



OneSite Patch Express

with Microsoft Defender

Table of Contents

Adaptiva Copyright	1
Legal Notice	1
Revision History	1
Getting Started with OneSite Patch	1
Supported Operating Systems, Software, Drivers, and BIOS	3
Supported Browsers	4
Logs for Server	4
Customer Support	5
Adaptiva OneSite Admin Portal	5
Log in to the Admin Portal	5
Licensing Products	6
Add a License Key	6
Target Collections for the Licensed Product	6
Dashboard	7
Access the Dashboard	7
Setup Wizard	7
Welcome to Patch Express	7
Detection Integrations	8
Integrate a Partner Product	8
Use Copy From	9
Select a Remediation Schedule	11
Enable Vulnerability Detection	12
Enable Patch Pre-staging	12
Configure Deployment Notifications	12
Configure Deployment Approval	13
Configure Test Deployment	16
Configure Test Approval	17
Complete	19
Best Practices for Patch Express	19
Integrate Defender	20
Create a Microsoft Entra Application	20
Add Permissions to an Entra Application	21
Create a Shared Secret ID	22
Locate and Record the Microsoft Entra IDs	23
Integrate Defender with OneSite Patch	24
Security	25
Access Security Settings	25
View Administrators	25
View Roles	25
Menu Objects for OneSite Patch	26
Patching Analytics Dashboards	26
Using Search in OneSite Patch	26
Patching Analytics Overview	26
Products View	27
Patches View	29
Devices View	32
Flex Controls	34
Blocklisting	34
Blocklist Settings	34
Managing Blocklist Notification Settings	35
Cycle Operations	36

Patching Cycles	37
Deployment Cycles	38
Rollout Cycles	40
Patching Exceptions	40
Using Patching Exceptions	41
Create a Patching Exception	41
Set Override Details for Patch Exceptions	41
Set Last Allowed Patch Versions	42
Add Target Business Units for Patch Exceptions	43
Global Pause	44
Stop All Patching Activity Immediately	45
Resume All Paused Patching Activity Immediately	46
Pause Patching for Specific Objects	46
Pause Deployment of a Specific Software Product	47
Pause Deployment of a Specific Patch	49
Pause Specific Cycles	51
Pause Deployment to a Business Unit	58
Rollbacks Overview	59
Rollback	59
Rollback to Version	71
Approval Requests	83
Approve or Reject a Patch Request	83
Auto Remediation	84
Access Auto Remediation and Deployment Settings	84
Using Auto Remediation Settings	85
Enable Auto Remediation	86
Vulnerability Detection Source Settings	87
Production Deployment Settings for Auto Remediation	87
Test Deployment Settings for Auto Remediation	87
Verify that Auto Remediation Works as Expected	88
Patching Preferences	88
Using Patching Preferences	88
Access Patching Preferences	88
Create a New Patching Preference	89
Add a Target Business Unit	90
Select a Server Maintenance Window	90
Select Server User Interaction Settings	91
Business Units	92
Understanding Business Units	92
Parent and Child Business Units	92
Managing Inheritance Settings	94
Enable Inheritance	94
Disable Inheritance	94
Organizing the Business Unit Hierarchy	95
Best Practices when Changing Priorities	95
Change the Order of the Hierarchy	95
Creating a Business Unit	96
Open and Save a Business Unit Template	97
Add Evaluation Schedules to a Business Unit	98
Configure Business Unit Scopes	98
Add User Interaction Settings	104
Add Approval Chains to a Business Unit	105
Customer Extension Data	107
Add a Notification Chain	107

Content Prestaging Settings in Object Templates	108
Verify Business Unit Members	108
Create a Lab Business Unit	108
Create a Custom Lab Business Unit	108
Maintenance Windows	108
Open and Save a Maintenance Window Template	109
Dynamic Settings	109
Add Dynamic Detection Workflow (Optional)	109
Maintenance Windows by Urgency	109
Apply a Maintenance Window to All Urgencies	110
Save and Deploy the Maintenance Window	110
User Interaction Settings	111
Open and Save a User Interaction Template	111
Choose Urgency Settings	111
Configure Deployment Notification Settings	112
Reboot Notification Settings	113
Configure Reboot Settings	113
Managing Snooze Settings	114
Configure Snooze Settings	115
Save and Deploy User Interaction Settings	116
Customized Products	116
Manage Settings for Customized Products	116
Open and Save a Customized Product Template	116
Add a Deployment Wave to a Customized Product Template	117
Add a Target Product	117
Configure Software Install Settings	117
Navigating the OneSite Patch Dashboard	118
Date Settings, Export, and Refresh	118
Set Dates for Status Views	119
Export Widget Data	119
Refresh the Status View	120
Patch Menus	120
Home Menu	121
Patch Express Home Menu	121
Integration Menu	122
Intent Schema Menu	122
Platform Features Menu	123
Dashboard and Performance Widgets	123
Patching Metrics	124
Patching Status	124
Overall Compliance	125
Risk Score	125
Patching Metadata	126
Patching System Health	126
Patching Activity	126
Top 5 Non-Compliant Products	127
Top 5 Missing Patches	127
Appendices	128
Software Products	128
Metadata Catalog	128
Endpoint Scans	128
Request a Scan	128

Adaptiva Copyright

Copyright © 2023-2025 Adaptive Protocols, Inc. - All Rights Reserved

Legal Notice

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
April 2, 2025	9.2.967.xx	v2	<ul style="list-style-type: none">• Cross-platform support for macOS third-party patching and Linux repository based patching.• Unified cross-platform visibility in Patch for customers with macOS, Linux, and Windows devices.• Allow users to specify a maintenance window for deployments and another for reboots when creating Business Units.• Allow users to suppress reboots using User Interaction Settings.• Updated content to improve usability and revised for clarity
March 3, 2025	9.1.965.58	v1.2	Added support for Mozilla Firefox and instructions for successful log in using Firefox. Other text edits to enhance clarity and fix minor, non-technical issues.
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 Patch

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

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

Supported Operating Systems, Software, Drivers, and BIOS

- **Windows**

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

- **Linux**

Automated OS package updates, libraries, and applications from official repositories for key Linux distributions (updates within the same distribution release within those repositories).

- CentOS Stream 9
- CentOS Stream 10
- Debian 11
- Debian 12
- RHEL 8
- RHEL 9
- Ubuntu 18.04 LTS
- Ubuntu 20.04 LTS
- Ubuntu 22.04 LTS
- Ubuntu 24.04 LTS



TIP

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

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

Some limitations apply. See [Customer Facing FAQ Cross Platform 2025](#) for details.

- **Mac**

Third-party patching only. Support for devices running the following macOS versions:

- macOS 13 (Ventura)
- macOS 14 (Sonoma)
- macOS 15 (Sequoia)



NOTE

MacOS Patching is not supported at this time.

Supported Browsers

Adaptiva OneSite supports the following browsers:


- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Safari



IMPORTANT

Do not use Microsoft Internet Explorer.


Logs for Server

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

<path>\Adaptiva\Adaptiva Server\Logs



NOTE

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

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

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

Customer Support

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

Adaptiva OneSite Admin Portal

OneSite Patch uses the Admin Portal for configuration and management.

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

Log in to the Admin Portal

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



TIP

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

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

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

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

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

3. Log in using one of the following methods:

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



TIP

If you are using Mozilla Firefox, see Resolve the [Mozilla Firefox Active Directory Login Issue](#) KB article.

After successfully logging in, the Home page appears.

Licensing Products

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

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

Add a License Key

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

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

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

Target Collections for the Licensed Product

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

1. Select the OneSite Patch product name in the **Product Licensing** list.
2. Select **+ Browse** under **Target Collections**.

This opens the **Select Group** dialog.

3. Select one or more Groups from the **All Groups** table.
4. Select **OK** on the lower-left corner to return to the **Product Licensing** workspace.

Dashboard

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

Access the Dashboard

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

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

Setup Wizard

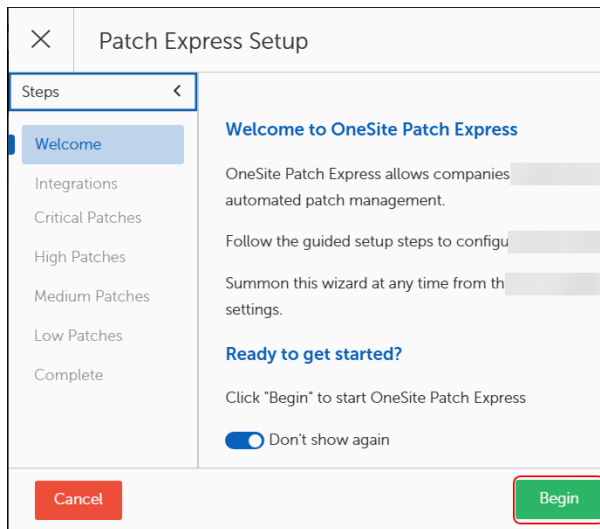
The setup wizard provides step-by-step guidance for your first introduction to . The wizard walks you through automatic deployment of patch remediation for each patch vulnerability level (Critical, High, Medium, and Low).

Welcome	Use the guided setup to configure to meet the needs of your organization. See Welcome to Patch Express .
Integrations	
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 Detection Integrations .
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 .

Welcome to Patch Express

You may choose to walk through the guided process 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](#).



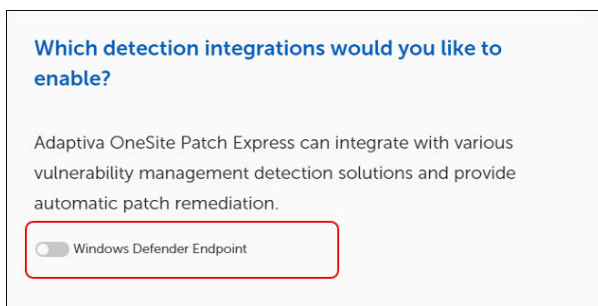
Detection Integrations

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

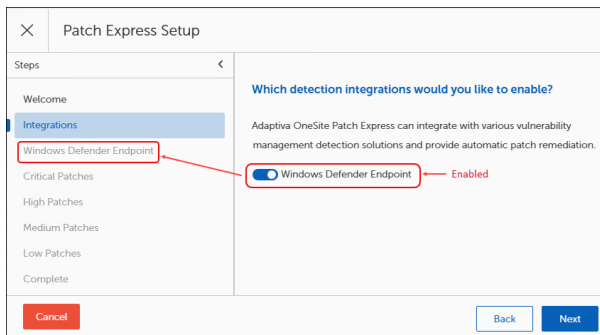
To integrate a partner product, you must have a valid license for the partner product. This is in addition to the base license for . Without a valid license installed, the integration pane has no options for integration. If you do not have a license for your partner product, contact .

Integrate a Partner Product

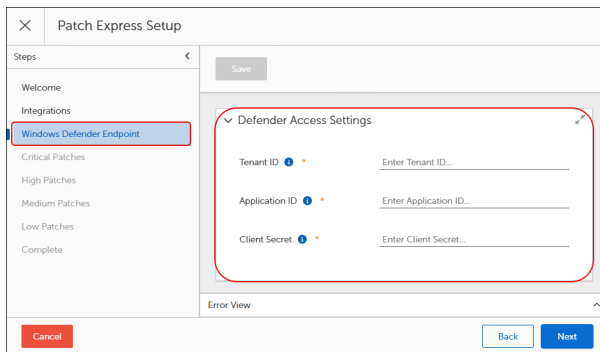
1. Select **Begin** on the **Welcome** screen of the Patch Express Setup Wizard. This opens the Integrations pane.
 - If you have licensed a partner product in Patch Express, you will see it listed here. Continue to the next step.
 - If you do not use a partner product, skip to [Enablement](#).



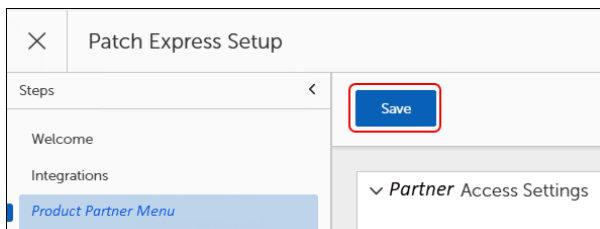
2. Select the **[Partner Product]** toggle to enable or disable (default) integration of your partner product.
With the product enabled, the Steps of the left navigation menu include a new item related to product integration.



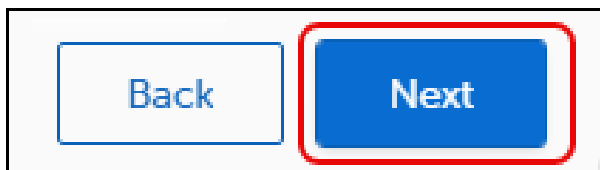
3. Select **Next** to enter the partner product integration details. If you do not have these details, see [Integrate Defender](#) to create or find them.



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

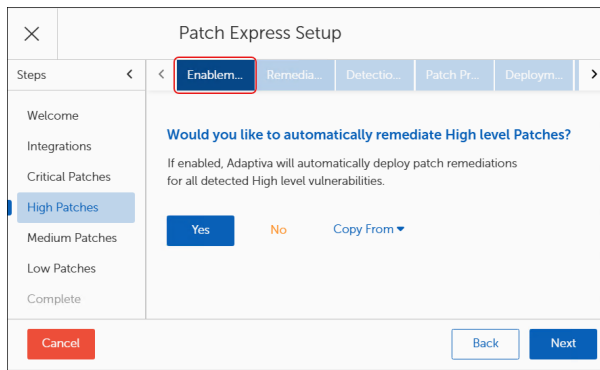


5. Select **Next** on the bottom right corner of the **Patch Express Setup Wizard** to enable auto remediation.

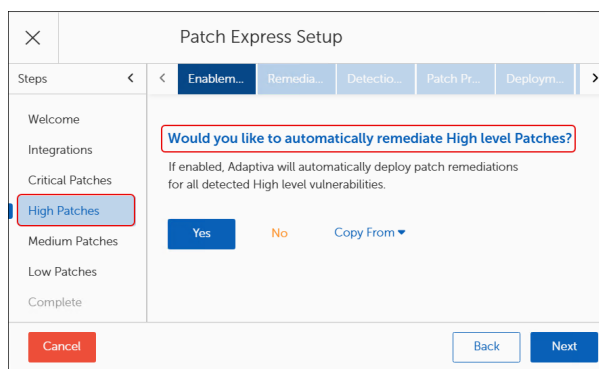


Use Copy From

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:



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



- 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

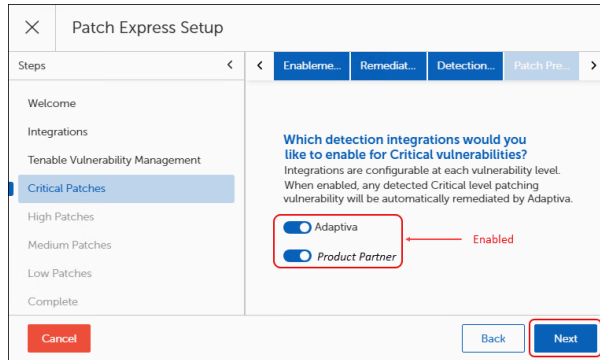
Selecting No to cycle through each patch severity level in the wizard without configuring them enables each selection in the Steps menu for easier navigation between levels.

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.

Enable Vulnerability Detection

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

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



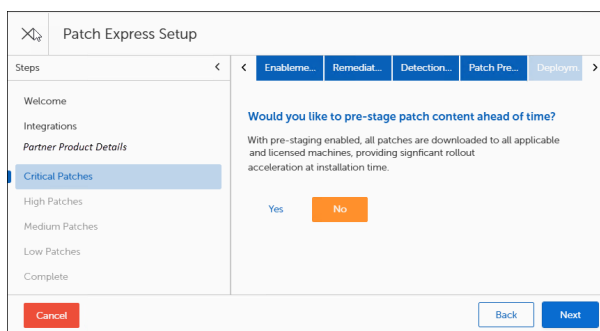
2. Select **Next** to [prestage patch content](#).

Enable Patch Pre-staging

When you pre-stage patches, 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](#).

The screenshot shows the 'Patch Express Setup' dialog box. The 'Steps' bar at the top indicates the current step is 'Enabl...'. The main content area asks the question 'Do you want to notify a group of employees about deployment?' with 'Yes' and 'No' buttons. A left sidebar lists navigation options: Welcome, Integrations, Critical Patches (selected), High Patches, Medium Patches, Low Patches, and Complete. At the bottom are 'Cancel', 'Back', and 'Next' buttons.

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

The screenshot shows the 'Patch Express Setup' dialog box at Step 2. The question is 'Do you want to seek approval before deploying Critical level?' with 'Yes' and 'No' buttons. Below the question, there 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 request patches to be deployed, then the approval request will not be sent.' At the bottom, there is an 'Add Role' text field with a 'BROWSE' button next to it. The left sidebar and bottom buttons are the same as in the previous screenshot.

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

The screenshot shows the 'Add Role' dialog box. On the left, there is a tree view under 'Roles' with 'Metadata Roles' and 'Patch Roles' as sub-items. The main area is a table titled 'Roles' with a search bar and a 'Show All' button. The table lists three roles: 'All Admin Role', 'Read-Only Admins Role', and 'Super Admin Role'. The 'All Admin Role' is highlighted with a red box. At the bottom left are 'Add Role' and 'Cancel' buttons.

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](#).

Patch Express Setup

Steps: < < Enabl... Remen... Detec... Patch ... Deplo... Appro... > >

Welcome

Integrations

Critical Patches

High Patches

Medium Patches

Low Patches

Complete

Do you want to seek approval before deploying Critical level

Yes No

Cancel Back Next

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

Patch Express Setup

Steps: < < Enabl... Remen... Detec... Patch ... Deplo... Appro... > >

Welcome

Integrations

Critical Patches

High Patches

Medium Patches

Low Patches

Complete

Do you want to seek approval before deploying Critical level

Yes No

If specified, an Adaptive production patch approval request will be sent to belong to the specified role. Any of the Administrators can approve the request. If no role is specified, the approval request will not be sent.

Add Role BROWSE

Cancel Back Next

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

Add Role

Select a Folder

Search...

Roles

Metadata Roles

Patch Roles

Search Columns...

Show All

Search

Name

All Admin Role

Read-Only Admins Role

Super Admin Role

Rows Per Page: 10 1-3 of 3

Add Role Cancel

- 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

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

< Enab... 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.

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

< Enab... 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**

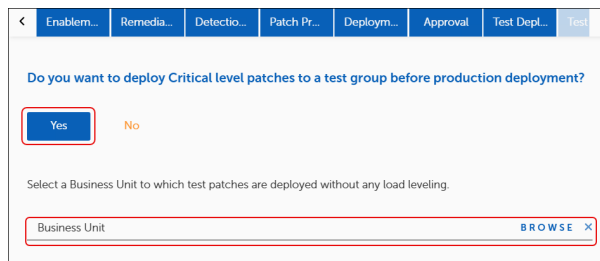
- Select **Yes** to enable load leveling for the specified level patch deployments. When enabled, load leveling for the production patch installation occurs across all target devices.
- Set the number of **Days**, **Hours**, or **Minutes** for load leveling to occur prior to initiating production patch 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).



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.



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:

- 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.

Do you want to seek approval before deploying Critical level patches to test devices?

Yes No

BROWSE 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.

Add Role

Select a Folder

Search...

Roles

- Metadata Roles
- Patch Roles

Roles

Show All

Search Columns...

Search

Name

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

1 / 1

Add Role Cancel

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

Approval Timeout

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

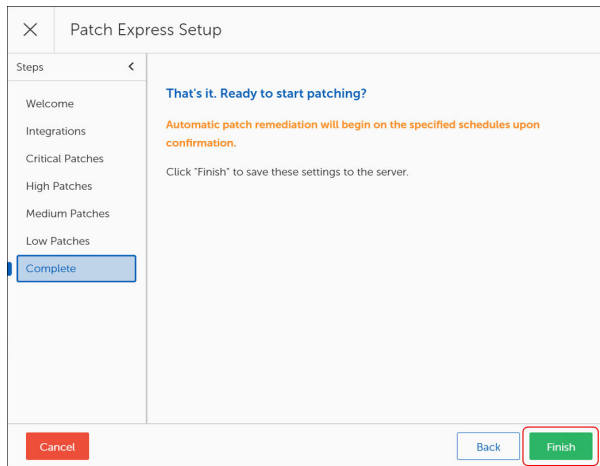
0 Days 0 Hours 0 Minutes

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

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 wizard.



Best Practices for Patch Express

After licensing , you can enable Auto Remediation, set a schedule, and begin using immediately. Auto Remediation targets every licensed Client. The 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.

recommends customizing a few administrative items before you begin.

- Create Administrators and assign roles using the 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

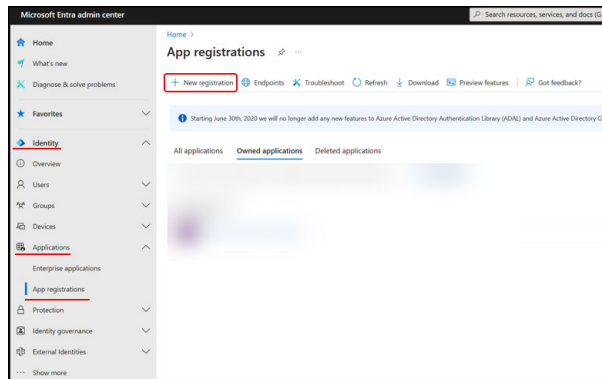
Integrating Microsoft Defender requires the following Microsoft Entra ID information:

- **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 OneSite Patch, 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:

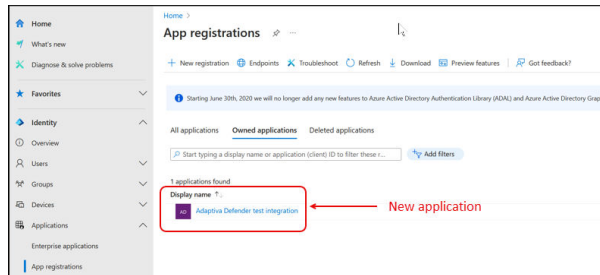
A screenshot of the 'Register an application' form within the Microsoft Entra admin center. The form is titled 'Register an application'. The 'Name' field, which is for the user-facing display name, is highlighted with a red box. Below this, the 'Supported account types' section is visible, where the option 'Accounts in this organization's directory only (Adaptive Authentication only - Single tenant)' is selected and highlighted with a red box. Other options include 'Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)' and 'Personal Microsoft accounts only'. The 'Redirect (optional)' section is also visible. At the bottom of the form, there is a checkbox for 'By proceeding, you agree to the Microsoft Platform Policies' and a 'Register' button, both of which are highlighted with red boxes.

- a. Enter a **Name** that identifies the Adaptive integration.
 - b. Select **Accounts in this organization's 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.](#)

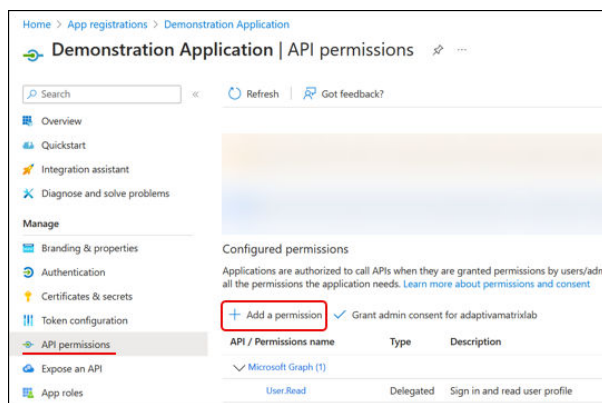
Add Permissions to an Entra Application

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.

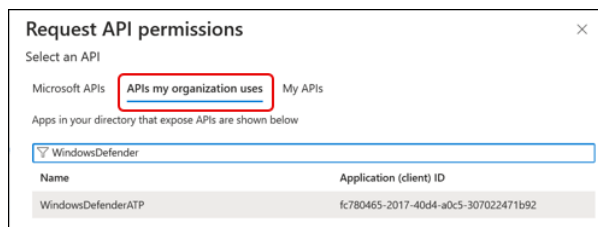
1. Access the **API Permissions** workspace from the **App registrations** page:



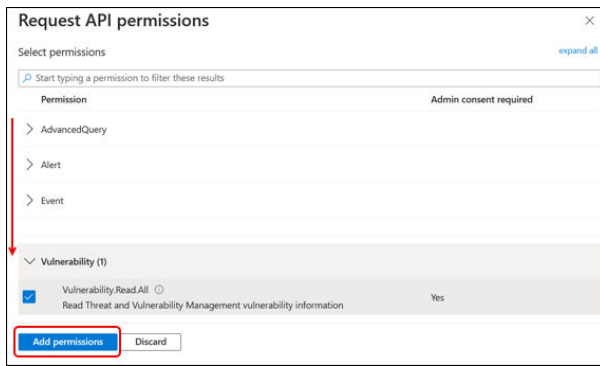
- a. Select the **Name** of the newly created application on the **App registrations** page. This opens the application and a new list of menu options.
- b. Select **API permissions** on the left navigation menu, and then select **Add a Permission**.



