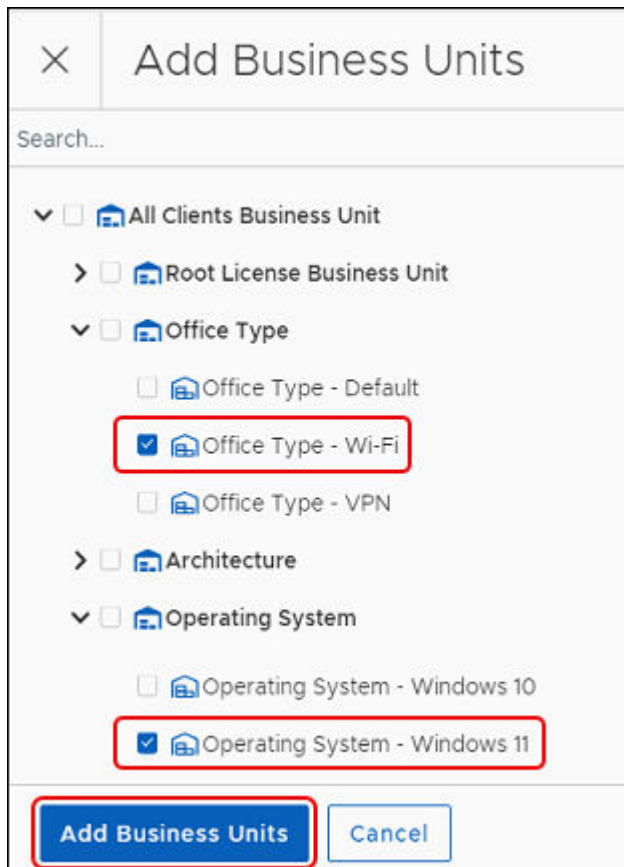
[Add Software Product](#) [Cancel](#)

- Use the navigation tools on the bottom right to scroll through the pages and select one or more **Software Products** from the table.
 - Enter a product name on the search line, and then click **Search** to find a specific product
2. Select **Add Software Product** to return to the **Create Product Pause** dialog, and then choose one of the following methods to proceed:

- To create a **Global Pause** for the selected products, click **Create Product Pause**. This pauses the deployment of the selected software product on all devices in the estate.
 - 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 **+ Add Business Units** in the open workspace or dialog.



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



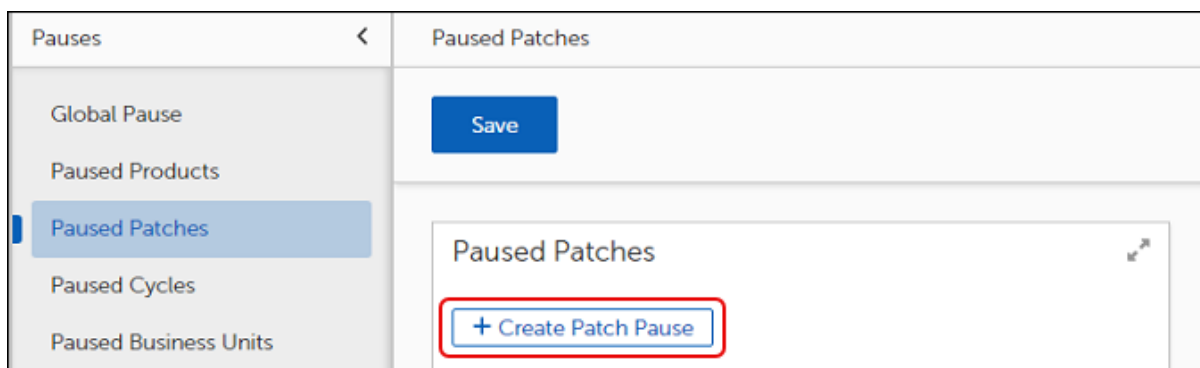
- b. Select one or more **Business Units** to add, and then click **Add Business Units**.
4. Select **Create Product Pause** and then click **Save** to create a global pause for the selected products.

Pause Deployment of a Specific Patch

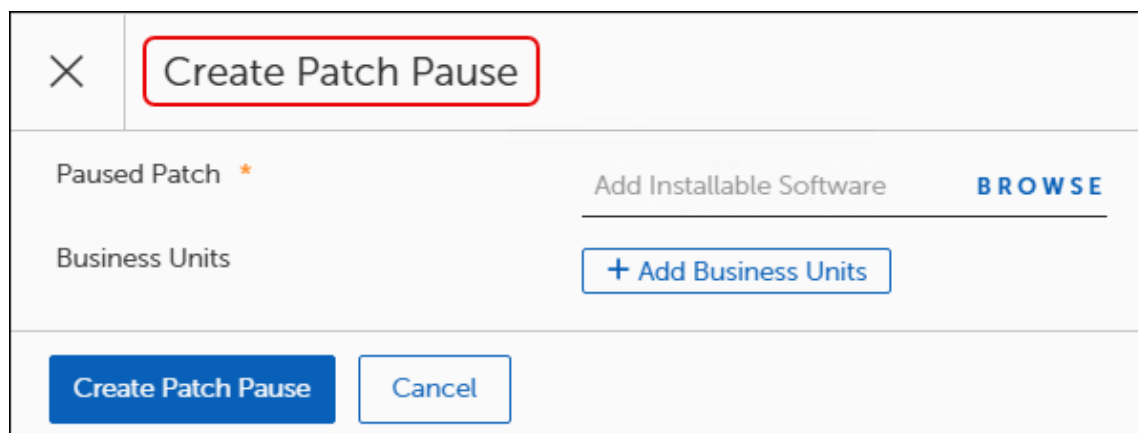
To stop patching activity for a specific patch, complete the following steps:

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

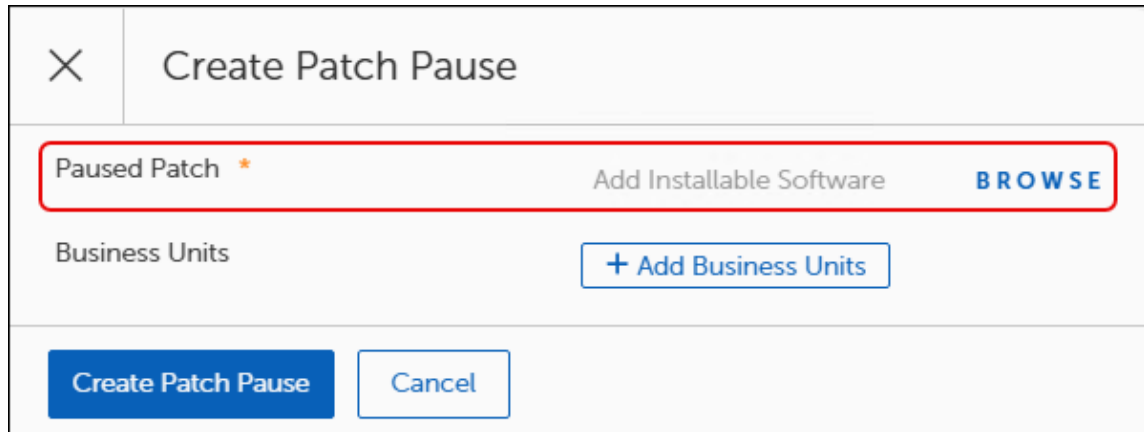
This opens the Paused Patches dialog:



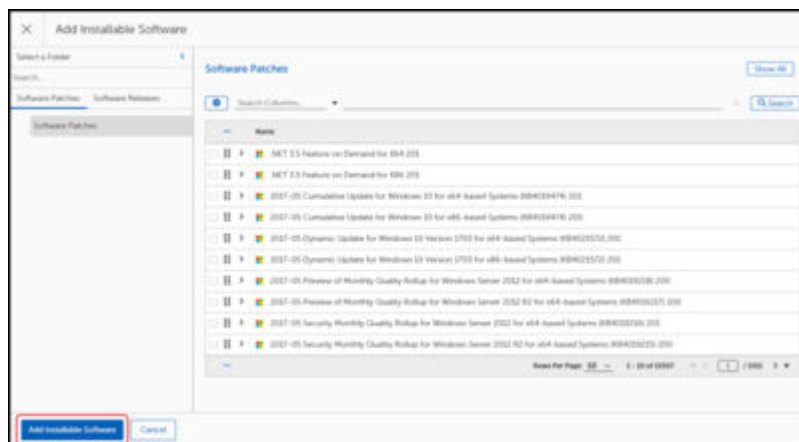
- a. Select **+Create Patch Pause** to open the **Create Product Pause** dialog, and then select Browse to find the Software patch you want to pause:



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



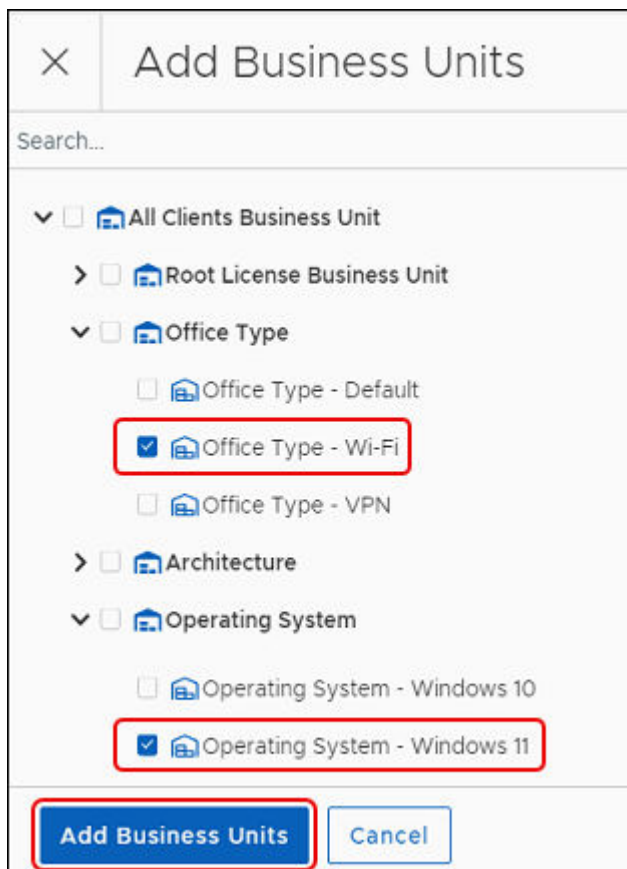
- c. Select the patch you want to pause:



2. Select **Add Installable Software Product** to return to the **Create Patch Pause** dialog, and then choose one of the following methods to proceed:
 - To create a **Global Pause** for the selected products, click **Create Patch Pause**. This pauses the deployment of the selected software patch on all devices in the estate.
 - 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 **+ Add Business Units** in the open workspace or dialog.



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



- b. Select one or more **Business Units** to add, and then click **Add Business Units**.
4. Select **Create Patch Pause** and then click **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

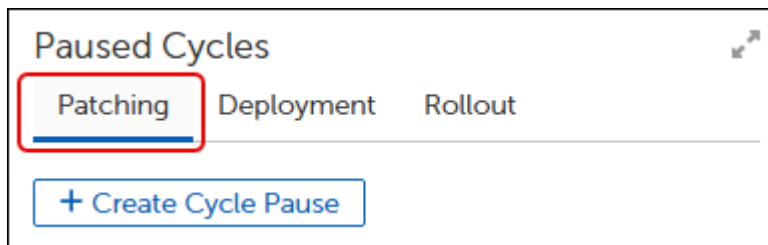
Pausing a cycle that is currently in a WAITING state (has not run yet), prevents that cycle from running until you remove the pause. This is the only server-side behavior related to pausing.

Pause a Patching Cycle

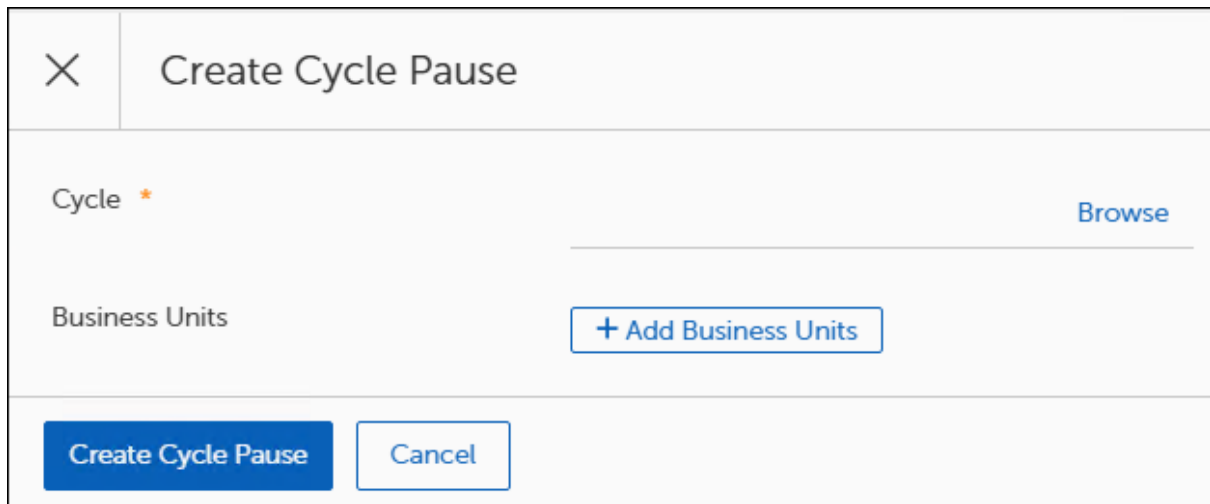
To stop patching activity for a specific patching cycle, complete the following steps:

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 click **Browse**.



×

Create Cycle Pause

Cycle * Browse

Business Units + Add Business Units

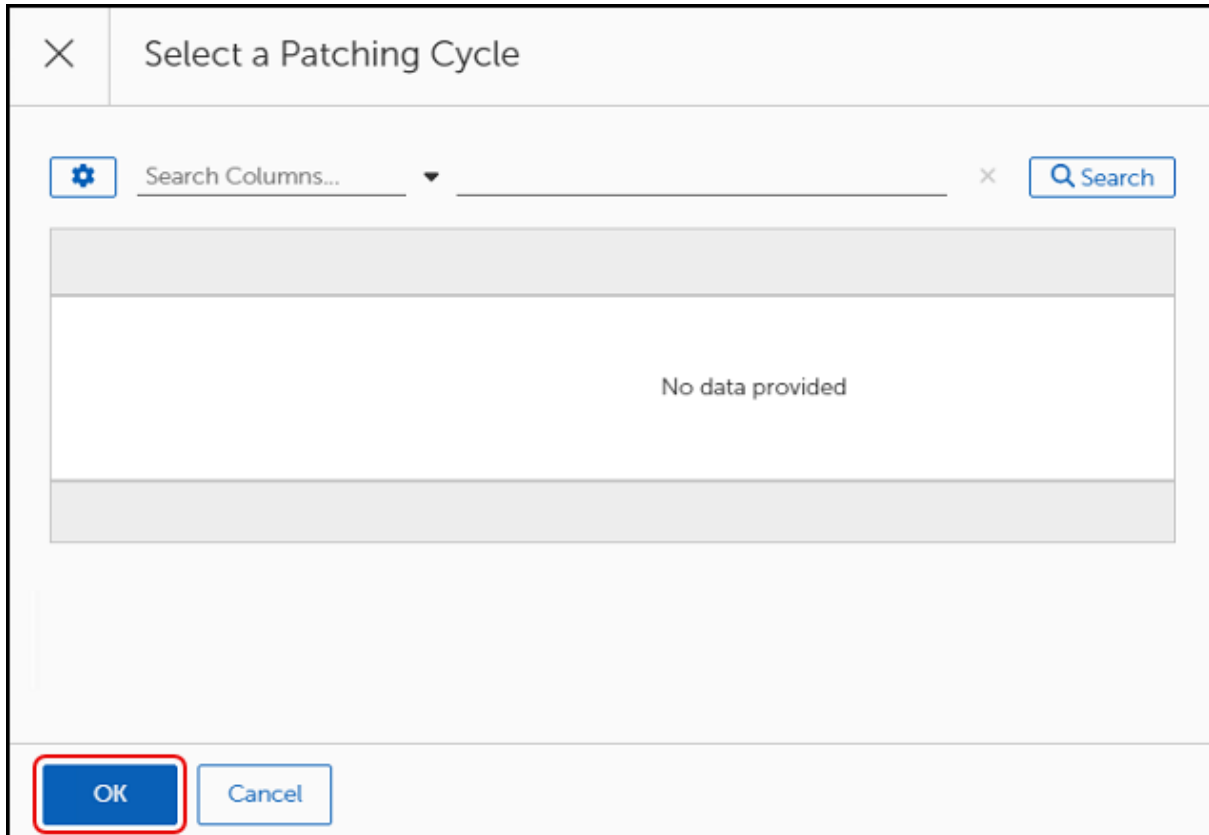
Create Cycle Pause Cancel

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



IMPORTANT

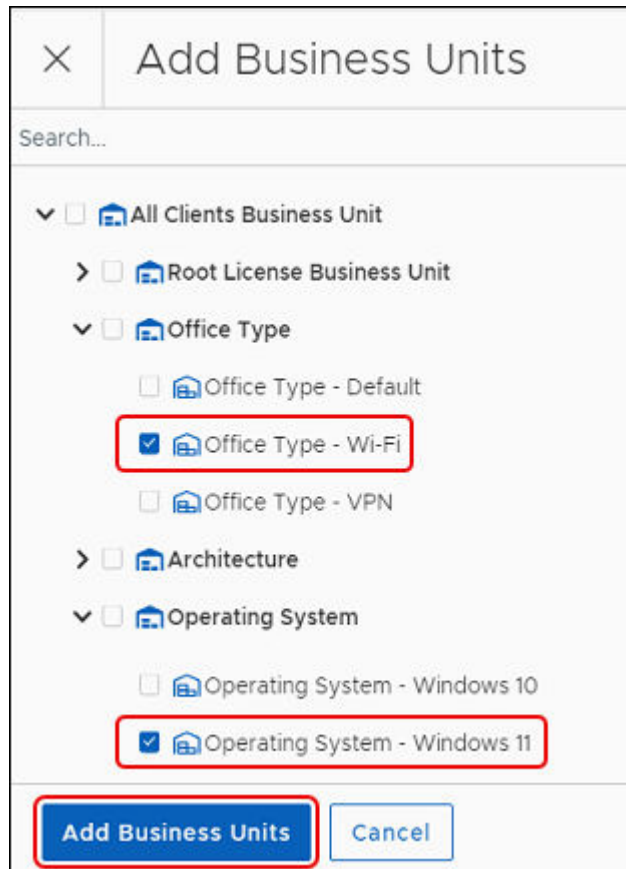
Cycles do not appear unless you have created them previously. If you do not have a cycle to stop, do not complete this section.



- 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 on the search line, and then click **Search** to find and select a specific cycle.
4. Select **OK**, and then choose one of the following options to proceed:
 - 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 **+ Add Business Units** in the open workspace or dialog.



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



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

Pause a Deployment Cycle

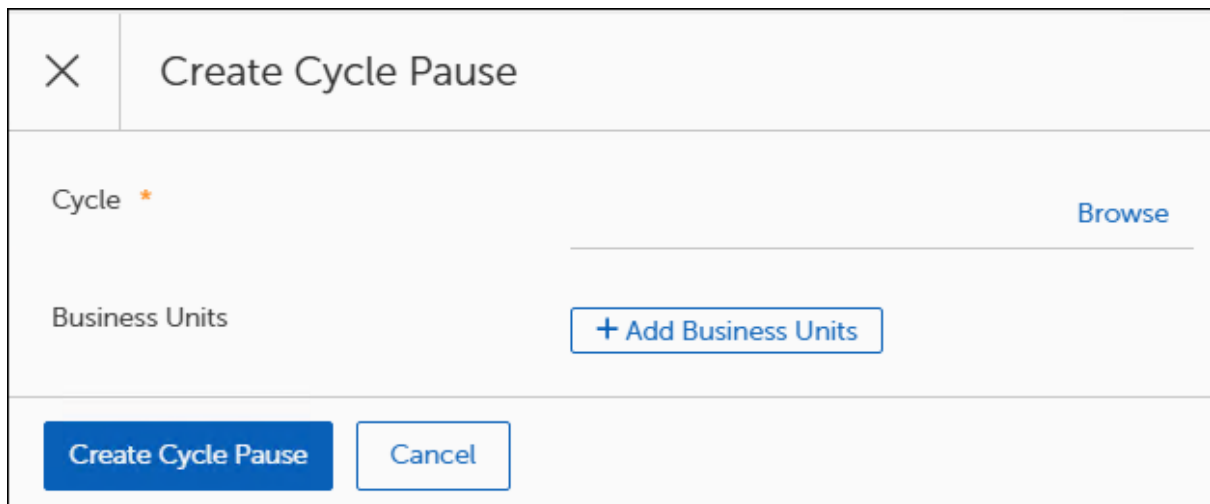
To stop all patching activity for a specific deployment cycle, complete the following steps:

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

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



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

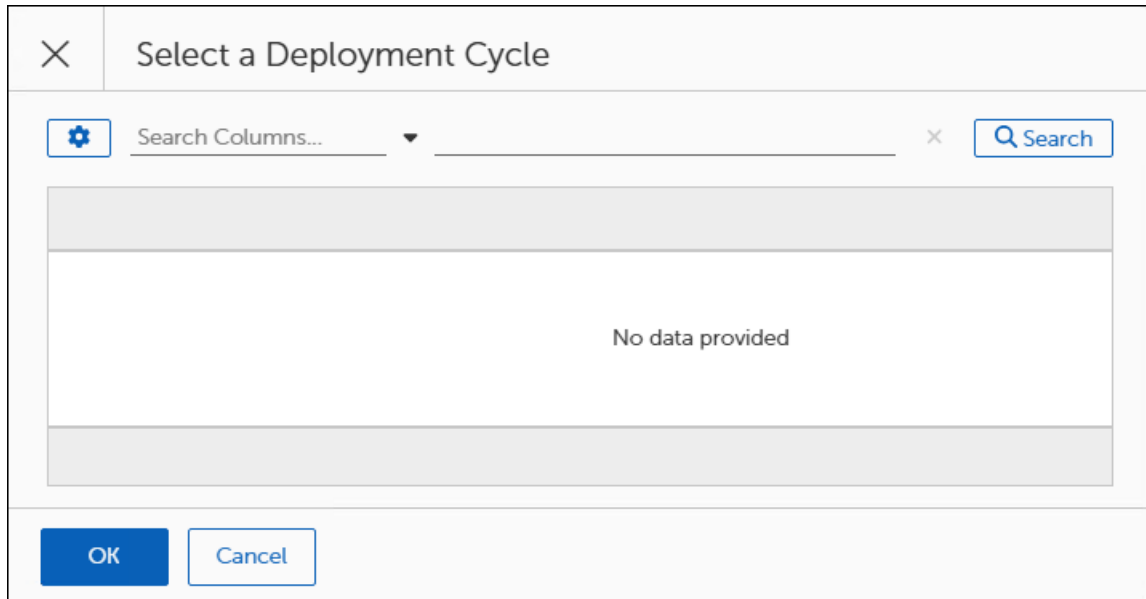


3. Select **Browse** to open the Select a Deployment Cycle dialog, and then use one of the methods below to find and select a cycle.



IMPORTANT

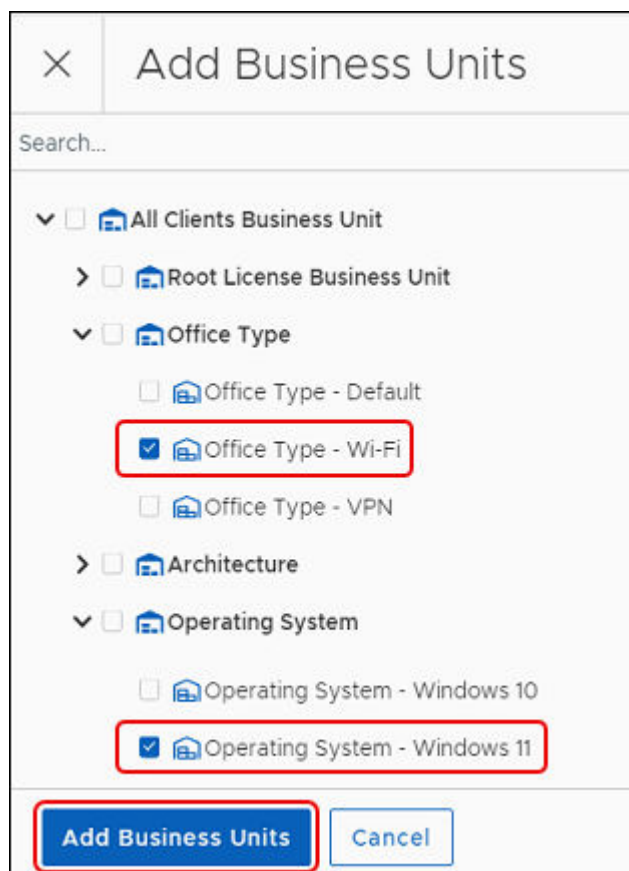
Cycles do not appear unless you have created them previously. If you do not have a cycle to pause, choose a different pause method.



- Use the navigation tools on the bottom right to scroll through the pages to find and select a cycle from the table.
 - Enter a cycle name on the search line, and then click **Search** to find and select a specific cycle
4. Select **OK** to save your entry, and then choose one of the following options to proceed:
- 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 **+ Add Business Units** in the open workspace or dialog.



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



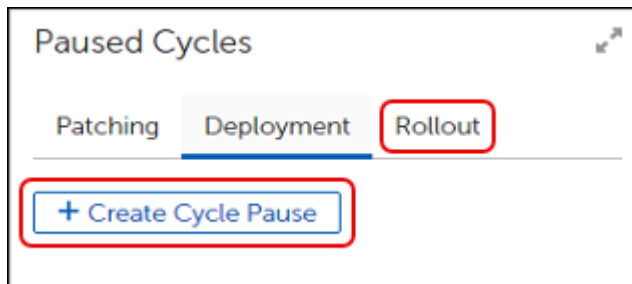
- b. Select one or more **Business Units** to add, and then click **Add Business Units**.
6. Select **Create Cycle Pause** and then click **Save** to create a pause for the selected cycle.

