



Tenable Patch Management User Guide

Last Revised: August 28, 2025



Table of Contents

Welcome to the Tenable Patch Management Guide	28
Set Up the Patch Server	29
Prerequisites	29
Tenable Patch Server	29
Tenable Patch Server Account and Permission Settings	30
Communication Ports	32
Antivirus Exceptions	32
Excluding Folders and Processes	33
Creating Antivirus Folder Exclusions	33
Server and Client Folder Exclusions	33
Internet Access	33
Internet Access Requirements	33
Allow Access to Internet Destinations	34
Tenable Patch Server Installation Folder	35
Licensing Tenable Products	35
Security Certificate Options	35
CA Requirements	36
Self-signed Certificate Requirements	36
HTTP Communication	37
HTTP Communication Requirements	37
Adaptiva Database	37
Database Considerations	37
System Account	38



Domain Account	38
Database Read Only Account	38
Windows Authentication	39
SQL Server Database	39
Choosing the SQL Server Edition	40
SQL Server Requirements	40
SQL Server Express Edition Details	41
SQL Server Standard Edition Details	42
SQL Server Enterprise Edition Details	42
Database Creation	42
Create the Database in Same SQL Server	42
Install Clients	43
Software Requirements	43
On-Prem Supported Platforms and Distributions	43
Windows	44
Linux	44
Mac	44
Supported Browsers	45
Welcome to Tenable Patch Management Express	45
Use Copy From	46
Getting Started with Tenable Patch Management Express	49
Prerequisites	49
Supported Browsers	49
Logs for Server	50



Customer Support	50
Tenable Patch Management ExpressAdmin Portal	50
Log in to the Admin Portal	51
Licensing Products	52
Add a License Key	53
Target Collections for the Licensed Product	53
Dashboard	53
Access the Dashboard	54
Tenable Patch Management Express Setup Wizard	54
Welcome to Patch Express	55
Use Copy From	56
Select a Remediation Schedule	59
Enable Vulnerability Detection	60
Enable Patch Pre-staging	61
Configure Deployment Notifications	62
Configure Deployment Approval	64
Configure Test Deployment	68
Configure Test Approval	71
Complete Setup	74
Best Practices for Tenable Patch Express	74
Security	75
Access Security Settings	75
View Administrators	76
View Roles	76



Menu Objects for Tenable Patch Management Express	76
Patching Analytics Dashboards	77
Using Search in Tenable Patch Management Express	77
Patching Analytics Overview	77
Products View	78
Patches View	81
Devices View	83
Flex Controls	85
Blocklisting	86
Blocklist Settings	86
Managing Blocklist Notification Settings	87
View Blocklist Settings	87
Select a Notification Chain for Blocklisted Patches	88
Choose Communication Providers for Notification Chains	88
Cycle Operations	89
Patching Cycles	89
View the Running Patch Cycles	90
View Patching Cycle History	91
Deployment Cycles	92
View the Running Deployment Cycles	92
View Deployment Cycle History	93
Rollout Cycles	94
View the Running Rollout Cycles	94
View Rollout Cycle History	95



Patching Exceptions	95
Using Patching Exceptions	96
Create a Patching Exception	96
Set Override Details for Patch Exceptions	97
Set Last Allowed Patch Versions	98
Add Target Business Units for Patch Exceptions	99
Global Pause	100
Stop All Patching Activity Immediately	101
Resume All Paused Patching Activity Immediately	102
Pause Patching for Specific Objects	103
Pause Deployment of a Specific Software Product	105
Pause Deployment of a Specific Patch	108
Pause Specific Cycles	110
Pause a Patching Cycle	111
Pause a Deployment Cycle	113
Pause a Rollout Cycle	116
Pause Deployment to a Business Unit	118
Rollbacks Overview	119
Rollback	120
Create a Rollback	120
Edit a Rollback Template	123
Copy a Rollback	124
Customize Patching Rollback Table Settings	126
Delete a Rollback	128



Select All Rollbacks	130
Bulk Delete Rollbacks	130
Export Rollbacks	132
Configure Object Export Settings	134
Show Rollback References	135
Rollback to Version	136
Create a Rollback to Version	137
Choose the Software Patch or Release Version to Roll Back From	139
Choose the Software Patch or Release Version to Roll Back To	139
Add Business Units for a Rollback to Version	140
Edit a Rollback to Version Template	141
Copy a Rollback to Version Template	143
Customize Patching Rollback Table Settings	144
Delete a Rollback to Version	146
Select All Rollback to Version Objects	148
Bulk Delete Rollback to Version	148
Export Rollback to Version	150
Configure Object Export Settings	152
Show Rollback to Version References	153
Approval Requests	154
Approve or Reject a Patch Request	155
Auto Remediation	155
Access Auto Remediation and Deployment Settings	156
Using Auto Remediation Settings	157



Enable Auto Remediation	158
Vulnerability Detection Source Settings	160
Production Deployment Settings for Auto Remediation	160
Test Deployment Settings for Auto Remediation	161
Verify that Auto Remediation Works as Expected	162
Patching Preferences	162
Using Patching Preferences	162
Access Patching Preferences	163
Create a New Patching Preference	164
Add a Target Business Unit	164
Select a Server Maintenance Window	165
Select Server User Interaction Settings	167
Business Units	168
Understanding Business Units	168
Parent and Child Business Units	169
Managing Inheritance Settings	170
Enable Inheritance	170
Disable Inheritance	171
Organizing the Business Unit Hierarchy	171
Best Practices when Changing Priorities	172
Change the Order of the Hierarchy	172
Creating a Business Unit	173
Open and Save a Business Unit Template	174
Add Evaluation Schedules to a Business Unit	176



Configure Business Unit Scopes	178
Add Locations	179
Add SQL Queries	179
Add Devices	180
Add Sensors	181
Set Base Scope	183
Add Multiple Groups or Business Units	184
Remove Groups or Operators	186
Add Approval Chains to a Business Unit	186
Customer Extension Data	188
Add a Notification Chain	189
Content Prestaging Settings in Object Templates	189
Verify Business Unit Members	190
Create a Lab Business Unit	190
Create a Custom Lab Business Unit	190
Maintenance Windows	190
Open and Save a Maintenance Window Template	191
Dynamic Settings	191
Add Dynamic Detection Workflow (Optional)	192
Maintenance Windows by Urgency	192
Apply a Maintenance Window to All Urgencies	192
Save and Deploy the Maintenance Window	193
User Interaction Settings	194
Open and Save a User Interaction Template	194



Choose Urgency Settings	195
Configure Deployment Notification Settings	196
Reboot Notification Settings	197
Configure Reboot Settings	198
Managing Snooze Settings	199
Configure Snooze Settings	199
Save and Deploy User Interaction Settings	201
Customized Products	201
Manage Settings for Customized Products	202
Open and Save a Customized Product Template	202
Add a Deployment Wave to a Customized Product Template	202
Add a Target Product	203
Configure Software Install Settings	204
Navigating the Tenable Patch Management Express Dashboard	205
Date Settings, Export, and Refresh	205
Set Dates for Status Views	205
Export Widget Data	206
Refresh the Status View	208
Patch Menus	208
Home Menu	208
Home Menu Object Descriptions	209
Tenable Patch Management Express Home Menu	210
Home Menu Object Descriptions in Patch Express	210
Intent Schema Menu	211



Intent Schema Object Descriptions	211
Platform Features Menu	212
Tenable Patch Management ExpressDashboard and Performance Widgets	212
Patching Metrics	213
Patching Status	213
Overall Compliance	214
Risk Score	214
Patching Metadata	215
Patching System Health	215
Patching Activity	215
Top 5 Non-Compliant Products	216
Top 5 Missing Patches	216
Appendices	217
Software Products	217
Metadata Catalog	217
Endpoint Scans	218
Request a Scan	218
Tenable Patch Management Enterprise	221
Bots - Patch Deployment and Notification Bots	225
Deployment Bots	225
Patch Deployment Bot Template Naming Conventions	225
Descriptions of Bot Settings	226
Open and Save a Patch Deployment Bot Template	227
Patch Filter Conditions	228



Edit or Remove Existing Patch Filter Conditions	229
Add Patch Filter Conditions	230
Set and Change Patch Filter Conditions	231
Add or Remove an Operator	231
Change an Operator	232
Add an Operating Condition	233
Filter Out Specific Patches by Product ID	234
Preview Filtered Patches	236
Preview Software Filtered by Conditions	236
Preview Software Filtered by a Strategy	237
Configure Bot Settings	237
Select Deployment Settings	237
Business Units for Bot Deployment Settings	238
Use a Custom Deployment Bot Workflow	240
Notification Bots	241
Patch Notification Bot Template Naming Conventions	242
Creating Notification Bots	242
Open and Save a Patch Notification Bot Template	242
Create an Output Expression	243
Configure Notification Bot Settings	243
View a Staged Patching Strategy	244
Communication Providers	245
Using Communication Providers	246
Open and Save a Communication Provider Template	246



Set Communication Provider Properties	246
Patching Processes	247
Creating Patching Processes	248
Patching Process Templates	248
Immediate Deployment, No Phasing, Initial Patch Manager Approval	248
Immediate Deployment, No Approvals Needed	248
Phased Deployment Processes, Approval Required	248
Content Prestaging Settings	249
Defining Content Prestaging Settings	249
Set Content Prestaging Settings	250
Enable Client Content Pull	251
Enable Server Content Push	251
Start the Patching Strategy Manually	252
New in this Tenable Patch Management Release	253
Getting Started with Tenable Patch Management	253
Prerequisites	254
Supported Platforms and Distributions	254
Supported Browsers	255
Logs for Server and Client	255
Customer Support	256
Tenable Patch Management Admin Portal	256
Log in to the Admin Portal	256
Resolve Mozilla Firefox Active Directory Login Issue	258
Licensing Tenable Patch Management	259



Add a License Key	259
Target Collections for the Licensed Product	260
Patch Management Dashboard	261
Access the Patch Management Dashboard	261
Administrators and Roles	261
Access Security Settings	261
View Administrators	262
Create a New Administrator	262
Create a Microsoft Teams Webhook URL	265
View Roles	265
Create a New Role	266
Business Units	269
Understanding Business Units	269
Parent and Child Business Units	270
Managing Inheritance Settings	272
Enable Inheritance	272
Disable Inheritance	272
Organizing the Business Unit Hierarchy	273
Best Practices when Changing Priorities	273
Change the Order of the Hierarchy	274
Creating a Business Unit	275
Open and Save a Business Unit Template	275
Add Evaluation Schedules to a Business Unit	277
Configure Business Unit Scopes	279



Add Locations	280
Add SQL Queries	280
Add Devices	281
Add Sensors	282
Set Base Scope	284
Add Multiple Groups or Business Units	285
Remove Groups or Operators	287
Maintenance Windows in Business Units	287
Add User Interaction Settings	288
Add Approval Chains to a Business Unit	289
Customer Extension Data	291
Add a Notification Chain	292
Content Prestaging Settings in Object Templates	293
Verify Business Unit Members	293
Create a Lab Business Unit	293
Create a Custom Lab Business Unit	293
Patching Analytics Dashboards	294
Using Search in Tenable Patch Management	294
Patching Analytics Overview	294
Products View	295
Patches View	298
Devices View	301
Flex Controls	303
Blocklisting	304



Blocklist Settings	304
Managing Blocklist Notification Settings	305
View Blocklist Settings	305
Select a Notification Chain for Blocklisted Patches	306
Choose Communication Providers for Notification Chains	307
Cycle Operations	307
Patching Cycles	308
View the Running Patch Cycles	308
View Patching Cycle History	309
Deployment Cycles	310
View the Running Deployment Cycles	310
View Deployment Cycle History	311
Rollout Cycles	312
View the Running Rollout Cycles	312
View Rollout Cycle History	313
Patching Exceptions	314
Using Patching Exceptions	314
Create a Patching Exception	315
Set Override Details for Patch Exceptions	315
Set Last Allowed Patch Versions	317
Add Target Business Units for Patch Exceptions	318
Global Pause	319
Stop All Patching Activity Immediately	319
Resume All Paused Patching Activity Immediately	321



Pause Patching for Specific Objects	322
Pause Deployment of a Specific Software Product	323
Pause Deployment of a Specific Patch	326
Pause Specific Cycles	329
Pause a Patching Cycle	330
Pause a Deployment Cycle	332
Pause a Rollout Cycle	335
Pause Deployment to a Business Unit	338
Rollbacks Overview	340
Rollback	340
Create a Rollback	340
Edit a Rollback Template	343
Copy a Rollback	345
Customize Patching Rollback Table Settings	346
Delete a Rollback	348
Select All Rollbacks	350
Bulk Delete Rollbacks	350
Export Rollbacks	352
Configure Object Export Settings	354
Show Rollback References	355
Rollback to Version	357
Create a Rollback to Version	357
Choose the Software Patch or Release Version to Roll Back From	359
Choose the Software Patch or Release Version to Roll Back To	360



Add Business Units for a Rollback to Version	361
Edit a Rollback to Version Template	362
Copy a Rollback to Version Template	364
Customize Patching Rollback Table Settings	366
Delete a Rollback to Version	367
Select All Rollback to Version Objects	369
Bulk Delete Rollback to Version	369
Export Rollback to Version	371
Configure Object Export Settings	373
Show Rollback to Version References	374
Patching Strategies	376
Purpose of a Patching Strategy	376
View built-in Patching Strategies	377
Appendices	377
Software Products	378
Metadata Catalog	378
Endpoint Scans	378
Request a Scan	378
Menu Objects for Tenable Patch Management	380
Patch Content	380
Customer Extension Data	381
Deployment Channels and Deployment Channel Processes	381
Deployment Channels	382
Understanding Channel Merging Rules	382



Creating a Deployment Channel	382
Open and Save a Deployment Channel Template	382
Deployment Process Settings	383
Add or Change a Deployment Process Schedule	384
Add or Change a Deployment Channel Process	385
Deployment Control	386
Enable Deployment Control	386
Disable Deployment Control	387
Approval Chains	388
Add an Approval Chain	388
Notifications	389
Add a Notification Chain	389
Create Notification Settings	390
Set Notification Urgency	390
Add Execution Schedules	391
Enable Notifications for Patching Strategy and Business Unit Chains	392
Choose a Notification Cycle Workflow	392
Set the Time Limit	393
Add Patch Notification Bots	394
Create Channel Merging Rules	394
Content Prestaging Settings	395
Set Content Prestaging Settings	395
Enable Client Content Pull	396
Enable Server Content Push	396



Customer Extension Data	397
Deployment Channel Processes	398
Creating Deployment Channel Processes	398
Integrate Tenable Vulnerability Manager	398
Minimum User Role Requirements for APIs	398
Add Tenable Access Settings to Tenable Patch Management	399
Configure Tenable Vulnerability Management Settings	400
Configure Tenable Security Center Settings	401
Administrators and Roles	403
Access Security Settings	403
View Administrators	403
Create a New Administrator	403
Create a Microsoft Teams Webhook URL	406
View Roles	406
Create a New Role	407
User Interaction Settings	410
Open and Save a User Interaction Template	410
Choose Urgency Settings	411
Configure Deployment Notification Settings	413
Reboot Notification Settings	414
Configure Reboot Settings	415
Managing Snooze Settings	416
Configure Snooze Settings	417
Save and Deploy User Interaction Settings	418



Rollout Processes	419
Including Rollouts in Business Units	419
Business Units and Rollout Processes	420
Creating a Patching Strategy	420
Open and Save a Patching Strategy Template	420
Managing Software Product Selections	421
Include All Software Products	422
Include Specific Software Products	422
Exclude Products from a Patching Strategy	423
Include or Exclude Platforms in a Patching Strategy	424
Manage Trigger Metadata Properties	425
View All Trigger Metadata Properties	426
Select from all Trigger Properties	426
Select Only Windows Defender Antivirus Trigger Properties	427
Select Only Tenable Trigger Properties	428
Remove Trigger Metadata Properties	428
Deployment Settings	429
Add a Deployment Wave	429
Deployment Bot Runtime Settings	431
Create Deployment Bot Runtime Scenarios	431
Add a Patch Deployment Bot (Required)	432
Add a Patching Process (Required)	433
Add a Deployment Channel (Optional)	434
Add Business Units (Optional)	434



Set the Patching Process Runtime	436
Present Patches to the First Matching Deployment Bot	438
Add Approval Chains to a Patching Strategy	438
Managing Notification Settings	440
Add a Notification Chain	440
Add Patch Notification Bots	441
Create Notification Settings	442
Set Notification Urgency	442
Add Execution Schedules	443
Enable Notifications for Patching Strategy and Business Unit Chains	444
Choose a Notification Cycle Workflow	444
Set the Time Limit	445
Customer Extension Data	446
Content Prestaging Settings	446
Defining Content Prestaging Settings	447
Set Content Prestaging Settings	448
Enable Client Content Pull	448
Enable Server Content Push	449
Business Unit Addition Settings	450
Business Unit Addition Settings in Patching Strategies	450
Configure Business Unit Addition Settings	451
Select a Business Unit	451
Select a Patching Process	452
Enable the Patching Strategy	452



Maintenance Windows	453
Open and Save a Maintenance Window Template	453
Dynamic Settings	454
Add Dynamic Detection Workflow (Optional)	454
Maintenance Windows by Urgency	454
Apply a Maintenance Window to All Urgencies	455
Save and Deploy the Maintenance Window	456
Customized Products	457
Manage Settings for Customized Products	457
Open and Save a Customized Product Template	457
Add a Deployment Wave to a Customized Product Template	457
Add a Target Product	458
Configure Software Install Settings	459
Deployment Waves	460
Using Deployment Waves	460
Open and Save a Deployment Wave Template	460
Add a Deployment Wave Entry	461
Create a Wave Entry	462
Edit or Remove a Wave Entry	463
Chains	463
Approval Chains	464
Using Approval Chains	464
Open and Save an Approval Chain Template	464
Managing Approval Chain Settings	465



Enable or Disable Automatic Approval of Timed Out Patches	466
Enable or Disable Reapproval for Modifications after Approval	467
Create an Approval Layer	467
Add and Order Approval Roles	468
Add Approval Roles to an Approval Layer	469
Set Unanimous Approval or Number of Approvals Needed	471
Add Backup Roles to an Approval Layer	472
Set Reminder Intervals	473
Set Approval Timeouts	474
Add Communication Providers to an Approval Layer	475
Managing Approval Settings in Object Templates	476
Add Approval Chains to a Patching Strategy	476
Add Approval Chains to a Business Unit	478
Notification Chains	480
Using Notification Chains	480
Open and Save a Notification Chain Template	481
Manage Notification Chain Settings	481
Add Roles to Notify	482
Managing Notification Settings	483
Add a Notification Chain	483
Add Patch Notification Bots	484
Create Notification Settings	484
Set Notification Urgency	484
Add Execution Schedules	485



Enable Notifications for Patching Strategy and Business Unit Chains	486
Choose a Notification Cycle Workflow	487
Set the Time Limit	487
Tenable Patch Management Enterprise	488
Organize New Patch Objects	492
Create a New Folder for Objects	492
Move an Object Template Between Folders	494
Navigating the Tenable Patch Management Dashboard	495
Date Settings, Export, and Refresh	495
Set Dates for Status Views	495
Export Widget Data	496
Refresh the Status View	498
Tenable Patch Management Patch Menus	498
Home Menu	498
Home Menu Object Descriptions	499
Patch Express Home Menu	500
Home Menu Object Descriptions in Patch Express	500
Integration Menu	501
Intent Schema Menu	501
Intent Schema Object Descriptions	502
Platform Features Menu	502
Tenable Patch Management Dashboard and Performance Widgets	503
Patching Metrics	503
Patching Status	504



Overall Compliance	504
Risk Score	505
Patching Metadata	505
Patching System Health	506
Patching Activity	506
Top 5 Non-Compliant Products	507
Top 5 Missing Patches	507
Introduction to Patching Strategies	508
Patching Strategy Use Case	508
Open and Save a Patching Strategy Template	508
Configure Deployment Settings	509
Add a Deployment Wave	510
Add Software Products	511
Enable the Patching Strategy	512
View a Staged Patching Strategy	513
Start the Patching Strategy Manually	515
Optional Objects in Patching Strategy Templates	515
Schedules	516
View Available Schedules	516
Create a Custom Schedule	518
Open and Save a Schedule Template	518
Create Schedule Settings	520
Set Start Time (Required) and End Time (Optional)	520
Set Repeat and Recurrence Intervals	521



Set Additional Time Constraints	522
Set Load Leveling Duration	523
Set Override Duration	523
Deploy Schedules	523
Delete a Schedule	524
Risk Assessment Settings	524
Risk Score Settings	525
Custom Risk Settings	525
Create Custom Product Criticalities	526
Create Custom Risk Scores	527
Approval Requests	528
Approve or Reject a Patch Request	528
Patching Strategy Templates	529
Patching Strategy Template Naming Conventions	530
Initial Patch Manager Approval Strategies	531
No Approval Strategies	532
Phase Approval Strategies	533



Welcome to the Tenable Patch Management Guide

Last Updated: August 28, 2025

Tenable Patch Management 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. This guide explains how to use Tenable Patch Management to patch vulnerabilities found by Tenable Vulnerability Management or Tenable Security Center, which integrate through an API.

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

Installing Tenable Patch Management

Tip: Tenable Patch Management is an on-premises product with two versions: *Enterprise* and *Express*. Use Express if your environment has fewer than 5,000 assets.

Download the Tenable Patch Management installation files from the [Tenable downloads page](#). For installation considerations and prerequisites, see the [Tenable Patch Management Installation Guide](#) and the [Tenable Patch Management Cross-platform Installation Guide](#).

Generating Tenable API Keys

To configure Tenable Patch Management, you need to enter your Tenable Vulnerability Management and/or Tenable Security Center API keys in the Tenable Admin Portal. The following topics explain how to generate API keys.

- [Generate API Keys for Tenable Vulnerability Management](#)
- [Generate API Keys for Tenable Security Center](#)

Using Tenable Patch Management



The following guides explain how to install and use Tenable Patch Management. For detailed workflows, see the Enterprise and Express guides.

- [Tenable Patch Management Quick Reference Guide](#)
- [Tenable Patch Management Enterprise User Guide](#)
- [Tenable Patch Management Express User Guide](#)

Set Up the Patch Server

Tenable Patch Management components include the Tenable Patch Server, the Tenable Patch Client, and the Admin Portal. After purchasing Tenable Patch Management, Tenable provides a compressed file that contains these components. The installation begins with the Tenable Patch Server followed by the Tenable Patch Client, also installed on the Tenable Patch Server. The Admin Portal facilitates the distribution and installation of the Client to the endpoint devices.

Prerequisites

Before installing the Tenable Patch Server, review the following details, complete the configuration requirements, and record information for use during the installation process.

Follow the sequence of prerequisites in the order presented.

Tenable Patch Server

The Tenable Patch Server is a key component of the Tenable Patch Management. The Tenable Patch Server provides administration services and policy deployments for products and connects with the Adaptiva Database, either locally or on a remote server.

The Tenable Patch Server hosts both the Server software and a Tenable Patch Client instance. Tenable Patch Management uses both components to facilitate and simplify complex endpoint management processes, including caching, peer communication, content acquisition, and result reporting.

Tenable Patch Server Requirements

The information in the table below details the minimum requirements for the Tenable Patch Server installation.



Component	Minimum Requirement
Operating System	Windows Server 2016 and later, Standard or Datacenter Edition
Processor	Single Quad-core Xeon Processor.
RAM	32 GB minimum
Storage	Installation files require 1.5 GB for the Tenable Patch Server, and the Tenable Patch Client. Logging requires 5 GB for default logging retention In addition to the general storage requirements, the Tenable Patch Server requires disk space to store published content in the Content Library. The estimated size is the same amount of storage used for the content source files, plus 20% for policy files and DIFF files.

Tenable Patch Server Installation Path Details

The Tenable Patch Server installation wizard uses the following default location for files and logs:

C:\Program Files\Tenable\PatchServer

Tenable strongly recommends changing the default drive location to something other than C:\ because the Content Library and log files grow over time, increasing space usage, which can and impact storage and performance on the C:\ drive.

You may also choose your own installation path. Record the installation path details for use during the Server installation.

The Server and Client installations create a system environment variable that points to the respective install locations. For example, %ADAPTIVASERVER% maps to the following location:

C:\Program Files\Tenable\PatchServer\

%ADAPTIVACLIENT% maps to the following location:

C:\Program Files\Tenable\PatchClient\

Tenable Patch Server Account and Permission Settings



The Tenable Patch Server installation requires an installation account with local administrator permissions on the chosen server. The installation creates a local service named `AdaptivaServer`, which runs under the Local System account by default.

If you use SQL Server Standard Edition or SQL Server Enterprise Edition, the installation account must also have `sysadmin` permissions on the SQL Server that hosts the database. For more information, see [Choosing the SQL Server Edition](#). You may change this permission after the installation. In addition, you may also change the service account from local system to a specified service account after installation.

Server	Account	Permissions
Tenable Patch Server	Installation account	System account add to Local Administrators group
	Optional Service account	If used, the account must be granted the Log On As A Service User right.
	Reporting Account	Domain (recommended) or Local account
SQL Server hosting the Adaptiva Database	Tenable Patch Server SYSTEM Account	During the Tenable Patch Server installation, grant <code>sysadmin</code> permission to the Tenable Patch Server SYSTEM account (see Set System Account Permission in SQL Management Studio). You may reduce these permissions after completing the after the Tenable Patch Server installation. SQL Server Role <code>Sysadmin</code> (installation account for initial installation) Minimum permissions (after installation) <code>Adaptiva Database Security User Mapping</code> (account running the <code>AdaptivaServerservice</code>) <code>db_datareader</code> <code>db_datawriter</code> <code>db_ddladmin</code>
	Installation Account	
	Option Service Account	



Server	Account	Permissions
		db_executer
Content Library	<domain>\PatchServer \$ or Optional Service Account	If you choose to change the location of the Adaptiva Content Library to a remote drive/share, allow the Tenable Patch Server service account the Create, Modify, and Delete permissions to the location
Adaptiva Database	Reporting Account	The Server installation automatically grants db_datareader (read only) permissions for the SQL server (Adaptiva Database) you specify during installation.

Communication Ports

Tenable Patch Management communicates between the server and clients on a range of different ports as a network application. For a list of required ports, see Communication Port and Flow Diagrams.

Tenable Patch Server installation automatically creates Windows Firewall rules for ports in all network profiles during the Tenable Patch Server installation. If using a firewall, other than Windows Defender, you may need to manually configure the required ports to ensure communications are available.

Antivirus Exceptions

Tenable Patch Management Enterprise acquires content directly from the Adaptiva Content Library on the Tenable Patch Server and from the AdaptivaCache folder on individual devices (Clients).

Because antivirus scanning of these files can cause performance degradation, Tenable recommends excluding Tenable folders from antivirus scans. Tenable uses a secure hash to protect all distributed content against tampering or corruption, either in transit or when stored.

The Server and Client installations create a system environment variable that points to the respective install locations. For example, %ADAPTIVASERVER% maps to the following location:

C:\Program Files\Tenable\PatchServer\

%ADAPTIVACLIENT% maps to the following location:



C:\Program Files\Tenable\PatchClient\

Excluding Folders and Processes

There are two types of antivirus exclusions:

- **Folders:** Excludes Parent folders, including sub-folders
- **Process:** Excludes processes. For use when aggressive antivirus programs identify .exe processes as high-risk.

Creating Antivirus Folder Exclusions

Exclude the folders listed in the server and client exclusion tables below. The tables list the parent folders only. Make sure to exclude all sub folders.

Server and Client Folder Exclusions

Description	Exclusion
Server Installation Folder	<path>\Adaptiva\AdaptivaServer
Adaptiva Content Library (if different from the default location)	The default location of the Content Library is <path>\Adaptiva\AdaptivaServer\Data\ContentLibrary
Client Installation Folder	<path>\Adaptiva\AdaptivaClient

Internet Access

The Tenable Patch Server requires access to the Internet when allowing Internet-based clients to communicate with the server. This is an outbound connection only and uses the TCP port 443. See [Connecting to Internet Destinations](#).

Internet Access Requirements

The Tenable Patch Server requires access to the following URL:

https://*Adaptiva.Cloud

Ensure that the following Request Methods are allowed:



HEAD, GET, POST

When using proxies, verify whether you must explicitly allow these request methods. Additionally, use the DELETE request method (required) when using CDN services in the Adaptiva Cloud Service for the customer server.

Note: Disable the SSL inspection feature.

Allow Access to Internet Destinations

Tenable Patch Server and Internet-based clients must be allowed to connect to the Internet destinations in the table below. All ports are outbound only.

Source	Description	Destination	Ports
Tenable and Internet-based clients	Adaptiva Services	*.Adaptiva.cloud *.opendns.com	https (TCP port 443, ICMP, or UDP 3478)
Tenable and Internet-based clients	Adaptiva CDN	*.Adaptivacd.cloud cloud.tenable.com	https (TCP port 443)
Tenable Patch Server	Approval messaging, email and sms messages	api.sendgrid.com api.twilio.com	https (TCP port 443)

Note: Tenable uses external partners (Twilio and SendGrid) to send notification texts and emails for alerts such as patch approvals or password change requests. Per their documentation, they do retain message content for a brief period of time. Tenable does not send any personal identification over these channels.



As of December 1, 2020, in the Adaptiva CDN Service Level Agreement provides CDN storage without additional cost, unless storage exceeds certain limits. The table below shows the included storage and overage costs for the Adaptiva CDN service

Storage Use	Included Storage	Overage Costs
Data Storage	2 TB per customer	\$300 per 1TB (or part thereof), per year
Data Transfer / Egress	1 GB per licensed endpoint per month	\$0.02 per 1GB, per month

Tenable Patch Server Installation Folder

The first user input required for the Tenable Patch Server installation is the installation folder location. The default is C:\Program Files\Tenable\PatchServer.

You may choose a custom installation folder location. Tenable recommends either not installing on the Operating System C:\ drive or moving the Content Library after the installation.

Caution: Do not install the Server on the Operating System (OS) C: drive. The product log files and the Adaptiva Content Library installed with the Server grow over time, which impacts storage and performance on the OS C: drive.

Licensing Tenable Products

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

Have your license key available for the Server installation. You may enter the license key when installing the Server, or enter the license key using the after completing the installation. If you are starting the for the first time or your key has expired, the software prompts you for a license key at login.

Security Certificate Options

The Server installation defaults to enabling TLS for the using a self-signed certificate. The Tenable Patch Server, installation provides the following TLS security options:



- Add your own TLS certificate, authorized through a CA such as Active Directory Certificate Services or a third-party CA like GoDaddy, DigiCert, Let's Encrypt and so on.
- Use the self-signed TLS certificate that the Tenable Patch Server creates during Server installation. This certificate is 4096 bits, uses SHA-512 hash, and expires in 12 years from the date of creation.
- Use plain HTTP protocol. The Tenable Patch Server, installation allows this option for lab testing only. Tenable does not support this choice on product servers.

When deciding on the type of TLS certificate to use for your Server installation, consider whether your security organization has any requirements for using certificates, such as the following:

- Self-signed certificates versus CA certificates.
- Wildcard certificates versus a certificate specific to a server.
- Key size, Hash algorithm, and expiration length requirements.

In addition, identify all administrators who require access to the Admin Portal and whether they require access to all devices. After completing the Server installation, install the Server certificate in the certificate store of each remote device that requires secure access to the Admin Portal (see Import a TLS Certificate).

CA Requirements

CAs issue SSL certificates as PFX files, which you must convert to PEM files for use with the Tenable Patch Server. The two separate .pem files required by the Tenable Patch Server include a certificate file and a private key file in the UTF-8 format. You can convert the .pfx files to .pem with a converter (such as openssl).

Self-signed Certificate Requirements

List the x.500 protocol common and alternate comma-separated names you want to use for the self-signed certificate. These include the following server details:

- FQDN
- DNS aliases



- IP addresses
- NETBIOS

HTTP Communication

Tenable Patch Clients use the UDP to communicate with the Tenable Patch Server. When Clients are unable to use UDP, such as when the company uses cloud-based VPN products like ZScaler, Microsoft Direct Access, or other NAT scenarios, the Tenable Patch Server installation allows you to configure the server to communicate using a defined HTTP port instead of UDP.

HTTP Communication Requirements

Review the following HTTP Communication requirements before choosing the HTTP Communication port to use:

- If s are able to communicate with the using UDP, the installer configures the website component to default to using port 443.
- If s are not able to communicate with the using UDP, the server may be configured to allow binding on HTTP by enabling the direct client mode.
- If installing the on a server with the Web Server role or with SQL Server Reporting Services installed, use a different port or choose to install the on a different server.
- Record the required port information to the Installation Checklist.

Adaptiva Database

The Tenable Patch Server requires its own SQL Server database (Adaptiva Database).

Database Considerations

Prepare for the Adaptiva Database prior to installing the Tenable Patch Server. Choose either a local server or a remote server to host the database and choose the SQL Server Edition.

Adaptiva Database Host Server



- **Local server:** This is the server that also hosts the Tenable Patch Server.
- **Remote server:** This is any remote server you choose, including an existing SQL database or a SQL database associated with an integrated third-party product (ConfigMgr or Workspace ONE).

Adaptiva Database SQL Server Edition

- SQL Server Express Edition
- SQL Server Standard or Enterprise Edition
- An existing SQL Server instance

Make note of the server details and the SQL Server Edition you choose. The Tenable Patch Server installation may require configuration details such as the following:

- Database name
- Server location
- Communication port
- Domain
- Read-only Login information
- Encryption status of the SQL database

System Account

During the installation, Adaptiva defaults to using the Local System account to log into the website. If installing the on the ConfigMgr, the installation requires access to the Local System account. This account requires the **Log On As A Service User** permission.

Domain Account

During the installation, you may choose to use a Domain account to log into the ConfigMgr website. Before using this account, you must enable the ConfigMgr Database role. If choosing to use this account, you will be required to periodically change your password based on the security requirements set by your company.

Database Read Only Account



The Adaptiva database requires a Read-Only SQL Login to display the product dashboard. If the login does not exist, the Server installation creates one. If you use Windows Authentication, the Windows account must exist before running the Server installation.

All data providers for the Tenable Patch Server use the Database read-only account to query the Adaptiva database. During the installation, the account is granted db_datareader permission to the Adaptiva database, preventing any data changes by this account in the Adaptiva database.

If creating a domain account, the Server installation requires entering the NETBIOS Domain, User Name, and Password for the SQL reporting account. Record the required SQL Reporting account credentials on the Tenable Patch Management Installation Guide. Use the following best practices when deciding whether to create a domain account or a SQL account:

- Tenable recommends creating this account to operate the Tenable Patch Server at the highest security level for your SQL Server environment.
- Tenable recommends using an Adaptiva Reporting account. When the SQL Server is remote, the Tenable Patch Server installer can use a domain account.
- All Tenable Patch Server data providers require this account to query the Adaptiva Database.

Windows Authentication

During the Tenable Patch Server installation, you may log into the Tenable Patch Server using Windows Authentication. The Tenable Patch Server Installer automatically enables Windows Authentication when the Windows account is selected in the SQL Server.

Using Windows Authentication requires the following:

- You must already have a Windows account.
- Use Windows Authentication when the reporting account is in the domain and the SQL Server is remote from the Tenable Patch Server.

SQL Server Database

The Tenable Patch Server requires a SQL Server instance to host the Adaptiva database. You may choose to install the Adaptiva database on the same server, a separate SQL Server, or a stand-alone SQL Server Express free version. If hosting with the ConfigMgr database, make sure to review the licensing requirements.



If you use SQL Server Express, you may pre-install the SQL Server Express or select SQL Server Express during installation, which automatically downloads and installs on the server.

Choosing the SQL Server Edition

The Tenable Patch Server installation wizard requires specific input depending on the SQL Server Edition you choose to use. You may choose to install one of the following SQL Server Editions:

- SQL Sever Express
- SQL Server Standard
- SQL Server Enterprise

Use the information in this section to help determine which SQL Server Edition works best in your environment to host the Adaptiva Database. For a full list of the differences between Editions, see [Compare SQL Server versions on the Microsoft website](#).

- SQL Server Express Edition
- SQL Server Standard or Enterprise Edition
- An existing SQL Server instance

SQL Server Requirements

Review the requirements in the table below when deciding which SQL Server Edition to use with the Tenable

Patch Server. A SQL Server Always On availability group may also host the Adaptiva Database.

Component	Requirement
SQL Server Version	• SQL Server 2022 • SQL Server 2019 • SQL Server 2017 • SQL Server 2016 SP2
Database Compatibility	Minimum level is SQL 2016 (130)



Component	Requirement
Level	
Database Sizing	Minimum database size is 5 GB. Storage allocation per managed device is approximately 2.5 MB. Use the following equation to determine your database size requirements: $5 \text{ GB} + (2.5 \text{ MB} \times \text{licensed clients}) = x \text{ GB}$ SQL Server Express supports no more than 10 GB
Memory	64 GB minimum
Disk Infrastructure	SSD or NVMe drives for the database files (recommended), including tempdb and log files.

SQL Server Express Edition Details

The Tenable installation wizard provides a choice to download and install the free SQL Server Express Edition as part of the Server installation. The SQL Server Express Edition has no licensing requirement.

Downloading and installing the free SQL Server Express Edition from Microsoft requires an Internet connection and specific Internet Settings. See [Configure Internet Settings](#) for details and to make the required changes. In addition, using this version requires enabling Microsoft .NET Framework 4.0. For details on how to download .NET Framework 4.0, see [Microsoft .NET Framework 4 Full Language Pack \(x86 x64\)](#) on the Microsoft website.

SQL Server Express Edition has the following limitations:

- No Built-In Scheduled Backups (work around available)
- SSRS is only available with SQL Express with Advanced Services
- Maximum Allowed Memory Capacity - 1410 MB
- Maximum Database Size - 10 GB
- Maximum Number of Cores - 1 socket, up to 8 cores
- No High Availability



Although the Server installer configures all necessary settings, consider the following default settings:

- Installs SQL Server 2022 Express Edition.
- Names the SQL Express instance `AdaptivaSQL`.

If choosing to pre-download the SQL Server 2022 SQLEXPRESS_x64_ENU.exe, record the specified download folder to the Installation Checklist.

SQL Server Standard Edition Details

- Install on the Tenable Patch Server or to a remote location.
- Standard SQL licensing requirements apply. Consult with a Microsoft licensing specialist to ensure you have purchased the proper licenses.
- If you choose this option, ensure you have access to the accounts and permissions for required settings.
- Required if more than 2000 devices are licensed.

SQL Server Enterprise Edition Details

- The Enterprise edition includes the SQL Server Standard Edition statements.
- Required when using a high availability configuration.

Database Creation

When installing the you have the following database creation options:

-
-
-
-

Create the Database in Same SQL Server



- Record the Adaptiva database name as `adaptiva`.
- If not using the default SQL Server instance, record the instance name as `AdaptivaSQL`.
- If not using the default SQL port, choose a different port and record it.
- Identify the SQL Server machine FQDN.
- Choose the SQL Login account, and then record the information in a secure location.
- Enter the SQL Server details on the Installation Checklist.

Install Clients

Software Requirements

Tenable Patch Management supports the following Linux, Windows, and macOS operating systems:

Operating System	Supported Versions
Linux	Red Hat Enterprise Linux (RHEL) 8 and RHEL 9 Ubuntu 22.04 LTS Ubuntu 24.04 LTS CentOS Stream 9 CentOS Stream 10 Debian 11 Debian 12
Windows	Windows 10 + 11 Windows Server 2016 and later, Standard or Datacenter Edition
macOS	macOS 13, 14, and 15 (Apple Silicon only)

On-Prem Supported Platforms and Distributions



Windows

- OS and third-party patching
- Driver patching for Dell, HP, and Lenovo
- BIOS updates.

Linux

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

- Ubuntu 22.04 LTS
- Ubuntu 24.04 LTS
- Debian 11
- Debian 12
- CentOS Stream 9
- CentOS Stream 10

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 for details.](#)

Mac

Third-party patching (no OS patching).

Support for devices running the following macOS versions:



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

Supported Browsers

Tenable Patch Management supports the following browsers:

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

Caution: Do not use Microsoft Internet Explorer.

Note: * If you receive an Admin Portal login error when using Mozilla Firefox, see [Resolve Mozilla Firefox Active](#).

Welcome to Tenable Patch Management 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.



×

Patch Express Setup

Steps <

Welcome

Integrations

Critical Patches

High Patches

Medium Patches

Low Patches

Complete

Welcome to OneSite Patch Express

OneSite Patch Express allows companies [REDACTED] automated patch management.

Follow the guided setup steps to configu [REDACTED]

Summon this wizard at any time from th [REDACTED] settings.

Ready to get started?

Click "Begin" to start OneSite Patch Express

☒ Don't show again

Cancel

Begin

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:



×

Patch Express Setup

Steps

<

<

Enablem...

Remedia...

Detectio...

Patch Pr...

Deploym...

>

Welcome

Integrations

Critical Patches

High Patches

Medium Patches

Low Patches

Complete

Would you like to automatically remediate High level Patches?

If enabled, Adaptiva will automatically deploy patch remediations for all detected High level vulnerabilities.

Yes

No

Copy From ▼

Cancel

Back

Next

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

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

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

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

2. Select **Copy From**, and then select a **patch severity level** to copy. The example begins with High level patch remediation, so the available levels available to select are as follows:



Getting Started with Tenable Patch Management Express

Tenable Patch Management Express automates even the most complex enterprise patching processes, allowing IT and security teams to precisely mirror their patching strategies and tailor processes for specific device groups. Tenable Patch Management Express is powered by Tenable. Tenable is committed to providing the best tools for our customers to achieve their security outcomes. Tenable Patch Management Express provides users with the option to set up and use a multi-tenant environment. Tenant environments allow maintenance of separate data for all customers on a single administrative console.

Prerequisites

Before using any Tenable Patch Management Express, you must set up your Tenable Patch Management Express environment. See the [Tenable Patch Management Express Platform Site Planning Guide](#) for details. For more information on the supported operating systems, see [Supported Operating Systems, Software, Drivers, and BIOS](#).

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

Supported Browsers

Tenable Patch Management Express supports the following browsers:



- Google Chrome
- Microsoft Edge
- Mozilla Firefox*
- Safari

Note: Do not use Microsoft Internet Explorer.

Note: If you receive an Admin Portal login error when using Mozilla Firefox, see [Resolve the Mozilla Firefox Active Directory Login Issue](#) KB article.

Logs for Server

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

<path>\Tenable\Adaptiva Server\Logs

Note: Tenable Patch Management Express 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).

Tenable Patch Management ExpressAdmin Portal



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 Tenable Patch Management Express installation, the administrator creates a SuperAdmin account using either a native Tenable login, OIDC-enabled account, SAML-enabled account, or a Windows Active Directory account (recommended).

Note: 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.



Log in with Email

Email

Password

☐ Remember my email

Log in

[Forgot Password?](#)

[Log in with Active Directory](#)

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.

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

After successfully logging in, the Home page appears.

Licensing Products



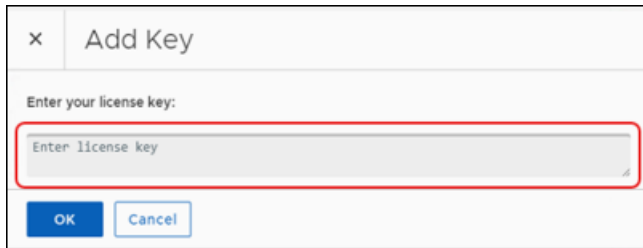
Tenable Patch Management Express requires a license for each active client. The license key contains the licensed company name and client count. The Adaptiva Server periodically counts all active, healthy, reporting clients as licensed clients.

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

Tenable Patch Management Express Setup Wizard

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

Welcome	Use the guided setup to configure Tenable Patch Management Express to meet the needs of your organization. Refer to Welcome to Patch Express .
Integrations	
Enablement	Enable automatic deployment of patch remediation for the specified vulnerability level. Refer Use Copy From .
Remediation Schedule	Schedule automatic remediation of the specified patch vulnerability level. Refer to Select a Remediation Schedule .
Detection Integrations	Enable detection integrations for the specified patch vulnerability level.
Patch Pre-staging	Enable content pre-staging to download all patches to applicable and licensed devices prior to deployment. Refer to Enable Patch Pre-staging .
Deployment Notifications	Notify administrators about the specified patch deployment. Refer to Configure Deployment Notifications .
Approval	Setup approval before deploying the specified patch vulnerability level



	patches. Refer to Configure Deployment Approval .
Test Deployment	Deploy the specified patch vulnerability level patches to a test group before production deployment. Refer to Configure Test Deployment .
Test Approval	Setup approval before deploying the specified patch vulnerability level patches to test devices. Refer to Configure Test Approval .
Complete	Complete the Tenable Patch Management Express Setup process and save the settings to the server. Refer to Complete Setup .

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, refer to [Enable or Disable Guided Setup](#).

Select **Begin** to get started. Your first step is Integrations.



×

Patch Express Setup

Steps <

Welcome

Integrations

Critical Patches

High Patches

Medium Patches

Low Patches

Complete

Welcome to OneSite Patch Express

OneSite Patch Express allows companies automated patch management.

Follow the guided setup steps to configure

Summon this wizard at any time from the settings.

Ready to get started?

Click "Begin" to start OneSite Patch Express

☒ Don't show again

Cancel

Begin

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:

×

Patch Express Setup

Steps

<

<

Enablem...

Remedia...

Detectio...

Patch Pr...

Deploym...

>

Welcome

Integrations

Critical Patches

High Patches

Medium Patches

Low Patches

Complete

Would you like to automatically remediate High level Patches?

If enabled, Adaptiva will automatically deploy patch remediations for all detected High level vulnerabilities.

Yes

No

Copy From ▼

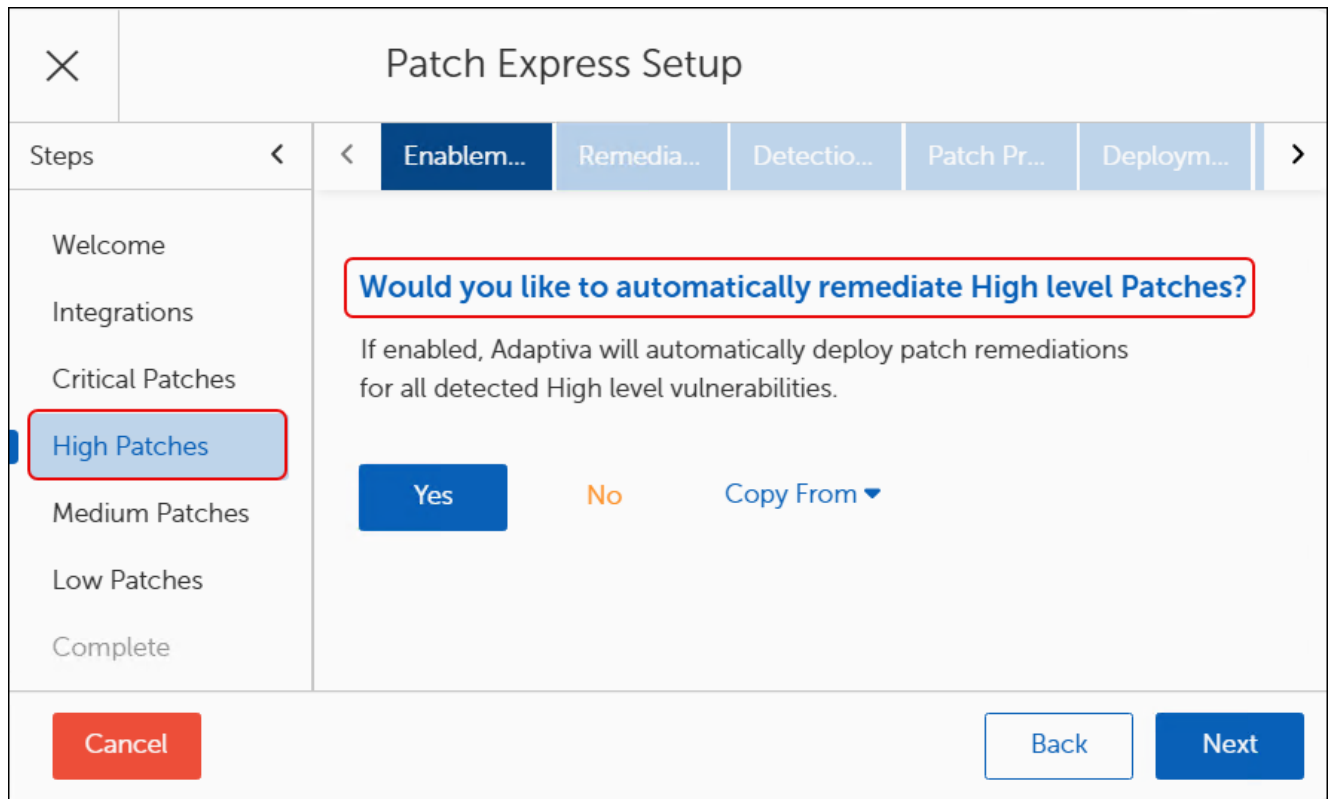
Cancel

Back

Next

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

- 57 -



Patch Express Setup

Steps: Welcome, Integrations, Critical Patches, **High Patches**, Medium Patches, Low Patches, Complete

Would you like to automatically remediate High level Patches?

If enabled, Adaptiva will automatically deploy patch remediations for all detected High level vulnerabilities.

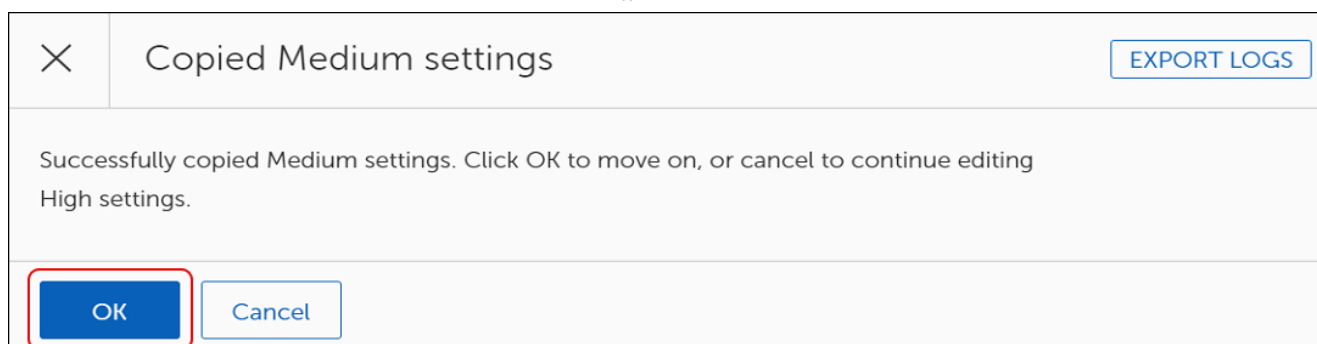
Yes **No** **Copy From ▼**

Cancel **Back** **Next**

- 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.

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

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



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

Select a Remediation Schedule

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



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

×

Add Schedule

Select a Folder

Search...

▼

Schedules

>

Patching Schedules

Schedules

Show All

+ Create Schedule

⚙

Search Columns...

×

Q Search

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

Rows Per Page: 10

1 - 10 of 12

1 / 2

Add Schedule

Cancel

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

<

Enable...

Remedi...

Detecti...

Patch P...

Deploy...

Approval

Test De...

Test Ap...

>

When should Medium level auto-remediation run?

Choose a Schedule on which automatic remediations should execute.

Every 12 Hours

BROWSE ×

Back

Next

Enable Vulnerability Detection

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



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

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

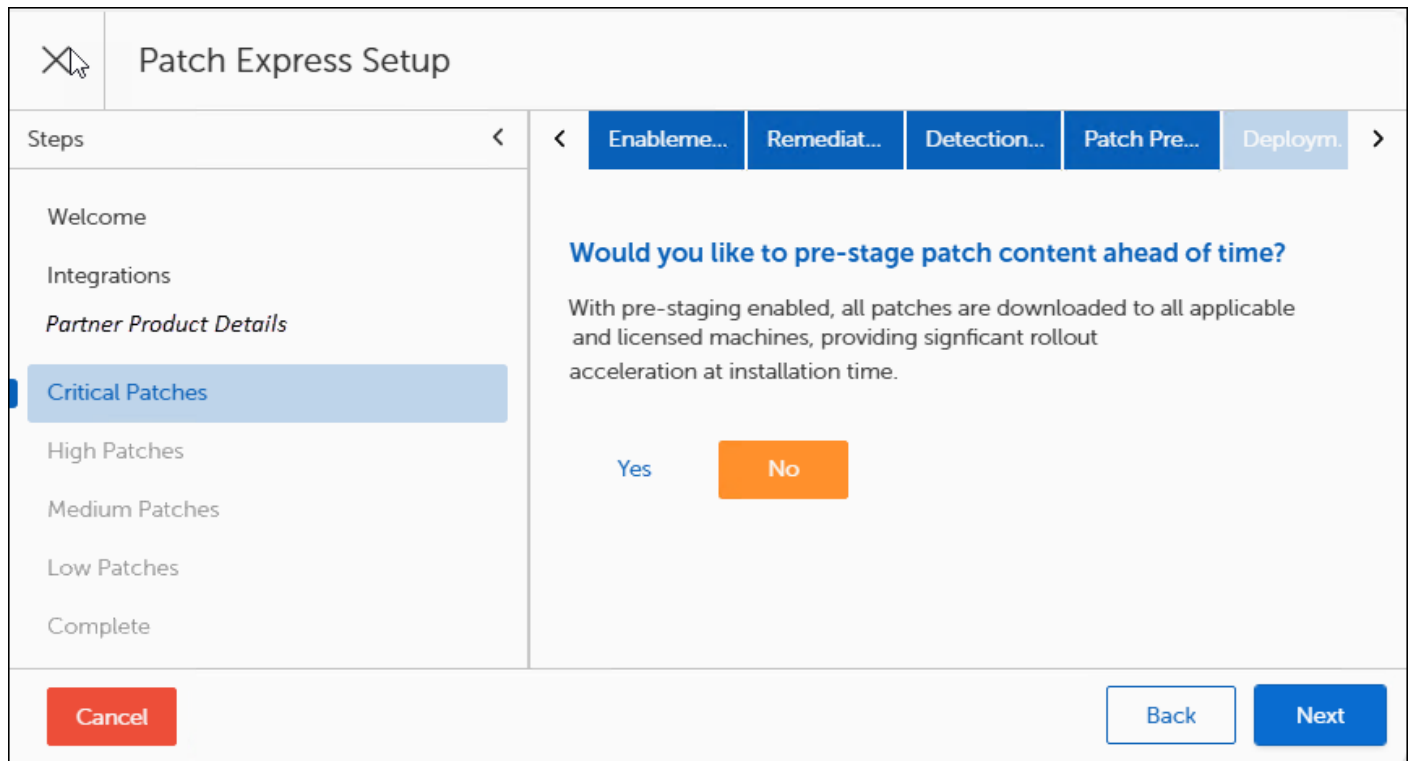
Enable Patch Pre-staging

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

Choose whether to pre-stage patches:

- Select **Yes** to enable patch pre-staging. This takes you to [Configure Deployment Notifications](#).
- Select **No** to skip patch pre-staging. This takes you to [patch approvals](#) (no deployment notification required).

- There is no need to click Next from this tab. If you do click Next, it takes you to the Deployment Notifications tab.



The screenshot shows the 'Patch Express Setup' window. On the left, a 'Steps' sidebar lists: Welcome, Integrations, Partner Product Details, **Critical Patches** (selected), High Patches, Medium Patches, Low Patches, and Complete. The main area displays a confirmation dialog: 'Would you like to pre-stage patch content ahead of time?'. Below the question, it states: 'With pre-staging enabled, all patches are downloaded to all applicable and licensed machines, providing significant rollout acceleration at installation time.' There are two buttons: 'Yes' and 'No'. At the top right, a progress bar shows steps: Enableme..., Remediat..., Detection..., Patch Pre..., and Deploym... (highlighted). At the bottom, there are 'Cancel', 'Back', and 'Next' buttons.

Configure Deployment Notifications

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

1. Decide whether to notify administrators about the patch deployment:
 - 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](#).

×

Patch Express Setup

Steps

<

<

Enabl...

Reme...

Detec...

Patch ...

Deplo...

>

Welcome

Integrations

Critical Patches

High Patches

Medium Patches

Low Patches

Complete

Do you want to notify a group of employees about deployment?

Yes

No

Cancel

Back

Next

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

×

Patch Express Setup

Steps

<

<

Enabl...

Reme...

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 Adaptiva production patch approval request will be sent to belong to the specified role. Any of the Administrators can approve the re patches to be deployed, then the approval request will not be sent.

Add Role

BROWSE

Cancel

Back

Next

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

×

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

Rows Per Page: 10

1 - 3 of 3

1 / 1

Add Role

Cancel

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... Reme... 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...

Reme...

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 Adaptiva production patch approval request will be sent to belong to the specified role. Any of the Administrators can approve the re patches to be deployed, then the approval request will not be sent.

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

Roles

Show All

Search Columns...

Search

Name

All Admin Role

Read-Only Admins Role

Super Admin Role

Rows Per Page: 10

1 - 3 of 3

1 / 1

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:

<

Enablen...

Remedia...

Detectio...

Patch Pr...

Deploym...

Approval

Test Depl...

Test Appr...