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**.

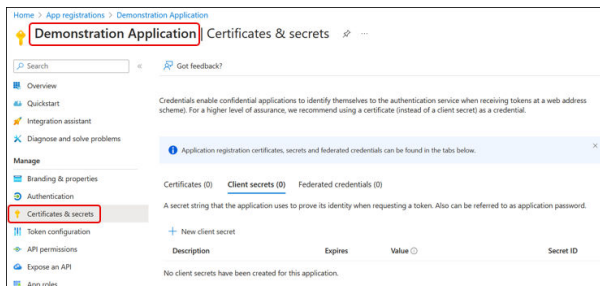


4. Scroll down to and expand **Vulnerability**, and then select **Vulnerability Read All**.
5. Select **Add Permissions**. If prompted, follow the required steps to provide administrator consent to make the change.
6. [Create a Client Secret ID](#) for the application.

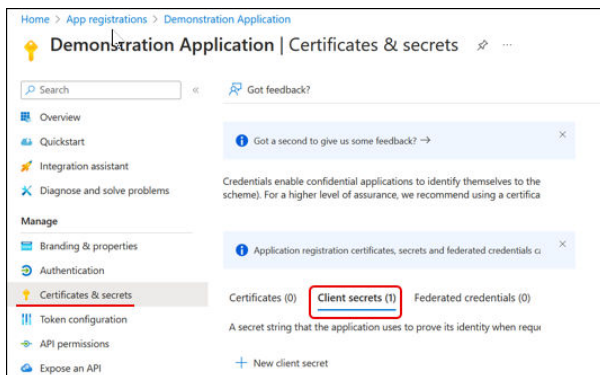
Create a Shared Secret ID

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 Defender for the application you created.

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

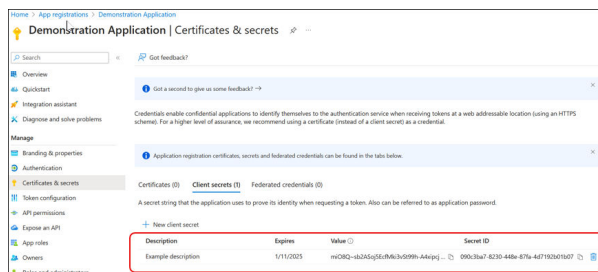


2. Select **Client secrets**.



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

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



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

!

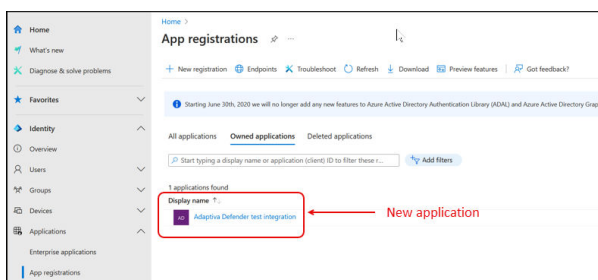
IMPORTANT

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.

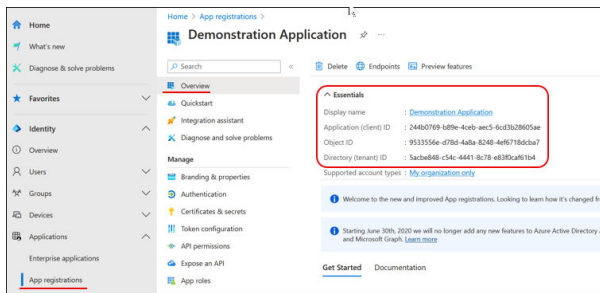
5. Gather the [integration details](#) you have created.

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 Adaptive 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.


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

Security

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

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

Access Security Settings

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

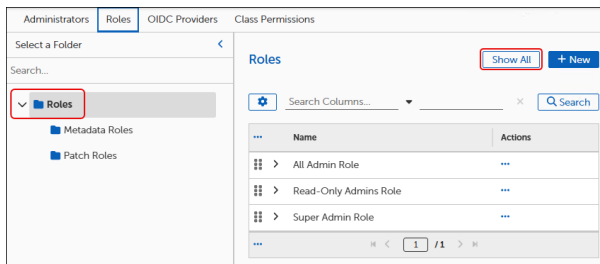
View Administrators

- Select the **Roles** tab of [Security Settings](#).

Name	Last Modification Time	Actions
abc@123.com		
abc@123.com		
abc@123.com		
abc@123.com	5/29/25, 7:37 AM	
abc@123.com	5/5/25, 7:46 AM	
abc@123.com	2/24/25, 11:02 AM	

View Roles

- Select the **Roles** tab of [Access Security Settings](#) to view the list of roles.



Menu Objects for OneSite Patch

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

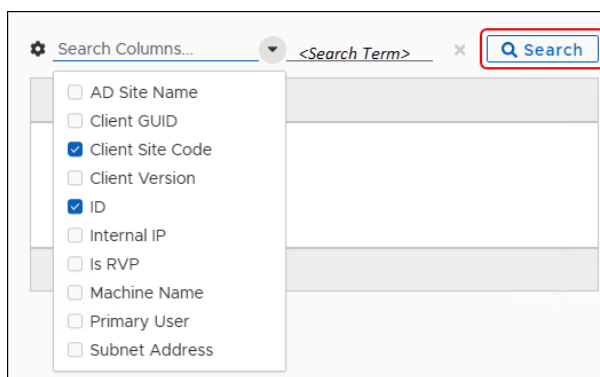
Patching Analytics Dashboards

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

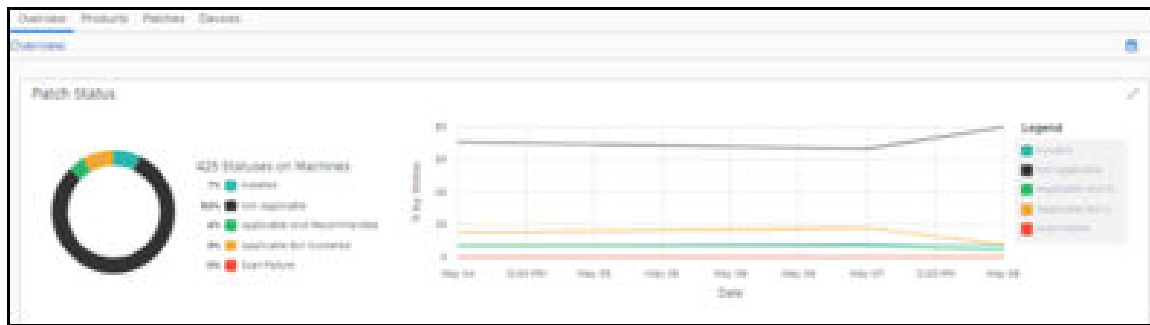
For tables in any dashboard view, the drop-down list next to **Search** allows you choose a column to search within. This provides several options for searching depending on the search term you have selected. Column choices change depending on the menu object.



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	Patch...	Mach...	Devic...	Comp...	Risk ...	Actions
TPassword x64	TPassword ...	Ablebits Inc.	38	0	0	100%	0	...

ID: 1000000270

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

Percentage Installed On: 0%

Strategies Including this Product: 0

Average Risk Score: 0

Risk Contribution: 0

Criticality: 50

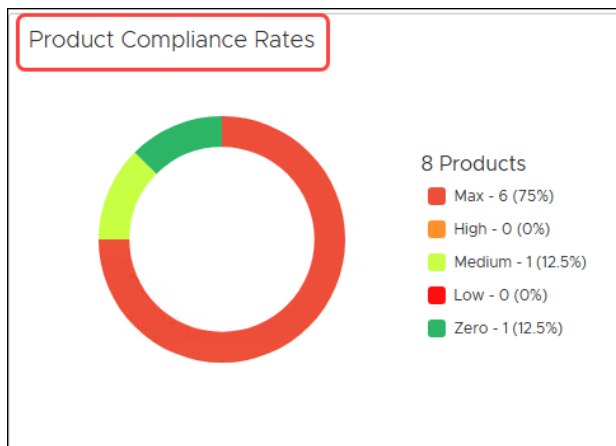
Products View

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

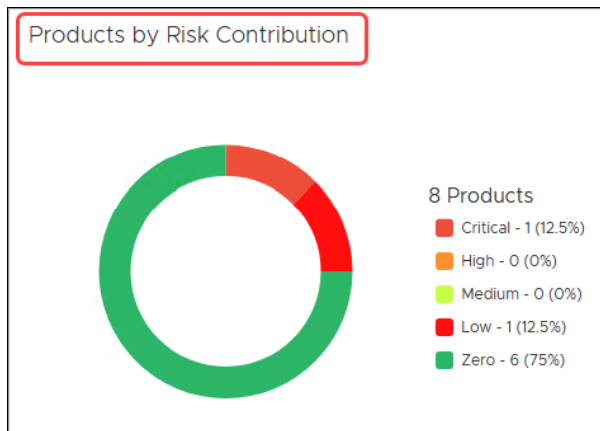
Product Metrics tracks supported products, detected products, and patching requirements, and provides a visual indication of product patching over time.



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



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



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



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

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

Product Status

Search Columns...

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

ID: 1000000270

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

Percentage Installed On: 0%

Strategies Including this Product: 0

Average Risk Score: 0

Risk Contribution: 0

Criticality: 50

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.



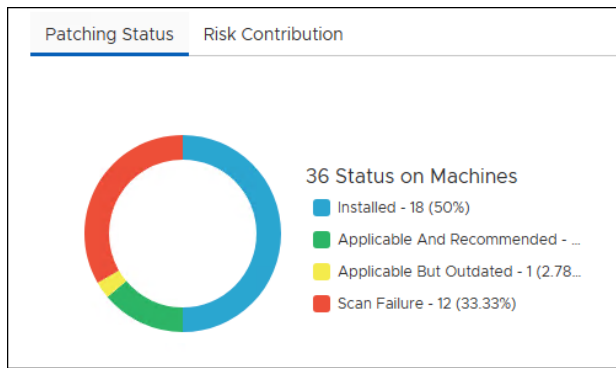
Active Product Deployments provides the number of patches undergoing installation and the percentage of completion.



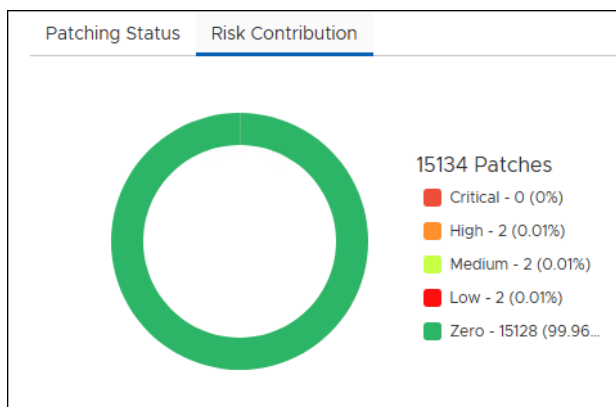
Patch Trends includes two tabs, one for **Patching Status** and one for **Risk Contribution**.



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.

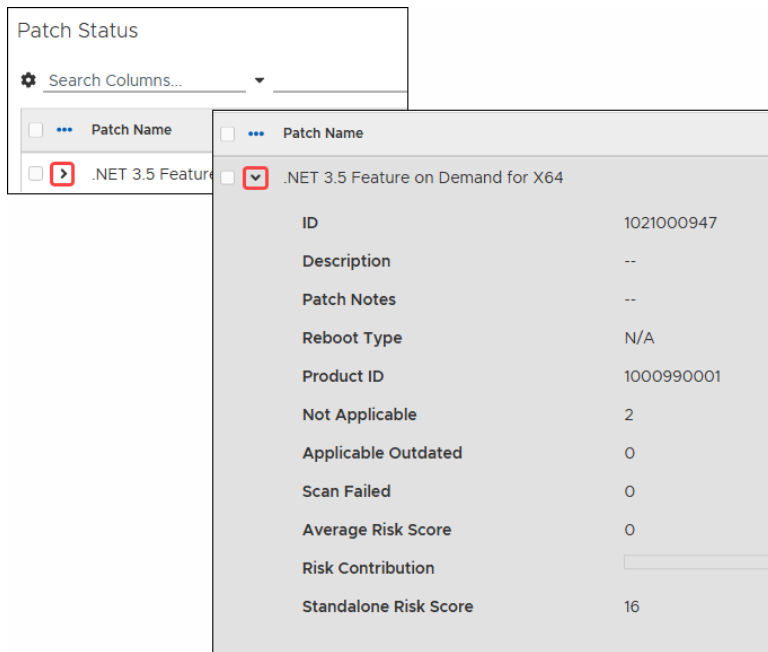


Top 10 Most Critical Patches tracks the risk contribution of the top ten most critical patches in the environment.

Top 10 Most Critical Patches			
	Patch Name ↑	Risk Contribution	Actions
<input type="checkbox"/>	2023-11 Cumulative Upd:	<div><div></div></div> 15%	...

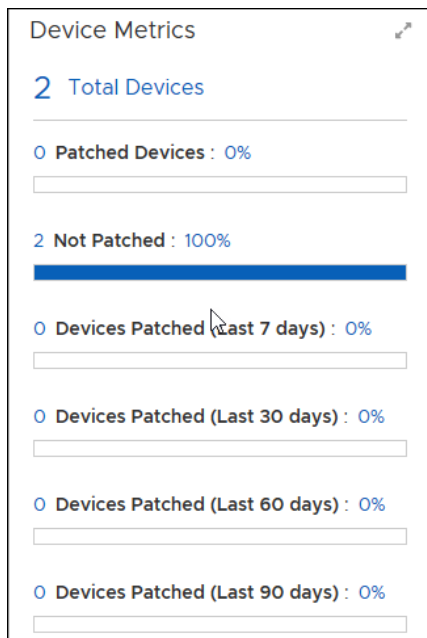
Patch Status is a table that lists each patch that OneSite Patch looks for during a scan, the installation/applicability status of each, and the status, compliance, and Risk Score for each.

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

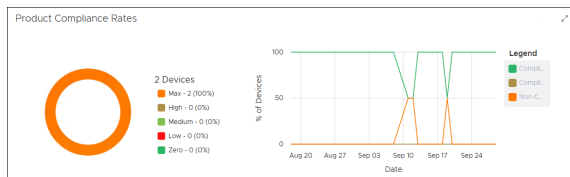


Devices View

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.



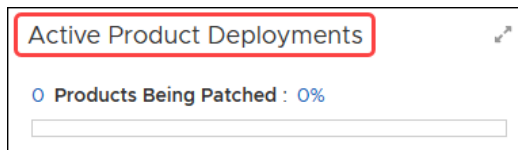
The **Product Compliance Rates** for Devices shows the rate of compliance for each device in the environment based on the latest device scan information. The graph displays the percentage of devices that fall into each category of compliance (max, high, medium, low, and zero), and the line graph shows 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					
<div> <div> <div></div> <div>Search Columns...</div> </div> </div>					
Device Name	Device Name	Compliance	Risk Score	Risk Contribu...	Proc
<div> <div></div> <div>adaptivaserver</div> </div>	<div> <div></div> <div>adaptivaserver</div> </div>	<div> <div></div> <div>67%</div> </div>	153	<div> <div></div> <div>60%</div> </div>	6
<div> <div>Device ID</div> <div>2</div> </div>					
<div> <div>Primary User</div> <div>ADAPTIVASERVER\Administrator</div> </div>					
<div> <div>IP Address</div> <div></div> </div>					
<div> <div>Client Version</div> <div>9.0.963.2</div> </div>					
<div> <div>Last Check In</div> <div>11/29/23, 6:11 PM</div> </div>					
<div> <div>Operating System</div> <div>Microsoft Windows Server 2022 Standard</div> </div>					
<div> <div>Location</div> <div>No Office</div> </div>					
<div> <div>Compliant Products</div> <div>4</div> </div>					
<div> <div>Non-Compliant Products</div> <div>2</div> </div>					
<div> <div>Applicable Patches / Releases</div> <div>4</div> </div>					

Flex Controls

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

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

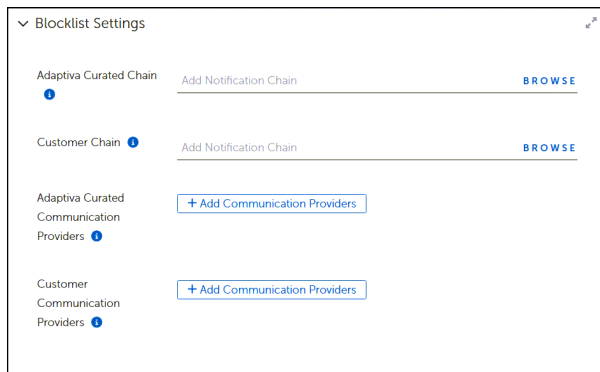
Blocklisting

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

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

Blocklist Settings

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



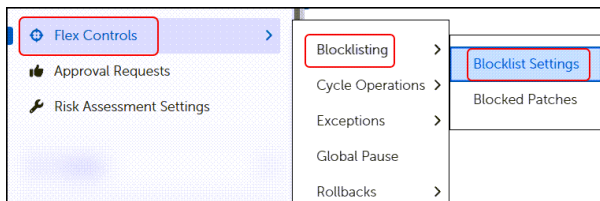
Managing Blocklist Notification Settings

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

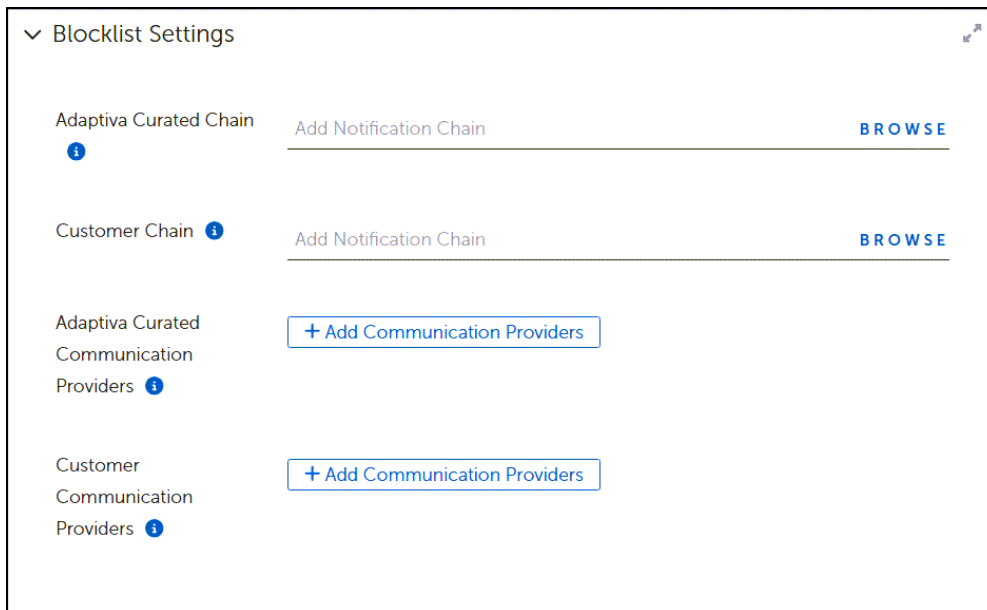
View Blocklist Settings

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

1. Mouse over or select **Flex Controls** on the Home menu, and then select **Blocklisting > Blocklisted Patches**.



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



Select a Notification Chain for Blocklisted Patches

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

Choose Communication Providers for Notification Chains

1. Navigate to [Blocklist Settings](#).
2. Select **+ Add Communication Providers** for either or **Customer Communication Providers** from the **Blocklist Settings**.
3. Select one or more **Names** from the **Communications Provider** table, and then select **Add Communication Providers** at the bottom left of the dialog.
If you need to add providers to the table, see [Create a New Communication Provider](#).

Cycle Operations

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

Details available for each cycle type include the following:

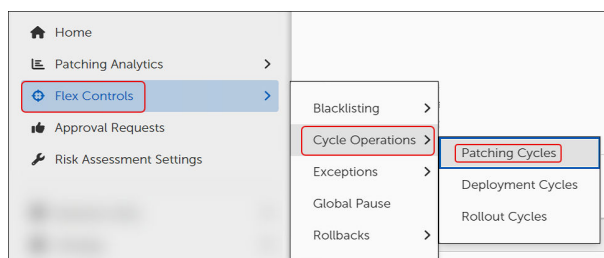
- **Cycle Information:** Provides general information about the Patch Process, such as the Current State, the creation date and time, and the Patch Process schedule. This section also contains controls to manually start, stop, or delay a Patch Process.
- **Overall Metrics:** This section contains information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

Patching Cycles

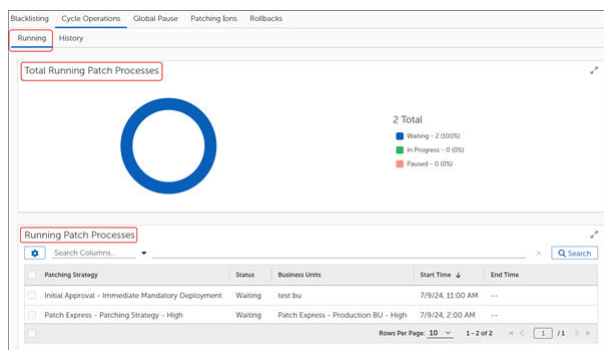
This dashboard shows information about the active Patch Processes in the environment. Patch Processes represent the workflow that models and performs the defined patching routine. As part of the overall Patching Strategy, Patch Deployment Bots use configured criteria to identify patches that apply to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

View the Running Patch Cycles

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

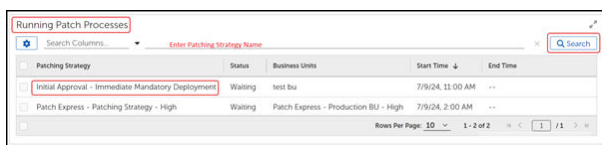


This opens to the **Running** tab of the **Patching Cycles** workspace:



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

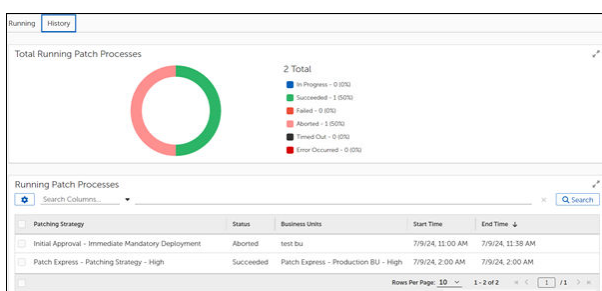
2. Enter a **Patching Strategy** name in the search bar above the **Running Patch Processes** table, and then select **Search**.



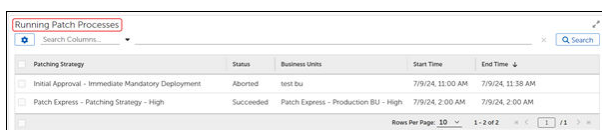
3. Select the **Patching Strategy** name in the **Running Patch Processes** table to see specific details about that process.

View Patching Cycle History

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



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



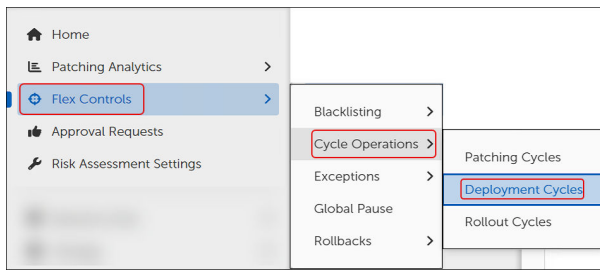
4. Select the **Patching Strategy** name in the **Running Patch Processes** table to see specific details about that process.