Pause a Rollout Cycle

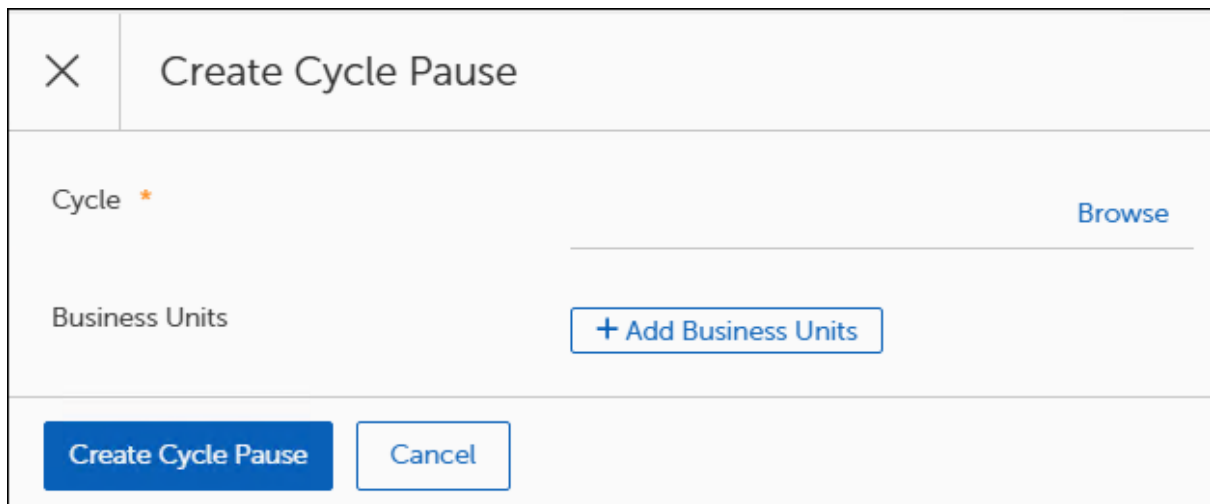
To stop all patching activity for a specific rollout cycle, complete the following steps:

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

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



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

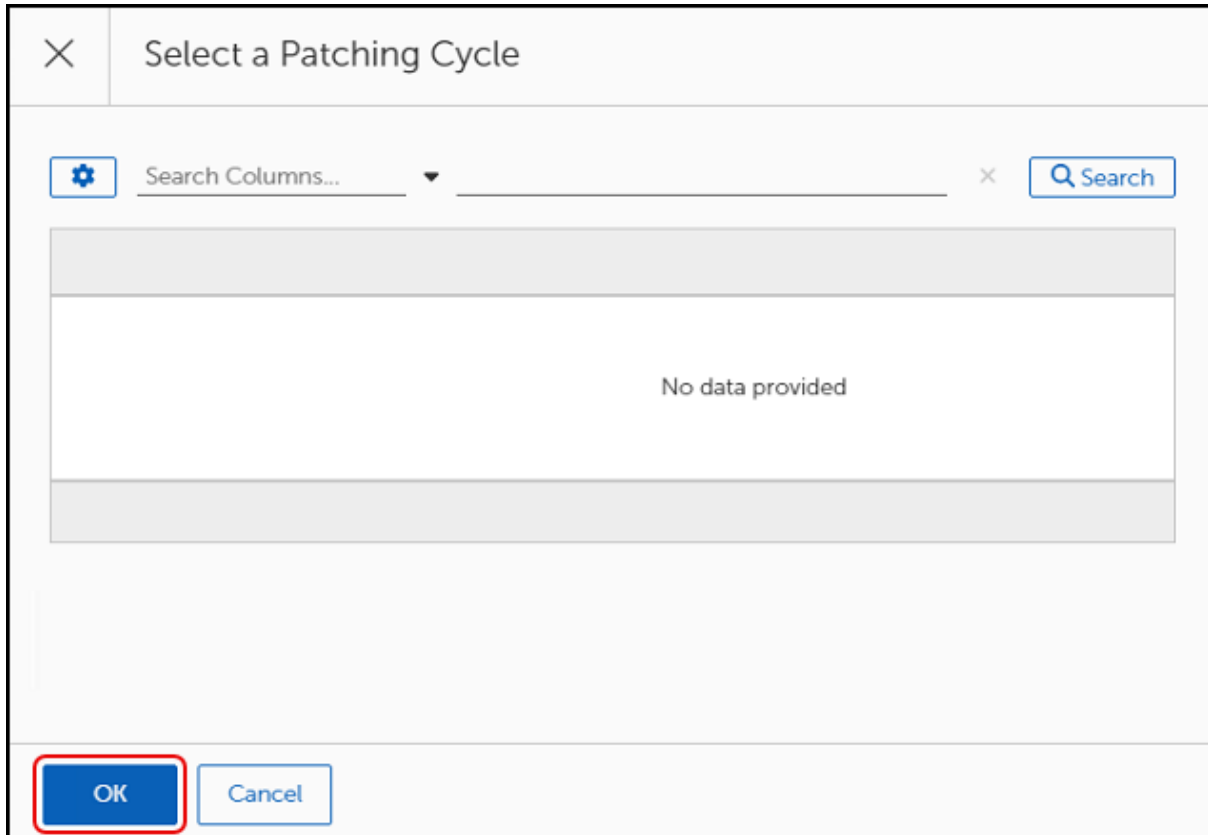


3. Select **Browse** to select the rollout cycle you want to pause. This opens the **Select a Rollout Cycle** dialog.



IMPORTANT

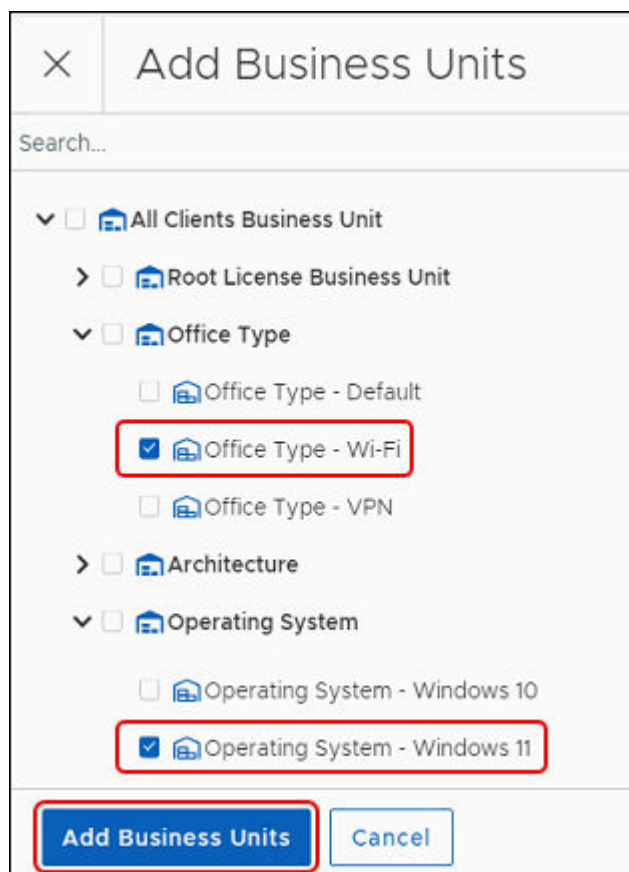
Cycles do not appear unless you have created them previously. If you do not have a cycle to stop, do not complete this section.



- Use the navigation tools on the bottom 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 click **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 **+ Add Business Units** in the open workspace or dialog.



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



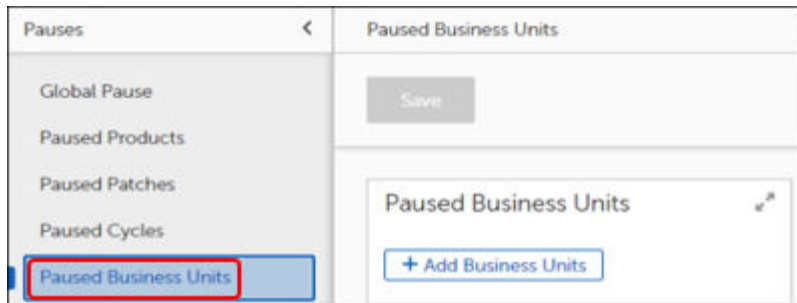
- b. Select one or more **Business Units** to add, and then click **Add Business Units**.
6. Select **Create Cycle Pause** and then click **Save** to create a pause for the selected rollout cycle.

Pause Deployment to a Business Unit

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

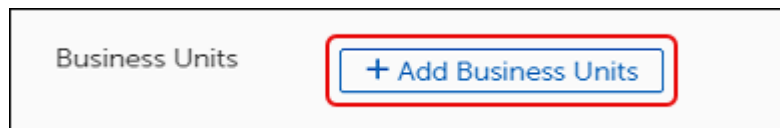
1. Navigate to the Pauses menu (see [Pause Patching for Specific Objects](#)), and then select **Paused Business Units**.

This opens the Paused Business Units dialog:

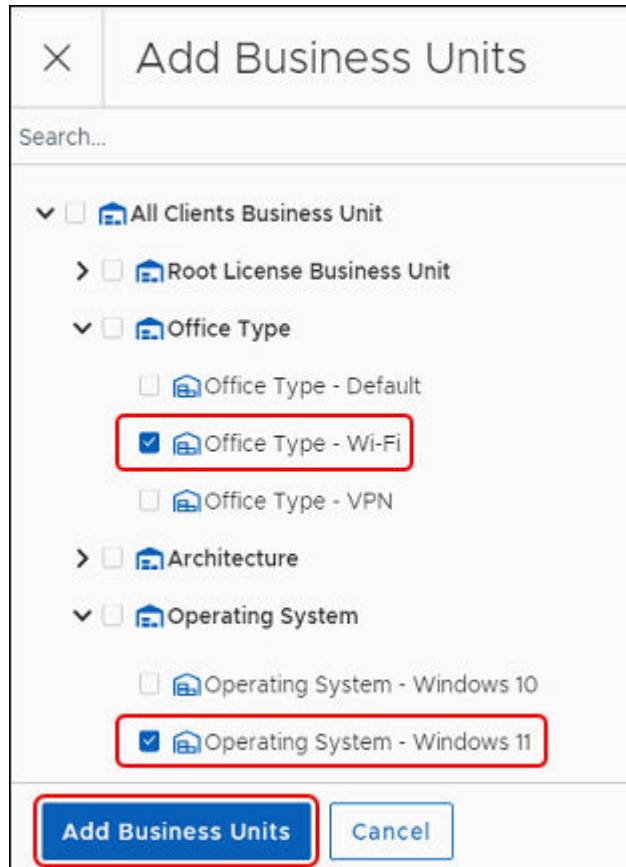


2. Add or remove **Business Units**:

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



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



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

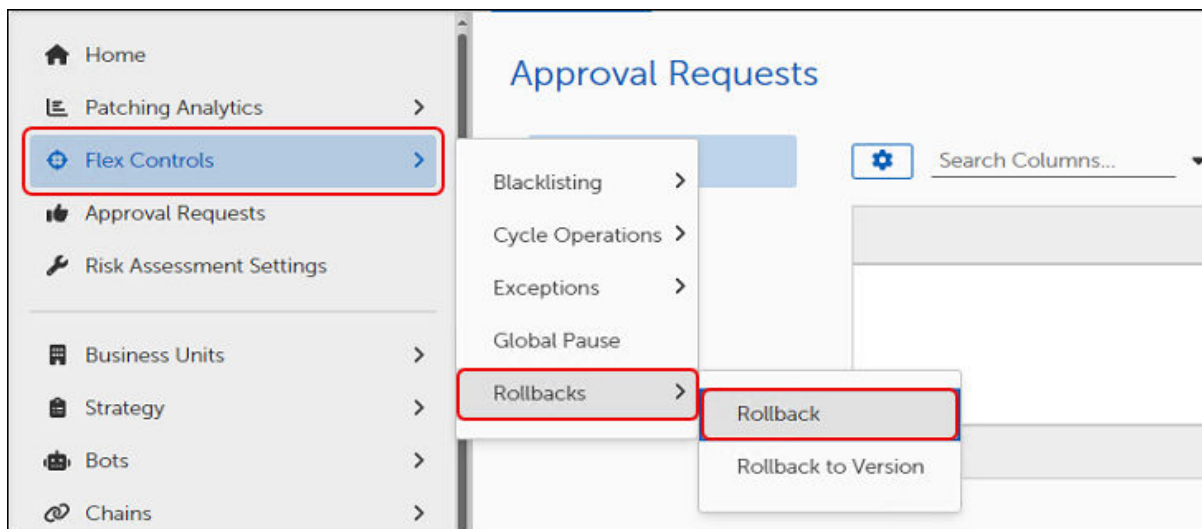
Rollback

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](#).

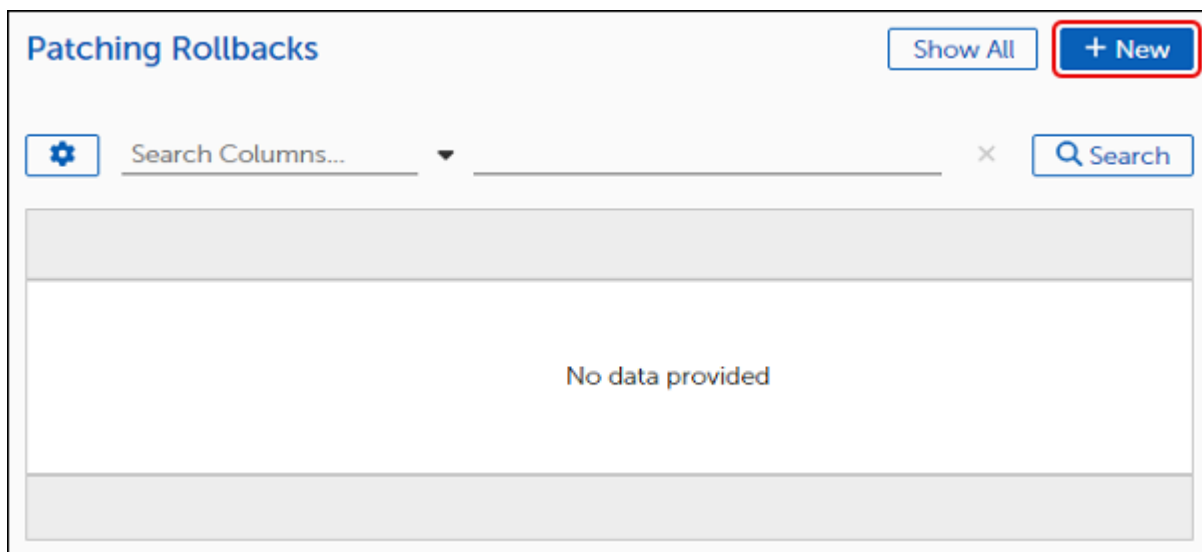
Create a Rollback

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 [OneSite 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.

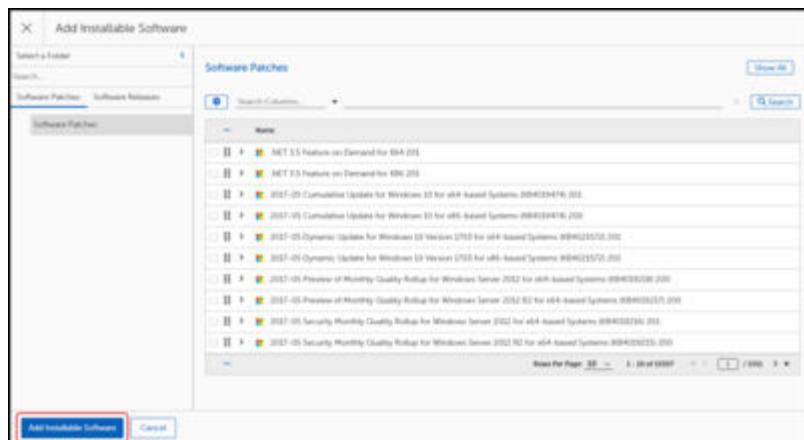
The screenshot shows a 'General Settings' dialog box with the following fields and controls:

- Name ***: A text input field with the placeholder text 'Name'.
- Description**: A large text area with the placeholder text 'Description'.
- Patch *i* ***: A label with an information icon and a red asterisk, positioned above the 'Add Installable Software' text.
- Add Installable Software**: A text label with a blue **BROWSE** button to its right.
- Target Business Units *i* ***: A label with an information icon and a red asterisk, positioned above a blue button labeled **+ Add Business Units**.

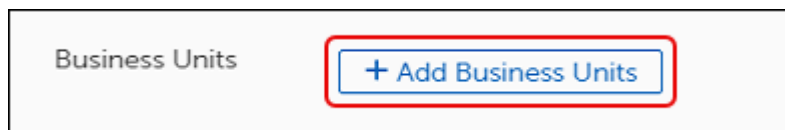
3. Locate the patch or release you want to roll back:

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

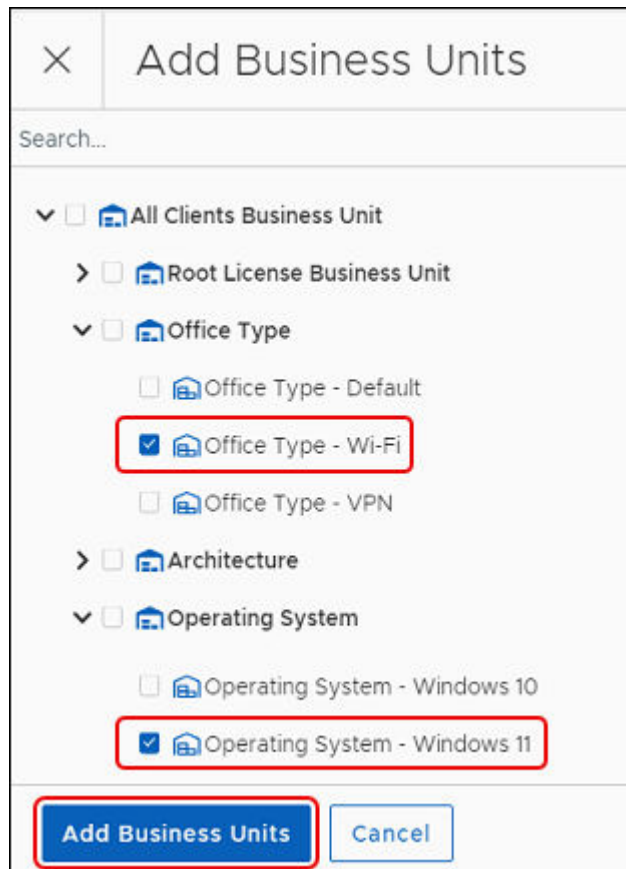
4. Select a Software patch or release :
- Select one of the following tabs from the left-side column of the **Add Installable Software** dialog box:
 - Select the Software Patches tab to choose a patch release.
 - Select the Software Releases tab to choose a product release.
 - Choose one of the methods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



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



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



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

Edit a Rollback Template

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

The screenshot shows a table titled "Patching Rollbacks". The table has columns for "Name", "Patch", and "Actions". The first row is selected, showing "Windows" with the patch ".NET 3.5 Feature on Demand for X64".

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

At the bottom of the table, there is a footer showing "Rows Per Page: 10" and "1 - 3 of 3".

This opens the template.



NOTE

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

General Settings

Name *

Description

Patch ⓘ * [BROWSE](#) ×

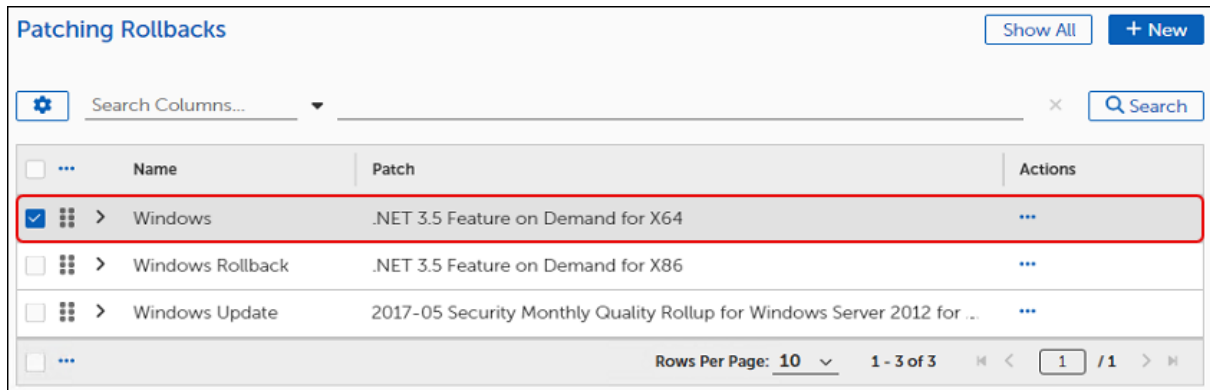
Target Business Units ⓘ * [+ Add Business Units](#)

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

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

Copy a Rollback

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



Patching Rollbacks Show All + New

Search Columns... × Search

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

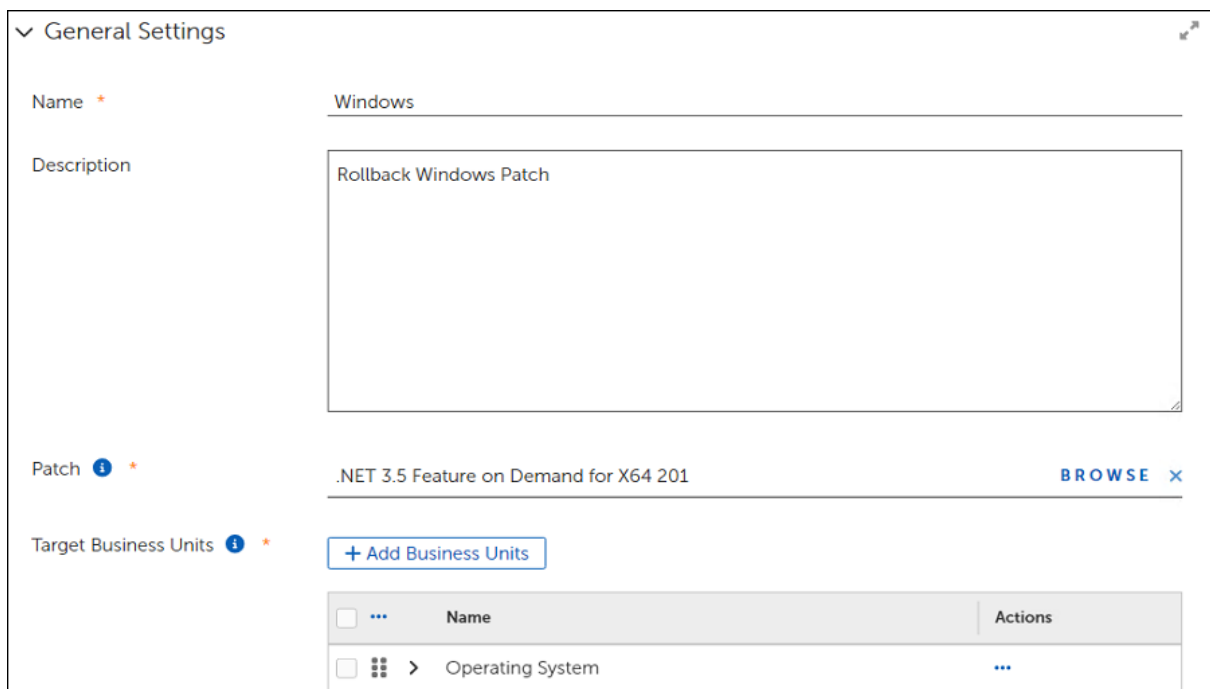
Rows Per Page: 10 1 - 3 of 3 1 / 1

This opens the template.



NOTE

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



General Settings

Name * Windows

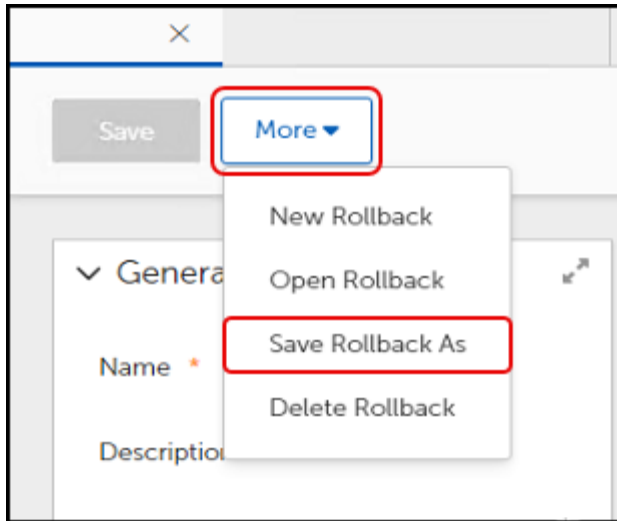
Description Rollback Windows Patch

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

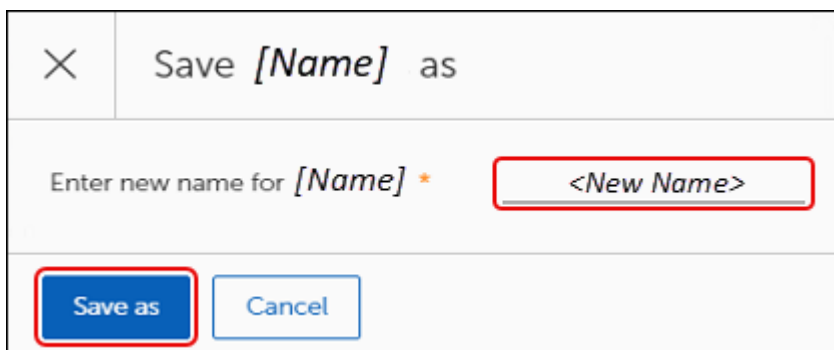
Target Business Units ⓘ * + Add Business Units

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

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



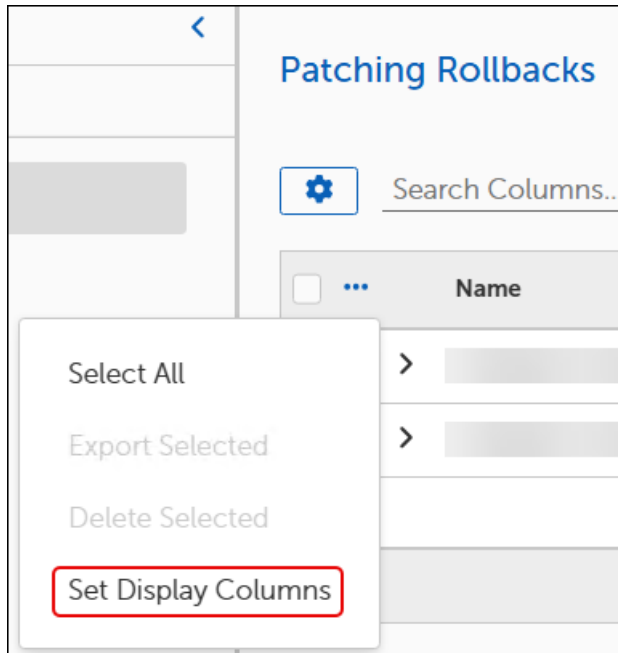
3. Enter a new **Name** for the template, and then click **Save as**.



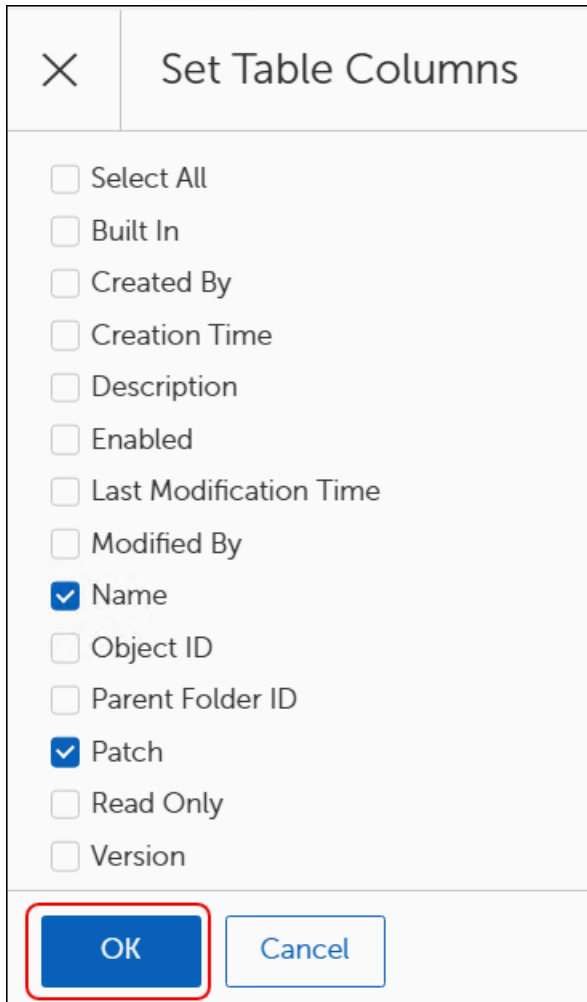
4. Revise the **Description** to reflect any changes needed for the copy, and then click **Save**.
5. Select **Back to Rollbacks** on the upper-left corner of the template to return to the **Rollbacks** table and view your changes.

Customize Patching Rollback Table Settings

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



This opens the Set Table Columns dialog.



Set Table Columns

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

OK Cancel

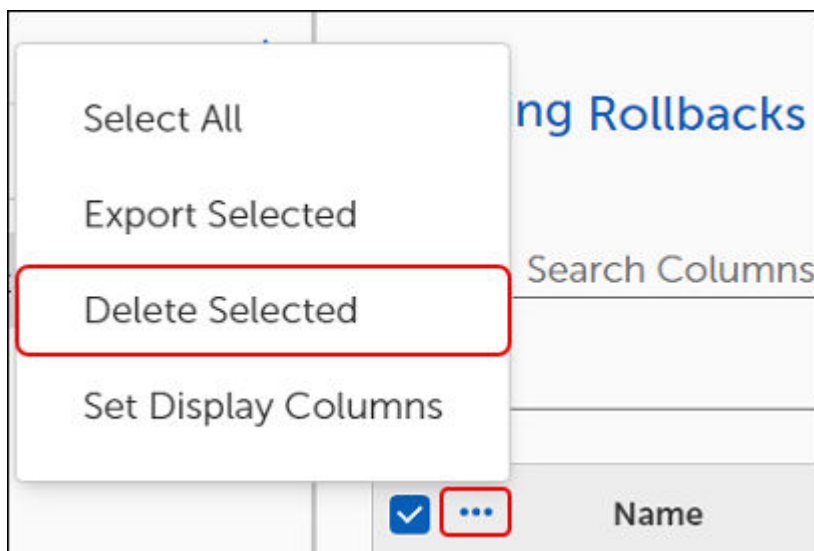
3. Select the **column names** you want the **Patching Rollbacks** table to display, and then click **OK**.