>

Approval Timeout

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

0

Days

0

Hours

0

Minutes

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:

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

If you don't specify a load leveling time, production patch installation deployment to all devices occurs immediately.
- c. Select **Next** to set up deployment to a test environment prior to production

Configure Test Deployment

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



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

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

Yes No

Back Next

1. Decide whether to deploy the patch installation to a test group (recommended):

- 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.

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

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

Yes No

Select a Business Unit to which test patches are deployed without any load leveling.

Business Unit BROWSE ×



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.

×

Add Business Unit



Search Columns... 



 Search

☐	...	Name
☐	>	All Clients Business Unit
☐	>	Architecture
☐	>	Architecture - 32-bit Systems
☐	>	Architecture - 64-bit Systems
☐	>	Office Type
☐	>	Office Type - Default
☐	>	Office Type - VPN
☐	>	Office Type - Wi-Fi
☐	>	OneSiteCloud License Business Unit

Add Business Unit

Cancel

4. Choose whether to create preferences or test duration:

Enablen...

Remedia...

Detectio...

Patch Pr...

Deploym...

Approval

Test Depl...

Test Appr...

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

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

+ Create Preferences

Test Deployment Duration

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

0

 Days

0

 Hours

0

 Minutes

Back

Next

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

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

Configure Test Approval

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



1. Decide whether to request administrator approval of the patch deployment:

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

The screenshot shows a software interface with a horizontal tab bar at the top. The tabs are labeled: 'Enablen...', 'Remedia...', 'Detectio...', 'Patch Pr...', 'Deploym...', 'Approval', 'Test Depl...', and 'Test Apr...'. The 'Approval' tab is currently selected. Below the tabs, the main content area displays the question: 'Do you want to seek approval before deploying Critical level patches to test devices?'. There are two buttons: a blue 'Yes' button and an orange 'No' button. The 'Yes' button is highlighted with a red rectangular border. Below the buttons is a text input field with a red border. To the right of the input field is a blue 'BROWSE' button with a small 'X' icon next to it.

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:

<

Enablen...

Remedia...

Detectio...

Patch Pr...

Deploym...

Approval

Test Depl...

Test Appr...

>

Approval Timeout

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

0

Days

0

Hours

0

Minutes

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 Setup

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

×

Patch Express Setup

Steps <

Welcome

Integrations

Critical Patches

High Patches

Medium Patches

Low Patches

Complete

That's it. Ready to start patching?

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

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

Cancel

Back

Finish

Best Practices for Tenable Patch Express



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

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

Tenable Patch Management 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.

Security

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

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

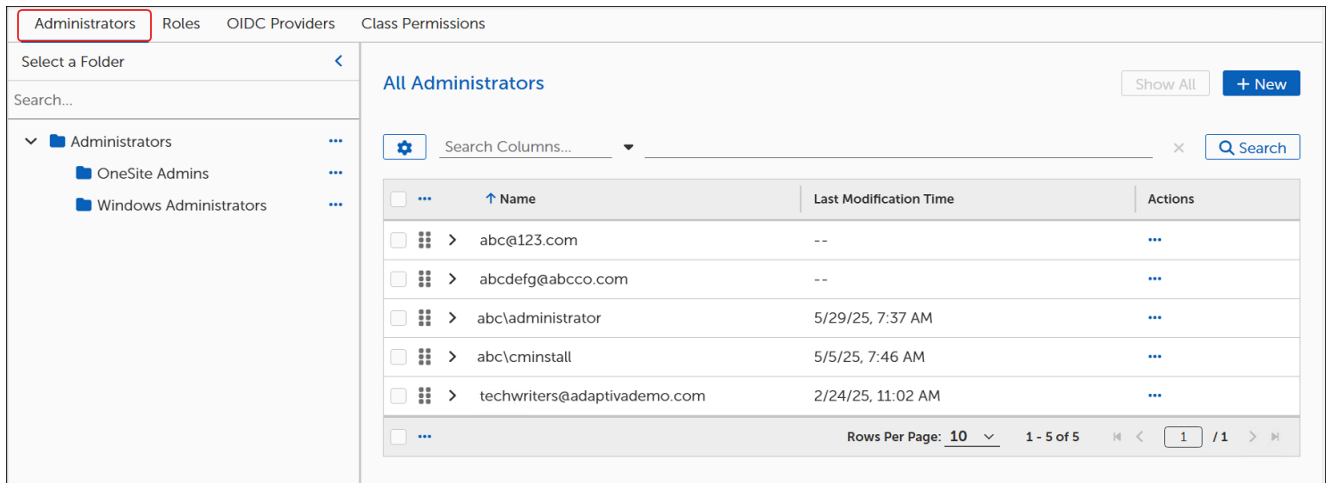
Access Security Settings



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

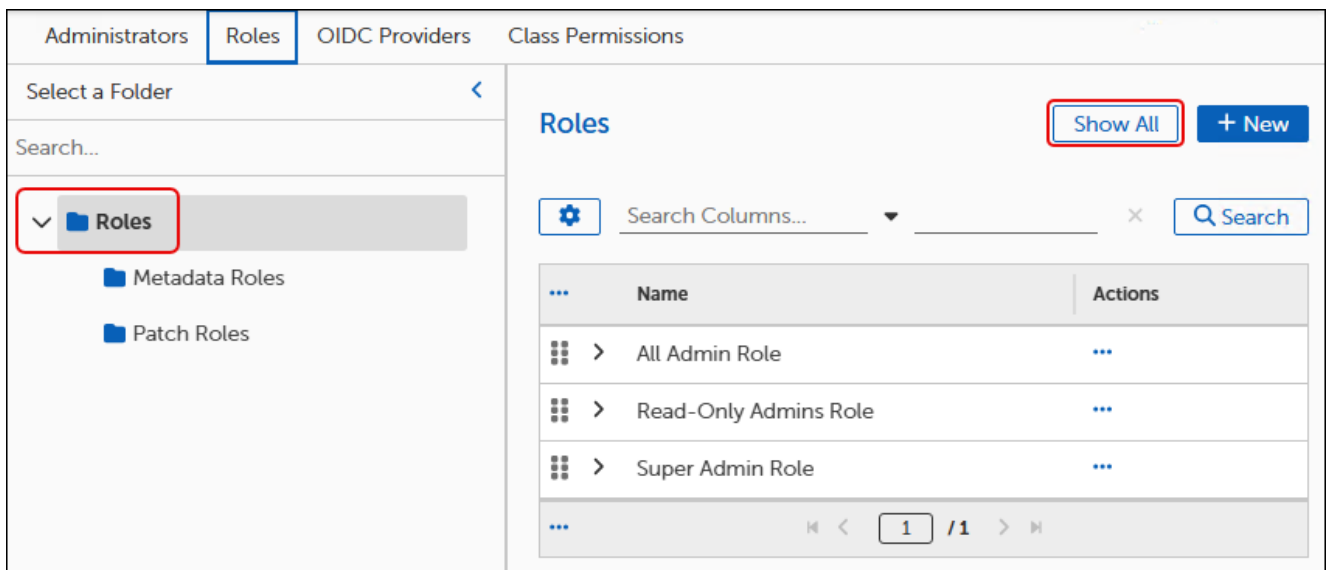
- Select the Roles tab of [Security Settings](#).



Name	Last Modification Time	Actions
abc@123.com	--	...
abcdefg@abcco.com	--	...
abc\administrator	5/29/25, 7:37 AM	...
abc\cminstall	5/5/25, 7:46 AM	...
techwriters@adaptivademo.com	2/24/25, 11:02 AM	...

View Roles

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



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

Menu Objects for Tenable Patch Management Express



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

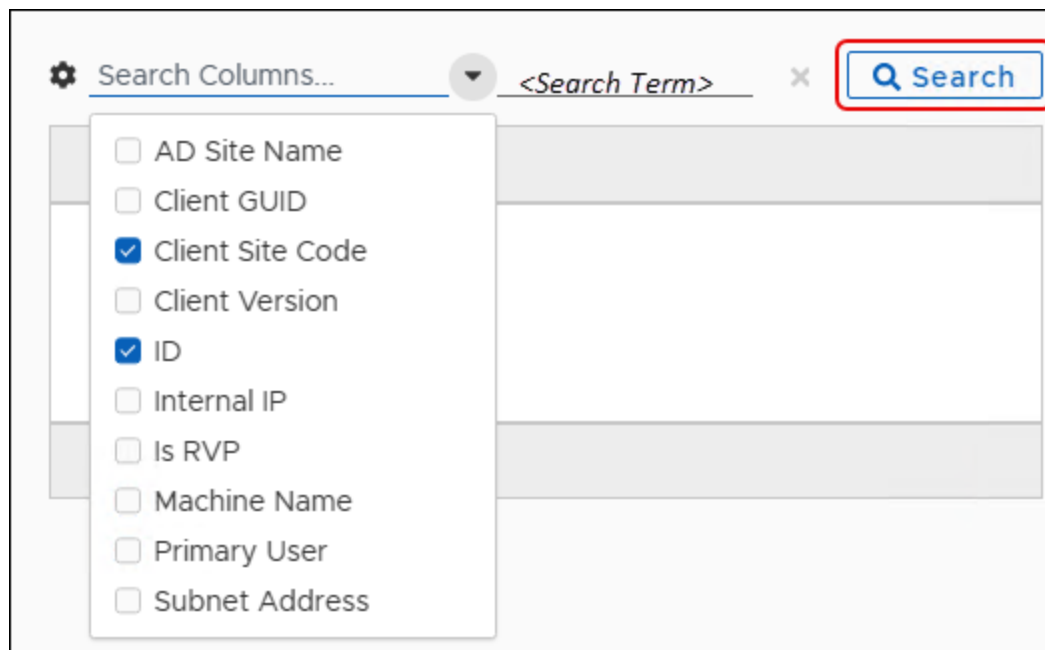
Patching Analytics Dashboards

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 (refer to [Date Range, Export, and Refresh](#)).

Using Search in Tenable Patch Management Express

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

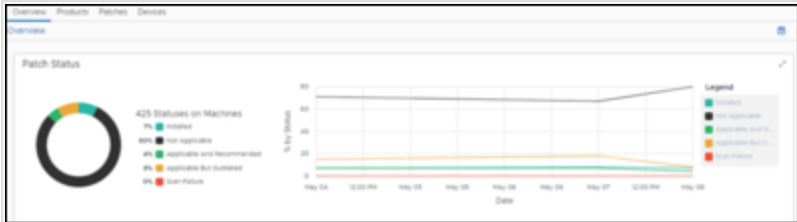


Patching Analytics Overview

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



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



Product Status is a table that lists each product that Tenable Patch Management Express 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

1Password x64

Product Name

1Password ..

Publisher

Agilebits Inc.

Patc...

18

Mach...

0

Devic...

0

Comp...

100%

Risk ...

0

Actions

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

0%

Installed On

Strategies

0

Including this

Product

Average Risk Score

0

Risk Contribution

0

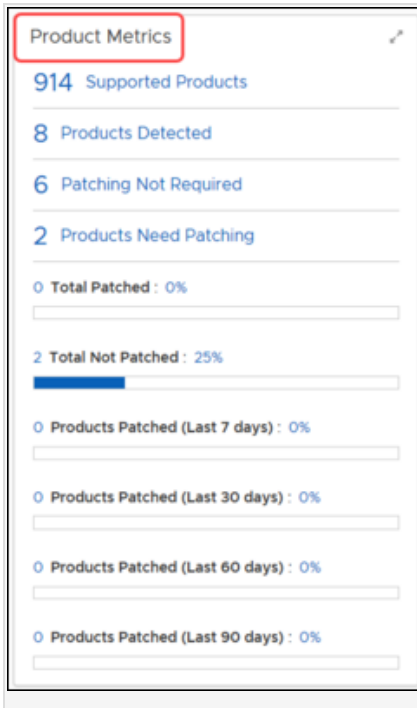
Criticality

50

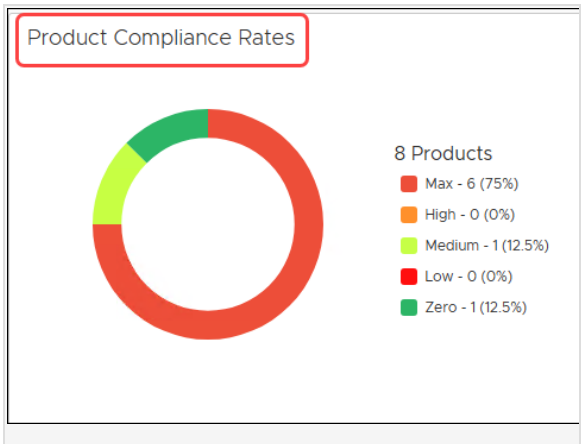
Products View

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

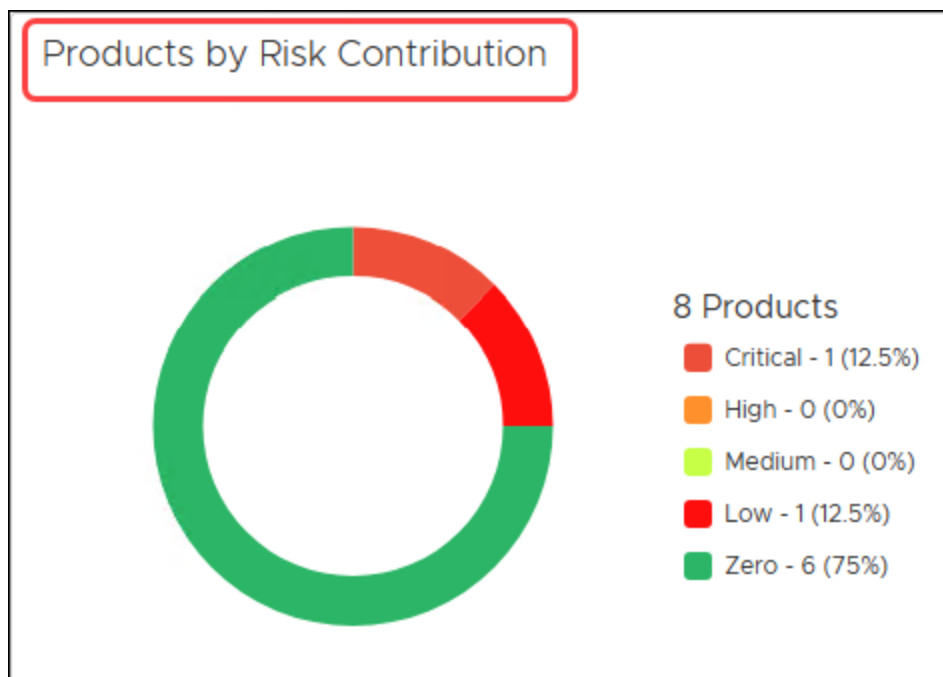
Product Metrics tracks supported products, detected products, and patching requirements, and provides a visual indication of product patching over time.



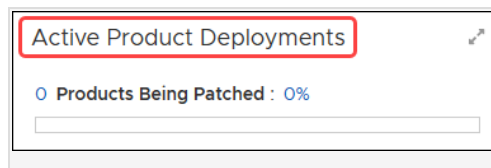
Product Compliance Rates show the number of products in the environment and the compliance rates by percentage. It also includes a chart that shows the level of compliance (Compliant, Compliant by Exclusions, and Non-Compliant) over time.



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 Tenable Patch Management Express 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
IPassword x64	IPassword ..
	Agilebits Inc.
	18 0 0 100% 0
ID	1000000270
Description	IPassword keeps track of password breaches and other security problems so you can keep your accounts safe. It checks for weak, compromised, or duplicated passwords and lets you know which sites are missing two-factor authentication or using unsecured HTTP.
Percentage Installed On	0%
Strategies Including this Product	0
Average Risk Score	0
Risk Contribution	0
Criticality	50

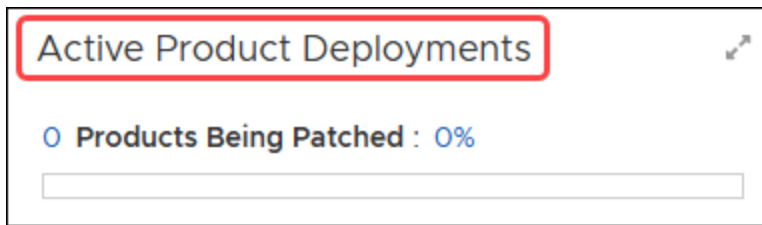
Patches View

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

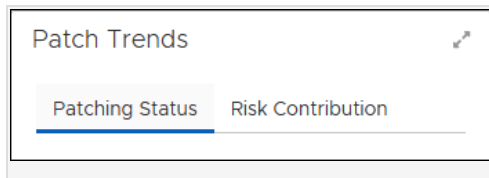
Patch Metrics tracks total patches, patches consumed, installed, or not required, and provides a visual indication of patch installation over time.

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

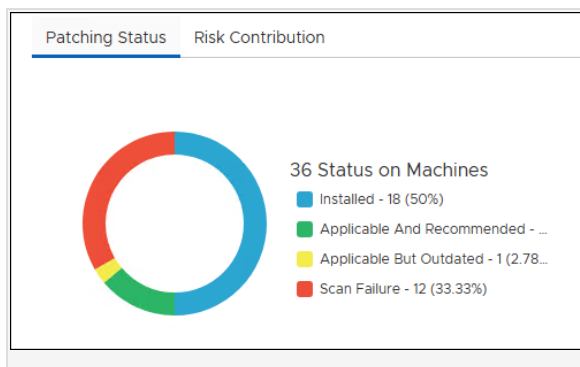
Active Product Deployments provides the number of patches undergoing installation and the percentage of completion.



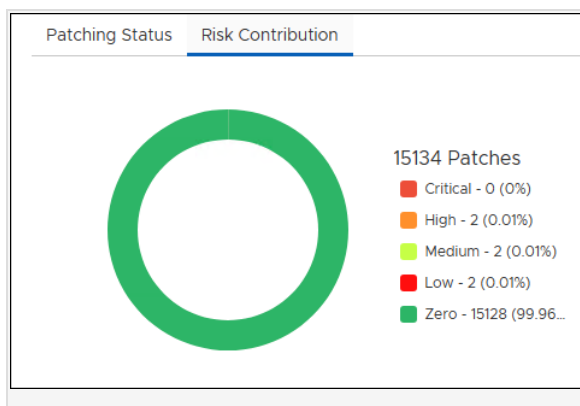
Patch Trends includes two tabs, one for Patching Status and one for Risk Contribution.



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



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



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



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

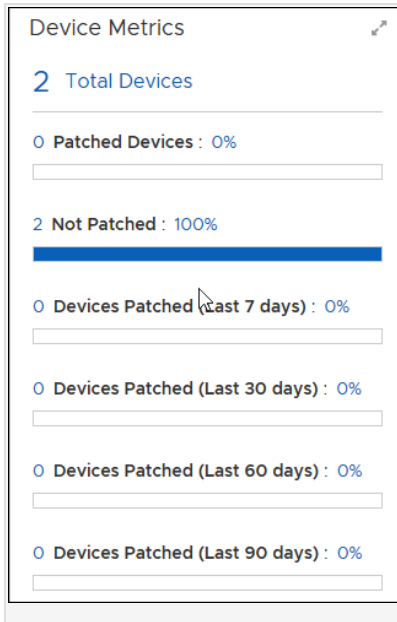
Patch Status is a table that lists each patch that Tenable Patch Management Express looks for during a scan, the installation/applicability status of each, and the status, compliance, and Risk Score for each.

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

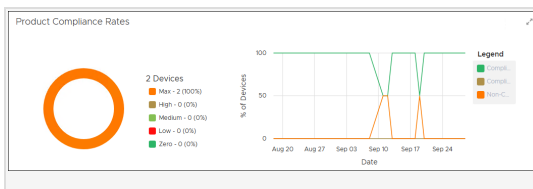
Patch Status	
⚙ Search Columns...	
☐ ... Patch Name	☐ ... Patch Name
☐ .NET 3.5 Feature	☒ .NET 3.5 Feature on Demand for X64
	ID 1021000947
	Description --
	Patch Notes --
	Reboot Type N/A
	Product ID 1000990001
	Not Applicable 2
	Applicable Outdated 0
	Scan Failed 0
	Average Risk Score 0
	Risk Contribution
	Standalone Risk Score 16

Devices View

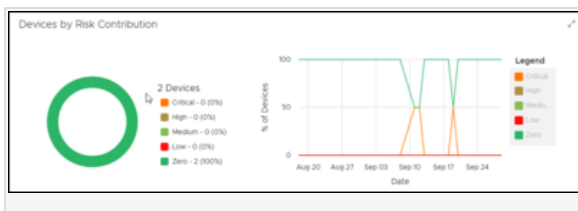
The **Device Metrics** widget shows the total number of devices in the environment, the percentage of patched and unpatched devices, and the percentage of devices patched in the last 7, 30, 60, and 90 days.



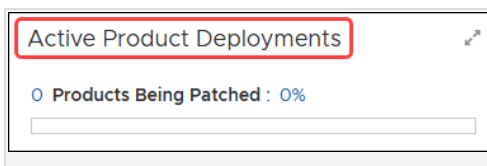
The **Product Compliance Rates** for Devices shows the rate of compliance for each device in the environment based on the latest device scan information. The graph displays the percentage of devices that fall into each category of compliance (max, high, medium, low, and zero), and the line graph shows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



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



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





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

Device Status	
⚙ Search Columns...	
☐ ... Device Name	☐ ... Device Name
☐ > adaptivaserver	☐ ▼ adaptivaserver
	67%153 60%6
	Device ID 2
	Primary User ADAPTIVASERVER\Administrator
	IP Address
	Client Version 9.0.963.2
	Last Check In 11/29/23, 6:11 PM
	Operating System Microsoft Windows Server 2022 Standard
	Location No Office
	Compliant Products 4
	Non-Compliant Products 2
	Applicable Patches / Releases 4

Flex Controls

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

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. Refer to 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. Refer to 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. Refer to 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. Refer to Global Pause .
Rollbacks	Create a Rollback object to rollback a patch to a previous version. Refer to Rollbacks .

Blocklisting

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

When a vendor releases products and patches, the Tenable metadata team reviews the content and determines whether the patch has any issues that might cause unexpected behavior. The 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](#).



▼ Blocklist Settings

Adaptiva Curated Chain

Add Notification Chain

BROWSE

Customer Chain

Add Notification Chain

BROWSE

Adaptiva Curated Communication Providers

+ Add Communication Providers

Customer Communication Providers

+ Add Communication Providers

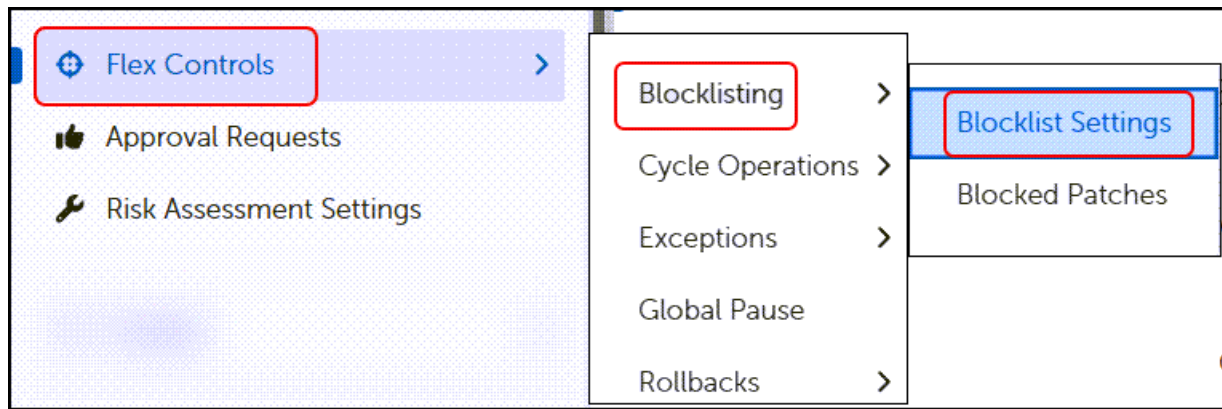
Managing Blocklist Notification Settings

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

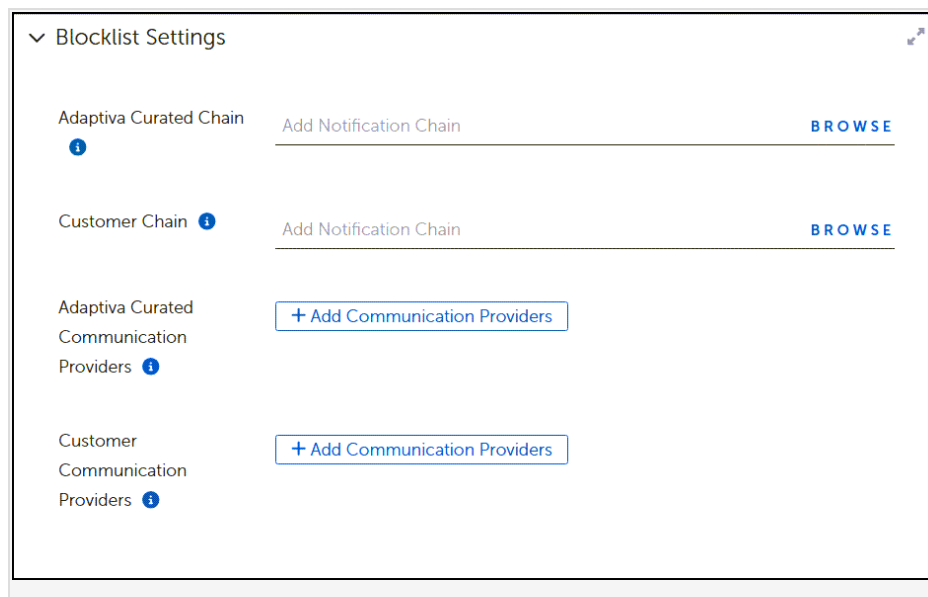
View Blocklist Settings

Blocklist Settings include notification details for blocklisted patches, including Notification Chains and Communication Providers. You can use the Tenable provided details (Tenable 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 **Tenable Curated Chain** or the **Customer Chain** to list the available Notification Chains.
3. Select the **Name** of the Notification Chain you want to use for whichever field you are editing - the **Tenable Curated Chain** or the **Customer Chain**.
4. Select **Add Notification Chain** on the 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.

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

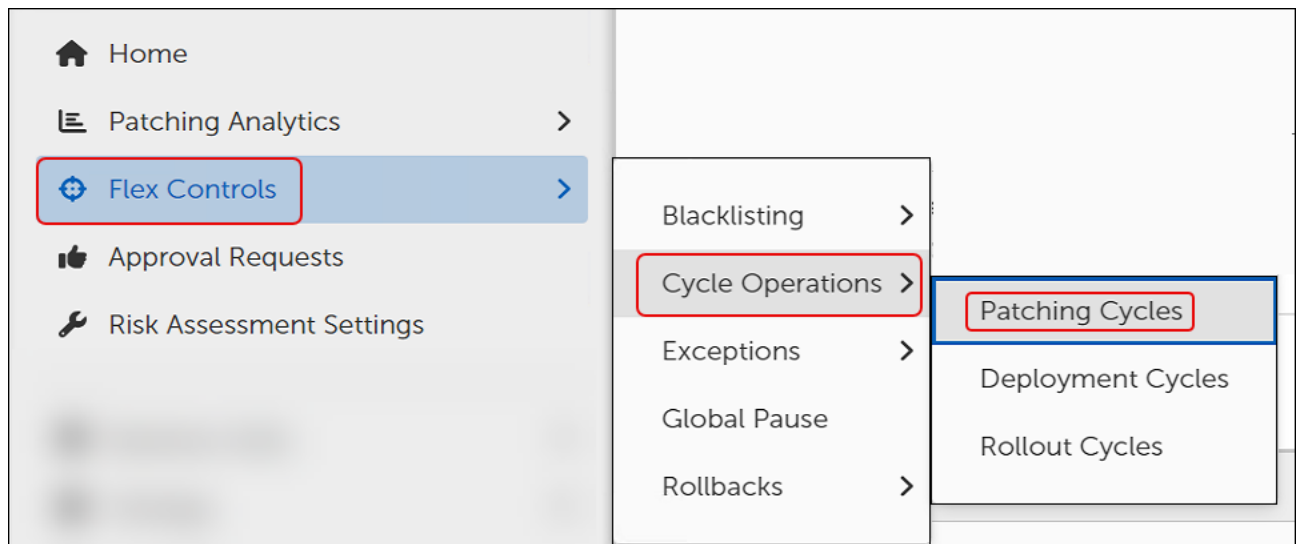
This dashboard shows information about the active Patch Processes in the environment. Patch Processes represent the workflow that models and performs the defined patching routine. As part of



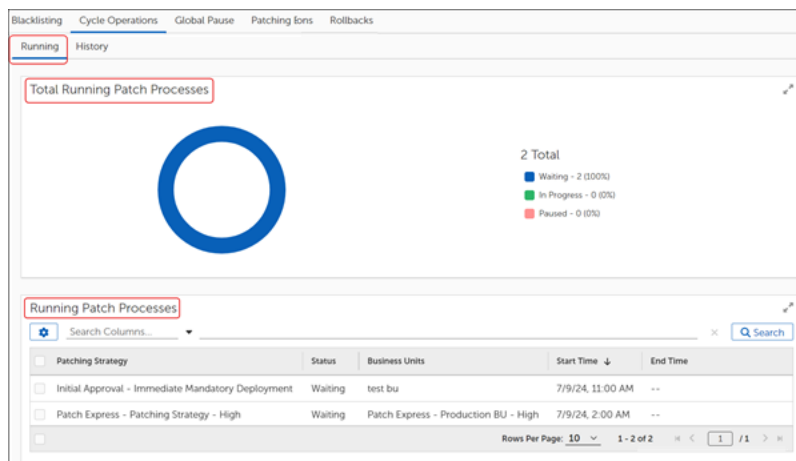
the overall Patching Strategy, Patch Deployment Bots use configured criteria to identify patches that apply to endpoints. Once approved, the Bot submits those patches to the Patch Process, which creates a Patch Cycle. The Patch Cycle executes at either a scheduled time or you can start it manually.

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.

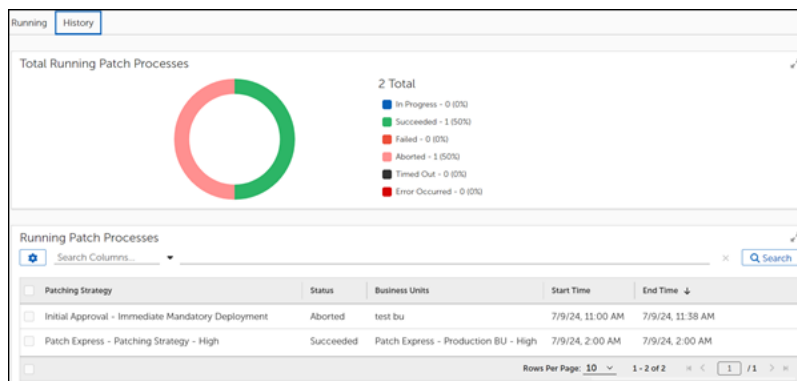
2. Enter a **Patching Strategy** name in the search bar above the Running Patch Processes table, and then select **Search**.

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

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

View Patching Cycle History

1. Mouse over or 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**.

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

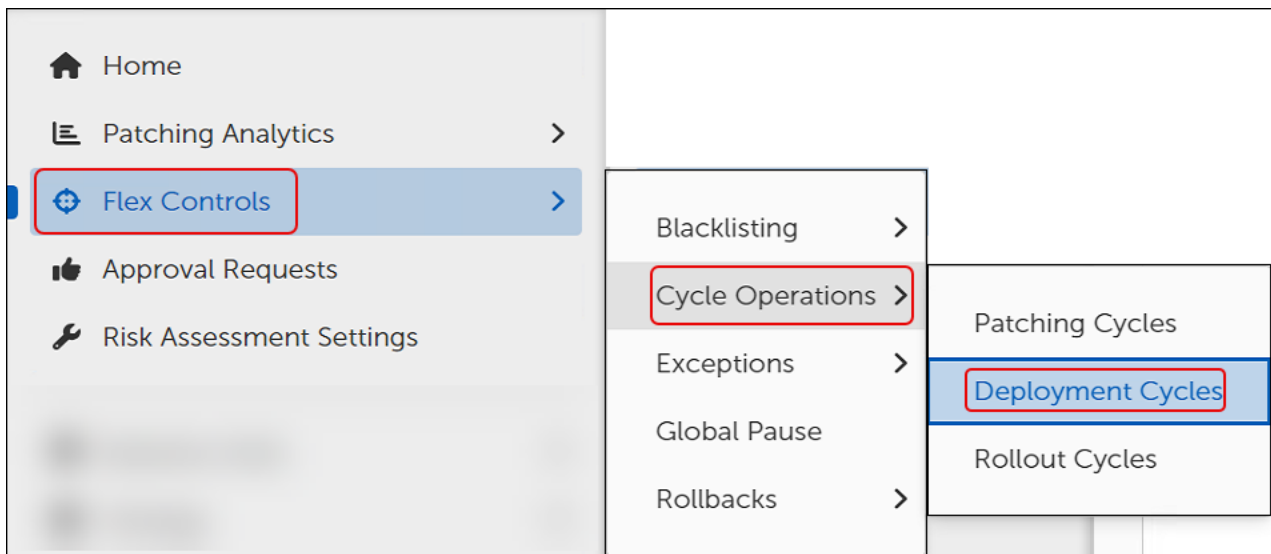
4. Select the **Patching Strategy** name in the **Running Patch Processes** table to see specific details about that process.

Deployment Cycles

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

View the Running Deployment Cycles

1. Mouse over or 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**.

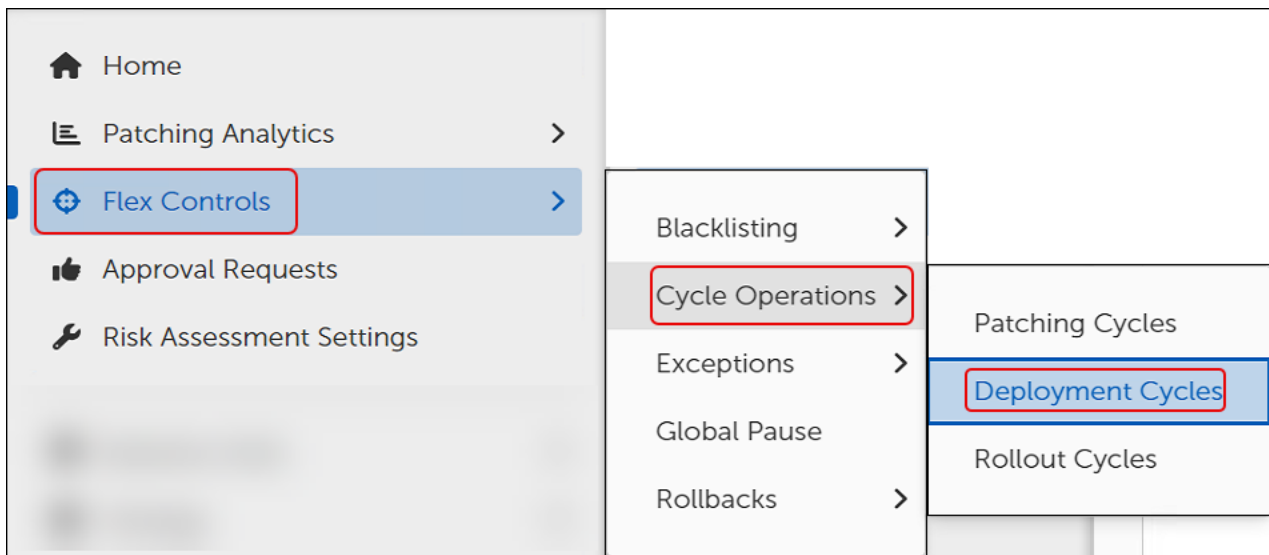
The screenshot shows the 'Running Patch Processes' interface. A search bar at the top contains the text 'Enter Patching Strategy Name' and a 'Search' button. Below the search bar is a table with the following columns: Patching Strategy, Status, Business Units, Start Time, and End Time. The table contains two rows of data. The first row is 'Initial Approval - Immediate Mandatory Deployment' with status 'Waiting' and business units 'test bu'. The second row is 'Patch Express - Patching Strategy - High' with status 'Waiting' and business units 'Patch Express - Production BU - High'. The table has a pagination bar at the bottom showing 'Rows Per Page: 10' and '1 - 2 of 2'.

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

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

View Deployment Cycle History

1. Mouse over or 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:



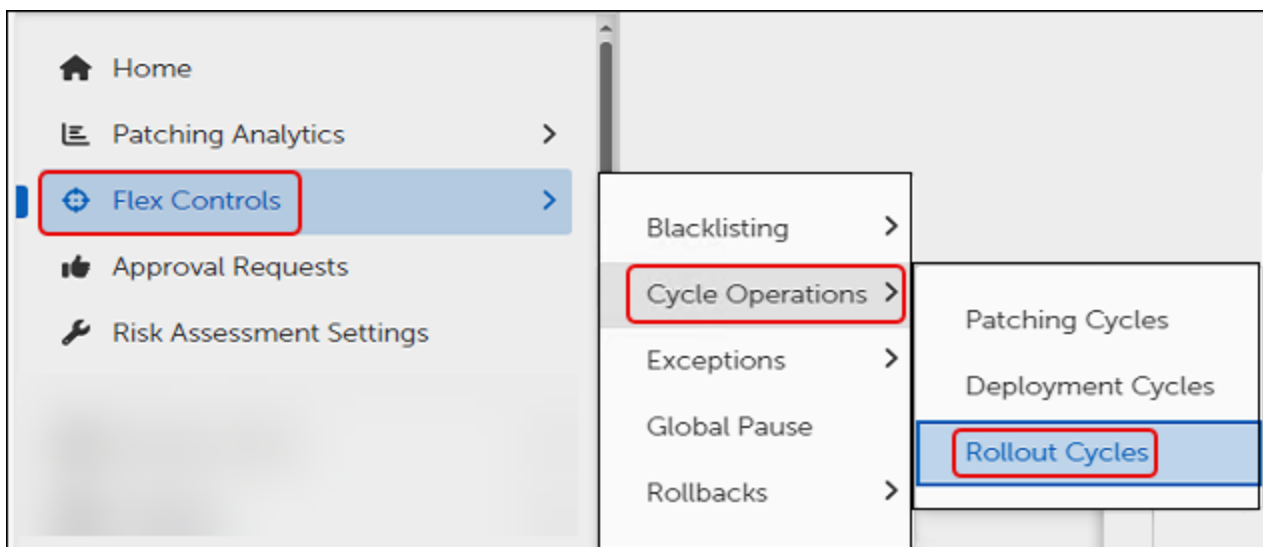
- The Total Running Deployments widget displays deployment processes and their corresponding states (Waiting, In Progress, or Paused).
 - The Running Deployments widget table lists the completed Deployment Strategies by name.
3. Enter a **Deployment Strategy** name in the search bar above the Running 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

Tenable Patch Management Express 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 Tenable Patch Management Express 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

Note: 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) +

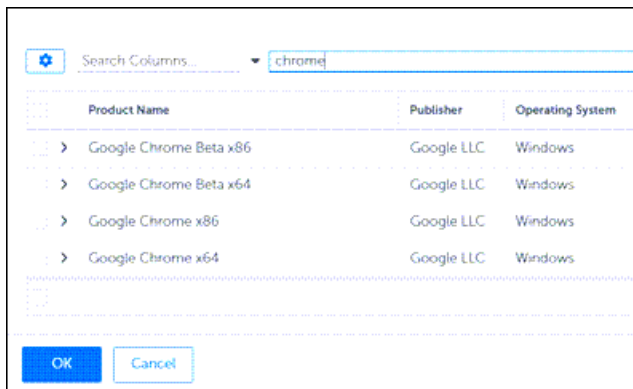
Target Business Units ⓘ *

+ 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:
 1. Enter a product name in the search line, and then select **Search**. This example uses Google Chrome.
- 4.



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



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

Set Last Allowed Patch Versions

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

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.



1. Enter a product name in the search line, and then select **Search**. This example uses Google Chrome.
2. Select the product from the list, and then select **OK**.

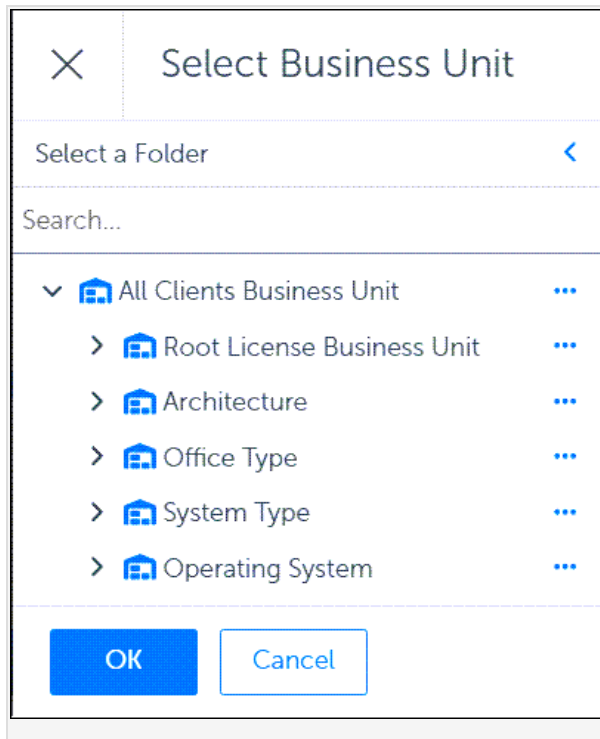
Product Name	Publisher	Operating System
> Google Chrome Beta x86	Google LLC	Windows
> Google Chrome Beta x64	Google LLC	Windows
> Google Chrome x86	Google LLC	Windows
> Google Chrome x64	Google LLC	Windows

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 Tenable Patch Management Server side, and the Tenable Patch Management Client pauses the deployment of patches identified in the pause settings.

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

When activated, Pause All Patching immediately stops all patch deployments across all licensed clients. When deactivated (Resume Patching) Tenable Patch Management Express 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.

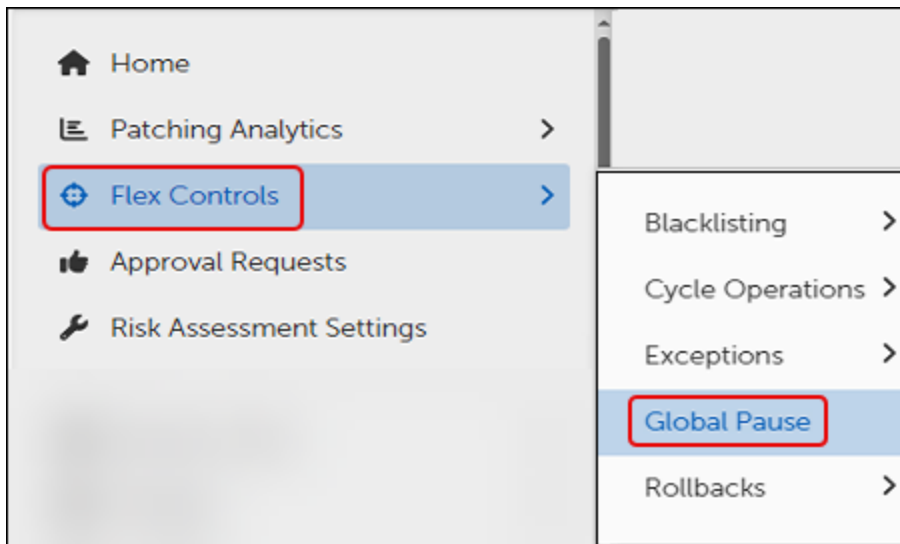
Paused Cycles: Pause Patching, Deployment, or Rollout Cycles either for specified Business Units or for the Business Units already targeted by the Cycle.

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

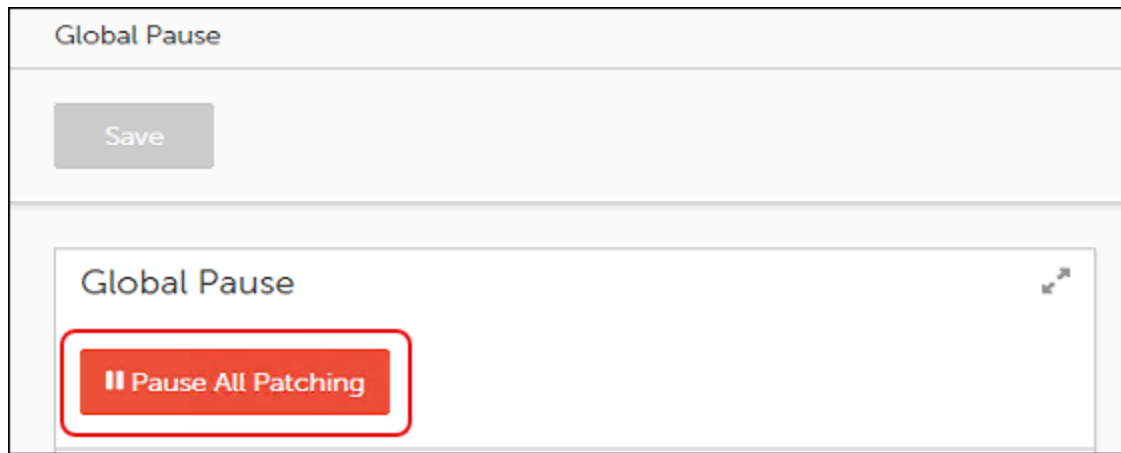
Stop All Patching Activity Immediately

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

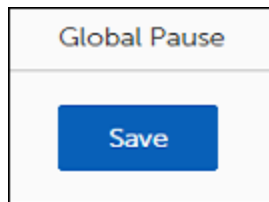
1. Select **Flex Controls** on the Home menu, and then select **Global Pause**.



This opens the Global Pause dialog:



2. Select **Pause All Patching**.



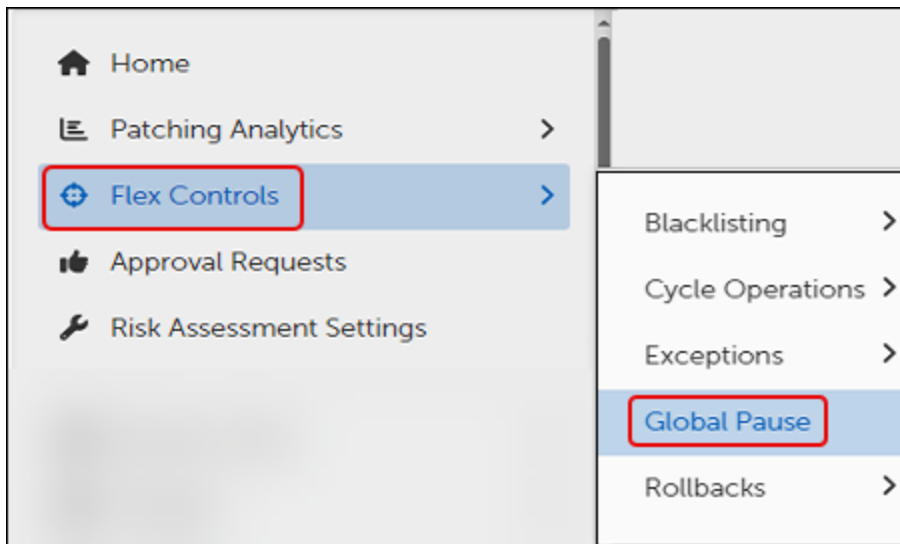
3. Select **Save** to activate Global Pause. This immediately stops all patch deployments across all licensed clients:
- All patch deployments in progress that have not reached an irreversible state are paused immediately.
 - All newly initiated patch deployments are paused automatically.

Resume All Paused Patching Activity Immediately

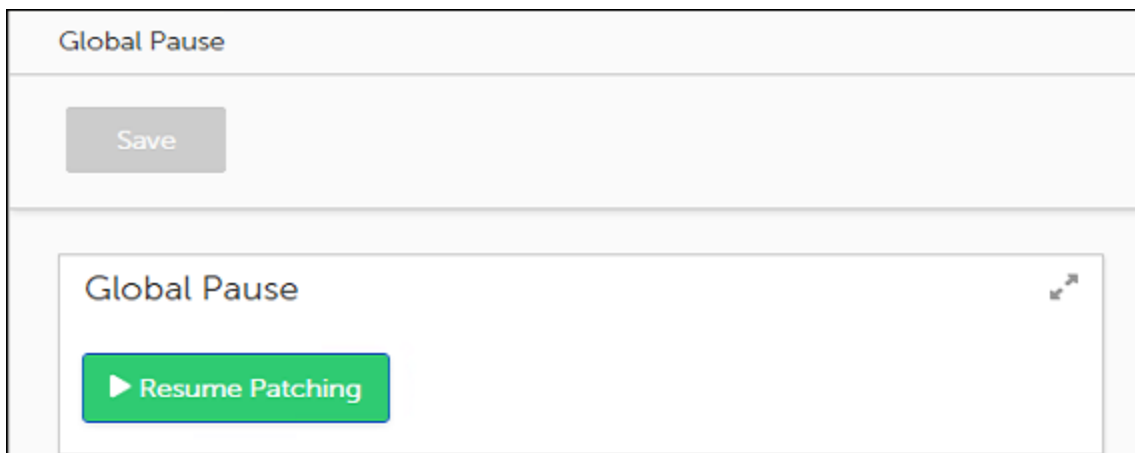
To resume all paused patching activity on all licensed clients, use the following steps to revoke a Global Pause.



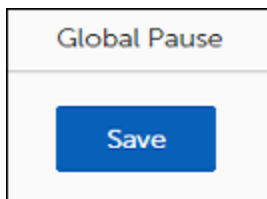
1. Select **Flex Controls** on the Home menu, and then select **Global Pause**.



This opens the Global Pause dialog:



2. Select **Resume Patching**.



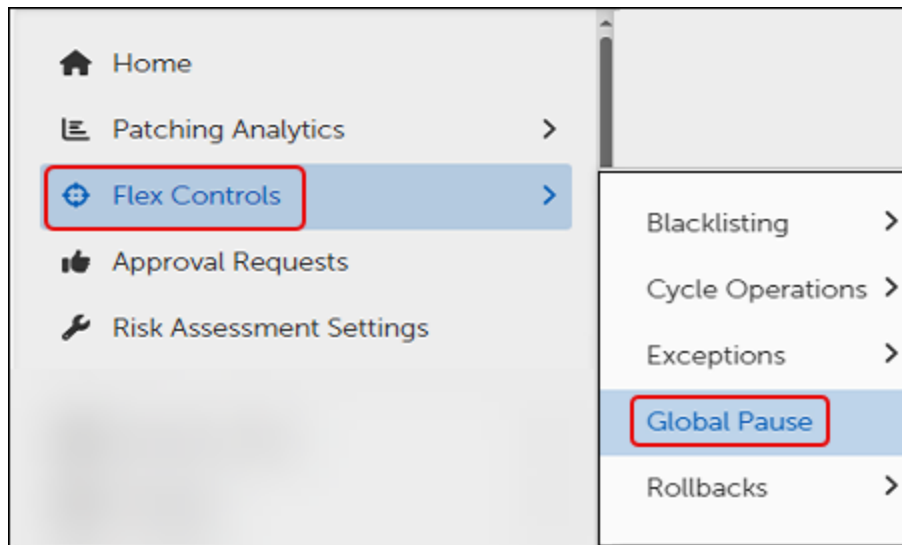
3. Select **Save** to revoke the Global Pause. This immediately revokes the Global Pause and allows patching activity to occur as configured.

Pause Patching for Specific Objects

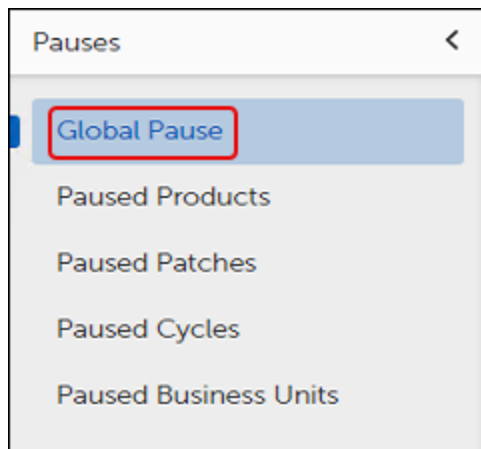


To stop patching activity for specific objects, such as Products, Patches, Cycles, and Business units, use the following steps to access the Pause menu items:

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](#)).



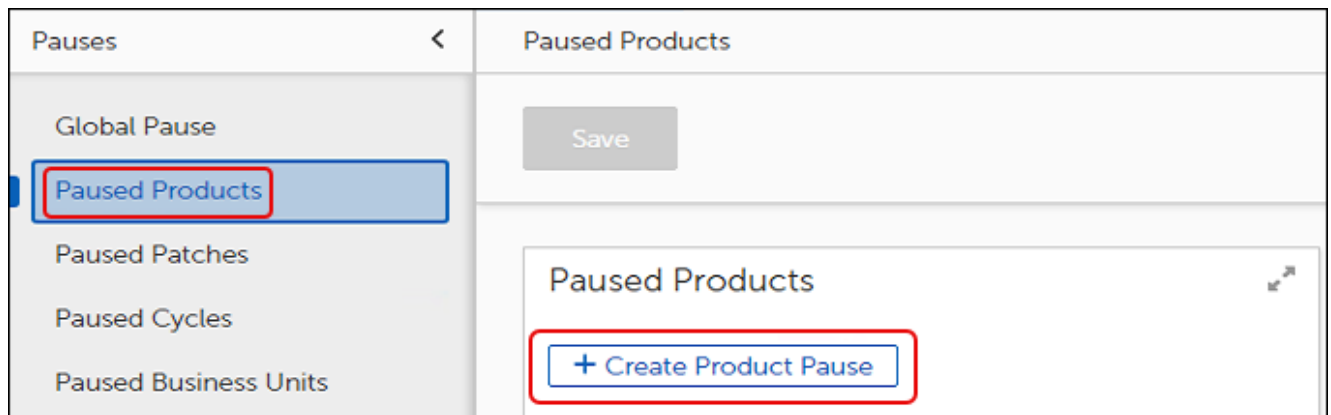
- **Pause Patches:** Pause deployment of a software patch or release for one or more products ([Paused Patches](#)).
- **Paused Cycles:** Specify a [Patching](#), [Deployment](#), or [Rollout](#) cycle to pause for one or more products.
- **Pause Business Units:** Pause patch deployments for one or more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

Pause Deployment of a Specific Software Product

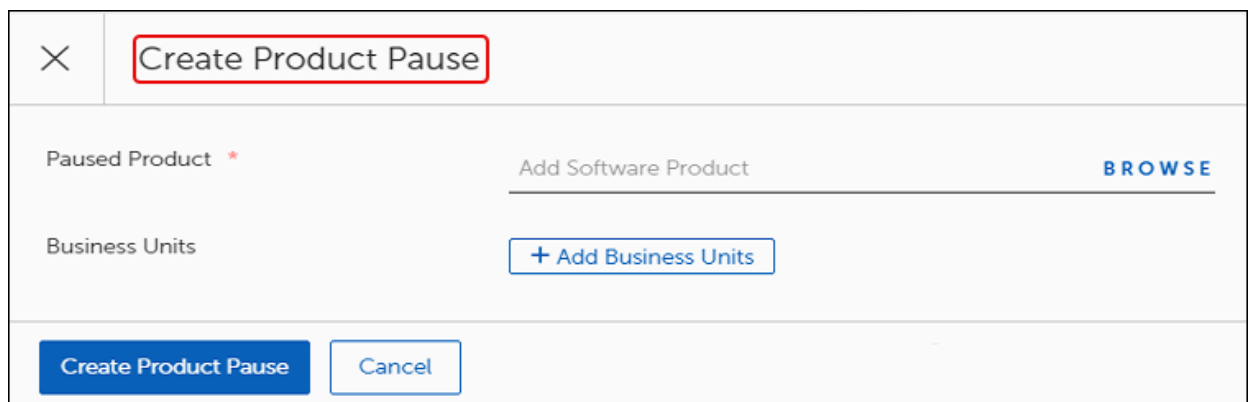
To stop patching activity for specific software products or patches, complete the following steps:

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

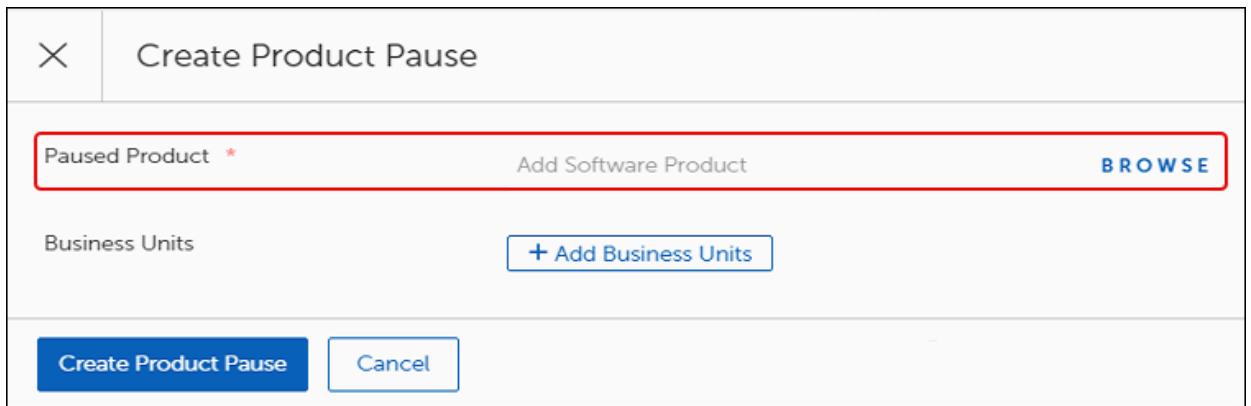
This opens the Paused Products dialog:



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

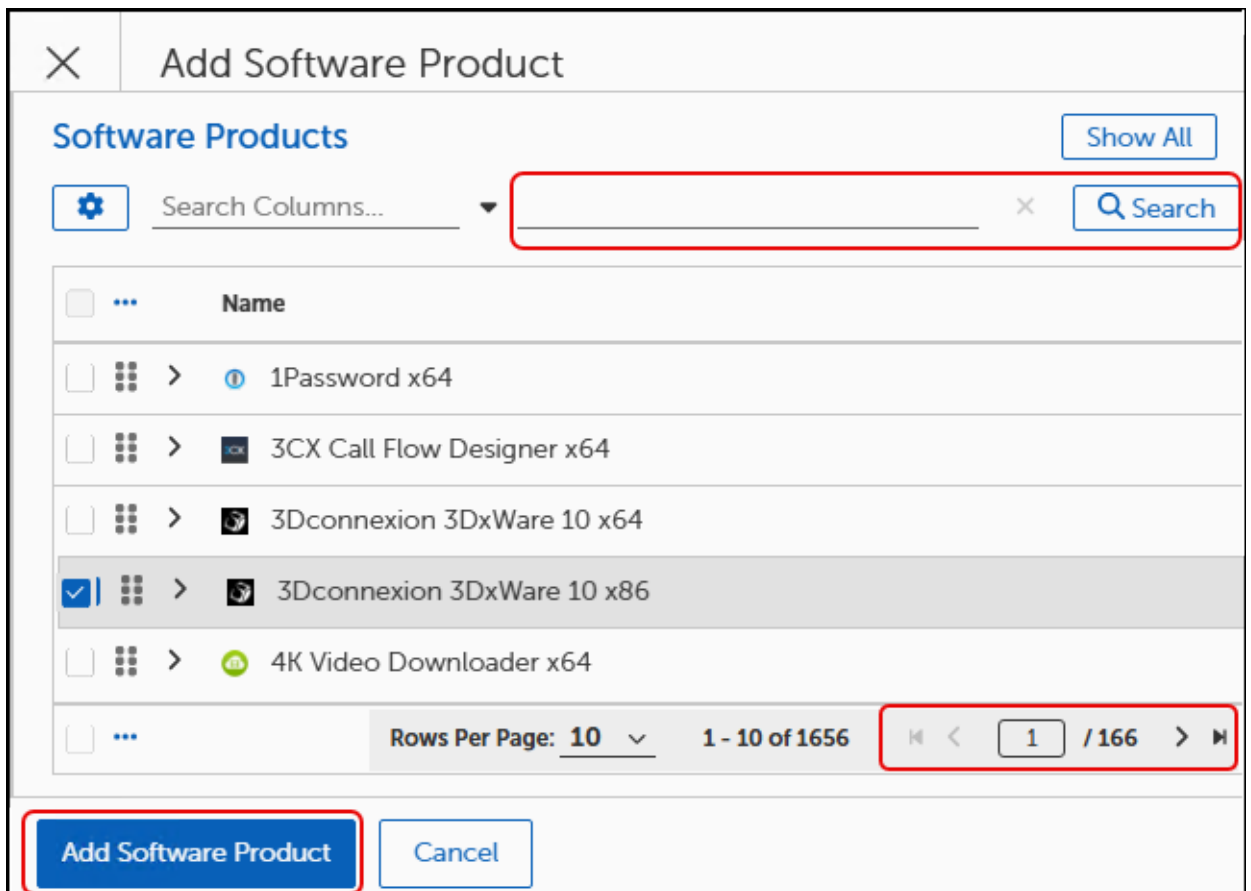


- b. Select **Browse** to find the software product to pause.