Deployment Cycles

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

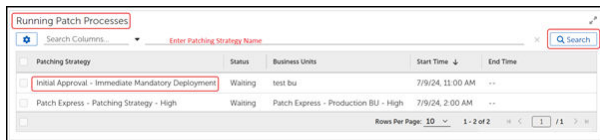
View the Running Deployment Cycles

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



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

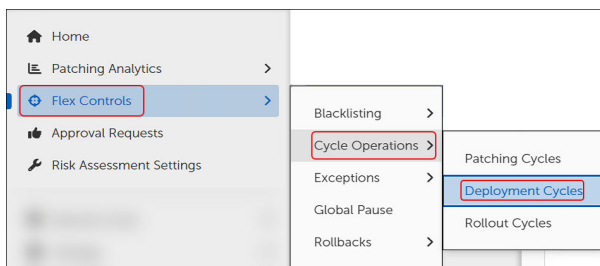
- The **Total Running Deployments** widget shows an aggregate summary of all patch processes and their corresponding states (Waiting, In Progress, or Paused).
 - The **Running Deployments** widget table lists the running Deployment Strategies by name.
2. Enter a **Deployment Strategy** name in the search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



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

View Deployment Cycle History

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



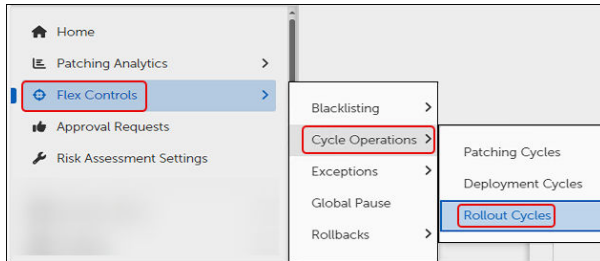
2. Select **History** on the upper left to change to the **History** tab:
 - The **Total Running Deployments** widget displays deployment processes and their corresponding states (Waiting, In Progress, or Paused).
 - The **Running Deployments** widget table lists the completed Deployment Strategies by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

Rollout Cycles

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

View the Running Rollout Cycles

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



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

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

View Rollout Cycle History

1. Mouse over or select **Flex Controls** on the **Home** menu, and then select **Cycle Operations > Rollout Cycles**.
2. Select **History** on the upper left to change to the **History** tab:
 - The **Total Running Deployments** widget displays an aggregate summary of all deployment processes and their corresponding states (Waiting, In Progress, or Paused).
 - The **Running Deployments** widget table lists the completed Deployment Strategies by name.
3. Enter a **Rollout Cycle** name in the search bar above the **Running Rollout Cycles** table, and then select **Search**.
4. Select the **Rollout Cycle** name in the **Finished Cycles** table to see specific details about that process.

Patching Exceptions

When Business Units require exemption from specific updates on certain products, or the entire enterprise must remain at a specific version of a product, Patching Exceptions provide a mechanism for creating and implementing the rules. Patching Exceptions provides version-level patch support, allowing administrators to exert granular control over patch deployment. For example, use Patching Exceptions to target and completely remove a product from an environment when the product is no longer required.

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

Using Patching Exceptions

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

Desired State Override Options

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

Last Allowed Version

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

Create a Patching Exception

1. Select **Flex Controls** from the **Home** menu, and then select **Exceptions > Patches**.
2. Select **+New** on the upper-right to open a Patching Exception template.
3. Name and describe the exception:
 - a. Enter a descriptive Name for this exception in the **Name** field.
 - b. Enter a detailed **Description** of the purpose for this exception.
4. Select **Save** on the upper-left to save your new template:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.
5. Choose an Override Strategy:
 - If you choose **Override Desired States**, see [Set Override Details for Patch Exception](#).
 - If you choose **Select Last Allowed Versions**, see [Set Last Allowed Patch Versions](#).

Set Override Details for Patch Exceptions



IMPORTANT

Choose only one software version per override exception.

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

Override Strategy

☒ Override Desired States
☐ Select Last Allowed Versions

Desired State Overrides ⓘ

Mandatory Install (0) -

+ Browse

Do Not Install (0) +

Rollback (0) +

Uninstall (0) +

Target Business Units ⓘ +

+ Browse

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

Search Columns... chrome

Product Name	Publisher	Operating System
Google Chrome Beta x86	Google LLC	Windows
Google Chrome Beta x64	Google LLC	Windows
Google Chrome x86	Google LLC	Windows
Google Chrome x64	Google LLC	Windows

OK Cancel

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

Set Last Allowed Patch Versions

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

Override Strategy

☐ Override Desired States
☒ Select Last Allowed Versions

Desired State Overrides ⓘ

Last Allowed Version Patches ⓘ

+ Browse

Target Business Units ⓘ *

+ Browse

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

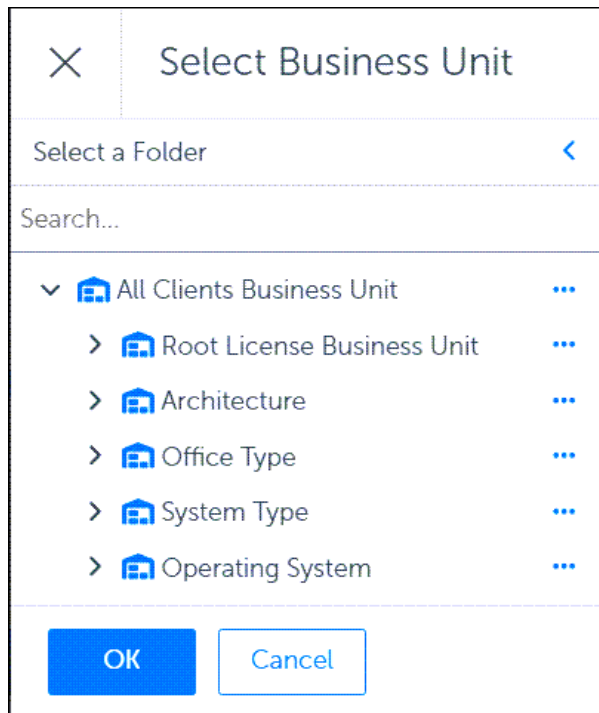
Product Name	Publisher	Operating System
Google Chrome Beta x86	Google LLC	Windows
Google Chrome Beta x64	Google LLC	Windows
Google Chrome x86	Google LLC	Windows
Google Chrome x64	Google LLC	Windows

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

Add Target Business Units for Patch Exceptions

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

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



3. Select **OK** on the lower-left of the **Select Business Unit** dialog.
4. Select **Save** on the upper-left of the **Patching Exceptions** dialog to save your progress:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.

Global Pause

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

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

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

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

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

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

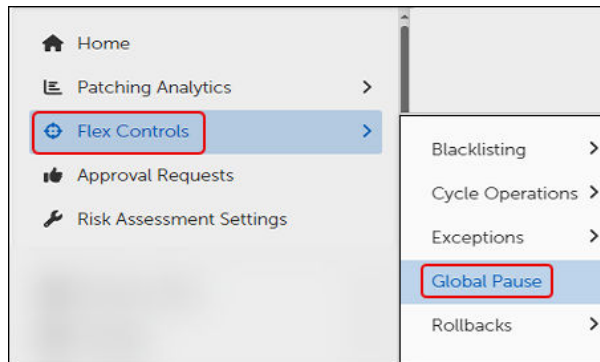
Paused Cycles: Pause Patching, Deployment, or Rollout Cycles either for specified Business Units or for the Business Units already targeted by the Cycle.

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

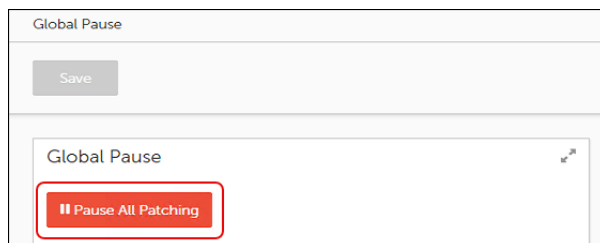
Stop All Patching Activity Immediately

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

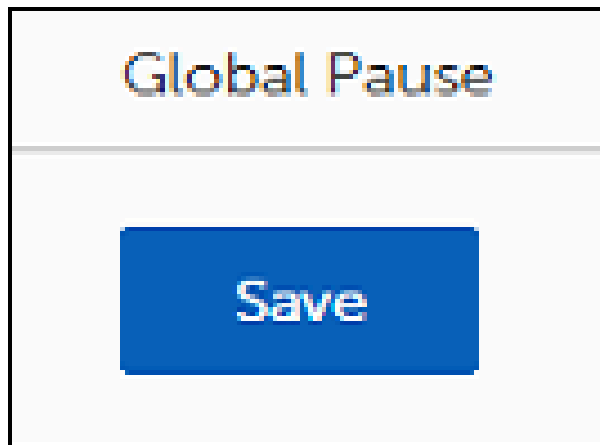
1. Select **Flex Controls** on the Home menu, and then select **Global Pause**.



This opens the **Global Pause** dialog:



2. Select **Pause All Patching**.

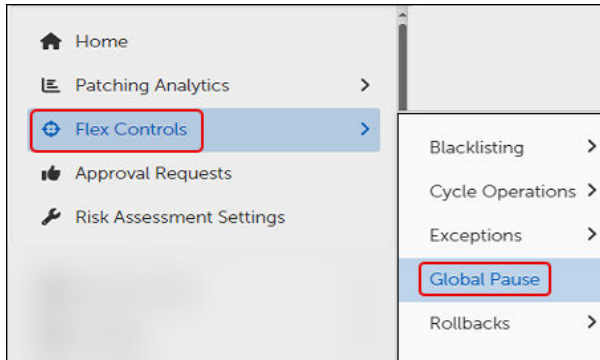


3. Select **Save** to activate Global Pause. This immediately stops all patch deployments across all licensed clients:
 - All patch deployments in progress that have not reached an irreversible state are paused immediately.
 - All newly initiated patch deployments are paused automatically.

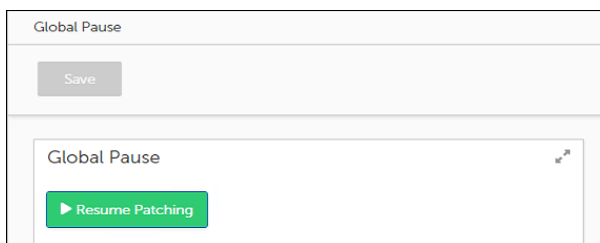
Resume All Paused Patching Activity Immediately

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

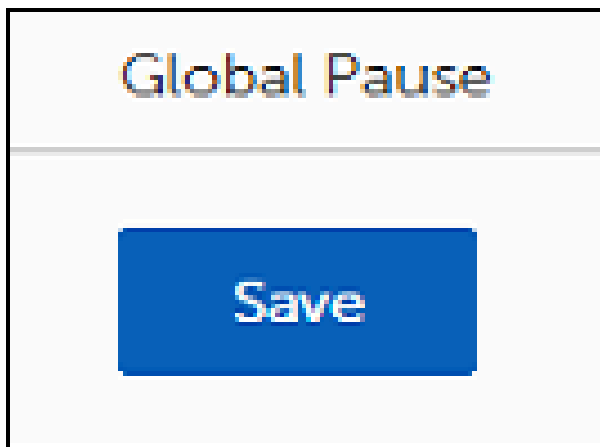
1. Select **Flex Controls** on the Home menu, and then select **Global Pause**.



This opens the **Global Pause** dialog:



2. Select **Resume Patching**.

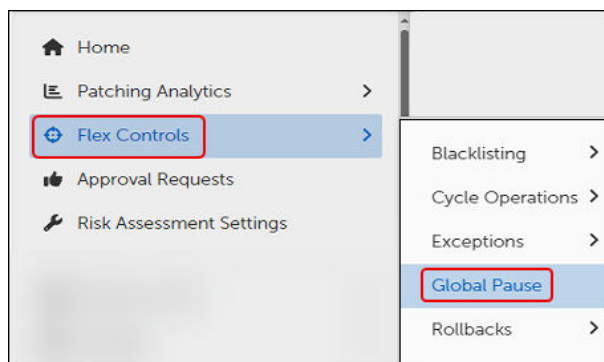


3. Select **Save** to revoke the Global Pause. This immediately revokes the Global Pause and allows patching activity to occur as configured.

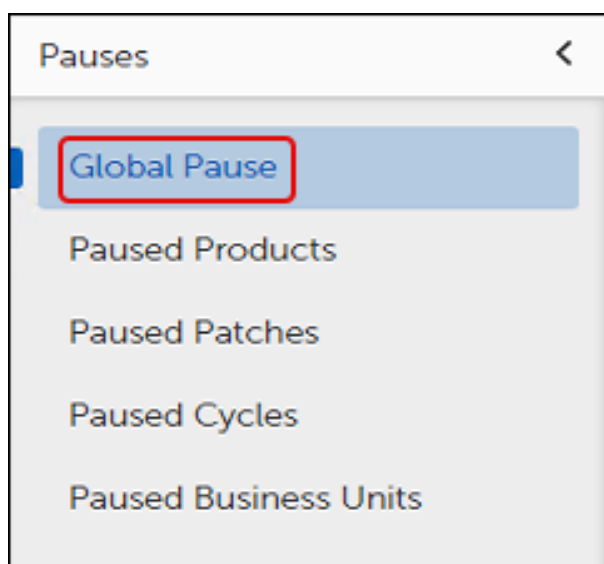
Pause Patching for Specific Objects

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

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



This opens the Pauses menu:



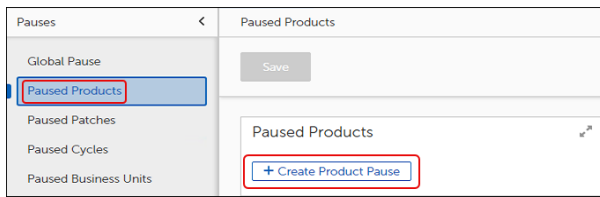
2. Select the pause you want to configure. You can configure multiple types of pauses, but you must configure them separately.
 - **Global Pause:** Pause all patching activity immediately ([Stop All Patching Activity Immediately](#)).
 - **Paused Products:** Pause patch deployments for one or more products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

Pause Deployment of a Specific Software Product

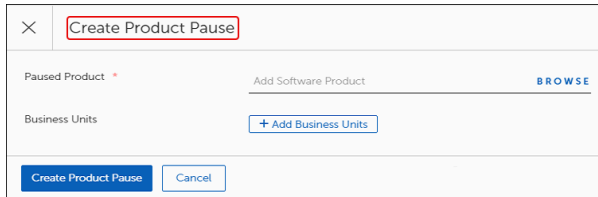
To stop patching activity for specific software products or patches, complete the following steps:

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

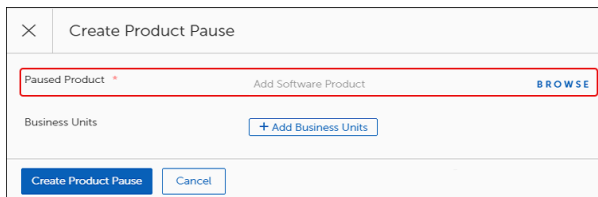
This opens the Paused Products dialog:



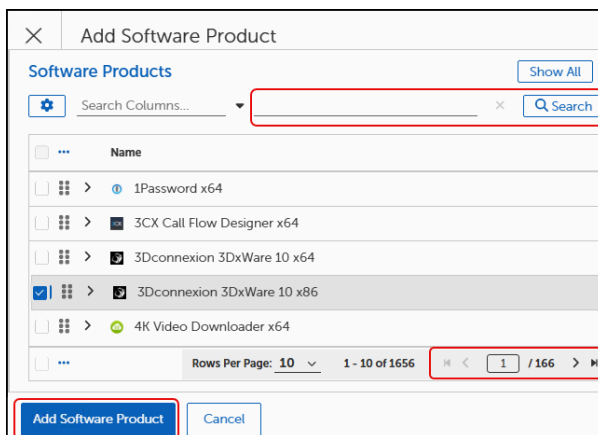
- a. Select **+Create Product Pause** to open the **Create Product Pause** dialog:



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

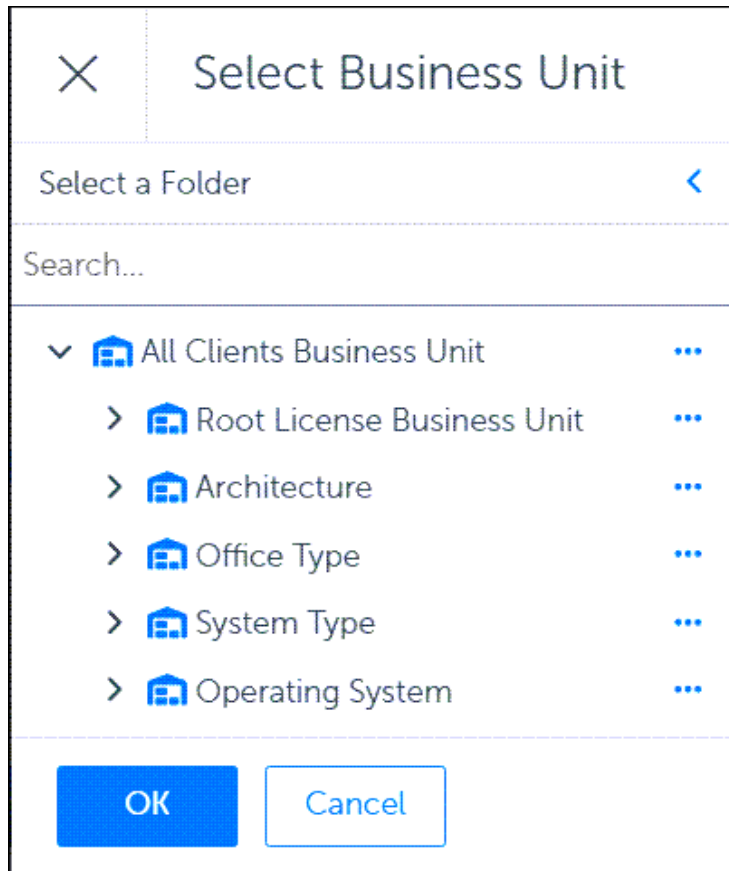


- c. Select the software product you want to pause using either of the following methods:



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

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



- b. Select **OK**.

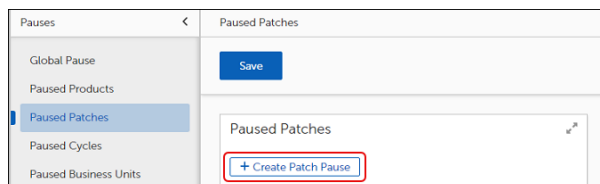
4. Select **Create Product Pause**, and then select **Save** to create a global pause for the selected products.

Pause Deployment of a Specific Patch

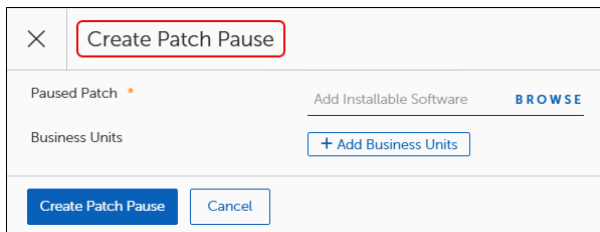
To stop patching activity for a specific patch, complete the following steps:

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

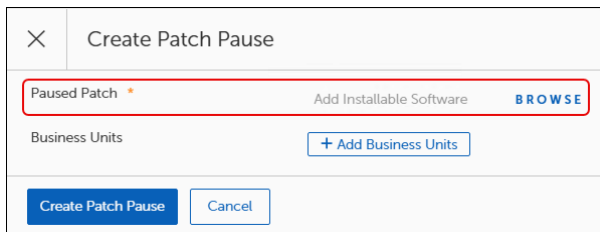
This opens the Paused Patches dialog:



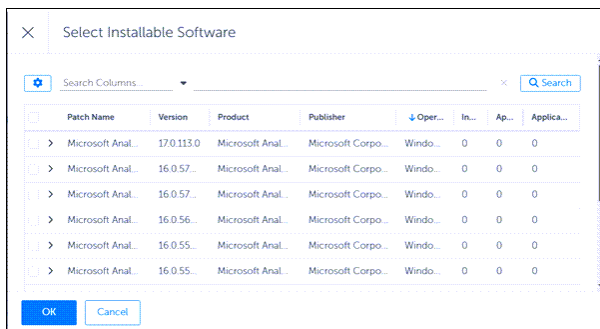
- a. Select **+Create Patch Pause** to open the **Create Product Pause** dialog, and then select **Browse** to find the Software patch you want to pause:



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

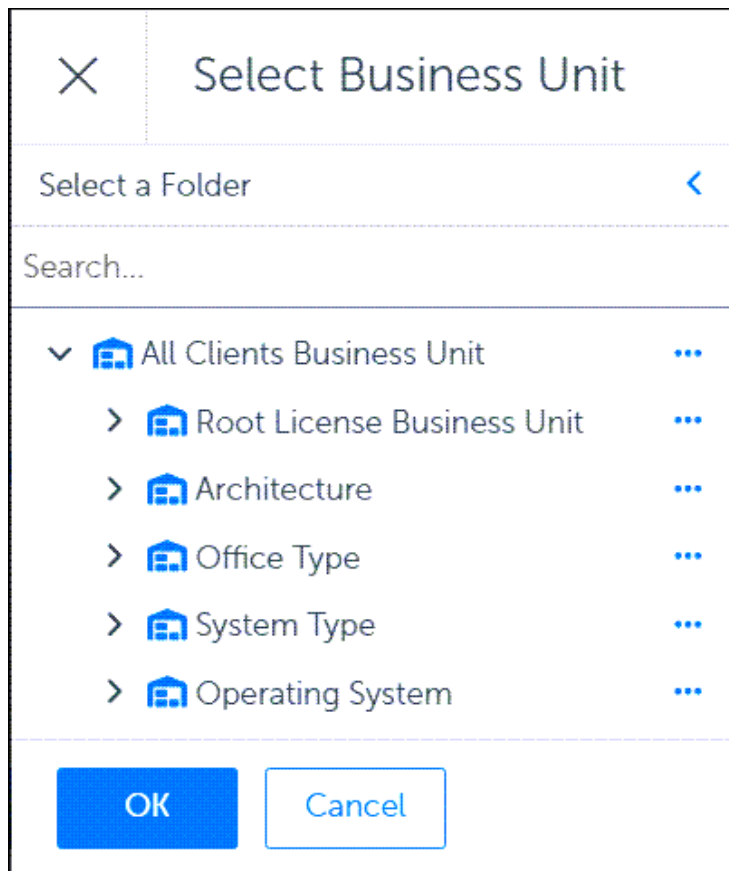


c. Select the patch you want to pause:



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

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



- b. Select **OK**.

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

Pause Specific Cycles

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

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



IMPORTANT

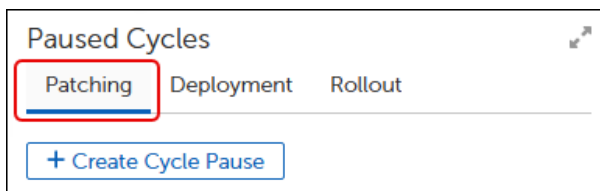
Pausing a cycle that is currently in a WAITING state (has not run yet), prevents that cycle from running until you remove the pause. This is the only server-side behavior related to pausing.

Pause a Patching Cycle

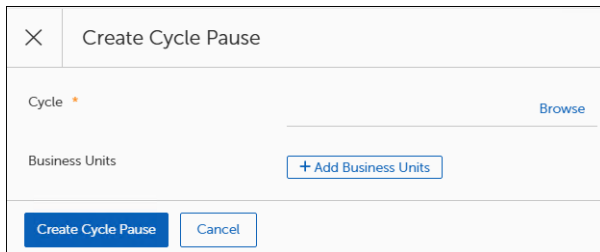
To stop patching activity for a specific patching cycle, complete the following steps:

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

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



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

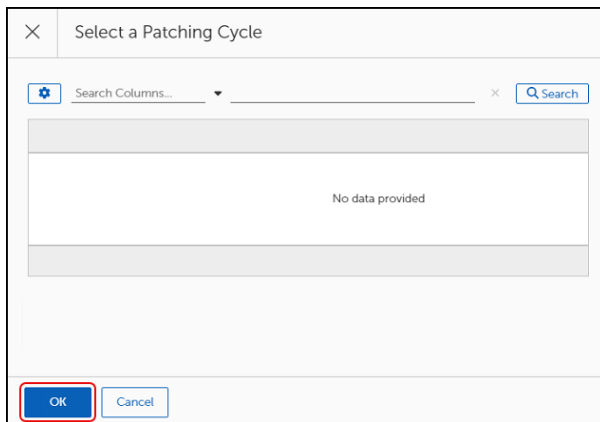


3. Search for and select the patching cycle you want to pause using one of the methods described below:



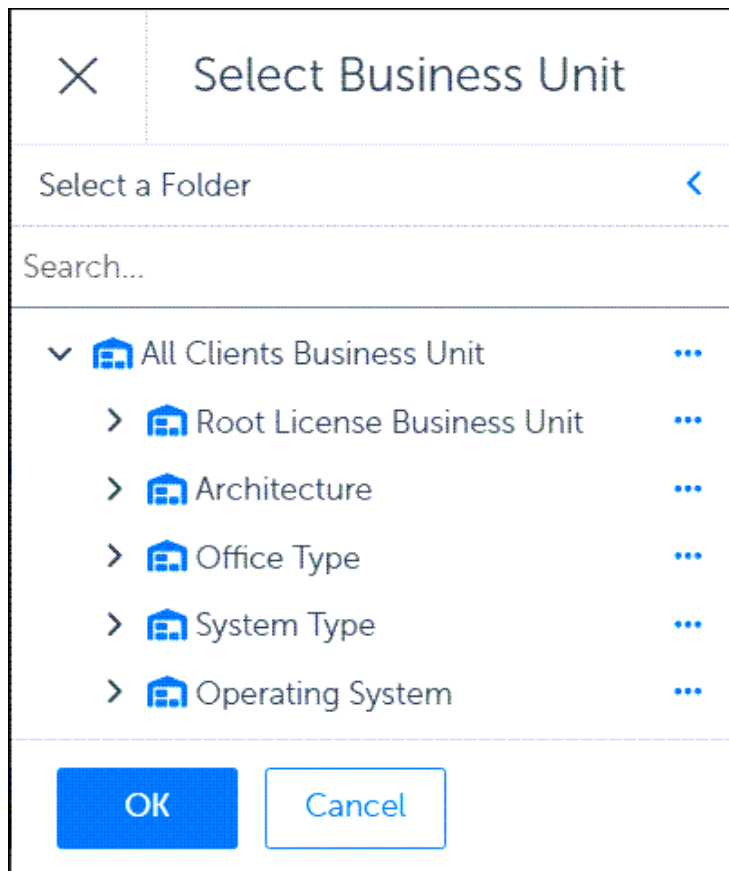
IMPORTANT

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



- Use the navigation tools on the bottom right to scroll through the pages to find and select a Patching Cycle from the table.
 - Enter a cycle name in the search line, select **Search** to find, and then select a specific cycle.
4. Select **OK**, and then choose one of the following options to proceed:
- To create a **Global Pause** for the selected cycle, skip to **Step 6**. This pauses the deployment of the selected cycle on all devices in the estate.
 - To specify a pause for specific devices, continue with the next step to **Add Business Units**.
5. Add or remove **Business Units**:

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



- b. Select **OK**.