Delete a Rollback

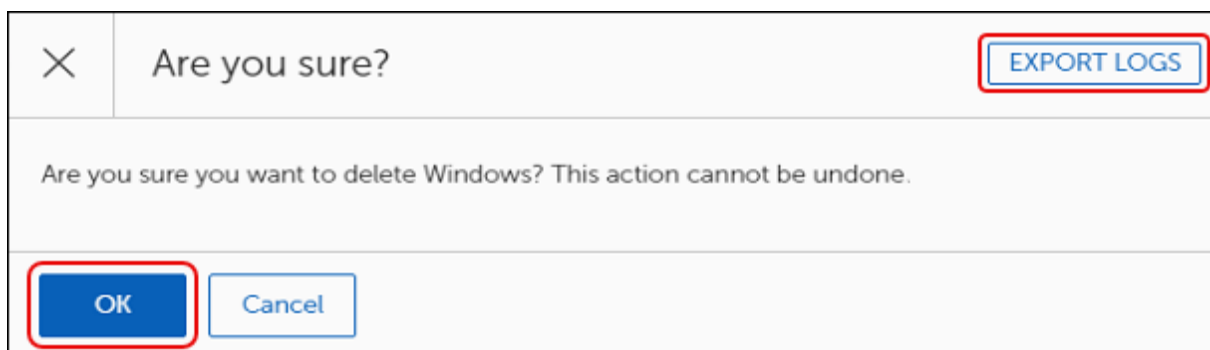
1. Select a **Rollback** template from the **Patching Rollbacks** table of an open [Patching Rollbacks](#) template.

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

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



- Review the Are you sure? dialog:

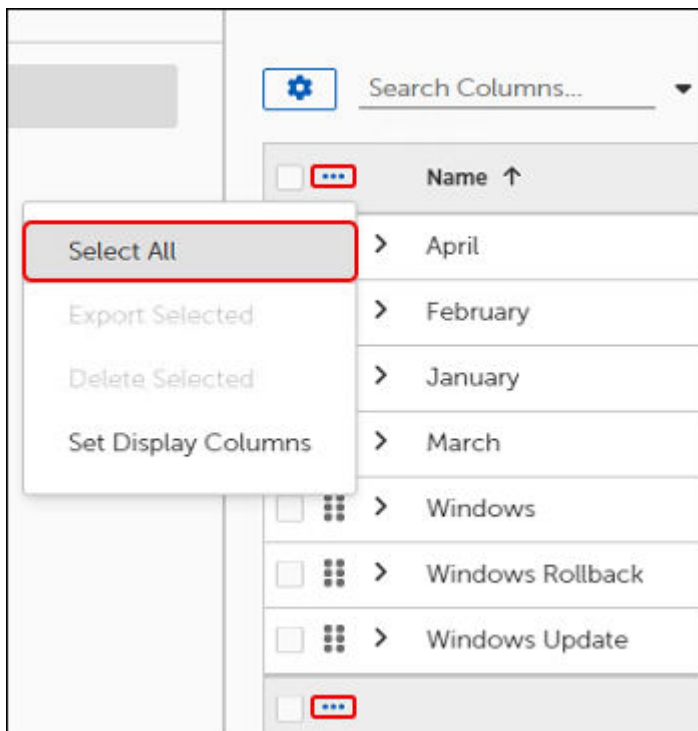


- Select **Export Logs** on the top-right corner of the **Are you sure?** dialog to export trace logs. The trace logs download to your device as a file with a .log extension.

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

Select All Rollbacks

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

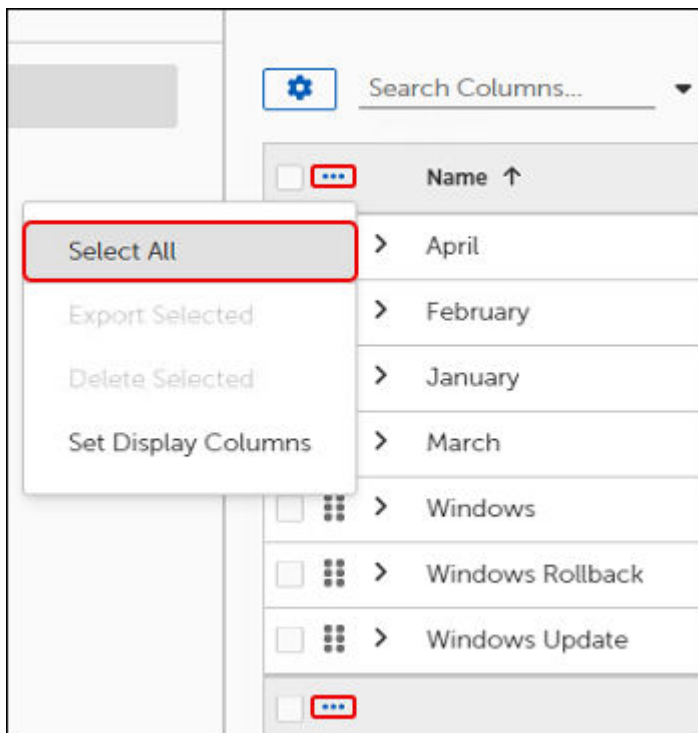


3. Select the ellipsis (...) again, and then choose what you want to do with the selected Rollbacks:
 - To export the selected Rollbacks, see [Select All Rollback to Version Objects](#).
 - To delete the Selected templates, see [Bulk Delete Rollbacks](#).
 - To customize the display columns of the Patching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

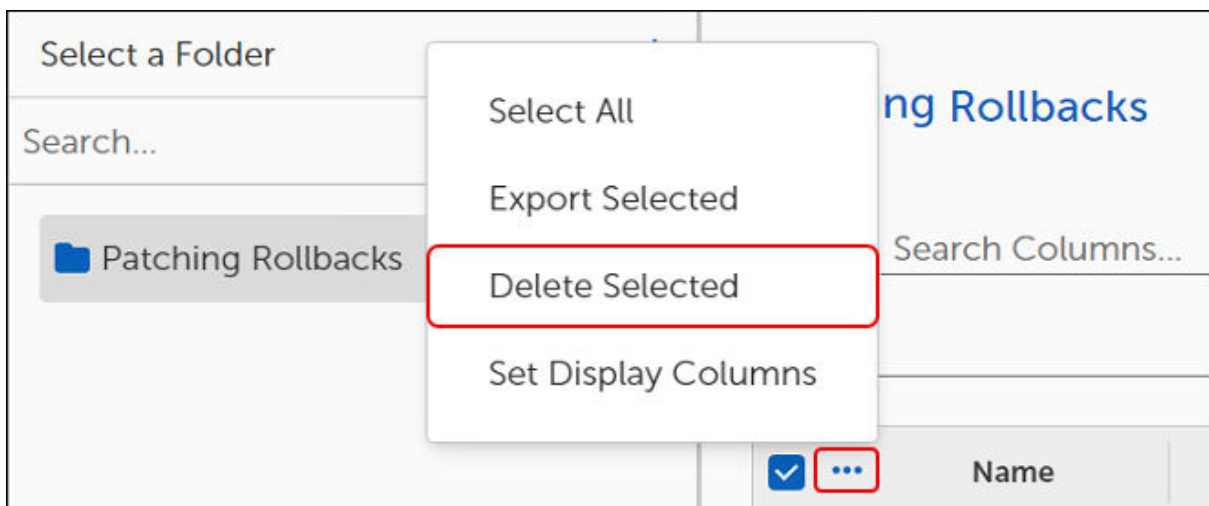
Bulk Delete Rollbacks

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

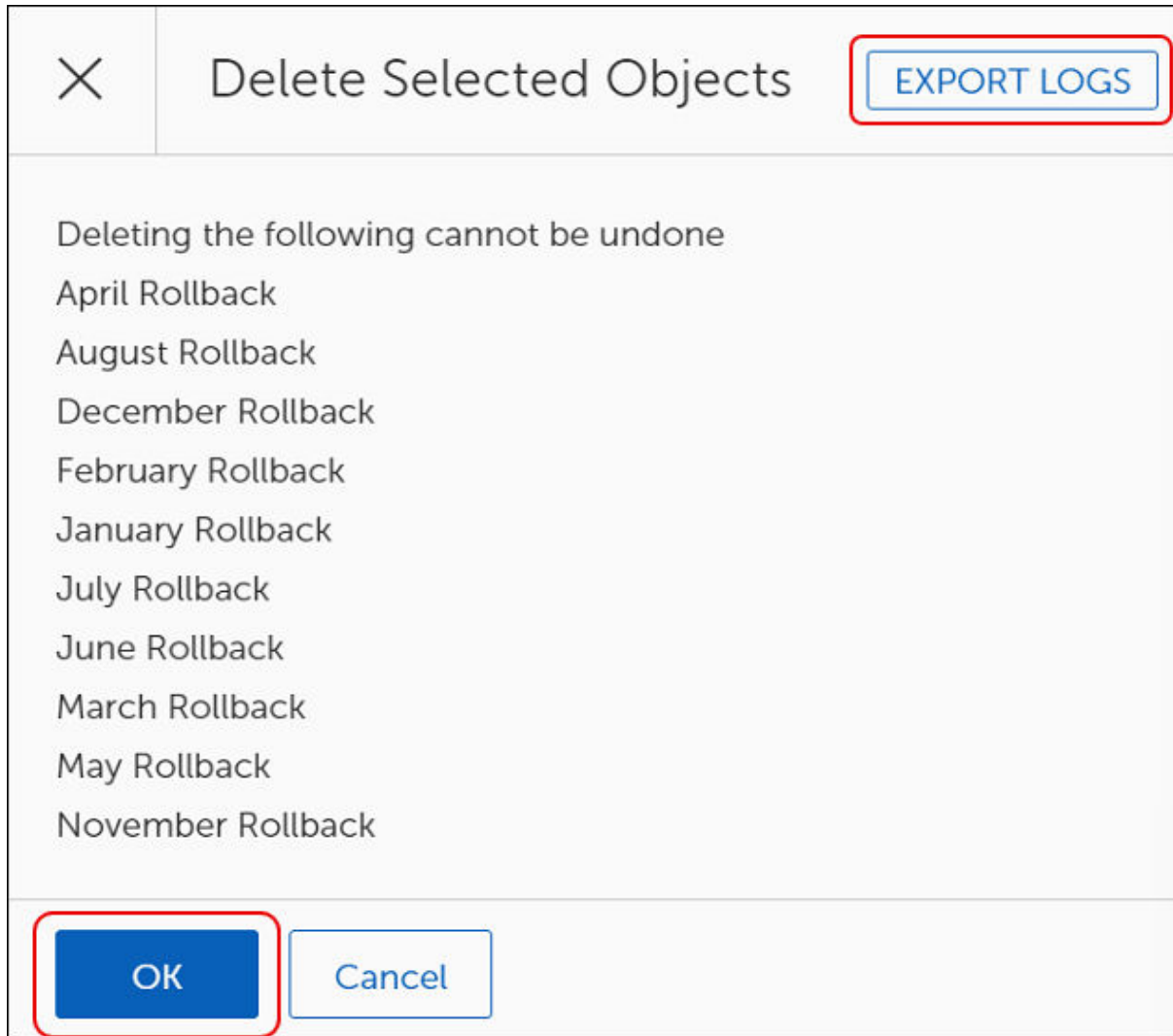
2. Select the **ellipsis (...)** next to **Name**, and then click **Select All**.



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



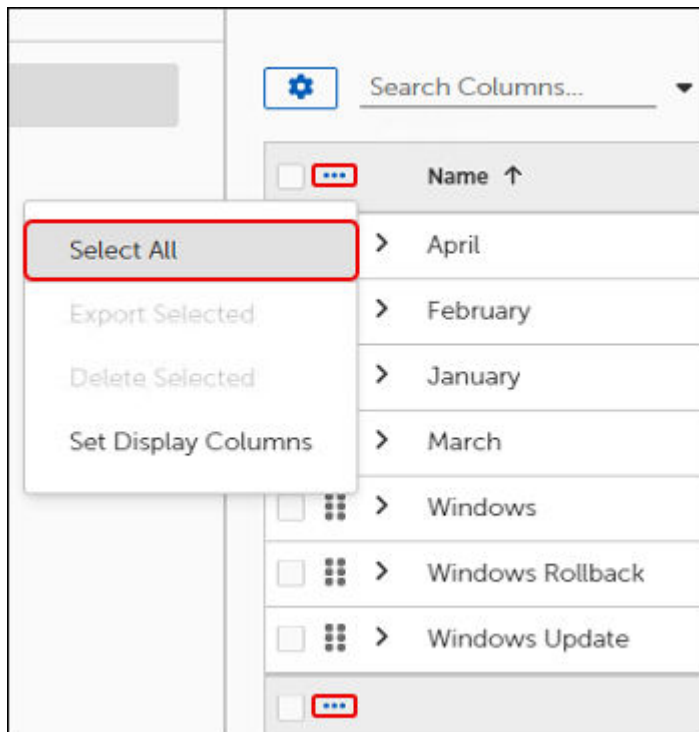
This opens the **Delete Selected Objects** dialog:



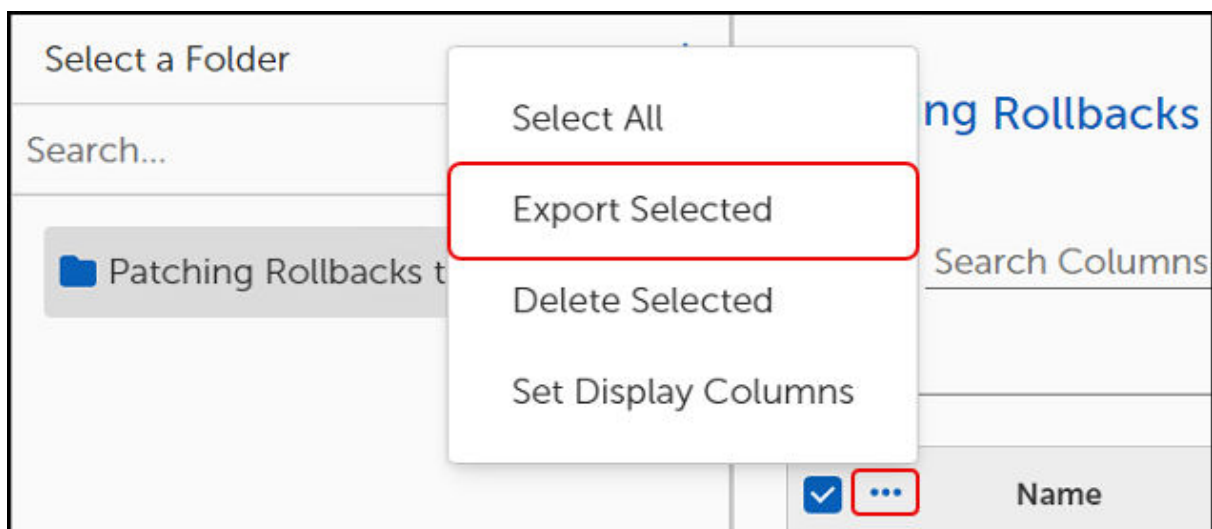
4. (Optional) Select **Export Logs** on the top-right corner of the **Delete Selected Objects** dialog to export trace logs. The trace logs download to your device as a file with a `.log` extension.
5. Select **OK** to delete the Rollbacks. This returns you to the **Patching Rollbacks to** table where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

Export Rollbacks

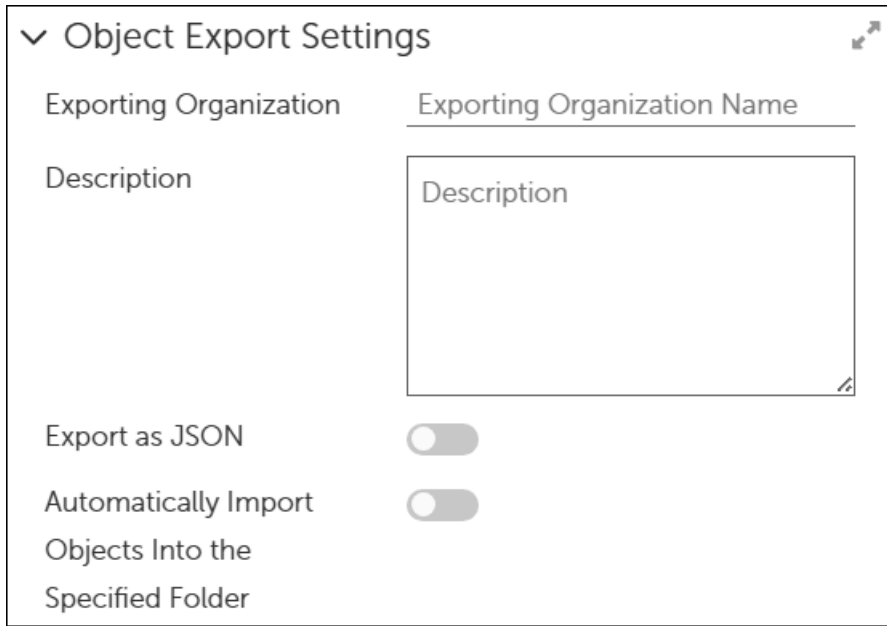
1. Open the **Patching Rollbacks** table (Flex Controls > Rollbacks > Rollback).
2. Select a single **Patching Rollback** from the table, or click the **ellipsis (...)** next to Name, and then click **Select All** to export all Rollbacks



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

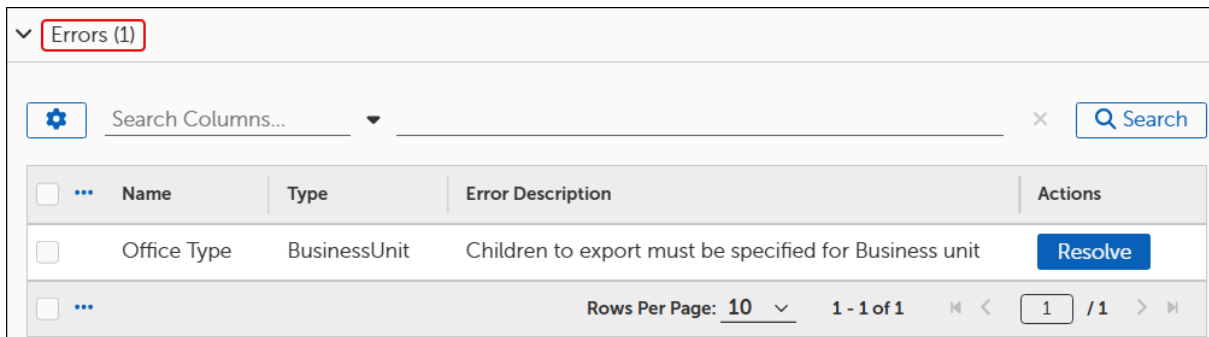


This opens the **Object Export Settings**:



The screenshot shows the 'Object Export Settings' configuration panel. It includes a dropdown for 'Exporting Organization' with the value 'Exporting Organization Name', a text area for 'Description', and two toggle switches: 'Export as JSON' and 'Automatically Import Objects Into the Specified Folder', both of which are currently turned off.

If Object Export Settings command returns an error similar to the following, see [Resolve Export Errors](#) errors:



The screenshot shows an error message table with the following structure:

Name	Type	Error Description	Actions
Office Type	BusinessUnit	Children to export must be specified for Business unit	Resolve

Additional details from the screenshot include a search bar, a 'Search Columns...' dropdown, and pagination controls showing 'Rows Per Page: 10' and '1 - 1 of 1'.

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

Configure Object Export Settings

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



Object Export Settings

Exporting Organization

Description

Export as JSON

Automatically Import Objects Into the Specified Folder

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



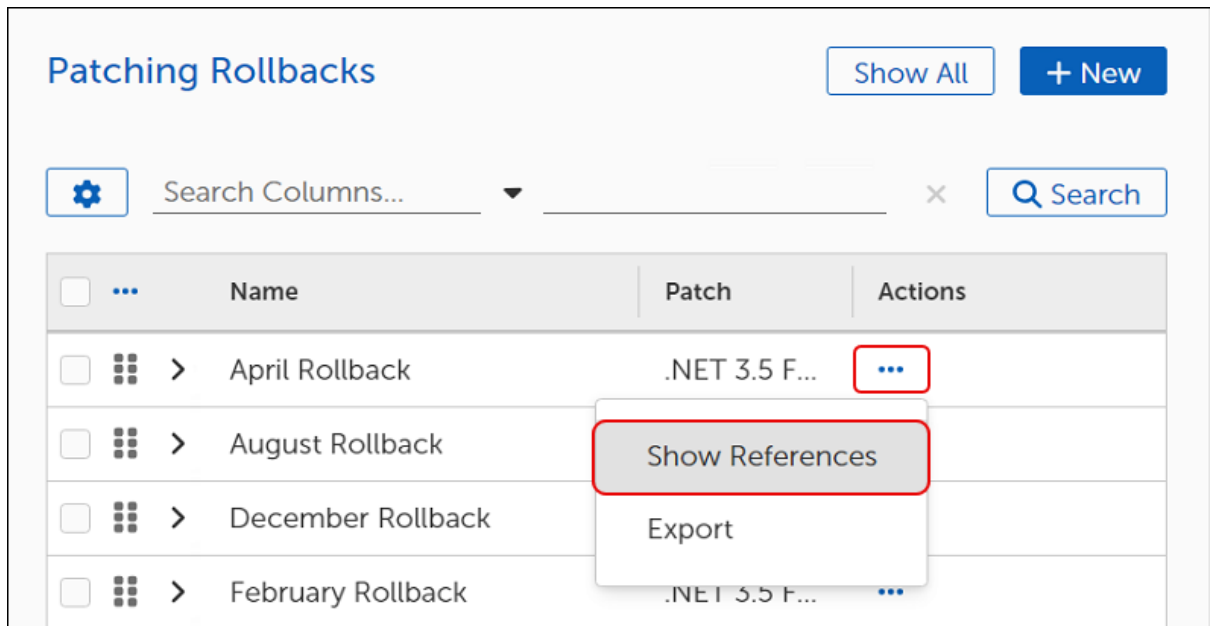
IMPORTANT

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

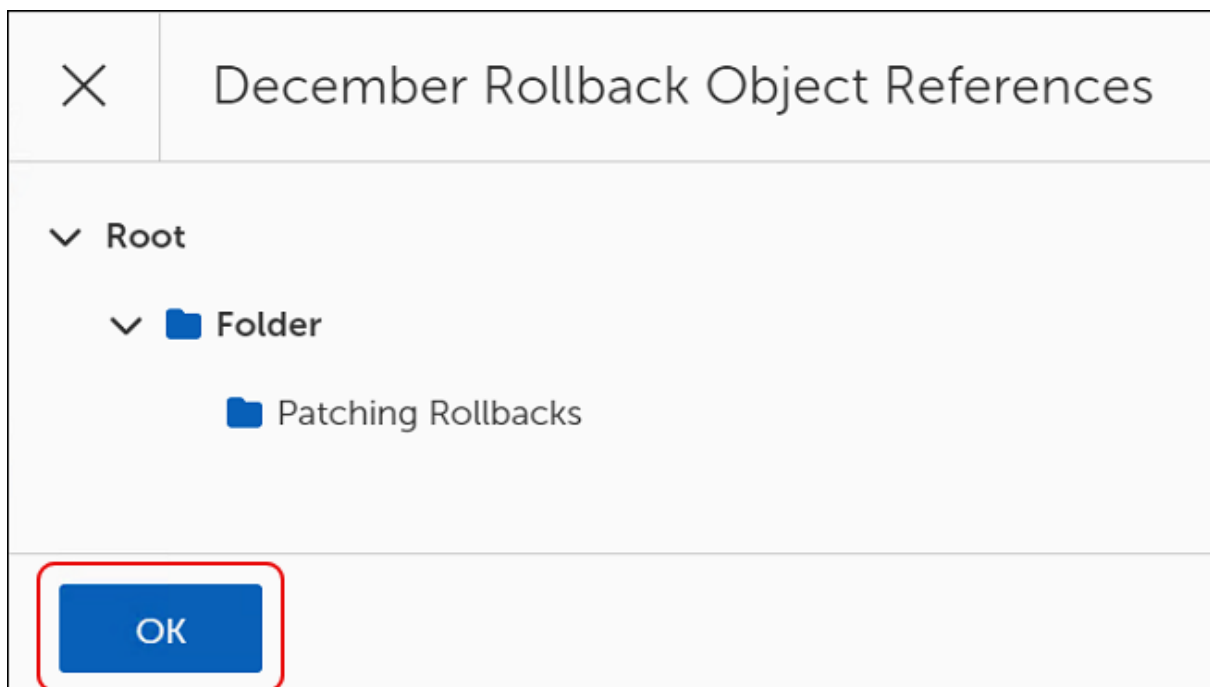
Show Rollback References

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.

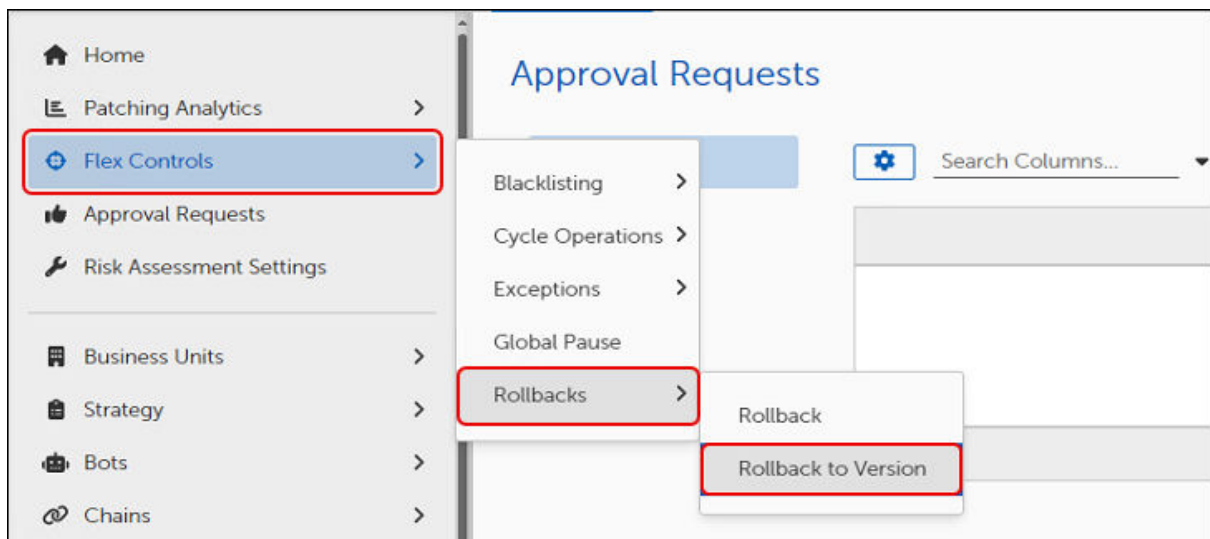
Rollback to Version

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](#).

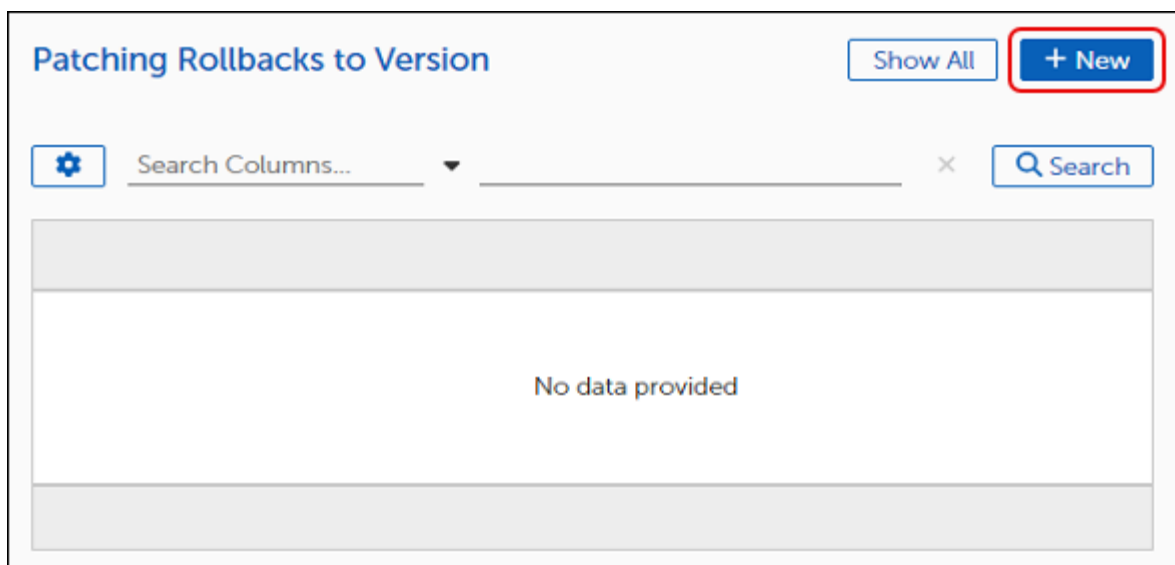
Create a Rollback to Version

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 [OneSite 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.