The 'Create Product Pause' dialog box features a close button (X) in the top left. The main area contains a 'Paused Product' field with a red asterisk, an 'Add Software Product' link, and a blue 'BROWSE' button. Below this is a 'Business Units' section with a '+ Add Business Units' button. At the bottom are 'Create Product Pause' and 'Cancel' buttons.

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



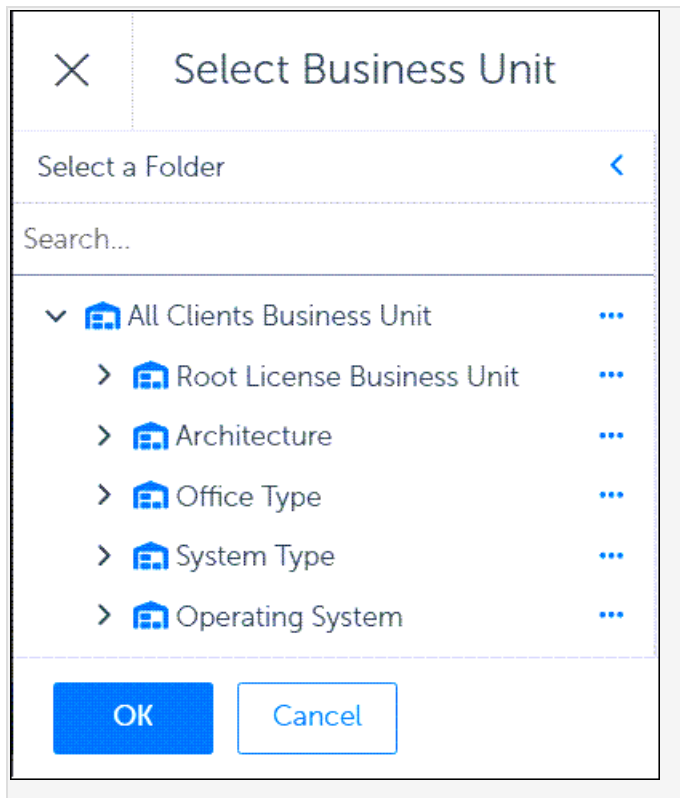
The 'Add Software Product' dialog box includes a close button (X) and a title bar. It features a 'Software Products' section with a 'Show All' button. Below this is a search bar with a 'Search' button. A table lists software products with checkboxes and icons. The product '3Dconnexion 3DxWare 10 x86' is selected. At the bottom right, there are pagination controls showing '1 - 10 of 1656' and a page number '1'. At the bottom left is an 'Add Software Product' button and a 'Cancel' button.

☐	Name
☐	1Password x64
☐	3CX Call Flow Designer x64
☐	3Dconnexion 3DxWare 10 x64
☒	3Dconnexion 3DxWare 10 x86
☐	4K Video Downloader x64

- 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**.



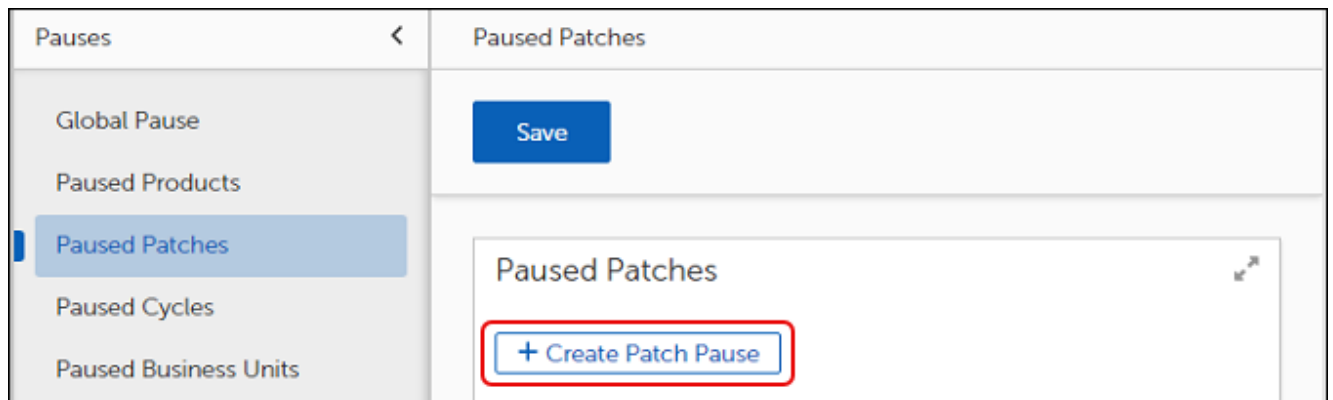
4. Select **Create Product Pause**, and then select **Save** to create a global pause for the selected products.

Pause Deployment of a Specific Patch

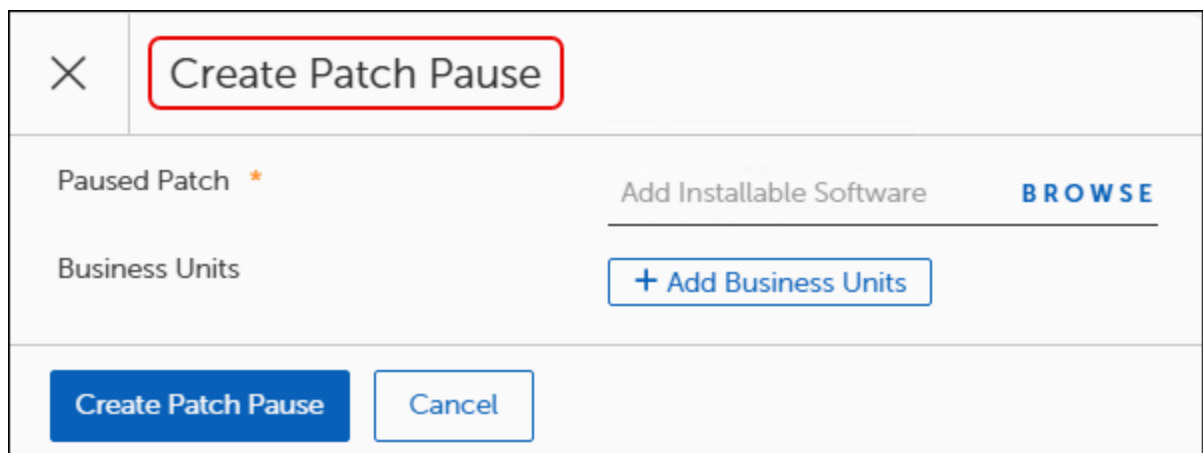
To stop patching activity for a specific patch, complete the following steps:

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

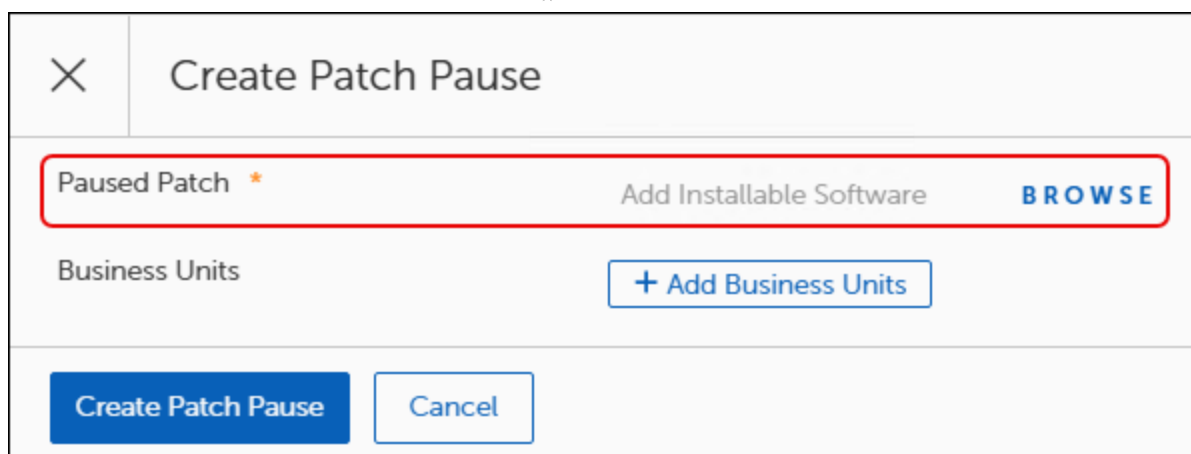
This opens the Paused Patches dialog:



- 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:

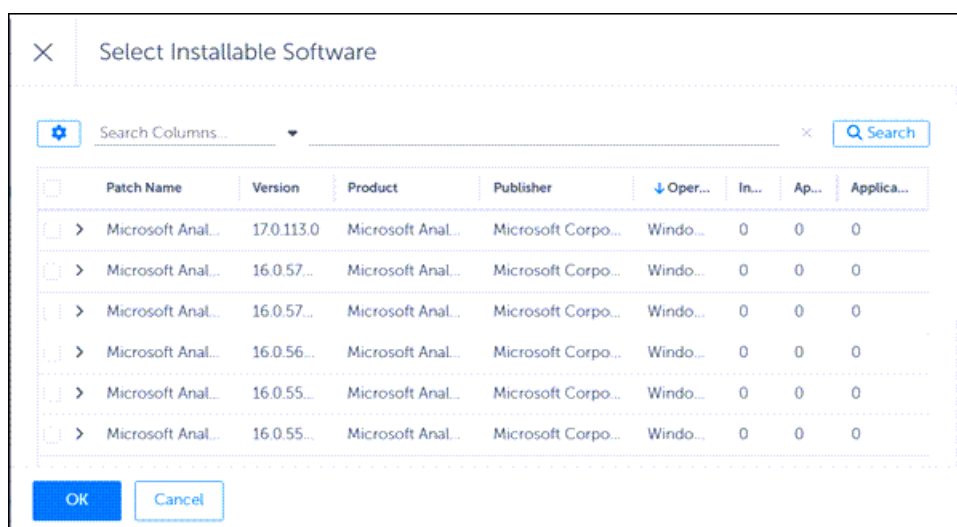


- b. Select **Browse** to find the Software Patch to pause:



The 'Create Patch Pause' dialog box features a close button (X) in the top-left corner. The main title is 'Create Patch Pause'. Below the title bar, there is a section with a red border containing the text 'Paused Patch' followed by a star icon, the text 'Add Installable Software', and a blue 'BROWSE' button. Below this section, the text 'Business Units' is displayed next to a blue button labeled '+ Add Business Units'. At the bottom of the dialog, there are two buttons: a blue 'Create Patch Pause' button and a white 'Cancel' button with a blue border.

c. Select the patch you want to pause:



The 'Select Installable Software' dialog box has a close button (X) and a title 'Select Installable Software'. It includes a search bar with a magnifying glass icon and a 'Search' button. Below the search bar is a table with columns: Patch Name, Version, Product, Publisher, Oper..., In..., Ap..., and Applica... (truncated). The table contains six rows of data, all from Microsoft Corporation. At the bottom, there are 'OK' and 'Cancel' buttons.

	Patch Name	Version	Product	Publisher	Oper...	In...	Ap...	Applica...
☐	> Microsoft Anal...	17.0.113.0	Microsoft Anal...	Microsoft Corpo...	Windo...	0	0	0
☐	> Microsoft Anal...	16.0.57...	Microsoft Anal...	Microsoft Corpo...	Windo...	0	0	0
☐	> Microsoft Anal...	16.0.57...	Microsoft Anal...	Microsoft Corpo...	Windo...	0	0	0
☐	> Microsoft Anal...	16.0.56...	Microsoft Anal...	Microsoft Corpo...	Windo...	0	0	0
☐	> Microsoft Anal...	16.0.55...	Microsoft Anal...	Microsoft Corpo...	Windo...	0	0	0
☐	> Microsoft Anal...	16.0.55...	Microsoft Anal...	Microsoft Corpo...	Windo...	0	0	0

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**.

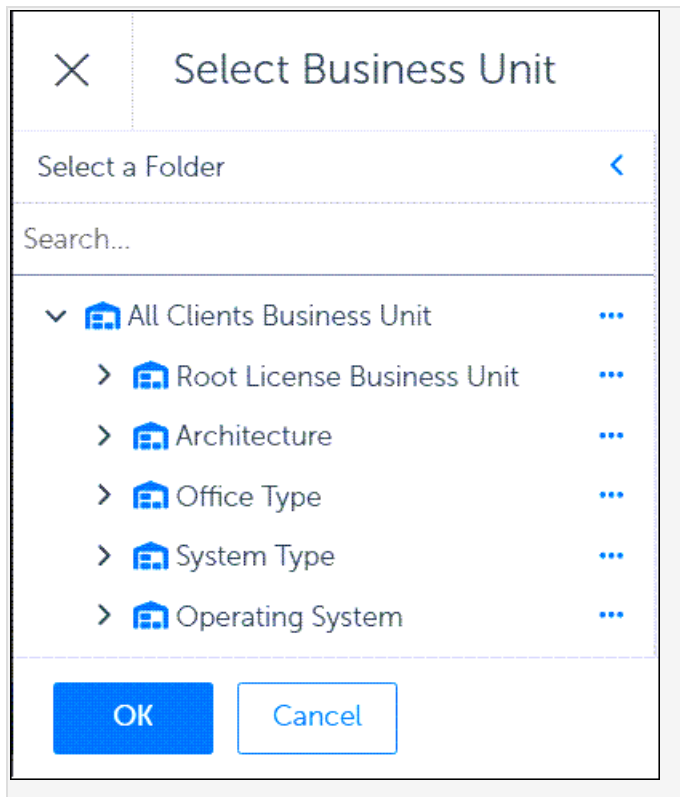
3. Add or remove **Business Units**:

- 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

Tenable Patch Management Express 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](#)



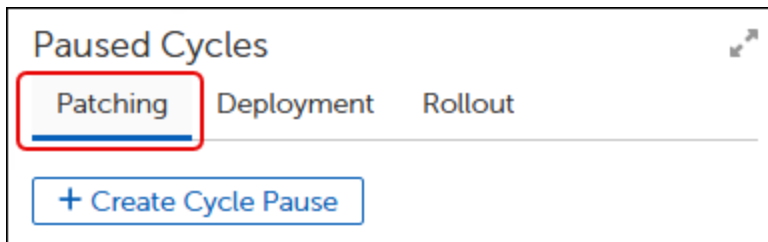
Note: Pausing a cycle that is currently in a WAITING state (has not run yet), prevents that cycle from running until you remove the pause. This is the only server-side behavior related to pausing.

Pause a Patching Cycle

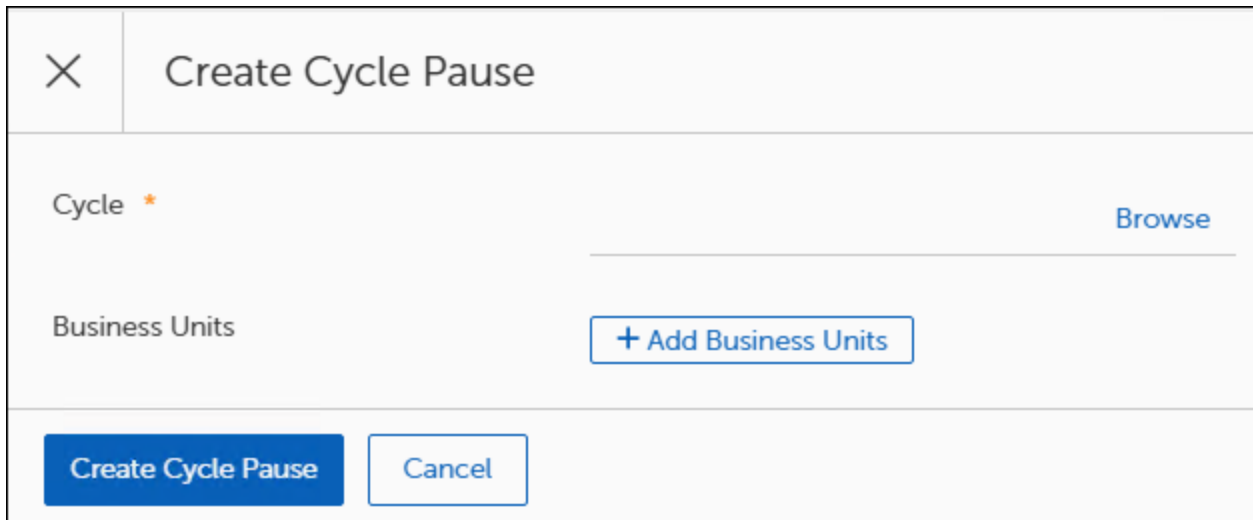
To stop patching activity for a specific patching cycle, complete the following steps:

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:

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

×

Select a Patching Cycle

⚙ Search Columns... × 🔍 Search

No data provided

OK Cancel

- 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.

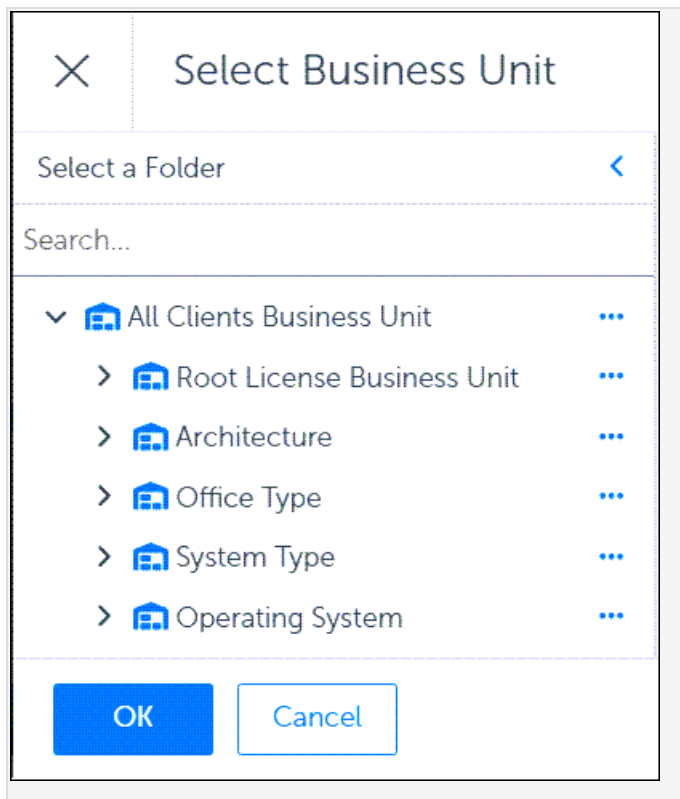
4. Select **OK**, and then choose one of the following options to proceed:

- 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**.

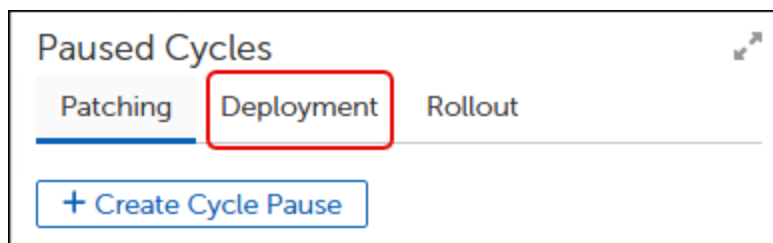
6. Select **Create Cycle Pause**, and then select **Save** to create a pause for the selected cycle.

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 title bar with a close button (X) and the title 'Create Cycle Pause'. Below the title bar, there are two main sections. The first section is labeled 'Cycle' with an orange star icon and a 'Browse' button on the right. The second section is labeled 'Business Units' and contains a '+ Add Business Units' button. At the bottom of the dialog, 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.

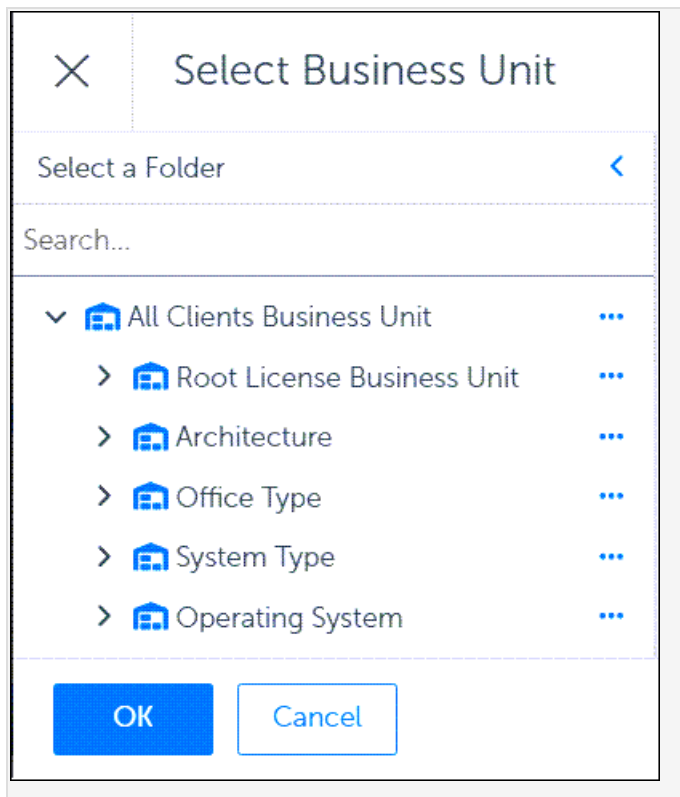
Note: Cycles do not appear unless you have created them previously. If you do not have a cycle to pause, choose a different pause method.

The 'Select a Deployment Cycle' dialog box has a title bar with a close button (X) and the title 'Select a Deployment Cycle'. Below the title bar, there is a search bar with a gear icon, a 'Search Columns...' dropdown, a close button (X), and a 'Search' button. The main area of the dialog is a table that currently displays 'No data provided'. At the bottom, there are two buttons: 'OK' (highlighted in blue) and 'Cancel'.

- Use the navigation tools on the lower-right to scroll through the pages to find and select a cycle from the table.



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



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

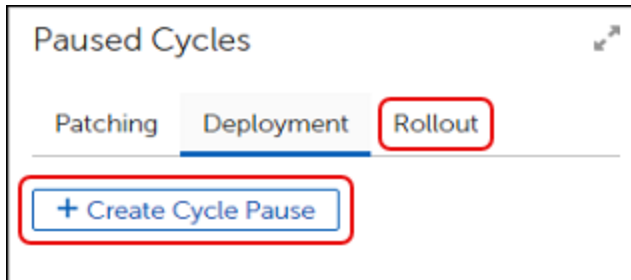


Pause a Rollout Cycle

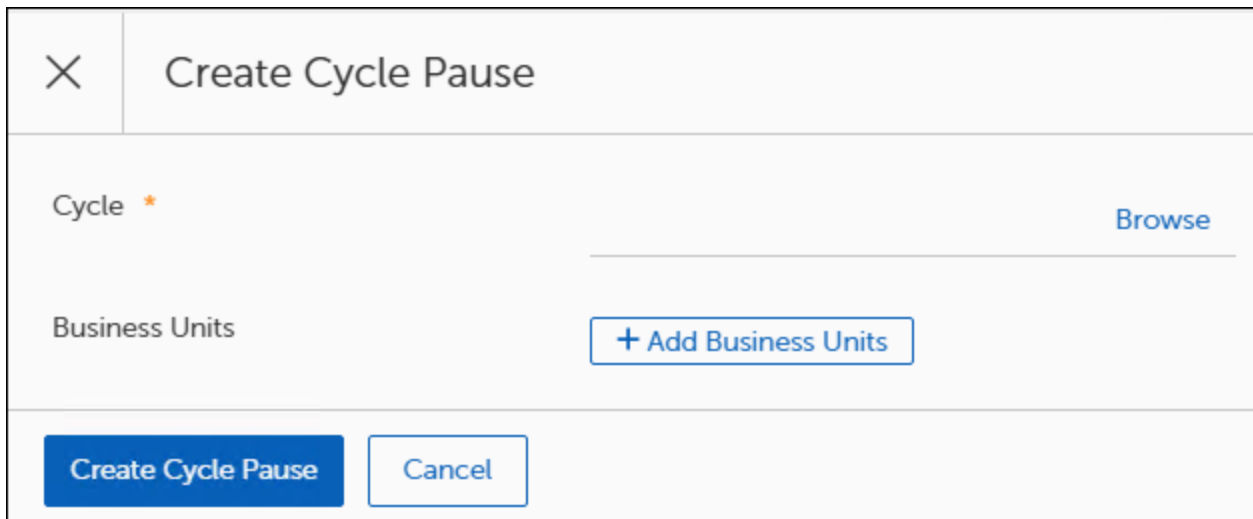
To stop all patching activity for a specific rollout cycle, complete the following steps:

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

This opens the Paused Cycles dialog to the Rollout tab:

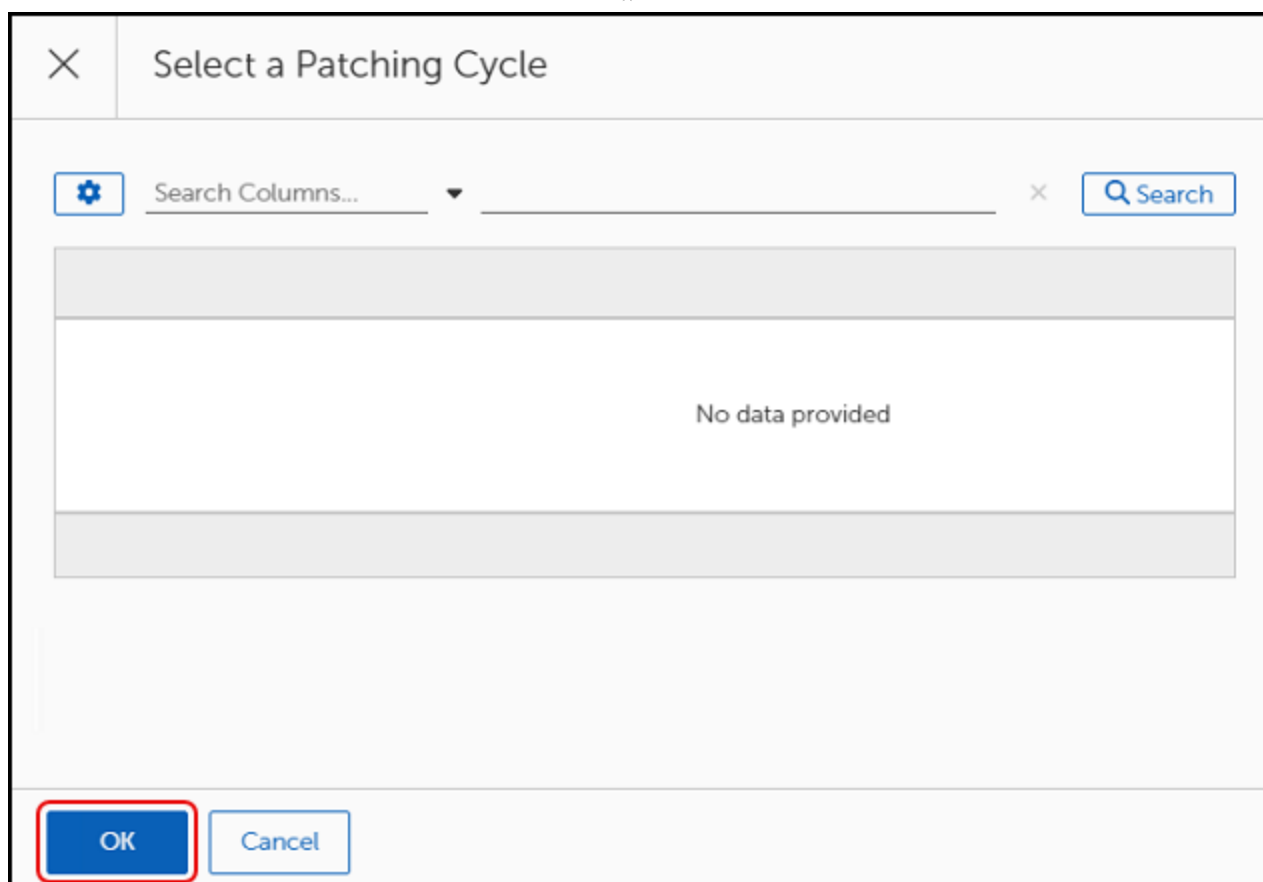


2. Select **+Create Cycle Pause**. This opens the Create Cycle Pause dialog:



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

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



×

Select a Patching Cycle

⚙ Search Columns... × 🔍 Search

No data provided

OK Cancel

- 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:

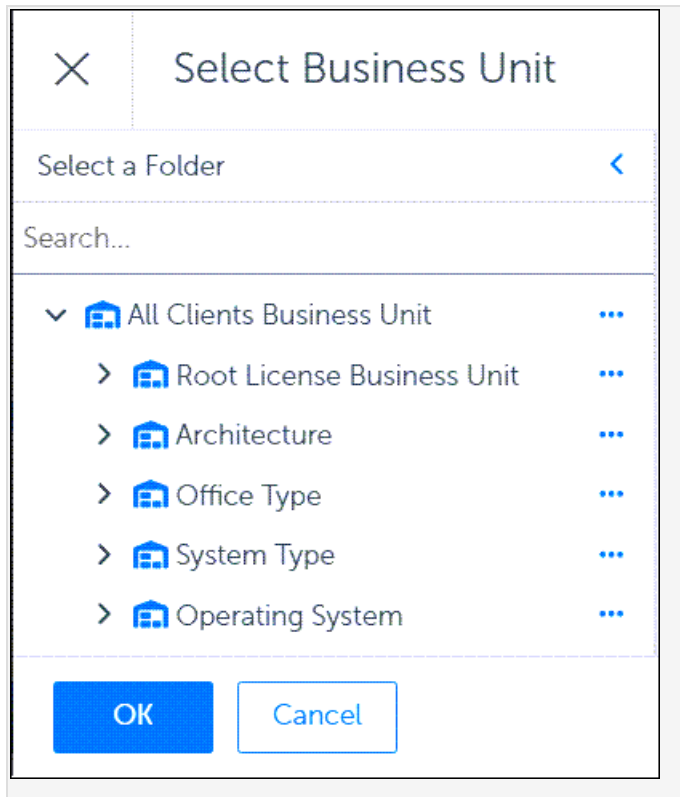
- To create a Global Pause for the selected cycle, skip to **Step 6**. This pauses the deployment of the selected software product on all devices in the estate.
- To specify a pause for specific devices, continue with the next step to **Add Business Units**.

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**.

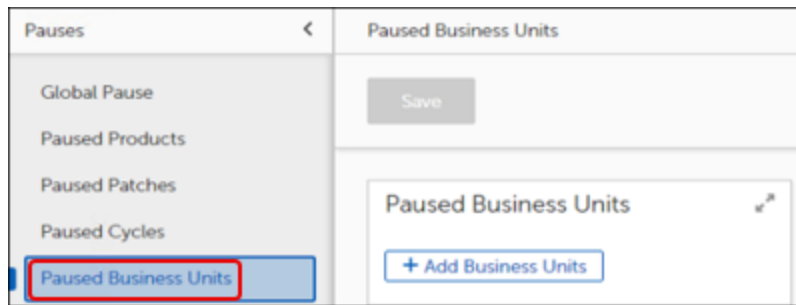
6. Select **Create Cycle Pause**, and then select **Save** to create a pause for the selected rollout cycle.

Pause Deployment to a Business Unit

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

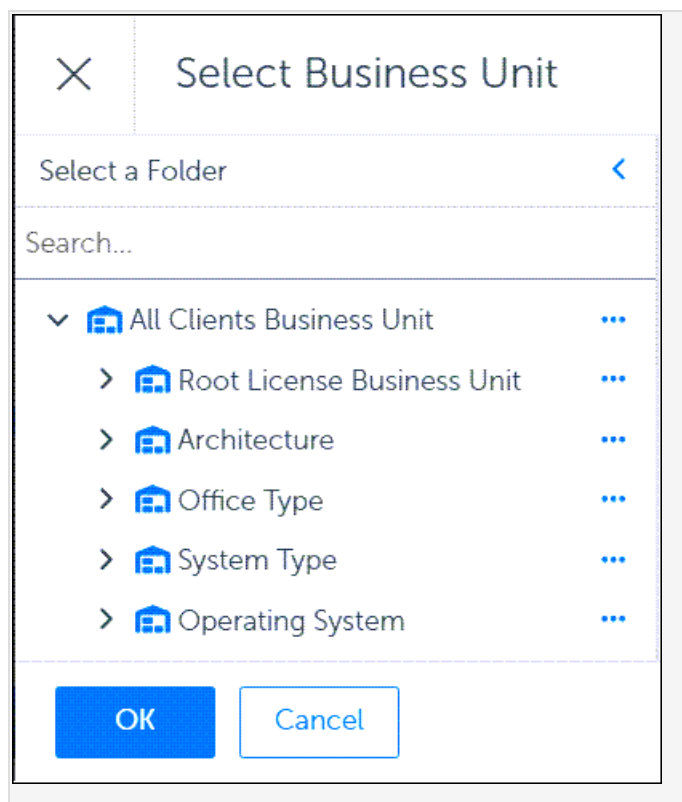
1. Navigate to the Pauses menu (see [Pause Patching for Specific Objects](#)), and then select **Paused Business Units**.

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 Tenable Patch Management Express 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.

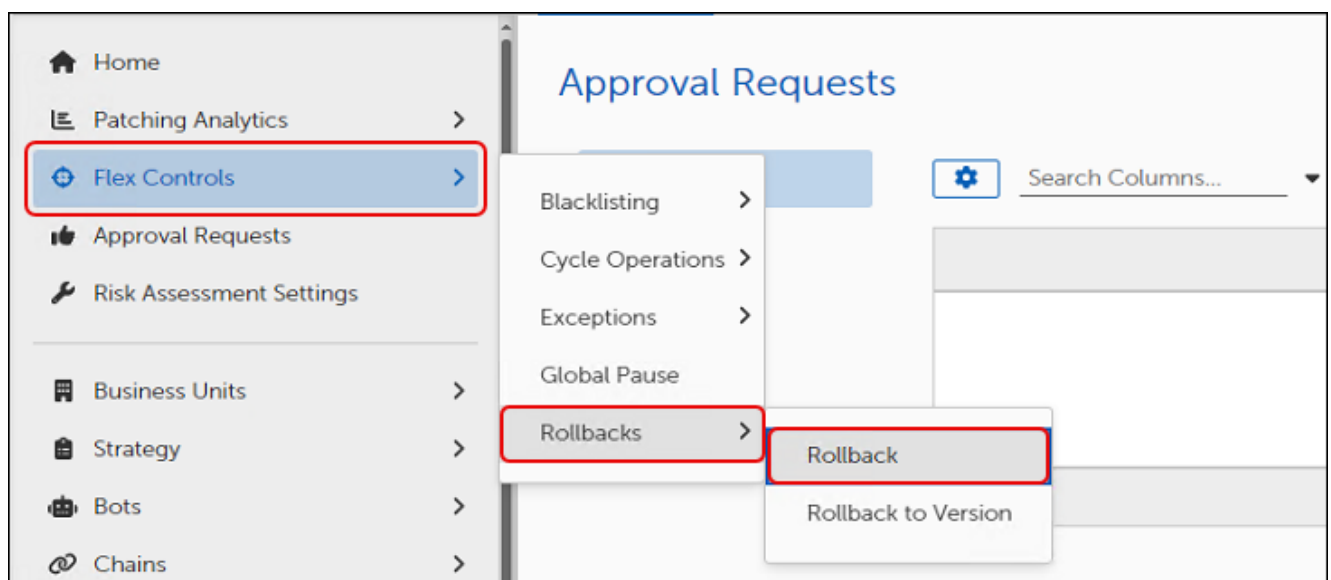
Rollback

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.

Patching Rollbacks

Show All + New

Search Columns...

×

Search

No data provided

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

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

▼

General Settings

Name *

Name

Description

Description

Patch ⓘ *

Add Installable Software

BROWSE

Target Business Units ⓘ *

+ Add Business Units

- 121 -

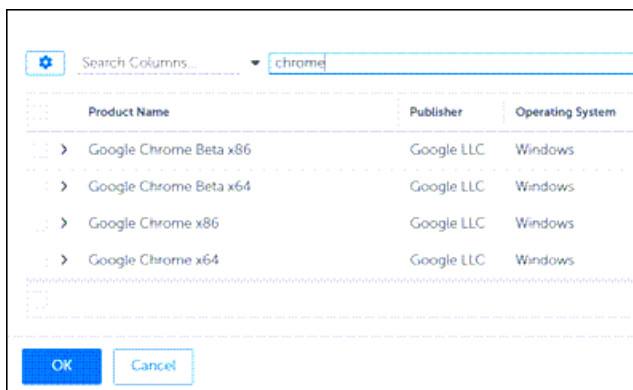


3. Locate the patch or release you want to roll back:



4. Select a Software patch or release:

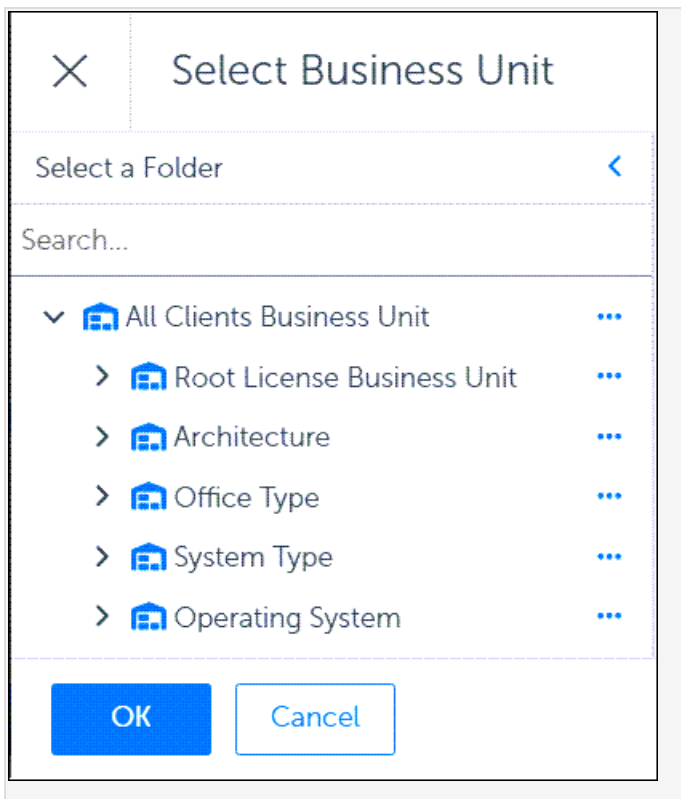
- a. Enter a product name in the search line, and then select **Search**. This example uses Google Chrome.
- b. Select the product from the list, and then select **OK**.



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



- a. Select the Business Units.



- b. Select **OK**.

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

Edit a Rollback Template

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

Patching Rollbacks

Show All + New

Search Columns...

Search

☐	...	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 ..	...
☐	...			

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. Modify the Rollback settings:

- Select **Browse** to choose a different patch or release to roll back.
- 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...

×

 Search

☐ ...	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 ...	

☐ ...

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

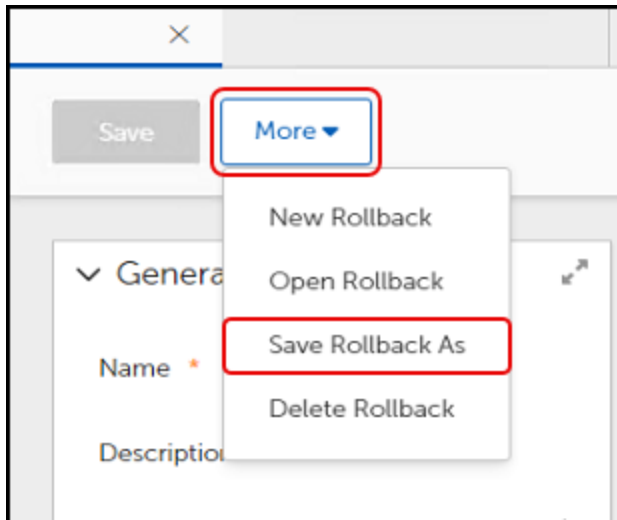
BROWSE ×

Target Business Units *

+ Add Business Units

☐	...	Name	Actions
☐		> Operating System	...

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

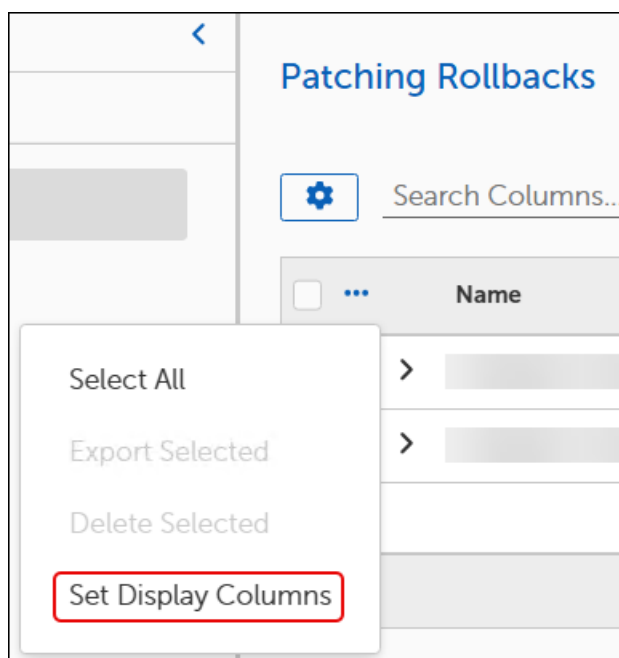


3. Enter a new **Name** for the template, and then select **Save as**.

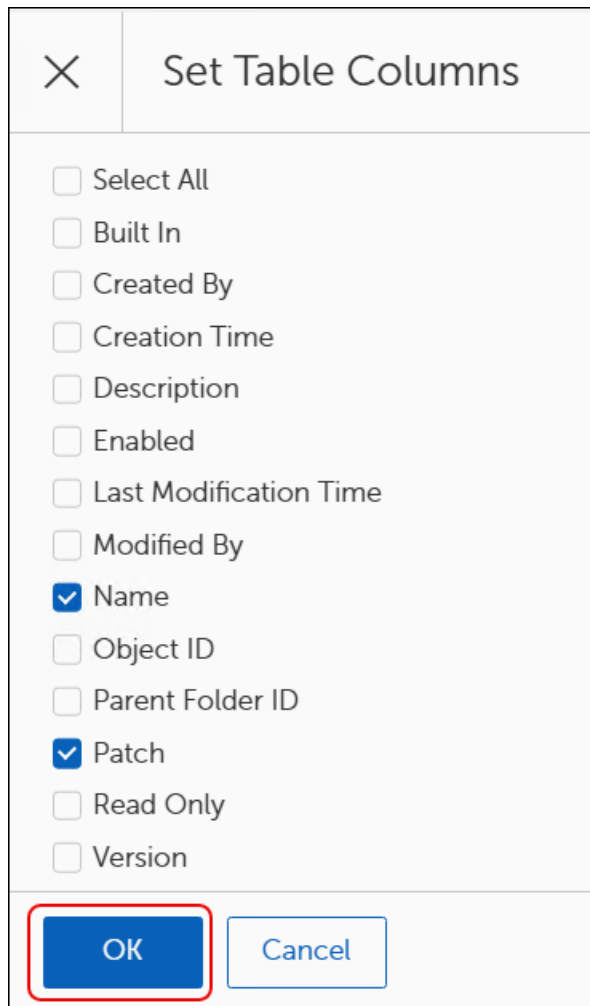
4. Revise the **Description** to reflect any changes needed for the copy, and then select **Save**.
5. Select **Back to Rollbacks** on the upper-left of the template to return to the Rollbacks table and view your changes.

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.



Set Table Columns

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

OK Cancel

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

Delete a Rollback

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

Patching Rollbacks

Show All + New

Search Columns...

×

Search

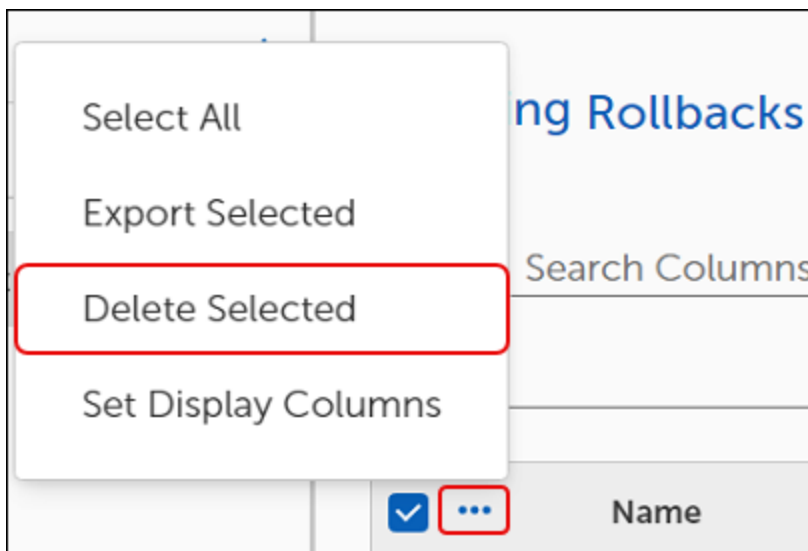
☐	...	Name	Patch	Actions
☒	⋮	> Windows	.NET 3.5 Feature on Demand for X64	⋮
☐	⋮	> Windows Rollback	.NET 3.5 Feature on Demand for X86	⋮
☐	⋮	> Windows Update	2017-05 Security Monthly Quality Rollup for Windows Server 2012 for ..	⋮
☐	⋮			

Rows Per Page: 10

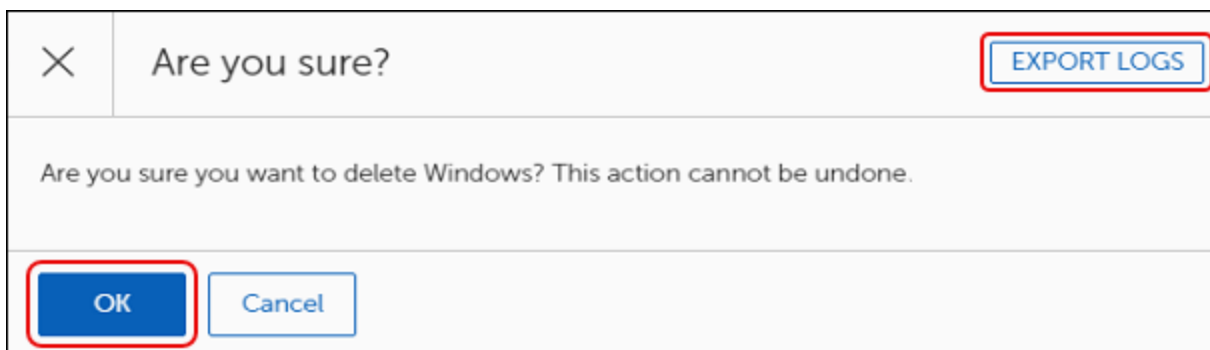
1 - 3 of 3

1 / 1

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



- Review the Are you sure? dialog:

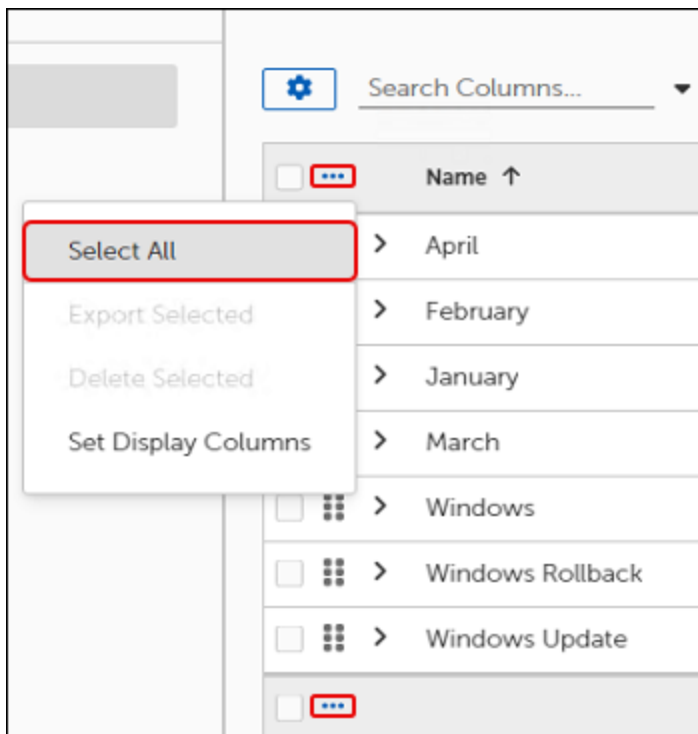




- a. Select **Export Logs** on the upper-right of the Are you sure? dialog to export trace logs. The trace logs download to your device as a file with a .log extension.
 - b. Select **OK** to delete the Rollback.
4. Select **Back to Rollbacks** on the upper-left of the template to return to the Rollbacks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

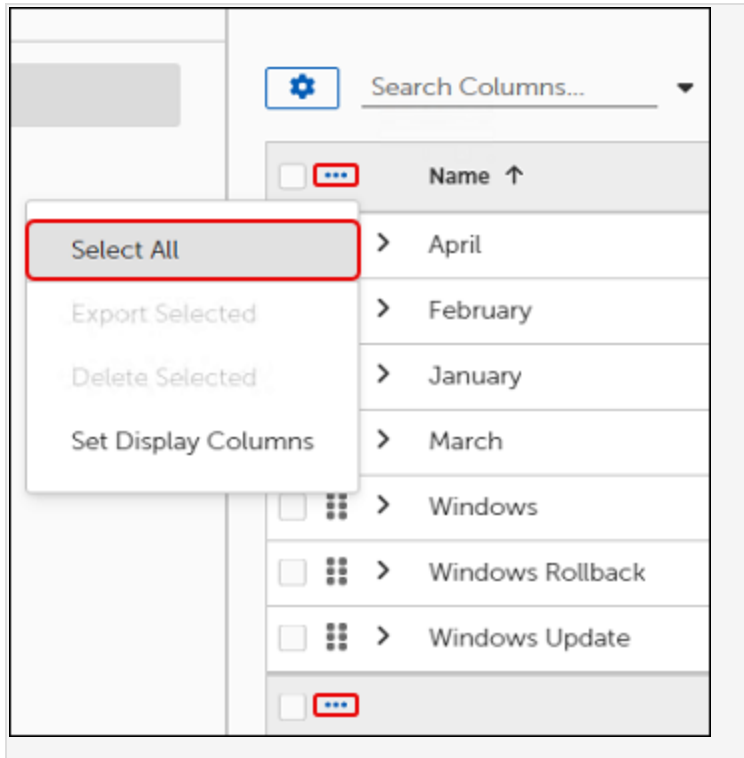


3. Select the ellipsis (...) again, and then choose what you want to do with the selected Rollbacks:
 - To export the selected Rollbacks, see [Select All Rollback to Version Objects](#).
 - To delete the selected templates, see [Bulk Delete Rollbacks](#).
 - To customize the display columns of the Patching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

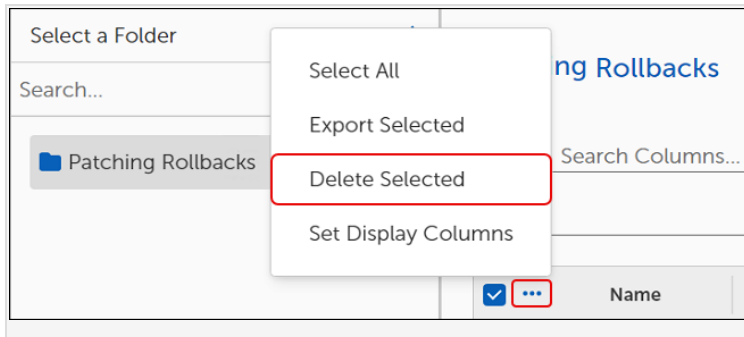
Bulk Delete Rollbacks



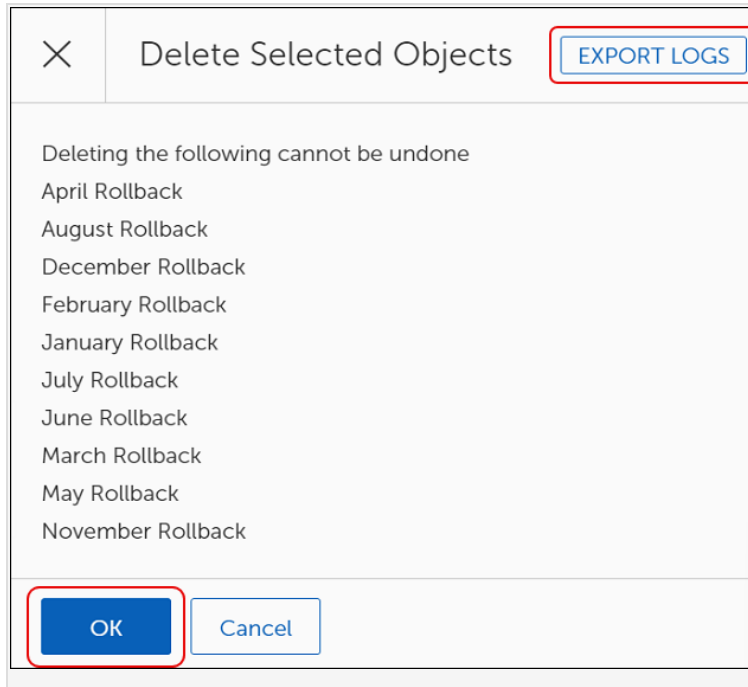
1. Open the **Patching Rollbacks** table (Flex Controls > Rollbacks > Rollback).
2. Select the **ellipsis (...)** next to Name, and then select **Select All**.