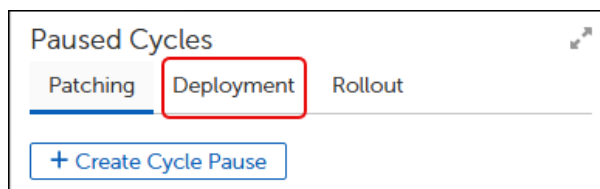
6. Select **Create Cycle Pause**, and then select **Save** to create a pause for the selected cycle.

Pause a Deployment Cycle

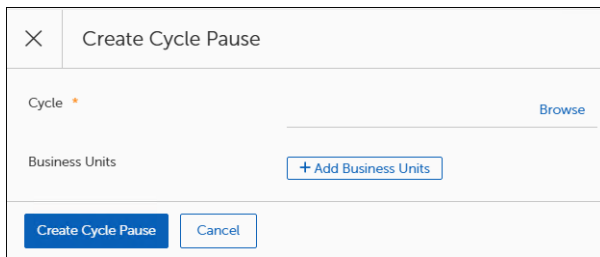
To stop all patching activity for a specific deployment cycle, complete the following steps:

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

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



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



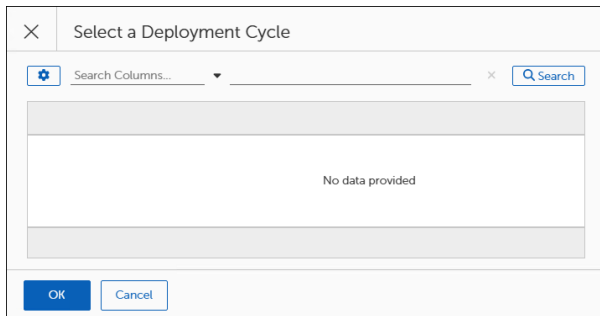
The 'Create Cycle Pause' dialog box features a close button (X) in the top-left corner. Below the title bar, there is a 'Cycle' field with a red asterisk and a 'Browse' link to its right. Underneath, the 'Business Units' section includes a '+ Add Business Units' button. At the bottom, there are two buttons: 'Create Cycle Pause' (highlighted in blue) and 'Cancel'.

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



IMPORTANT

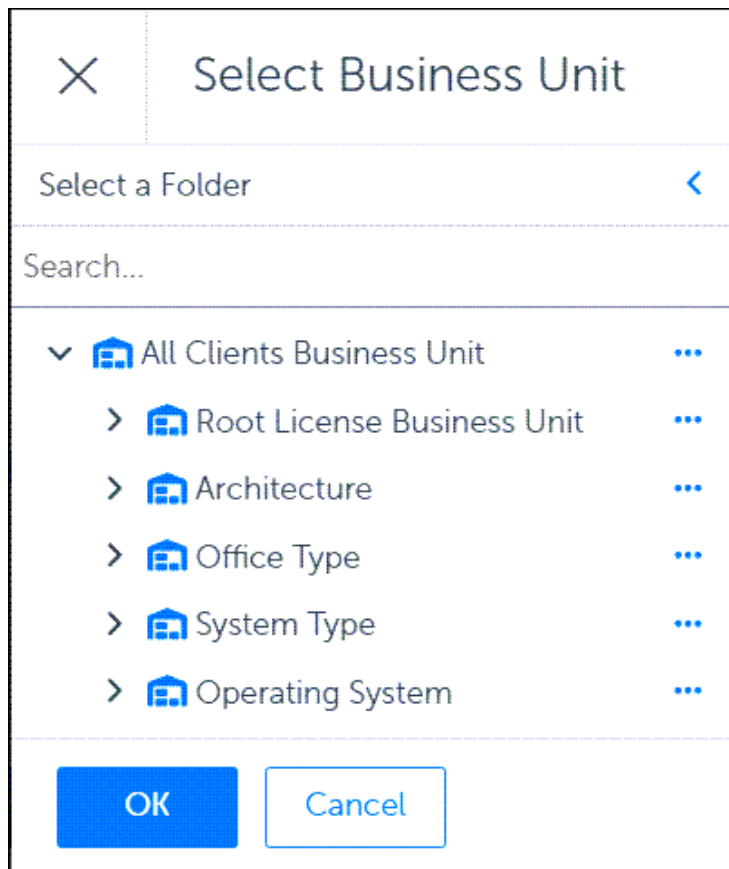
Cycles do not appear unless you have created them previously. If you do not have a cycle to pause, choose a different pause method.



The 'Select a Deployment Cycle' dialog box has a close button (X) in the top-left corner. Below the title bar, there is a search bar with a 'Search Columns...' dropdown, a search icon, and a 'Search' button. The main area contains a table with the message 'No data provided' in the center. At the bottom, there are 'OK' (highlighted in blue) and 'Cancel' buttons.

- Use the navigation tools on the lower-right to scroll through the pages to find and select a cycle from the table.
 - Enter a cycle name in the search line, select **Search** to find, and then select a specific cycle
4. Select **OK** to save your entry, and then choose one of the following options to proceed:
 - To create a **Global Pause** for the selected cycle, skip to **Step 6**. This pauses the deployment of the selected software product on all devices in the estate.
 - To specify a pause for specific devices, continue with the next step to **Add Business Units**.
 5. Add or remove **Business Units**:

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



- b. Select **OK**.

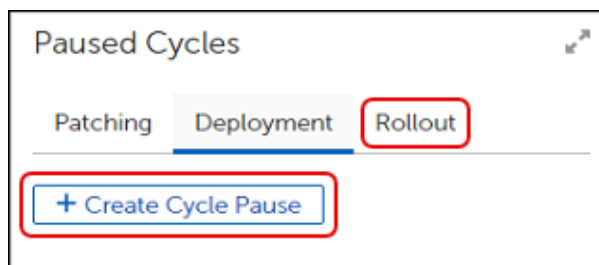
6. Select **Create Cycle Pause**, and then select **Save** to create a pause for the selected cycle.

Pause a Rollout Cycle

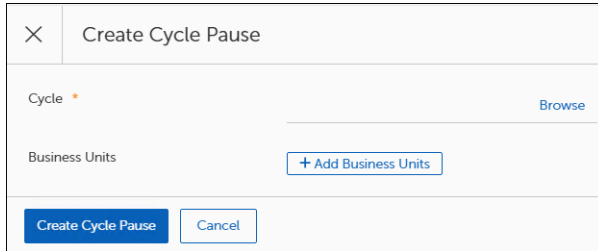
To stop all patching activity for a specific rollout cycle, complete the following steps:

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

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



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



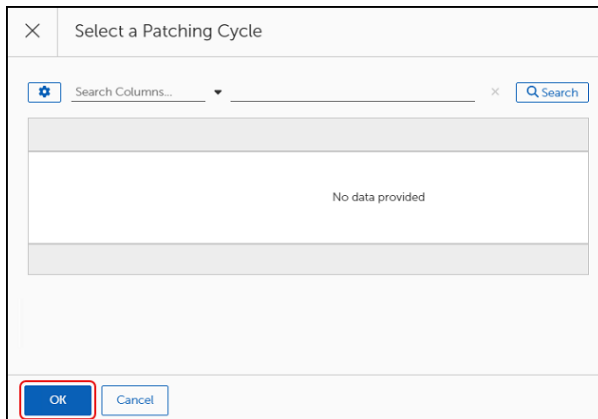
The 'Create Cycle Pause' dialog box features a title bar with a close button (X) and the text 'Create Cycle Pause'. Below the title bar, there is a 'Cycle' field with a red asterisk and a 'Browse' button. Underneath, the 'Business Units' section includes a '+ Add Business Units' button. At the bottom, there are two buttons: 'Create Cycle Pause' and 'Cancel'.

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



IMPORTANT

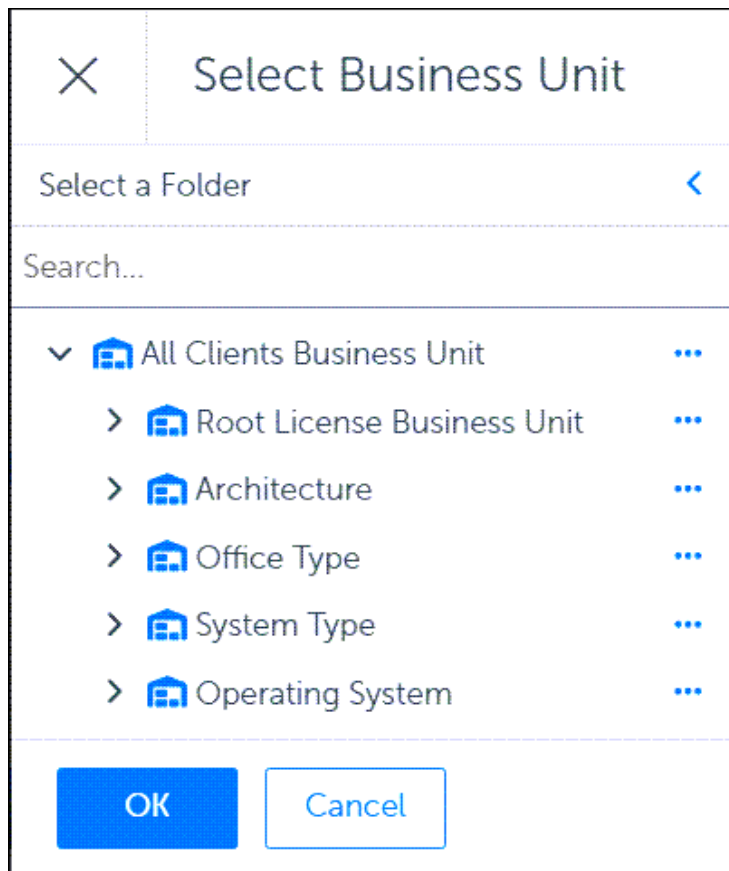
Cycles do not appear unless you have created them previously. If you do not have a cycle to stop, do not complete this section.



The 'Select a Patching Cycle' dialog box has a title bar with a close button (X) and the text 'Select a Patching Cycle'. It includes a 'Search Columns...' dropdown menu and a 'Search' button. The main area displays 'No data provided'. At the bottom, there are 'OK' and 'Cancel' buttons, with the 'OK' button highlighted by a red rectangle.

- Use the navigation tools on the lower-right to scroll through the pages to find and select a **Rollout Cycle** from the table.
 - Enter a cycle name on the search line, and then select **Search** to find and select a specific cycle.
4. Select **OK** , and then choose one of the following options to proceed:
 - To create a **Global Pause** for the selected cycle, skip to **Step 6**. This pauses the deployment of the selected software product on all devices in the estate.
 - To specify a pause for specific devices, continue with the next step to **Add Business Units**.
 5. Add or remove **Business Units**:

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



- b. Select **OK**.

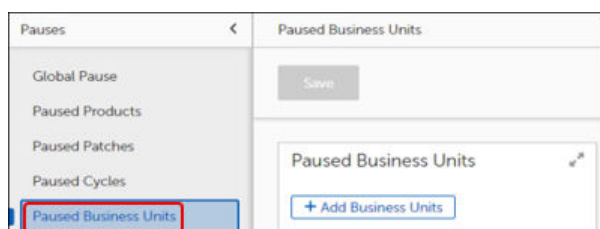
6. Select **Create Cycle Pause**, and then select **Save** to create a pause for the selected rollout cycle.

Pause Deployment to a Business Unit

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

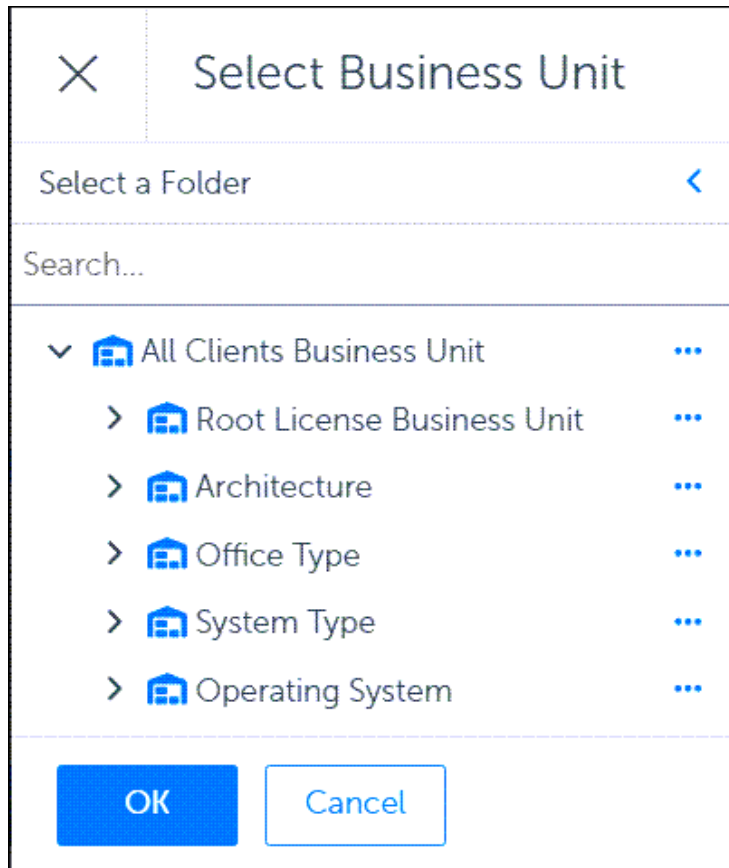
1. Navigate to the Pauses menu (see [Pause Patching for Specific Objects](#)), and then select **Paused Business Units**.

This opens the **Paused Business Units** dialog:



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

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



- b. Select **OK**.

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

Rollbacks Overview

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

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

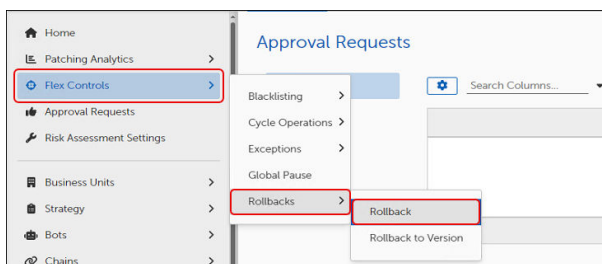
Rollback

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

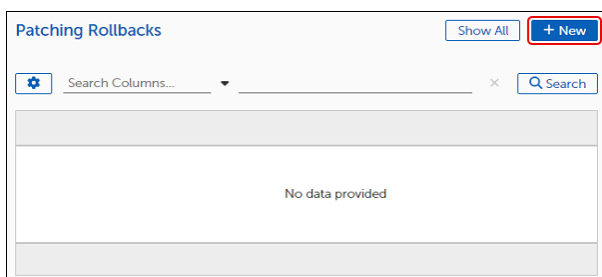
Create a Rollback

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


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



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



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

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

General Settings

Name *

Name

Description

Description

Patch ⓘ *

Add Installable Software

BROWSE

Target Business Units ⓘ *

+ Add Business Units

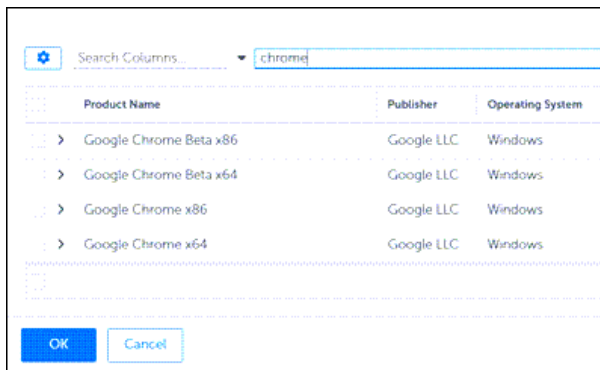
3. Locate the patch or release you want to roll back:

Patch ⓘ *

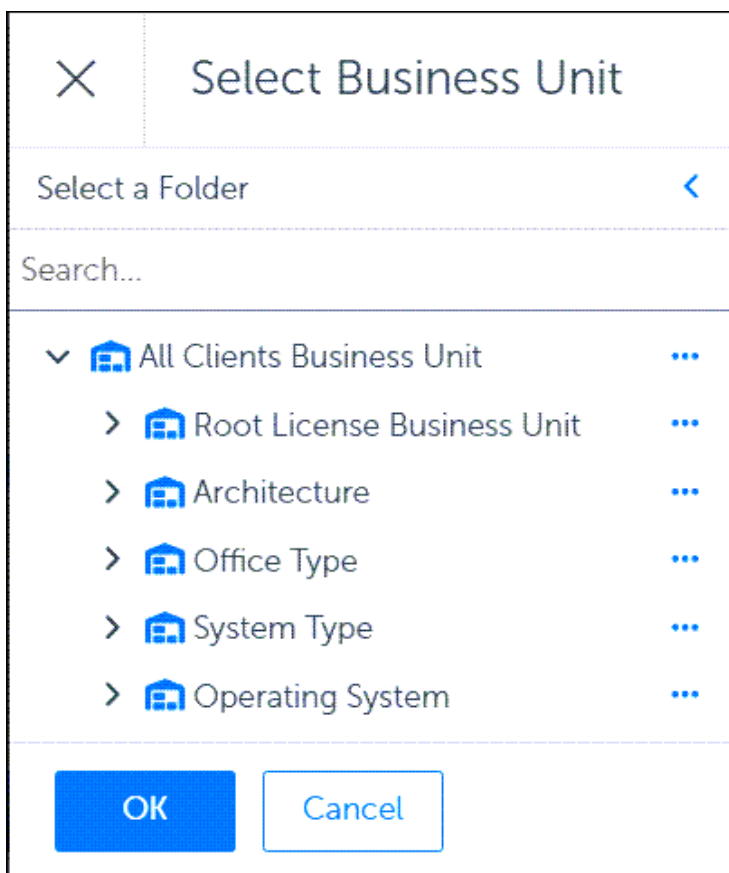
Add Installable Software

BROWSE

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



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



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

Edit a Rollback Template

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

Patching Rollbacks Show All + New

Search Columns... Q Search

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

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 *

Description

Patch * BROWSE x

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 of the template to save the new settings.

Copy a Rollback

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

Patching Rollbacks Show All + New

Search Columns... Q Search

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

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](#)

Name	Actions
Operating System	

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

Save More

- New Rollback
- Open Rollback
- Save Rollback As
- Delete Rollback

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

Save [Name] as

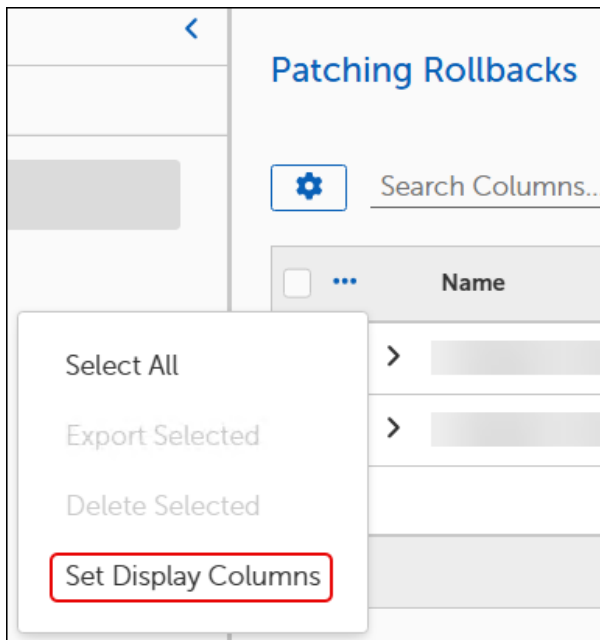
Enter new name for [Name] *

Save as Cancel

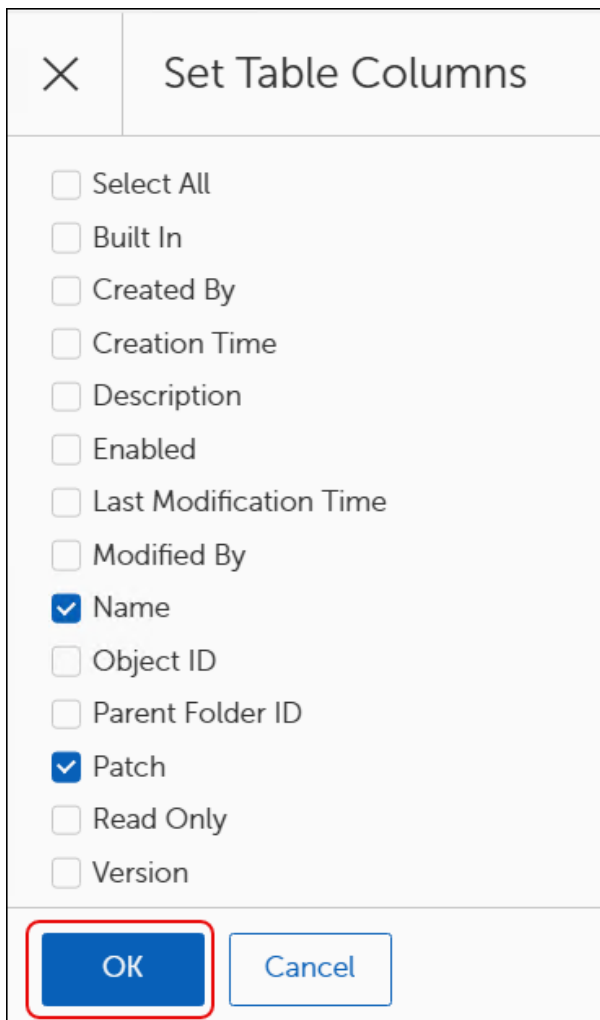
4. Revise the **Description** to reflect any changes needed for the copy, and then select **Save**.
5. Select **Back to Rollbacks** on the upper-left of the template to return to the **Rollbacks** table and view your changes.

Customize Patching Rollback Table Settings

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



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



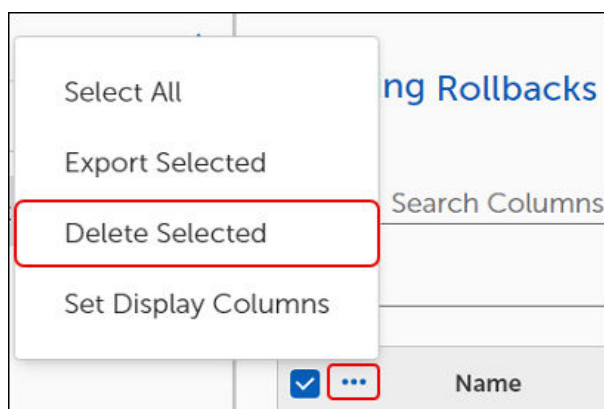
3. Select the **column names** you want the **Patching Rollbacks** table to display, and then select **OK**.

Delete a Rollback

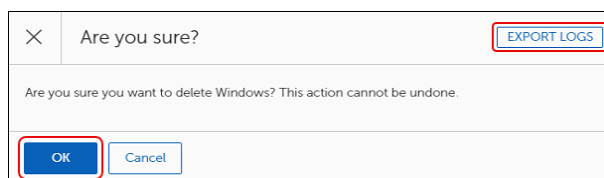
1. Select a **Rollback** template from the **Patching Rollbacks** table of an open [Patching Rollbacks](#) template.

Name	Patch	Actions
Windows	NET 3.5 Feature on Demand for X64	...
Windows Rollback	NET 3.5 Feature on Demand for X86	...
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**.