General Settings

Name *

Description

Patch  * **BROWSE**

Rollback  * **BROWSE**

Target Business Units  *

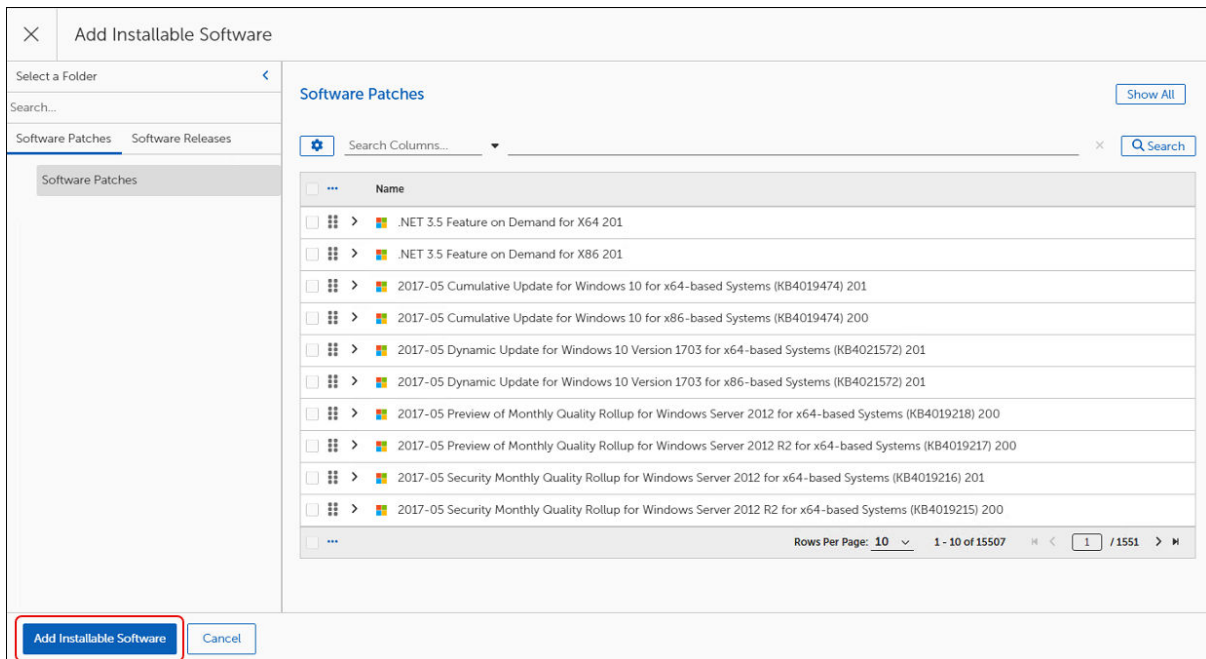
3. Enter a **Name** and a detailed **Description** of your Rollback to Version.
4. [Add the patch or release to roll back from.](#)

Choose the Software Patch or Release Version to Roll Back From

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

Patch  * **BROWSE**

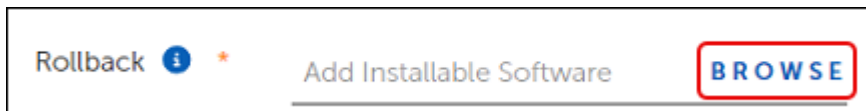
- Choose the **Software Patch** or **Software Release** from the **Add Installable Software** table to roll back from. You can select only one Patch or Release to roll back from.



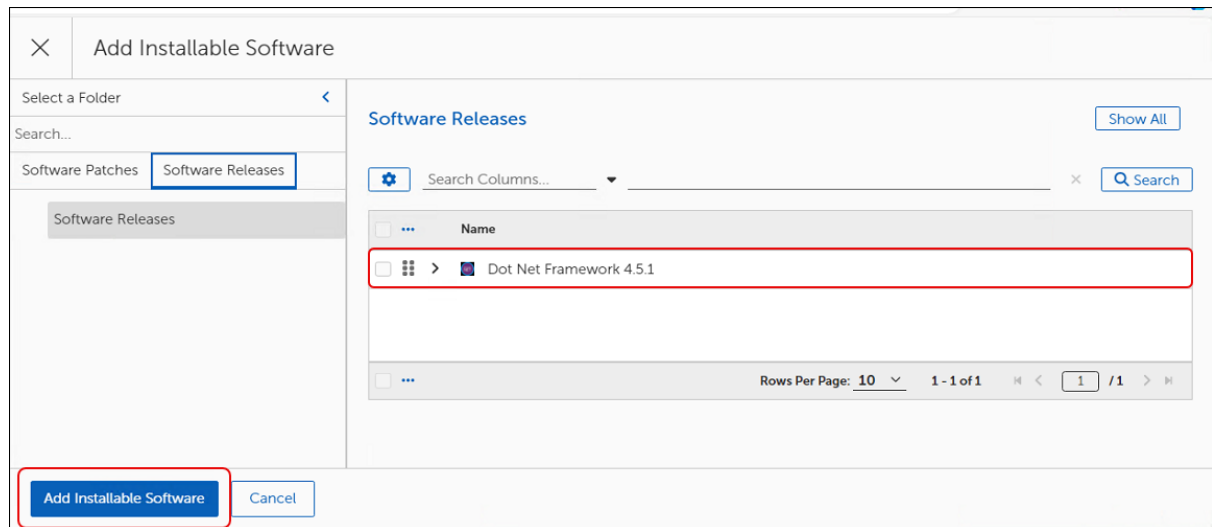
- Select **Add Installable Software** to return to the Rollback to Version template.
- [Choose the software patch or release version to roll back to.](#)

Choose the Software Patch or Release Version to Roll Back To

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



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



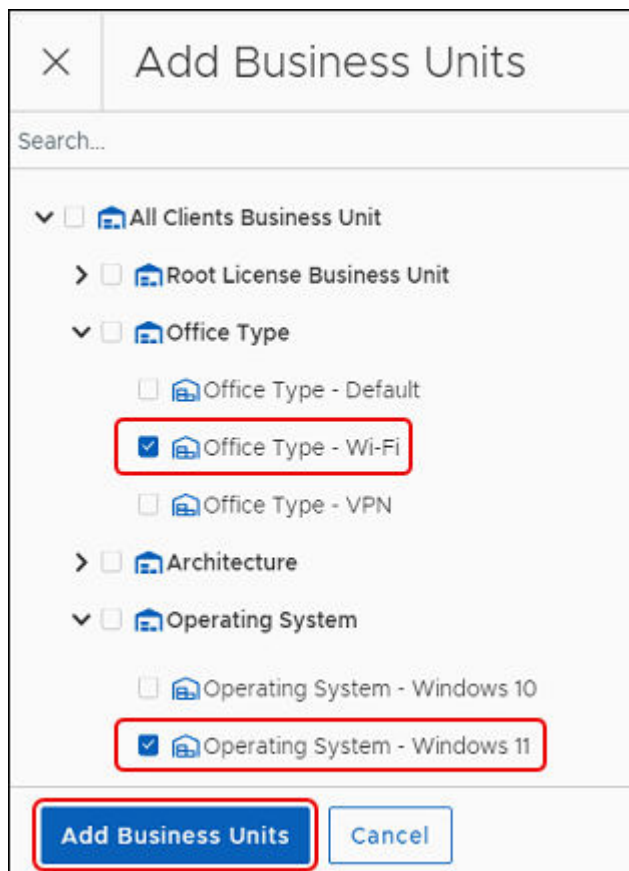
3. Select **Add Installable Software**.
4. [Add target Business Units for the Rollback to Version](#).

Add Business Units for a Rollback to Version

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



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



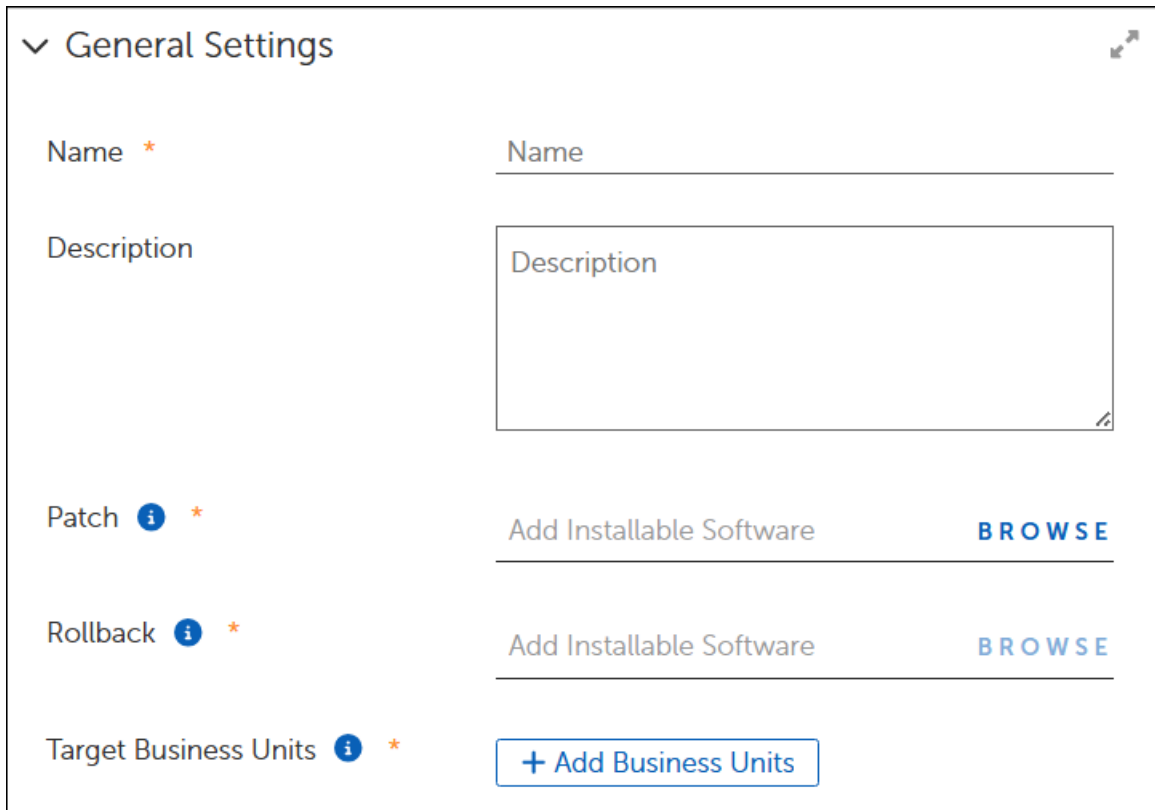
- b. Select one or more **Business Units** to add, and then click **Add Business Units**.
2. Select **Save** to rollback a patch to a prior version.

Edit a Rollback to Version Template

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

Patching Rollbacks to Version			
			<input type="button" value="Show All"/> <input type="button" value="+ New"/>
<input type="button" value="Settings"/>	Search Columns...	<input type="button" value="Search"/>	
<input type="checkbox"/> ...	Name	Patch	Actions
<input checked="" type="checkbox"/> ...	> Windows	.NET 3.5 Feature on Demand for X64	...
<input type="checkbox"/> ...	> Windows Rollback	.NET 3.5 Feature on Demand for X86	...
<input type="checkbox"/> ...	> Windows Update	2017-05 Security Monthly Quality Rollup for Windows Server 2012 for
Rows Per Page: <input type="text" value="10"/>			1 - 3 of 3 <input type="button" value="1"/> / 1

This opens the template.



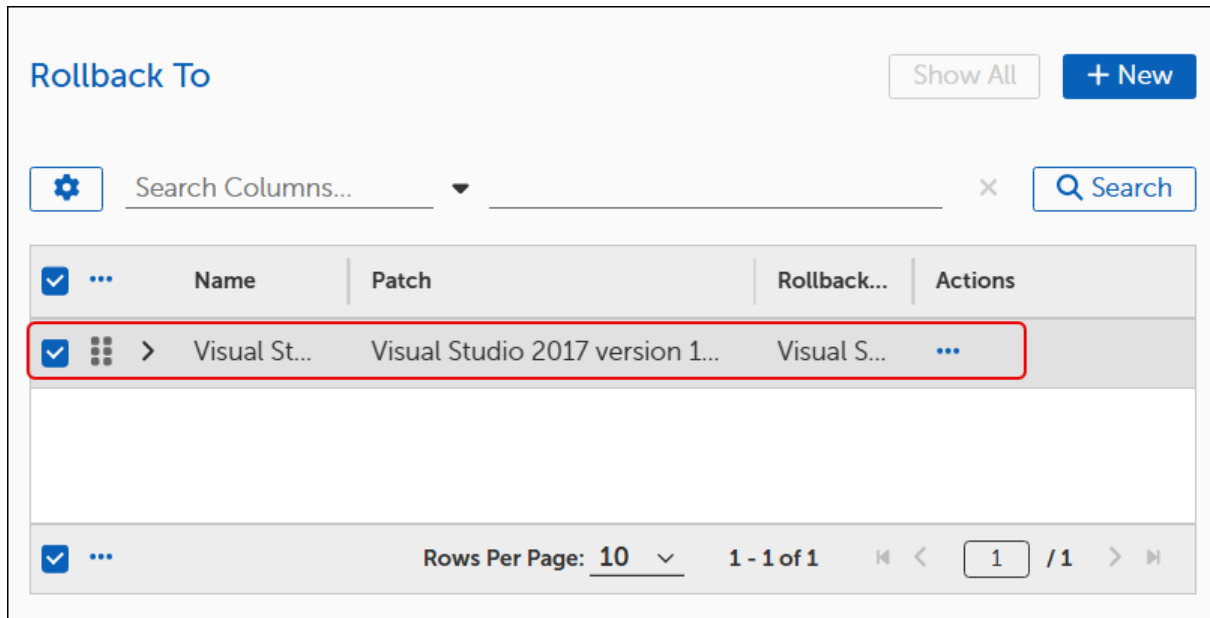
The screenshot shows a 'General Settings' form with the following fields and controls:

- Name ***: A text input field with the placeholder text 'Name'.
- Description**: A large text area with the placeholder text 'Description'.
- Patch** (with an information icon and asterisk): A text input field with the placeholder text 'Add Installable Software' and a blue 'BROWSE' button to its right.
- Rollback** (with an information icon and asterisk): A text input field with the placeholder text 'Add Installable Software' and a blue 'BROWSE' button to its right.
- Target Business Units** (with an information icon and asterisk): A button labeled '+ Add Business Units'.

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

Copy a Rollback to Version Template

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

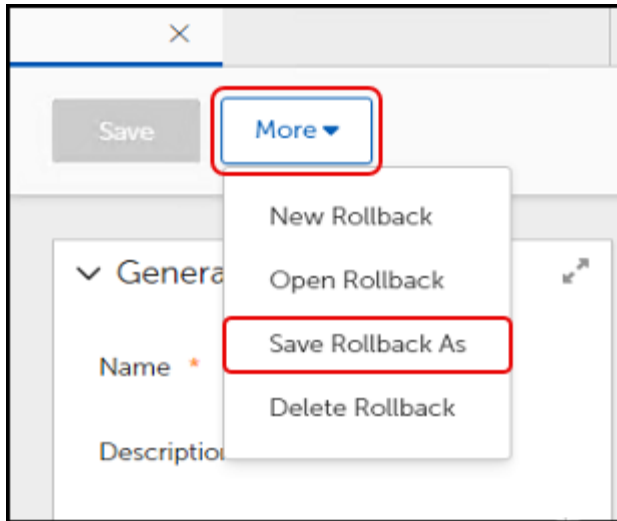


This opens the template.

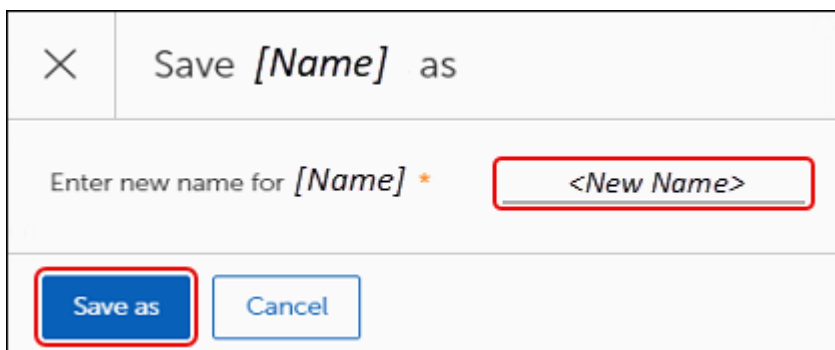
The screenshot shows the 'General Settings' form for a rollback template. The form has the following fields:

- Name ***: Visual Studio
- Description**: This example of a Rollback to Version rolls back Visual Studio 15.9.62 to 15.9.54.
- Patch i ***: Visual Studio 2017 version 15.9.62 update **BROWSE** **X**
- Rollback i ***: Visual Studio 2017 version 15.9.54 update **BROWSE** **X**

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



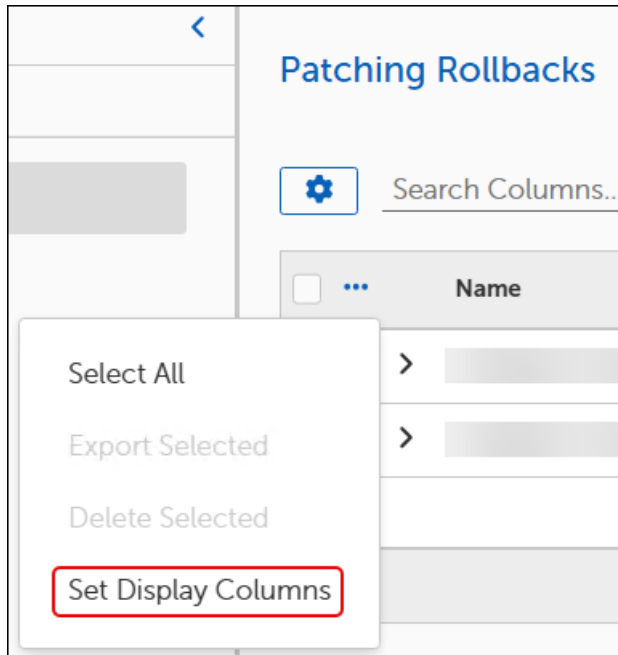
3. Enter a new **Name** for the template, and then click **Save as**.



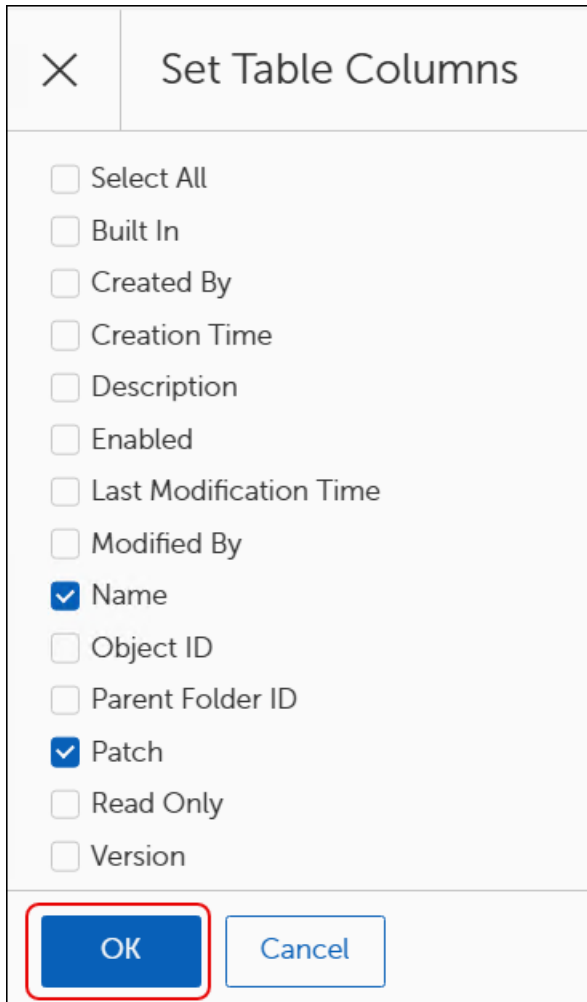
4. Revise the **Description** to reflect any changes needed for the copy, and then click **Save**.
5. Select **Back to Rollbacks** on the upper-left corner of the template to return to the **Rollbacks** table and view your changes.

Customize Patching Rollback Table Settings

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



This opens the Set Table Columns dialog.



Set Table Columns

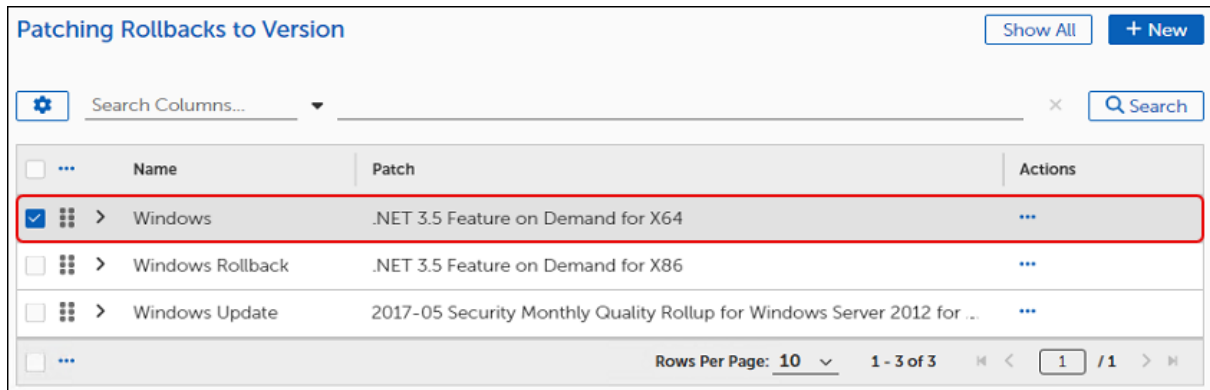
- Select All
- Built In
- Created By
- Creation Time
- Description
- Enabled
- Last Modification Time
- Modified By
- Name
- Object ID
- Parent Folder ID
- Patch
- Read Only
- Version

OK Cancel

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

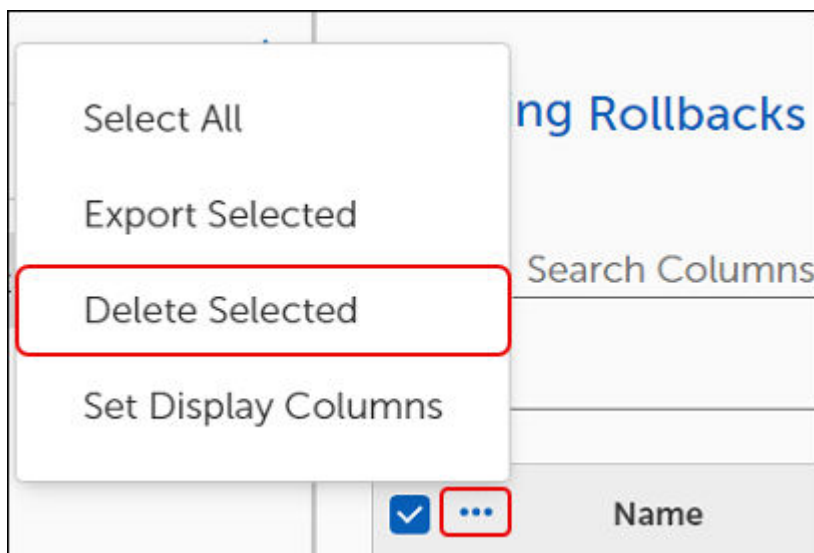
Delete a Rollback to Version

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

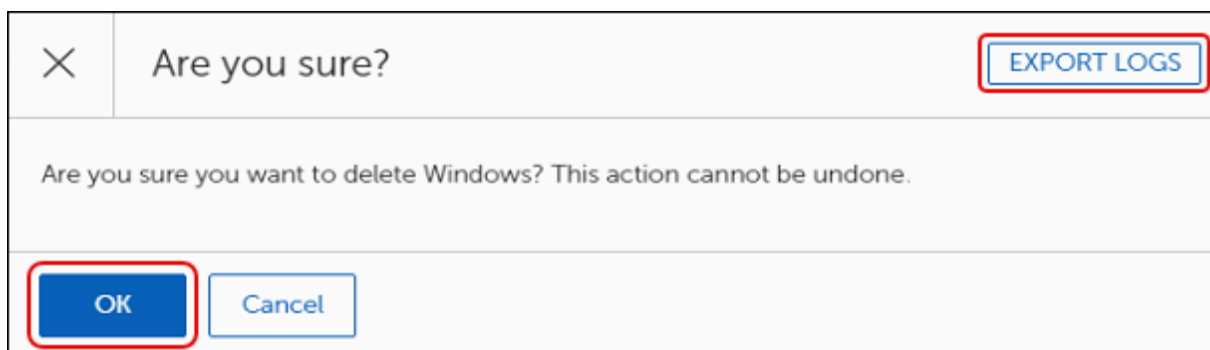


	Name	Patch	Actions
<input checked="" type="checkbox"/>	> Windows	.NET 3.5 Feature on Demand for X64	...
<input type="checkbox"/>	> Windows Rollback	.NET 3.5 Feature on Demand for X86	...
<input type="checkbox"/>	> Windows Update	2017-05 Security Monthly Quality Rollup for Windows Server 2012 for

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



3. Review the Are you sure? dialog:

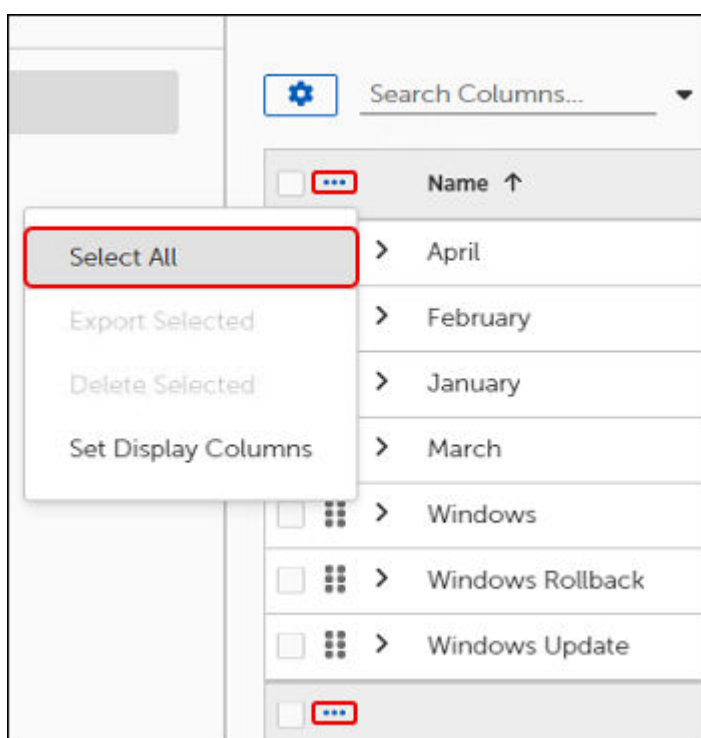


- a. Select **Export Logs** on the top-right corner of the **Are you sure?** dialog to export trace logs. The trace logs download to your device as a file with a .log extension.