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



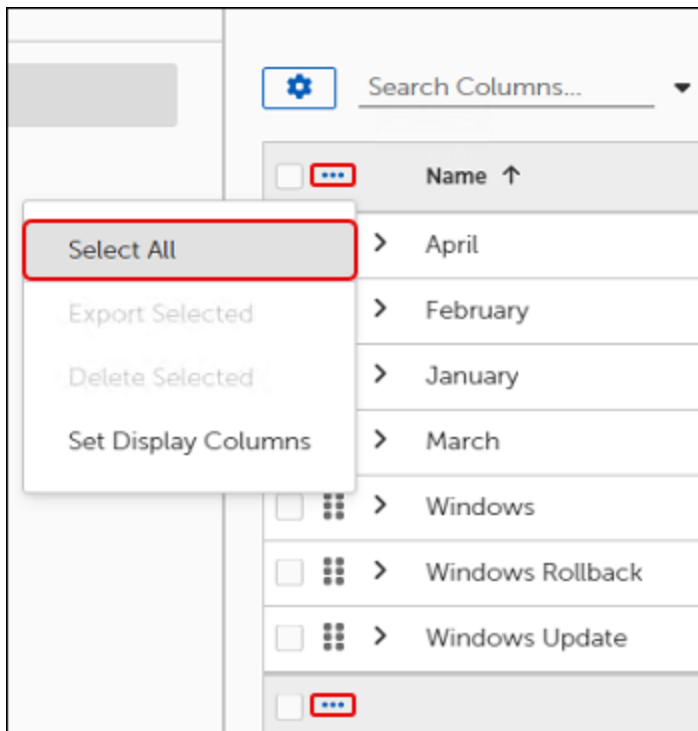
This opens the Delete Selected Objects dialog:



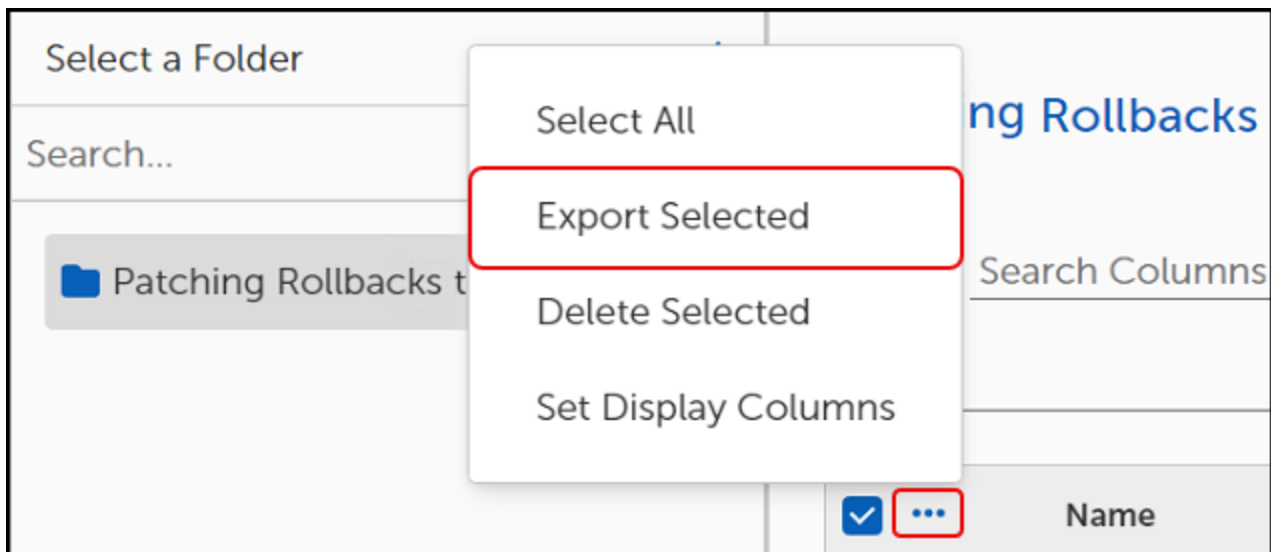
4. (Optional) Select **Export Logs** on the top-right corner of the Delete Selected Objects dialog to export trace logs. The trace logs download to your device as a file with a .log extension.
5. Select **OK** to delete the Rollbacks. This returns you to the **Patching Rollbacks** table where the deleted 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:



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

Object Export Settings

Exporting Organization

Exporting Organization Name

Description

Description

Export as JSON

☐

Automatically Import
Objects Into the
Specified Folder

☐

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

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

Show Rollback References

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

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

Patching Rollbacks

Show All

+ New

Search Columns...

Search

	Name	Patch	Actions
☐	> April Rollback	.NET 3.5 F...	...
☐	> August Rollback		
☐	> December Rollback		
☐	> February Rollback	.NET 3.5 F...	...

Show References

Export

This opens the [Rollback Name] Object References dialog.

×

December Rollback Object References

√

Root

√

Folder

Folder

Patching Rollbacks

OK

3. Select the **caret** next to 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

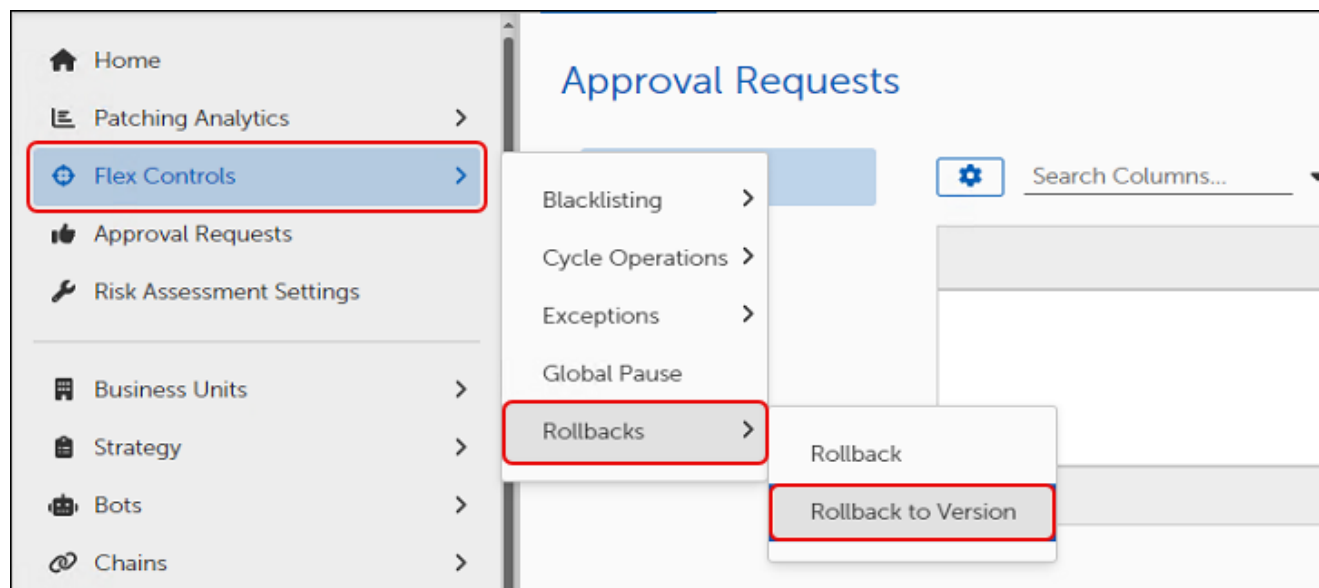


Use the Rollback to Version template to rollback a patch or release to a specific release or version. To rollback to the previous version, see [Rollback](#).

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.

Patching Rollbacks to Version

Show All

+ New

Search Columns...

×

Search

No data provided

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

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

▼

General Settings

Name *

Name

Description

Description

Patch

i

*

Add Installable Software

BROWSE

Rollback

i

*

Add Installable Software

BROWSE

Target Business Units

i

*

+ Add Business Units

3. Enter a **Name** and a detailed **Description** of your Rollback to Version.

- 138 -

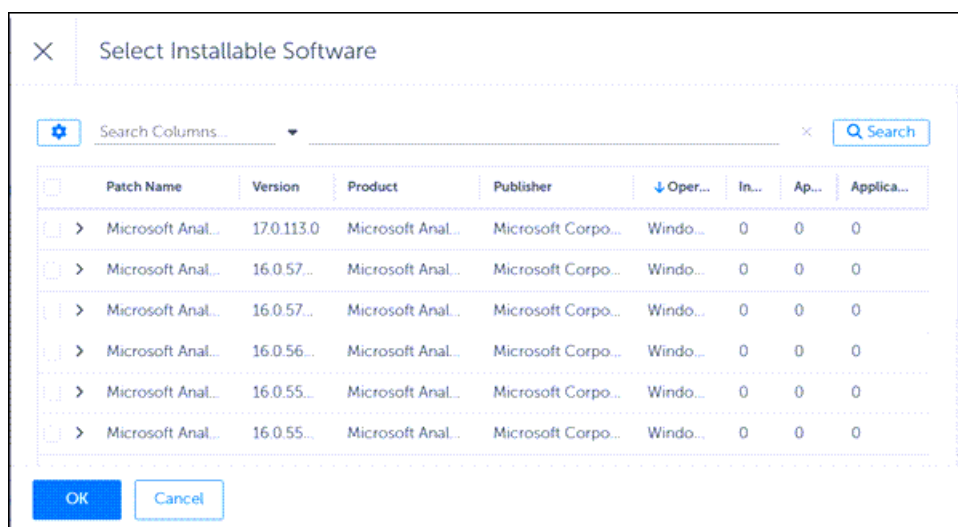
4. [Add the patch or release to roll back from.](#)

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](#).



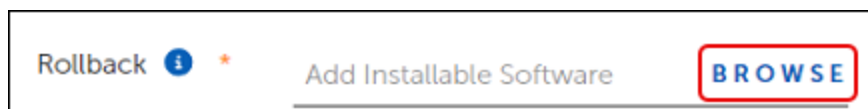
2. Choose the **Software Patch** or **Software Release** from the Add Installable Software table to roll back from. You can select only one Patch or Release to roll back from.



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.](#)

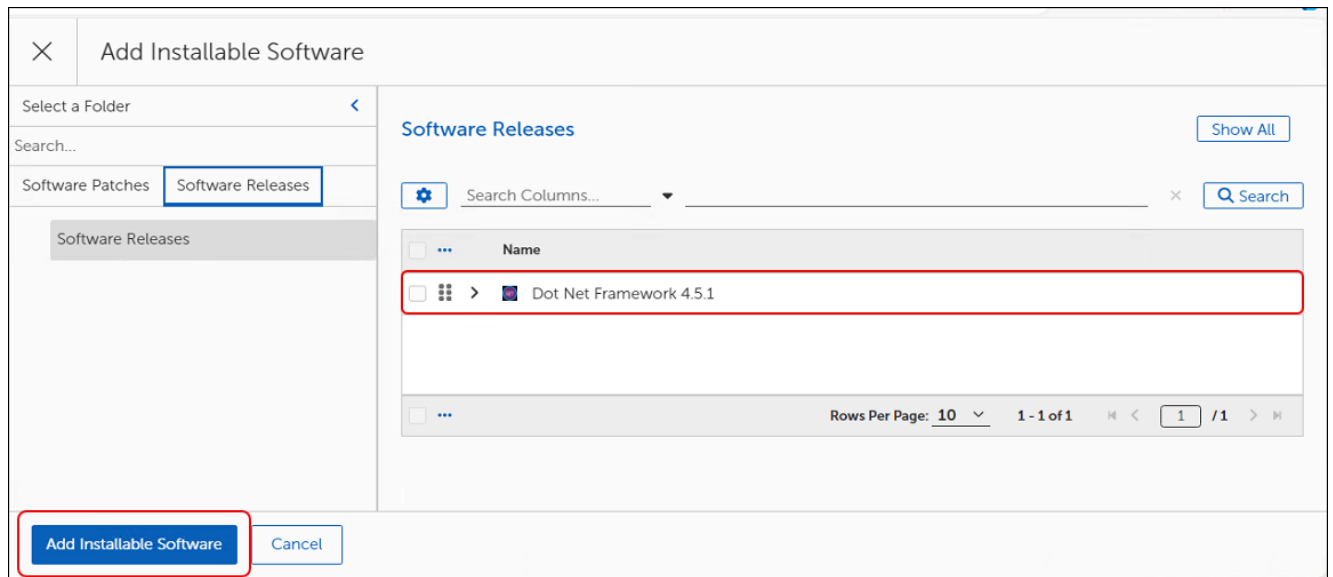
Choose the Software Patch or Release Version to Roll Back To

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.



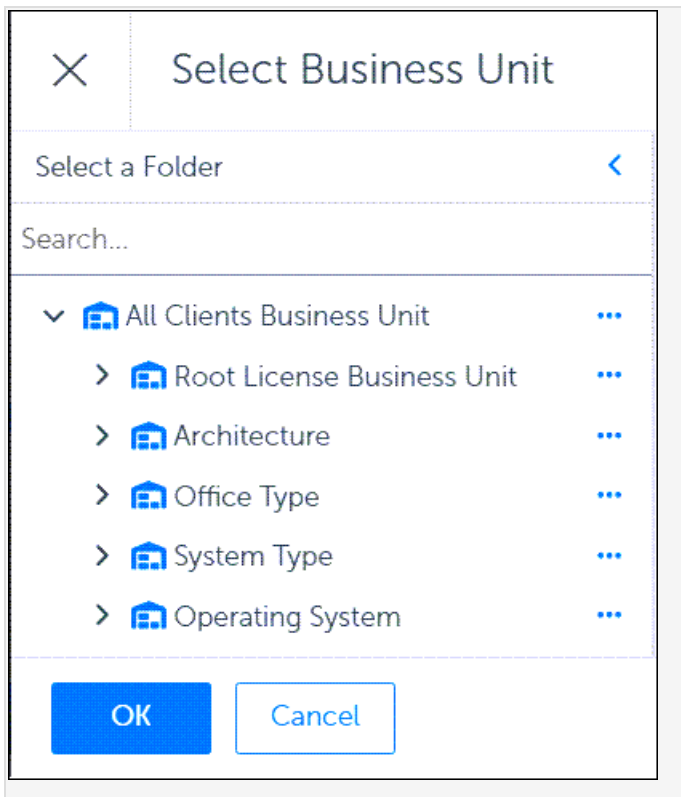
3. Select **Add Installable Software**.
4. [Add target Business Units for the Rollback to Version.](#)

Add Business Units for a Rollback to Version



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

1. Select the Business Units.



2. 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...

×

Search

☐	...	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 ..	...
☐	...			

Rows Per Page: 10

1 - 3 of 3

1 / 1

This opens the template.

▼

General Settings

Name *

Name

Description

Description

Patch ⓘ *

Add Installable Software

BROWSE

Rollback ⓘ *

Add Installable Software

BROWSE

Target Business Units ⓘ *

+ Add Business Units

2. Modify the Rollback settings:

- Select **Browse** for Patch to choose a patch or release to roll back from.
- Select **Browse** for Rollback to choose the version of the patch or release to roll back to.
- 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 1...	Visual S...	⋮

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

This opens the template.

General Settings

Name *

Visual Studio

Description

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

Patch ⓘ *

Visual Studio 2017 version 15.9.62 update

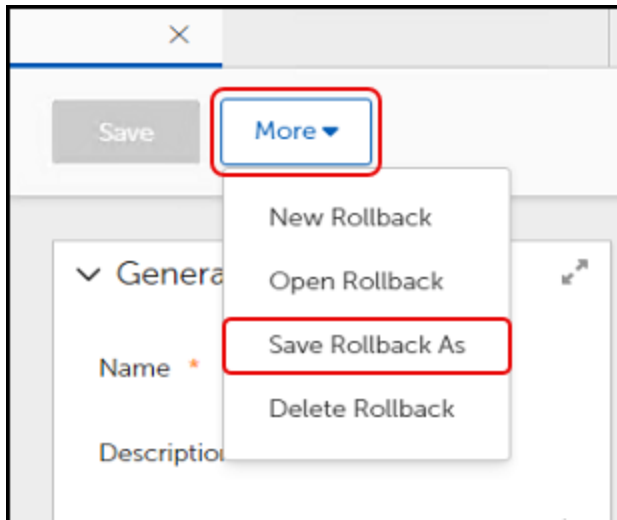
BROWSE ✕

Rollback ⓘ *

Visual Studio 2017 version 15.9.54 update

BROWSE ✕

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

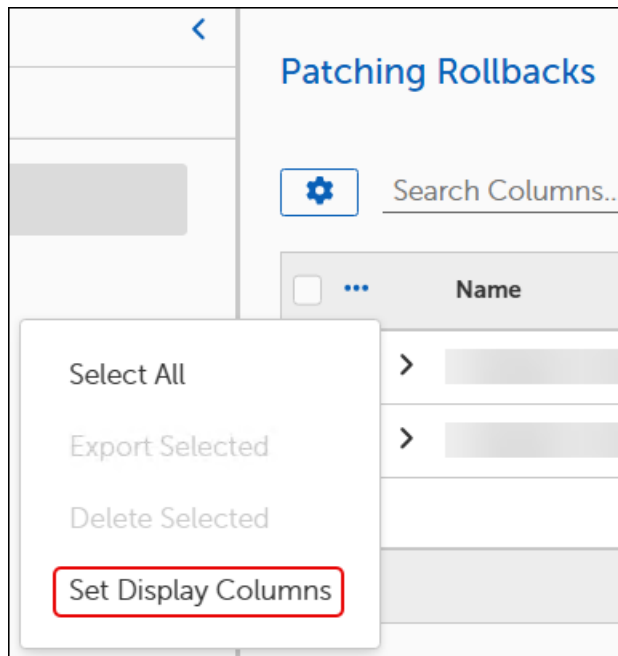


3. Enter a new **Name** for the template, and then select **Save as**.

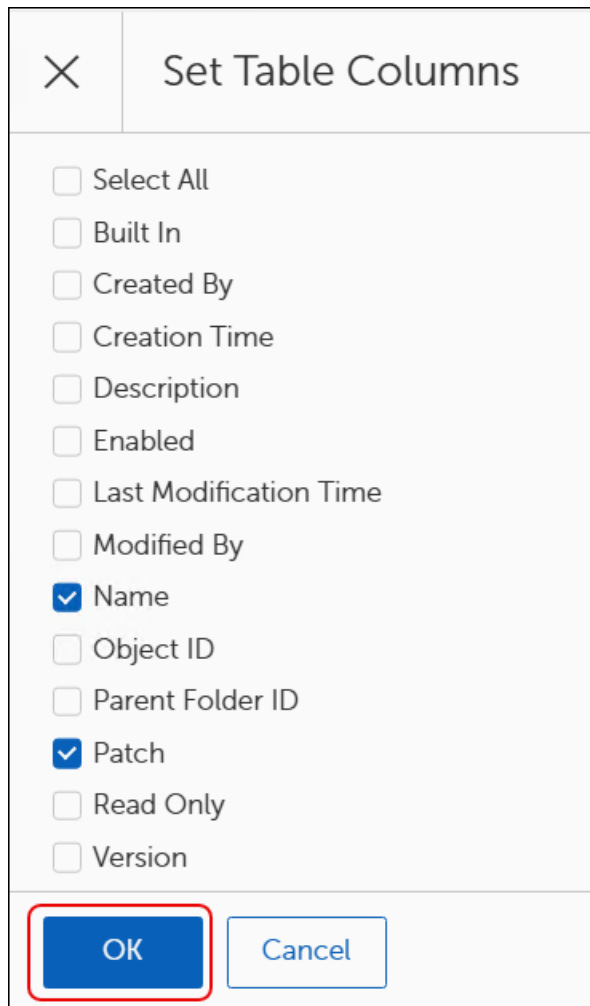
4. Revise the **Description** to reflect any changes needed for the copy, and then select **Save**.
5. Select **Back to Rollbacks** on the upper-left of the template to return to the Rollbacks table and view your changes.

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.



Set Table Columns

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

OK Cancel

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

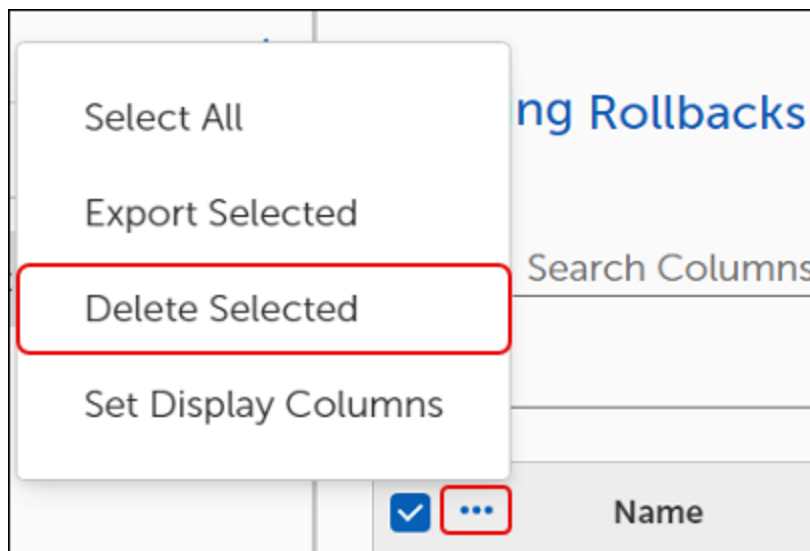
Patching Rollbacks to Version Show All + New

Search Columns... Search

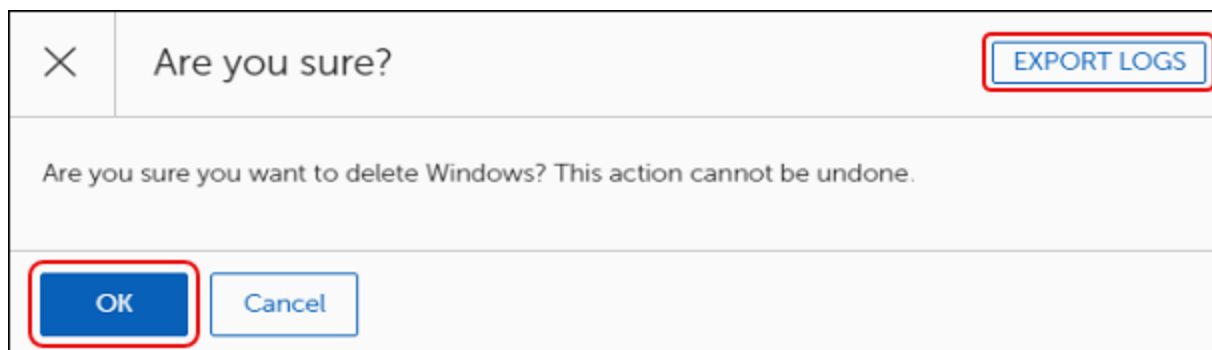
☐	Name	Patch	Actions
☒	> Windows	.NET 3.5 Feature on Demand for X64	...
☐	> Windows Rollback	.NET 3.5 Feature on Demand for X86	...
☐	> Windows Update	2017-05 Security Monthly Quality Rollup for Windows Server 2012 for ..	...

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

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



- Review the Are you sure? dialog:

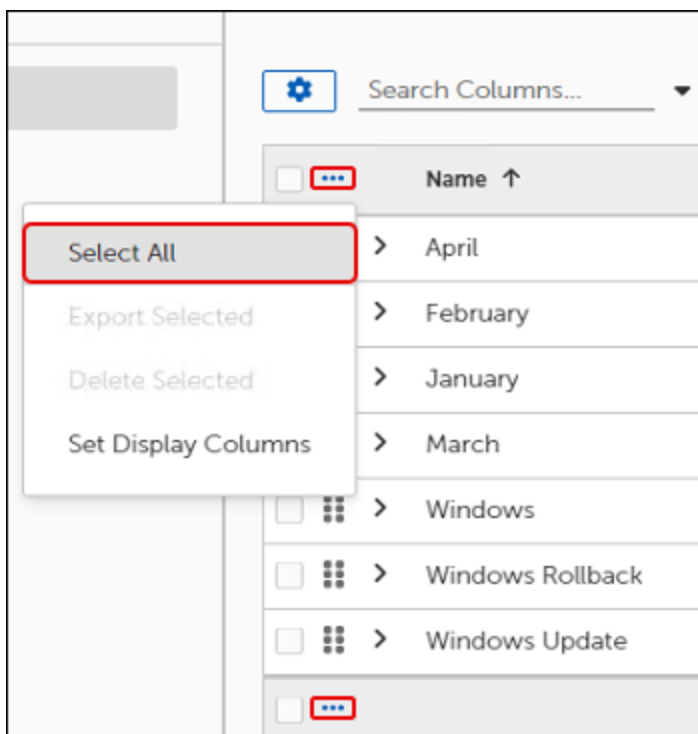




- a. Select **Export Logs** on the upper-right of the Are you sure? dialog to export trace logs. The trace logs download to your device as a file with a .log extension.
 - b. Select **OK** to delete the Rollback.
4. Select **Back to Rollbacks** on the upper-left of the template to return to the Rollbacks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



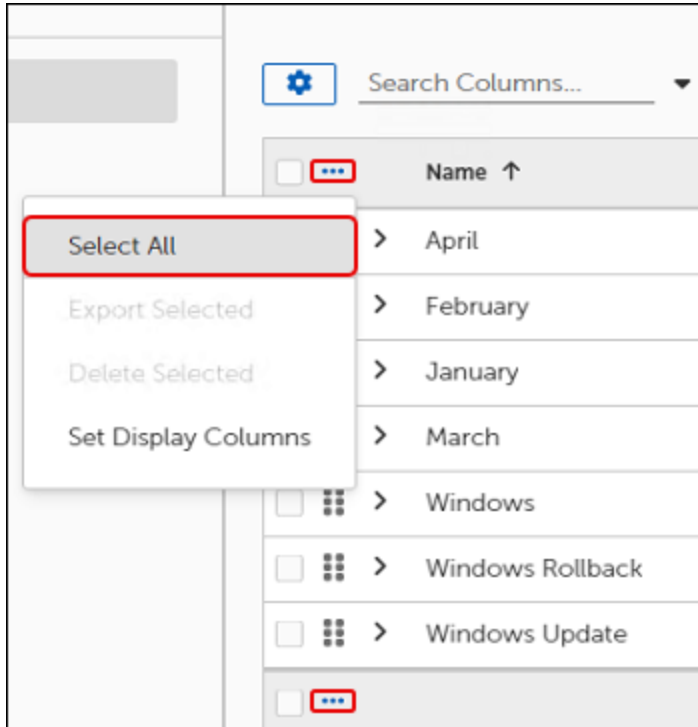
3. Select the ellipsis (...) again, and then choose what you want to do with the selected Rollbacks:
 - To export the selected Rollbacks, see [Select All Rollback to Version Objects](#).
 - To delete the selected templates, see [Bulk Delete Rollbacks](#).
 - To customize the display columns of the Patching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

Bulk Delete Rollback to Version

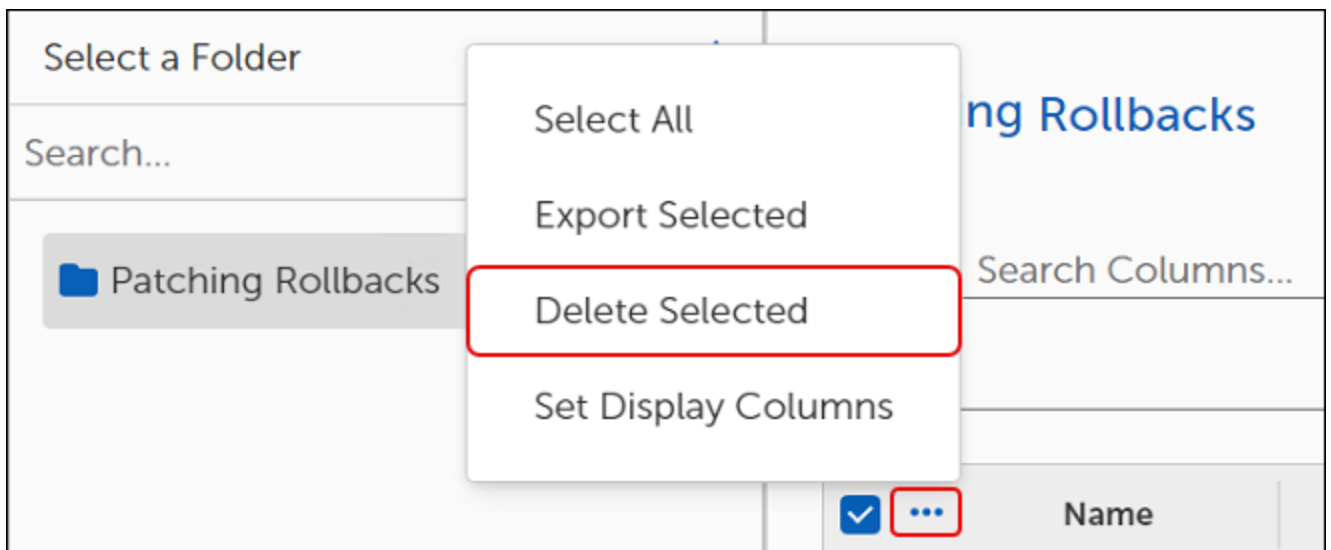


Use the following task to delete all Rollback to Version templates.

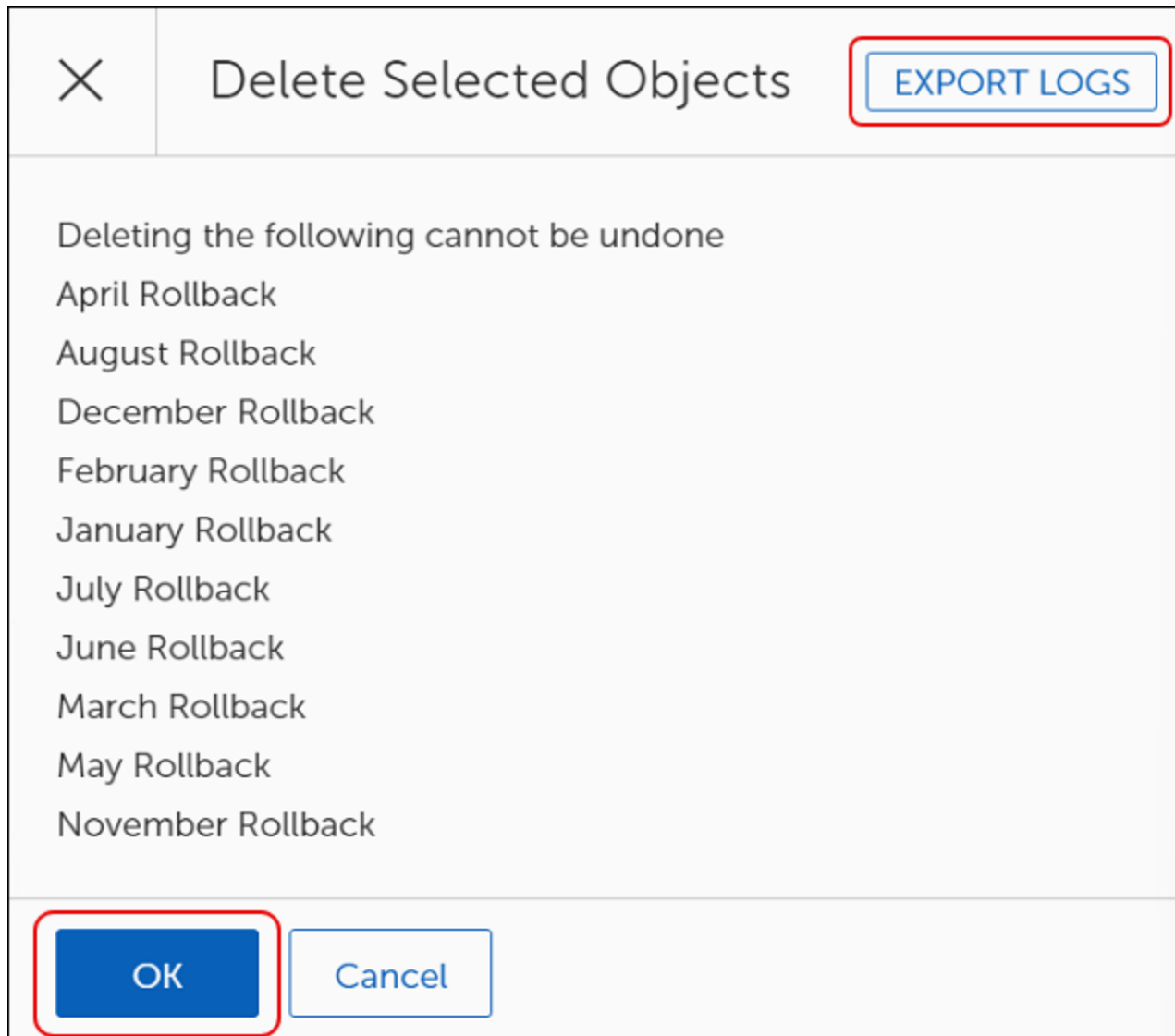
1. Open the **Patching Rollbacks** table (**Flex Controls > Rollbacks > Rollback to Version**).
2. Select the **ellipsis (...)** next to Name, and then select **Select All**.



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



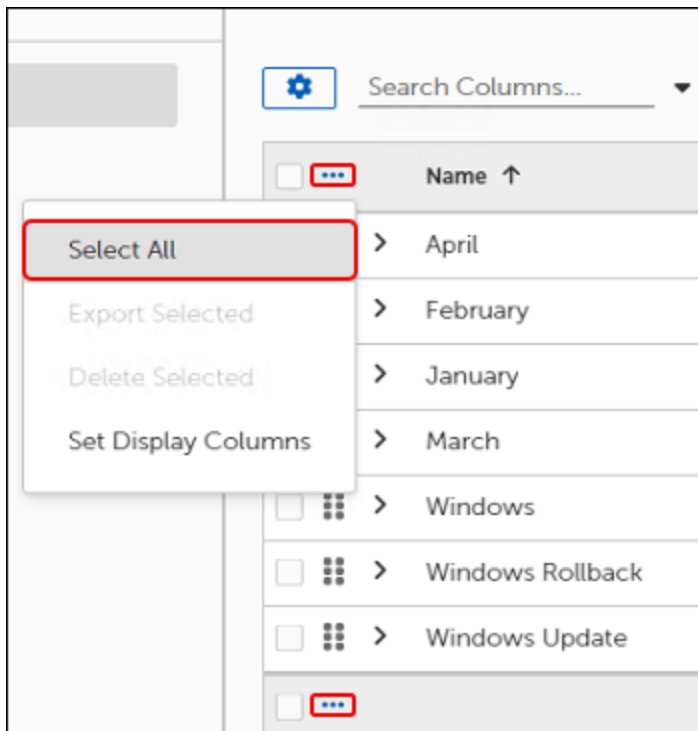
This opens the Delete Selected Objects dialog:



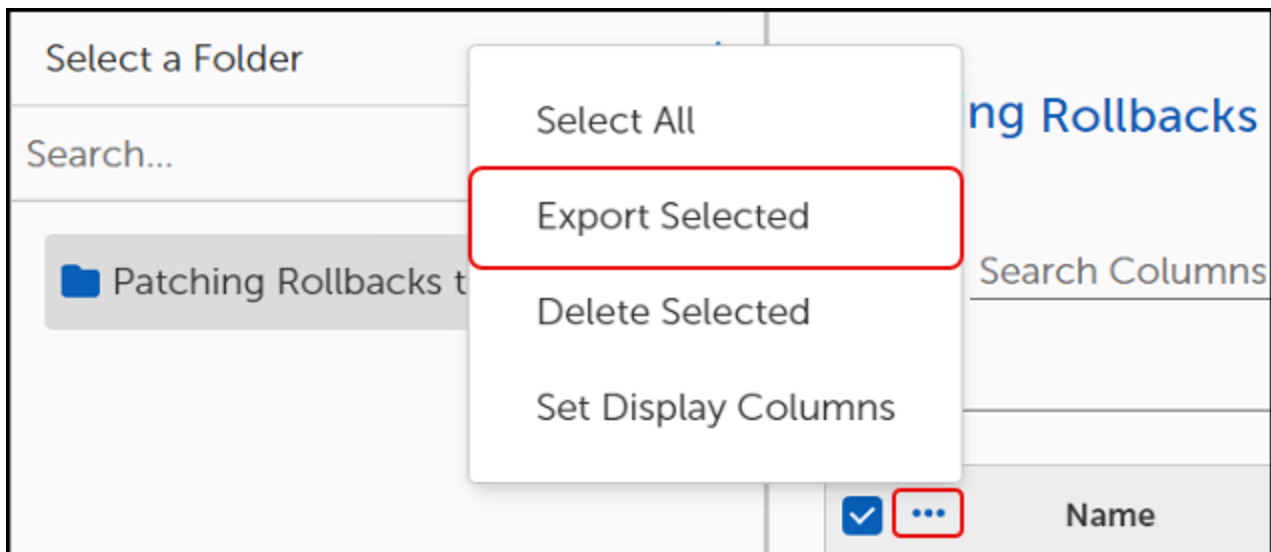
4. (Optional) Select **Export Logs** on the top-right corner of the Delete Selected Objects dialog to export trace logs. The trace logs download to your device as a file with a .log extension.
5. Select **OK** to delete the Rollbacks. This returns you to the **Patching Rollbacks to Version** table where 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:



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

Object Export Settings

Exporting Organization

Exporting Organization Name

Description

Description

Export as JSON

☐

Automatically Import
Objects Into the
Specified Folder

☐

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

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

Show Rollback to Version References

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

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

Patching Rollbacks to Version

Show All

+ New

Search Columns...

Search

☐	...	Name	Patch	Actions
☐		> April Rollback	.NET 3.5 F...	...
☐		> August Rollback		
☐		> December Rollback		
☐		> February Rollback	.NET 3.5 F...	...

Show References

Export

This opens the [Rollback Name] Object References dialog.

×

December Rollback Object References

√

Root

√

Folder

Patching Rollbacks

OK

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

Approval Requests



Some Patching Strategies require patch manager approval before beginning a patch cycle. The Patching Process looks for an Approval Chain to use when processing approvals and sends 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:

Approval Requests

All

Search Columns

Search

Pending

Completed

Approval Summary	Request Send To	Scope Object	Request Status	Your Response	Actions
> Patching Process Appr...	3/23/25, 1:58 PM	Enabled Patching Strategy Ch...	In Progress	Awaiting response	...
> Patching Process Appr...	3/21/25, 8:32 AM	Enabled Patching Strategy Ch...	Completed, Approved	Approved	...

Rows Per Page: 101 - 2 of 2View

- 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.

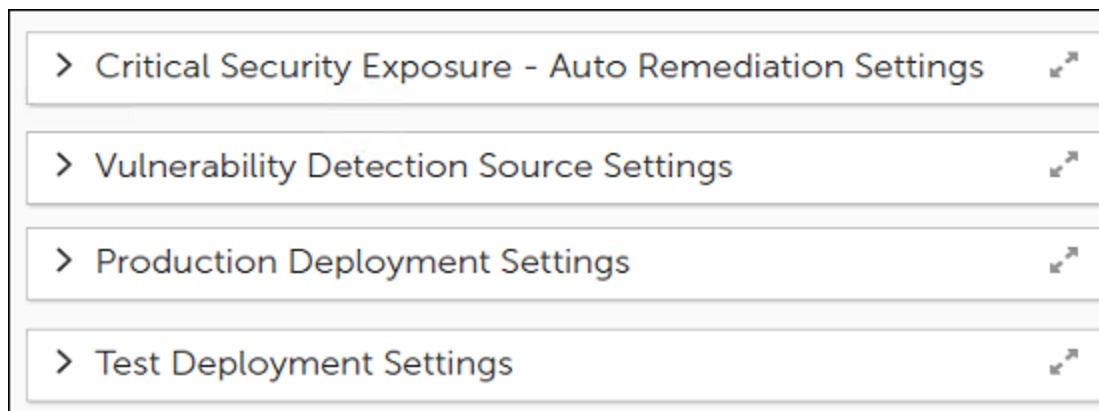
Auto Remediation

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.

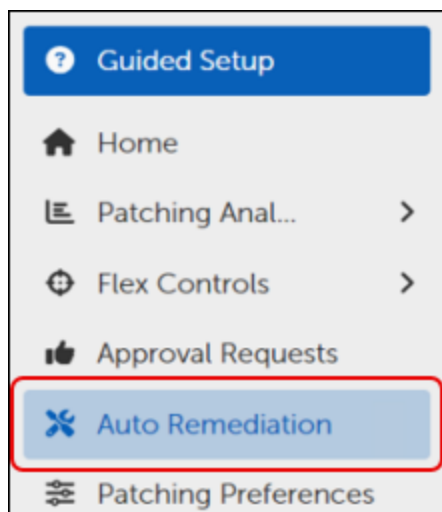
Tenable includes the following configuration options for Auto Remediation:



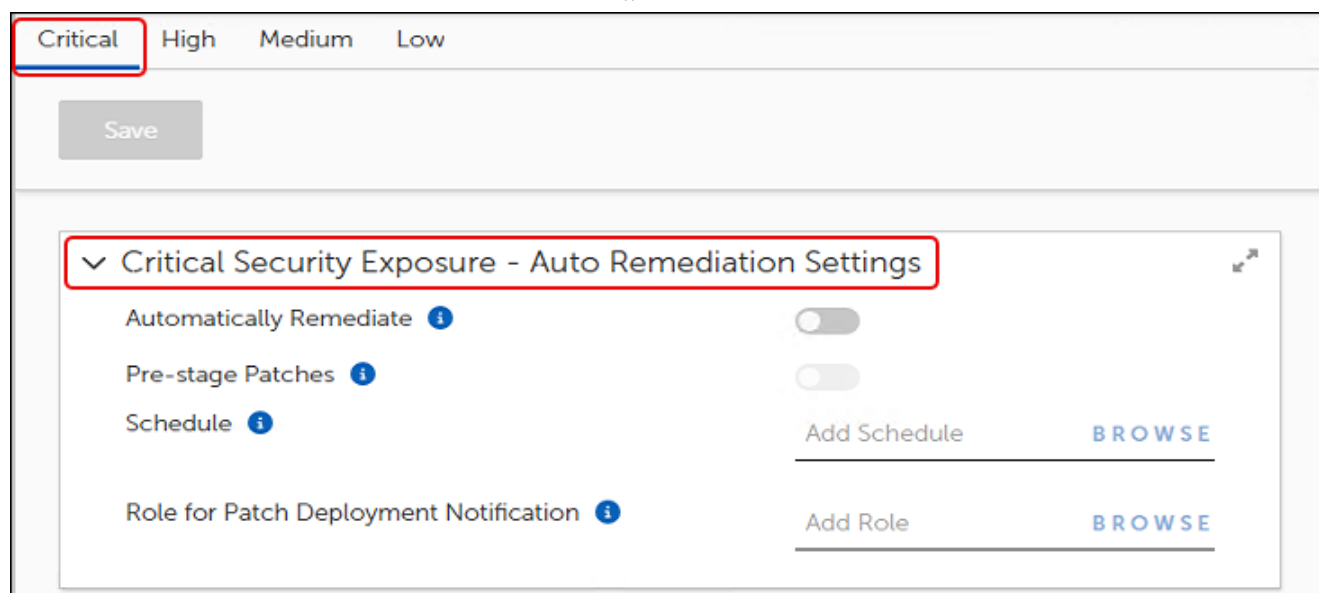
Tenable provides configuration options for Critical, High, Medium, or Low Security Exposure Levels.

Access Auto Remediation and Deployment Settings

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



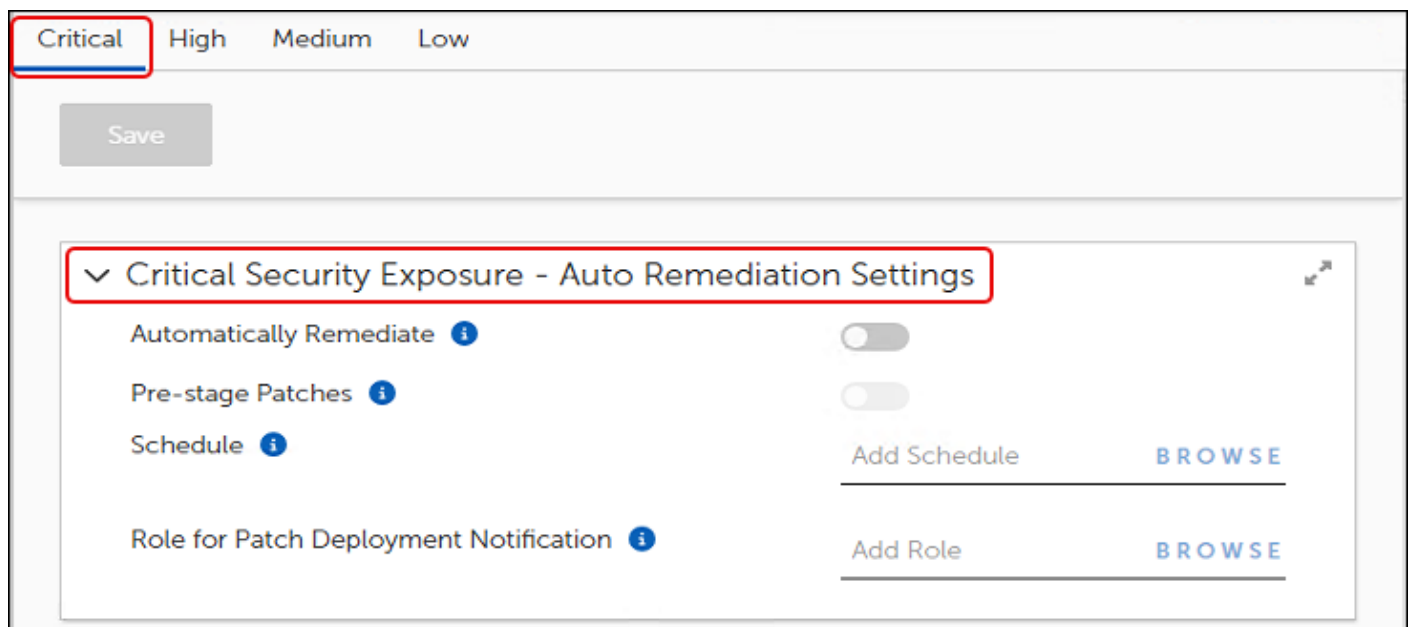
This opens the Auto Remediation workspace, which defaults to the Critical exposure level settings.



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

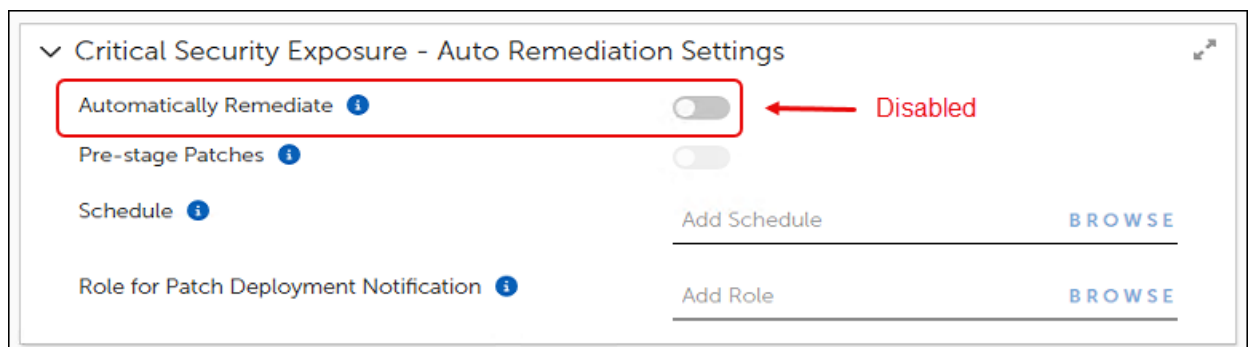
Enable automatic remediation to automatically correct all issues associated with a security level. With Auto Remediation enabled, you can also enable pre-staging of patches, which downloads the content to devices as soon as the patch becomes available. This makes the patch content available on the devices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



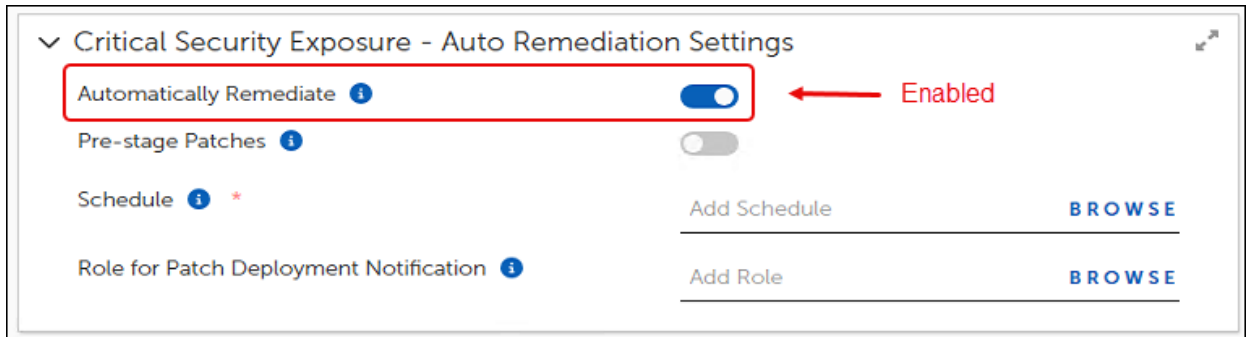
Additional settings include adding a schedule to begin the remediation process and identifying roles that receive notification of the deployment. Repeat the Auto Remediation steps for each urgency level that will use auto remediation. At any time during these configuration steps, click **Save** on the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



✓ Critical Security Exposure - Auto Remediation Settings

Automatically Remediate ⓘ ☒ ← Enabled

Pre-stage Patches ⓘ ☐

Schedule ⓘ * [Add Schedule](#) [BROWSE](#)

Role for Patch Deployment Notification ⓘ [Add Role](#) [BROWSE](#)

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.

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

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

Schedules [Show All](#) [+ Create Schedule](#)

⚙️ Search Columns... × 🔍 Search

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

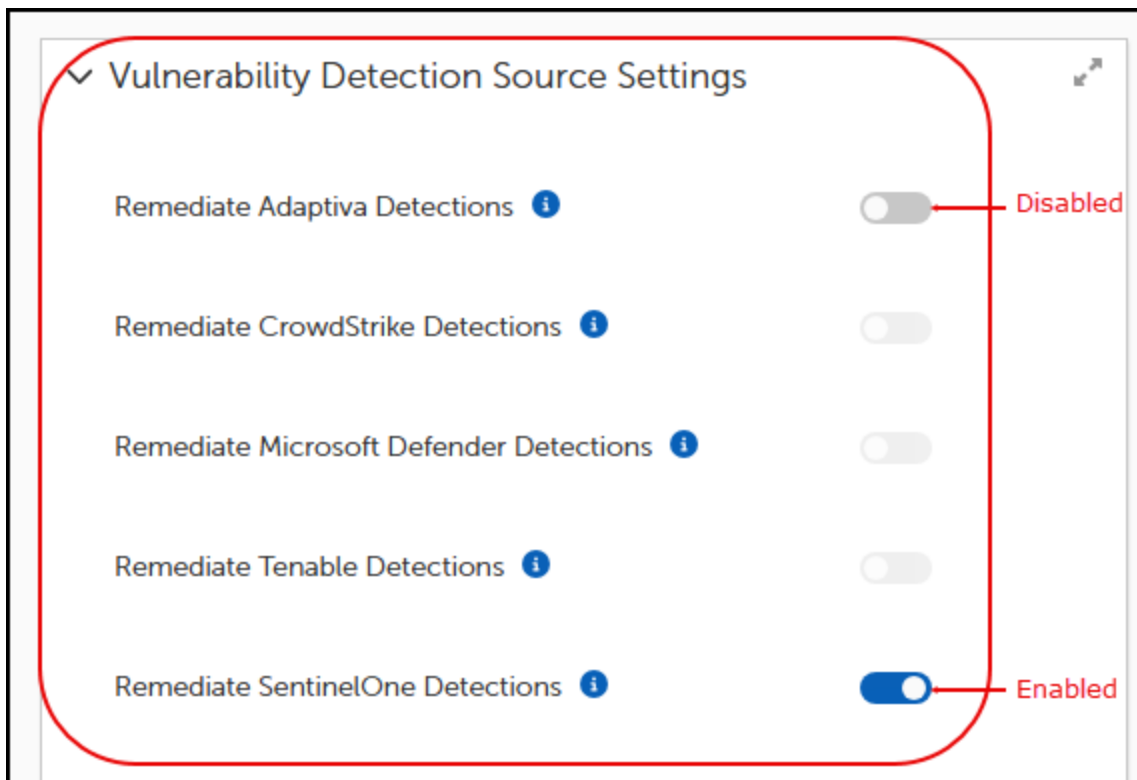
Rows Per Page: 10 1 - 10 of 12 1 / 2



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

Vulnerability Detection Source Settings

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



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

Production Deployment Settings for Auto Remediation



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

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

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

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

Test Deployment Settings for Auto Remediation

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

✓ Test Deployment Settings

Deploy to Test Group First i

Business Unit for Test Deployment i *

Add Business Unit

BROWSE

Test Deployment Duration i

0

Days

0

Hours

0

Minutes

Role for Test Deployment Approval i

Add Role

BROWSE

Time Until Automatic Test Deployment Approval i

0

Days

0

Hours

0

Minutes

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



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

Verify that Auto Remediation Works as Expected

1. Select **Home** on the left navigation menu of the [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.

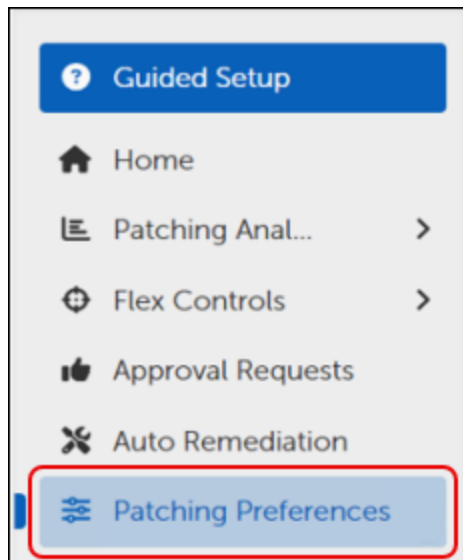
Using Patching Preferences



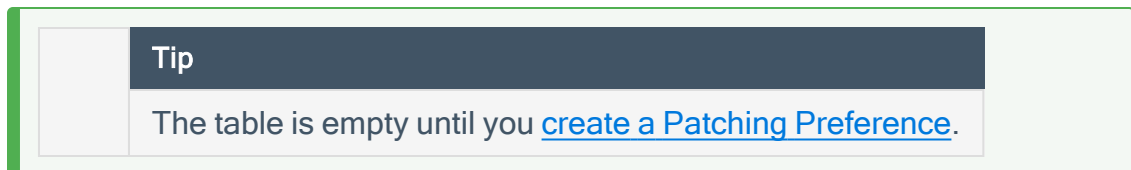
Administrators can set preferences for Maintenance Window and User Interaction Settings and apply those preferences to a specific Business Unit. In Patching Preferences, you may set preferences for either a Maintenance Window or for Server User Interaction Settings, or both.

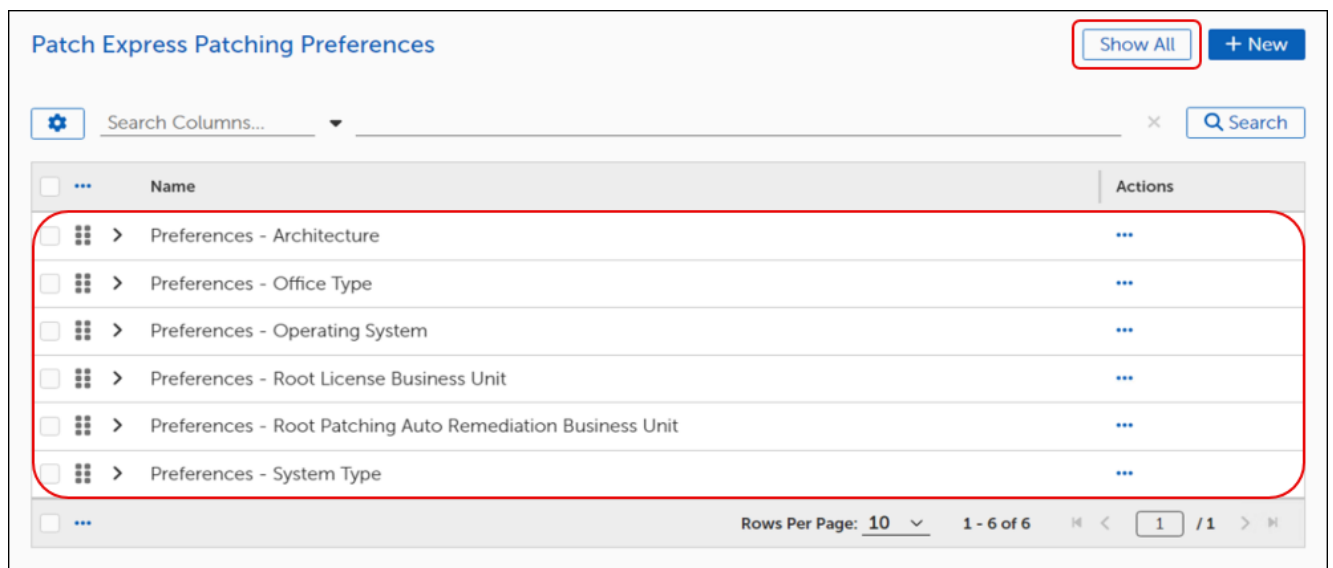
Access Patching Preferences

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



This opens the Patch Express Patching Preferences dialog.