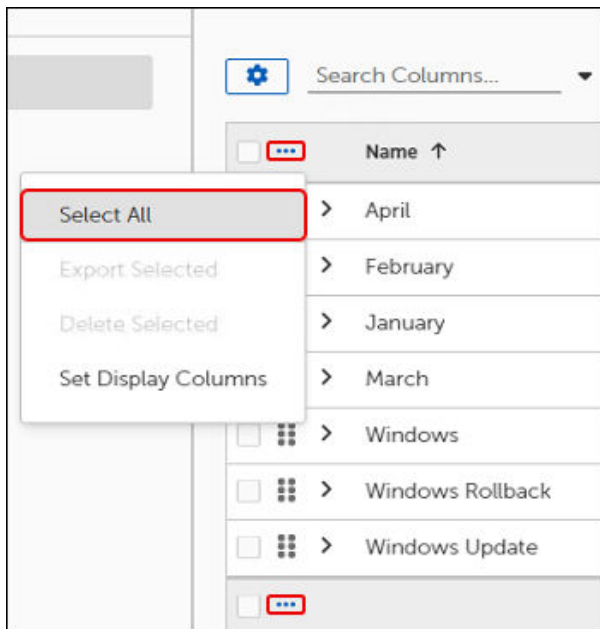
3. Review the **Are you sure?** dialog:



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

Select All Rollbacks

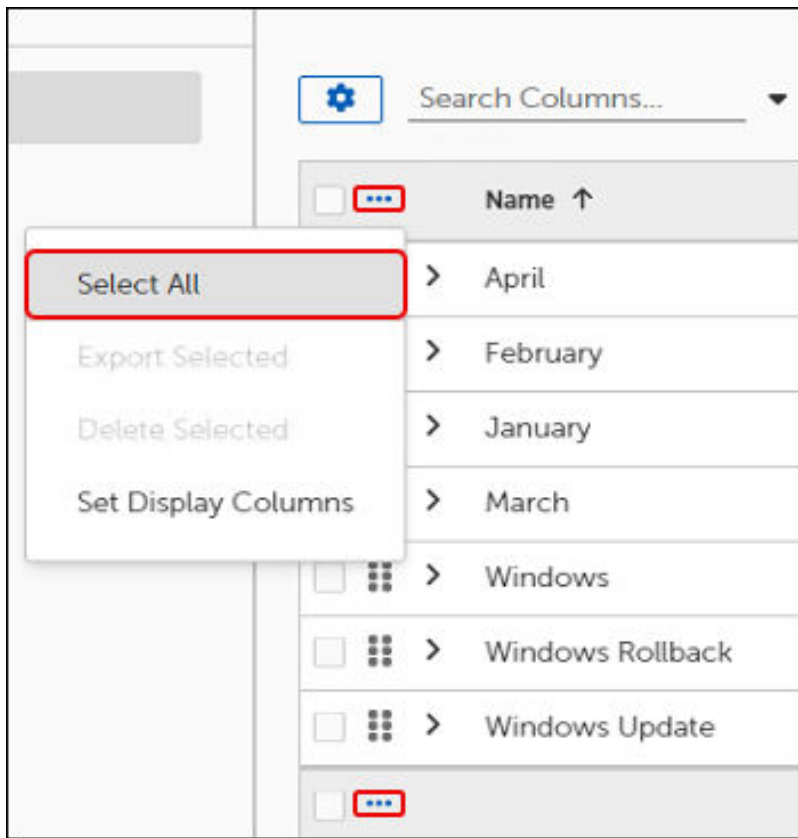
1. Open the **Patching Rollbacks** table (**Flex Controls > Rollbacks > Rollback**).
2. Select the **ellipsis (...)** next to **Name**, and then select **Select All**.



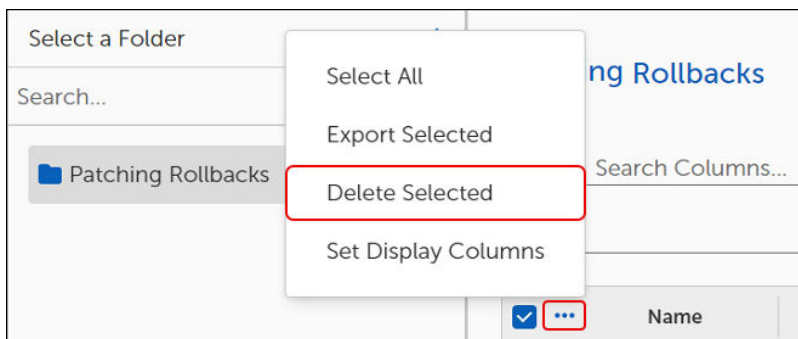
3. Select the ellipsis (...) again, and then choose what you want to do with the selected Rollbacks:
 - To export the selected Rollbacks, see [Select All Rollback to Version Objects](#).
 - To delete the selected templates, see [Bulk Delete Rollbacks](#).
 - To customize the display columns of the **Patching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

Bulk Delete Rollbacks

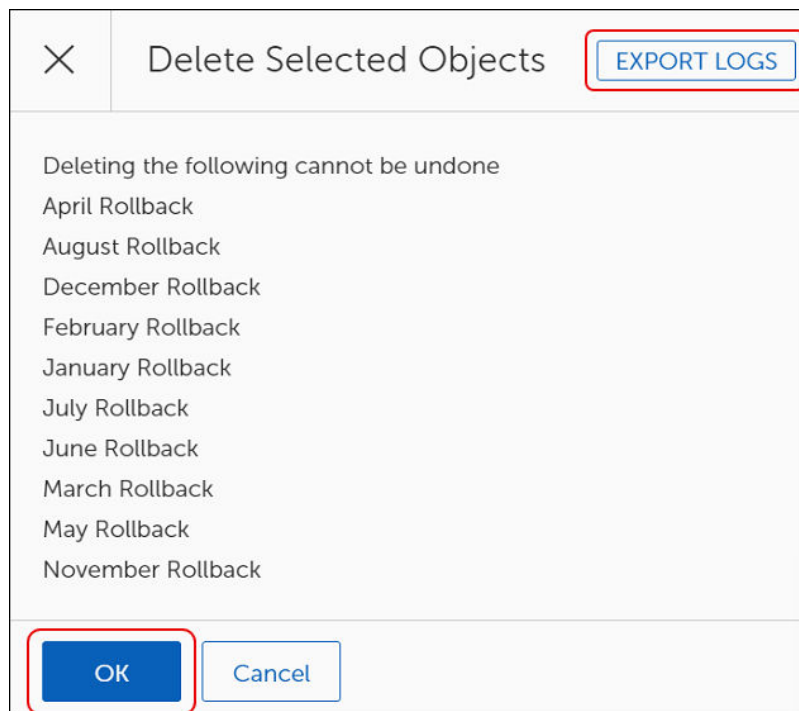
1. Open the **Patching Rollbacks** table (Flex Controls > Rollbacks > Rollback).
2. Select the **ellipsis (...)** next to **Name**, and then select **Select All**.



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



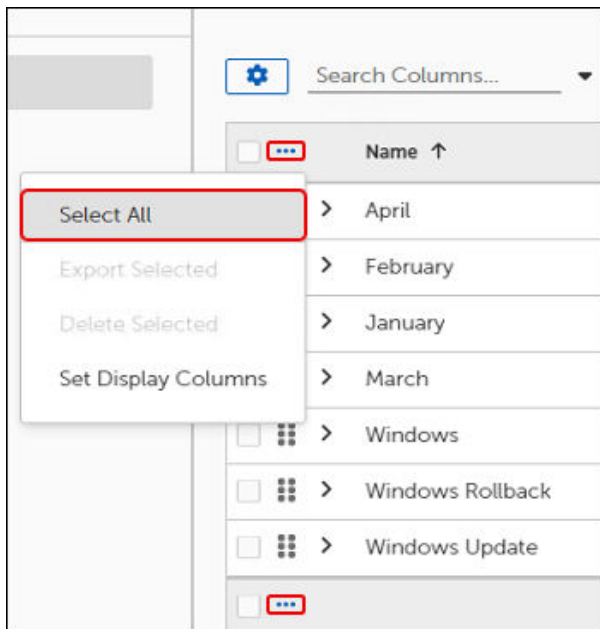
This opens the **Delete Selected Objects** dialog:



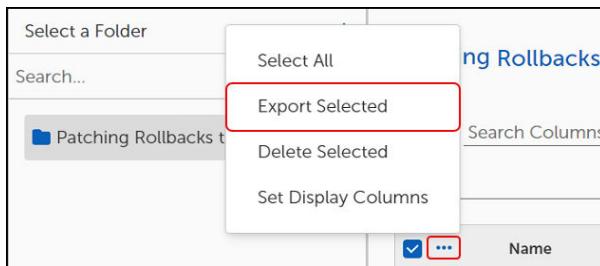
4. (Optional) Select **Export Logs** on the top-right corner of the **Delete Selected Objects** dialog to export trace logs. The trace logs download to your device as a file with a `.log` extension.
5. Select **OK** to delete the Rollbacks. This returns you to the **Patching Rollbacks** table where the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

Export Rollbacks

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



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



This opens the **Object Export Settings**:

 A screenshot of the "Object Export Settings" dialog box. It has a title bar with a checkmark icon and a close button. The dialog is divided into two main sections. The top section is titled "Exporting Organization" and contains a text input field labeled "Exporting Organization Name". The bottom section is titled "Description" and contains a large text area labeled "Description". At the bottom of the dialog, there are two toggle switches: "Export as JSON" and "Automatically Import Objects Into the Specified Folder". Both toggle switches are currently turned off.

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

Errors (1)			
<div> <div>Search Columns...</div> <div>Search</div> </div>			
<input type="checkbox"/> Name	Type	Error Description	Actions
<input type="checkbox"/> Office Type	BusinessUnit	Children to export must be specified for Business unit	Resolve
<div> <div>Rows Per Page: 10</div> <div>1 - 1 of 1</div> <div>1 / 1</div> </div>			

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

Configure Object Export Settings

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

Object Export Settings

Exporting Organization

Exporting Organization Name

Description

Description

Export as JSON

Automatically Import

Objects Into the

Specified Folder

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



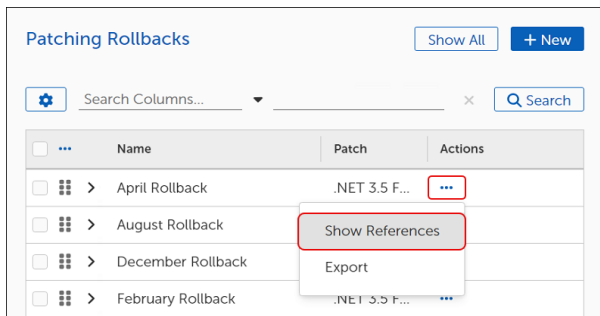
IMPORTANT

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

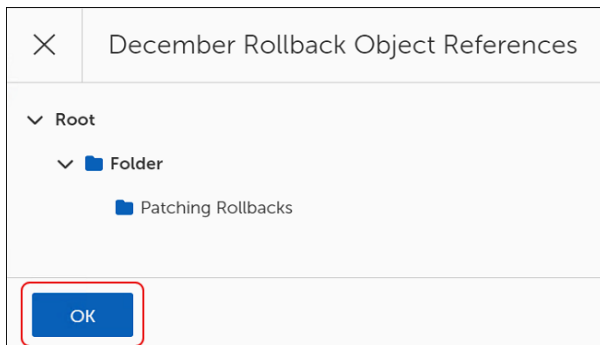
Show Rollback References

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

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



This opens the [Rollback Name] Object References dialog.



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

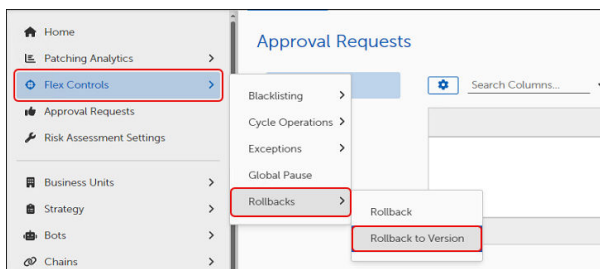
Rollback to Version

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

Create a Rollback to Version

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

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



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

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



NOTICE

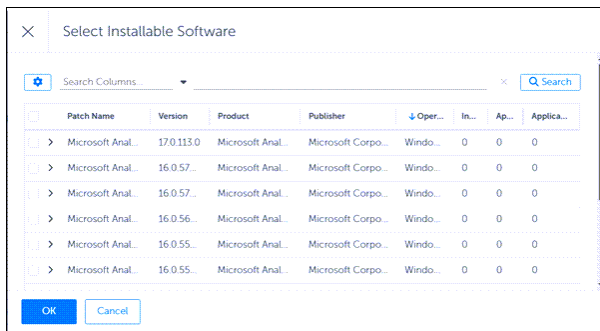
A red asterisk next to a field name indicates a required field.

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

Choose the Software Patch or Release Version to Roll Back From

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

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



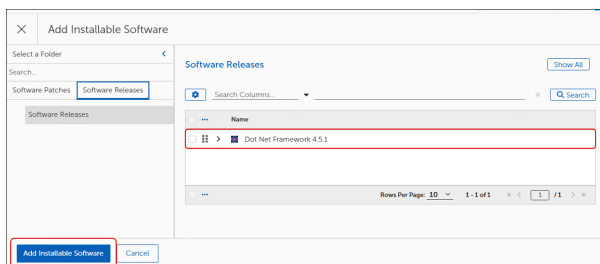
3. Select **Add Installable Software** to return to the Rollback to Version template.
4. [Choose the software patch or release version to roll back to.](#)

Choose the Software Patch or Release Version to Roll Back To

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



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



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

Add Business Units for a Rollback to Version

1. Add one or more **Business Units** using the following steps:
 - a. Select the Business Units.

×

Select Business Unit

Select a Folder <

Search...

▼

🏠 All Clients Business Unit

...

>

🏠 Root License Business Unit

...

>

🏠 Architecture

...

>

🏠 Office Type

...

>

🏠 System Type

...

>

🏠 Operating System

...

OK

Cancel

b. Select **OK**.

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

Edit a Rollback to Version Template

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

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

This opens the template.

General Settings

Name *

Description

Patch ⓘ *

Rollback ⓘ *

Target Business Units ⓘ *

Add Installable Software BROWSE

Add Installable Software BROWSE

+ 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** upper-left of the template to save the changes.

Copy a Rollback to Version Template

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

Rollback To

Show All + New

Search Columns... Search

Name	Patch	Rollback...	Actions
Visual St...	Visual Studio 2017 version 15.9.62 update	Visual S...	...

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

This opens the template.

General Settings

Name *

Description

Patch ⓘ *

Rollback ⓘ *

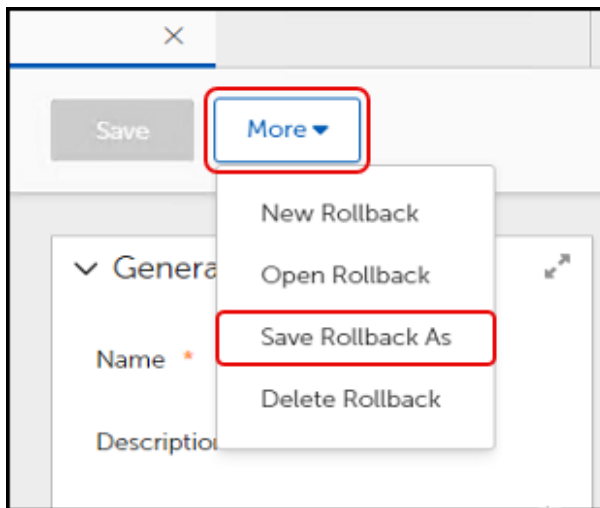
Visual Studio

This example of a Rollback to Version rolls back Visual Studio 15.9.62 to 15.9.54.

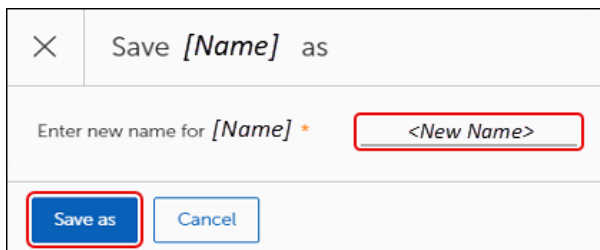
Visual Studio 2017 version 15.9.62 update BROWSE X

Visual Studio 2017 version 15.9.54 update BROWSE X

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



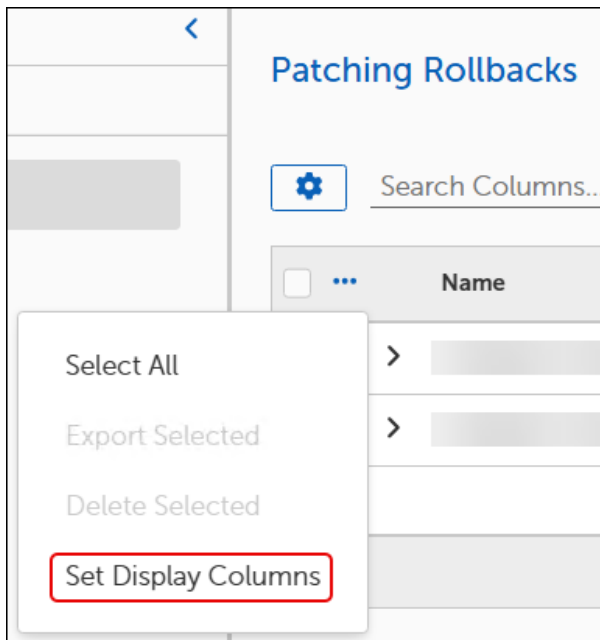
3. Enter a new **Name** for the template, and then select **Save as**.



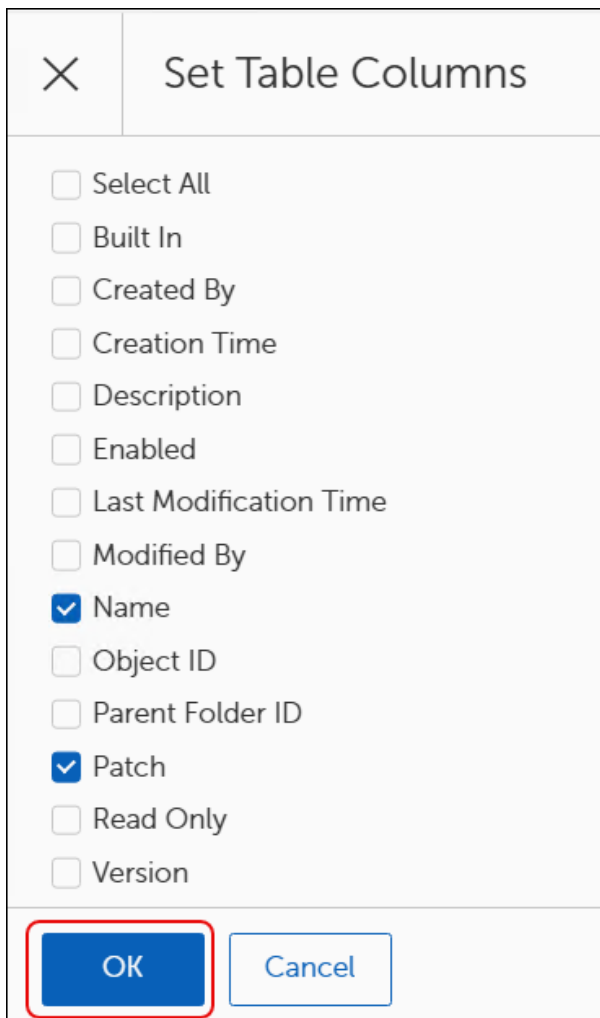
4. Revise the **Description** to reflect any changes needed for the copy, and then select **Save**.
5. Select **Back to Rollbacks** on the upper-left of the template to return to the **Rollbacks** table and view your changes.

Customize Patching Rollback Table Settings

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



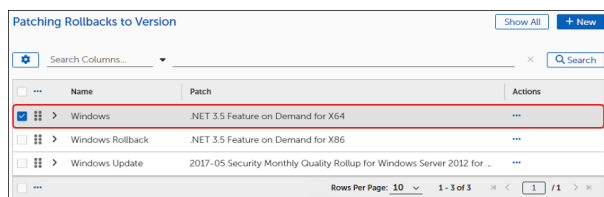
This opens the **Set Table Columns** dialog.



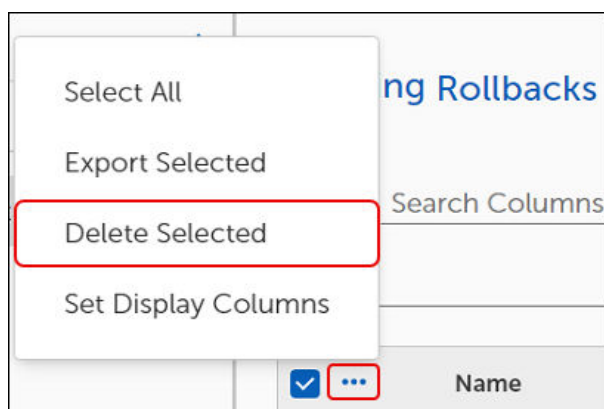
3. Select the **column names** you want the **Patching Rollbacks** table to display, and then select **OK**.

Delete a Rollback to Version

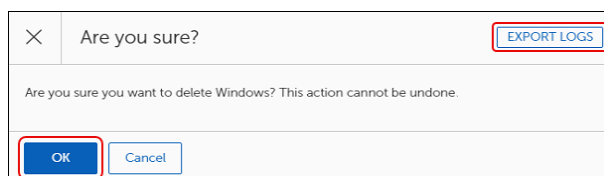
1. Select a **Rollback to Version** template from the **Patching Rollbacks to Version** table of an open [Patching Rollbacks](#) template.



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



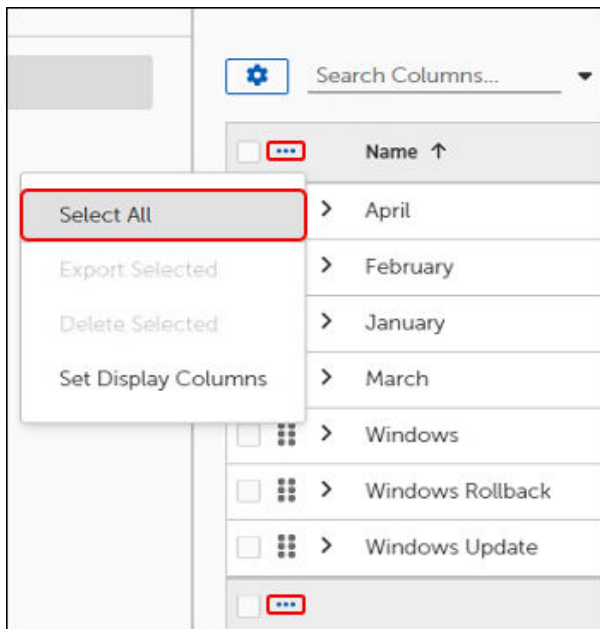
3. Review the **Are you sure?** dialog:



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

Select All Rollback to Version Objects

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

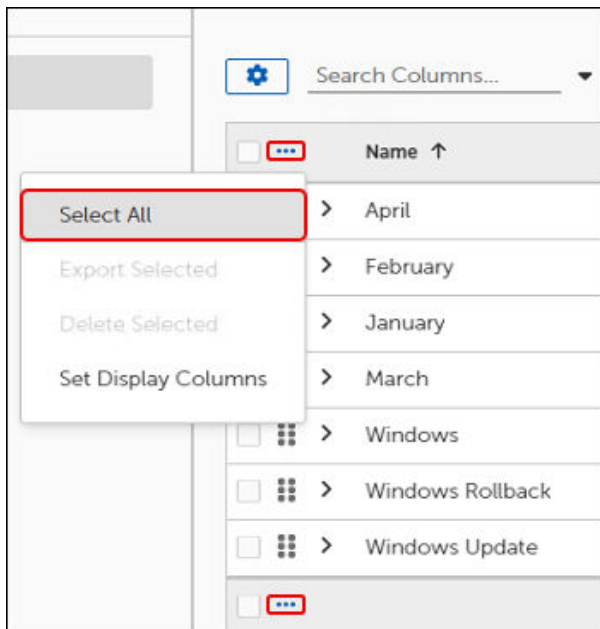


3. Select the ellipsis (...) again, and then choose what you want to do with the selected Rollbacks:
 - To export the selected Rollbacks, see [Select All Rollback to Version Objects](#).
 - To delete the selected templates, see [Bulk Delete Rollbacks](#).
 - To customize the display columns of the **Patching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

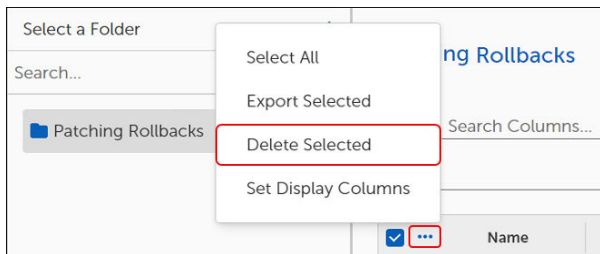
Bulk Delete Rollback to Version

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

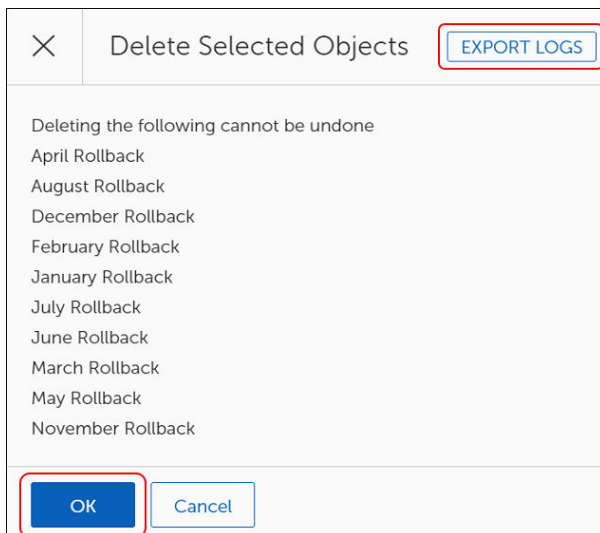
1. Open the **Patching Rollbacks** table (Flex Controls > Rollbacks > Rollback to Version).
2. Select the ellipsis (...) next to **Name**, and then select **Select All**.