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

Select All Rollback to Version Objects

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

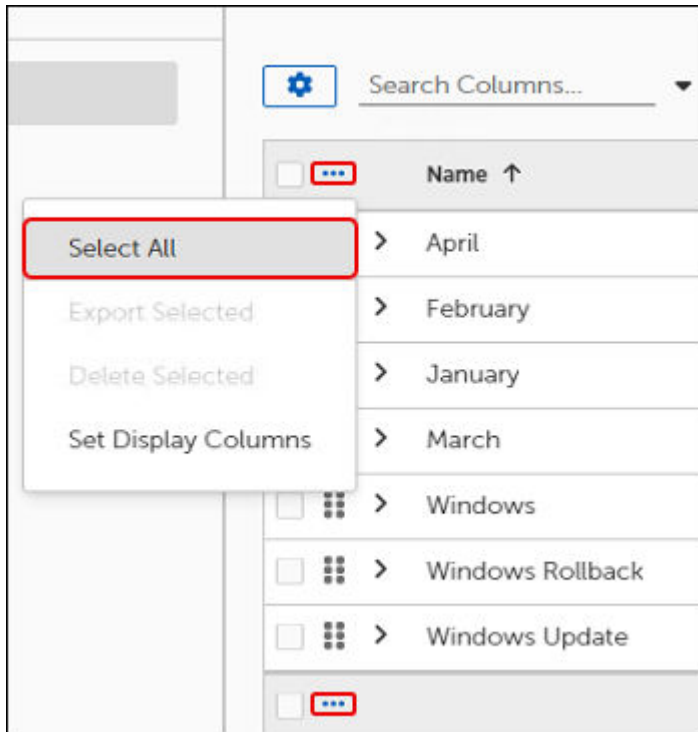


3. Select the ellipsis (...) again, and then choose what you want to do with the selected Rollbacks:
 - To export the selected Rollbacks, see [Select All Rollback to Version Objects](#).
 - To delete the Selected templates, see [Bulk Delete Rollbacks](#).
 - To customize the display columns of the Patching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

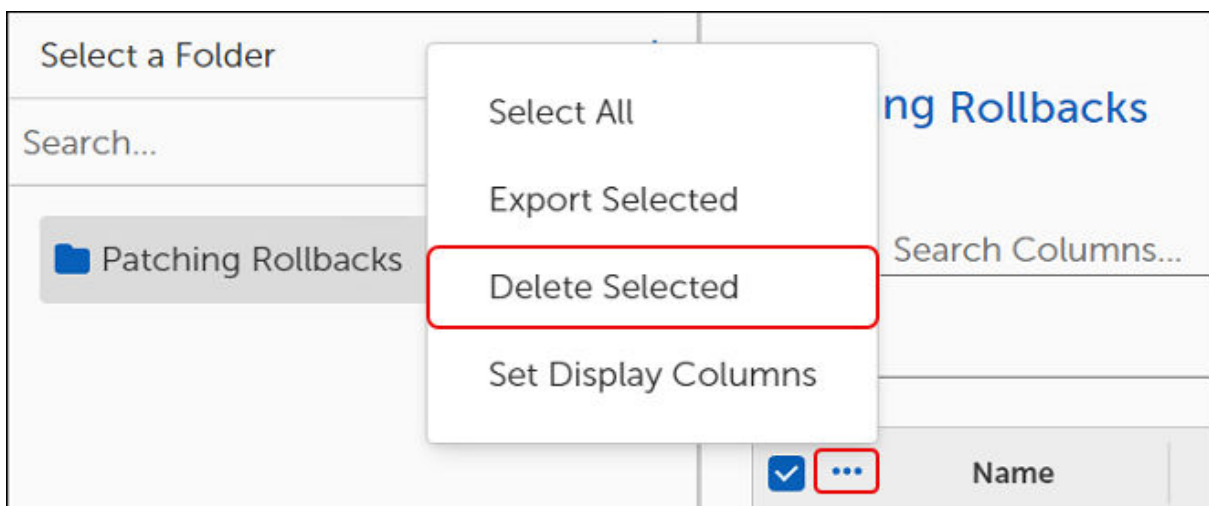
Bulk Delete Rollback to Version

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

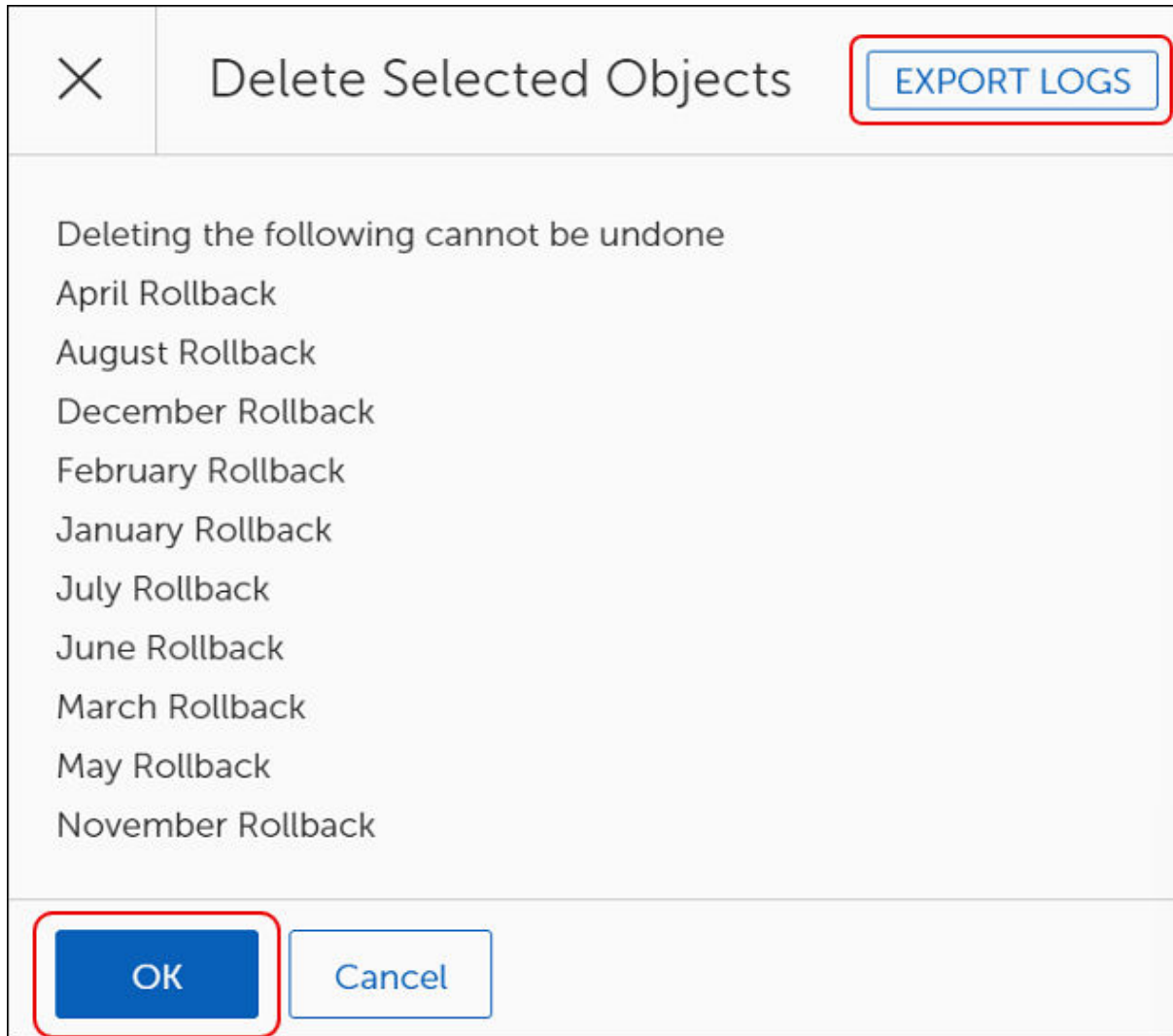
1. Open the **Patching Rollbacks** table (**Flex Controls > Rollbacks > Rollback to Version**).
2. Select the **ellipsis (...)** next to Name, and then click **Select All**.



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



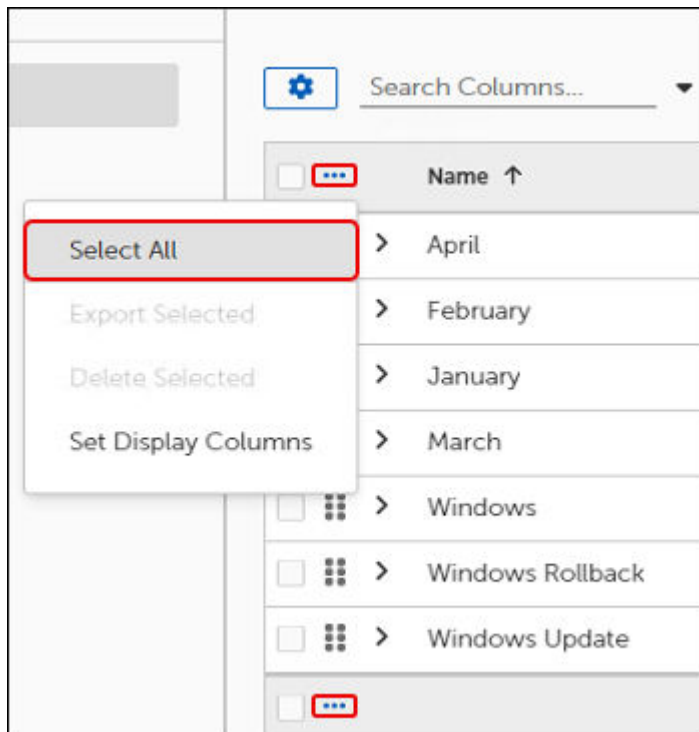
This opens the **Delete Selected Objects** dialog:



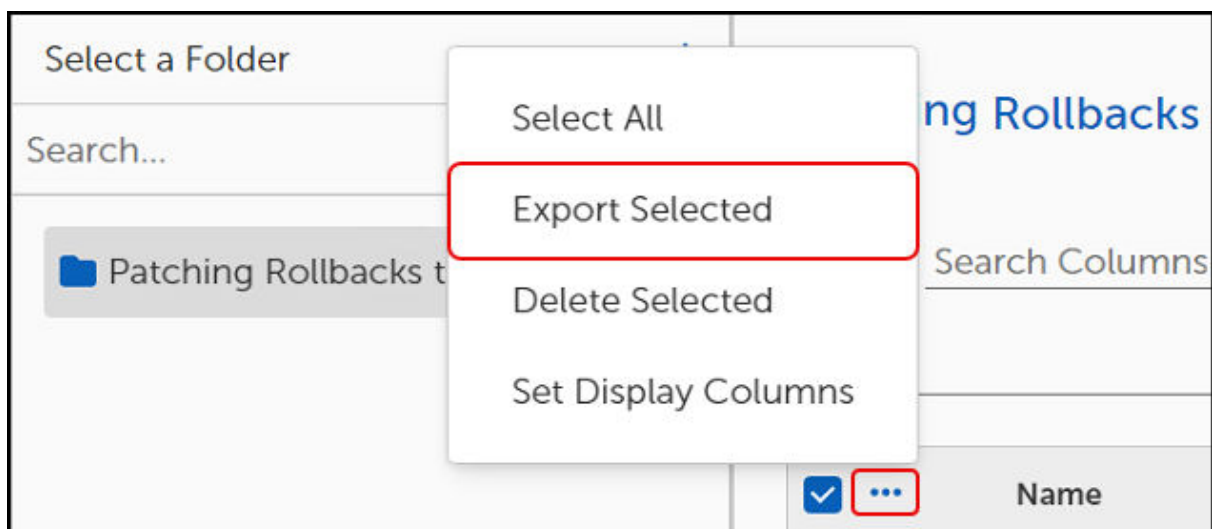
4. (Optional) Select **Export Logs** on the top-right corner of the **Delete Selected Objects** dialog to export trace logs. The trace logs download to your device as a file with a .log extension.
5. Select **OK** to delete the Rollbacks. This returns you to the **Patching Rollbacks to Version** table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

Export Rollback to Version

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



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



This opens the **Object Export Settings**:

▼ Object Export Settings ↗

Exporting Organization

Description

Description

Export as JSON

Automatically Import Objects Into the Specified Folder

If Object Export Settings command returns an error similar to the following, see [Resolve Export Errors](#) errors:

▼ Errors (1)

Search Columns... ✕

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

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

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

Configure Object Export Settings

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



Object Export Settings

Exporting Organization

Description

Export as JSON

Automatically Import Objects Into the Specified Folder

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



IMPORTANT

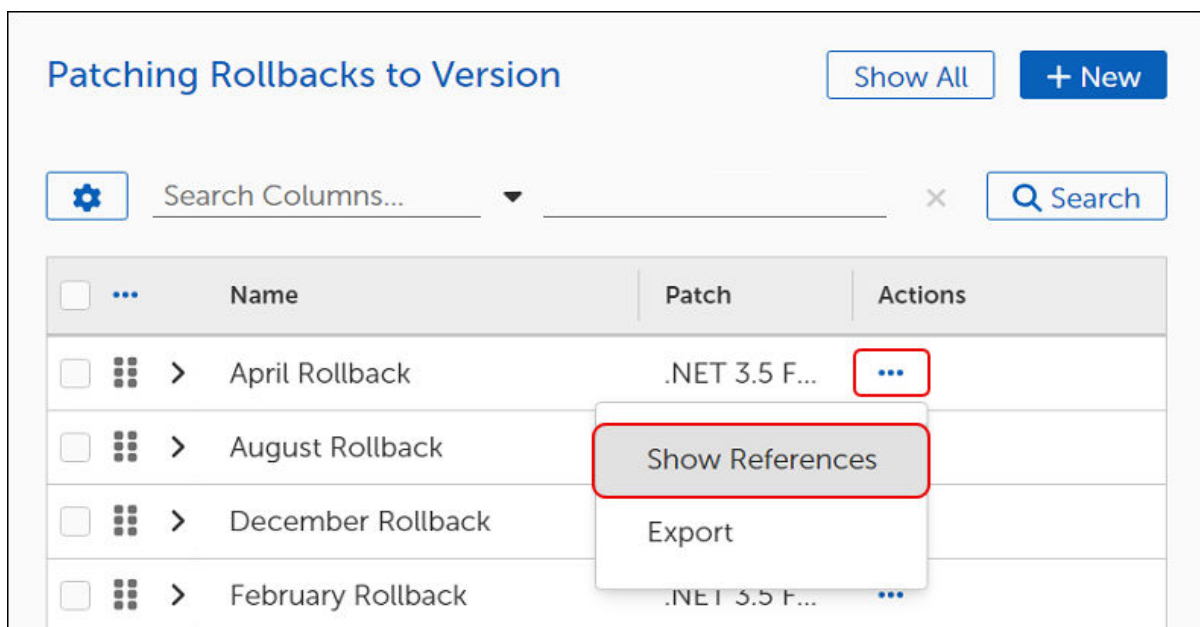
Adaptiva no longer supports the **Export to Linked Servers** functionality. Do not make any changes to the default settings.

Show Rollback to Version References

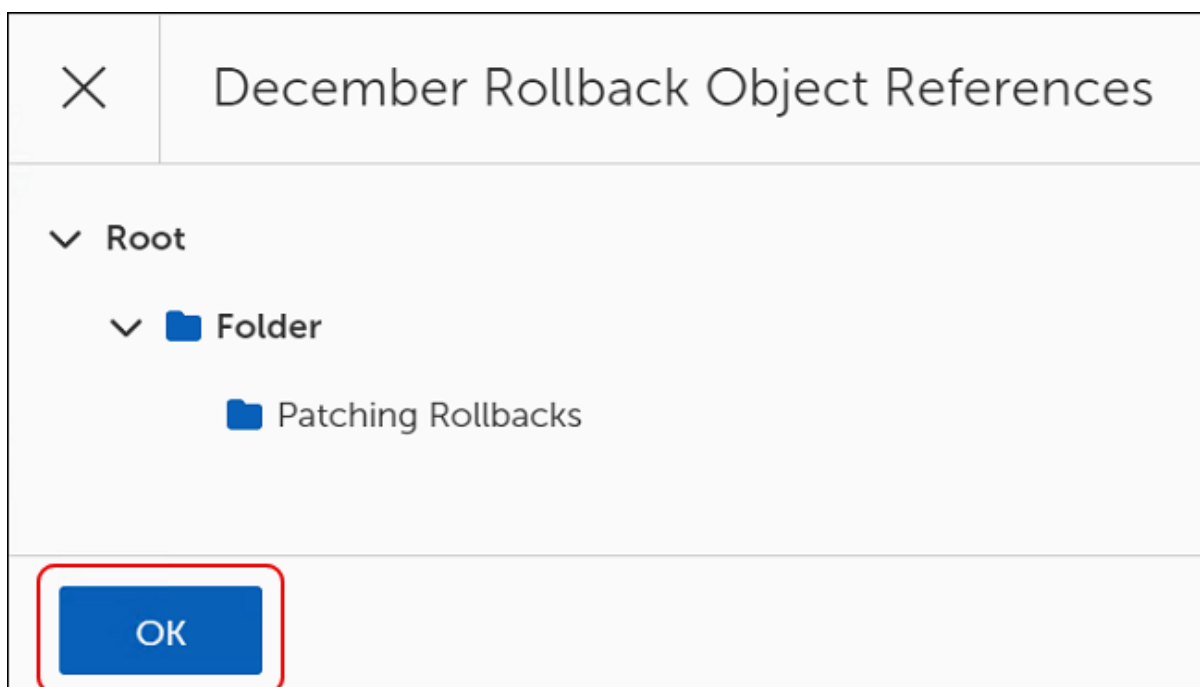
To view the folder location of a Rollback to Version template, complete the following steps:

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

2. Select the **ellipses (...)** in the **Actions** column in the Patching Rollbacks to Version table, and then select **Show References**.



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



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

Approval Requests

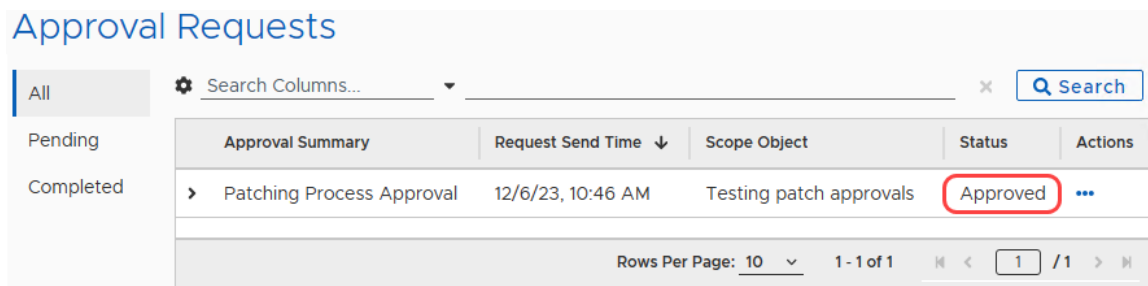
Some Patching Strategies require patch manager approval before beginning a patch cycle. The Patching Process looks for an Approval Chain to use when processing approvals and sends notification based on the communication process configured for each approver.

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

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

Approve or Reject a Patch Request

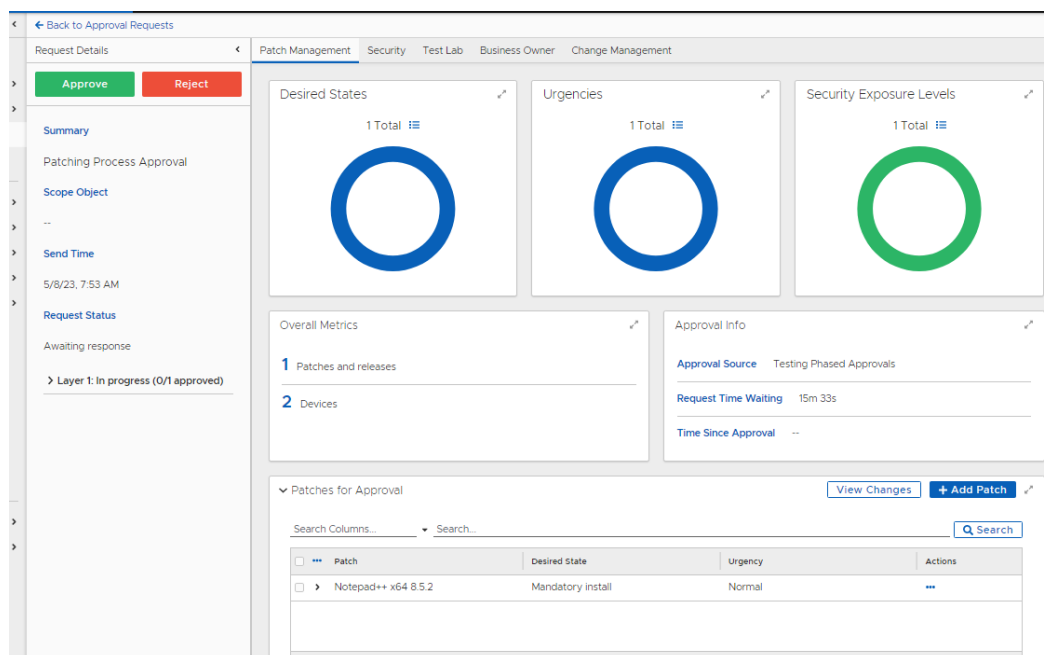
1. Select the **Status** of an item to view details of a request.



The screenshot shows the 'Approval Requests' dashboard. It features a table with columns: Approval Summary, Request Send Time, Scope Object, Status, and Actions. A single row is visible with the following data: Patching Process Approval, 12/6/23, 10:46 AM, Testing patch approvals, and Approved. The 'Approved' status is circled in red. The dashboard also includes a search bar, a 'Search Columns...' dropdown, and a 'Rows Per Page: 10' indicator.

	Approval Summary	Request Send Time ↓	Scope Object	Status	Actions
Completed	> Patching Process Approval	12/6/23, 10:46 AM	Testing patch approvals	Approved	...

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

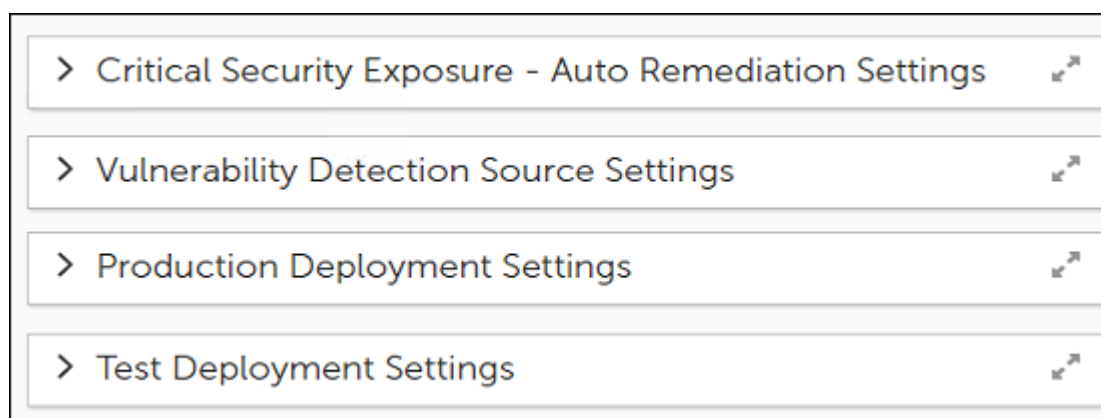


3. Select **Approve** or **Reject**:
 - Select **Approve** to allow the Patching Process to continue processing the patches.
 - Select **Reject** to stop the Patching Process and update the status for the administrator.
4. Select **Back to Approval Requests** at the top of the screen to return to the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

Auto Remediation

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

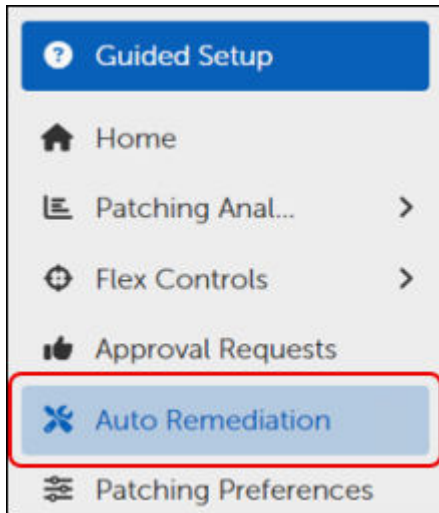
OneSite Patch includes the following configuration options for Auto Remediation:



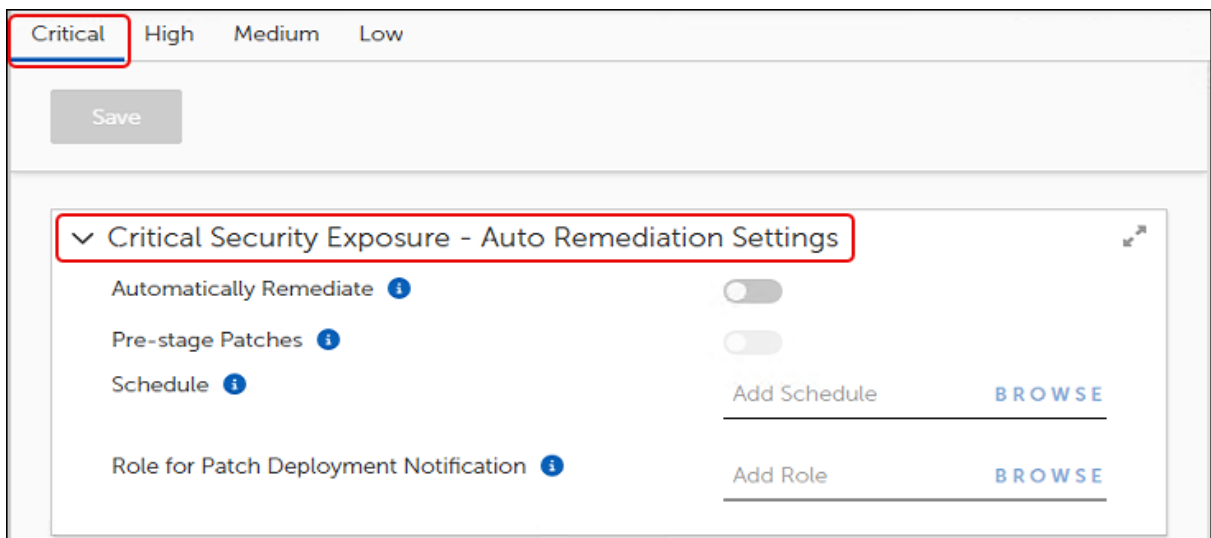
Adaptiva provides configuration options for Critical, High, Medium, or Low Security Exposure Levels.

Access Auto Remediation and Deployment Settings

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



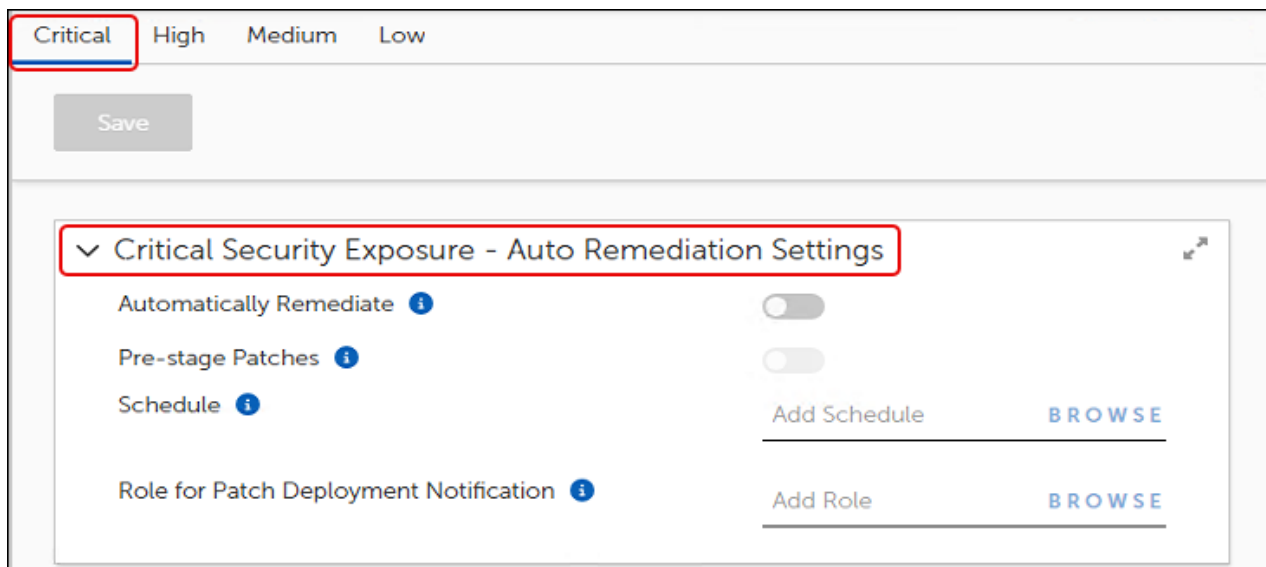
This opens the **Auto Remediation** workspace, which defaults to the Critical exposure level settings.