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.

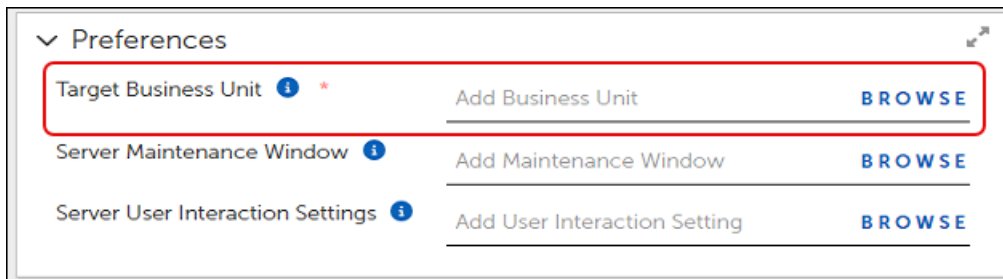
1. In an open Patching Preferences template (**+ New**), enter a Description of the preference you are creating. The system automatically generates a Name based on the target Business Unit.
2. When you finish modifying and saving the new patching preferences, click **Save** at the upper-left corner of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

Add a Target Business Unit

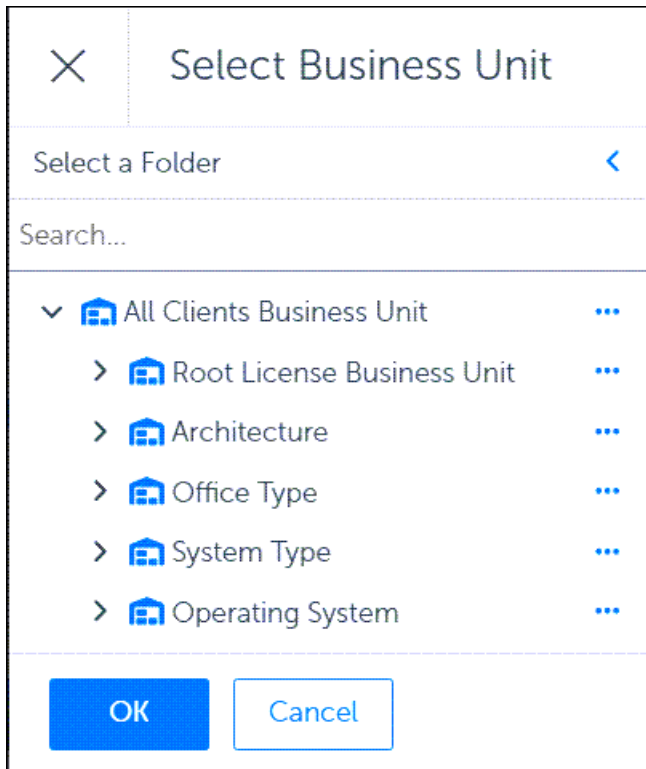
Add a Target Business Unit using the following steps:



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**.

Preferences

Target Business Unit ⓘ * Add Business Unit **BROWSE**

Server Maintenance Window ⓘ Add Maintenance Window **BROWSE**

Server User Interaction Settings ⓘ Add User Interaction Setting **BROWSE**

This opens the Add Maintenance Window dialog.

✕ Add Maintenance Window

Select a Folder <

Search...

▼ Maintenance Windows

■ All Urgencies

Maintenance Windows

⚙ Search Columns... × 🔍 Search

Show All + Create Maintenance Window

	Name
☐	> 00:00 - 03:00
☐	> 00:00 - 06:00
☐	> 00:00 - 09:00
☐	> 02:00 - 04:00
☐	> 02:00 - 06:00
☐	> 02:00 - 08:00
☐	> 08:00 - 12:00 and 14:00 - 18:00
☐	> 08:00 - 18:00
☐	> 09:00 - 12:00 and 14:00 - 17:00
☐	> 09:00 - 17:00

Rows Per Page: 10 1 - 10 of 16 1 / 2

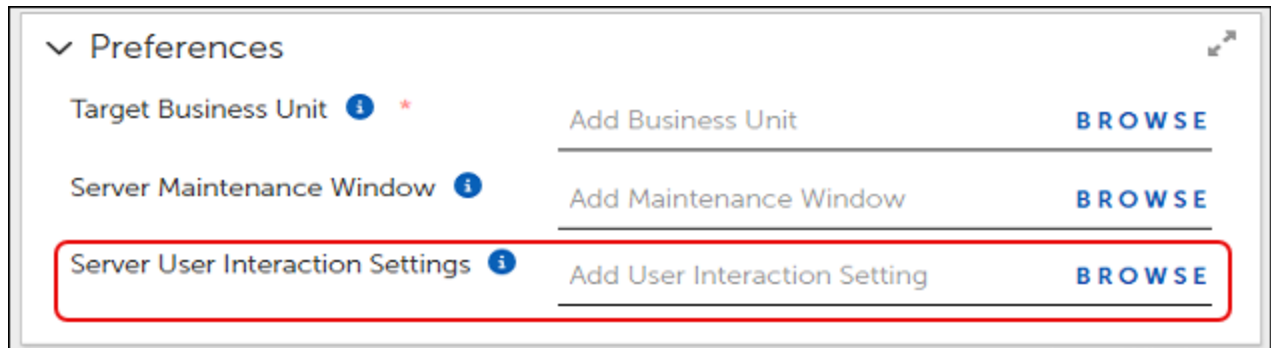
Add Maintenance Window Cancel

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, refer to [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

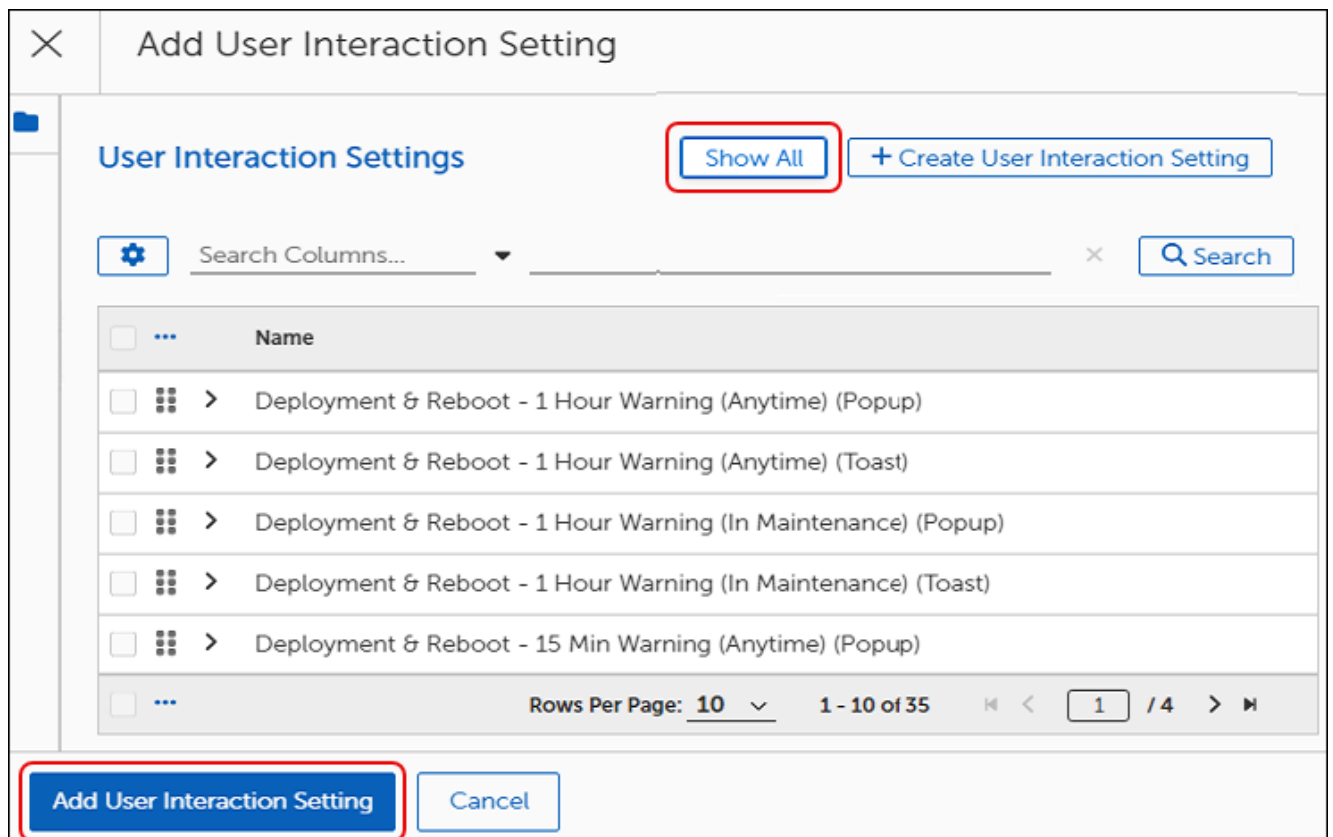
1. Select **Browse** at the far right of **Server User Interaction Settings**.



Preferences

Target Business Unit <i>i</i> *	Add Business Unit	BROWSE
Server Maintenance Window <i>i</i>	Add Maintenance Window	BROWSE
Server User Interaction Settings <i>i</i>	Add User Interaction Setting	BROWSE

This opens the Add User Interaction Setting dialog.



Add User Interaction Setting

User Interaction Settings

Show All + Create User Interaction Setting

Search Columns... Search

☐	...	Name
☐	>	Deployment & Reboot - 1 Hour Warning (Anytime) (Popup)
☐	>	Deployment & Reboot - 1 Hour Warning (Anytime) (Toast)
☐	>	Deployment & Reboot - 1 Hour Warning (In Maintenance) (Popup)
☐	>	Deployment & Reboot - 1 Hour Warning (In Maintenance) (Toast)
☐	>	Deployment & Reboot - 15 Min Warning (Anytime) (Popup)
☐	...	

Rows Per Page: 10 1 - 10 of 35 1 / 4

Add User Interaction Setting Cancel



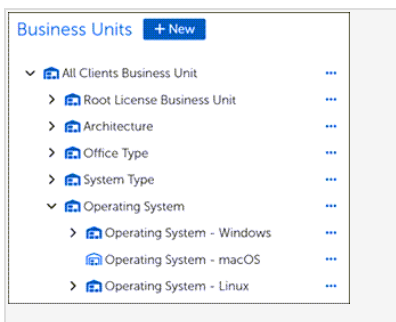
2. Select **Show All** at the upper-right corner to view the available options, and then select the checkbox aligned with the options you want to use. To create a new setting, refer to [User Interaction Settings](#), then return and repeat this step.
3. Select **Add User Interaction Setting** on the 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. Tenable Patch Management Express 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.



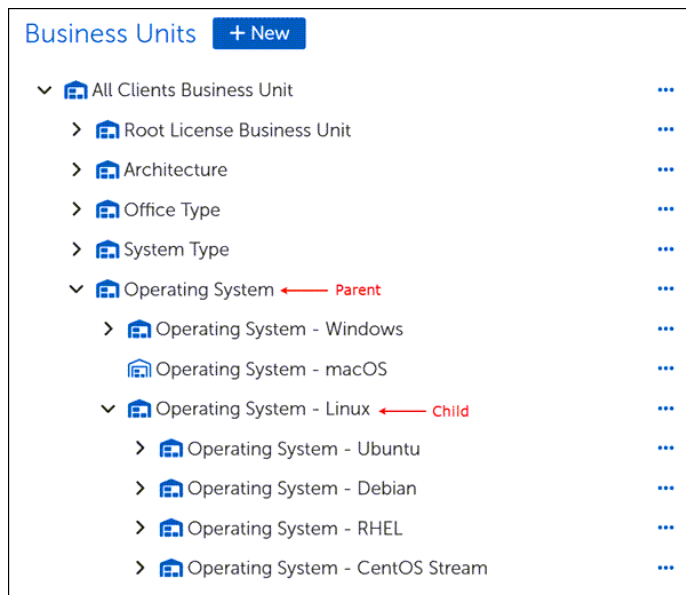
In addition to identifying the devices to include in a Business Unit, you can also specify various aspects of patching for endpoints, such as rollout processes, maintenance windows, approvals, and other relevant details.

Parent and Child Business Units

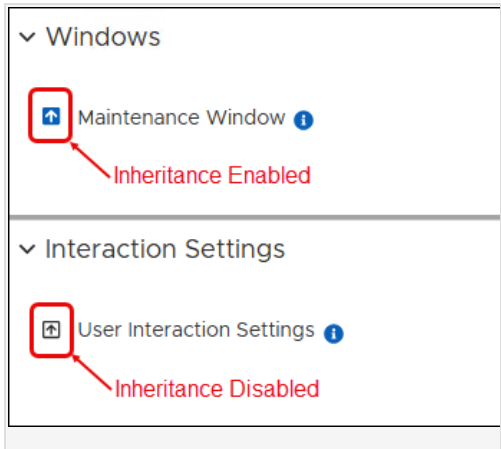
Business Unit objects use a parent-child hierarchy. A parent Business Unit may have multiple child Business Units, but a child Business Unit may have only one parent. The folder structure used in Tenable Patch Management Express shows the parent as the top-level folder and the child units as sub folders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

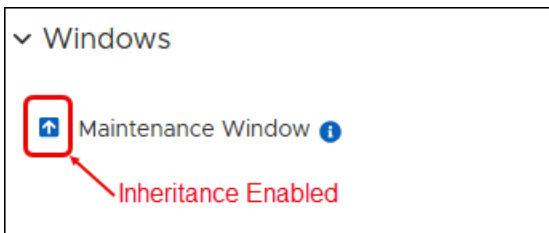


The hierarchical nature of Business Units allows a child Business Unit to inherit settings from its parent. An up-arrow with a blue background preceding a setting or process shows an inherited setting.

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

Managing Inheritance Settings

In Tenable Patch Management Express inheritance defaults to Enabled.



Important

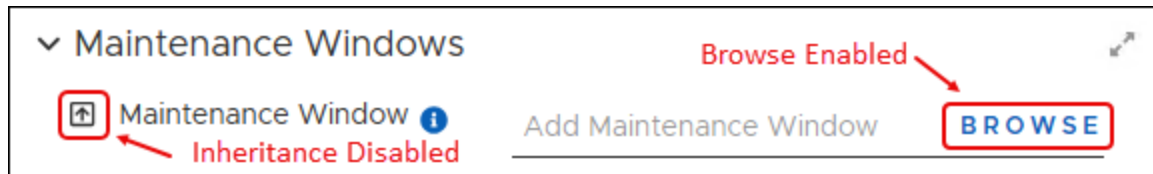
The colors shown here are default color settings. If you change the Admin Portal theme settings to use different colors, your arrows and backgrounds might be different.

Enable Inheritance

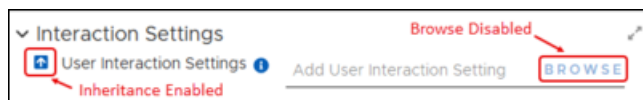


A white up-arrow with a blue background preceding a setting or process shows an inherited setting. Enabling inheritance disables the Browse button for the setting because you may not make any changes.

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



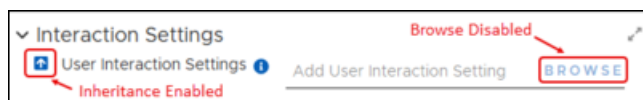
2. Select the up-arrow icon to enable inheritance



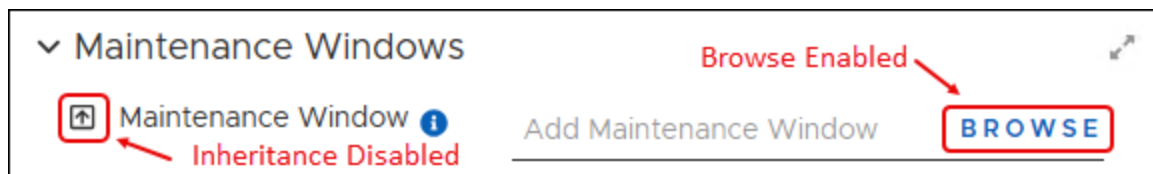
Disable Inheritance

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

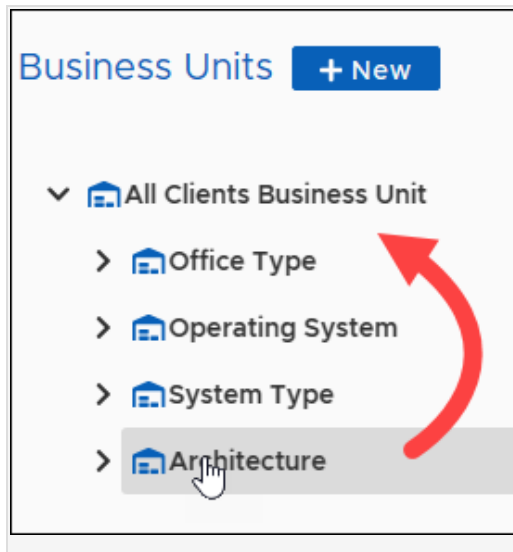
In the Business Unit hierarchy shown in the Tenable Patch Management Express dashboard, the Business Unit at the top of the list has the lowest priority. When changing the priority of a Business Unit in the hierarchy, consider the following items:

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

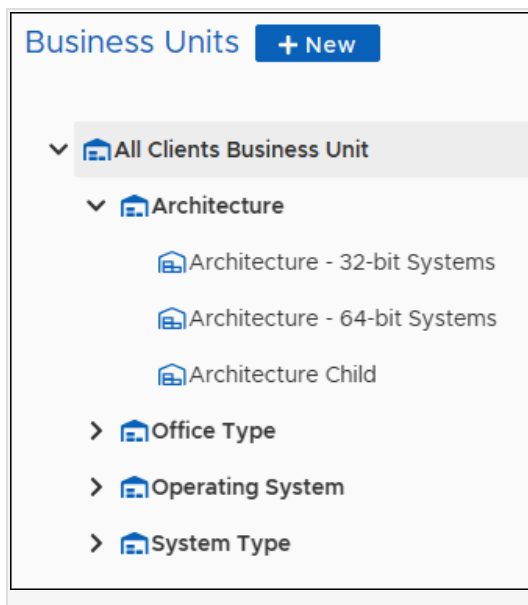
Further, is the new parent, or any ancestors, included in a Wave Entry that includes descendants? If yes, do you want the new BU included in those deployments?

Change the Order of the Hierarchy

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



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



Creating a Business Unit

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



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

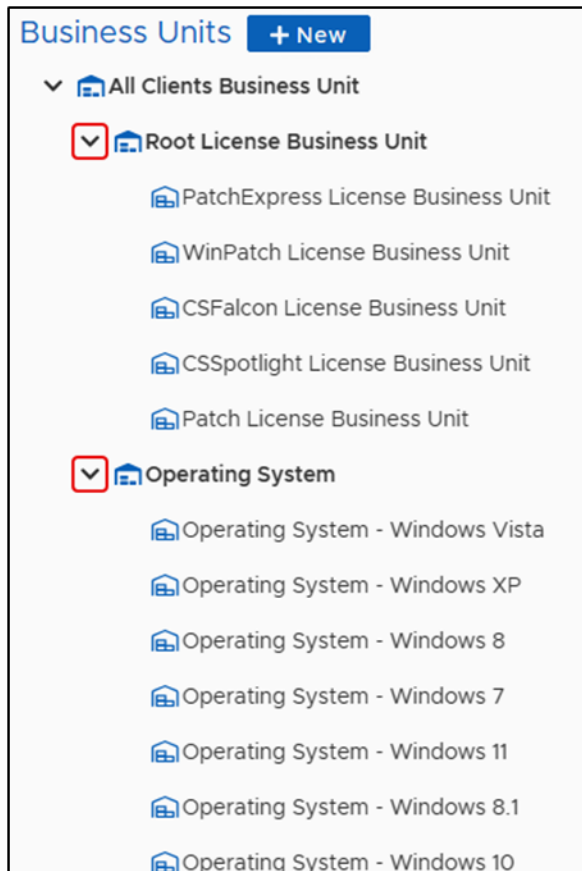
Open and Save a Business Unit Template

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.

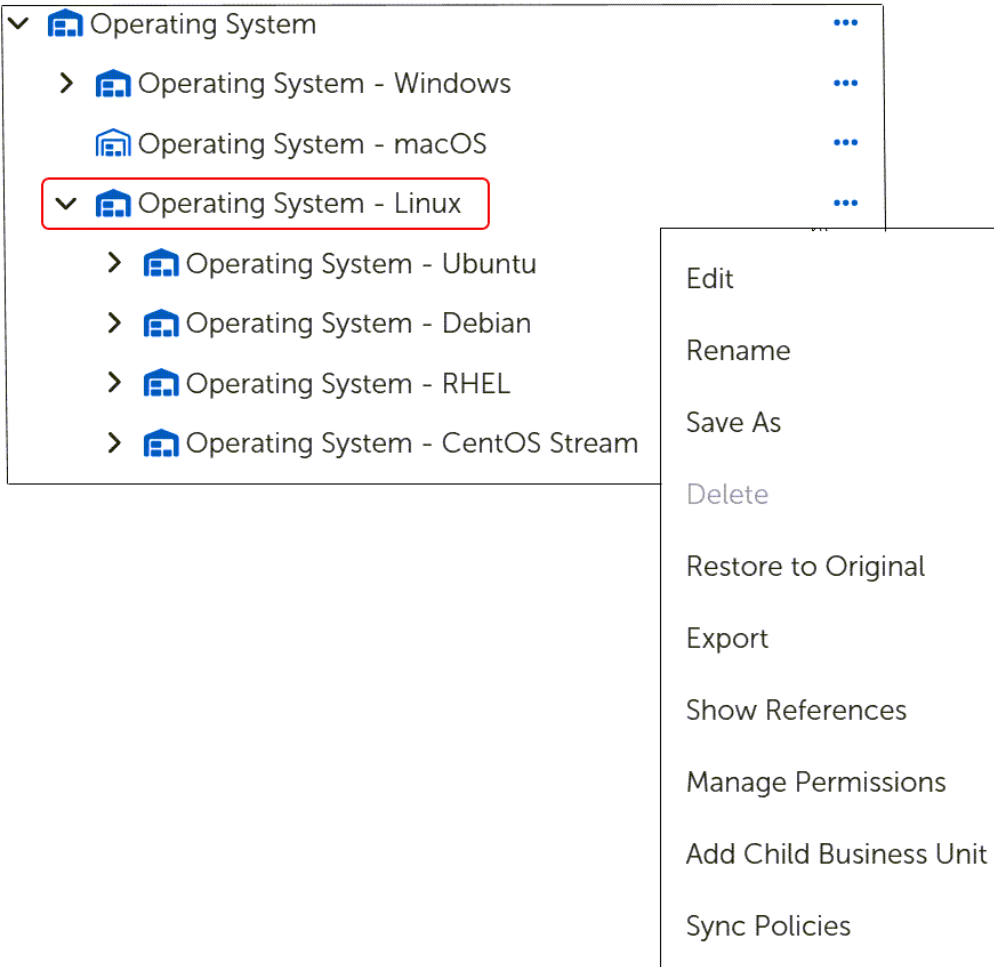
Important

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:

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

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](#)).

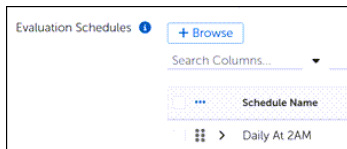
Add Evaluation Schedules to a Business Unit



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.



Select one or more schedules from the All Schedules table, and then select **OK** on the lower-

2. left of the dialog.

All Schedules

[Show All](#)[+ Create new Schedule](#)Search Columns...  Search

☐			↑ Schedule Name	Start Date	End Date	Last Modified
☐			00:00	1/1/00, 12:00 AM	--	3/22/23, 4:16 AM
☐			02:00	1/1/00, 2:00 AM	--	3/22/23, 4:16 AM
☐			08:00	1/1/00, 8:00 AM	--	3/22/23, 4:16 AM
☐			09:00	1/1/00, 9:00 AM	--	3/22/23, 4:16 AM
☐						