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



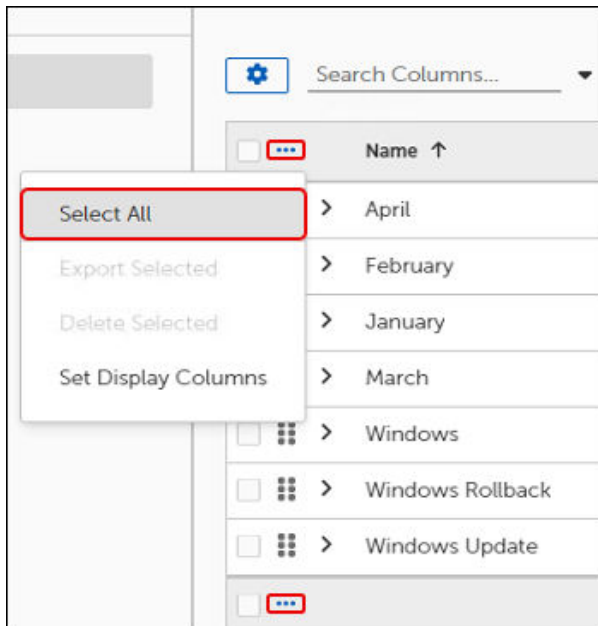
This opens the **Delete Selected Objects** dialog:



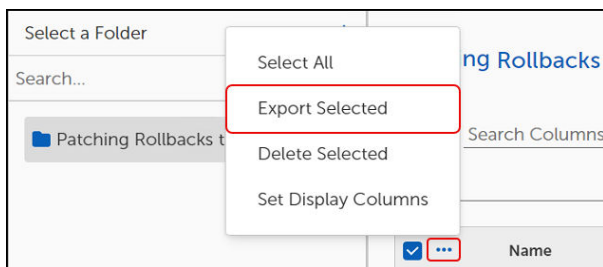
4. (Optional) Select **Export Logs** on the top-right corner of the **Delete Selected Objects** dialog to export trace logs. The trace logs download to your device as a file with a `.log` extension.
5. Select **OK** to delete the Rollbacks. This returns you to the **Patching Rollbacks to Version** table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

Export Rollback to Version

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



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



This opens the **Object Export Settings**:

A screenshot of the 'Object Export Settings' dialog box. It has a title bar with a dropdown arrow and a close button. The dialog contains several fields and controls: 'Exporting Organization' and 'Exporting Organization Name' are at the top; 'Description' is a text area below them; 'Export as JSON' is a toggle switch; 'Automatically Import Objects Into the Specified Folder' is another toggle switch. The dialog is styled with a light gray background and rounded corners.

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

Errors (1)			
<div> <div>Search Columns...</div> <div>Search</div> </div>			
<input type="checkbox"/>	Name	Type	Error Description
<input type="checkbox"/>	Office Type	BusinessUnit	Children to export must be specified for Business unit
			Resolve
<div> <div>Rows Per Page: 10</div> <div>1 - 1 of 1</div> <div>1 / 1</div> </div>			

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

Configure Object Export Settings

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

Object Export Settings

Exporting Organization

Exporting Organization Name

Description

Description

Export as JSON

Automatically Import

Objects Into the

Specified Folder

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



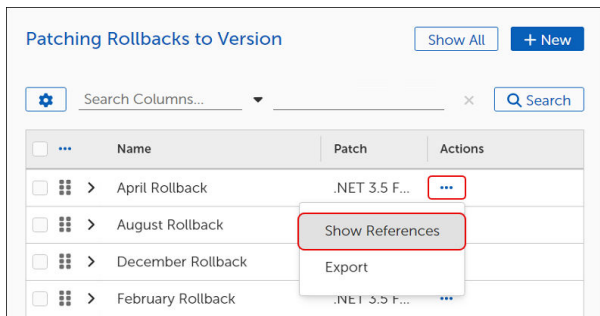
IMPORTANT

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

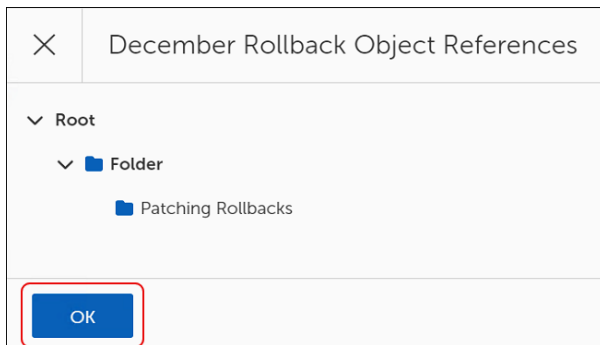
Show Rollback to Version References

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

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



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



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

Approval Requests

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

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

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

Approve or Reject a Patch Request

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

Request ID	Request Summary	Request Status	Your Response
Patching Process Appr	3/25/25, 3:58 PM	In Progress	Approve, Reject, View
Patching Process Appr	3/25/25, 8:52 AM	Completed	Approve, Reject, View

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

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.

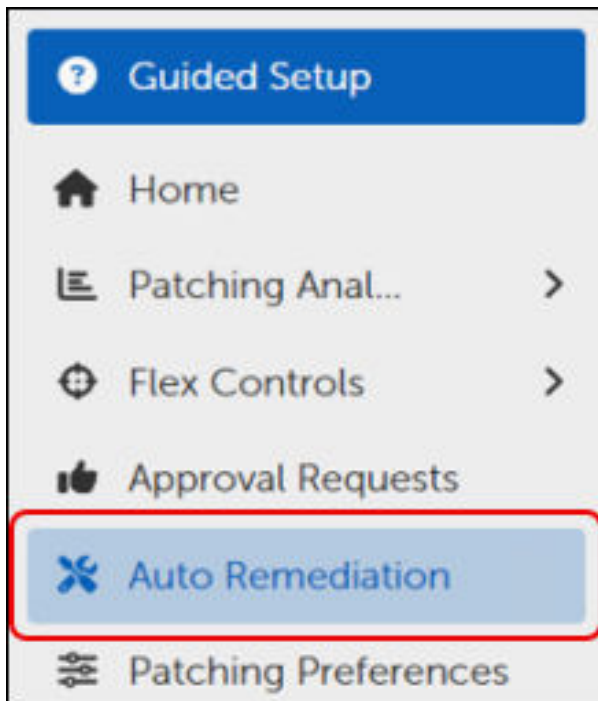
includes the following configuration options for Auto Remediation:

> Critical Security Exposure - Auto Remediation Settings	⚙️
> Vulnerability Detection Source Settings	⚙️
> Production Deployment Settings	⚙️
> Test Deployment Settings	⚙️

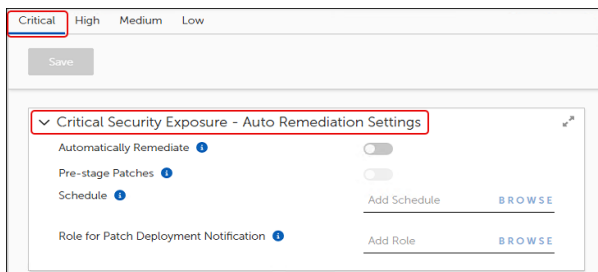
provides configuration options for Critical, High, Medium, or Low Security Exposure Levels.

Access Auto Remediation and Deployment Settings

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



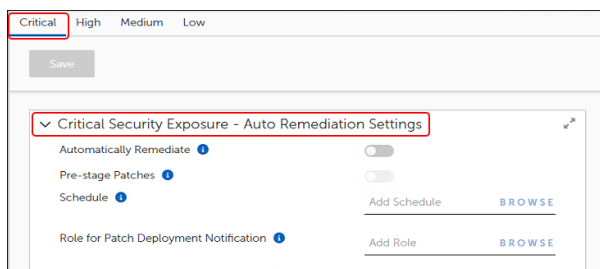
This opens the **Auto Remediation** workspace, which defaults to the Critical exposure level settings.



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

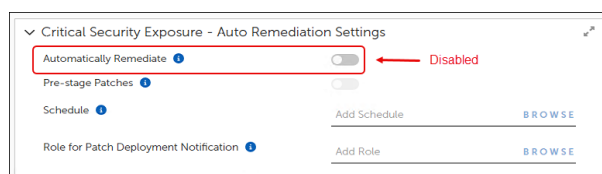
Enable automatic remediation to automatically correct all issues associated with a security level. With Auto Remediation enabled, you can also enable pre-staging of patches, which downloads the content to devices as soon as the patch becomes available. This makes the patch content available on the devices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



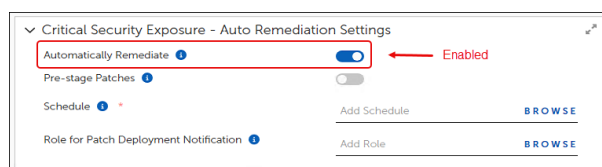
Additional settings include adding a schedule to begin the remediation process and identifying roles that receive notification of the deployment. Repeat the Auto Remediation steps for each urgency level that will use auto remediation. At any time during these configuration steps, click **Save** on the 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, remediates all vulnerabilities at the security level of the template.



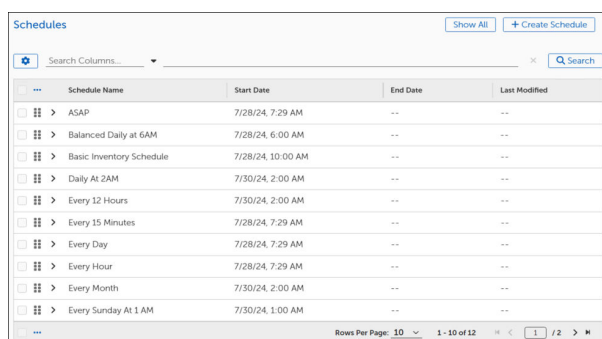
2. Select the **Pre-stage Patches** toggle to enable the automatic download of patch content to all applicable and licensed devices as soon as the patch becomes available.



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:

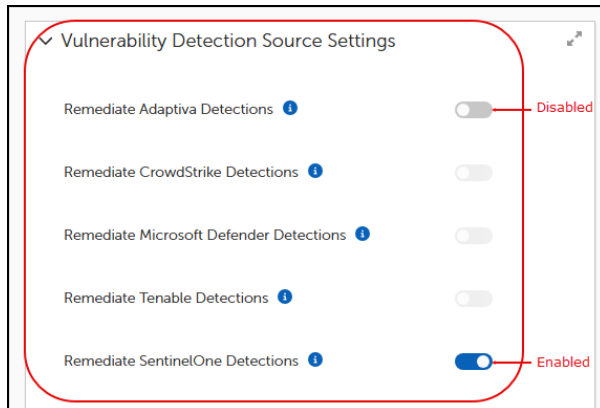


- a. Select **Show All** to see the available roles.
 - b. Select a Schedule on which to run auto remediation.
 - c. Select **Add Schedule** at the bottom left to save your changes.
4. Select **Browse** next to **Role for Patch Deployment Notification** to select the role of the administrators who require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

- Select **Show All** to see the available schedules.
- Select a **Role** to identify who receives notification of this deployment.
- 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.

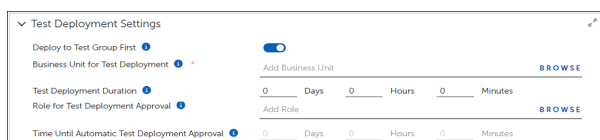
Approval Role: Roles that provide initial approval prior to deployment.

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.



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 [Patch Dashboard](#). Here you can view the high level-details of the patch environment. For more information, see [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.

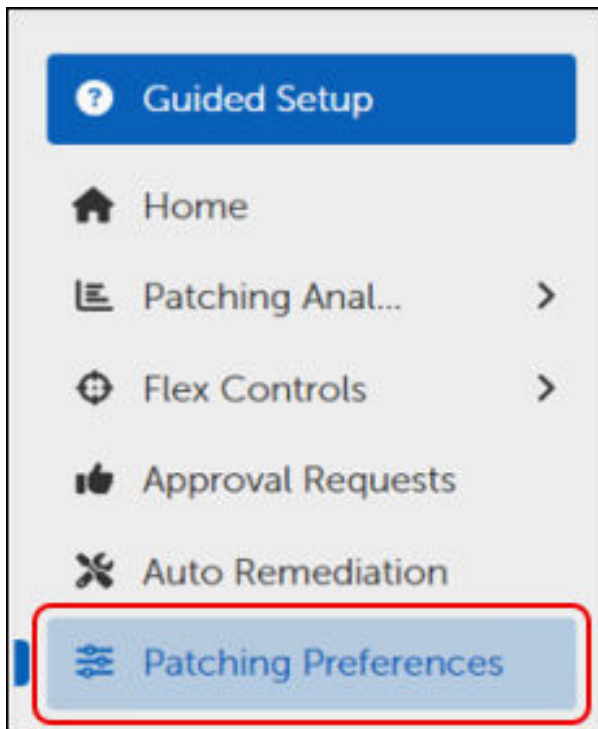
Each Patching Preference object creates its own Business Unit, which users may not edit. The Patching Preference Business Unit shares the same members (devices) as its target Business Unit, as well as any customized preferences.

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.

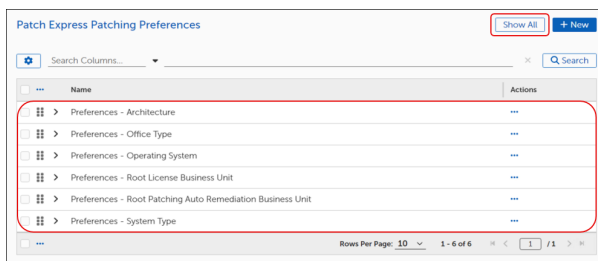


This opens the **Patch Express Patching Preferences** dialog.



TIP

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



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.

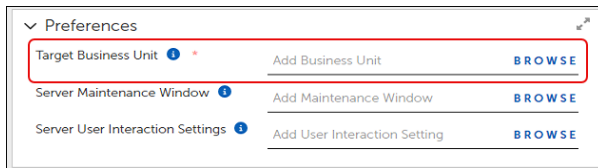
1. In an open Patching Preferences template (**+ New**), enter a Description of the preference you are creating. The system automatically generates a Name based on the target Business Unit.

2. When you finish modifying and saving the new patching preferences, click **Save** at the upper-left corner of the template.

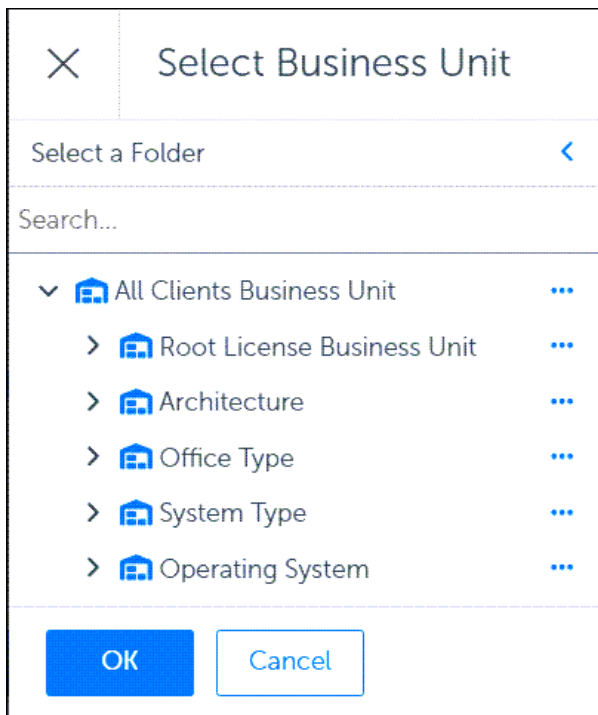
Add a Target Business Unit

Add a Target Business Unit using the following steps:

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



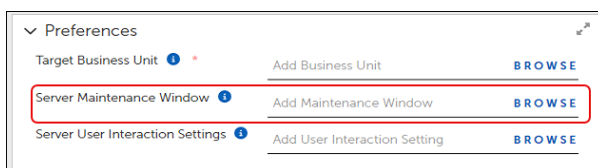
This opens the **Add Business Unit** dialog. The example shows possible choices.



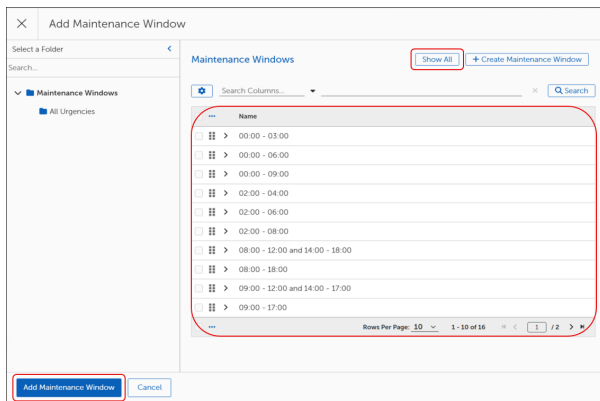
2. Select the Business Unit you want to target.
3. Select **Add Business Unit** on the bottom left of the dialog.

Select a Server Maintenance Window

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



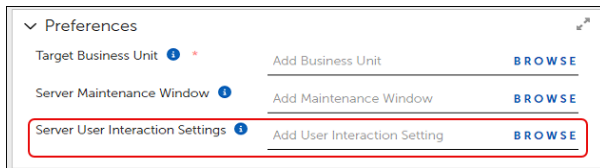
This opens the **Add Maintenance Window** dialog.



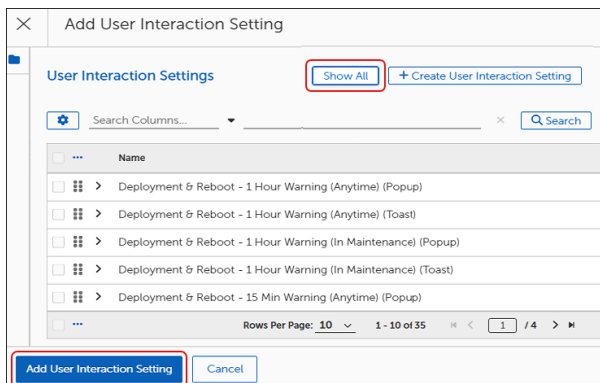
2. Select **Show All** at the upper right to view the available Maintenance Window settings.
3. Select the checkbox aligned with the setting you want to use. To create a new Maintenance Window setting, see [Maintenance Windows](#), then return and repeat this step.
4. Select **Add Maintenance Window**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



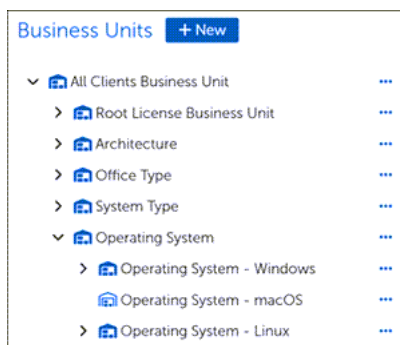
2. Select **Show All** at the upper-right corner to view the available options, and then select the checkbox aligned with the options you want to use. To create a new setting, see [User Interaction Settings](#), then return and repeat this step.
3. Select **Add User Interaction Setting** on the lower-left 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 manage notifications, approvals, and deployments using Rollout Processes. Each Business Unit can have its own unique settings and policies that apply to its member devices. These settings include rollouts, interaction settings, and more.

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



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



IMPORTANT

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

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

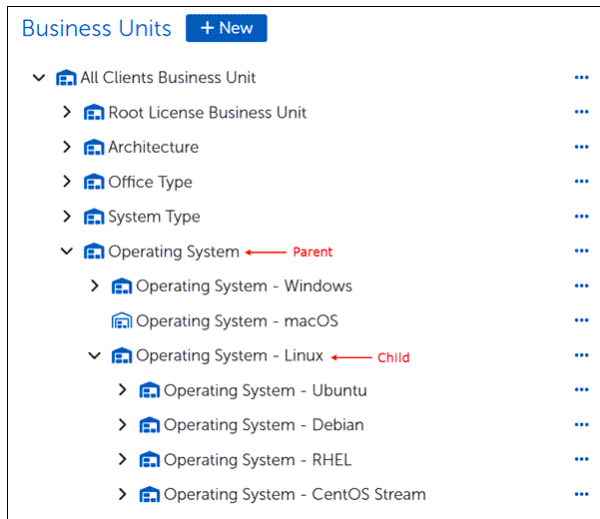
Parent and Child Business Units

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

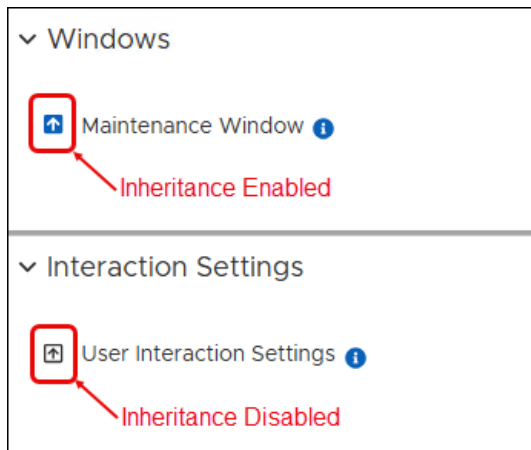


TIP

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



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

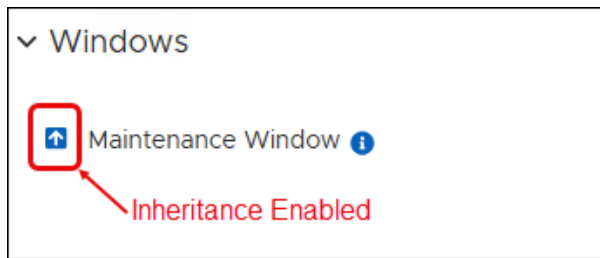


The hierarchical nature of Business Units allows a child Business Unit to inherit settings from its parent. An up-arrow with a blue background preceding a setting or process shows an inherited setting.

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

Managing Inheritance Settings

In OneSite Patch inheritance defaults to Enabled.