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

Using Auto Remediation Settings

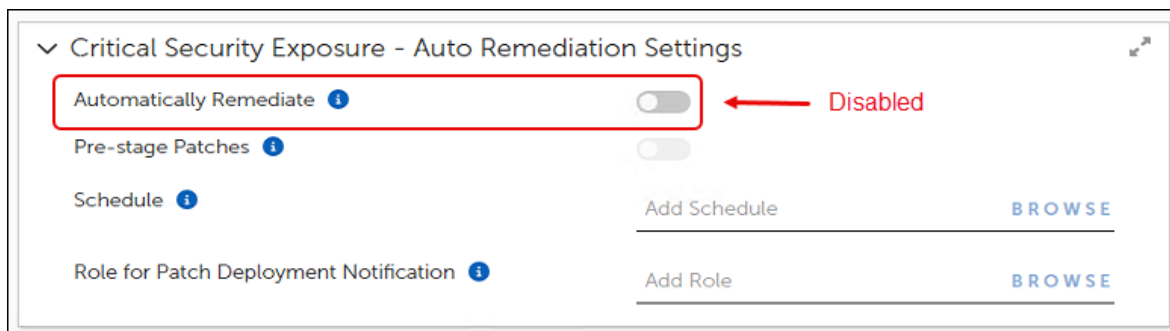
Enable automatic remediation to automatically correct all issues associated with a security level. With Auto Remediation enabled, you can also enable pre-staging of patches, which downloads the content to devices as soon as the patch becomes available. This makes the patch content available on the devices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



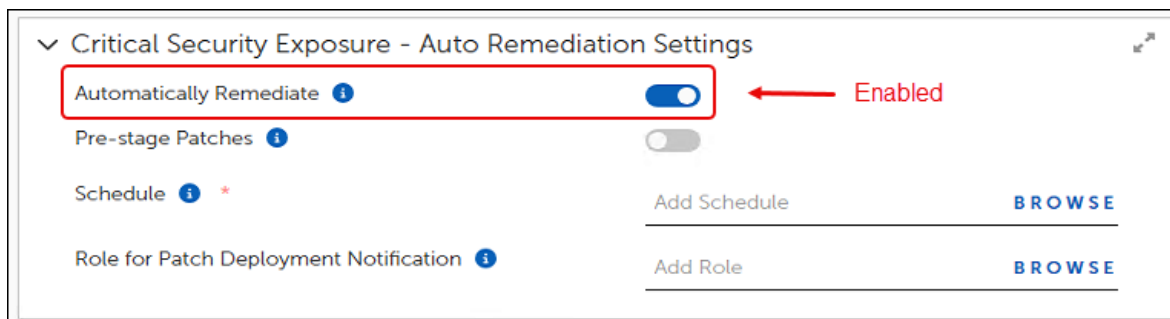
Additional settings include adding a schedule to begin the remediation process and identifying roles that receive notification of the deployment. Repeat the Auto Remediation steps for each urgency level that will use auto remediation. At any time during these configuration steps, click **Save** on the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

Enable Auto Remediation

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



- When enabled, OneSite Patch remediates all vulnerabilities at the security level of the template.



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



IMPORTANT

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

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

Schedules Show All + Create Schedule

Search Columns... × Q Search

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

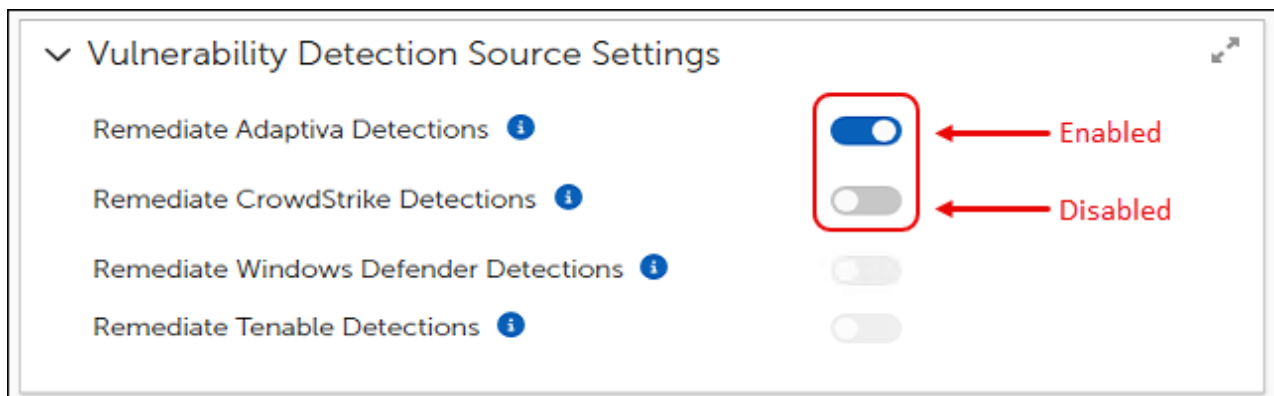
Rows Per Page: 10 1 - 10 of 12 1 / 2

- a. Select **Show All** to see the available roles.

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

Vulnerability Detection Source Settings

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



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

Production Deployment Settings for Auto Remediation

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

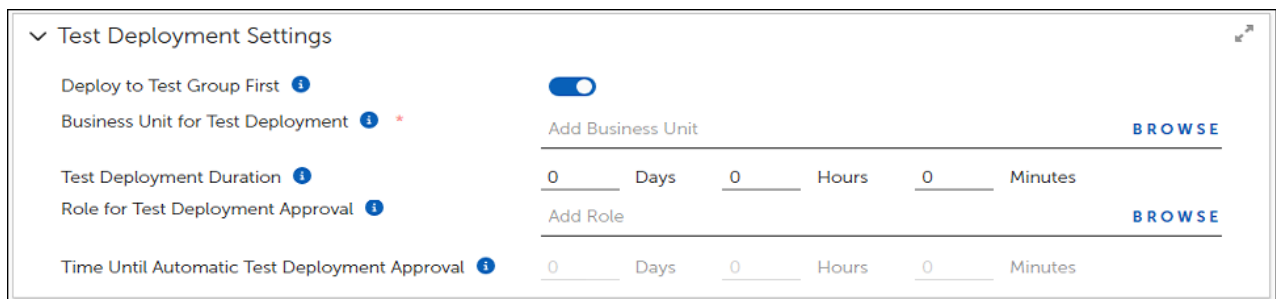
Approval Role: Roles that provide initial approval prior to deployment.

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

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

Test Deployment Settings for Auto Remediation

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



The screenshot shows the 'Test Deployment Settings' configuration page. It includes a toggle for 'Deploy to Test Group First' which is turned on. Below it is a 'Business Unit for Test Deployment' field with an 'Add Business Unit' button and a 'BROWSE' link. The 'Test Deployment Duration' is set to 0 Days, 0 Hours, and 0 Minutes. The 'Role for Test Deployment Approval' field has an 'Add Role' button and a 'BROWSE' link. The 'Time Until Automatic Test Deployment Approval' is also set to 0 Days, 0 Hours, and 0 Minutes.

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

Verify that Auto Remediation Works as Expected

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

Patching Preferences

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

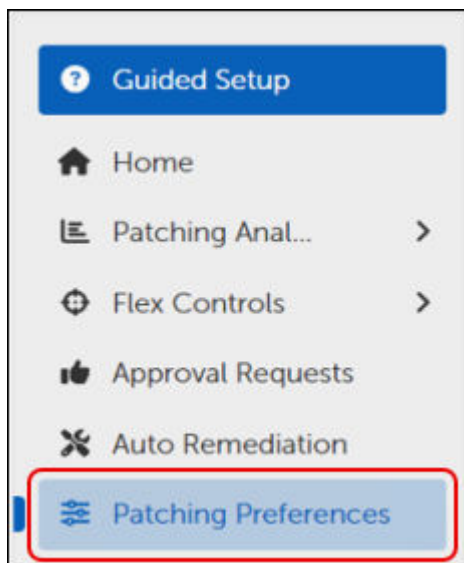
Each Patching Preference object creates its own Business Unit, which users may not edit. The Patching Preference Business Unit shares the same members (devices) as its target Business Unit, as well as any customized preferences.

Using Patching Preferences

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

Access Patching Preferences

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



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

**TIP**

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

Patch Express Patching Preferences			Show All	+ New
Search Columns...			Search	
<input type="checkbox"/>	Name	Actions		
<input type="checkbox"/>	> Preferences - Architecture	...		
<input type="checkbox"/>	> Preferences - Office Type	...		
<input type="checkbox"/>	> Preferences - Operating System	...		
<input type="checkbox"/>	> Preferences - Root License Business Unit	...		
<input type="checkbox"/>	> Preferences - Root Patching Auto Remediation Business Unit	...		
<input type="checkbox"/>	> Preferences - System Type	...		

Rows Per Page: 10 | 1 - 6 of 6 | 1 / 1

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

Create a New Patching Preference

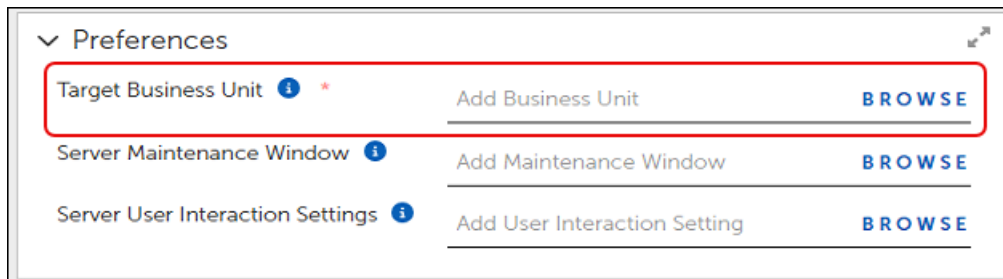
Create a patching preference for each Business Unit that requires unique maintenance window or user interaction settings. At any time during these configuration steps, click **Save** in the upper-left corner of the template to save your changes.

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

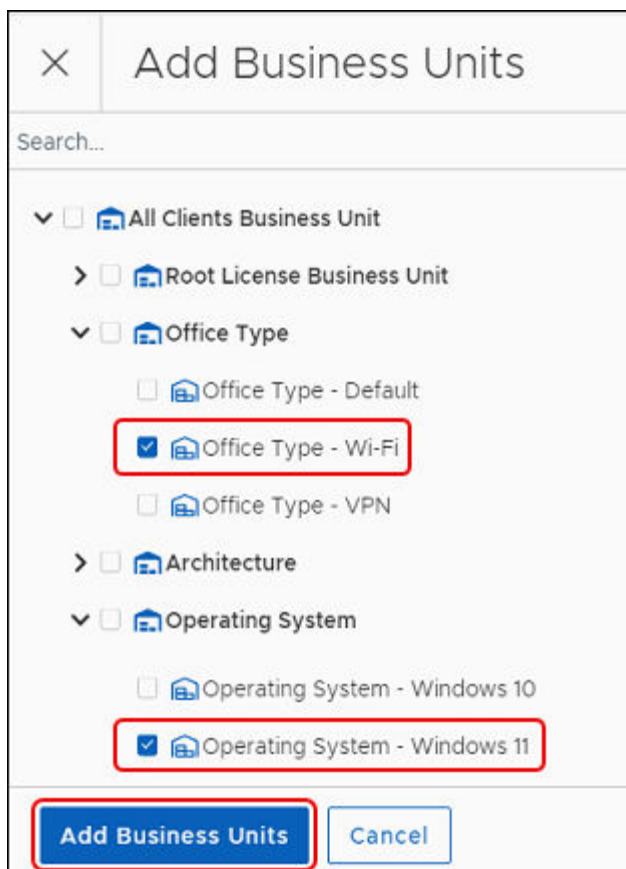
Add a Target Business Unit

Add a Target Business Unit using the following steps:

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



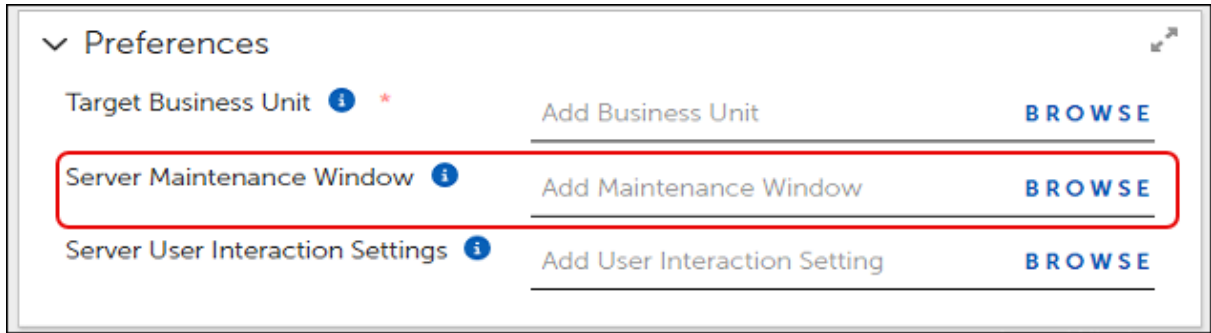
This opens the **Add Business Unit** dialog. The example shows possible choices.



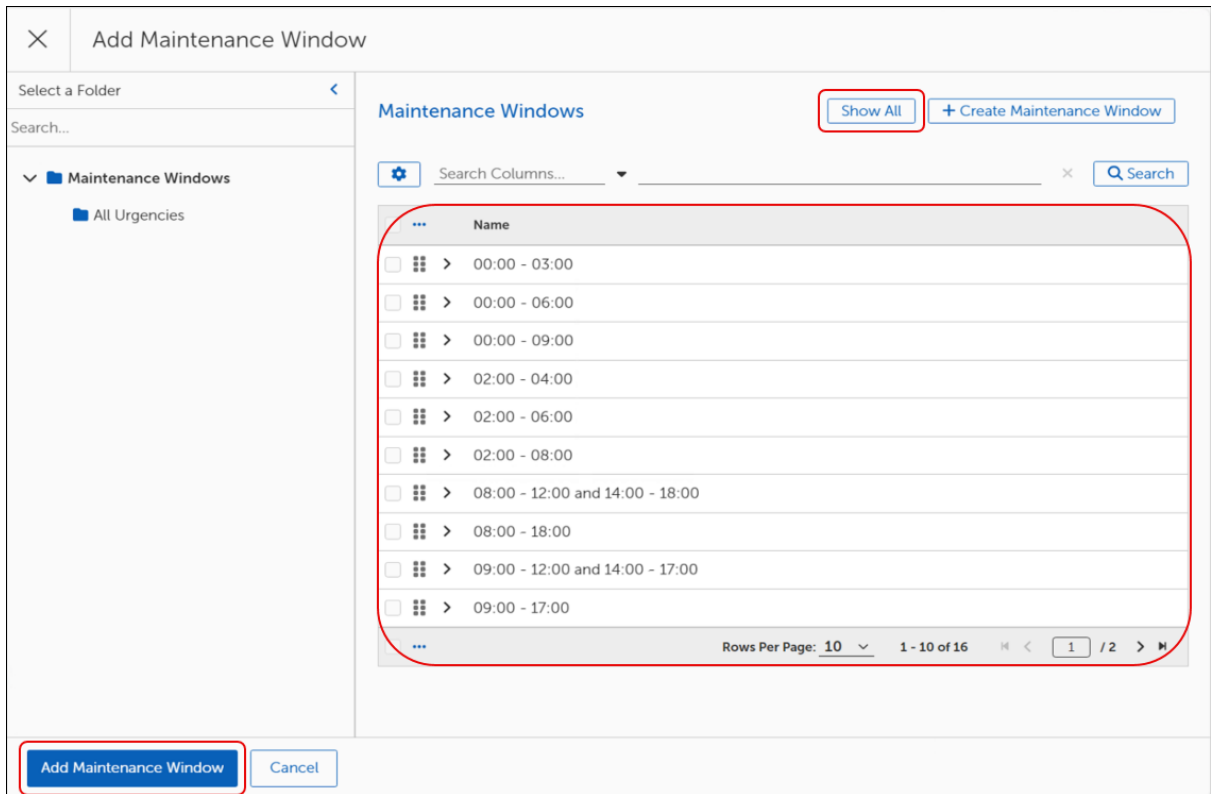
2. Select the Business Unit you want to target.
3. Select **Add Business Unit** on the bottom left of the dialog.

Select a Server Maintenance Window

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



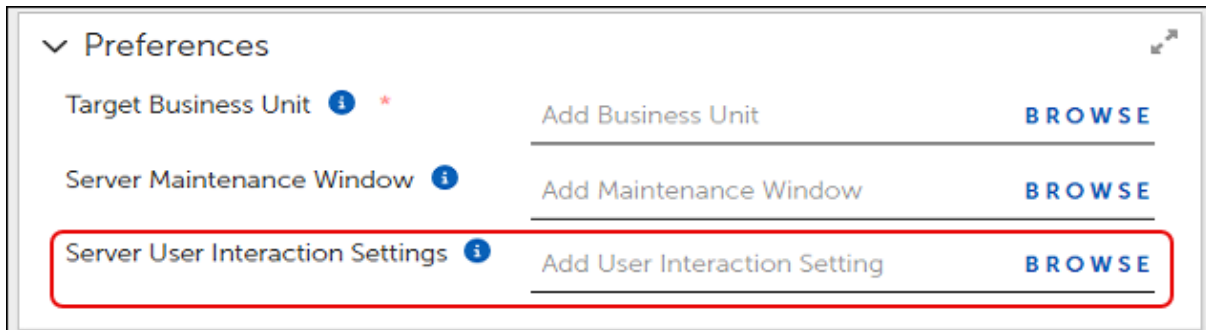
This opens the **Add Maintenance Window** dialog.



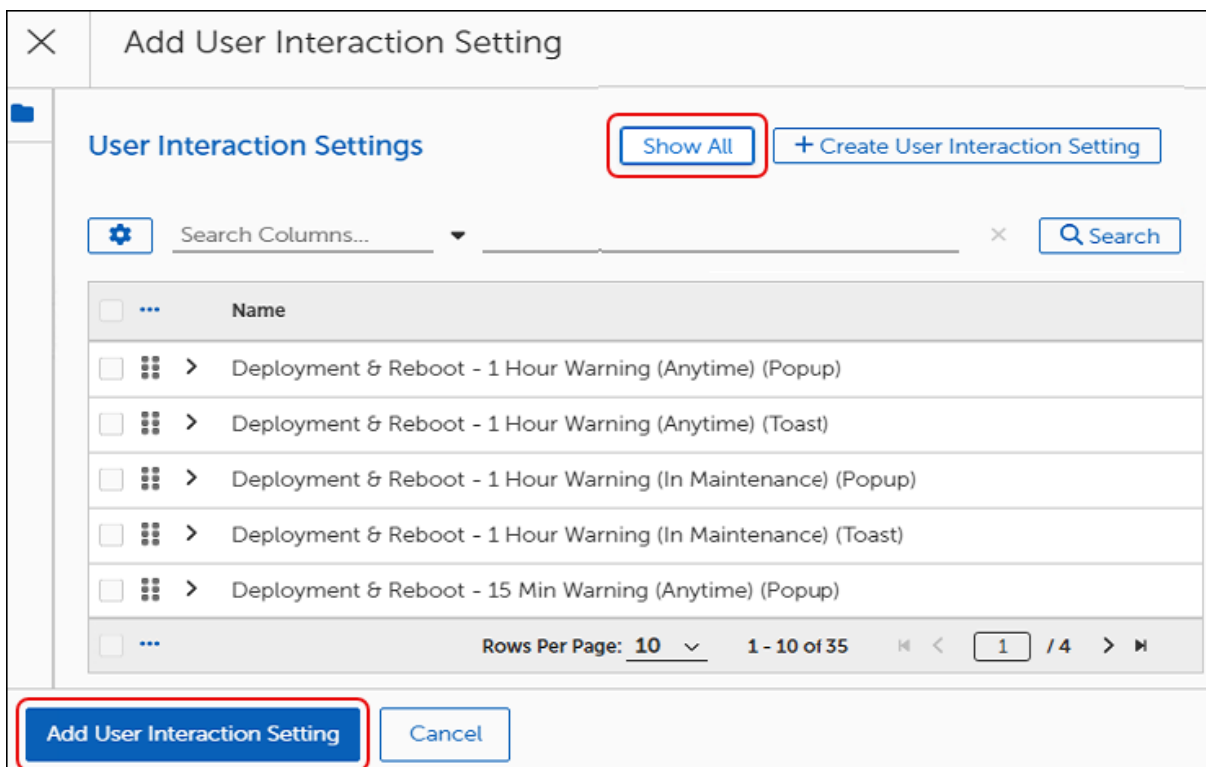
2. Select **Show All** at the upper right to view the available Maintenance Window settings.
3. Select the checkbox aligned with the setting you want to use. To create a new Maintenance Window setting, see [Maintenance Windows](#), then return and repeat this step.
4. Select **Add Maintenance Window**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

Select Server User Interaction Settings

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



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



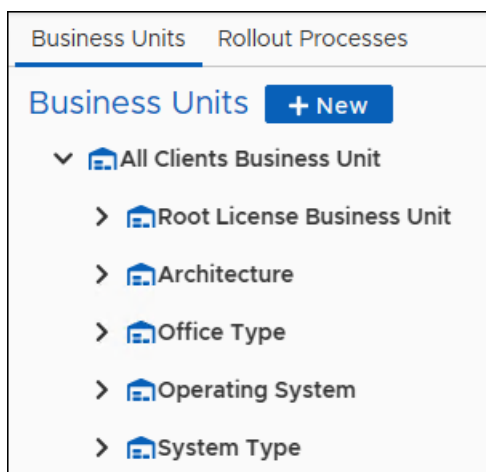
2. Select **Show All** at the upper-right corner to view the available options, and then select the checkbox aligned with the options you want to use. To create a new setting, see [User Interaction Settings](#), then return and repeat this step.
3. Select **Add User Interaction Setting** on the lower-left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

Business Units

Understanding Business Units

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

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



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



IMPORTANT

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

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

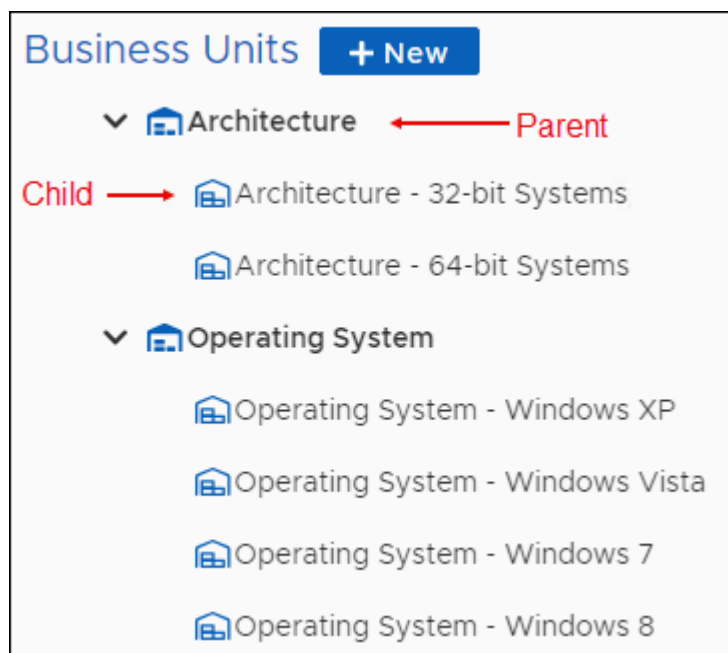
Parent and Child Business Units

Business Unit objects use a parent-child hierarchy. A parent Business Unit may have multiple child Business Units, but a child Business Unit may have only one parent. The folder structure used in 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.



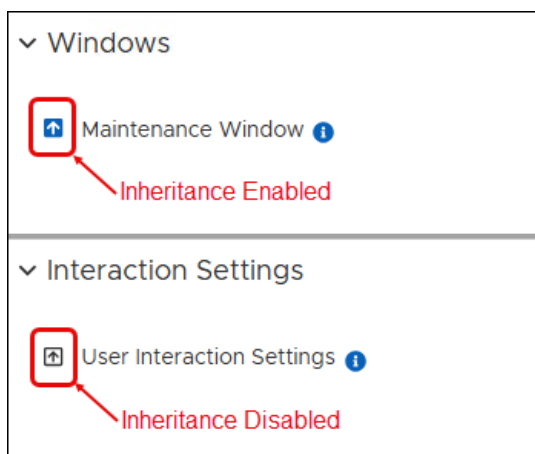
IMPORTANT

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



There is no functional difference between parent and child Business Units. The purpose of the parent/child hierarchy is to allow a child Business Unit to inherit settings from a Parent, which can simplify the creation of Business Units with both

distinct and common requirements. An up-arrow with a blue background preceding a setting or process shows an inherited setting.

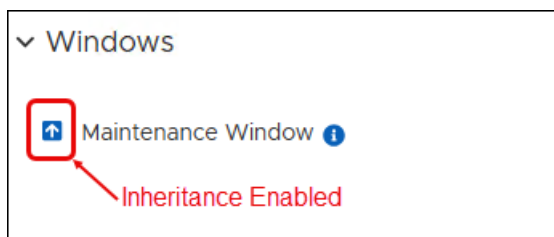


The hierarchical nature of Business Units allows a child Business Unit to inherit settings from its parent. An up-arrow with a blue background preceding a setting or process shows an inherited setting.

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.



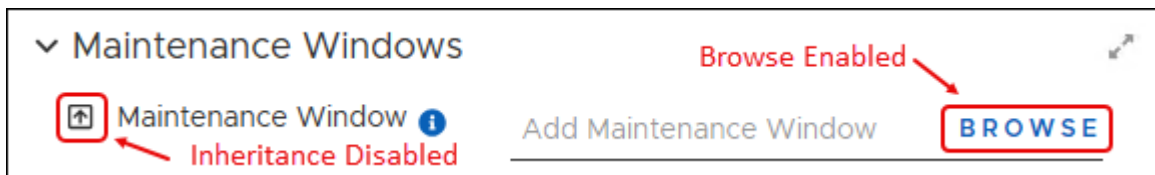
IMPORTANT

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.

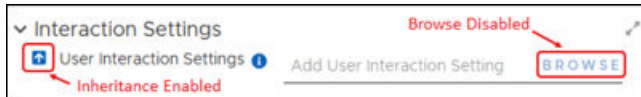
Enable Inheritance

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.



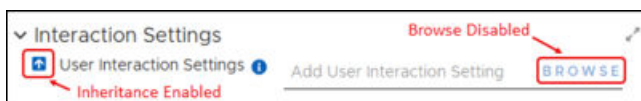
2. Select the up-arrow icon to enable inheritance



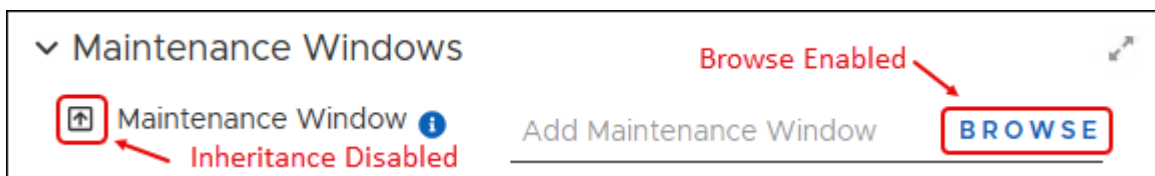
Disable Inheritance

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

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



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



Organizing the Business Unit Hierarchy

You can arrange the Business Unit view in hierarchies that meet the needs of your environment. Parent Business units – bold, top-level folders – pass attributes to child

Business Units – sub-folders – so it is important to maintain those relationships where they exist.

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

Best Practices when Changing Priorities

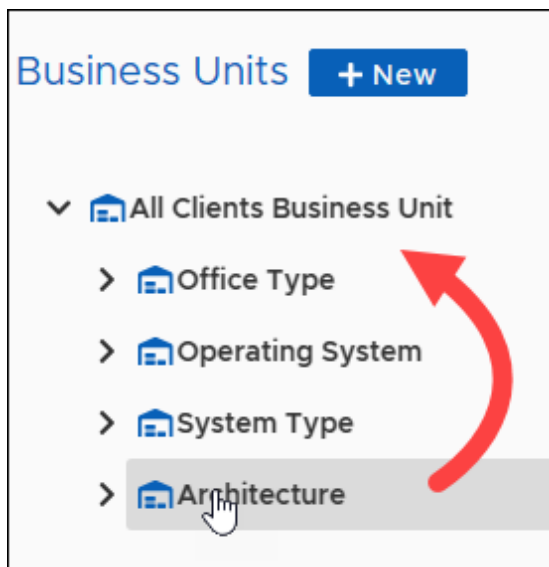
In the Business Unit hierarchy shown in the OneSite Patch dashboard, the Business Unit at the top of the list has the lowest priority. When changing the priority of a Business Unit in the hierarchy, consider the following items:

- **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?