OK

Cancel

3. Select **Save** on the upper-left of the dialog to save your progress.

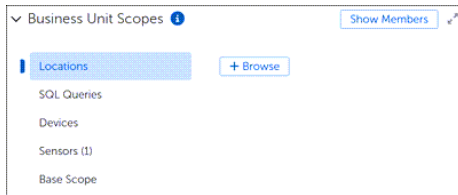
Configure Business Unit Scopes

Business Unit Scopes define the rules used to find and include devices in a named Business Unit. Tenable 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 *Tenable Patch Management Express*.
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 AdaptivaClientID from a_adaptivaclientdata
where machinename is ('machine1', 'machine2',
'machine3')

```

Add Query

Cancel

Important

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

- 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		
☐ ...	Query Name	Type	Actions
☐ >	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**.

Search Columns... <Search Term> x Search

- ☐ AD Site Name
- ☐ Client GUID
- ☒ Client Site Code
- ☐ Client Version
- ☒ ID
- ☐ Internal IP
- ☐ Is RVP
- ☐ Machine Name
- ☐ Primary User
- ☐ Subnet Address

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. Tenable 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**.

Sensors + 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.

× Sensor Group Scope

Scope Name * <Name>

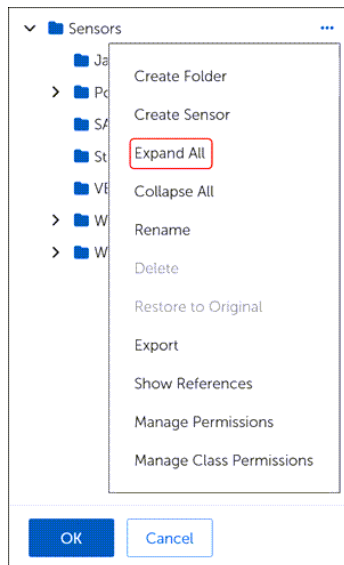
Scope Description <Detailed Description>

Sensor * BROWSE X

Filter Condition * Select Operator or Condition ...

OK Cancel

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.

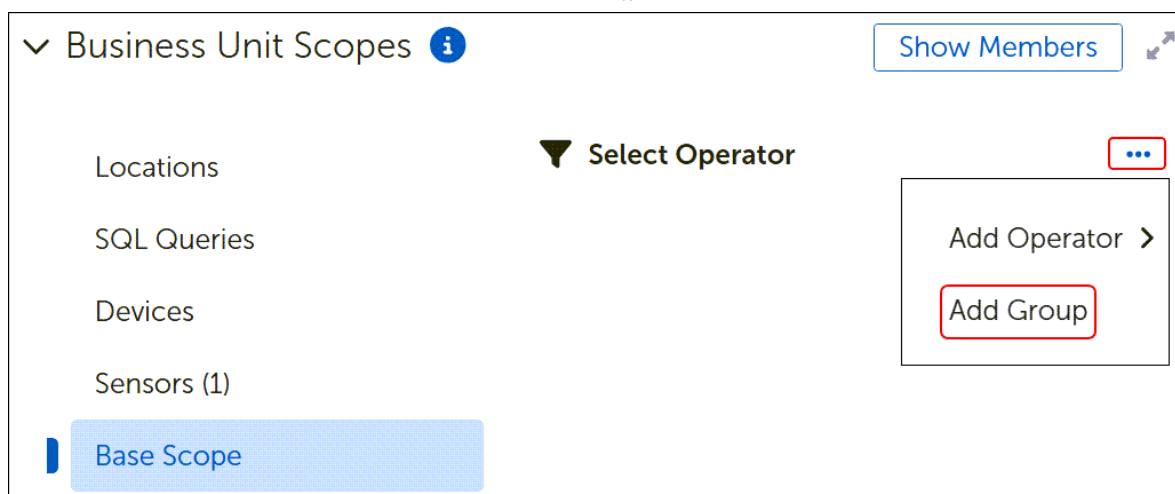


5. Select an item to use in your Sensor Group, and then select **Add Sensor**. This returns you to the Sensor Group Scope dialog. To add a Filter Condition, see [Patch Filter Conditions](#)
6. Select **OK** to return to the Business Unit template or change [Base Scope](#) settings.

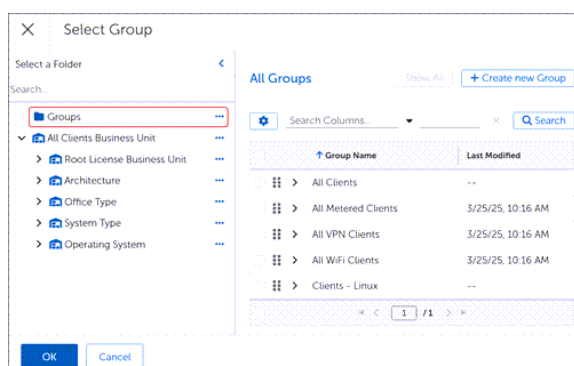
Set Base Scope

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**.

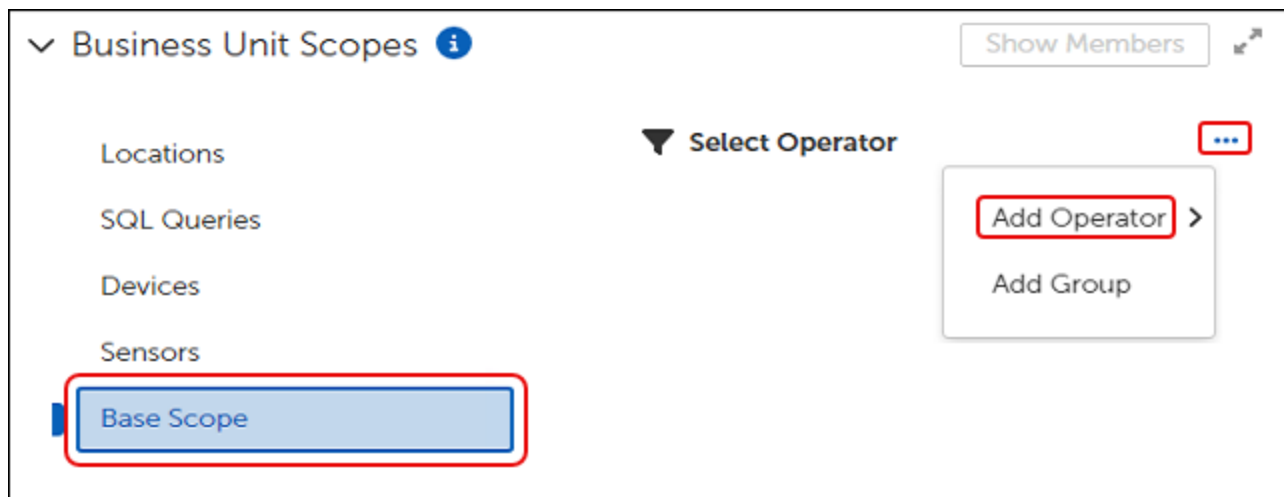
5. Select **OK** on the lower-left of the dialog. The entry under Business Unit Scopes shows the **AND** operator and the item you chose.

Add Multiple Groups or Business Units

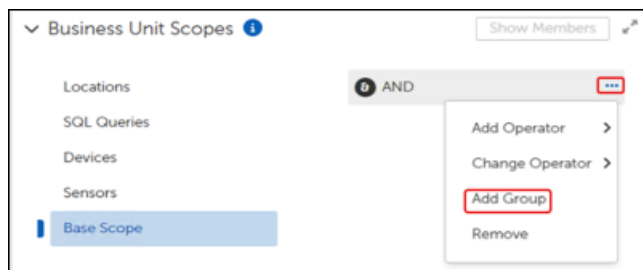
After setting the initial Base Scope, use this procedure to add additional Groups or Business Units to include in the Base Scope. You can add or exclude other Groups or Business Units or change Operators to customize your Base Scope depending on your needs.



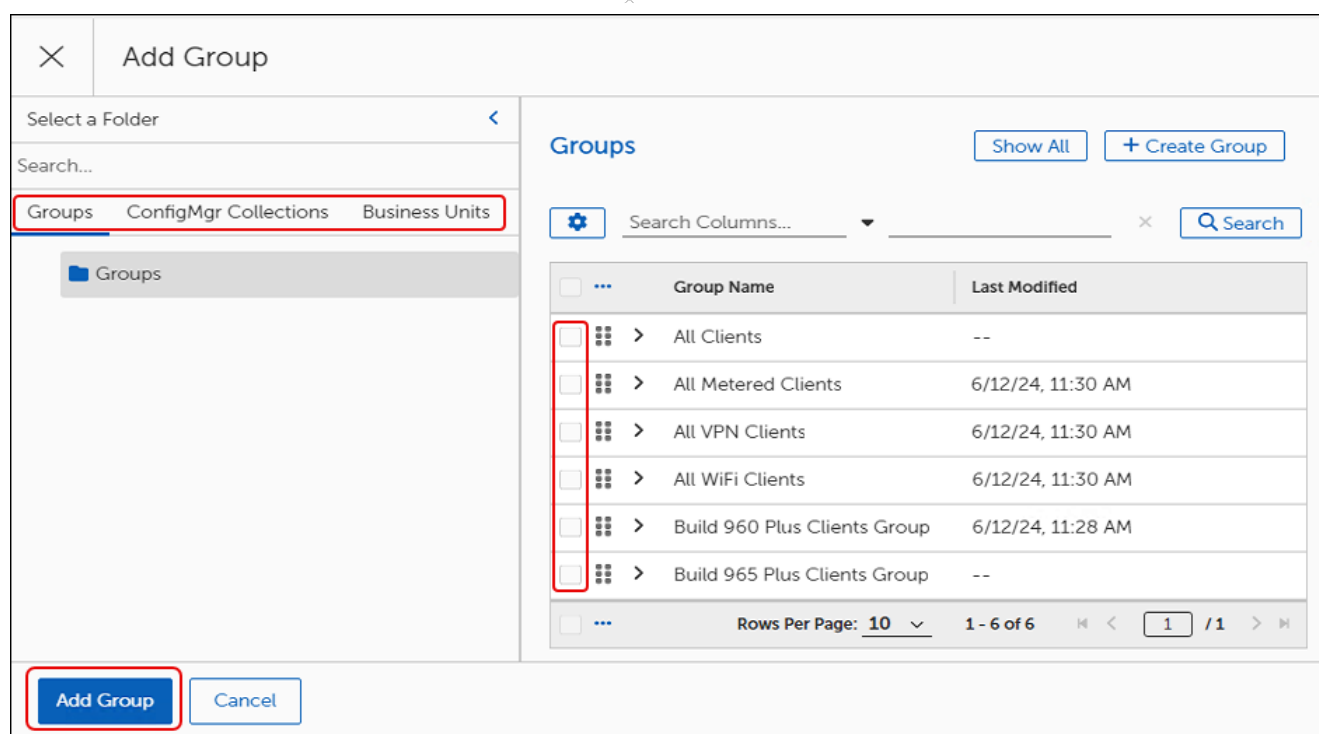
1. In the Business Unit Scopes section of an object template, select **Base Scope**.



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**.

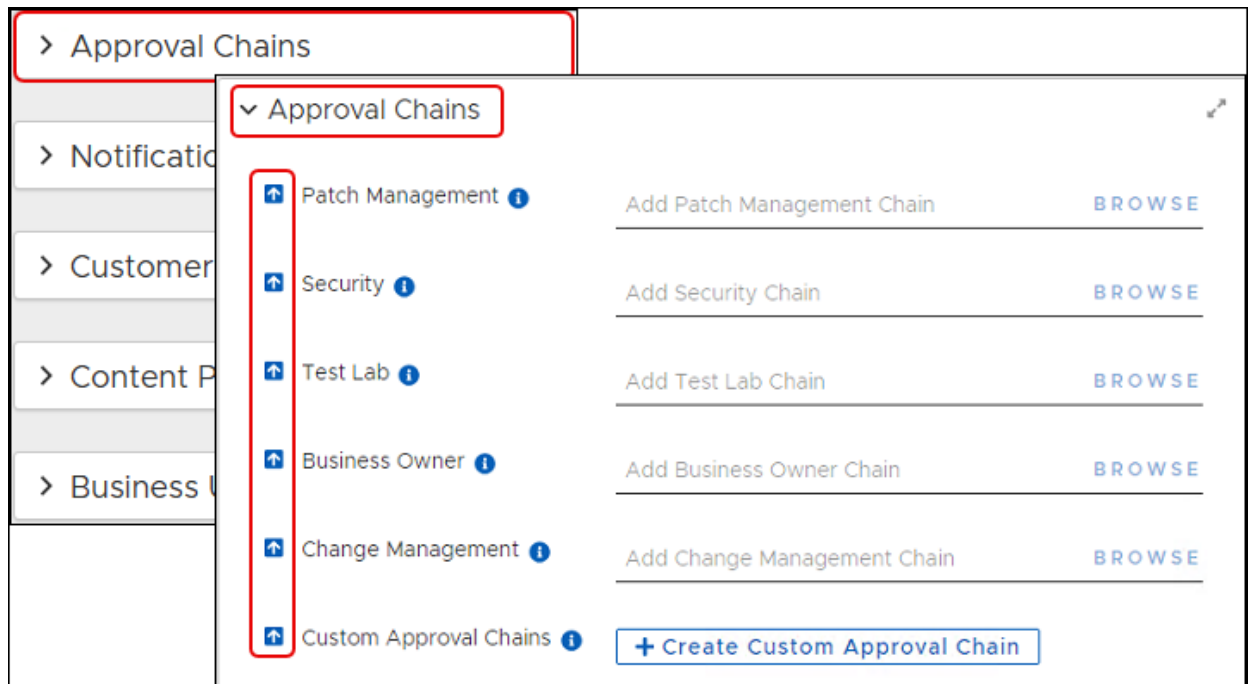
- Removing the top-level Operator removes everything beneath it.
- Removing a nested Operator also removes the associated Group or Business Unit.
- Removing a Group or Business Unit removes only that Group or Business Unit.

Add Approval Chains to a Business Unit

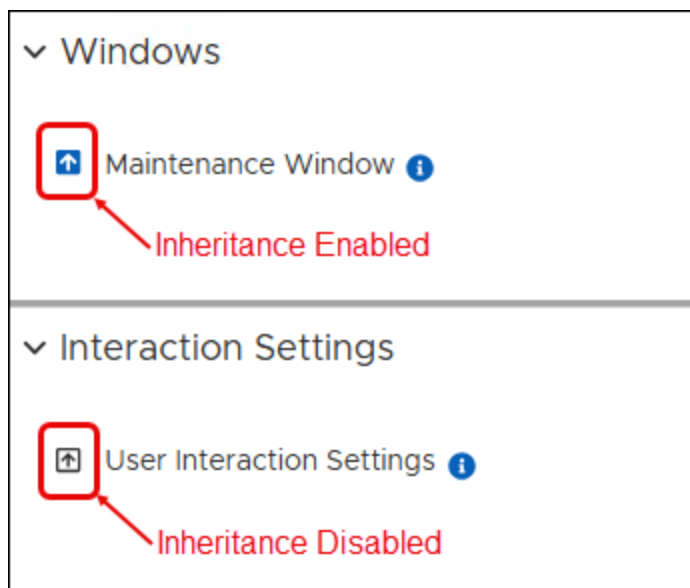
Adding Approval Chains to a Business Unit is an advanced feature. The Approval Chains fields allow advanced users to specify details for use in customized Patching Strategies, Deployment Chains, or Business Units when necessary to achieve different results.

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.

All Approval Chains

Show All + Create new Approval Chain

Search Columns... Search

☐	↑ Name
☒	> All Admins Approval Chain
☐	> Super Admins Approval Chain

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

OK Cancel

4. Select OK on the lower-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.

Customer Extension Data

Customer Extension Data is an advanced feature of Tenable. 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

Customer Extension Data New Key New Value

+ Add



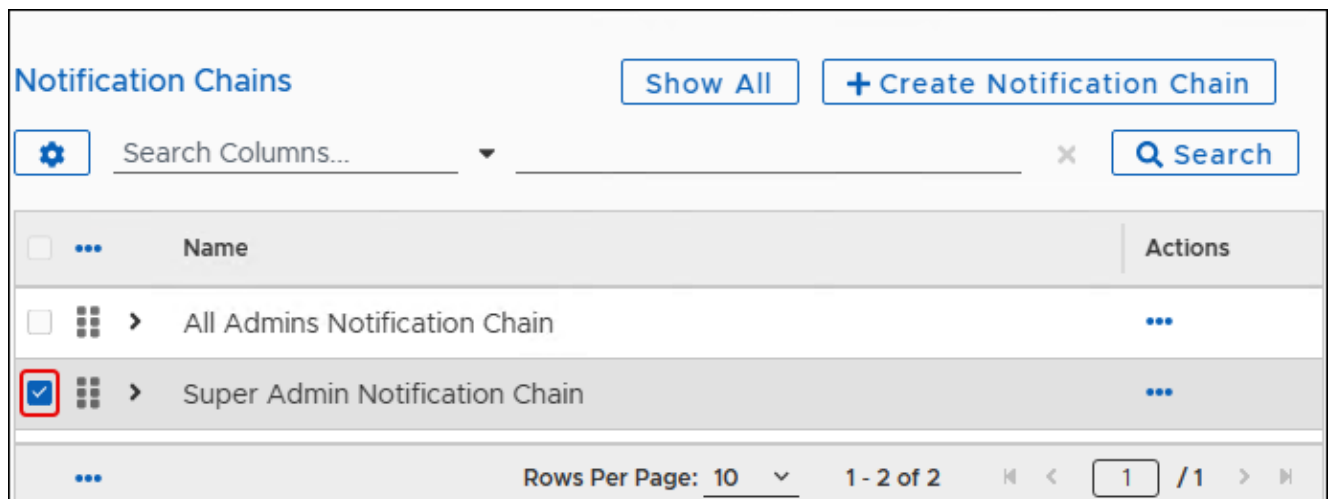
Customer Extension Data fields relate directly to fields in a customized template. If you do not have customized templates with key/value pairs you can modify, you do not need to configure or use this feature.

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

Add a Notification Chain

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

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



3. Select  **Notification Chains**, and then select **Show All** to see the available templates.
4. Select a **Notification Chain** from the table. To edit or create Notification Chains, see .
5. Continue editing the **Notification** settings, or select **OK** 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. Ensure that the devices you want to use in the lab have the Tenable Patch Management Client installed and are associated with an Tenable Patch Management Server.
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. Tenable Patch Management Express installs patches only during the defined Maintenance Window.



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

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

Tenable Patch Management Express 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](#).

Note: 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. In the upper-left of the dialog, select **More**, and then select **Save As**.
 - b. Enter a new name for the template, and then select **Save as**. 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**.

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 [Adaptiva 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 ⓘ [+ Create Maintenance Window](#)

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

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

☐	Start Time Schedule	Duration	Actions
☐	02:00	2h	...
☐	09:00	1h 2m 3s	...
☐	12:00	6d 4h	...
☐	Rows Per Page: 10 1 - 3 of 3		

3. Set an All Urgencies Override Duration.

These settings override any non-zero duration values set in 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

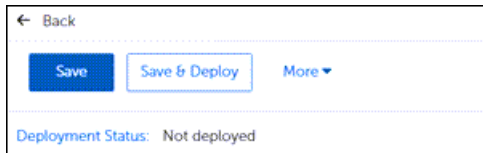
Deploy a Maintenance Window to make it available for use in a template. If you update a Maintenance Window template that was previously deployed, you must save and deploy it again for the changes to take effect.

1. Complete the Maintenance Window configuration (refer to [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.

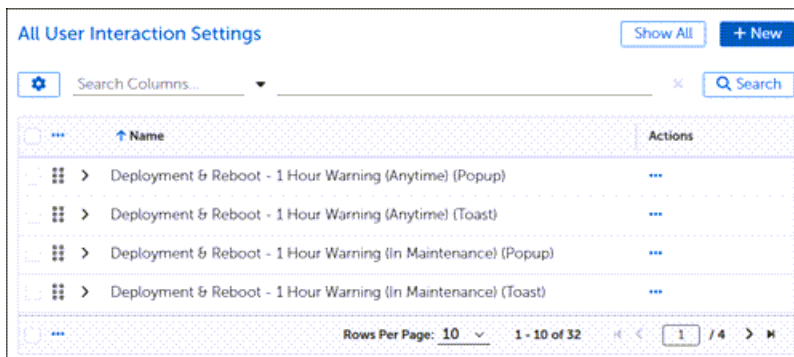


User Interaction Settings

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. In the upper-left of the dialog, select **More**, and then select **Save As**.
- b. Enter a new name for the template, and then select **Save as**. 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**.

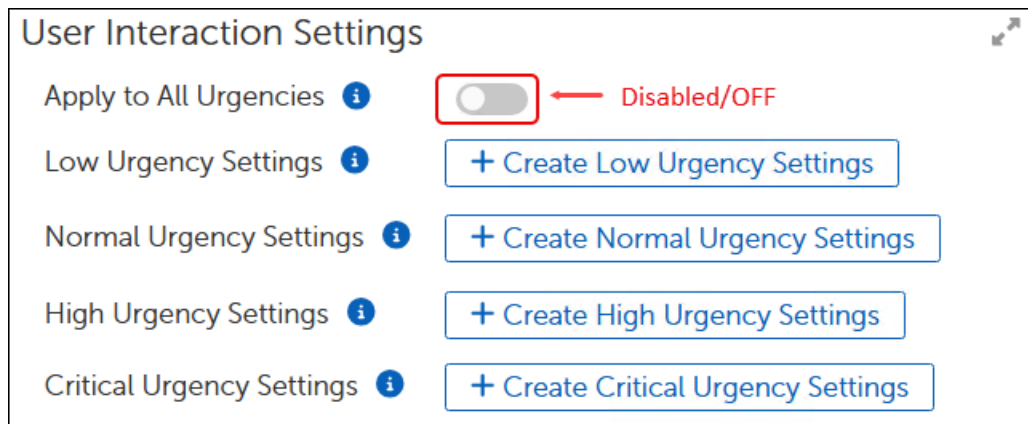
Choose Urgency Settings

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.

✕ All Urgency: User Interaction Settings

▼ Deployment Notification Settings

Notify User Before Installation ? ☐

▼ Reboot Notification Settings

Suppress Reboots ? ☐

Notify User Before Reboot ? ☐

OK Cancel

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.

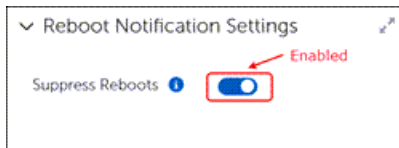


3. Enter **Notification Text** in the text box. The user sees this text when the notification arrives on their device.
4. Next, see [Reboot Notification Settings](#).

Reboot Notification Settings

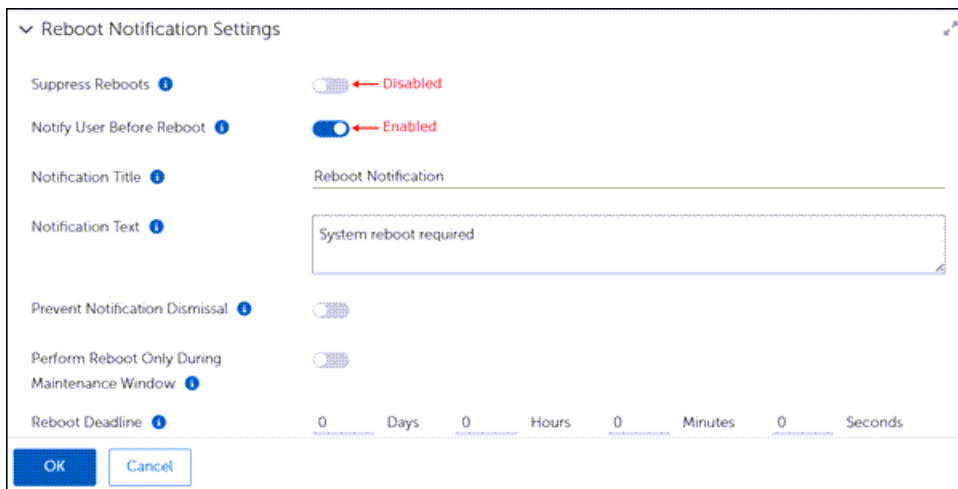
The Reboot Notification Settings in a [User Interaction Settings](#) dialog provides choices to Suppress Reboots and to Notify User Before Reboot.

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.

Prevent Notification Dismissal ⓘ	☒
Perform Reboot Only During Maintenance Window ⓘ	☒
Reboot Deadline ⓘ	0 Days 1 Hours 0 Minutes 0 Seconds
Allow Snooze ⓘ	☐

- These entries define the amount of time that may pass before the system forces the reboot to occur.



- If zero, Tenable Patch Management Express provides no warning to the user.

4. [Configure snooze settings.](#)

Managing Snooze Settings

When defining User Interaction Settings, Tenable Patch Management Express 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, refer to [Managing Snooze Settings](#).



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

Allow Snooze	☒	← Enabled		
Maximum Snooze Duration	0 Days	8 Hours	0 Minutes	0 Seconds
Snooze Reminder	0 Days	6 Hours	0 Minutes	0 Seconds
Snooze Durations	0 Days 0 Hours 0 Minutes 0 Seconds + Add			

- 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.

Days	Hours	Minutes	Seconds	
0	4	0	0	X
0	2	0	0	X
0	1	0	0	X
0	0	15	0	X
0	0	0	0	

+ Add

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.

← Back

Save Save & Deploy More ▼

Deployment Status: Not deployed

Customized Products



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

Tenable 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:

The screenshot shows a dialog box titled 'General Settings' with a close button in the top right corner. Inside the dialog, there are two input fields. The first field is labeled 'Name *' and has a placeholder text 'Enter a descriptive name'. The second field is labeled 'Description' and has a placeholder text '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 ⓘ * **BROWSE**

Target Product ⓘ * **BROWSE**

2. Select the **Deployment Wave** to which these Customized Product settings apply on the Deployment Waves dialog. See [Deployment Waves](#) for details.
3. Select **Add Deployment Wave** on the lower-left 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 Show All

☐	Name	Actions
☒	Google Chrome x64	...
☐	Google Chrome x86	...

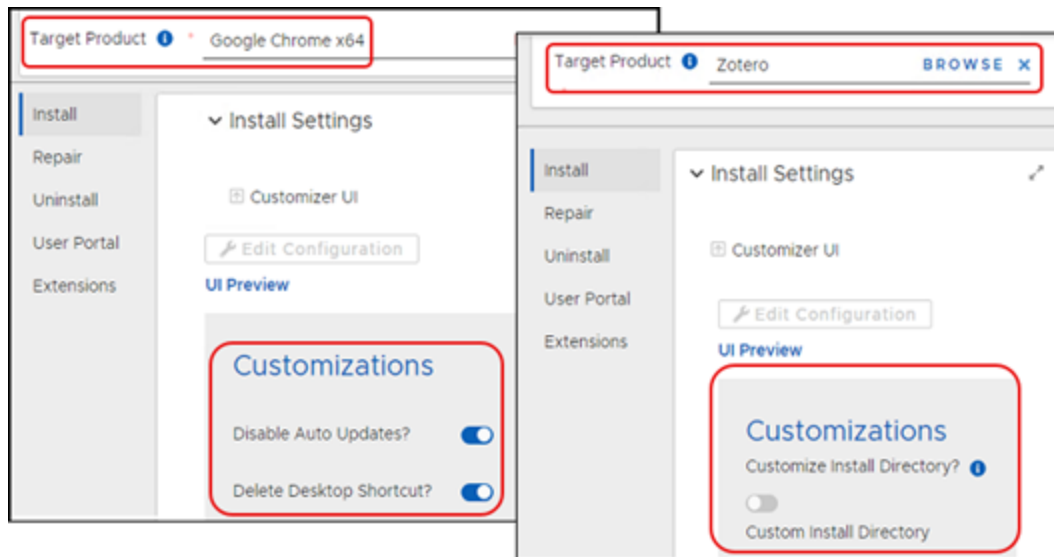
3. Select the **Software Product** you want to customize. You can target only one Software Product in each Customized Product entry.
4. Select **Add Software Product** to populate the configurable items in the static list of **Install Settings**. Settings change depending on the Target Product.



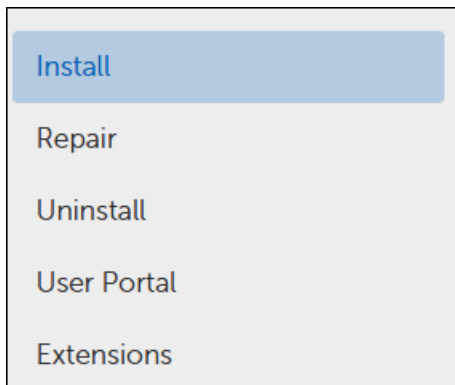
5. Select **Save** in the upper-left of the template to save your changes.
6. Continue with [Configure Software Install Settings](#).

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.



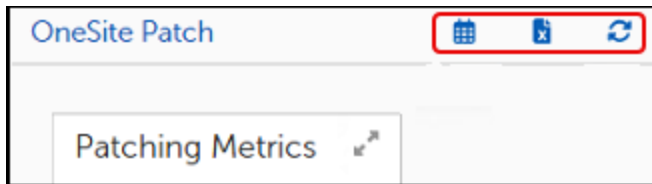


3. Select **Save** on the upper-left of the dialog to save your progress.
4. Select <-- **Back to Customized Products** above **General Settings**. The changes you have made take effect the next time the associated Deployment Wave runs.

Navigating the Tenable Patch Management Express Dashboard

Date Settings, Export, and Refresh

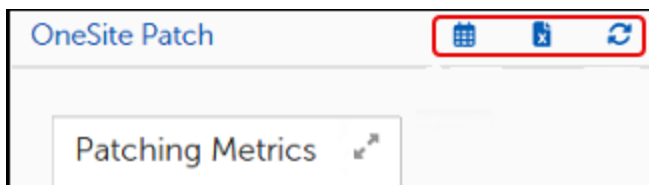
The three small icons (Calendar, Export and Refresh) on the upper right of the Home page and on any of the Patching Analytics pages (Overview, Products, Patches, or Devices) provide options to customize the date settings to a particular date range, choose some or all widgets on the page for exporting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



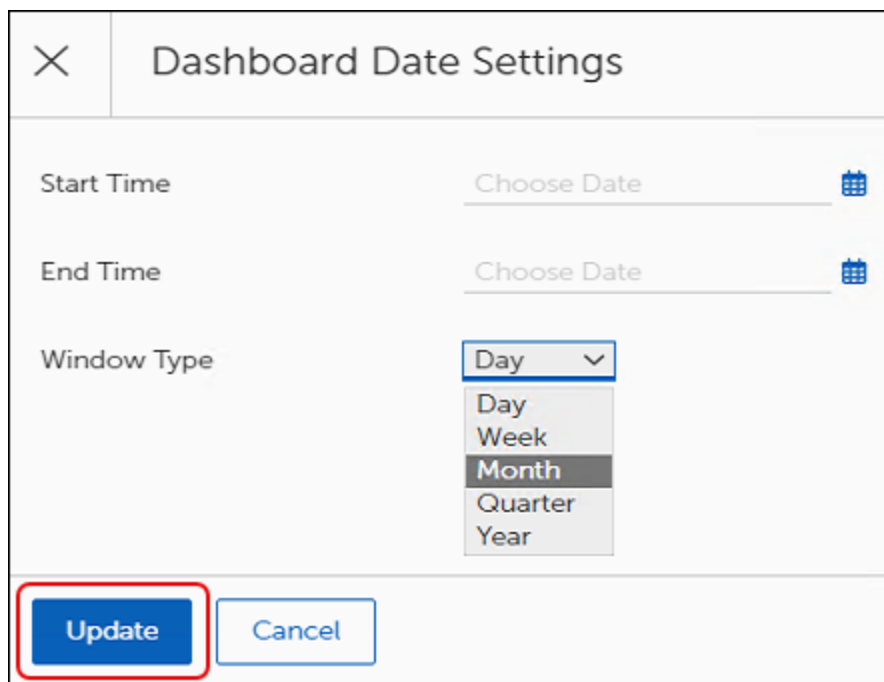
Set Dates for Status Views

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.



Dashboard Date Settings

Start Time Choose Date

End Time Choose Date

Window Type

Day Week Month Quarter Year

Update Cancel

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

Export Widget Data

1. Select  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.

OneSite Patch

Export Data

Select All

Cancel

Export Selected

Patching Metrics

17 Patching Strategy Objects

23 Products Discovered

33 Products in Strategies

0 Patching Exceptions

5 Devices

5 Scans Run (Last 30 days)

5 Patches Installed (Last 30 days)

Patching Status

449 Status on Machines

Installed - 23 (5.12%)

Outdated - 114 (25.39%)

Applicable - 28 (6.24%)

Scan Failure - 280 (62.36%)

Installation in Progress - 1 (0.22%)

Uninstallation in Progress - 0 (0%)

Rollback in Progress - 0 (0%)

Outdated but Excluded - 0 (0%)

Patching Metadata

Last Synced

5/21/24, 11:48 AM

Last Metadata Update

5/21/24, 6:53 AM

Supported Products

1614

Supported Patches & Releases

47059

Patching System Health

Overall Health: 90%

Metadata Feed Health: 98%

Scanning Health: 100%

Patch Installation Health: 73%

Patching Activity

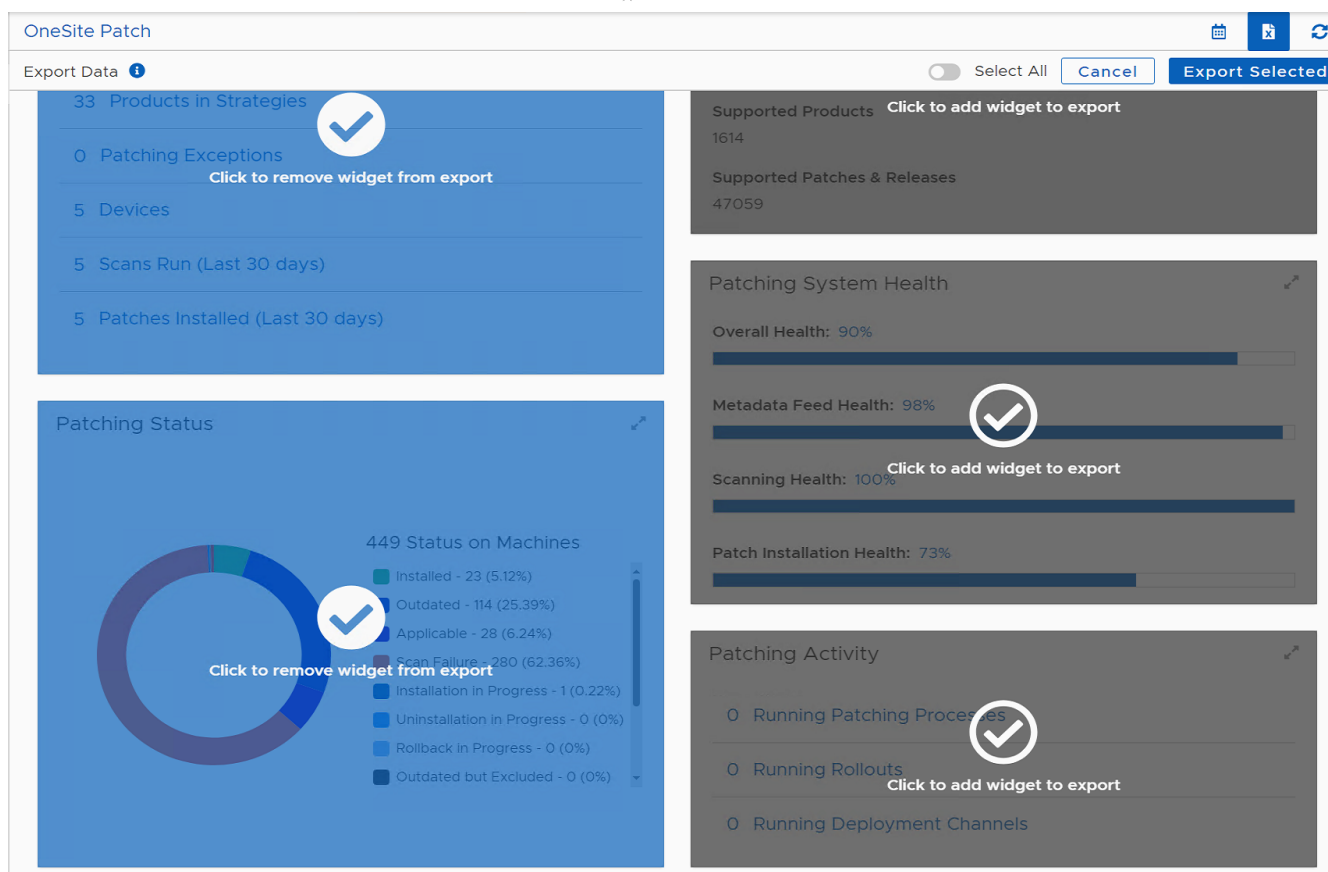
0 Running Patching Processes

0 Running Rollouts

0 Running Deployment Channels

2. Choose which widgets to export:

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



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

Refresh the Status View

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

Patch Menus

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

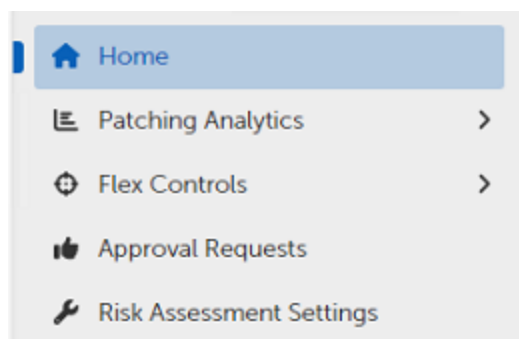
The left pane stays the same, regardless of which object you choose, and consists of three sections.

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 (refer to [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 Tenable Patch Management Express, select **Home** to return to the Home page. For a description of Home page widgets, refer to [Home dashboard and Performance Widgets](#).

Home Menu Object Descriptions

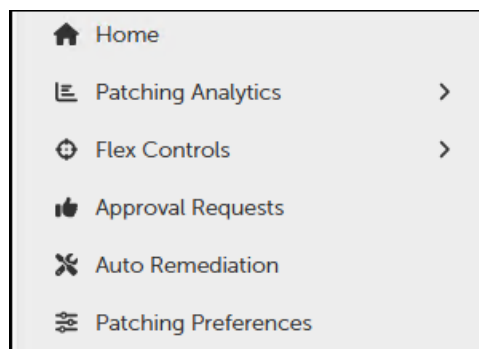
Object	Purpose
Home	Opens the Home page to view the overall status, metric, and compliance for patching in your environment. Refer to Tenable Patch Management ExpressDashboard and Performance Widgets .
Patching Analytics	Shows the status of patches and products in the environment. Change tabs to view metrics for Products, Patches, or Devices. Refer to 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, refer to Flex Controls
Approval Requests	View all approval requests and check the status of pending and completed requests. Refer to Approval Requests .



Object	Purpose
Risk Assessment Settings	Customize risk calculations and display risks in other dashboards. Refer to Risk Assessment Settings .

Tenable Patch Management 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 Patch Express functionality.



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

Home Menu Object Descriptions in Patch Express

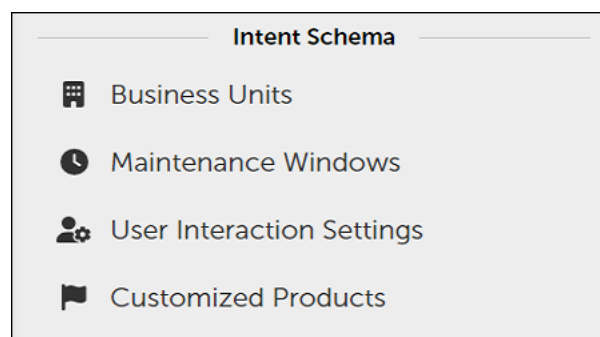
Object	Purpose
Home	Opens the Home page to view the overall status, metric, and compliance for patching in your environment. Refer to Tenable Patch Management ExpressDashboard and Performance Widgets .
Patching Analytics	Shows the status of patches and products in the environment. Change tabs to view metrics for Products, Patches, or Devices. Refer to Patching Analytics Dashboards . Sub menus include Overview, Products, Patches, and Devices.
Flex Controls	Review and manage settings for Blocklisting, Exceptions, Global Pause,



Object	Purpose
	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, refer to Flex Controls
Approval Requests	View all approval requests and check the status of pending and completed requests. Refer to 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.

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

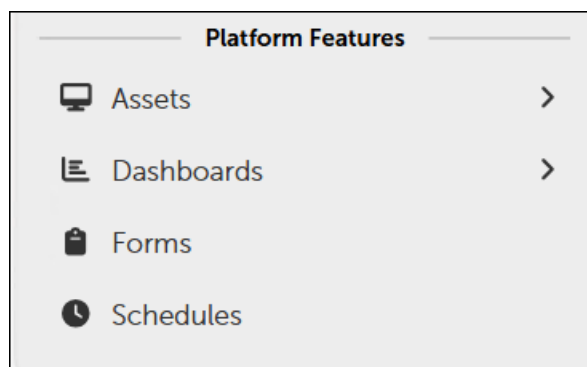
Object	Purpose
Business Units	Logically group and manage devices, settings, and other resources within a hierarchy. Refer to Business Units
Maintenance Windows	Define maintenance and reboot windows. Primarily associated with Business Unit configurations. Refer to Maintenance Windows .
User Interaction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



Object	Purpose
Settings	interacting with patching notifications and required reboots. Refer to User Interaction Settings .
Customized Products	Customization of installation for products with specific actions needed, such as license key entry or custom installation locations, before or after an installation. Refer to Customized Products .

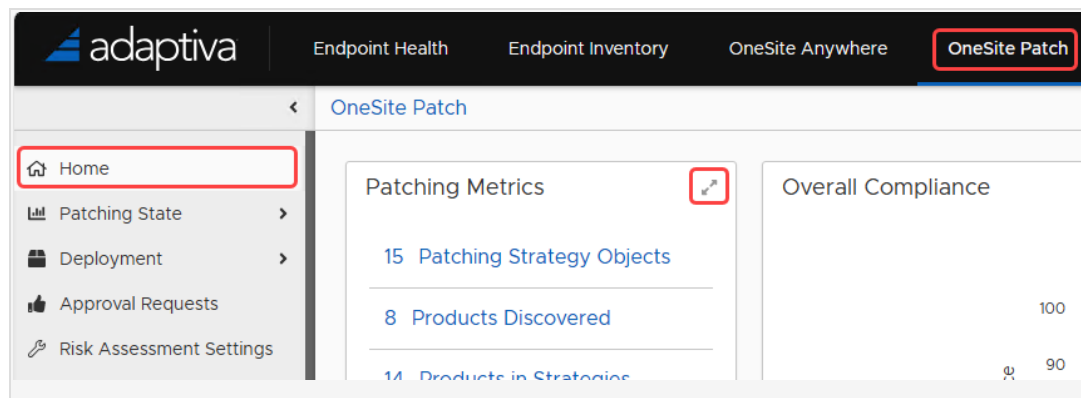
Platform Features Menu

These are common features available from every menu in Tenable Patch Management Express. For a description of the items in this menu, refer to the Tenable patch Management Express Platform User Guide.



Tenable Patch Management Express Dashboard and Performance Widgets

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



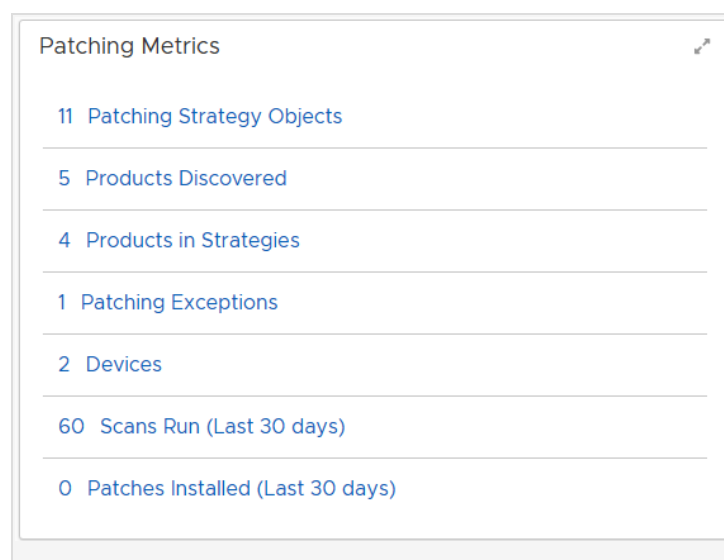


The layout of these widgets depends on the size of your computer monitor.

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

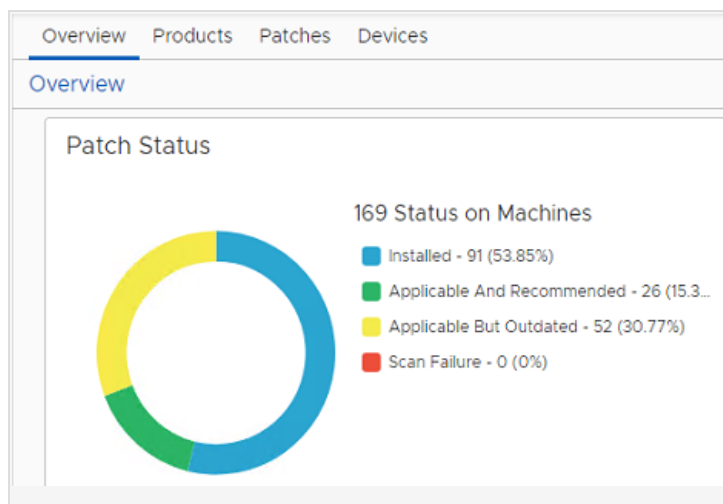
Patching Metrics

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.



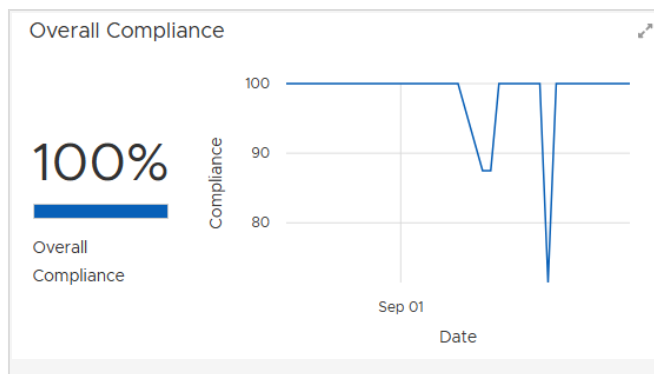
Patching Status

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.



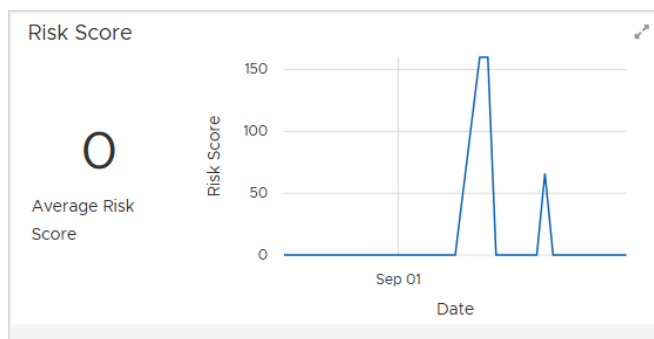
Overall Compliance

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. Refer to [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. Refer to [Risk Assessment Settings](#) for more information.

Patching Metadata

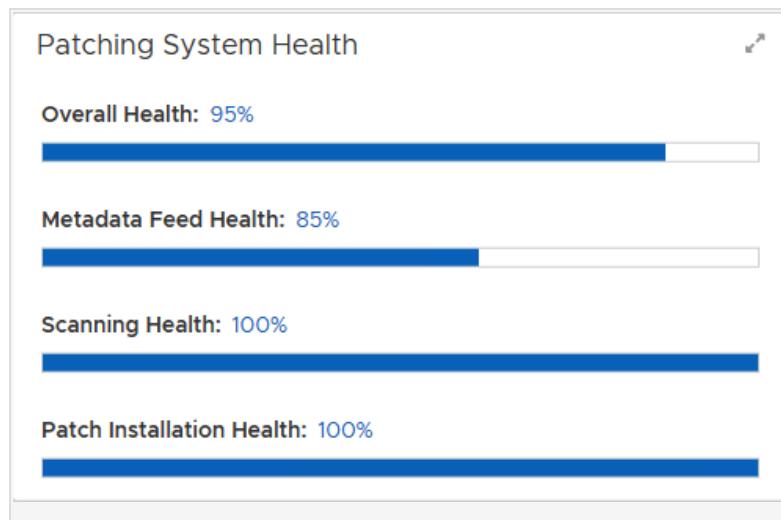
Summarizes the status of the latest endpoint scans and client product inventory updates. Metadata includes details about the products, patches, and updates approved by the company for installation. The Patch Metadata summary tells the administrator when the AdaptivaServer and AdaptivaClient last synchronized 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

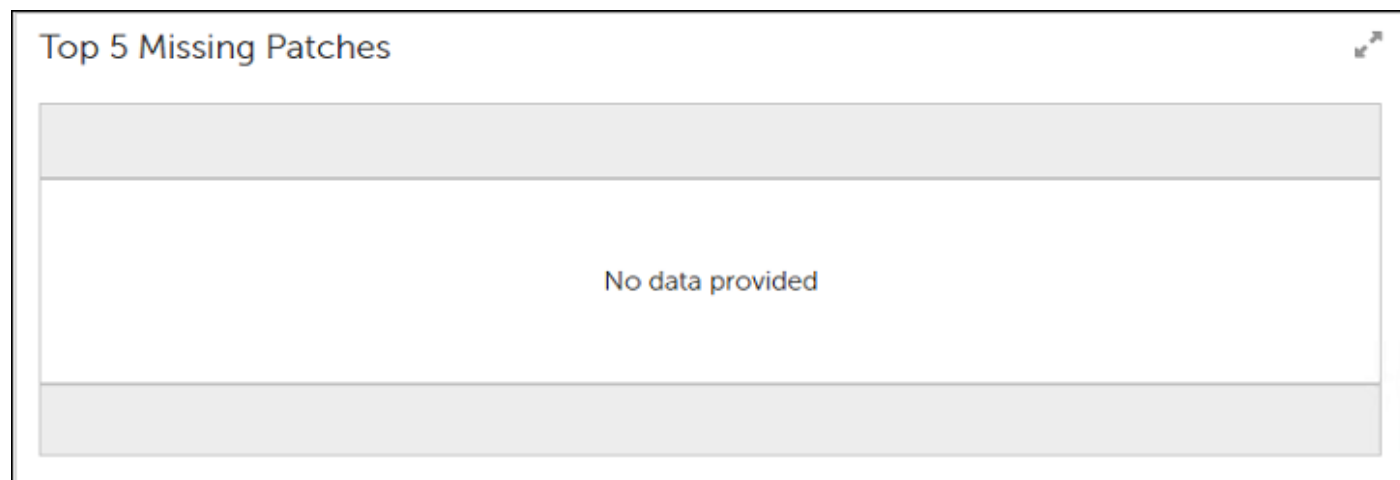


☐ ...	Product Name	Compliance Status	Actions
☐	Microsoft Analysis Services OLE DB Provider ...	0%	...
☐	Microsoft Orca	0%	...
☐	Microsoft Visual C++ 2015-2022 Redistribut...	0%	...
☐	Microsoft Visual C++ 2015-2022 Redistribut...	0%	...
☐	SQL Server Management Studio x64	0%	...
☐ ...	Rows Per Page: 1 - 5 of 5 1 / 1 2		

Top 5 Missing Patches



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



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

Appendices

Software Products

Tenable Patch Management Express 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

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

The metadata team receives 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 Tenable publishes the content to the Tenable CDN. The Tenable 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.

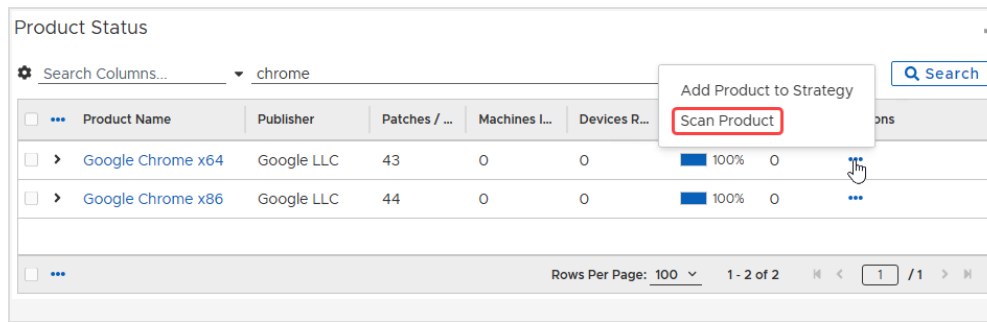
After confirming a successful update, the team creates, reviews, and approves the metadata before adding it to the metadata catalog. Refer to the [OneSite Patch 3rd Party App Catalog](#) for more information.

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



4. Select **Scan Product**.

- This opens the Request Scan dialog and prepopulates the Software section with all the software available on the item you chose to scan.
- **Request Scan** defaults to Scan All Software.

5. Select the **Scan All Clients** toggle to enable or disable scanning all clients. If disabled, add targets to scan.

×

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

☐	...	Name	Actions
☐	☰ >	 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.



Tenable Patch Management Enterprise

Table of Contents

[Tenable Patch Management Enterprise](#)

[New in this Tenable Patch Management Release](#)

[Getting Started with Tenable Patch Management](#)

[Prerequisites](#)

[Supported Platforms and Distributions](#)

[Supported Browsers](#)

[Logs for Server and Client](#)

[Customer Support](#)

[Tenable Patch Management Admin Portal](#)

[Resolve Mozilla Firefox Active Directory Login Issue](#)

[Licensing Tenable Patch Management](#)

[Patch Management Dashboard](#)

[Integrate Tenable Vulnerability Manager](#)

[Minimum User Role Requirements for APIs](#)

[Add Tenable Access Settings to Tenable Patch Management](#)

[Administrators and Roles](#)

[Administrators and Roles](#)

[Access Security Settings](#)

[View Administrators](#)

[Create a New Administrator](#)

[Create a Microsoft Teams Webhook URL](#)

[View Roles](#)

[Create a New Role](#)

[Introduction to Patching Strategies](#)

[Patching Strategy Use Case](#)

[Open and Save a Patching Strategy Template](#)

[Configure Deployment Settings](#)

[Add Software Products](#)



[Enable the Patching Strategy](#)

[View a Staged Patching Strategy](#)

[Start the Patching Strategy Manually](#)

[Optional Objects in Patching Strategy Templates](#)

[Organize New Patch Objects](#)

[Create a New Folder for Objects](#)

[Move an Object Template Between Folders](#)

[Menu Objects for Tenable Patch Management](#)

[Business Units and Rollout Processes](#)

[Business Units](#)

[Rollout Processes](#)

[Patching Strategies](#)

[Purpose of a Patching Strategy](#)

[View built-in Patching Strategies](#)

[Patching Strategy Templates](#)

[Creating a Patching Strategy](#)

[View a Staged Patching Strategy](#)

[Start the Patching Strategy Manually](#)

[Managing Enabled Patching Strategies](#)

[Delete an Enabled Patching Strategy](#)

[Submit Patches to an Enabled Patching Strategy](#)

[Approvals for Adding Patches](#)

[Resubmit an Enabled Strategy](#)

[Patching Processes](#)

[Creating Patching Processes](#)

[Patching Process Templates](#)

[Bots - Patch Deployment and Notification Bots](#)

[Deployment Bots](#)

[Notification Bots](#)



[Chains](#)

[Approval Chains](#)

[Notification Chains](#)

[Deployment Channels and Deployment Channel Processes](#)

[Deployment Channels](#)

[Deployment Channel Processes](#)

[Deployment Waves](#)

[Using Deployment Waves](#)

[Open and Save a Deployment Wave Template](#)

[Add a Deployment Wave Entry](#)

[Create a Wave Entry](#)

[Edit or Remove a Wave Entry](#)

[Maintenance Windows](#)

[Open and Save a Maintenance Window Template](#)

[Dynamic Settings](#)

[Add Dynamic Detection Workflow \(Optional\)](#)

[Maintenance Windows by Urgency](#)

[Apply a Maintenance Window to All Urgencies](#)

[Save and Deploy the Maintenance Window](#)

[Communication Providers](#)

[Using Communication Providers](#)

[Open and Save a Communication Provider Template](#)

[User Interaction Settings](#)

[Open and Save a User Interaction Template](#)

[Choose Urgency Settings](#)

[Configure Deployment Notification Settings](#)

[Reboot Notification Settings](#)

[Managing Snooze Settings](#)

[Configure Snooze Settings](#)



[Save and Deploy User Interaction Settings](#)

[Customized Products](#)

[Manage Settings for Customized Products](#)

[Patch Content](#)

[Schedules](#)

[View Available Schedules](#)

[Create a Custom Schedule](#)

[Patching Analytics Dashboards](#)

[Using Search in Tenable Patch Management](#)

[Patching Analytics Overview](#)

[Products View](#)

[Patches View](#)

[Devices View](#)

[Flex Controls](#)

[Blocklisting](#)

[Cycle Operations](#)

[Patching Exceptions](#)

[Global Pause](#)

[Rollbacks Overview](#)

[Approval Requests](#)

[Approve or Reject a Patch Request](#)

[Risk Assessment Settings](#)

[Risk Score Settings](#)

[Custom Risk Settings](#)

[Content Prestaging Settings](#)

[Defining Content Prestaging Settings](#)

[Set Content Prestaging Settings](#)



[Customer Extension Data](#)

[Navigating the Tenable Patch Management Dashboard](#)

[Date Settings, Export, and Refresh](#)

[Tenable Patch Management Patch Menus](#)

[Tenable Patch Management Dashboard and Performance Widgets](#)

[Appendices](#)

[Software Products](#)

[Endpoint Scans](#)

Bots - Patch Deployment and Notification Bots

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

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

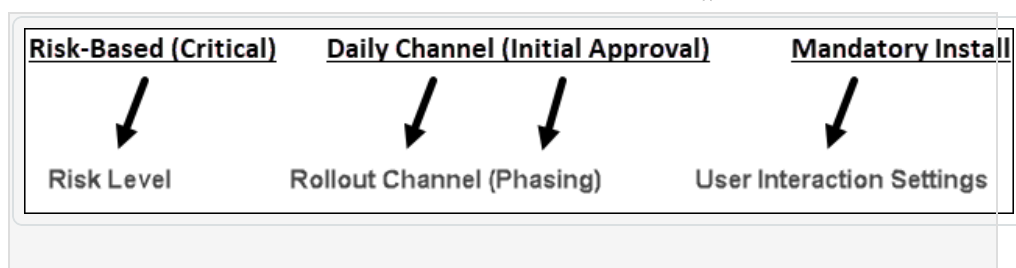
Deployment Bots

Patch Deployment Bot Template Naming Conventions

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

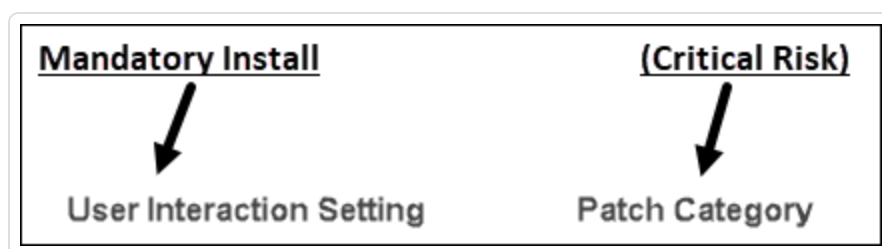
Risk-Based Filters

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



Mandatory Installation for Specific Categories

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



Descriptions of Bot Settings

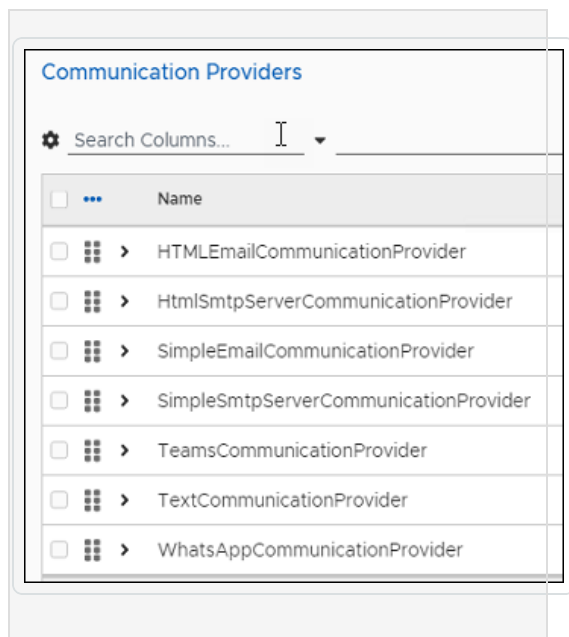
The Bot templates provided by Tenable Patch Management include the following settings:

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

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



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



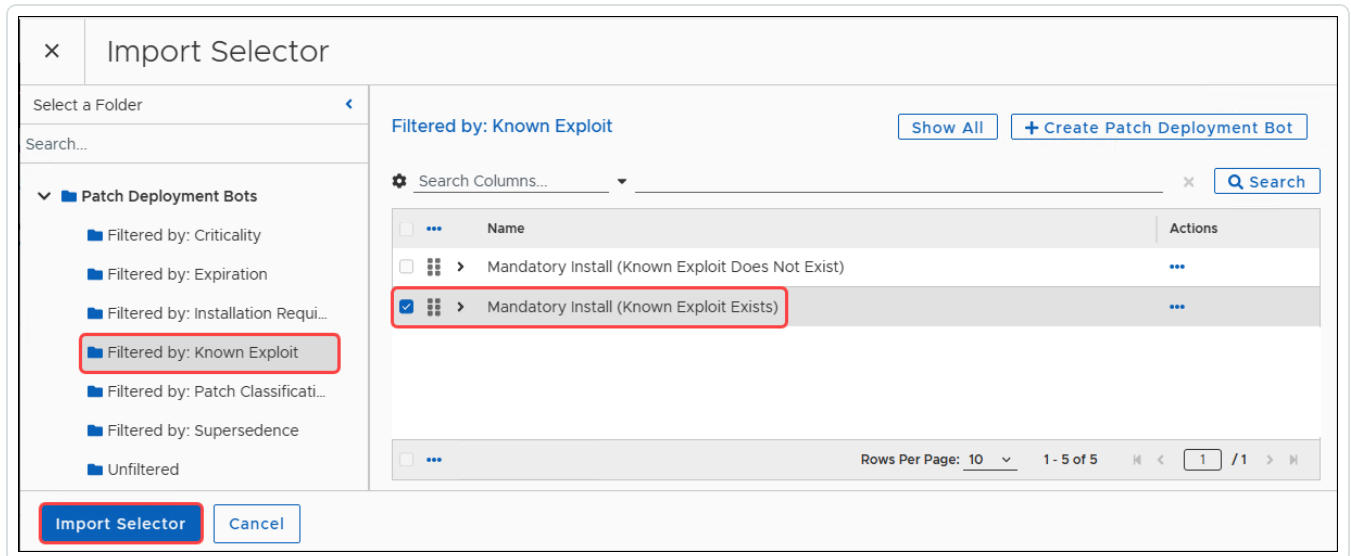
Open and Save a Patch Deployment Bot Template

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



Tip: To create customized Deployment Bots, Tenable Patch Management recommends entering a support ticket and requesting assistance from Tenable Patch Management.

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



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

Patch Filter Conditions



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

Proceed carefully when customizing Patch Filter Settings. Enter a support ticket and request assistance from Tenable Patch Management .

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

▼ Patch Filter Settings

Patch Filter Condition ⓘ [+ Import Selector](#)

▼ Select Operator or Condition

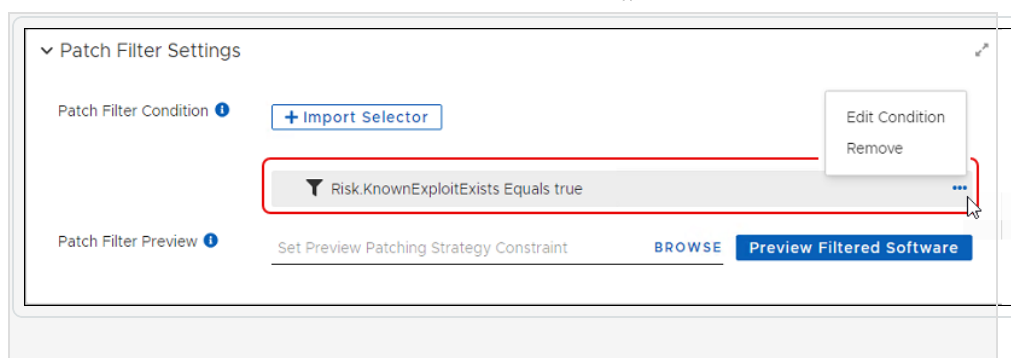
Patch Filter Preview ⓘ Initial Approval - Risk-Based Mandatory Deployment [BROWSE](#) × [Preview Filtered Software](#)

Configurable conditions include using **+ Import Selector**, which allows you to use an existing Patch Filter to validate new patches submitted to this Bot. You can also use the **Select Operator or Condition** to create a flexible patch filtering process. With no filter settings applied, the Bot processes all patches.

Edit or Remove Existing Patch Filter Conditions

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

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

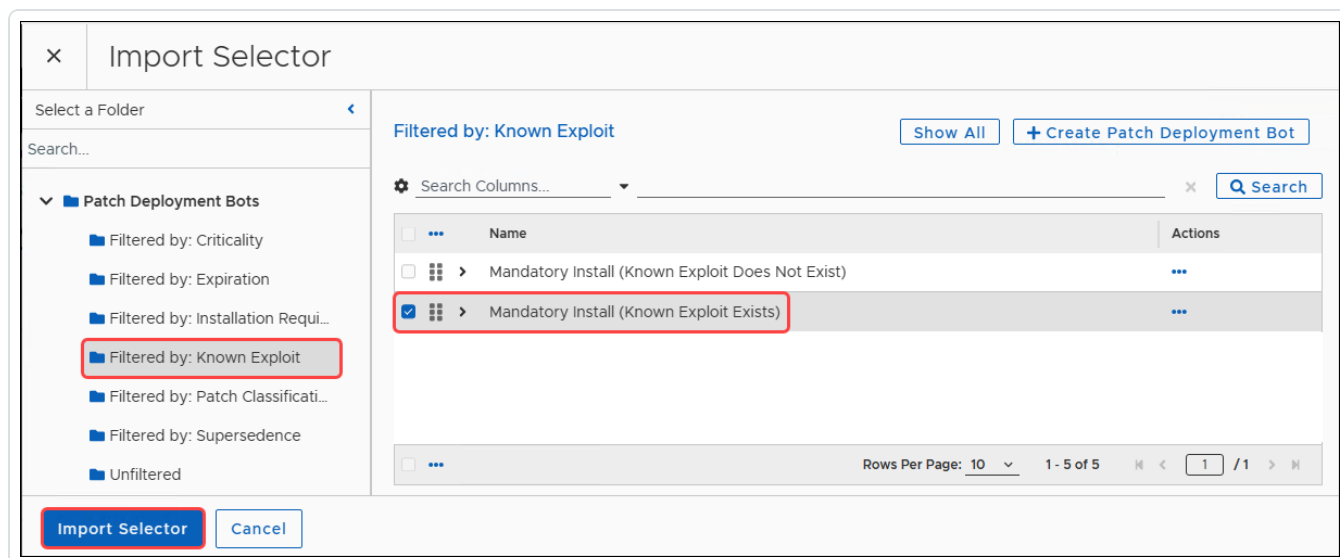


Add Patch Filter Conditions

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

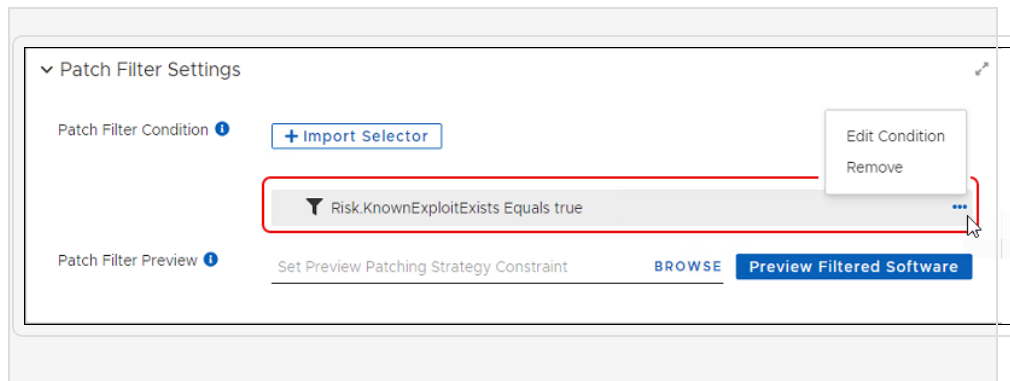
1. Select **+ Import Selector** in the Patch Filter Settings dialog of an [open Bot template](#).