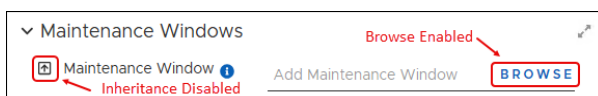
IMPORTANT

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

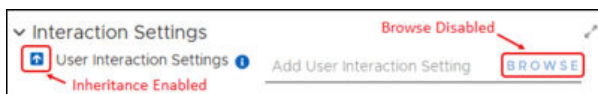
Enable Inheritance

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

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



2. Select the up-arrow icon to enable inheritance



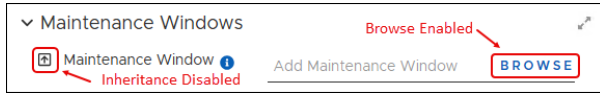
Disable Inheritance

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

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



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



Organizing the Business Unit Hierarchy

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

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

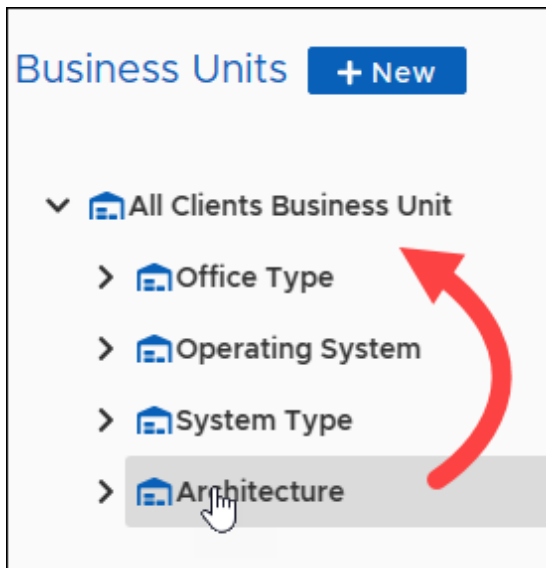
Best Practices when Changing Priorities

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

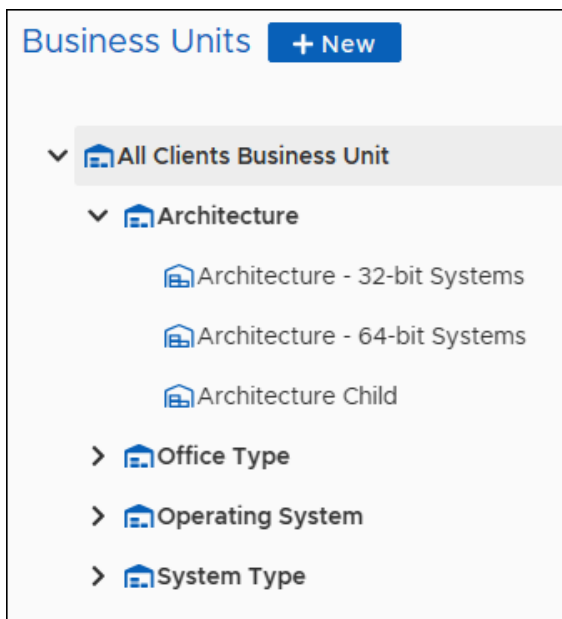
- **Priority:** Do the settings and desired state of the new priority Business Unit match your expectations for the moved Business Unit?
- **Membership:** Are the devices in the moved Business Unit compatible with the new priority Business Unit?
- **Inheritance:** Are the inheritance settings for the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

Change the Order of the Hierarchy

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



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



Creating a Business Unit

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

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

Open and Save a Business Unit Template

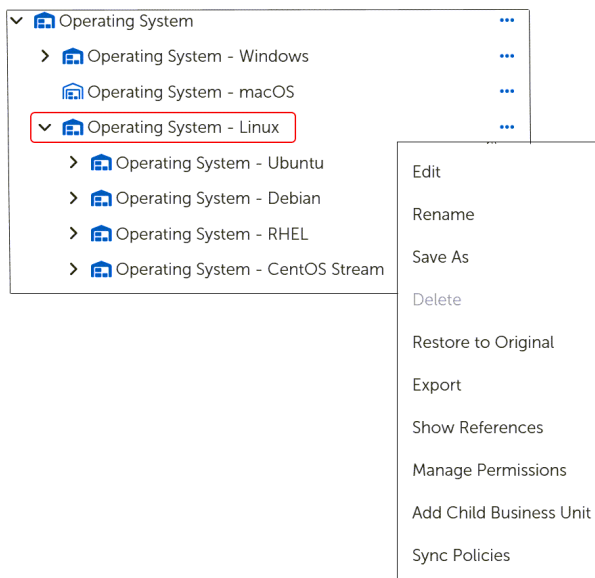
Except for Business Units provided for Root, you can copy the default templates and save them with new details or create a new Business Unit.



IMPORTANT

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

1. Mouse over or select **Business Units** in the left pane of the [Patch Dashboard](#), and then select **Business Units**.
2. Select the right arrow to the left of any folder to expand the list of available templates.
3. Select the **ellipses ...** next to the object you want to open, and then select **Save As**.



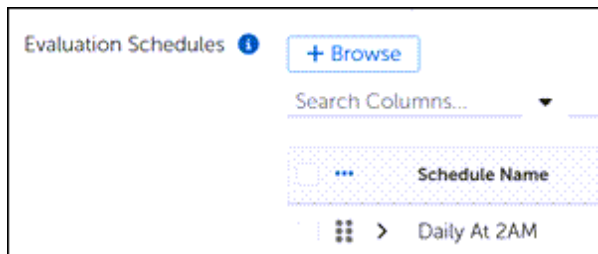
4. Save the template with a new title:
 - a. Select **More** in the upper-left of the dialog, and then select **Save As**.
 - b. Enter a new name for the template, and then select **Save as** on the lower-left of the dialog. This returns you to a copy of the template with the new name.
 - c. Enter a detailed **Description** of the process covered in this template, or leave the prepopulated description. Add a character to enable the Save button, and then select **Save** on the upper-left of the dialog.
5. Select **Save**. When you have finished modifying your new template, you can drag and drop it onto the folder you created (see [Patch Object Management](#)).

Add Evaluation Schedules to a Business Unit

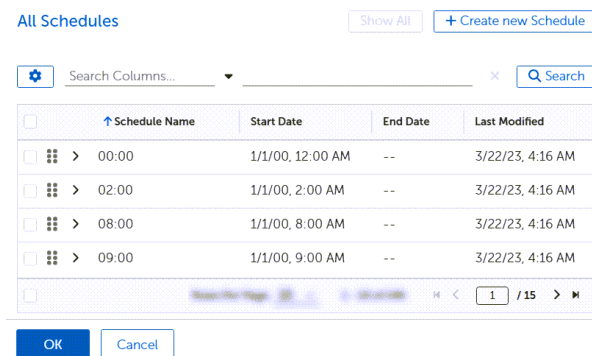
For Business Units with dynamic membership that may change over time, evaluation schedules determine when to check the membership of a Business Unit. Dynamic membership can occur based on Location or Sensor scopes, where a device moves between locations or Sensor results change over time.

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

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



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



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

Configure Business Unit Scopes

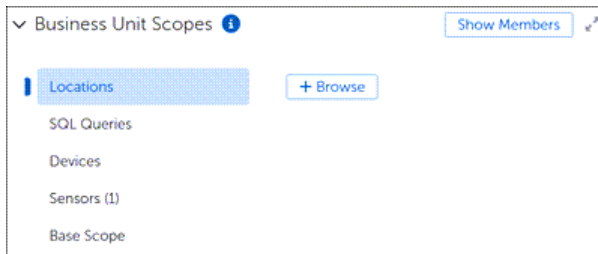
Business Unit Scopes define the rules used to find and include devices in a named Business Unit. Adaptiva supports using one or more scopes to create a Business Unit.



TIP

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

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



Add Locations

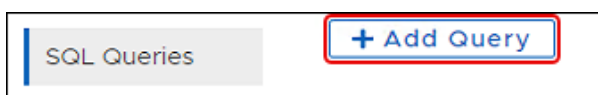
Use this option to define the Business Unit based on the location of devices. For example, you might want this Business Unit to include all devices in an office located in Chicago.

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

Add SQL Queries

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

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



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

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 AdaptiveClientID from a_adaptivaclientdata where machineame 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 lower-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**

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

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

Add Devices

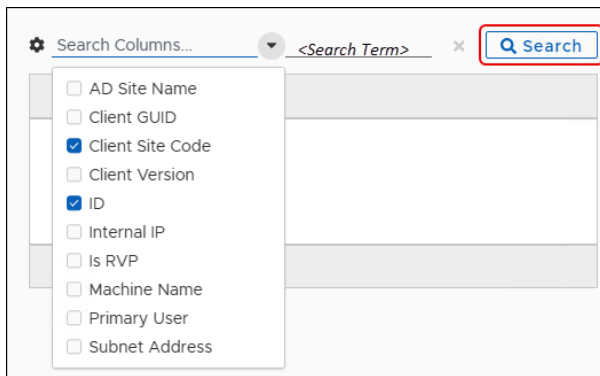
Choose one or more individual devices as members of this Business Unit.



IMPORTANT

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

1. Select **Devices** from **Business Unit Scopes**, and then select **+Browse**.
2. Use **Search** to define one or more search details you want to use to locate specific Client devices.
3. Enter your search term, and then select **Search**.



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

Add Sensors

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



TIP

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

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

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



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



NOTE

A red asterisk (*) indicates a required field.

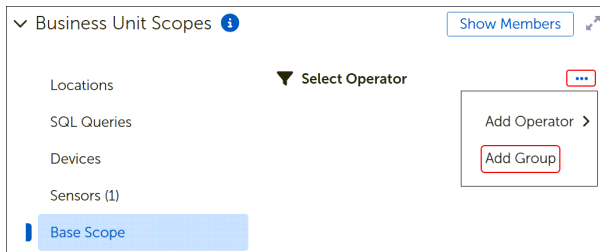
3. Select **Browse** to choose a Sensor.
4. Select the **ellipsis (...)** next to **Sensors**, and then select **Expand All** to view the list of available Sensor settings.

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

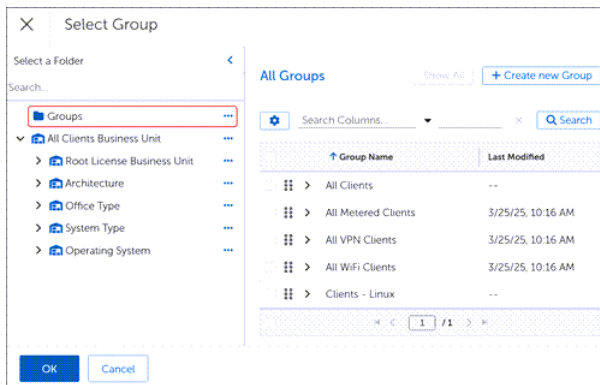
Set Base Scope

Use Base Scope settings to add or exclude devices in a Business Unit based groups, CM collections, or other business units. Using Operators and Conditions, you can extend Business Unit membership and group multiple devices together.

1. Select **Base Scope** from **Business Unit Scopes**.
2. Select the ellipsis (...) to the right of **Select Operator**, and then select **Add Group**.



3. Select the container type you want to use.

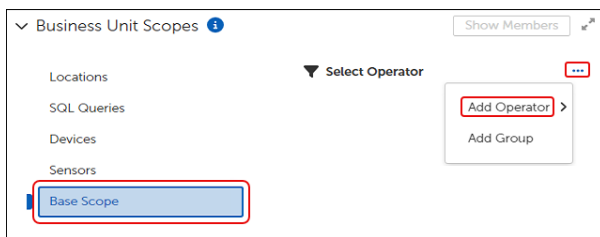


4. Select a **CM collection, Business Unit, or Group** to add to the **Base Scope**.
5. Select **OK** on the lower-left of the dialog. The entry under **Business Unit Scopes** shows the **AND** operator and the item you chose.

Add Multiple Groups or Business Units

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

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

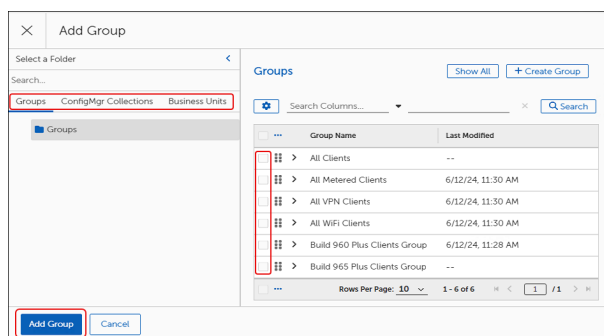


2. Select the ellipsis (...) to the right of **Select Operator** (or any existing Operator), and then select **Add Operator**.

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



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



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

Remove Groups or Operators

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

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

Add User Interaction Settings

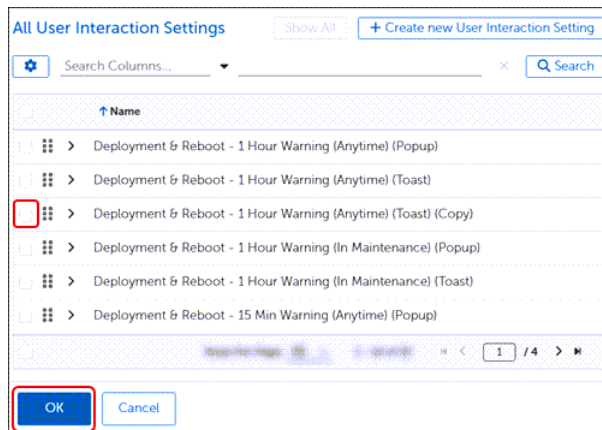
Choose a User Interaction Setting for the devices in this Business Unit. These settings control how end users are notified about upcoming installations and reboots. For more information about User Interaction Settings, see [User Interaction Settings](#).

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



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

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

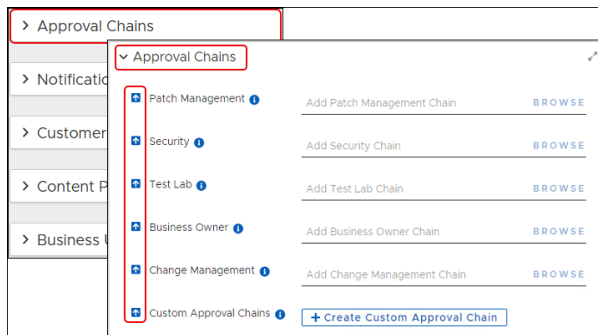


Add Approval Chains to a Business Unit

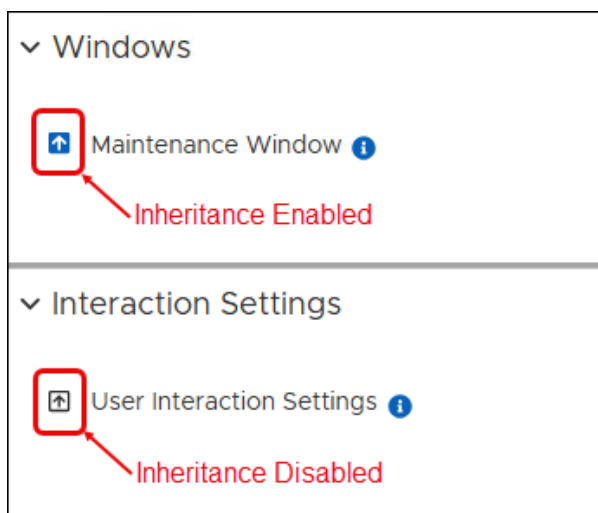
Adding Approval Chains to a Business Unit is an advanced feature. The **Approval Chains** fields allow advanced users to specify details for use in customized Patching Strategies, Deployment Chains, or Business Units when necessary to achieve different results.

1. In an open Business Unit template, select **Approval Chains**. This opens the **Approval Chains** workspace.

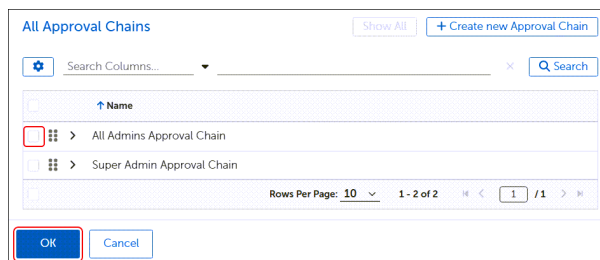
- Business Units inherit these settings from a parent by default. For more information about inheritance, see [Parent and Child Business Units](#)



- Disable inheritance to enable Browse, and then assign a different Approval Chain to a setting.



2. Select **Browse** next to the type of Approval chain you want to add (Product Owner, Patch Management, Security, and so on).
3. Select an **Approval Chain** from the **Approval Chains** table. This example uses an All Admins Approval Chain.



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

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

Customer Extension Data

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

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

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

Add a Notification Chain

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

1. Expand the **Notifications** box in an open object template to show the available configuration options.
2. Select **Browse** next to **Notification Chain**. This opens the **Notifications Chain** dialog.

Name	Actions
All Admins Notification Chain	...
Super Admin Notification Chain	...

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

Content Prestaging Settings in Object Templates

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

To configure these settings, see [Content Prestaging Settings](#).

Verify Business Unit Members

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



IMPORTANT

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

Create a Lab Business Unit

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

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

Create a Custom Lab Business Unit

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

Maintenance Windows

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

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

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

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

Schedules\Patching Schedules\Window Start

Open and Save a Maintenance Window Template

1. Select **Maintenance Windows** in the left navigation menu of the [Patch Dashboard](#).



IMPORTANT

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

2. Select **Show All** to display the available Maintenance Window settings. If Show All is grayed out, the table includes all available settings.
3. Select the **Name** of an existing template to open it, and then save the template with a new name:
 - a. Select **More** in the upper-left of the dialog, and then select **Save As**.
 - b. Enter a new name for the template, and then select **Save as** on the lower-left of the dialog. This returns you to a copy of the template with the new name.
 - c. Enter a detailed **Description** of the process covered in this template, or leave the prepopulated description. Add a character to enable the Save button, and then select **Save** on the upper-left of the dialog.

Dynamic Settings

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

Add Dynamic Detection Workflow (Optional)

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

Maintenance Windows by Urgency

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

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

Apply a Maintenance Window to All Urgencies

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

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

Maintenance Windows by Urgency

Apply to All Urgencies ☒ Enabled

All Urgencies Windows

Start Time Schedule	Duration	Actions
02:00	2h	...

Rows Per Page: 10 1 - 1 of 1

All Urgencies Override Duration: 0 Hours 0 Minutes 0 Seconds

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

All Urgencies Windows

Start Time Schedule	Duration	Actions
<input type="checkbox"/> 02:00	2h	...
<input type="checkbox"/> 09:00	1h 2m 3s	...
<input type="checkbox"/> 12:00	6d 4h	...

Rows Per Page: 10 1 - 3 of 3

All Urgencies Override Duration: 0 Hours 0 Minutes 0 Seconds

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

These settings override any non-zero duration values set inn the Maintenance Window when the Maintenance Window fails to open for urgency level updates.
4. Enter the number of **Hours**, **Minutes**, or **Seconds** to wait after the Maintenance Window fails to open to override the Maintenance Window duration settings.

Save and Deploy the Maintenance Window

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

1. Complete the Maintenance Window configuration (see [Open and Save a Maintenance Window Template](#)).
2. Save your changes:

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

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

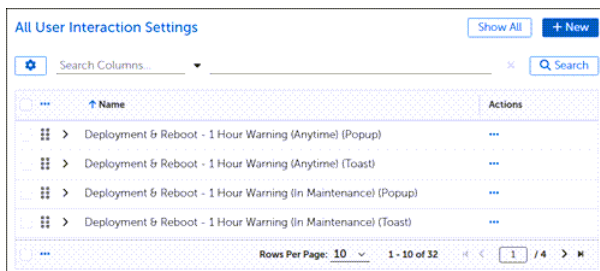


User Interaction Settings

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

Open and Save a User Interaction Template

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

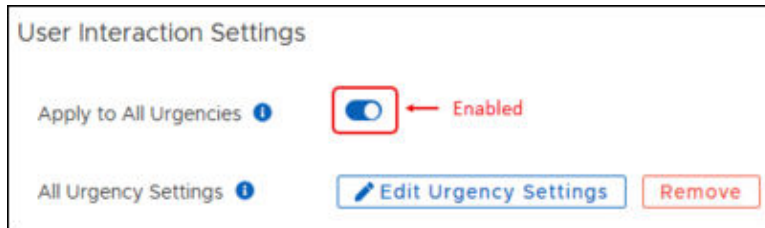


2. Select the Name of an existing template to open it. This example uses the Deployment & Reboot – 1 Hour Warning (Anytime)(Toast) template.
3. Save the template with a new name:
 - a. Select **More** in the upper-left of the dialog, and then select **Save As**.
 - b. Enter a new name for the template, and then select **Save as** on the lower-left of the dialog. This returns you to a copy of the template with the new name.
 - c. Enter a detailed **Description** of the process covered in this template, or leave the prepopulated description. Add a character to enable the Save button, and then select **Save** on the upper-left of the dialog.

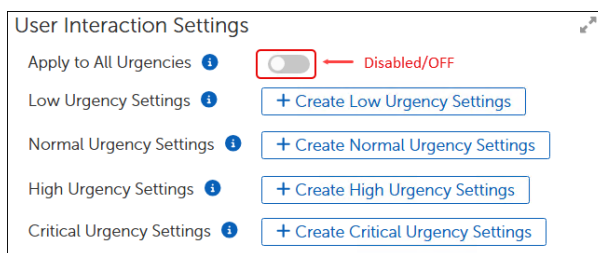
Choose Urgency Settings

1. Scroll down to **User Interaction Settings** in an [open User Interaction Settings](#) template:

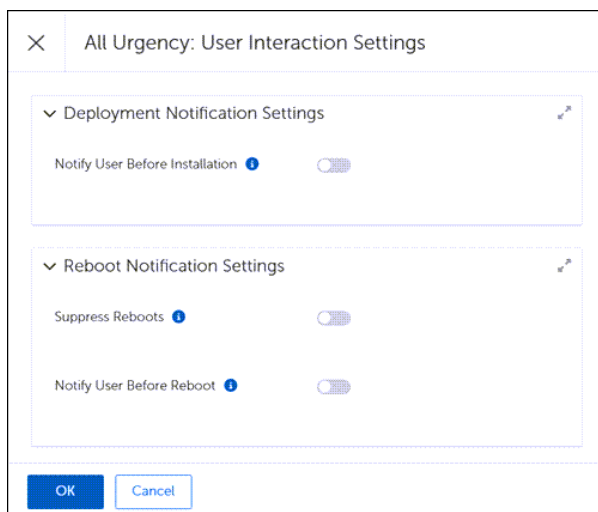
- When working from an existing template, these settings reflect the needs of the template you chose to modify. With **Apply to All Urgencies** enabled, you have the option to create a single set of urgency settings that apply to all urgency levels (Low, Normal, High, and Critical).



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



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



3. [Configure deployment notification settings.](#)

Configure Deployment Notification Settings

1. Select the toggle for **Notify User Before Installation** enable user notification when a deployment begins:

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

Reboot Notification Settings

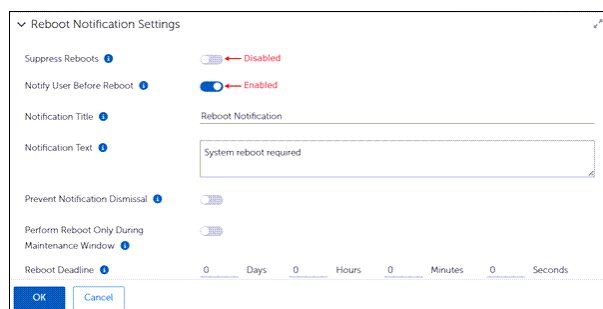
The Reboot Notification Settings in a [User Interaction Settings](#) dialog provides choices to Suppress Reboots and to Notify User Before Reboot.

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



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

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



Configure Reboot Settings

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

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



- Disable to allow reboot at any time.



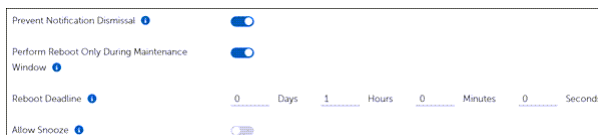
2. Select the **Prevent Notification Dismissal** toggle to enable or disable whether the client device user may dismiss the notification:
 - Enable to prevent the user from dismissing the notification.



- Disable to allow the user to dismiss the notification.



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



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

4. [Configure snooze settings.](#)

Managing Snooze Settings

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

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

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

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

Configure Snooze Settings

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

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

The screenshot shows the 'Allow Snooze' toggle set to 'Enabled' (indicated by a blue switch and a red arrow). Below the toggle are three input fields for duration settings: 'Maximum Snooze Duration' (0 Days, 8 Hours, 0 Minutes, 0 Seconds), 'Snooze Reminder' (0 Days, 6 Hours, 0 Minutes, 0 Seconds), and 'Snooze Durations' (0 Days, 0 Hours, 0 Minutes, 0 Seconds). A '+ Add' button is visible below the 'Snooze Durations' field.

- When enabled, you may define the timing of user interactions reboot notifications.
 - When disabled, the user receives no notification.
2. Define the Snooze settings:
 - a. **Maximum Snooze Duration:** This is the maximum amount of time the user may snooze the reboot.
Enter the **Days, Hours, Minutes** or **Seconds** that define the **Maximum Snooze Duration** (defaults to 8 hours).
 - b. **Snooze Reminder** settings: Sets the amount of time between the notifications the user receives after the first snooze.
Enter the **Days, Hours, Minutes** or **Seconds** that define the **Snooze Reminder** gap (defaults to 6 hours).
 - c. **Snooze Duration.** Leave settings at zero (0) to use the default settings.
Enter the **Days, Hours, Minutes** or **Seconds** that define the **Snooze Duration** (defaults to 4 hours, 2 hours, 1 hour, 15 minutes).