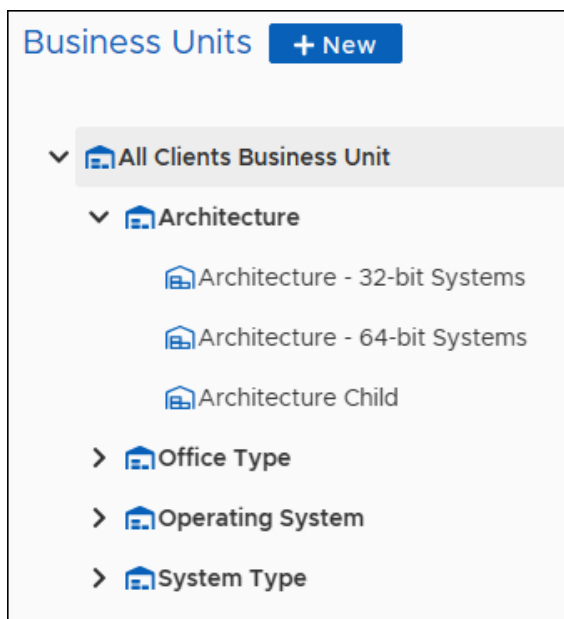
Further, is the new parent, or any ancestors, included in a Wave Entry that includes descendants? If yes, do you want the new BU included in those deployments?

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

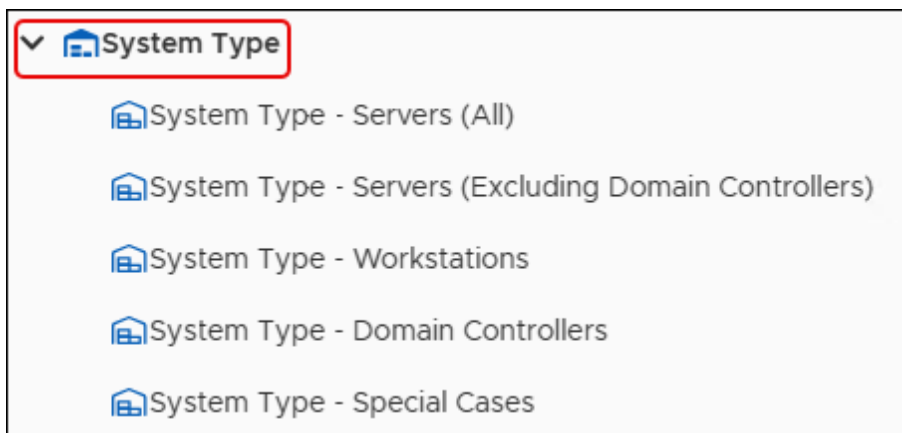
Units, including Child Business Units or Lab Business Units, provide another level of detail that administrators can use to further customize a patching environment.

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

Open and Save a Business Unit Template

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

1. Mouse over or click **Business Units** in the left pane [OneSite 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 Name of a template to open it.



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

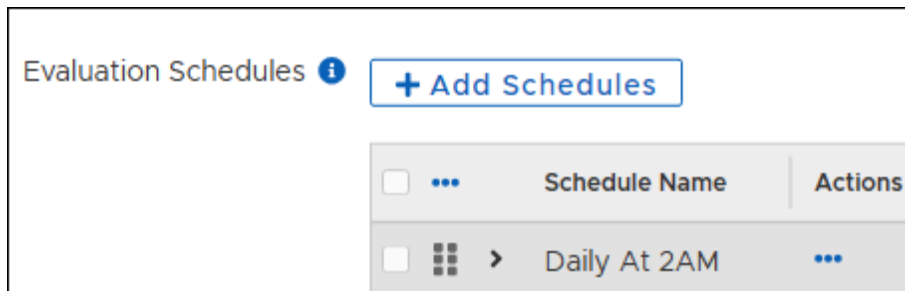
5. Select **Save**. When you have finished modifying your new template, you can drag and drop it into the folder you created (see [Organize New Patch Objects](#)).

Add Evaluation Schedules to a Business Unit

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

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

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



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

Add Schedules

Schedules
Show All
+ Create Schedule

Search Columns...

		Schedule Name	Start Date
<input type="checkbox"/>	⋮	[AutoUpgrade] Adaptiva Client Upgrade	5/2/24, 4:30 PM
<input type="checkbox"/>	⋮	ASAP	1/24/24, 12:44 PM
<input type="checkbox"/>	⋮	Balanced Daily at 6AM	1/24/24, 6:00 AM
<input type="checkbox"/>	⋮	Basic Inventory Schedule	1/24/24, 10:00 AM
<input type="checkbox"/>	⋮		

Rows Per Page: 10
1 - 10 of 13
1 / 2

Add Schedules
Cancel

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

Configure Business Unit Scopes

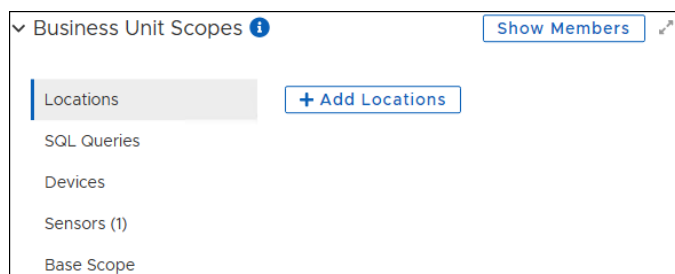
Business Unit Scopes define the rules used to find and include devices in a named Business Unit. OneSite Patch supports using one or more scopes to create a Business Unit.



TIP

If the scope type (Locations, and so on) has a number in parenthesis after the name, the template you copied included one or more of the identified scopes. Select the scope type to view the setting. You can either keep the included scope or click the **ellipsis (...)** after the scope name in the table to edit (if allowed) or delete it.

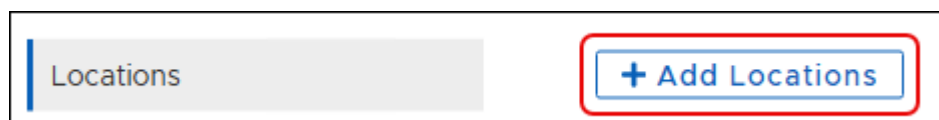
1. Scroll down to **Business Unit Scopes** in an open [Business Unit](#) template,
2. Select the Scope you want to use for this Business Unit.



Add Locations

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

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



2. Select one or more Location Names from the **Add Locations** table to assign them to the Business Unit. For information about managing available Location settings see the *Adaptiva OneSite Platform User Guide*.
3. Select **Add Locations** in the lower-left corner of the dialog. This returns you to the Business Unit template and populates a table with the selected Locations.

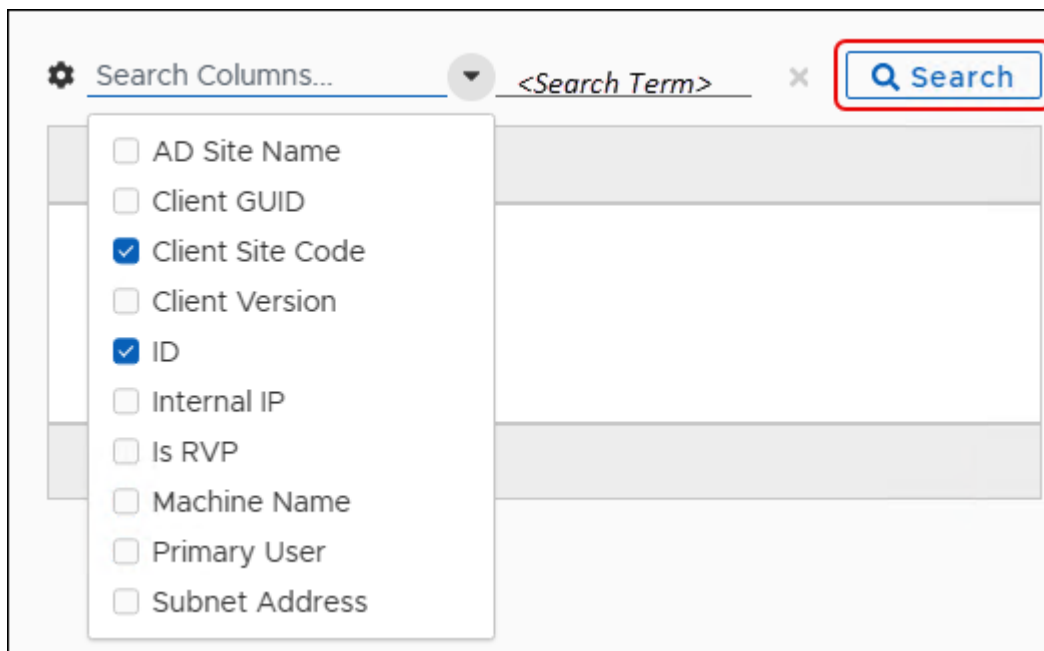
Add Devices

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

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



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



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

Add SQL Queries

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

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



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

×
Add Query

Name Example Query (do not use)

Description This is an example of a SQL query and not for reuse.

Type Client ID

Query

```
Select AdaptivaClientID from a_adaptivaclientdata
where machinename is ('machine1', 'machine2',
'machine3')
```

Add Query

Cancel



IMPORTANT

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

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

SQL Queries (1)
+ Add Query

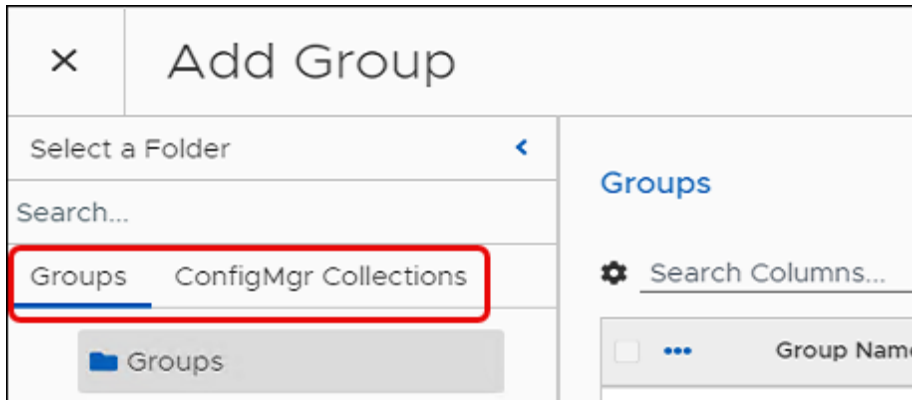
	Query Name	Type	Actions
<input type="checkbox"/>	Example Query	Client ID	⋮

⋮
Rows Per Page: 10
1 - 1 of 1
1 / 1

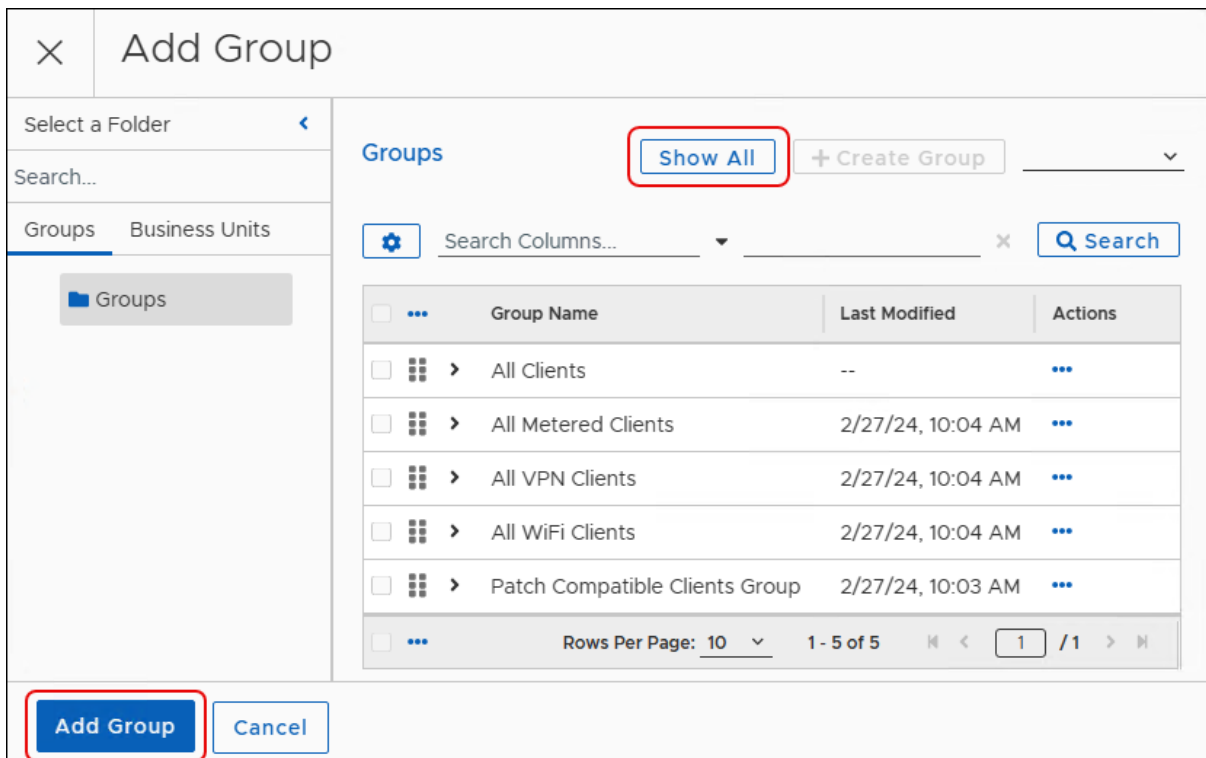
Set Base Scope

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

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



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



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

Add Sensors

Sensors mark device inventory using technology settings such as Java, PowerShell, WMI, and so on. OneSite Patch includes choices for common sensor settings, or you can create your own (see *Adaptiva OneSite Platform User Guide*).

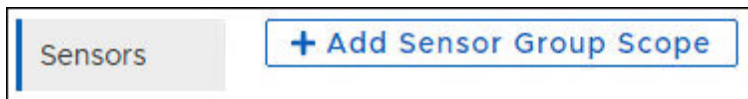


TIP

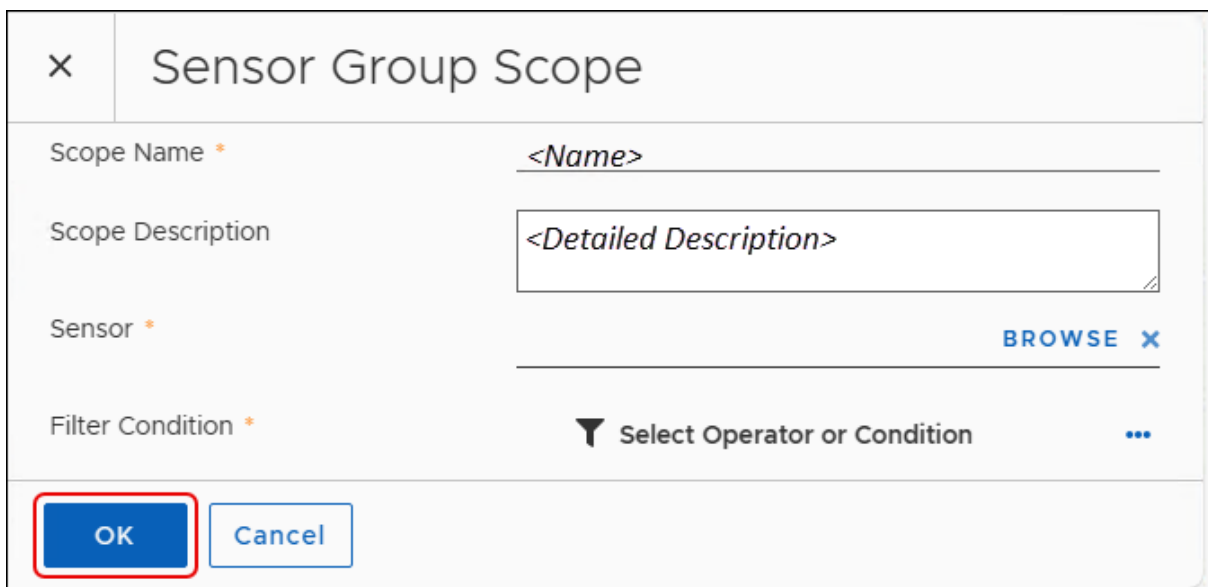
Selecting a Sensor from this location assumes you have already created the Sensor type you want to use, or that you intend to use one of the default sensors provided by Adaptiva.

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

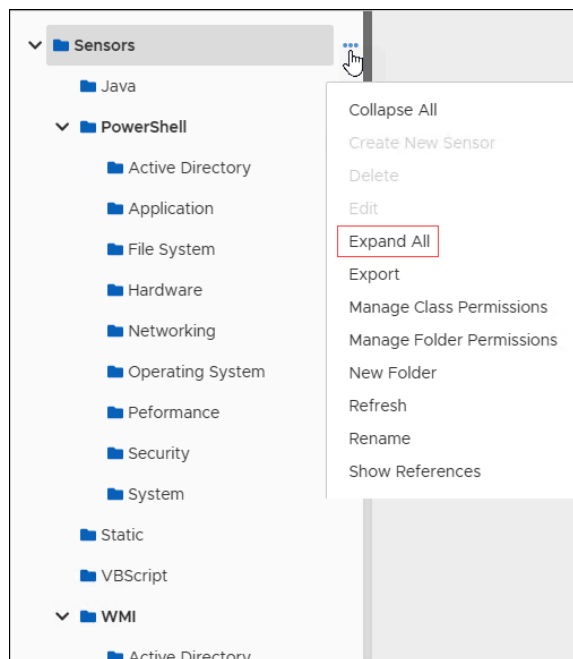
1. Select **Sensors** from **Business Unit Scopes**, and then click **+ Add Sensor Group Scope**.



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



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

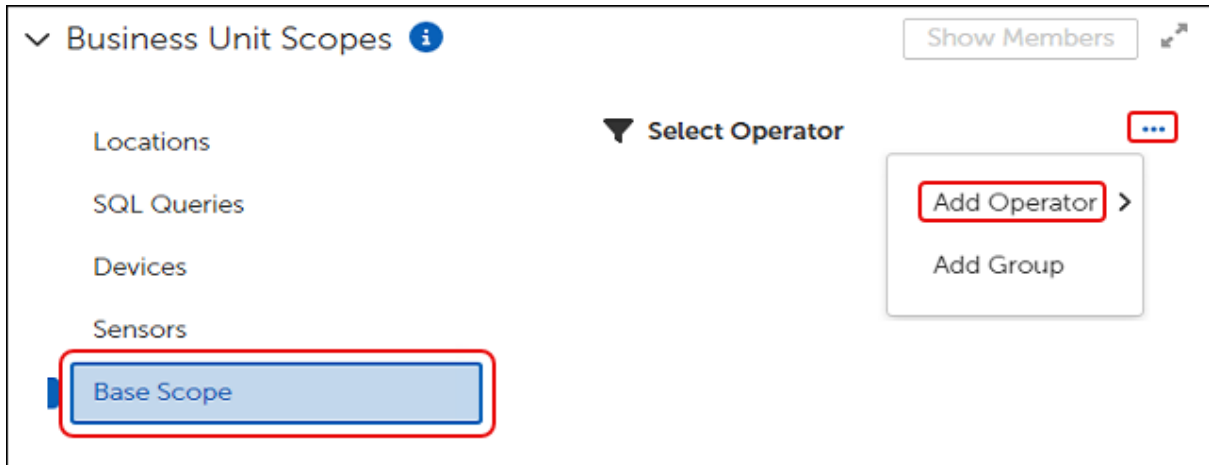


5. Select an item to use in your Sensor Group, and then click **Add Sensor**. This returns you to the **Sensor Group Scope** dialog.
6. Select **OK** to return to the Business Unit template or change [Base Scope](#) settings.

Add Multiple Groups or Business Units

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

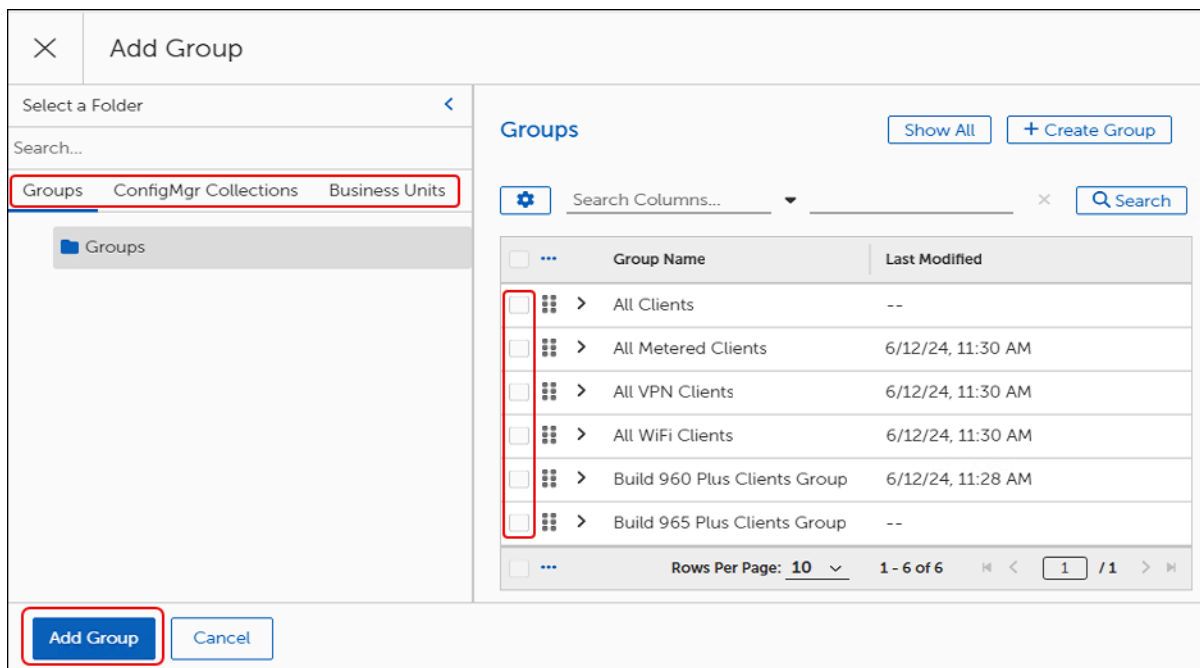
1. In the **Business Unit Scopes** section of an object template, click **Base Scope**.



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



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



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

Remove Groups or Operators

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

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

Verify Business Unit Members

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

Create a Lab Business Unit

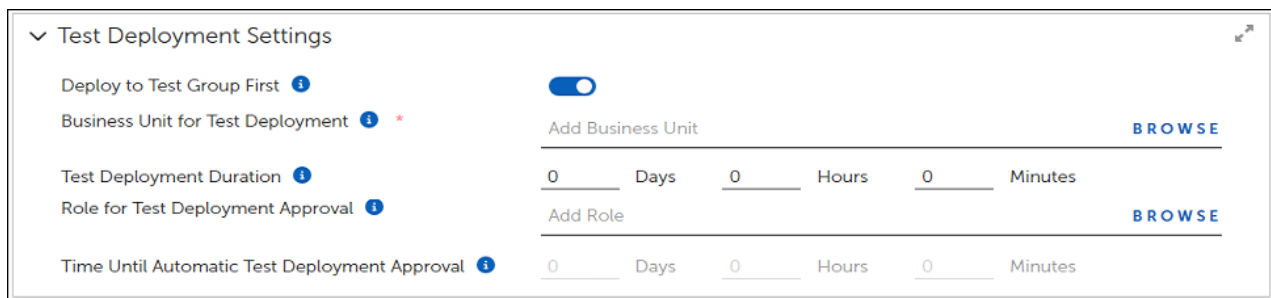
Designate Lab Business Units to use for testing purposes prior to production deployment.

- Make sure that the devices you want to use in the lab have the **AdaptivaClient** installed and are associated with an **AdaptivaServer**.

2. Follow the steps to [Create a Business Unit](#). When defining the Business Unit Scopes, use **Add Devices** to identify the devices in your lab or test environment and include them in the Lab Business Unit.
3. Define any other characteristics appropriate to your Lab Business Unit.

Test Deployment Settings for Auto Remediation

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



The screenshot shows the 'Test Deployment Settings' configuration panel. It includes a toggle for 'Deploy to Test Group First' which is turned on. Below it, there is a field for 'Business Unit for Test Deployment' with a 'BROWSE' button. The 'Test Deployment Duration' is set to 0 Days, 0 Hours, and 0 Minutes. There is a 'Role for Test Deployment Approval' field with a 'BROWSE' button. Finally, the 'Time Until Automatic Test Deployment Approval' is also set to 0 Days, 0 Hours, and 0 Minutes.

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

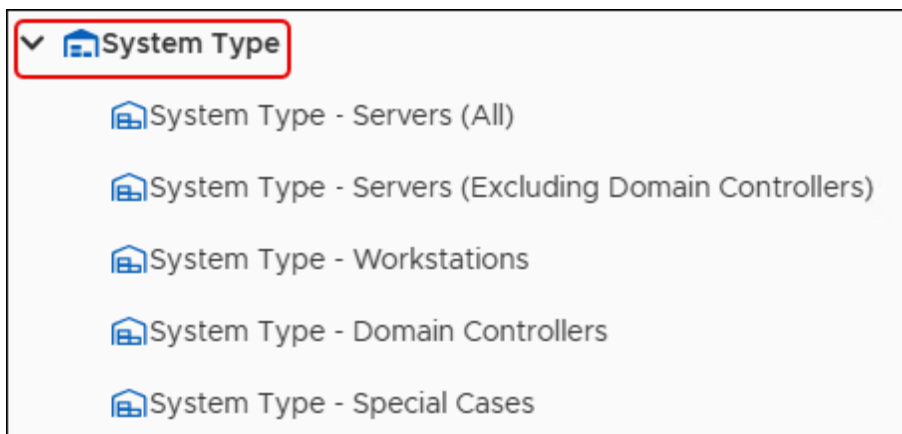
Create a Custom Lab Business Unit

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

Open and Save a Business Unit Template

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

1. Mouse over or click **Business Units** in the left pane [OneSite 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 Name of a template to open it.



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

Verify Business Unit Members

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

Create a Lab Business Unit

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

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

Test Deployment Settings for Auto Remediation

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

The screenshot shows the 'Test Deployment Settings' section of a configuration interface. It includes a toggle for 'Deploy to Test Group First' which is turned on. Below it is a 'Business Unit for Test Deployment' field with a 'BROWSE' button. The 'Test Deployment Duration' is set to 0 Days, 0 Hours, and 0 Minutes. There is also a 'Role for Test Deployment Approval' field with a 'BROWSE' button. At the bottom, 'Time Until Automatic Test Deployment Approval' is also set to 0 Days, 0 Hours, and 0 Minutes.

1. Select the **Deploy to Test Group First** toggle in the **Test Deployment Settings** workspace of Auto Remediation Settings. This enables automatic deployment of the Auto Remediation Settings to a test group.
2. Select **Browse** to select a **Business Unit** as the test destination.
3. Enter numbers for **Days**, **Hours**, and **Minutes** to set the **Test Deployment Duration**, which indicates how long production deployment waits after initiating test deployment to begin production deployment.

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

Create a Custom Lab Business Unit

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

Maintenance Windows

A Maintenance Window defines a period during which system maintenance occurs on a device. Business Unit configurations include Maintenance Window settings so administrators can schedule maintenance activities. 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 Adaptiva 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 [OneSite Patch Dashboard](#), and then click **Show All** to display the available Maintenance Window settings.



IMPORTANT

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

2. Select the **Name** of an existing template to open it, and then save the template with a new Name:
 - a. Select **More** in the upper-left corner of the template, and then select **Save <object> As**.
 - b. Enter a new Name for the template, and then click **OK** on the lower-left corner of the naming dialog. This returns you to the template with the new name.

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

Add Dynamic Detection Workflow (Optional)

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

1. Scroll down to **Dynamic Settings**, in an open Maintenance Window template.
2. Select **Browse** to the right of **Add Workflow**. This opens the **Add Workflow** dialog.
3. Select a workflow from the table, and then click **Add Workflow** in the lower-left corner.

Apply to All Urgencies

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

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

Set Maintenance Windows by Urgency

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

Create a Maintenance Window

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

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

Set the All Urgencies Override Duration

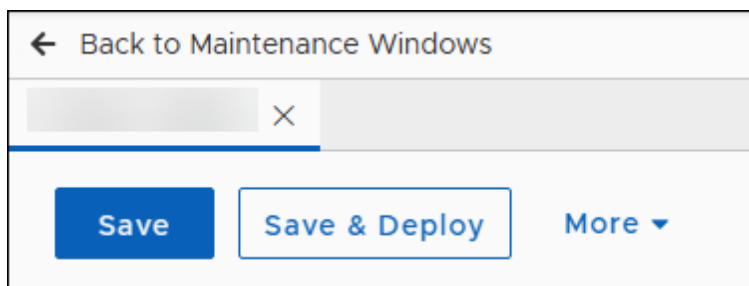
An override duration for the **All Urgencies Maintenance Window** sets the amount of time to wait for the Maintenance Window to open for all urgency level updates. After this time, the system overrides the Maintenance Window setting.