2. Select an existing **Filtered by:** folder from the list of Patch Deployment Bots, and then select one or more filters to use in this Bot.

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

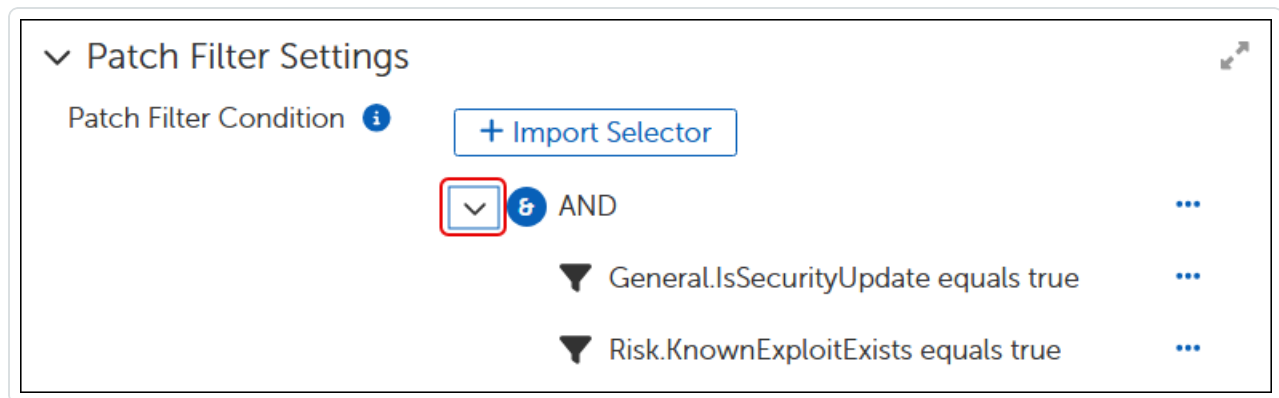


3. Select **Import Selector** at the bottom left of the dialog. This returns you to the Patch Filter Settings where the condition logic now displays as `Risk.KnownExploitExists Equals`

true.



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



Set and Change Patch Filter Conditions

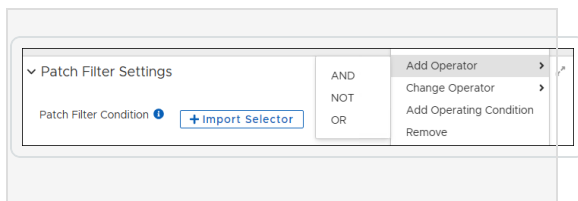
Use Operating Conditions and Operators to manually set multiple Patch Filter Conditions to use for this Bot. You must add the operator before you can add the condition. To add multiple conditions, repeat this section as needed.

Tip: SSL Verification - Splunk requires all connections to verify SSL by default and not be configurable via the UI. To configure your TSC connection to not verify SSL certificate you will need to modify `{SPLUNK_HOME}/etc/apps/TA-tenable/bin/tenable_consts.py` and set `verify_ssl_for_sc_cert = False`.

Add or Remove an Operator



1. In the Patch Filter Settings of an open Bot template, delete any existing Filter Conditions.
 - To **remove** an existing condition, click the ellipsis to the right of the existing filter, and select Remove.
 - To **add** the condition in again as part of a string, make note of the name for later use.
2. Select the **ellipsis (...)** to the right of Select Operator or Condition, and then select **Add Operator**.
3. Select the **operator** you want to use (AND, NOT, OR). For example, to filter out specific patches, select **NOT**.

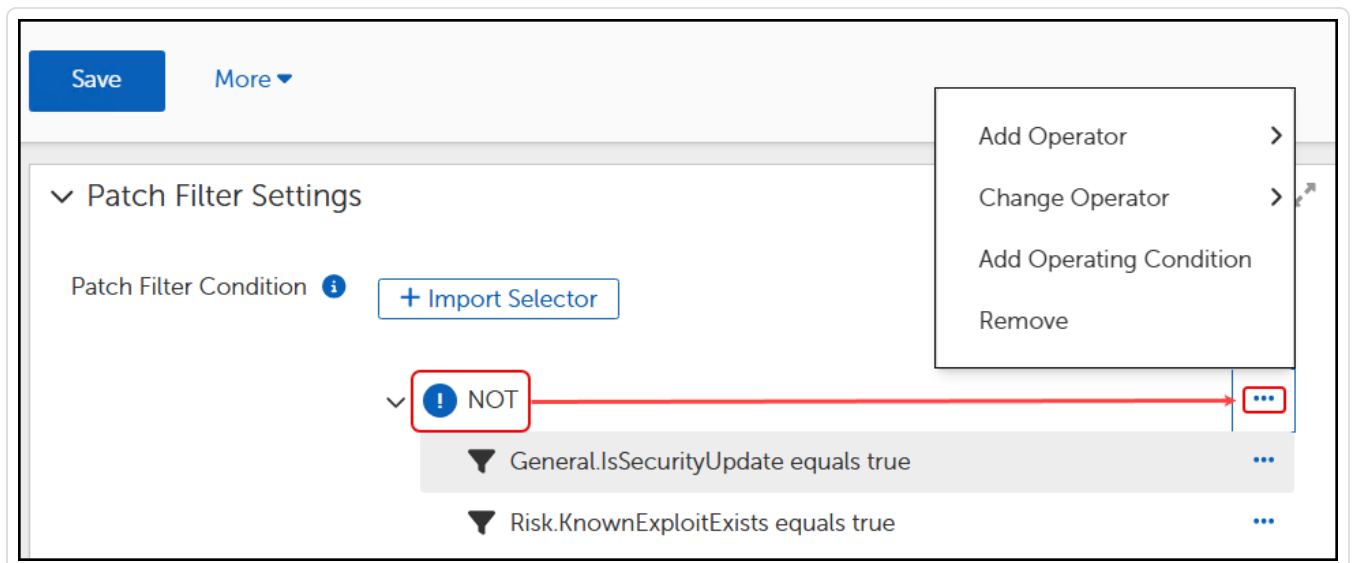


This returns you to the **Patch Filter Settings**, which shows the operator you selected.

4. Continue to [Add an Operating Condition](#).

Change an Operator

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





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

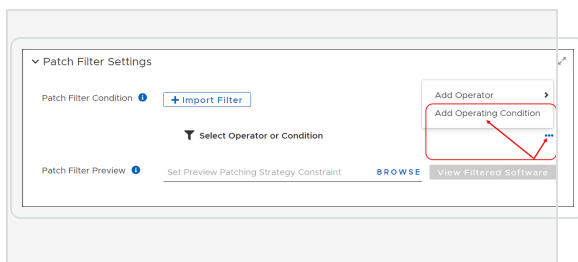


3. Select **Save** on the upper left-hand corner of the Patch Filter Settings workspace:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.

Add an Operating Condition

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

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



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

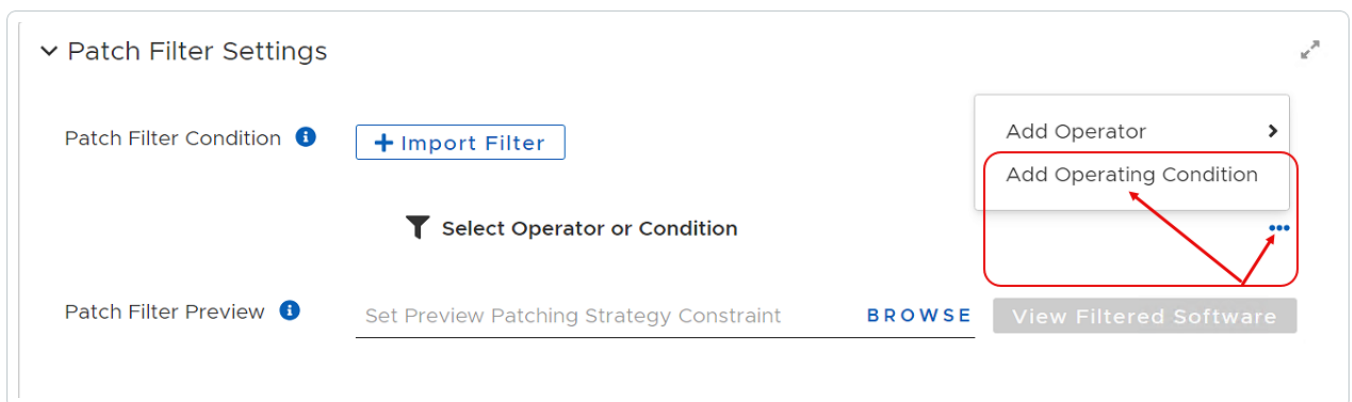


- See [Patch Filter Settings](#) for a description of each available setting.
 - If you removed a Patch Filter Condition previously, you may add it back here.
3. Set the **Operating Condition** to **Equals**, and then choose one of the following for the **Value**:
 - **Updates** - Exclude Windows updates.
 - **Upgrades** - Exclude Windows upgrades.
 - **Windows 11 upgrades** - Exclude upgrades to Windows 11.
 4. Select **OK**. This returns you to **Patch Filter Settings**, which now shows WSUS.Classification Equals *<selected value>* as a condition for excluding patches.
 5. See [Preview Software Filtered by Conditions](#) to confirm that the **Software Patches** listed do not include those you excluded.

Filter Out Specific Patches by Product ID

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

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



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

×

Creating Operating Condition

Data Column *

Operating Condition *

Values *

Relationships.Product

Realtime.FolderIndicators

Relationships.Product

Relationships.PrerequisiteInstallTree

Relationships.FollowupInstallTree

Relationships.PrerequisiteInstalls

Relationships.FollowupInstalls

Relationships.Supersedes

Relationships.SupersedesRemovalRequired

Relationships.SupersededBy

Relationships.Parent

Relationships.Children

Repair.InstallerType

Repair.PreActionSequence

Repair.ActionSequence

Repair.CustomizerUI

Repair.PostActionSequence

Repair.AutoItScript

Repair.InterferingProcesses

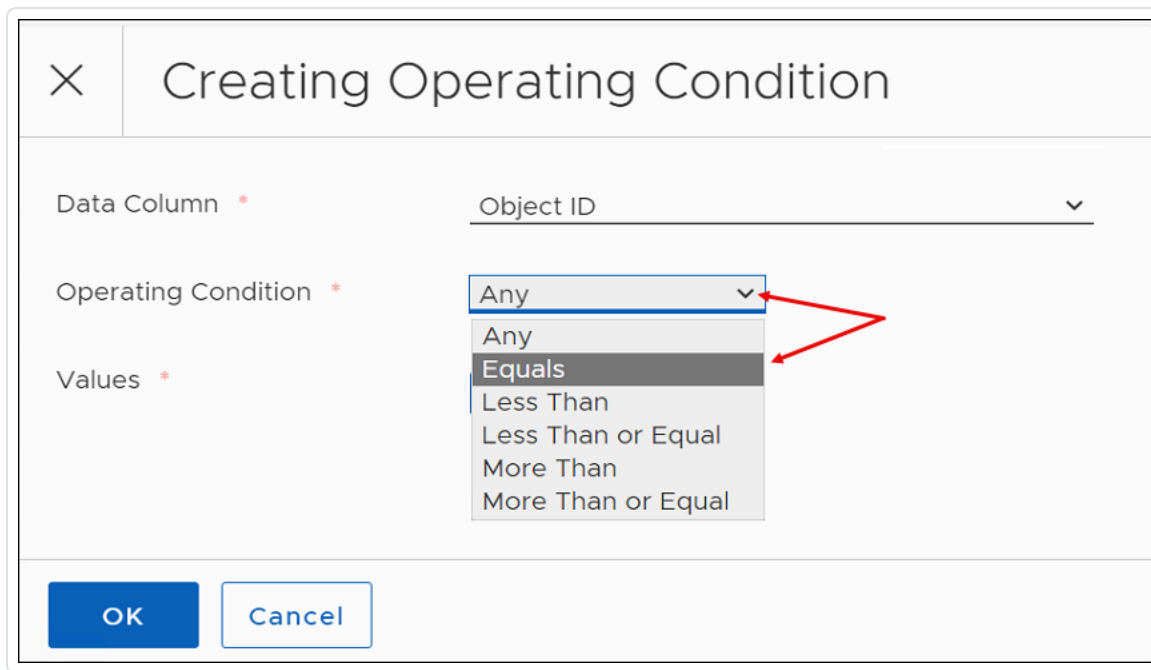
Repair.InterferingProcessesToWaitFor

Repair.InternetRequired

OK

Cancel

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



Creating Operating Condition

Data Column * Object ID ▼

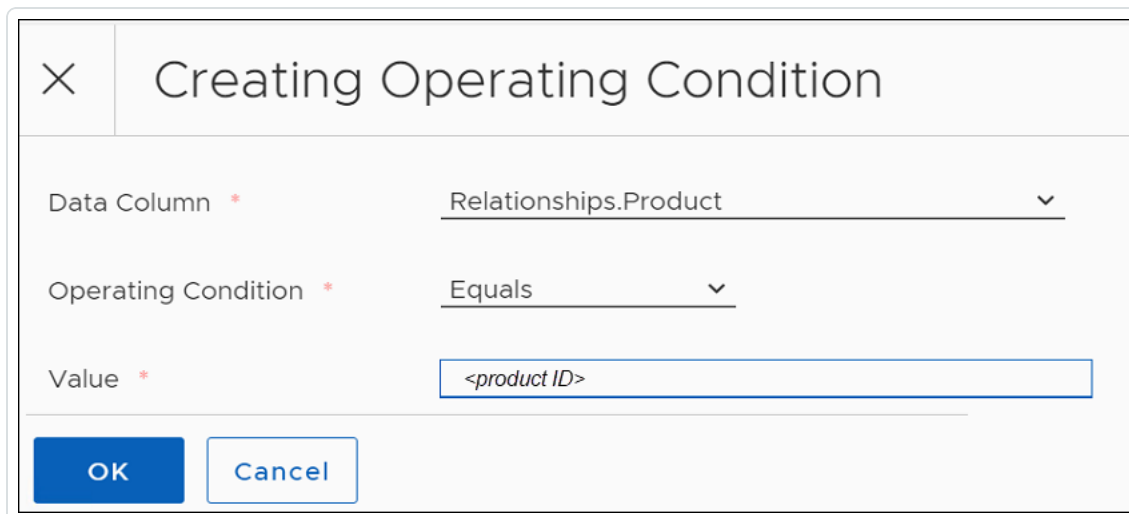
Operating Condition * Any ▼

Values *

Any
Equals
Less Than
Less Than or Equal
More Than
More Than or Equal

OK Cancel

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



Creating Operating Condition

Data Column * Relationships.Product ▼

Operating Condition * Equals ▼

Value * <product ID>

OK Cancel

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

Preview Filtered Patches

Preview Software Filtered by Conditions

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



1. Select **Preview Filtered Software** on the lower-right corner of the **Patch Filter Settings**.
2. Select the **Software Patches** tab to see the Software Patches included in this Bot with your filter.
3. Select the **Software Releases** tab to see the Software Releases included in this Bot with your filter.
4. Select **OK** to return to the **Patch Filter Settings**.

Preview Software Filtered by a Strategy

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

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

Configure Bot Settings

Select Deployment Settings

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



▼ Bot Settings

Bot Settings ⓘ

☒ Deployment Settings

☐ Bot Workflow

Desired State ⓘ

Mandatory Install ▼

Urgency ⓘ

Low ▼

Business Units ⓘ

[+ Add Business Units](#)

With Deployment Settings selected, complete the following steps.

1. Set the Desired State:
 - a. Select the input line for **Desired State** to view the menu options.
 - b. Select a **State** from the list (Mandatory Install, Do Not Install, Rollback, Uninstall).
2. Set the Urgency:
 - a. Select the input line for **Urgency** to view the menu options.
 - b. Select an **Urgency** setting from the list (Low, Normal, High, Critical).
3. Select **Save** at the upper left to save your progress:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.
4. Continue with [Add Business Units](#).

Business Units for Bot Deployment Settings

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



1. Select + Add Business Units:

Bot Settings

Bot Settings ⓘ ☒ Deployment Settings ☐ Bot Workflow

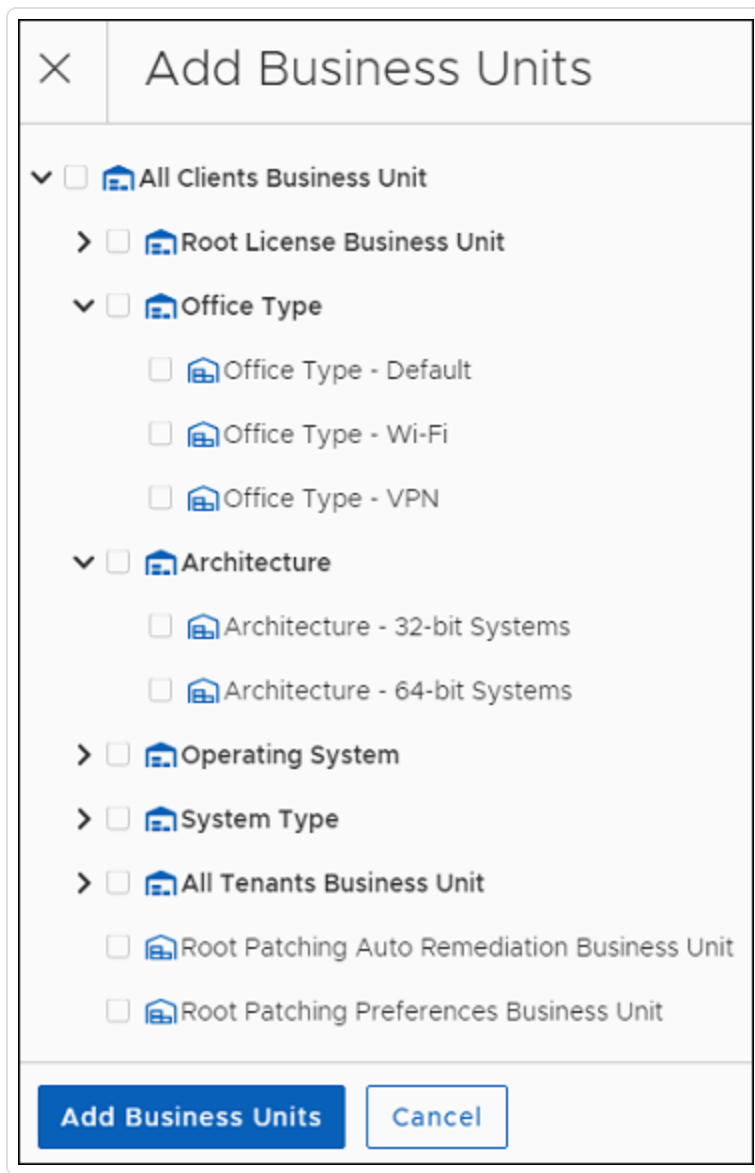
Desired State ⓘ Mandatory Install ▼

Urgency ⓘ Low ▼

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

- With no Business Units added to the Bot, the patching cycle patches the devices in all Business Units identified in the Patching Strategy.
- With one or more Business Units added to the Bot, the patching cycle patches the devices in the Business Units. The Patching Strategy must include the same Business Units as part of its assigned Deployment Wave (see [Deployment Settings](#)).

2. Select the right arrow next to a Business Unit type to expand one or more **Business Unit** structures.



× Add Business Units

▼ ☐ All Clients Business Unit

➤ ☐ Root License Business Unit

▼ ☐ Office Type

☐ Office Type - Default
 ☐ Office Type - Wi-Fi
 ☐ Office Type - VPN

▼ ☐ Architecture

☐ Architecture - 32-bit Systems
 ☐ Architecture - 64-bit Systems

➤ ☐ Operating System

➤ ☐ System Type

➤ ☐ All Tenants Business Unit

☐ Root Patching Auto Remediation Business Unit
 ☐ Root Patching Preferences Business Unit

Add Business Units Cancel

3. Select one or more **Business Units** to include in this Deployment Bot.
4. Select **Add Business Units** on the bottom left to return to the Deployment Bot template.
5. Select **Save** at the upper left to save your progress:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.

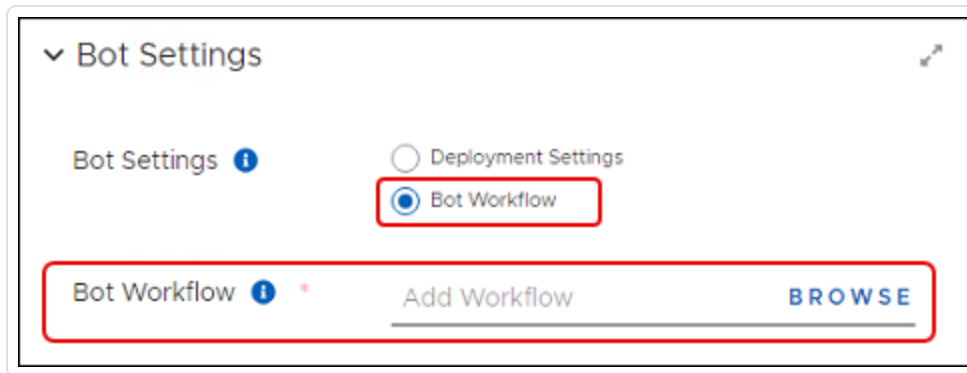
Now, when you need to add this Deployment Bot to a Patching Strategy or other object, you will see it in the list of available Deployment Bots.

Use a Custom Deployment Bot Workflow



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

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



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

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

3. Select the workflow **Name**, and then click **Add Workflow** on the bottom left to include the workflow in the Bot Settings.
4. Select **Save** at the upper left to save your progress:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.

Notification Bots

Patch Notification Bots generate notifications to alert administrators or users about the release or deployment of new patches that meet Patch Filter Settings in the Bot. When the Notification Bot detects patches that match a specified filter expression, the Bot generates a notification to include in the notification cycle. The notification cycle follows the Patching Strategy or Deployment Channel configuration that contains the Notification Bot.

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



Patch Notification Bot Template Naming Conventions

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

Normal Notification

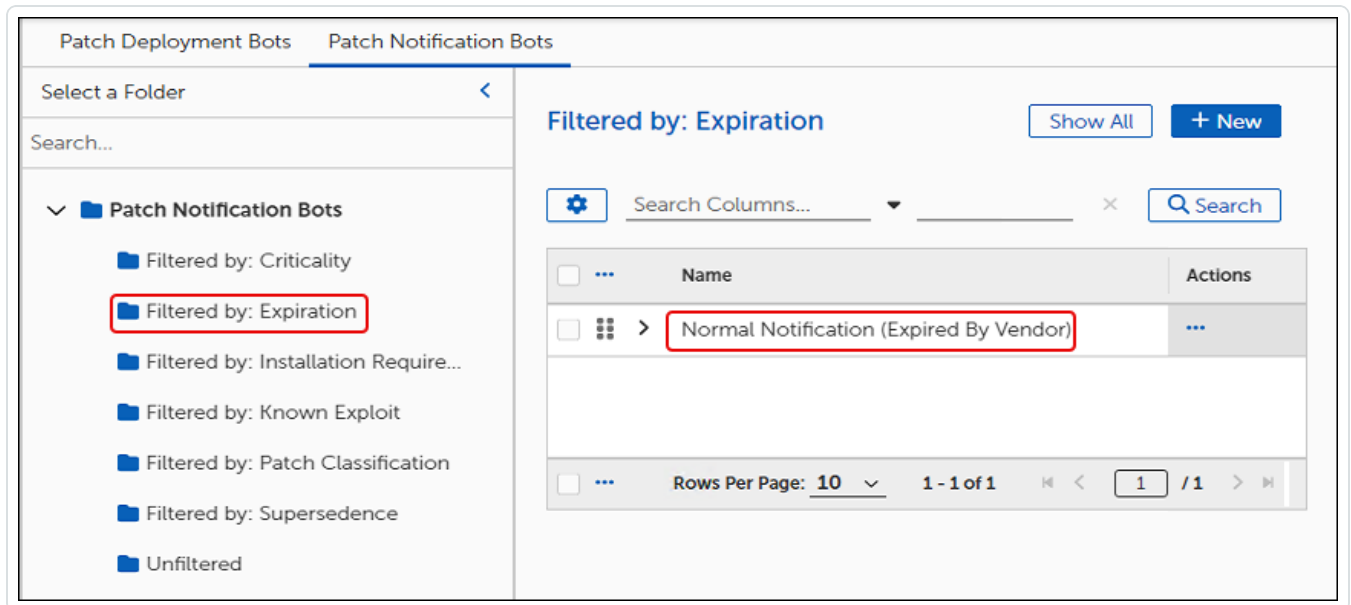
These templates filter several aspects of patches based on risk. They include different rollout schedules and approval levels, and all require mandatory installation.



Creating Notification Bots

Open and Save a Patch Notification Bot Template

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



5. Save the template with a new title:

- a. Select **More** in the upper-left corner of the dialog, and then select **Save As**.
- b. Enter a new name for the template, and then click **Save as** on the lower-left corner of 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 corner of the dialog.

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

Create an Output Expression

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

Configure Notification Bot Settings

Except for Communication Providers, use the previously configured settings in the template. For details, see [Communication Providers](#).

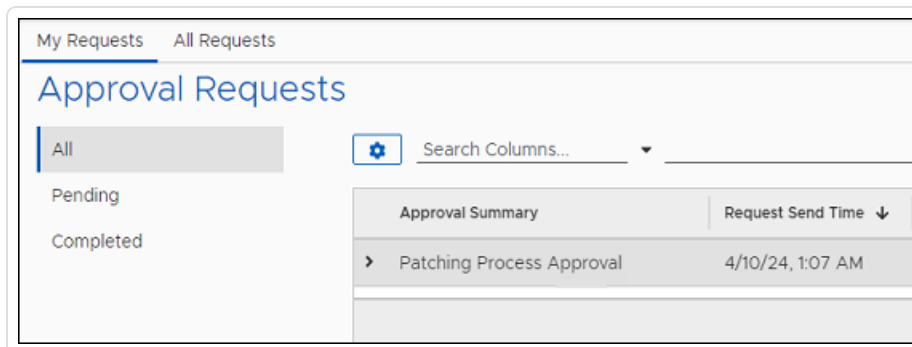


1. In the Notification Bot template, scroll down to **Communication Providers**, and then click **+ Add Communication Providers**.
 - Select one or more providers to use for notifications by this Bot.
 - If you do not see the provider you want to use, see [Communication Providers](#) to add it.
2. Select **Save** at the upper left to save your progress:
3. Check the **Error View** and resolve any errors.
4. Select **Save** again if you make any changes.

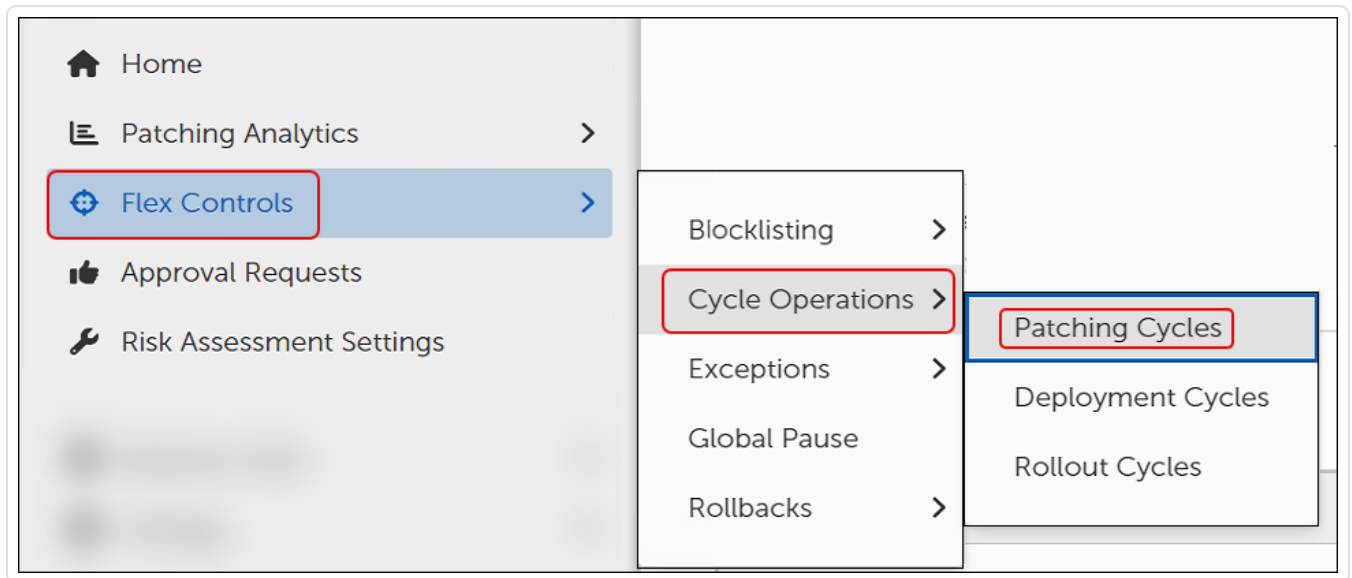
View a Staged Patching Strategy

After you [Enable the Patching Strategy](#), you can view the pending approval request.

1. Select the **Approval Requests** in the left navigation menu of the [Patch Management Dashboard](#).



- The view defaults to All requests, which includes pending and completed.
 - The Patching Strategy you just enabled appears in the Approval Summary table with a Request Status of In Progress and Awaiting Response.
2. Select **Flex Controls > Cycle Operations > Patching Cycles** from the left navigation menu of the [Patch Management Dashboard](#).



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

Running Patch Processes

Search Columns... Search

Patching Strategy	Status	Business Units	Start Time ↓
964 patching strategy	Waiting	All Clients Business Unit	4/19/24, 11:00 AM

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

4. Select **Approval Requests** in the left navigation menu, and then click the **Patching Strategy** in the table.
5. Select **Approve**, and then click **Back to Approval Requests**. You can wait until the patch time passes, or you can start the deployment manually.

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

Communication Providers



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

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

Using Communication Providers

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

Open and Save a Communication Provider Template

1. Select **Communication Providers** in the left navigation menu of the [Patch Management Dashboard](#).
2. Select the **Name** of an existing template to open it, and then save the template with a new title:
 - a. Select **More** in the upper-left corner of the dialog, and then select **Save As**.
 - b. Enter a new name for the template, and then click **Save as** on the lower-left corner of 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 corner of the dialog.

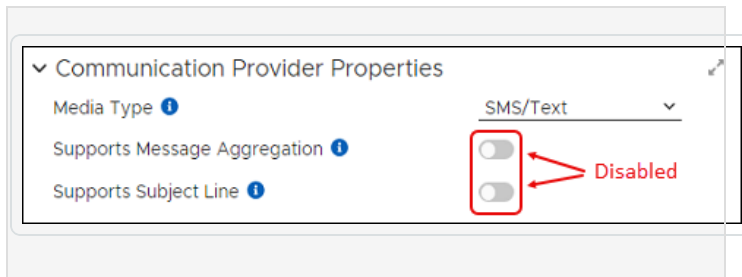
Set Communication Provider Properties

1. Scroll down to **Communication Provider Properties** box in an open Communication Provider template, and then choose a **Media Type**. This is the media type used by the provider you are creating.
 - If the **Media Type** is related to an **SMTP Server**, skip to **Step 5**. These Media Types use neither Message Aggregation nor Subject Line indicators. Both items default to disabled.



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

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



3. Select the **Supports Subject Line** button to enable or disable (default) whether this Communication Provider supports the ability to include a subject line with its messages.
4. Enter the **From Address** to use for communication using SMTP Server settings if the Communication Provider supports this field. If not, leave the field blank.
5. Select **Save** on the upper left to save your progress:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.

Patching Processes

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

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

- Approval processes for patches.
- User notifications.
- Prestaging content.
- Deploying to test labs before production.



- Routing patches to appropriate deployment channels, or directly routing them to business units for deployment.

Creating Patching Processes

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

Patching Process Templates

Immediate Deployment, No Phasing, Initial Patch Manager Approval

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

Immediate Deployment- Initial Patch Manager Approval

Approval required prior to deployment, then deploys at once.

Immediate Deployment, No Approvals Needed

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

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

No approval needed prior to deployment. Deploys in phases

- **Immediate Deployment No Approval**

No approval needed prior to deployment. Deploys at once.

- **Immediate Phased Deployment No Approval**

No approval needed prior to deployment. Deploys in phases.

Phased Deployment Processes, Approval Required

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

Approval required prior to deployment. Deploys in phases.



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

Approval needed prior to deployment. Deploys in phases.

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

Approval needed prior to deployment. Deploys in phases.

Content Prestaging Settings

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

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

Defining Content Prestaging Settings

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

Content Prestaging settings include two options:

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

Push Content



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

This push occurs at once when the metadata updates include the latest content that meets patching requirements.

- **Handled by Workflow** - When enabled as part of a Patching Process, Deployment Channel, or Business Unit template, pushes the content upon deployment of the Patching Process.

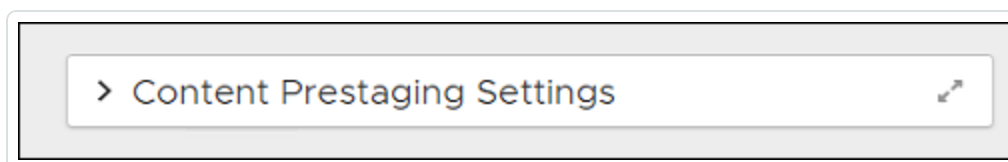
Pull Content

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

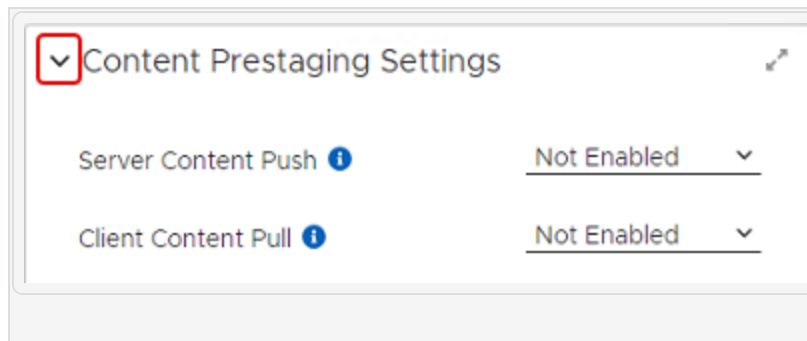
Set Content Prestaging Settings

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

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

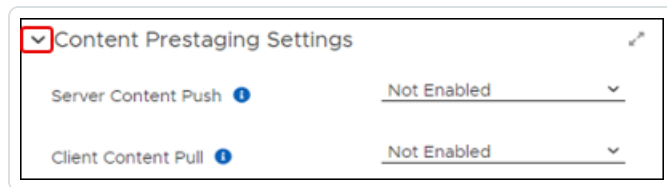


2. Expand the Content Prestaging Settings box to view the available settings.

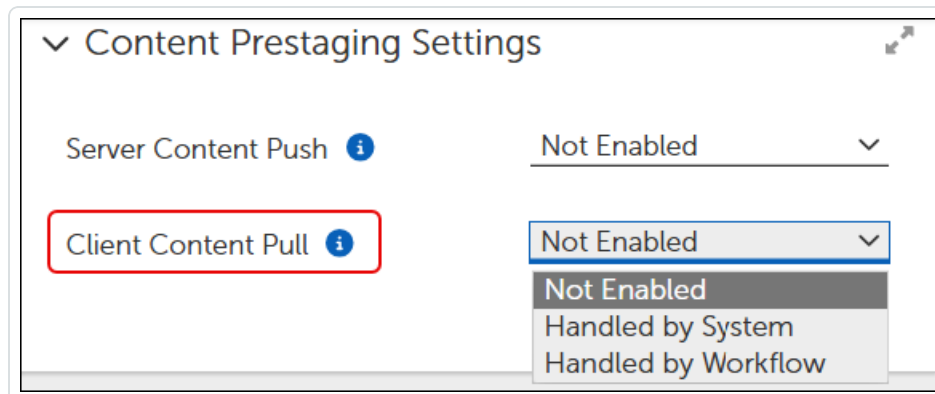


Enable Client Content Pull

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



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



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

Enable Server Content Push



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

Content Prestaging Settings

Server Content Push ⓘ Not Enabled ▼

Client Content Pull ⓘ Not Enabled ▼

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

Content Prestaging Settings

Server Content Push ⓘ

Client Content Pull ⓘ

Not Enabled ▼

Not Enabled

Handled by System

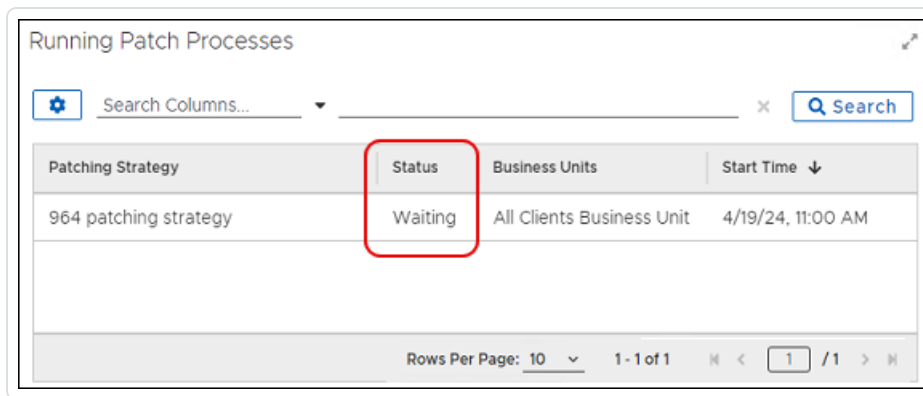
Handled by Workflow

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

Start the Patching Strategy Manually

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

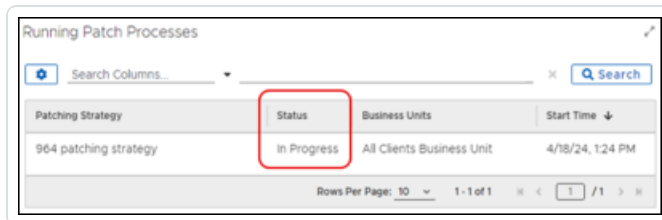
1. Select **Flex Controls > Patching Cycles**, and then click the name of the Patching Strategy to open the Cycle Information.



Patching Strategy	Status	Business Units	Start Time ↓
964 patching strategy	Waiting	All Clients Business Unit	4/19/24, 11:00 AM

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

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



Patching Strategy	Status	Business Units	Start Time ↓
964 patching strategy	In Progress	All Clients Business Unit	4/18/24, 1:24 PM

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

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

New in this Tenable Patch Management Release

Along with other improvements to usability and performance, the Tenable Patch Management product for v9.2.967.16 includes the following new features:

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

Getting Started with Tenable Patch Management

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



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

Prerequisites

Before using Tenable Patch Management, set up your environment using the *Tenable Patch Management Installation Guide*.

Supported Platforms and Distributions

- **Windows**

OS and third-party patching.

- Driver patching for Dell, HP, and Lenovo.
- BIOS updates.

- **Linux**

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

- Ubuntu 22.04 LTS
- Ubuntu 24.04 LTS
- Debian 11
- Debian 12
- CentOS Stream 9
- CentOS Stream 10

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 for details.

- **Mac**

Third-party patching (no OS patching).

Support for devices running the following macOS versions:

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

Supported Browsers

Tenable Patch Management supports the following browsers:

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

Note: Do not use Microsoft Internet Explorer

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

Logs for Server and Client



Access Server and Client logs using the  on the Admin Portal or by navigating to the locations below:

Tenable Patch Management/ Tenable Patch Management/Logs.

Tenable Patch Management/ Tenable Patch Management/Logs.

Tip: The Server and the Client installation set a path variable for all installed files and maps it to the relative install location. Use the %*Tenable Patch Management*% or %*Tenable Patch Management*% variable to identify file locations from a Command Line prompt.

Customer Support

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

Tenable Patch Management Admin Portal

Tenable Patch Management uses both the Admin Portal and the Patch dashboard for configuration and management.

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

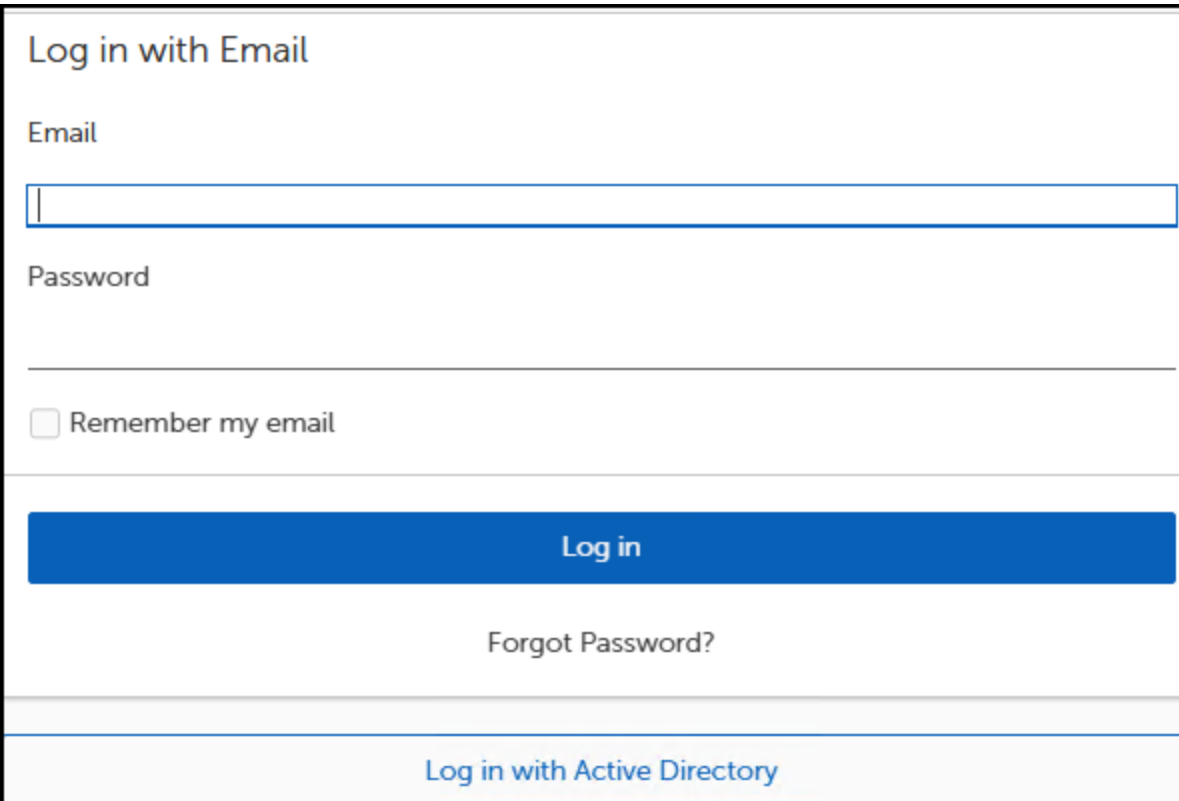
1. Enter the **Fully Qualified Domain Name (FQDN)** for the Tenable Patch Management followed by the **port (optional)** into the browser address bar:

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

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



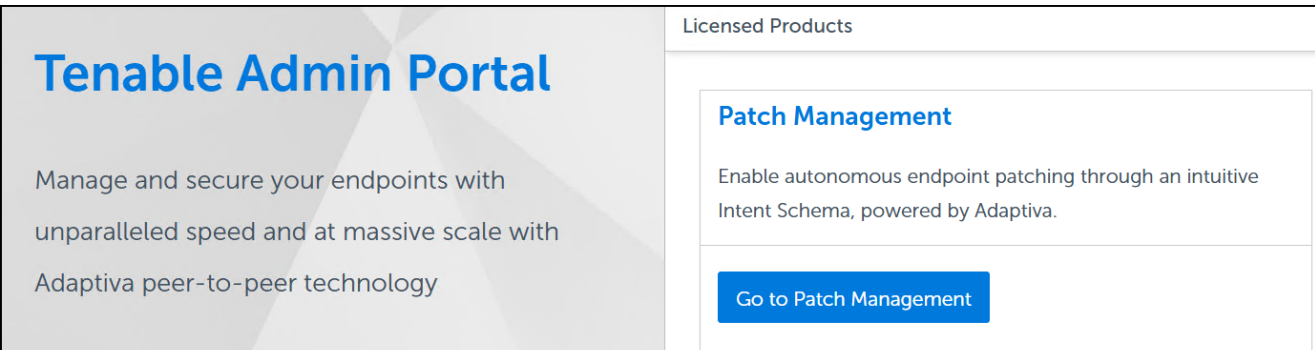
2. Press **Enter**. The Admin Portal login dialog opens.



The login dialog is titled "Log in with Email". It contains an "Email" label above a text input field, and a "Password" label above a password input field. Below the password field is a checkbox labeled "Remember my email". A large blue "Log in" button is centered below the inputs. Below the button is a link "Forgot Password?". At the bottom of the dialog is a link "Log in with Active Directory".

3. Log in using one of the following methods:

- Click **Login with Active Directory** (recommended). If you are unable to log in with Active Directory using Mozilla Firefox, see [Resolve Mozilla Firefox Active Directory Login Issue](#).
- Enter a native **Login ID** (email address) and password, and then click **Log in**. The email address does not need to be active.



The dashboard is split into two main sections. The left section has a large heading "Tenable Admin Portal" and a paragraph: "Manage and secure your endpoints with unparalleled speed and at massive scale with Adaptiva peer-to-peer technology". The right section is titled "Licensed Products" and contains a card for "Patch Management". The card text says: "Enable autonomous endpoint patching through an intuitive Intent Schema, powered by Adaptiva." Below this text is a blue button labeled "Go to Patch Management".

After successfully logging in, the dashboard appears.



Resolve Mozilla Firefox Active Directory Login Issue

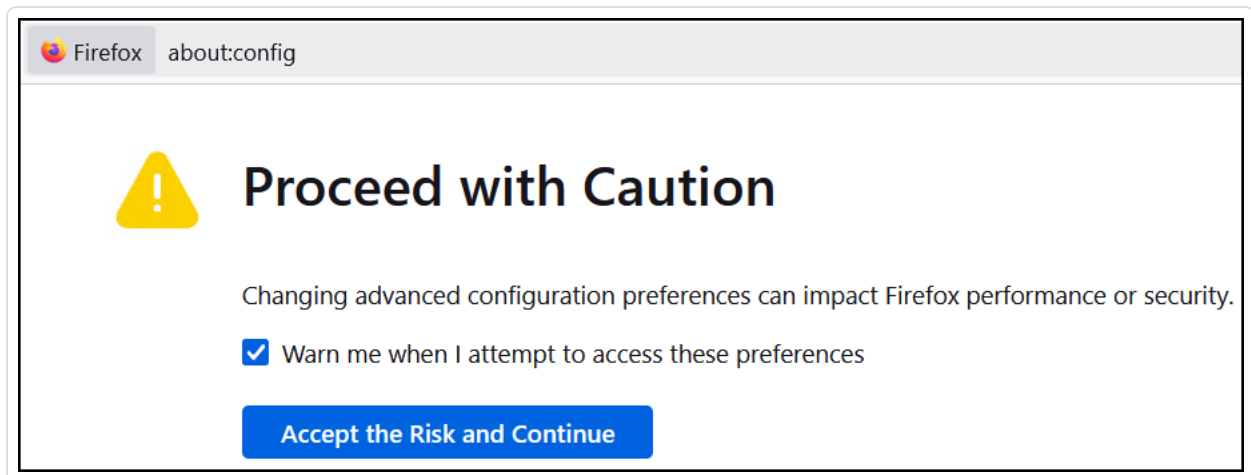
To access the Admin Portal using Active Directory, Mozilla Firefox requires adding the Tenable Patch Management as a trusted URI to enable SSPI/Kerberos authentication. If you receive the following message when using Mozilla Firefox to log into the Admin Portal using Active Directory, use the steps provided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

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

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

`about:config`

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



3. Add the Tenable Patch Management fully Qualified Domain Name (FQDN) as a trusted device:



- a. Enter `network.negotiate-auth.trusted-uris` on the search line.

Search: ☐ Show only modified preferences

network.negotiate-auth.allow-non-fqdn	false	
network.negotiate-auth.allow-proxies	true	
network.negotiate-auth.delegation-uris		
network.negotiate-auth.gsslib		
network.negotiate-auth.trusted-uris		
network.negotiate-auth.using-native-gsslib	true	

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

network.negotiate-auth.trusted-uris ☒

- c. Select the checkbox to save, and then return to the Admin Portal tab.

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

Licensing Tenable Patch Management

Tenable Patch Management requires a license for each active client. The license key contains the licensed company name and client count. The Tenable Patch Management 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 for the first time or your key has expired, the software prompts you for a license key at login.

Add a License Key



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

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



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

Target Collections for the Licensed Product

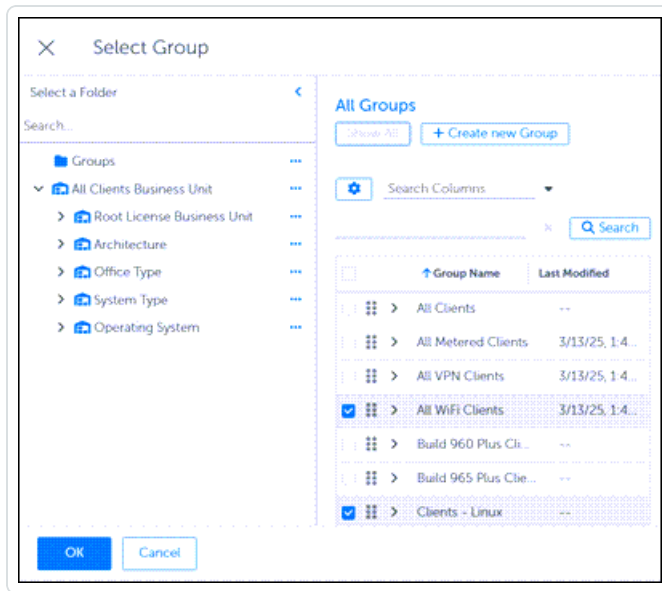
After entering a license key, select a Target Collection for the licensed product.

Caution: Use care when selecting **Use All Clients**. Earlier version of the installed Tenable Patch Management version do not support this feature and selecting it can corrupt the patch environment.

Tenable Patch Management recommends upgrading to the latest version of the product.

1. Select the Tenable Patch Management 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.

Patch Management Dashboard

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

Access the Patch Management Dashboard

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

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

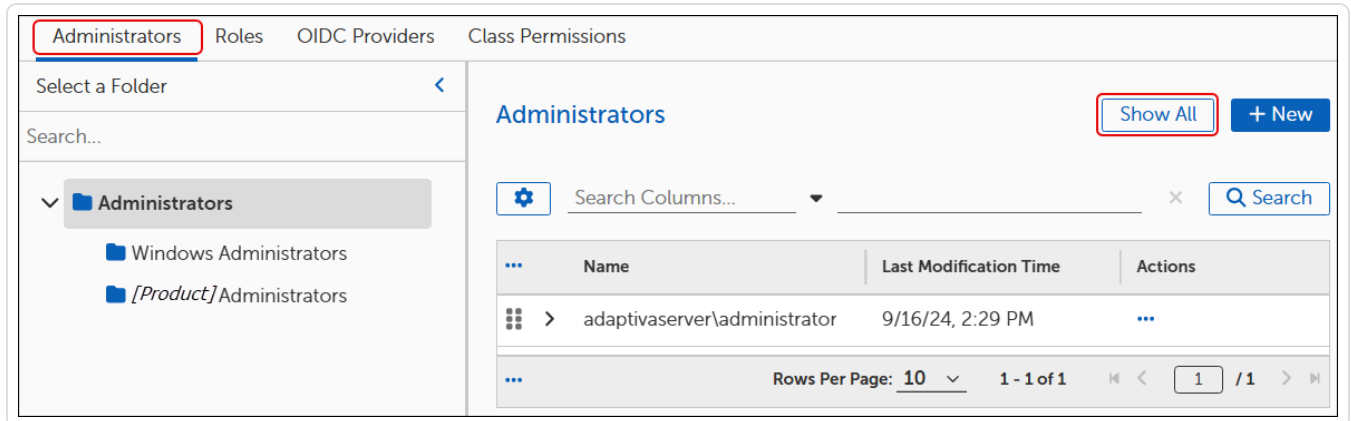
Administrators and Roles

View, create, or modify Administrators and Roles.

Access Security Settings

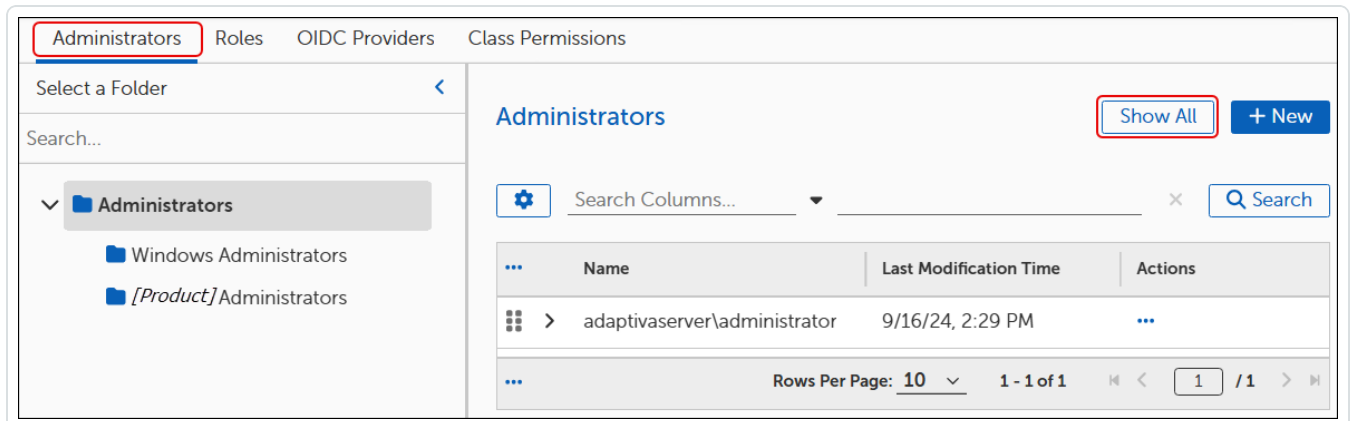


1. Select  on the upper right of the [Admin Portal](#) dashboard.
2. Select **Settings > Security > Administrator** to open the Settings page with the Administrators tab selected. To open to a different tab, select a different item from the final menu.
3. Select **Show All** to view existing administrators.



View Administrators

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

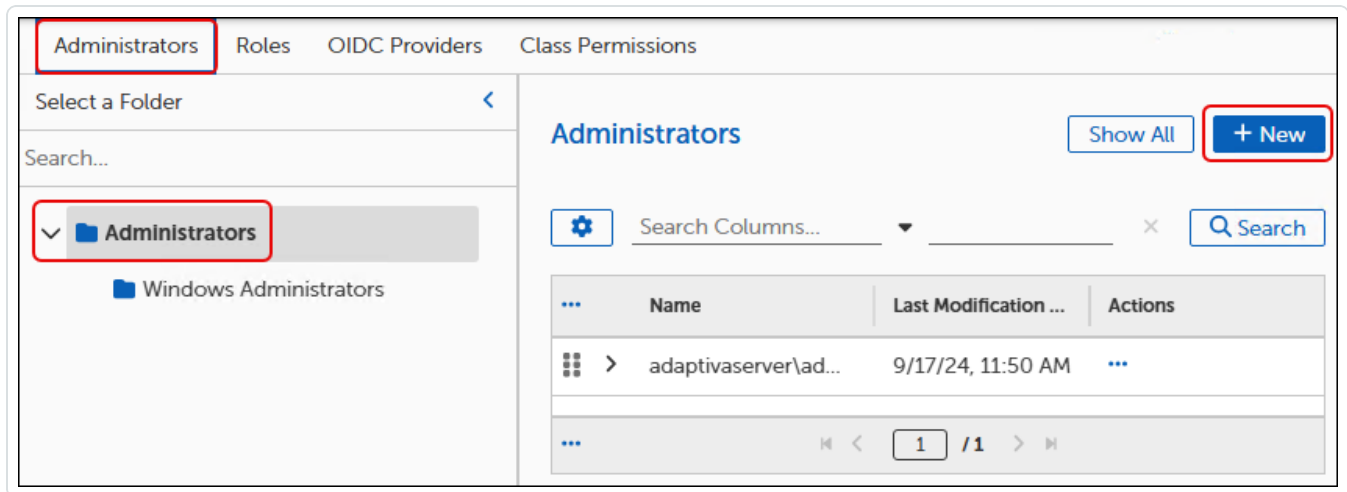


2. Select **Show All** to list all Administrators in the selected folder.

Create a New Administrator



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



2. Enter the **Administrator Details**:

1. Select the **Admin Type** login from the list. Tenable Patch Management recommends using Windows Active Directory.
2. Enter the email address and login details for the new administrator.

3. Enter the **User Details**:

1. Add the **Name** and contact details for the new administrator.
2. Choose country codes from the drop-down lists for phone numbers.