The screenshot shows the 'Snooze Durations' list with five rows. Each row has input fields for Days, Hours, Minutes, and Seconds, followed by a red 'x' icon. The first four rows are pre-filled with values: (0 Days, 4 Hours, 0 Minutes, 0 Seconds), (0 Days, 2 Hours, 0 Minutes, 0 Seconds), (0 Days, 1 Hour, 0 Minutes, 0 Seconds), and (0 Days, 0 Hours, 15 Minutes, 0 Seconds). The fifth row is empty (0 Days, 0 Hours, 0 Minutes, 0 Seconds). A '+ Add' button is visible at the bottom left of the list.

3. Select **+Add** to create additional **Snooze Duration** settings. You may add up to 5 additional lines.

4. Select **OK** on the bottom left corner to return to the User Interaction Settings workspace.

Save and Deploy User Interaction Settings

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

1. Complete the User Interaction configuration (see [User Interaction Settings](#)).
2. Save your changes:
Select **Save & Deploy** to save and deploy your configuration:
 - Select **Save & Deploy** to save and deploy your changes.
 - Select **Save** to save your changes without deploying. Be sure to return and **Deploy** the changes to make them available for use.



Customized Products

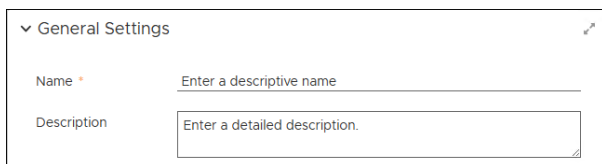
Software products and patches sometimes require user interaction when installing. Users enter details such as license information or request to show a menu at startup. Other default settings include auto update, or desktop shortcuts.

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

Manage Settings for Customized Products

Open and Save a Customized Product Template

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

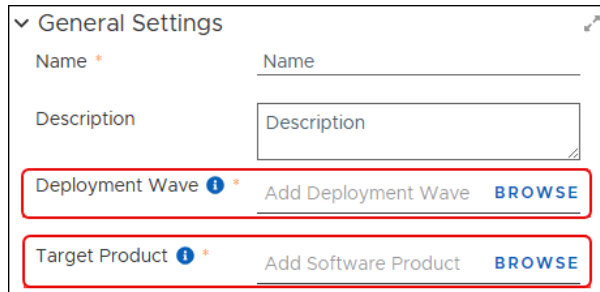
A screenshot of a 'General Settings' dialog box. It has a title bar with a dropdown arrow and a close button. Inside, there are two text input fields. The first is labeled 'Name' with a red asterisk and a placeholder 'Enter a descriptive name'. The second is labeled 'Description' with a placeholder 'Enter a detailed description.'.

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

Add a Deployment Wave to a Customized Product Template

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

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



General Settings

Name *

Description

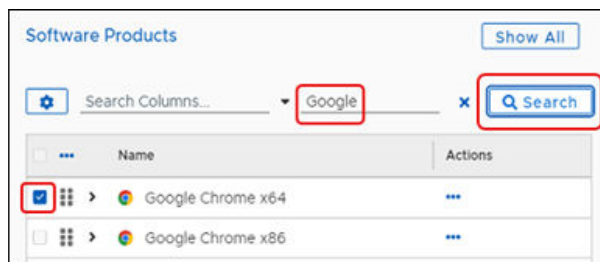
Deployment Wave ⓘ *

Target Product ⓘ *

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

Add a Target Product

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



Software Products

Search Columns...

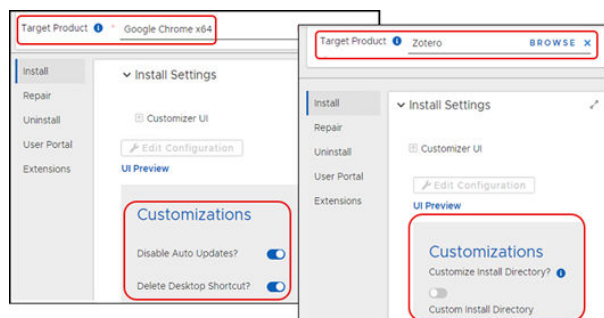
<input type="checkbox"/>	Name	Actions
<input checked="" type="checkbox"/>	Google Chrome x64	...
<input type="checkbox"/>	Google Chrome x86	...

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

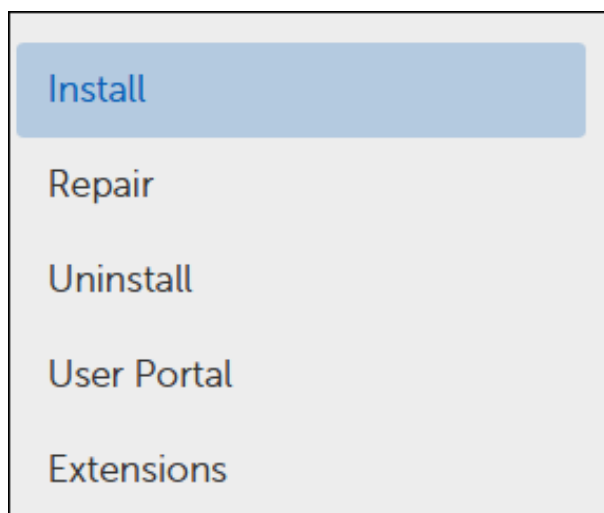
Configure Software Install Settings

1. Select **Install** in the left column of **Install Settings**.

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



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

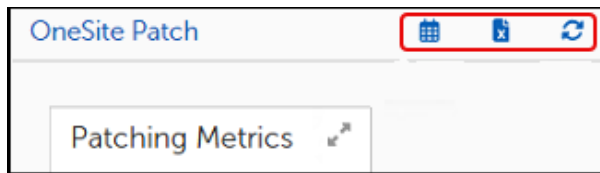


3. Select **Save** on the upper-left of the dialog to save your progress:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.
4. Select <-- **Back to Customized Products** above **General Settings**. The changes you have made take effect the next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

Navigating the OneSite Patch Dashboard

Date Settings, Export, and Refresh

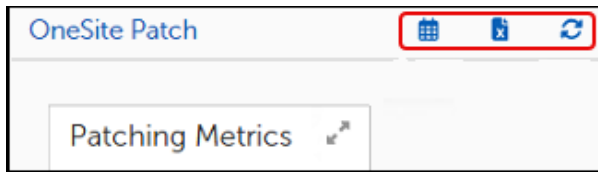
The three small icons (Calendar, Export and Refresh) on the upper right of the Home page and on any of the Patching Analytics pages (Overview, Products, Patches, or Devices) provide options to customize the date settings to a particular date range, choose some or all widgets on the page for exporting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



Set Dates for Status Views

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


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

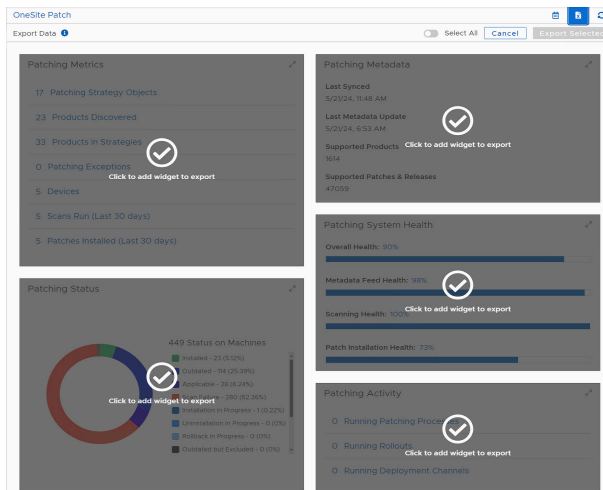


2. Enter the **starting and ending dates** for the range you want to view or use the calendar icon to the right of each date field to choose a date from the calendar.

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

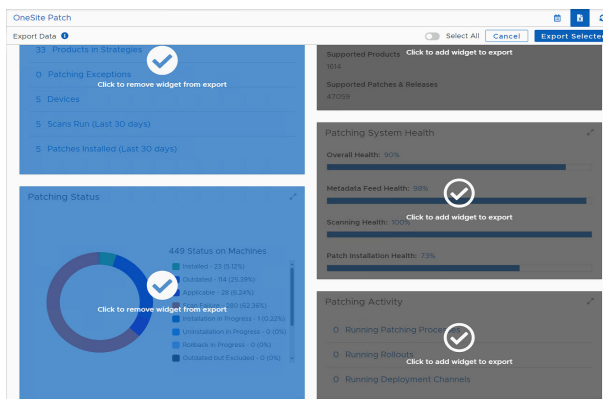
Export Widget Data

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




2. Choose which widgets to export:

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



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

Refresh the Status View

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

Patch Menu

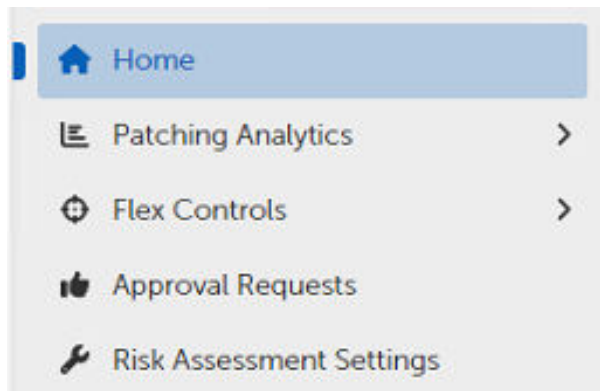
The left navigation menu lists the object available for configuring or monitoring in the OneSite Patch product. Those items with additional choices include a pop-out menu indicated by a right-angle bracket (>).

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

Home Menu

Home menu choices provide status information related to products, patches, devices, deployment, and approval requests, as well as access to settings for Risk Assessment and Flex Controls. Flex Controls contain tools that an administrator can use to monitor cycle operations, create patching exceptions, and pause or roll back patching strategies (see [Home Menu Object Descriptions](#)).

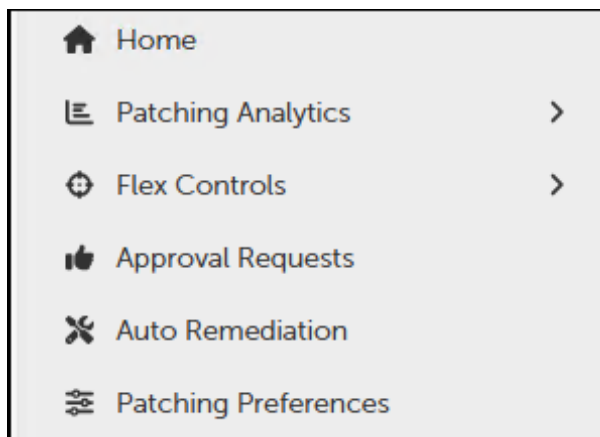
Administrators use this information to review performance and to help prioritize actions required to keep the environment updated, compliant, and risk free.



From any location within OneSite Patch, select **Home** to return to the Home page. For a description of Home page widgets, see [Home dashboard and Performance Widgets](#).

Patch Express Home Menu

The Home menu provides access to the status and statistical information you can use to analyze the performance and activities occurring in the estate by products, patches and devices. **Flex Controls**, **Auto Remediation**, and **Patching Preferences** provide configuration workspaces where you may customize specific functionality.



From any location within , click **Home** to return to the **Home** page. For a description of **Home** page widgets, see [Home Dashboard and Performance Widgets](#).

Home Menu Object Descriptions in Patch Express

Object	Purpose
Home	Opens the Home page to view the overall status, metric, and compliance for patching in your environment. See Dashboard and Performance Widgets .
Patching Analytics	Shows the status of patches and products in the environment. Change tabs to view metrics for Products, Patches, or Devices. See Patching Analytics Dashboards . Sub menus include Overview, Products, Patches, and Devices.
Flex Controls	Review and manage settings for Blocklisting, Exceptions, Global Pause, and Rollbacks. Review Patching Cycle statistics (Cycle Operations), and view both running and historic cycles for Patching, Deployment, and Rollout. For details on each selection, see Flex Controls
Approval Requests	View all approval requests and check the status of pending and completed requests. See Approval Requests .
Auto Remediation	Use this menu to enable and configure Auto Remediation details for security issues based on level of criticality (Critical, High, Medium, Low). Configure and test production deployment settings.
Patching Preferences	Create patching preferences based on target Business Unit including assignment of a Maintenance Window and User Interaction settings.

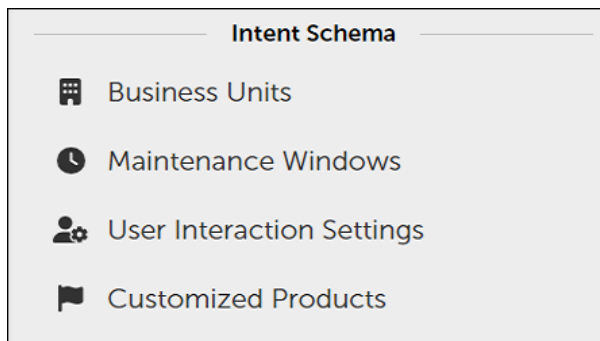
Integration Menu

The Integrations menu provides access to available integrations based on licensing.



Intent Schema Menu

The **Intent Schema Menu** refers to the menu items administrators use to customize and manage patching policies for Business Units.



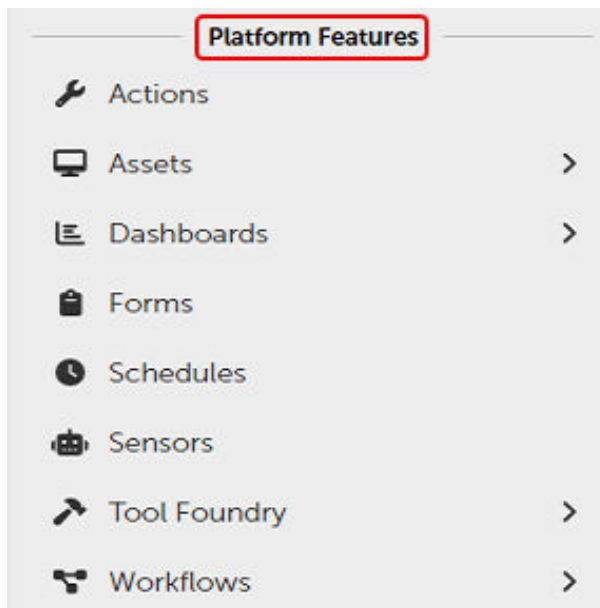
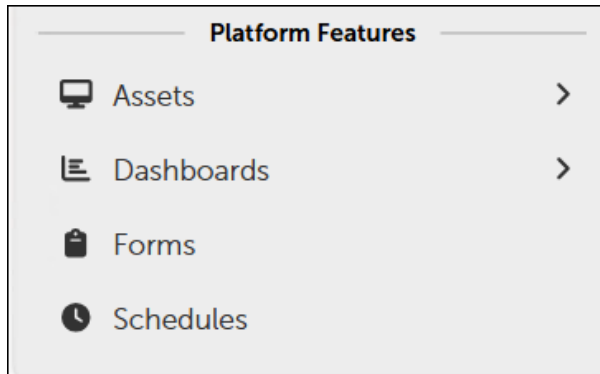
Intent Schema Object Descriptions

Object	Purpose
Business Units	Logically group and manage devices, settings, and other resources within a hierarchy. See Business Units
Maintenance Windows	Define maintenance and reboot windows. Primarily associated with Business Unit configurations. See Maintenance Windows .
User Interaction Settings	Control what the endpoint user sees and what options they have for interacting with patching notifications and required reboots. See User Interaction Settings .

Object	Purpose
Customized Products	Customization of installation for products with specific actions needed, such as license key entry or custom installation locations, before or after an installation. See Customized Products .

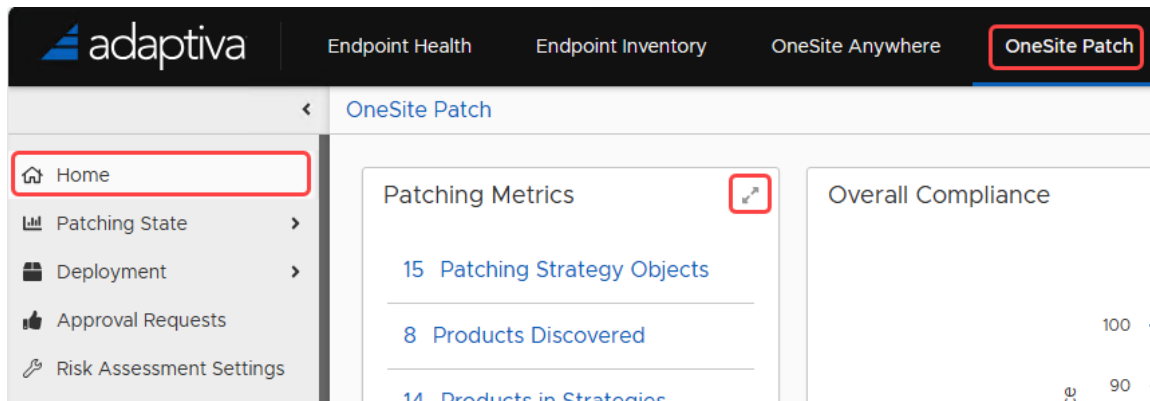
Platform Features Menu

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



Dashboard and Performance Widgets

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

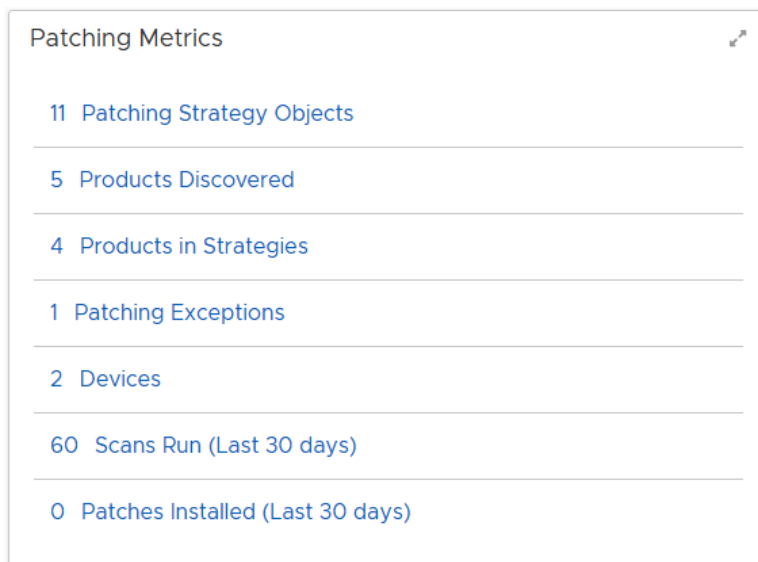


The layout of these widgets depends on the size of your computer monitor.

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

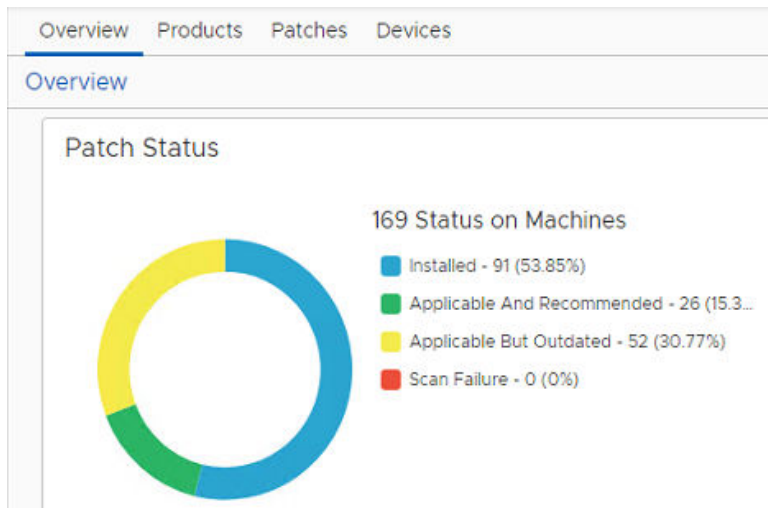
Patching Metrics

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



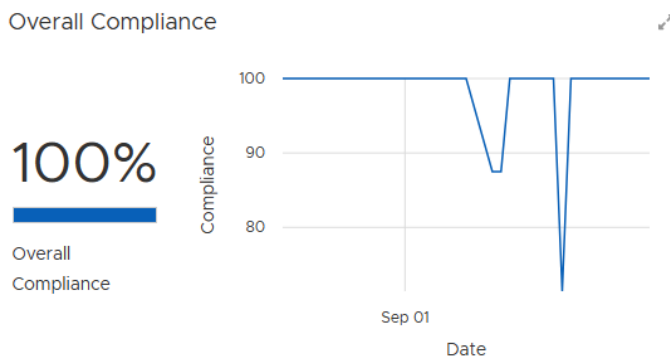
Patching Status

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



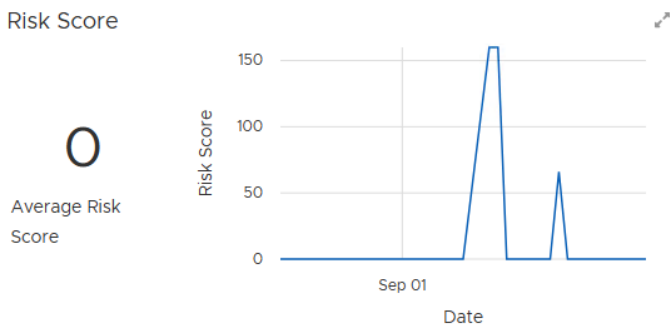
Overall Compliance

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



Risk Score

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



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

Patching Metadata

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

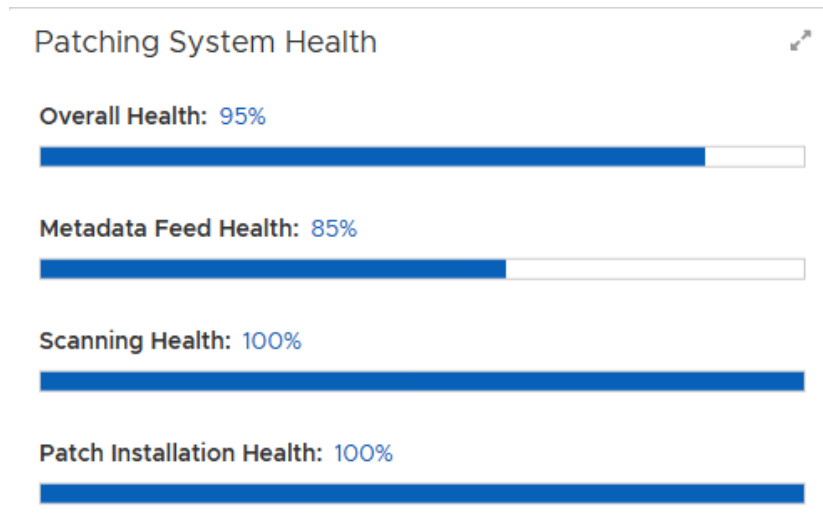
Patching Metadata

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 ...	0%	...
<input type="checkbox"/>	Microsoft Orca	0%	...
<input type="checkbox"/>	Microsoft Visual C++ 2015-2022 Redistribut...	0%	...
<input type="checkbox"/>	Microsoft Visual C++ 2015-2022 Redistribut...	0%	...
<input type="checkbox"/>	SQL Server Management Studio x64	0%	...
<input type="checkbox"/> ...	Rows Per Page: 1 - 5 of 5 < 1 / 1 >		

Top 5 Missing Patches

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

Top 5 Missing Patches	
No data provided	

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

Appendices

Software Products

OneSite Patch supports patching for multiple versions of products across licensed clients/endpoints. A dedicated team of metadata analysts constantly reviews and expands the Software Products Library (metadata catalog) with new products and new releases for existing products, covering most of the installed software within your environment.

Metadata Catalog

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

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

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

After confirming a successful update, the team creates, reviews, and approves the metadata before adding it to the metadata catalog. See [OneSite Patch 3rd Party App Catalog \(adaptiva.com\)](https://adaptiva.com/OneSitePatch3rdPartyAppCatalog) for more information.

Endpoint Scans

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

Request a Scan

1. From the Adaptiva Home menu in the left navigation panel, hover over **Patching Analytics**, and then select **Overview**, **Products**, **Patches**, or **Devices**.
2. Scroll down to the last table on the screen. The table name changes depending on the option you choose:
 - **Overview – Product Status** table: Actions include Scan Product and Reset Deployment Failures for Product.
 - **Products – Product Status** table: Actions include Scan Product and Reset Deployment Failures for Product.
 - **Patches – Patch Status** table: Actions include Scan Patch and Reset Deployment Failures for Patch.
 - **Devices – Device Status** table: Actions include Scan Product.
3. Select the **ellipsis (...)** in the **Actions** column for the product, overview, or device you want to scan.

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

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.

Request Scan

Scan All Clients ☒

Target Groups + Add Groups

Target Business Units + Add Business Units

Target Clients + Select Clients

Scan All Software ☐

Software + Add Software

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

1 / 1

OK 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`.