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

Save and Deploy the Maintenance Window

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

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



User Interaction Settings

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

Understanding User Interaction Settings

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

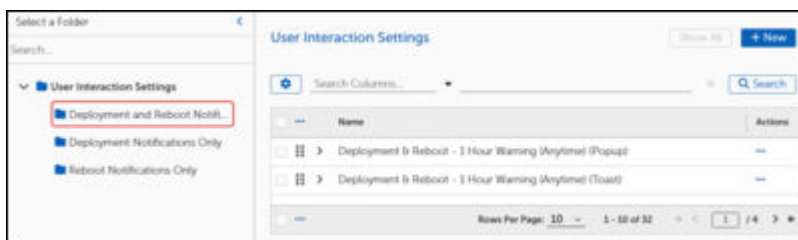
- Pre-install Notification
- Install Notification
- App Closure Notification
- Reboot Notification

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

Create User Interaction Settings

Open and Save a User Interaction Template

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

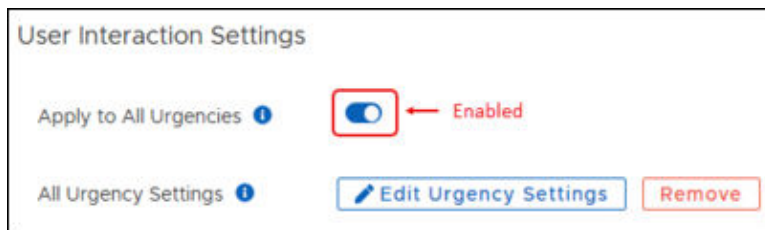


2. Select the Name of an existing template to open it. This example uses the Deployment & Reboot – 1 Hour Warning (Anytime)(Toast) template.

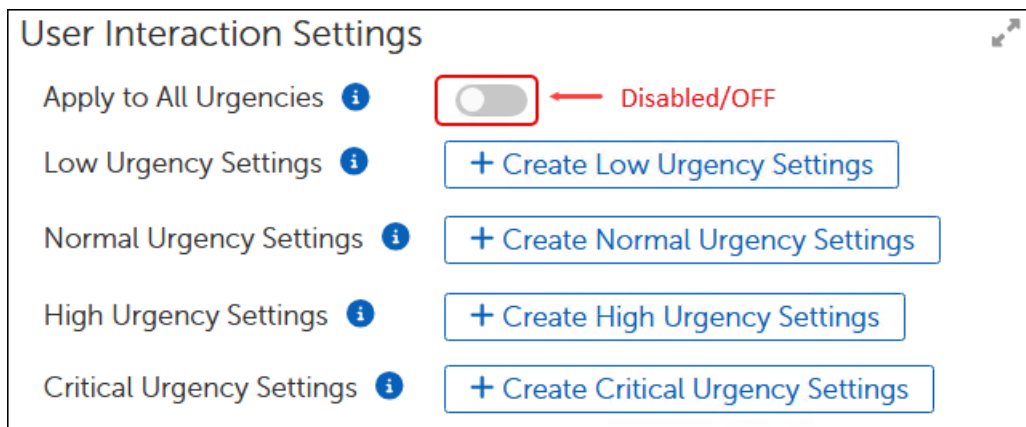
3. Save the template with a new Name:
 - a. Select **More** in the upper-left corner of the template, and then select **Save <object> As**.
 - b. Enter a new Name for the template, and then click **OK** on the lower-left corner of the naming dialog. This returns you to the template with the new name.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

Edit or Create Urgency Settings

1. Scroll down to **User Interaction Settings** in an open User Interaction Settings template:
 - 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 whether to set urgencies the same 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.
3. [Set deployment notification settings.](#)

Set Deployment Notification Settings

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



TIP

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

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

Deployment Notification Settings

Enabled

Mute Duration Days Hours Minutes Seconds

Notification Text

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

Create System Reboot Notification Settings

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

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

The screenshot shows the 'System Reboot Notification Settings' section. It includes a toggle for 'Notify User Before Reboot' which is turned on. Below this, there is a 'Notification Title' field containing the text 'Reboot Required'. The 'Notification Text' field contains the message: 'Software installation is complete but a reboot is necessary to apply the changes. Please save your work and restart your device.'

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

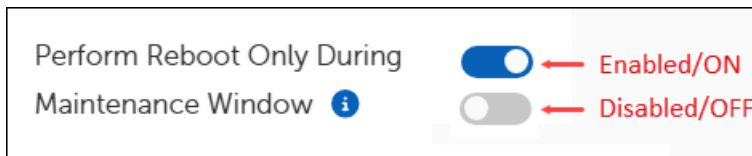
Configure Reboot Notification and Snooze Settings

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

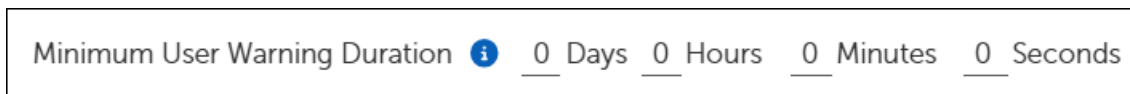
1. Select the **High Priority** toggled to enable or disable whether the user may dismiss notifications generated by the User Interaction Settings. Defaults to disabled in a new template:

The screenshot shows the 'High Priority' setting with an information icon. There are two toggle switches: the top one is blue and labeled 'Enabled/ON', and the bottom one is grey and labeled 'Disabled/OFF'.

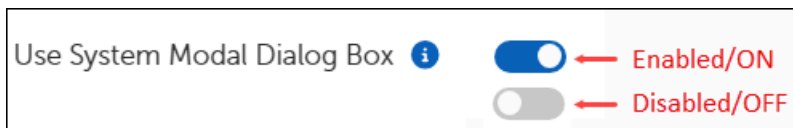
2. Select the **Perform Reboot Only During Maintenance Window** toggle to enable or disable whether reboots occur only during a maintenance window. Defaults to disabled in a new template:



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



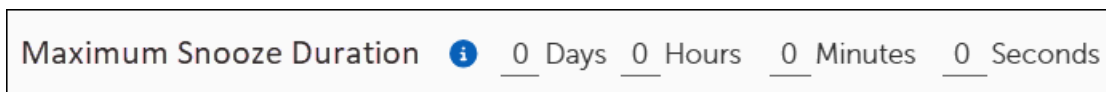
4. Select the **Use System Modal Dialog Box** to enable or disable whether the Dialog is a system modal. When enabled, the dialog appears in front of, and disables, the main window.



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



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



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

Save and Deploy User Interaction Settings

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

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

Customized Products

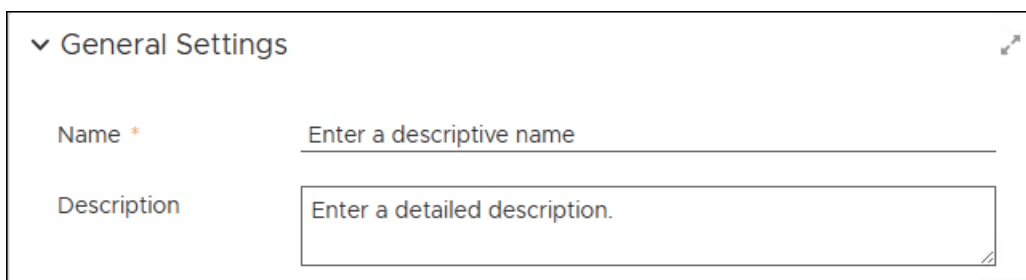
Software products and patches sometimes require user interaction when installing. Users enter details such as license information or request to show a menu at startup. Other default settings include auto update, or desktop shortcuts.

OneSite Patch 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 [OneSite Patch Dashboard](#).
2. Select **+ New** in the upper-right corner to open a new template:



The screenshot shows a form titled "General Settings" with a dropdown arrow on the left and a save icon on the right. It contains two input fields: "Name *" with a placeholder "Enter a descriptive name" and "Description" with a placeholder "Enter a detailed description." and a save icon in the bottom right corner.

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

Add a Deployment Wave to a Customized Product Template

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

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

General Settings

Name *

Description

Deployment Wave ⓘ * **BROWSE**

Target Product ⓘ * **BROWSE**

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

Add a Target Product

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

Software Products Show All

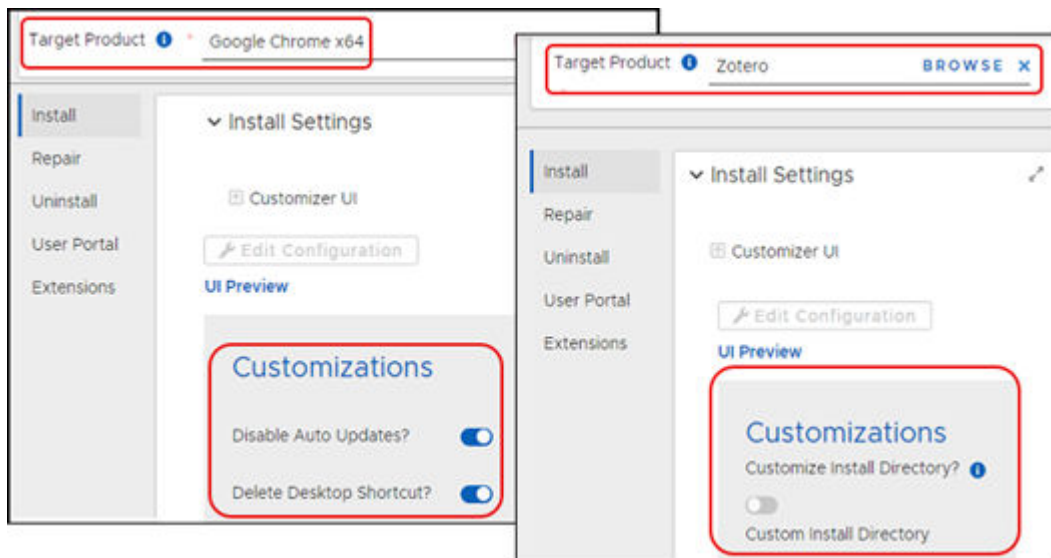
<input type="checkbox"/>	Name	Actions
<input checked="" type="checkbox"/>	Google Chrome x64	...
<input type="checkbox"/>	Google Chrome x86	...

3. Select the **Software Product** you want to customize. You can target only one Software Product in each Customized Product entry.
4. Select **Add Software Product** to populate the configurable items in the static list of **Install Settings**. Settings change depending on the Target Product.
5. Select **Save** in the upper-left corner of the template to save your changes.

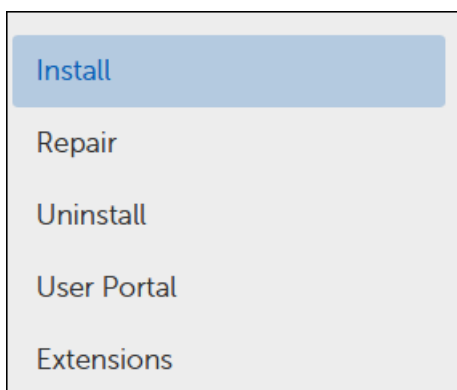
- Continue with [Configure Software Install Settings](#).

Configure Software Install Settings

- 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.



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



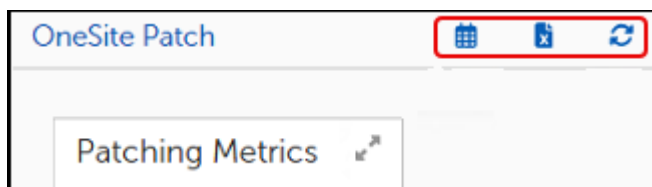
- Select **Save** at the upper left to save your progress:
 - Check the **Error View** and resolve any errors.
 - Select **Save** again if you make any changes.

4. Select <-- **Back to Customized Products** above the **General Settings** box. The changes you have made take effect the next time the associated Deployment Wave runs.

Navigating the OneSite Patch Dashboard


Date Settings, Export, and Refresh

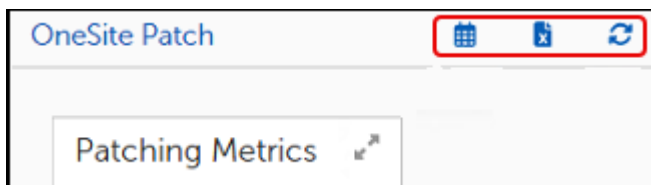
The three small icons (Calendar, Export and Refresh) on the upper right of the OneSite Patch Home page and on any of the Patching Analytics pages (Overview, Products, Patches, or Devices) provide options to customize the date settings to a particular date range, choose some or all widgets on the page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



Set Dates for Status Views

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

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



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

Dashboard Date Settings

Start Time

End Time

Window Type

- Day
- Week
- Month**
- Quarter
- Year

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

Export Widget Data

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

The screenshot shows the OneSite Patch dashboard with an 'Export Data' dialog box open. The dialog has a 'Select All' button checked, a 'Cancel' button, and an 'Export Selected' button. Several widgets on the dashboard have a white checkmark icon, indicating they are selected for export. These widgets include:

- Patching Metrics: 17 Patching Strategy Objects, 23 Products Discovered, 33 Products in Strategies (checked), 0 Patching Exceptions, 5 Devices, 5 Scans Run (Last 30 days), 5 Patches Installed (Last 30 days).
- Patching Metadata: Last Synced (5/21/24, 11:48 AM), Last Metadata Update (5/21/24, 6:53 AM) (checked), Supported Products (1614), Supported Patches & Releases (47059).
- Patching System Health: Overall Health: 90%, Metadata Feed Health: 98% (checked), Scanning Health: 100% (checked), Patch Installation Health: 73%.
- Patching Status: 449 Status on Machines (checked). Legend: Installed - 23 (5.12%), Outdated - 114 (25.39%), Applicable - 28 (6.24%), Scan Failure - 280 (62.36%), Installation in Progress - 1 (0.22%), Uninstallation in Progress - 0 (0%), Rollback in Progress - 0 (0%), Outdated but Excluded - 0 (0%).
- Patching Activity: 0 Running Patching Processes (checked), 0 Running Rollouts (checked), 0 Running Deployment Channels.

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 click multiple widgets to export.

The screenshot shows the OneSite Patch dashboard interface. At the top, there is a navigation bar with a calendar icon, a user profile icon, and a refresh icon. Below the navigation bar, there is an 'Export Data' section with a toggle switch for 'Select All', a 'Cancel' button, and an 'Export Selected' button. The main dashboard area is divided into several widgets:


- Export Data:** A list of widgets to be exported, including '33 Products in Strategies', '0 Patching Exceptions', '5 Devices', '5 Scans Run (Last 30 days)', and '5 Patches Installed (Last 30 days)'. Each item has a checkmark icon and a 'Click to remove widget from export' link.
- Supported Products:** A widget showing 'Supported Products: 1614' and 'Supported Patches & Releases: 47059'. It has a 'Click to add widget to export' link.
- Patching System Health:** A widget showing overall health metrics: 'Overall Health: 90%', 'Metadata Feed Health: 98%', 'Scanning Health: 100%', and 'Patch Installation Health: 73%'. Each metric has a progress bar and a checkmark icon. There is a 'Click to add widget to export' link.
- Patching Activity:** A widget showing '0 Running Patching Processes', '0 Running Rollouts', and '0 Running Deployment Channels'. It has a checkmark icon and a 'Click to add widget to export' link.
- Patching Status:** A donut chart showing the status of 449 machines. The data is as follows:

Status	Count	Percentage
Installed	23	5.12%
Outdated	114	25.39%
Applicable	28	6.24%
Scan Failure	280	62.36%
Installation in Progress	1	0.22%
Uninstallation in Progress	0	0%
Rollback in Progress	0	0%
Outdated but Excluded	0	0%

 The chart has a checkmark icon and a 'Click to remove widget from export' link.

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

Refresh the Status View

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

OneSite 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.

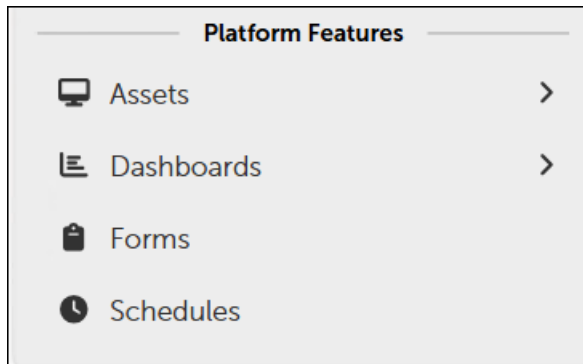
Integration Menu

The Integrations menu provides access for Adaptiva Partners to integrate client data into OneSite and create patching scenarios to update their partner hosts or or devices.




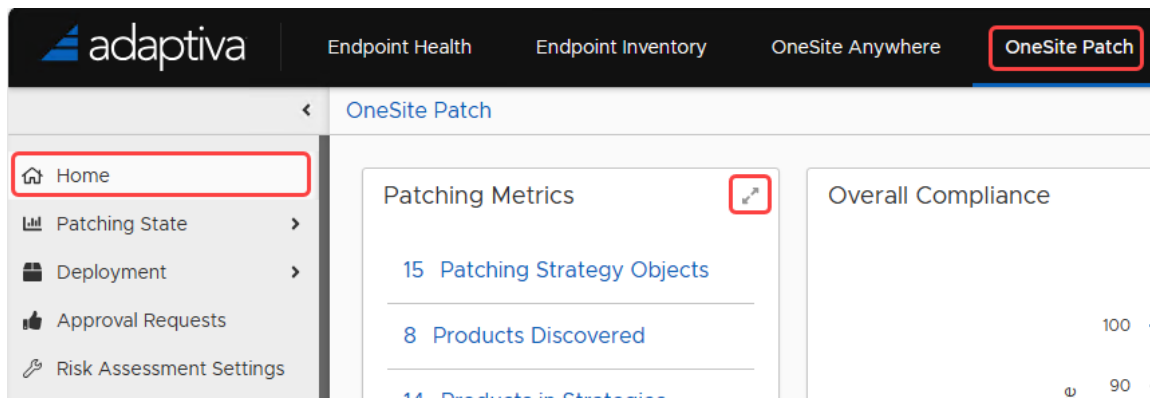
Platform Features Menu

These are common features available from every menu in OneSite Patch and across the full platform of OneSite products. For a description of the items in this menu, see the *Adaptiva OneSite Platform User Guide*.



OneSite Patch 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.

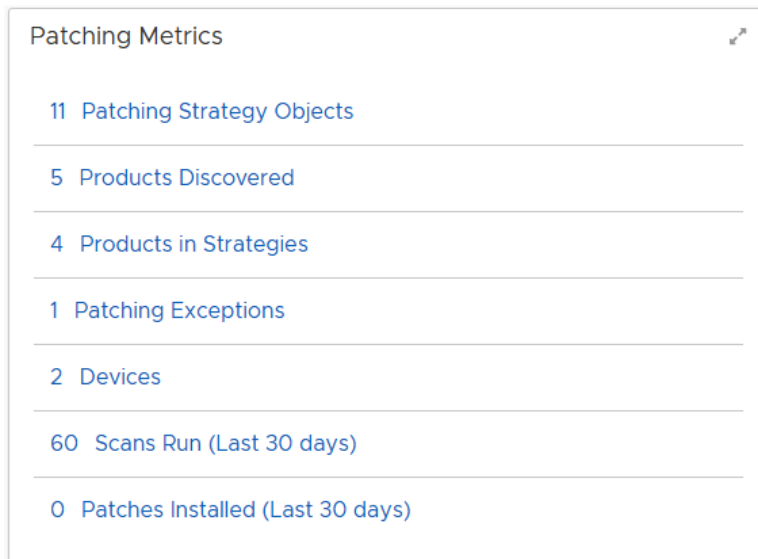


The layout of these widgets depends on the size of your computer monitor.

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.

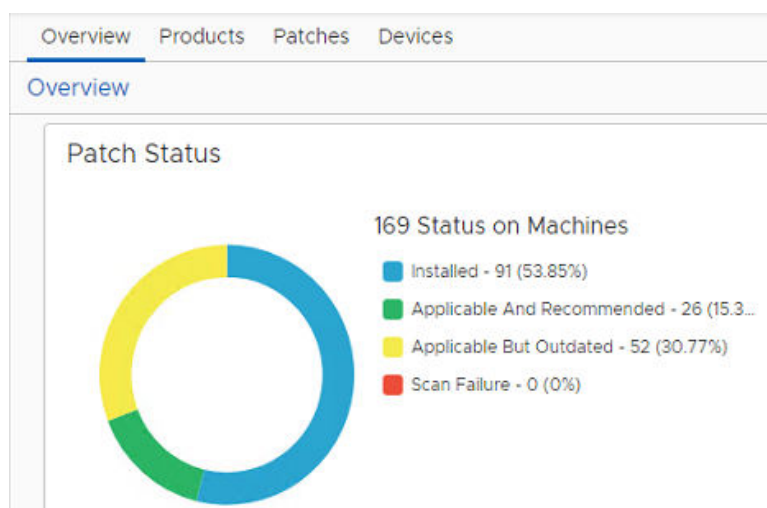
Patching Metrics

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**.



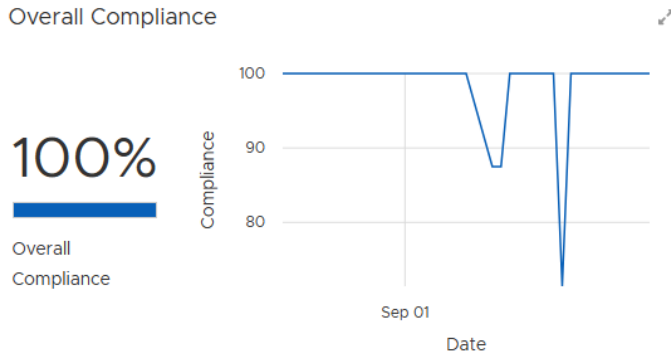
Patching Status

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



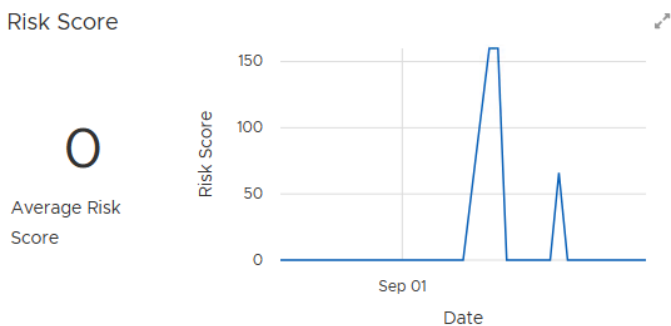
Overall Compliance

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



Risk Score

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



The average number reported here reflects a customized risk assessment for each product based on patch status, applicability, and weight of risk. See [Risk Assessment Settings](#) for more information.

Patching Metadata

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

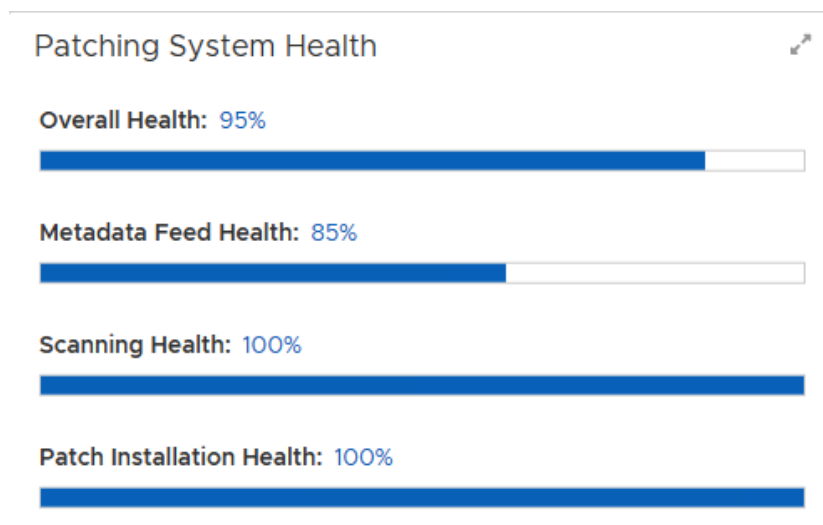
Patching Metadata

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

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

Patching System Health

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



Patching Activity

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

Patching Activity

0 Running Patching Processes


0 Running Rollouts

0 Running Deployment Channels

Top 5 Non-Compliant Products

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

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

Top 5 Non-Compliant Products 		
<input type="checkbox"/> ... Product Name	Compliance Status	Actions
<input type="checkbox"/> Microsoft Analysis Services OLE DB Provider ...	<input type="text" value="0%"/> 0%	...
<input type="checkbox"/> Microsoft Orca	<input type="text" value="0%"/> 0%	...
<input type="checkbox"/> Microsoft Visual C++ 2015-2022 Redistribut...	<input type="text" value="0%"/> 0%	...
<input type="checkbox"/> Microsoft Visual C++ 2015-2022 Redistribut...	<input type="text" value="0%"/> 0%	...
<input type="checkbox"/> SQL Server Management Studio x64	<input type="text" value="0%"/> 0%	...
<input type="checkbox"/> ...	Rows Per Page: <input type="text" value="5"/> 1 - 5 of 5	« < 1 / 1 > »

Top 5 Missing Patches

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



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

Appendices

Software Products Library

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

Metadata Catalog

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

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

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

After confirming a successful update, the team creates, reviews, and approves the metadata before adding it to the metadata catalog. Every Adaptiva customer server with an license downloads the metadata catalog update. 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 OneSite Patch Home menu in the left navigation panel, hover over **Patching Analytics**, and then select **Overview**, **Products**, **Patches**, or **Devices**.

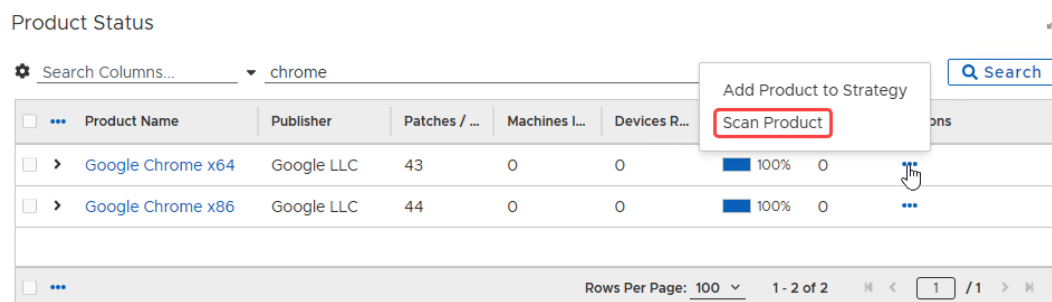
2. Scroll down to the last table on the screen. The table name changes depending on the option you choose:
 - **Overview – Product Status** table; Actions include Scan Product and Reset Deployment Failures for Product.
 - **Products – Product Status** table; Actions include Scan Product and Reset Deployment 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.

Product Status

Search Columns... chrome Search

<input type="checkbox"/>	Product Name	Publisher	Patches / ...	Machines I...	Devices R...				
<input type="checkbox"/>	Google Chrome x64	Google LLC	43	0	0	100%	0	...	
<input type="checkbox"/>	Google Chrome x86	Google LLC	44	0	0	100%	0	...	

Rows Per Page: 100 1 - 2 of 2 1 / 1

A screenshot of a web application interface titled "Product Status". It features a table with columns for Product Name, Publisher, Patches, Machines, and Devices. Two rows are visible, both for "Google Chrome" (x64 and x86). A context menu is open over the first row, with the "Scan Product" option highlighted in red. The menu also includes "Add Product to Strategy".

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.

The screenshot shows a 'Request Scan' dialog box with the following elements:

- Scan All Clients**: A toggle switch that is currently turned on (indicated by a blue circle).
- Target Groups**: A button labeled '+ Add Groups'.
- Target Business Units**: A button labeled '+ Add Business Units'.
- Target Clients**: A button labeled '+ Select Clients'.
- Scan All Software**: A toggle switch that is currently turned off (indicated by a grey circle).
- Software**: A section with a button labeled '+ Add Software' and a table below it.

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

At the bottom of the dialog, there are two buttons: **OK** (highlighted with a red box) and **Cancel**.

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`.