The screenshot shows the 'User Details' form in the Security Settings interface. The form is titled 'User Details' and contains several input fields with labels and red asterisks indicating required fields. The fields are: 'First Name', 'Last Name', 'Voice Phone Number' (with a dropdown menu), 'After Office Phone Number' (with a dropdown menu), 'Text Message Phone Number' (with a dropdown menu), 'WhatsApp Phone Number' (with a dropdown menu), and 'Teams Webhook URL'. Each field has a corresponding label on the right side of the form.



3. Add a **Teams Webhook URL**. If you need to create a Microsoft Teams Webhook URL see [Create a Microsoft Teams Webhook URL](#).

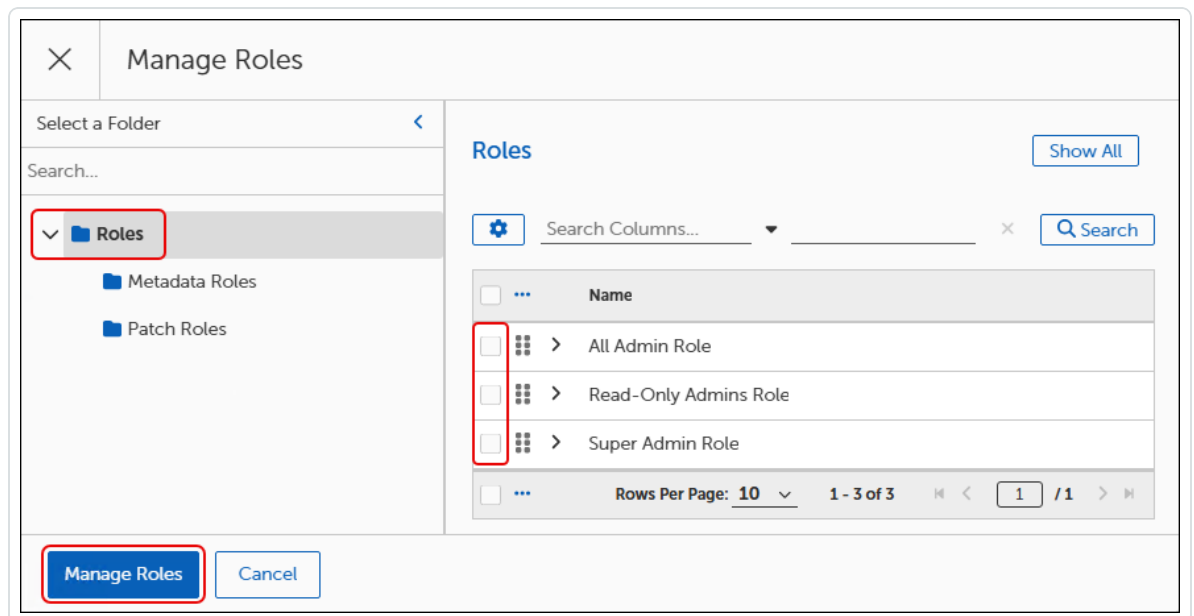
4. Assign **Direct Roles**:

1. Select **+ Manage Roles**.



2. Select one or more roles for the new administrator:

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



- To create additional roles, see [Create a New Role](#).

3. Select **Manage Roles** on the bottom-left corner of the dialog to return to the administrator details workspace.

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



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

Create a Microsoft Teams Webhook URL

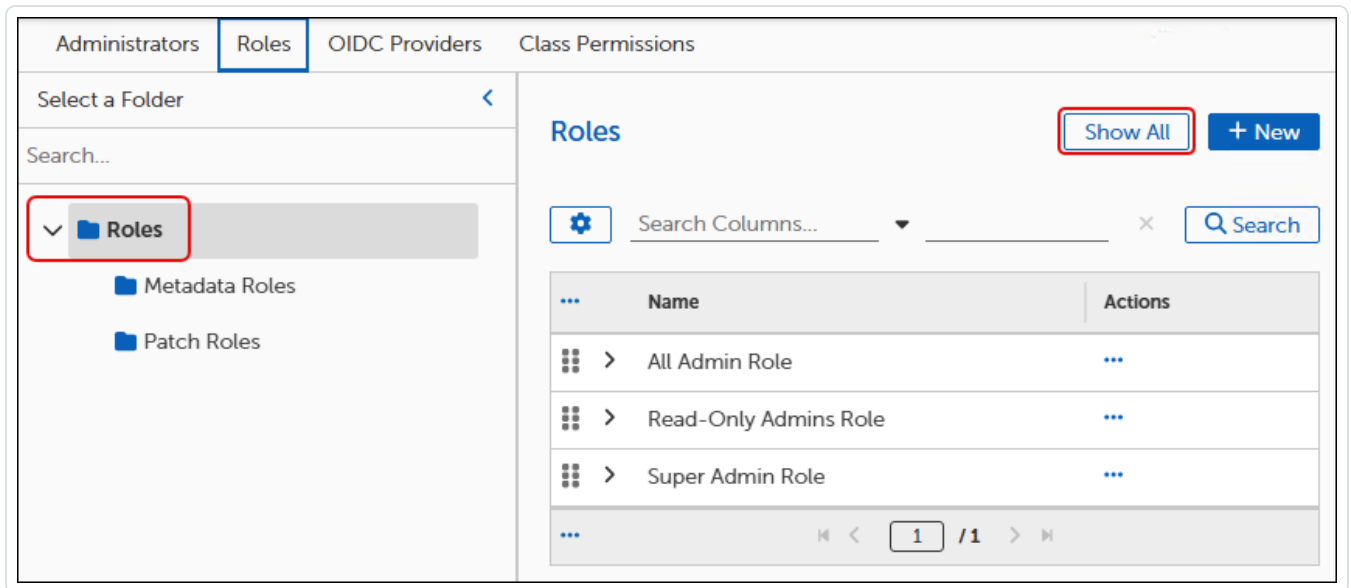
When adding a new administrator or modifying administrator details in Tenable Patch Management , add a Teams Webhook URL to post notices to a Teams channel, and then assign that URL to your administrators in Tenable Patch Management . Administrators can check the Teams channel for patch notifications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

1. Go to Microsoft.com for instructions on creating a Team and a Channel. The links below go to a third-party website outside of the Tenable Patch Management domain:
 - a. Go to [Microsoft Windows Team and Channel topics](#) to set up a new channel in an existing Team in Microsoft Teams, or create a new Team and add a channel for patch notification purposes.
 - b. Go to [Create an Incoming Webhook](#) to create the Webhook URL.
2. Open the **Admin Portal**, and then navigate to **Settings > Security > Administrators**.
3. Open an existing administrator or select **+NEW** to create a new Administrator.
4. Scroll down to **Teams Webhook URL** under User Details, and then paste the URL you generated in Step 1b into the associated text box.
5. Return to [Create a New Administrator](#) to complete any other administrator details.

View Roles



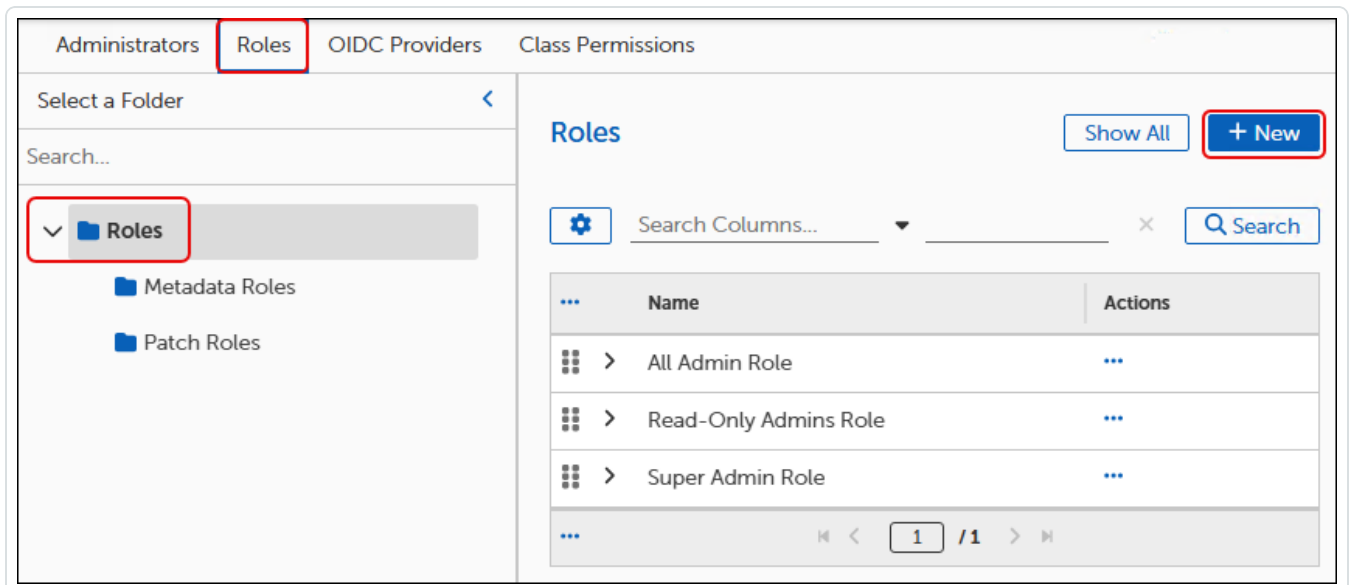
1. Select a **Roles** folder from the Roles tab of [Access Security Settings](#).



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

Create a New Role

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



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



▼ Role Properties

Role Name

Role Name

Role Description

Role Description

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

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

▼ Role Membership

Direct Administrators

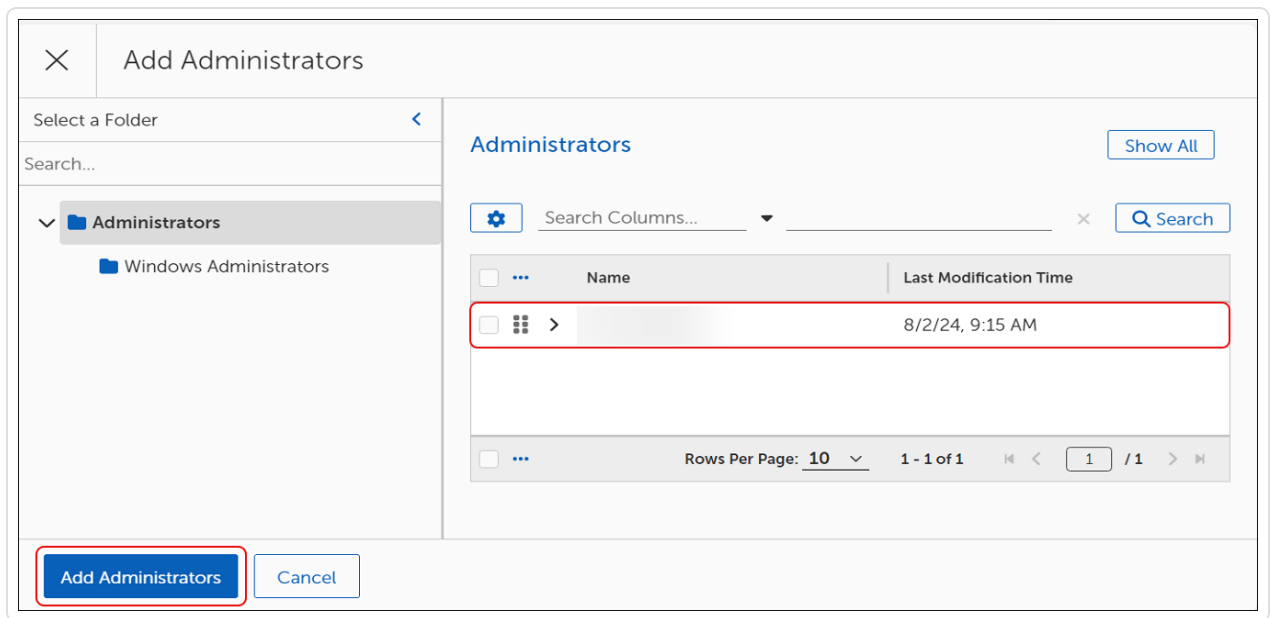
+ Add Administrators

Active Directory Groups

+ Add AD Group

No data provided

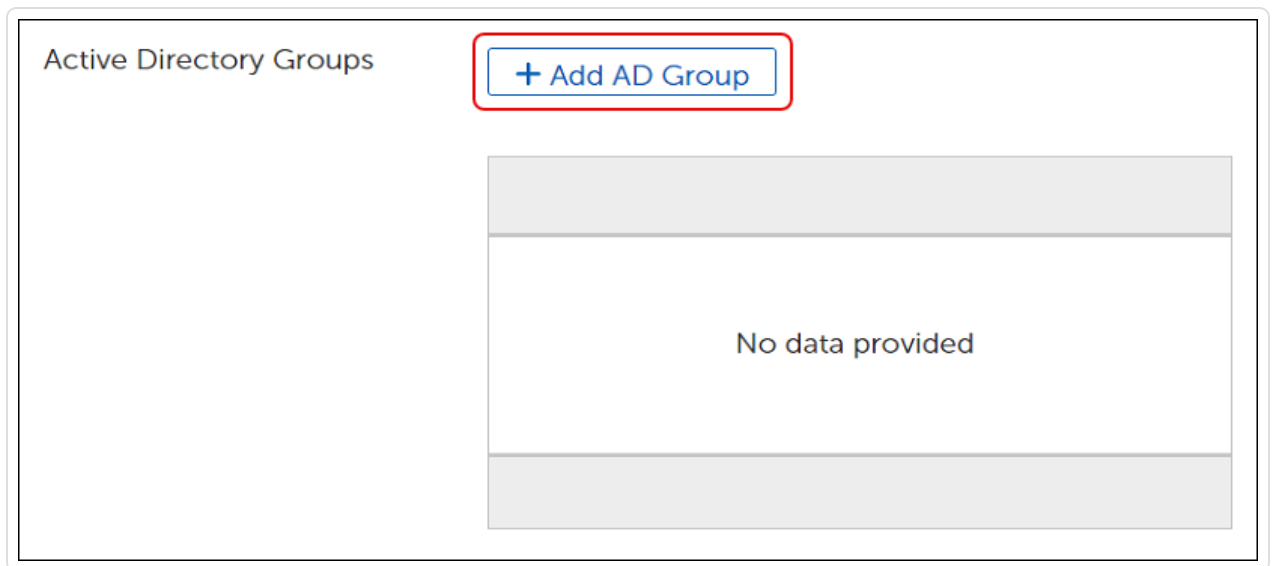
2. Select one or more administrators from the table for the new role.



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

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

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



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

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

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

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

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

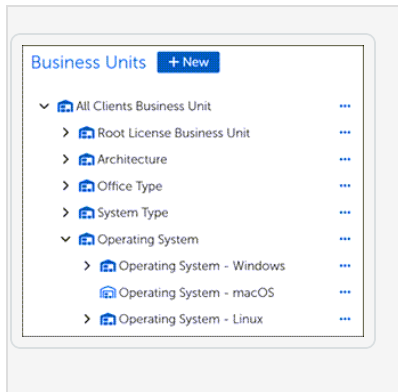
Business Units

Understanding Business Units

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



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



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

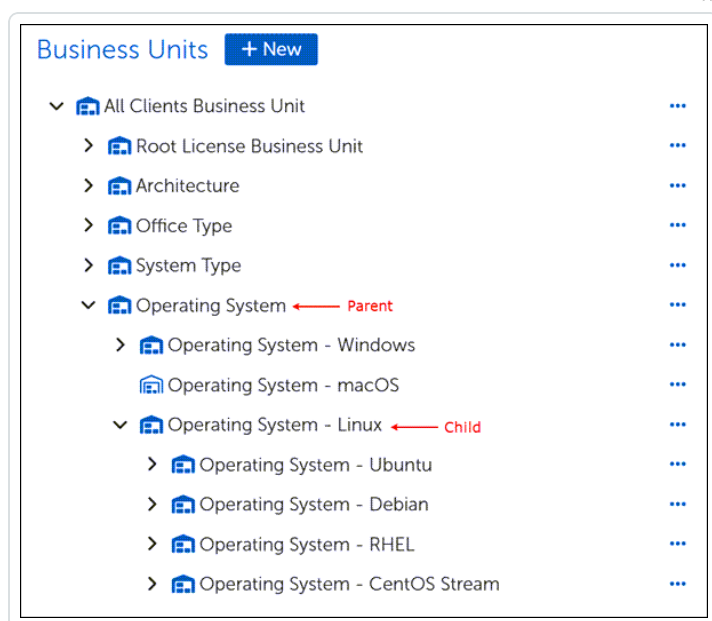
Note: When adding Business Units to a Patching Strategy, make sure that the Patch Deployment Bot for that Strategy specifies the same Business Units.

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

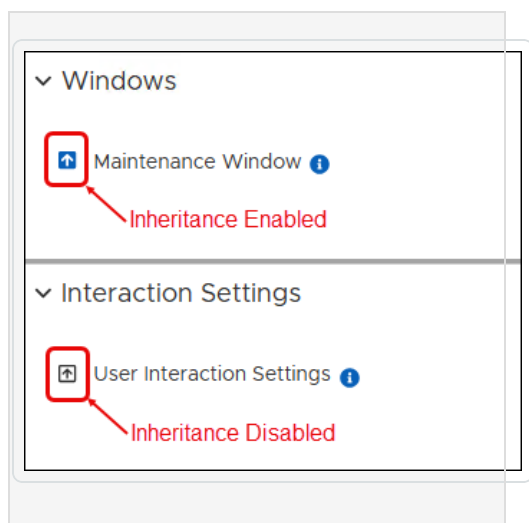
Parent and Child Business Units

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

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.



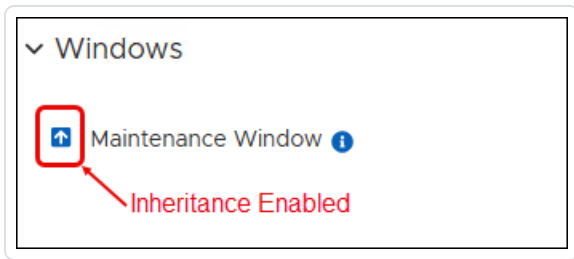
The hierarchical nature of Business Units allows a child Business Unit to inherit settings from its parent. An up-arrow with a blue background preceding a setting or process shows an inherited setting.

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



Managing Inheritance Settings

In Tenable Patch Management inheritance defaults to Enabled.

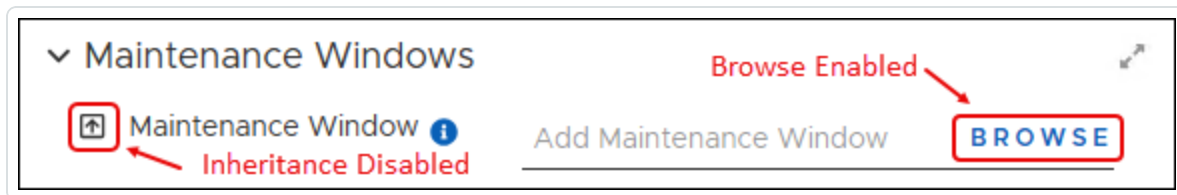


Note: The colors shown here are default color settings. If you change the Admin Portal theme settings to use different colors, your arrows and backgrounds might be different.

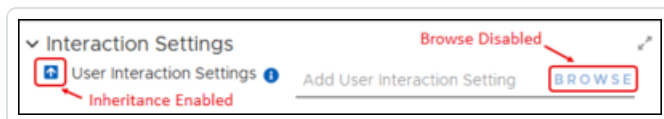
Enable Inheritance

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

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



2. Select the up-arrow icon to enable inheritance

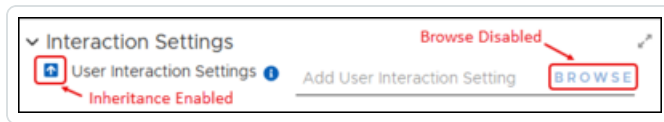


Disable Inheritance

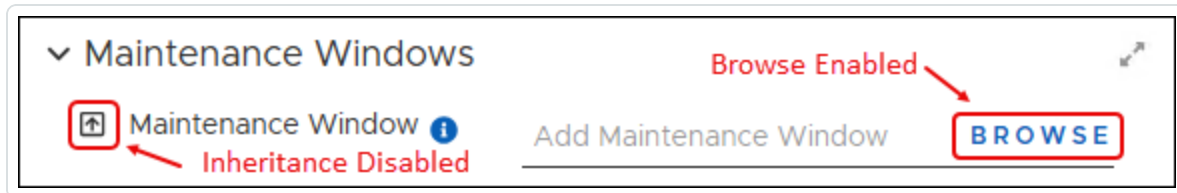
A black up-arrow with a white background preceding a setting or shows a disinherited setting. Disabling Inheritance enables the Browse button for the setting, which allows you to change the settings.



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



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



Organizing the Business Unit Hierarchy

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

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

Best Practices when Changing Priorities

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

- **Priority** - Do the settings and desired state of the new priority Business Unit match your expectations for the moved Business Unit?
- **Membership** - Are the devices in the moved Business Unit compatible with the new priority Business Unit?

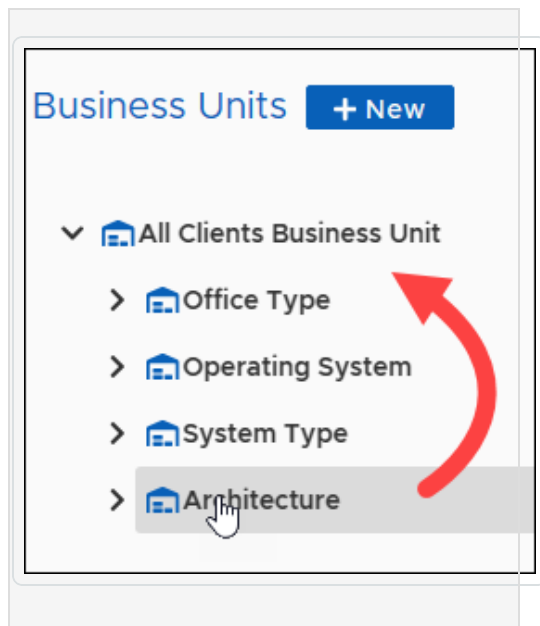


- **Inheritance** - Are the inheritance settings for the moved Business Unit still accurate in this new location?
- **Deployment Waves** - Is the Business Unit you are moving, or any of its ancestors included in a Wave Entry that includes descendants? If so, are those deployments still necessary?

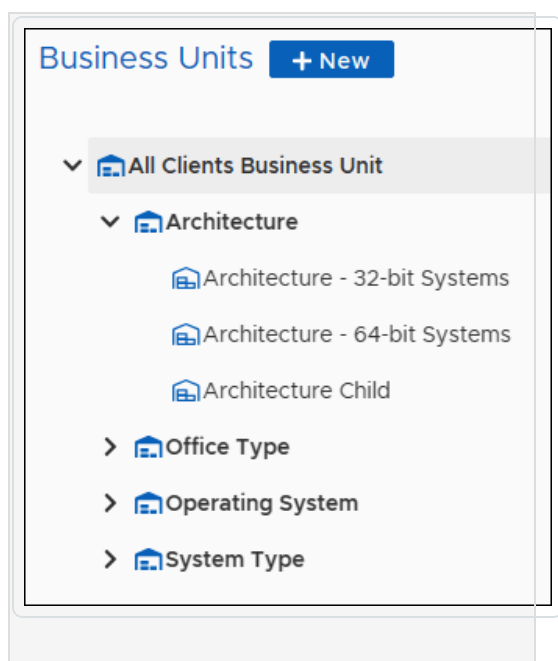
Further, is the new parent, or any ancestors, included in a Wave Entry that includes descendants? If yes, do you want the new BU included in those deployments?

Change the Order of the Hierarchy

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



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



Creating a Business Unit

Tenable Patch Management 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.

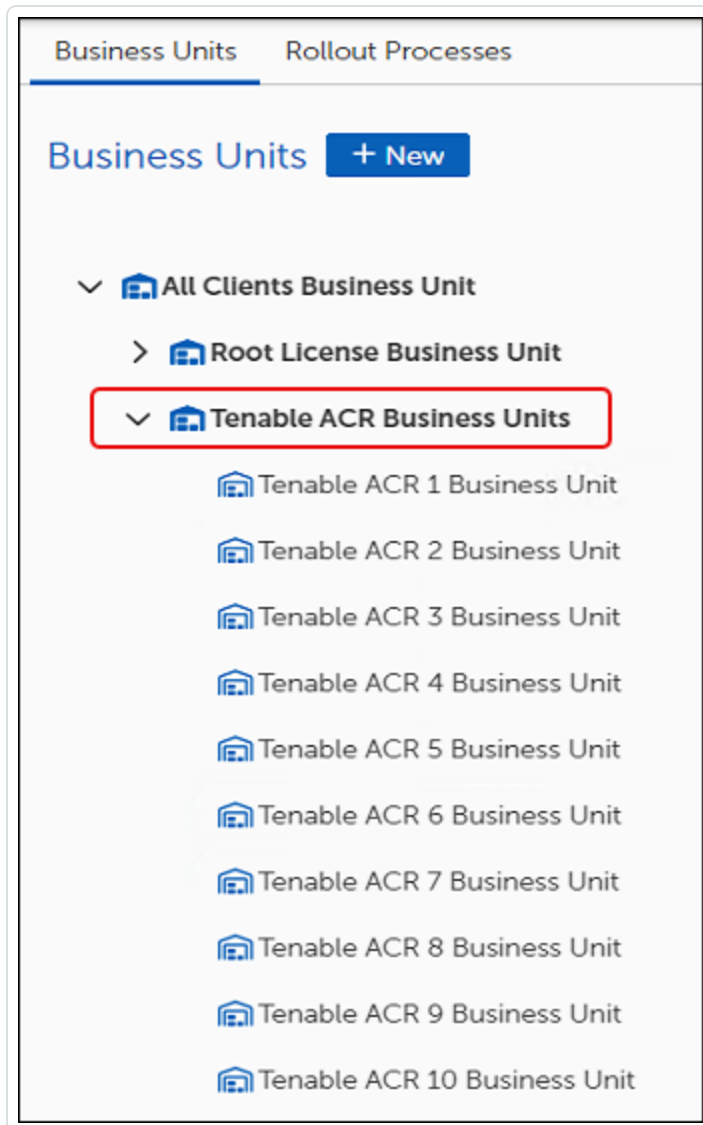
Caution: When modifying an existing Business Unit template to create a new configuration, be sure to verify that the Maintenance Window settings and the User Input Settings include the details you require for your Business Unit. Failure to provide these settings can result in installation failures.

Open and Save a Business Unit Template

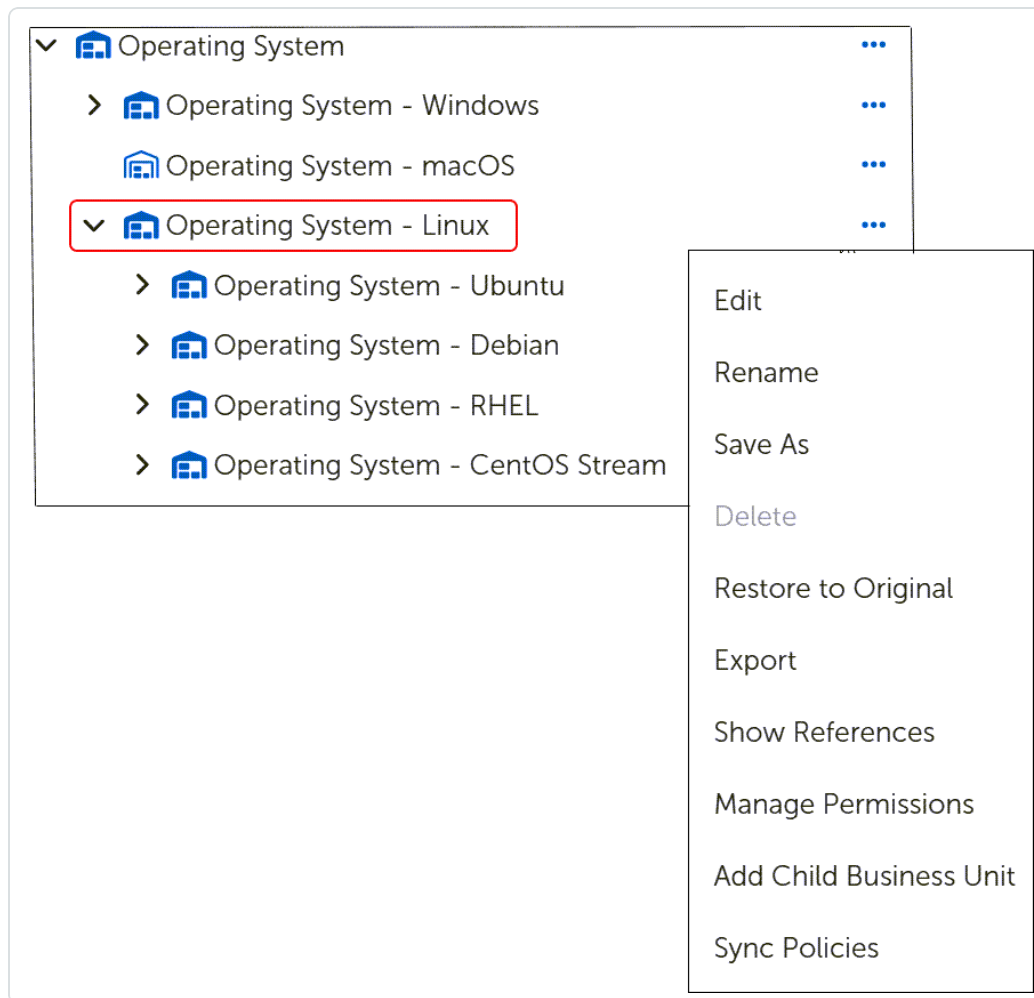
Except for Business Units provided for Root, you can copy the default templates and save them with new details, or you can create a new Business Unit.



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 corner of the dialog, and then select **Save As**.
- b. Enter a new name for the template, and then click **Save as** on the lower-left corner of 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 corner 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](#)).

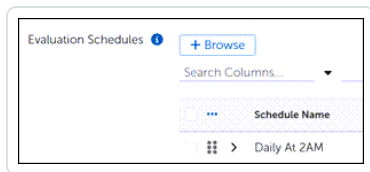
Add Evaluation Schedules to a Business Unit



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, click **+ Browse**, and then continue with the next step.



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

All Schedules

Show All

+ Create new Schedule

Search Columns...

Search

	↑ Schedule Name	Start Date	End Date	Last Modified
☐	> 00:00	1/1/00, 12:00 AM	--	3/22/23, 4:16 AM
☐	> 02:00	1/1/00, 2:00 AM	--	3/22/23, 4:16 AM
☐	> 08:00	1/1/00, 8:00 AM	--	3/22/23, 4:16 AM
☐	> 09:00	1/1/00, 9:00 AM	--	3/22/23, 4:16 AM

1 / 15

OK

Cancel

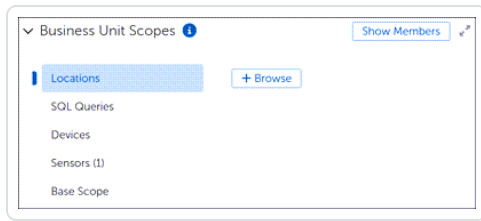
3. Select **Save** on the upper-left corner of the dialog to save your progress:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.

Configure Business Unit Scopes

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

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

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



Add Locations

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

1. Select **Locations** from Business Unit Scopes, and then click **+ 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 *Tenable Patch Management*.
3. Select **OK** on the lower-left corner 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 click **+ Add Query**. This opens the Add Query dialog.



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

×

Add Query

Name

Example Query (do not use)

Description

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

Type

☒ Client ID

Query

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

Add Query

Cancel

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

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

SQL Queries (1)

+ Add Query

☐	...	Query Name	Type	Actions
☐	>	Example Query	Client ID	...

☐ ...

Rows Per Page: 10

1 - 1 of 1

1 / 1

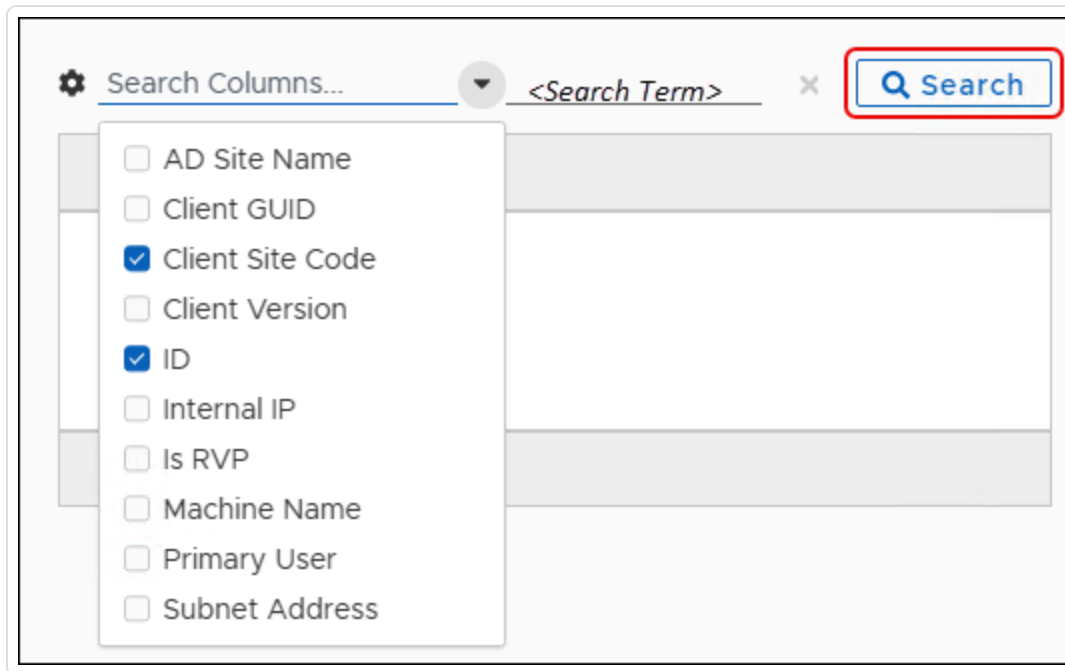
Add Devices

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

Note: 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 click **+ 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 click **Search**.



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

Add Sensors

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

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

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



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

Sensors + Add Sensor Group Scope

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

× Sensor Group Scope

Scope Name *

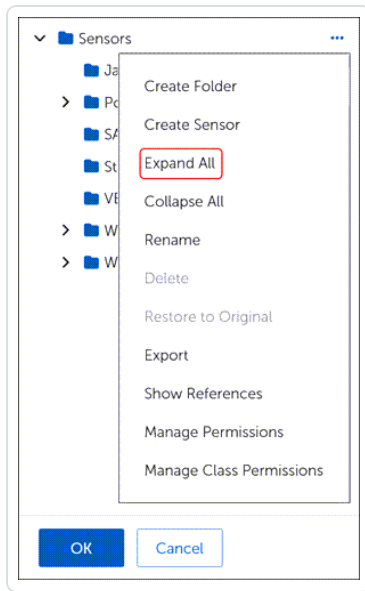
Scope Description

Sensor * BROWSE X

Filter Condition * ▼ Select Operator or Condition ...

OK Cancel

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

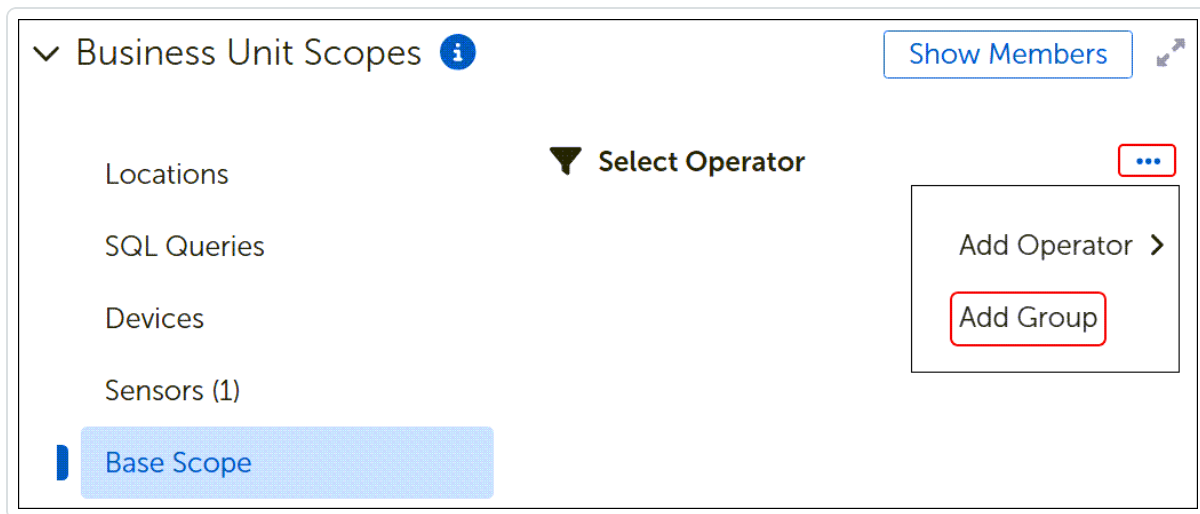


5. Select an item to use in your Sensor Group, and then click **Add Sensor**. This returns you to the Sensor Group Scope dialog. To add a Filter Condition, see [Patch Filter Conditions](#)
6. Select **OK** to return to the Business Unit template or change [Base Scope](#) settings.

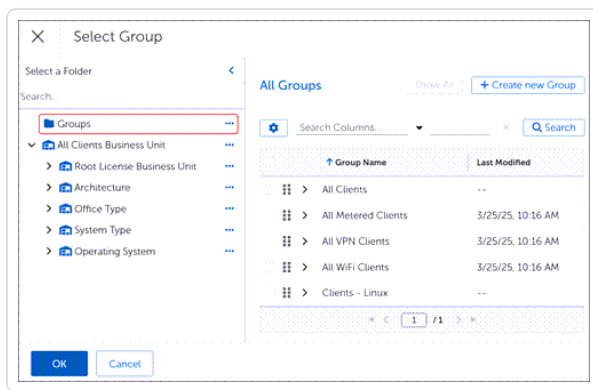
Set Base Scope

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**.

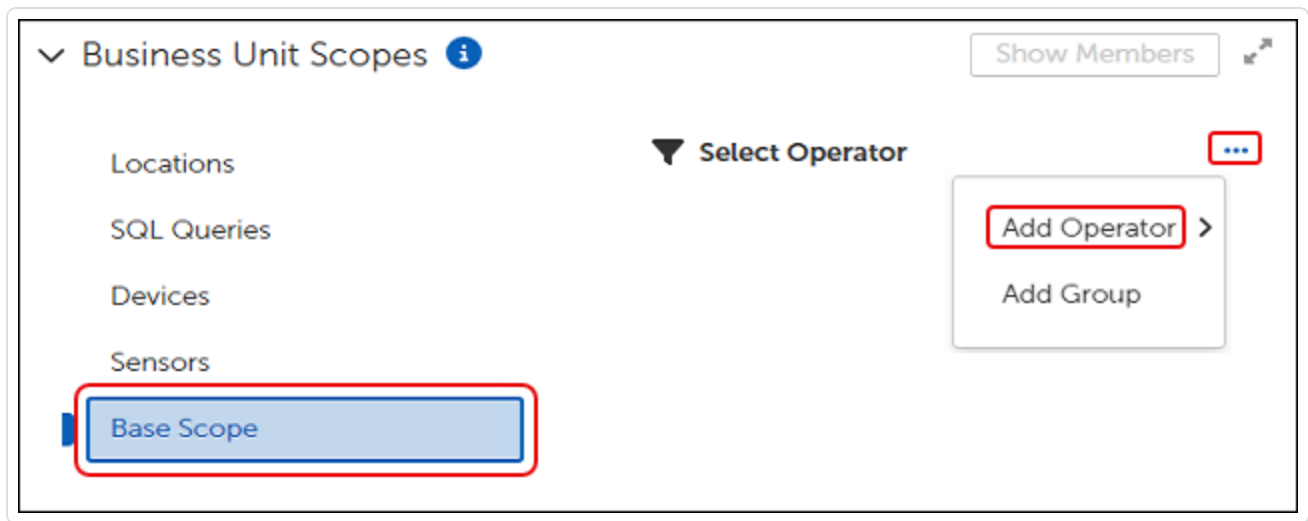
5. Select **OK** on the lower-left corner of the dialog. The entry under Business Unit Scopes shows the AND operator and the item you chose.

Add Multiple Groups or Business Units

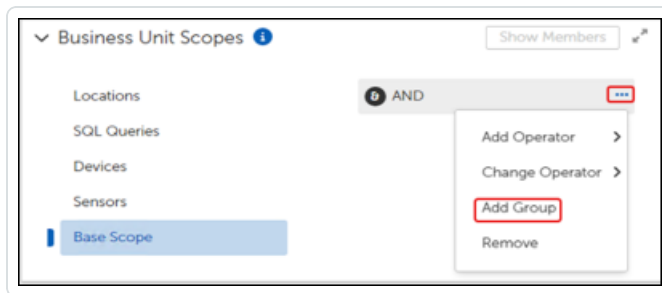
After setting the initial Base Scope, use this procedure to add additional Groups or Business Units to include in the Base Scope. You can add or exclude other Groups or Business Units or change Operators to customize your Base Scope depending on your needs.



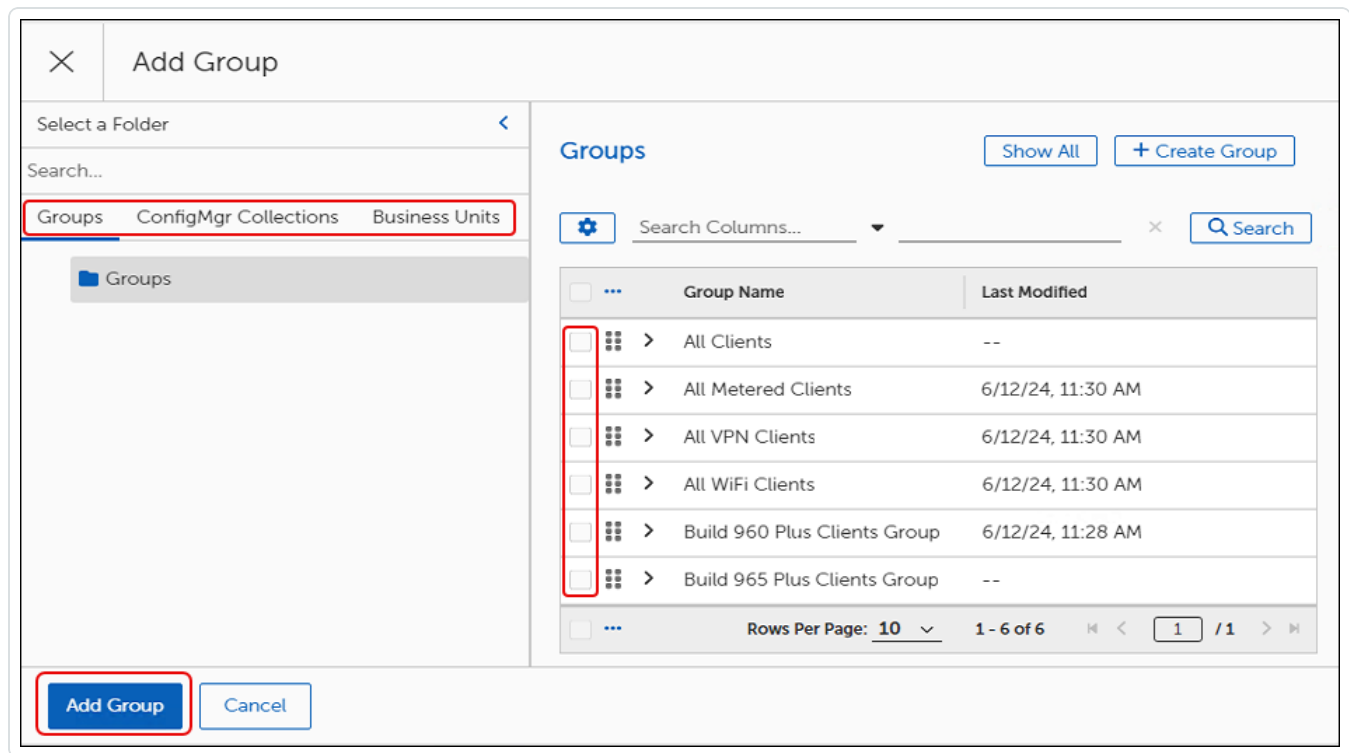
1. In the Business Unit Scopes section of an object template, click **Base Scope**.



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



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



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

Remove Groups or Operators

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

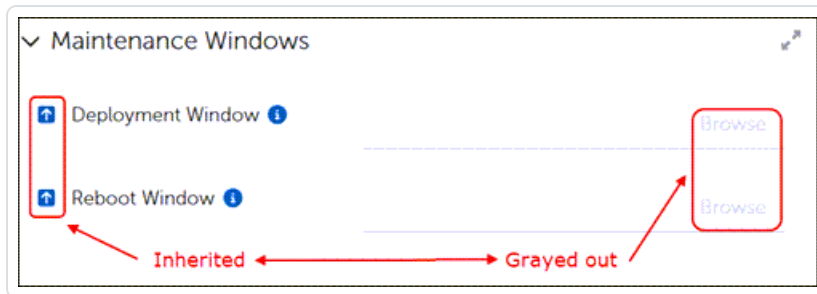
- Removing the top-level Operator removes everything beneath it.
- Removing a nested Operator also removes the associated Group or Business Unit.
- Removing a Group or Business Unit removes only that Group or Business Unit.

Maintenance Windows in Business Units

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



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



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

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

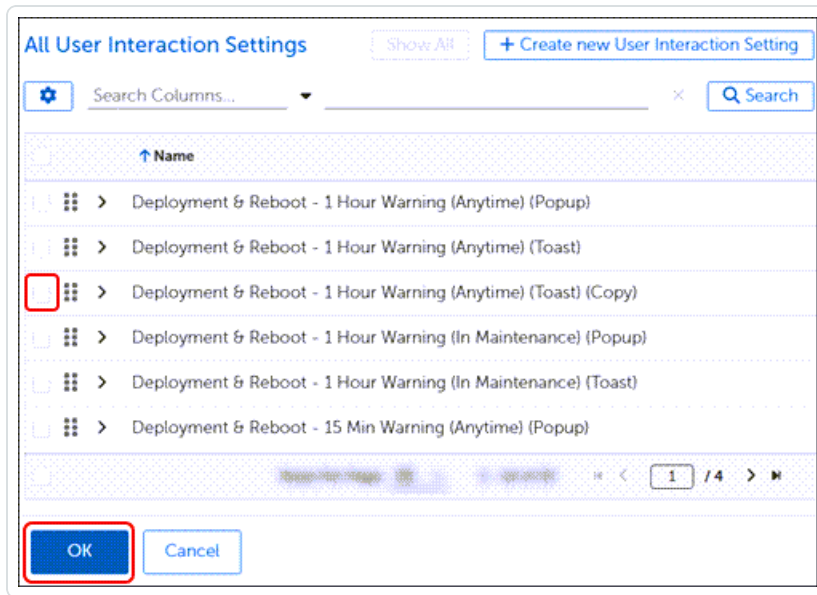
Add User Interaction Settings

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

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



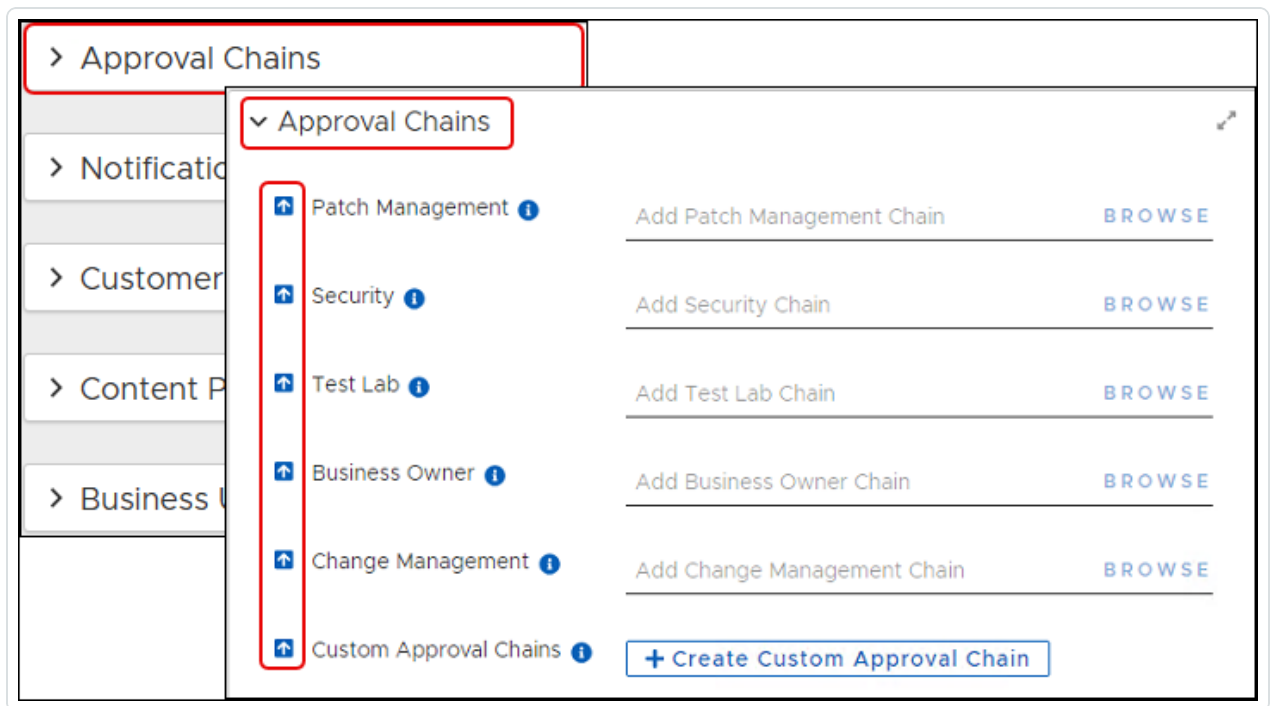
- If the Browse button is grayed out, the Business Unit template you are editing inherits these settings (if any) from a parent.
 - See [Managing Inheritance Settings](#) for additional details.
2. Select an **User Interaction Setting**, and then select **OK**.



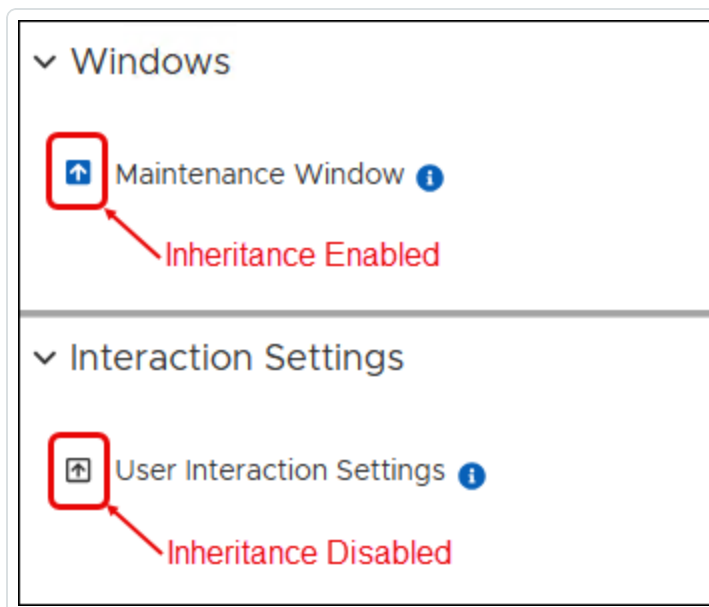
Add Approval Chains to a Business Unit

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

1. In an open Business Unit template, click **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 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.

The screenshot shows a window titled "All Approval Chains". At the top right, there are two buttons: "Show All" and "+ Create new Approval Chain". Below the title bar, there is a search section with a "Search Columns..." dropdown and a "Search" button. The main content area is a table with the following rows:

☐	↑ Name
☒	> All Admins Approval Chain
☐	> Super Admins Approval Chain

At the bottom of the table, there is a pagination bar showing "Rows Per Page: 10", "1 - 2 of 2", and a page indicator "1 / 1". At the bottom left of the dialog, there are two buttons: "OK" and "Cancel". The "OK" button is highlighted with a red box.

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



Customer Extension Data

Customer Extension Data

New Key

New Value

+ Add

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

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

Notification Chains

Show All

+ Create Notification Chain

Search Columns...

Search

☐	...	Name	Actions
☐	...	> All Admins Notification Chain	...
☒	...	> Super Admin Notification Chain	...

...

Rows Per Page: 10

1 - 2 of 2

1 / 1

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 .
5. Continue editing the **Notification** settings or click OK on the bottom 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, click **Show Members** to display the members of the Business Unit and verify that you have populated the Business Unit as you intend.

Note: 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 Tenable Patch Management installed and are associated with a Tenable Patch Management .
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 parent values when conflicting.



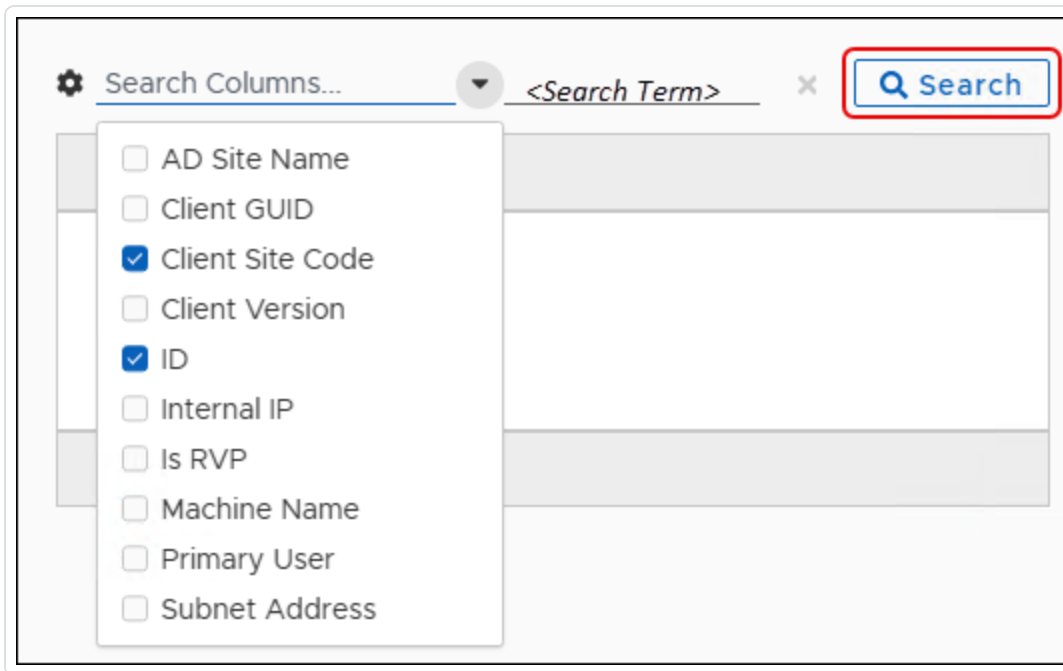
Patching Analytics Dashboards

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

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

Using Search in Tenable Patch Management

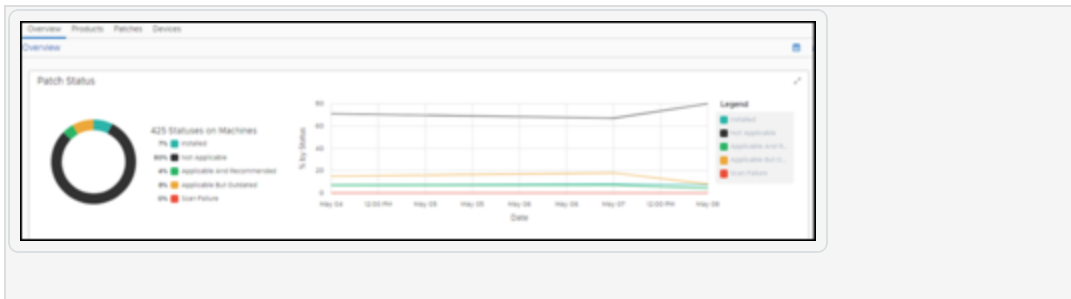
For tables in any dashboard view, the drop-down list next to **Search** allows you choose a column to search within. This provides several options for searching depending on the search term you have selected. Column choices change depending on the menu object.



Patching Analytics Overview

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

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



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

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

The screenshot shows the 'Product Status' table with columns: Product Name, Publisher, Patch..., Mach..., Devic..., Comp..., Risk..., and Actions. The 'IPassword x64' product is selected, and a dropdown menu is open showing details for 'IPassword ...' by Agilebits Inc.

Product Name	Publisher	Patch...	Mach...	Devic...	Comp...	Risk ...	Actions
IPassword x64	Agilebits Inc.	18	0	0	100%	0	...

IPassword ...	
ID	1000000270
Description	IPassword keeps track of password breaches and other security problems so you can keep your accounts safe. It checks for weak, compromised, or duplicated passwords and lets you know which sites are missing two-factor authentication or using unsecured HTTP.
Percentage Installed On	0%
Strategies Including this Product	0
Average Risk Score	0
Risk Contribution	0
Criticality	50

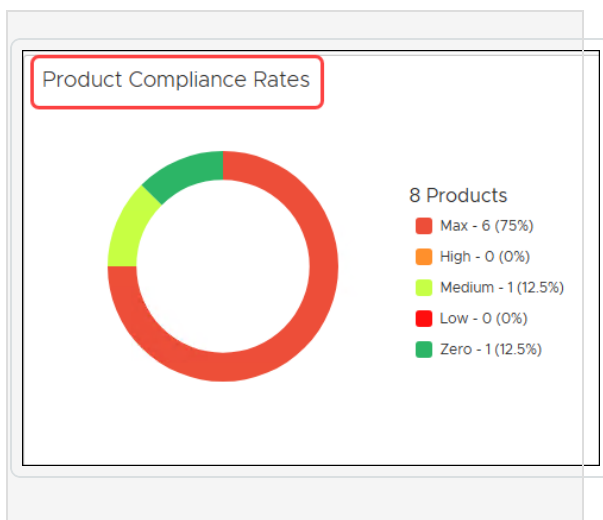
Products View

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

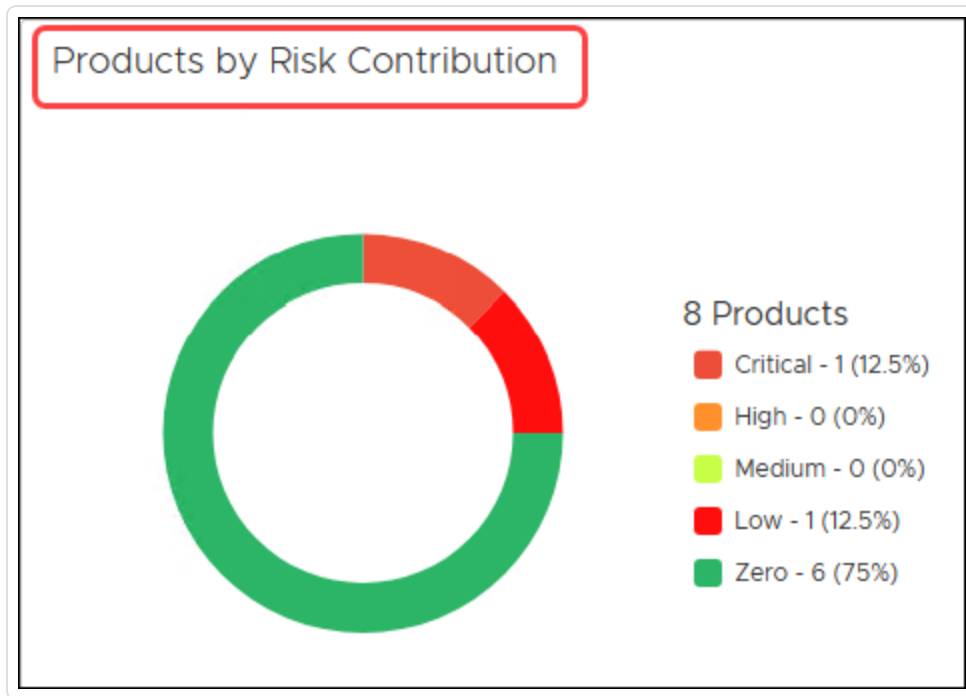
Product Metrics tracks supported products, detected products, and patching requirements, and provides a visual indication of product patching over time.



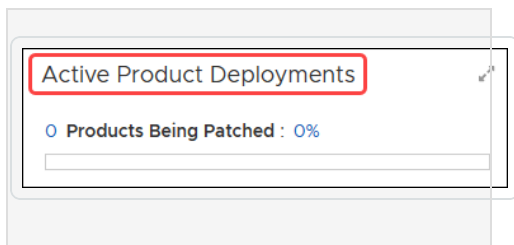
Product Compliance Rates show the number of products in the environment and the compliance rates by percentage. It also includes a chart that shows the level of compliance (Compliant, Compliant by Exclusions, and Non-Compliant) over time.



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



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



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

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



Product Status							
Search Columns...							
Product Name	Product Name	Publisher	Patc...	Mach...	Devic...	Comp...	Risk ...
IPassword x64	IPassword ...	Agilebits Inc.	18	0	0	100%	0
ID		1000000270					
Description		IPassword keeps track of password breaches and other security problems so you can keep your accounts safe. It checks for weak, compromised, or duplicated passwords and lets you know which sites are missing two-factor authentication or using unsecured HTTP.					
Percentage Installed On		0%					
Strategies Including this Product		0					
Average Risk Score		0					
Risk Contribution		0					
Criticality		50					

Patches View

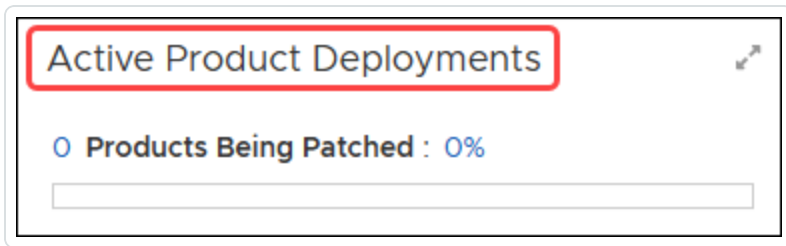
The **Patches** view summarizes information from the patch perspective.

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

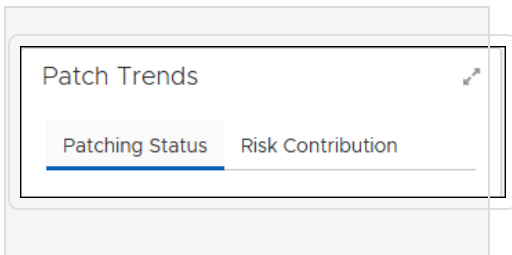
Patch Metrics	
19494	Total Patches
15134	Patches Consumed
17	Patches Installed
15128	Patches Not Required
0	Patches Installed (Last 7 days)
0	Patches Installed (Last 30 days)
0	Patches Installed (Last 60 days)
0	Patches Installed (Last 90 days)
0	Being Patched : 0%
6	Not Patched : 0%



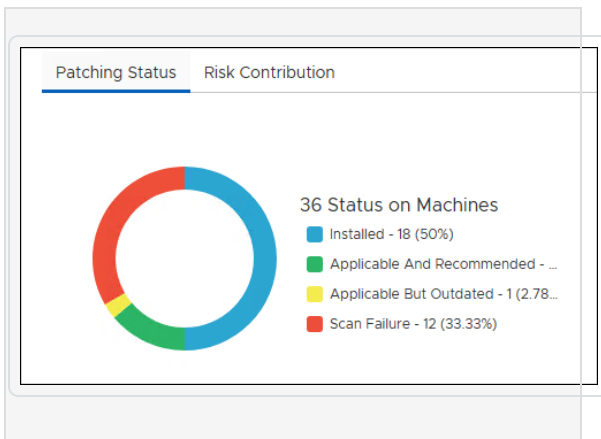
Active Product Deployments provides the number of patches undergoing installation and the percentage of completion.



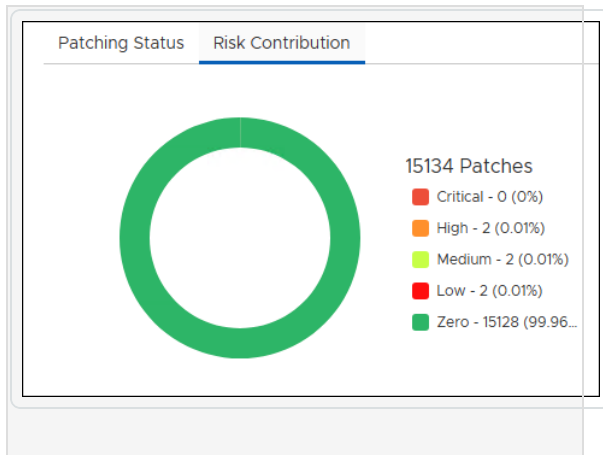
Patch Trends includes two tabs, one for Patching Status and one for Risk Contribution.



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



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



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

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

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

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



Patch Status

Search Columns...

...

Patch Name

...

.NET 3.5 Feature

...

.NET 3.5 Feature on Demand for X64

ID

1021000947

Description

--

Patch Notes

--

Reboot Type

N/A

Product ID

1000990001

Not Applicable

2

Applicable Outdated

0

Scan Failed

0

Average Risk Score

0

Risk Contribution

Standalone Risk Score

16

Devices View

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

Device Metrics

2 Total Devices

0 Patched Devices : 0%

2 Not Patched : 100%

0 Devices Patched (Last 7 days) : 0%

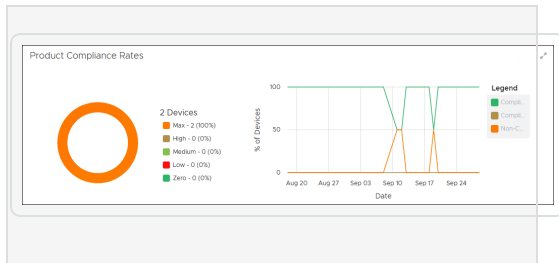
0 Devices Patched (Last 30 days) : 0%

0 Devices Patched (Last 60 days) : 0%

0 Devices Patched (Last 90 days) : 0%



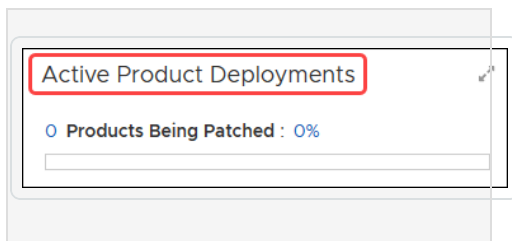
The **Product Compliance Rates** for Devices shows the rate of compliance for each device in the environment based on the latest device scan information. The graph displays the percentage of devices that fall into each category of compliance (max, high, medium, low, and zero), and the line graph shows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



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



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



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



Device Status					
⚙ Search Columns...					
☐ ... Device Name	☐ ... Device Name	Compliance	Risk Score	Risk Contribu...	Proc
☐ > adaptivaserver	☒ adaptivaserver	67%	153	60%	6
Device ID		2			
Primary User		ADAPTIVASERVER\Administrator			
IP Address					
Client Version		9.0.963.2			
Last Check In		11/29/23, 6:11 PM			
Operating System		Microsoft Windows Server 2022 Standard			
Location		No Office			
Compliant Products		4			
Non-Compliant Products		2			
Applicable Patches / Releases		4			

Flex Controls

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

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

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

When a vendor releases products and patches, the Tenable Patch Management 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](#).



▼ Blocklist Settings

Adaptiva Curated Chain

Add Notification Chain

BROWSE

Customer Chain

Add Notification Chain

BROWSE

Adaptiva Curated Communication Providers

+ Add Communication Providers

Customer Communication Providers

+ Add Communication Providers

Managing Blocklist Notification Settings

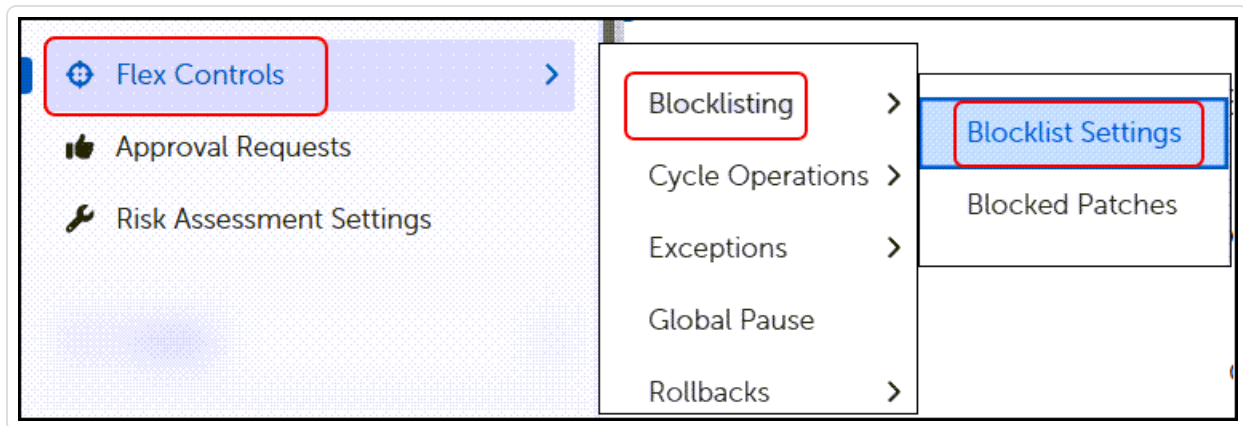
Set categories of notification by selecting a Notification Chain to use when Tenable Patch Management blocklists a patch/release. Select the same or different Notification Chain to notify administrators when you blocklist a patch or a release. You can also select specific communication providers for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

View Blocklist Settings

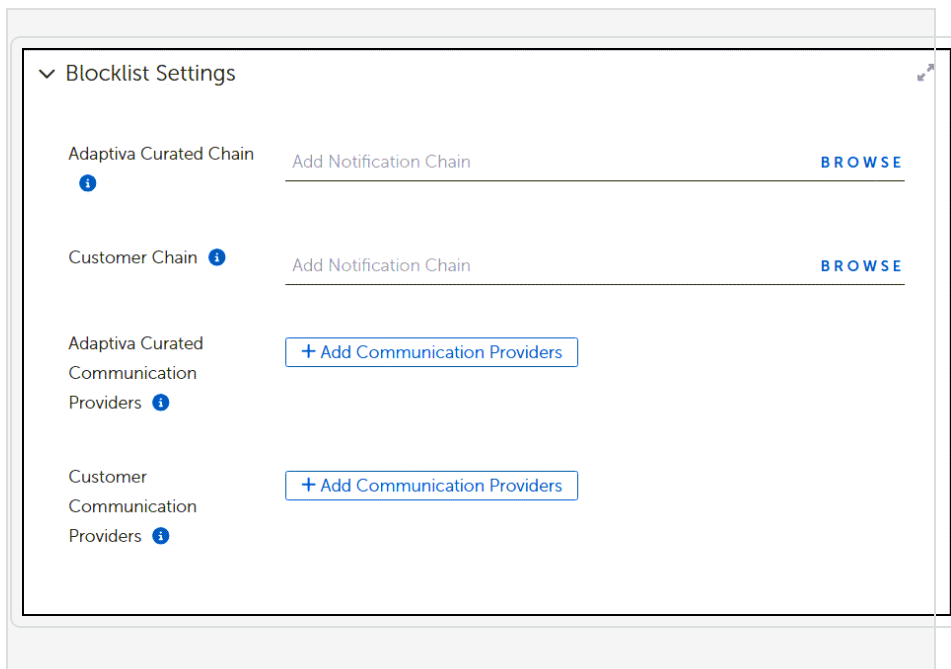
Blocklist Settings include notification details for blocklisted patches including Notification Chains and Communication Providers. You can use the Tenable Patch Management provided details (Tenable Patch Management Curated) or create your own (Customer). Update these settings as needed for your notification 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 **Tenable Patch Management Curated Chain** or the **Customer Chain** to list the available Notification Chains.If you need to create a new Notification Chain for these purposes, see [Create a Notification Chain](#) .



3. Select the **Name** of the Notification Chain you want to use for whichever field you are editing - the **Tenable Patch Management Curated Chain** or the **Customer Chain**.
4. Select **Add Notification Chain** on the bottom left of the dialog.

Choose Communication Providers for Notification Chains

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

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

Cycle Operations

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

Details available for each cycle type include the following:

- **Cycle Information:** Provides general information about the Patch Process such as the Current State, the creation date and time, and the Patch Process schedule. This section also contains controls to manually start, stop, or delay a Patch Process.
- **Overall Metrics:** This section contains information about the scope of the running process. This screen shows the number of business units and devices affected by this Patch Process, along with Urgency information.
- **Cycle History:** This section gives a historical perspective of the results of past runs. This view will show the number of devices that previously were successful, failed, aborted, timed out, or errored.



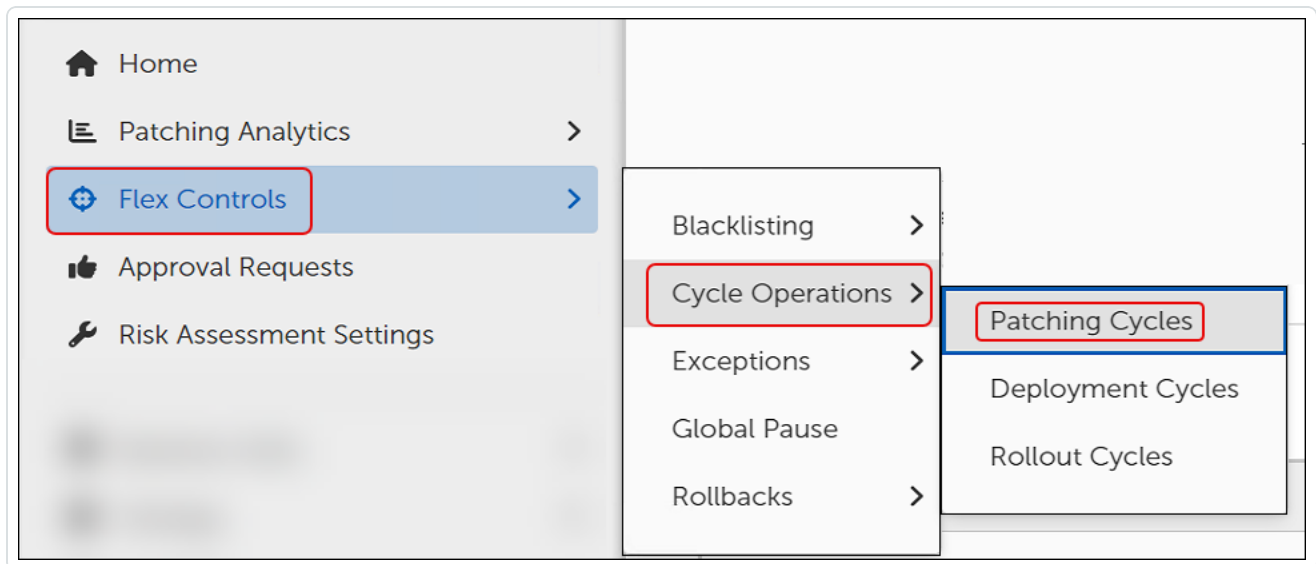
- **Patch Approvals:** One of the key functions of a Patch Process is to execute Approval Chains as defined in the Patching Strategy or Business Unit. This section displays pending Approvals. You cannot grant approvals from this view.
- **Cycle Logs:** Display events relating to the Patch Process. For instance, the Cycle Operation Logs can show the administrator who manually started a Patch Cycle and at what time.

Patching Cycles

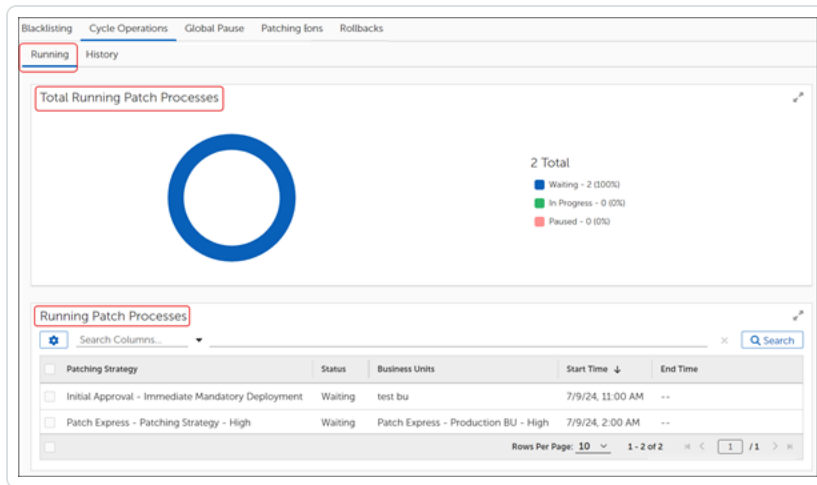
This dashboard shows information about the active Patch Processes in the environment. Patch Processes represent the workflow that models and performs the defined patching routine. As part of the overall Patching Strategy, Patch Deployment Bots use configured criteria to identify patches that apply to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

View the Running Patch Cycles

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



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



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

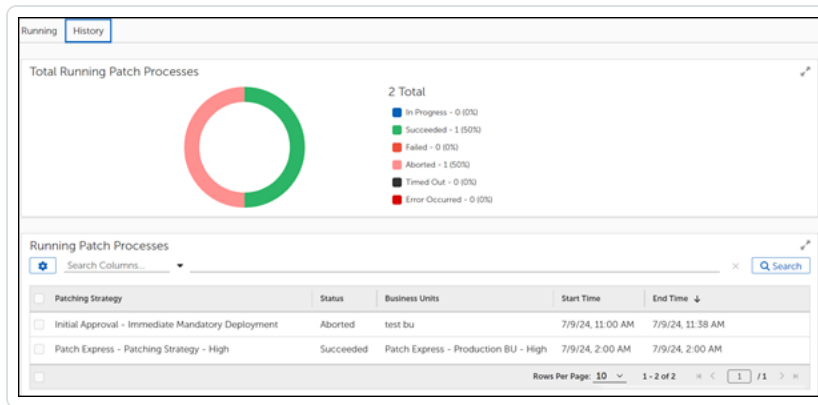
2. Enter a **Patching Strategy** name on the search bar above the Running Patch Processes table, and then click **Search**.



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

View Patching Cycle History

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



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

- The **Total Finished Patch Processes** widget on top shows an aggregate summary of all completed patch processes and their corresponding states (In Progress, Succeeded, Failed, Aborted, Timed Out, Error Occurred).
- The Running Patch Processes table lists the completed patch processes by Patching Strategy name.

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

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

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

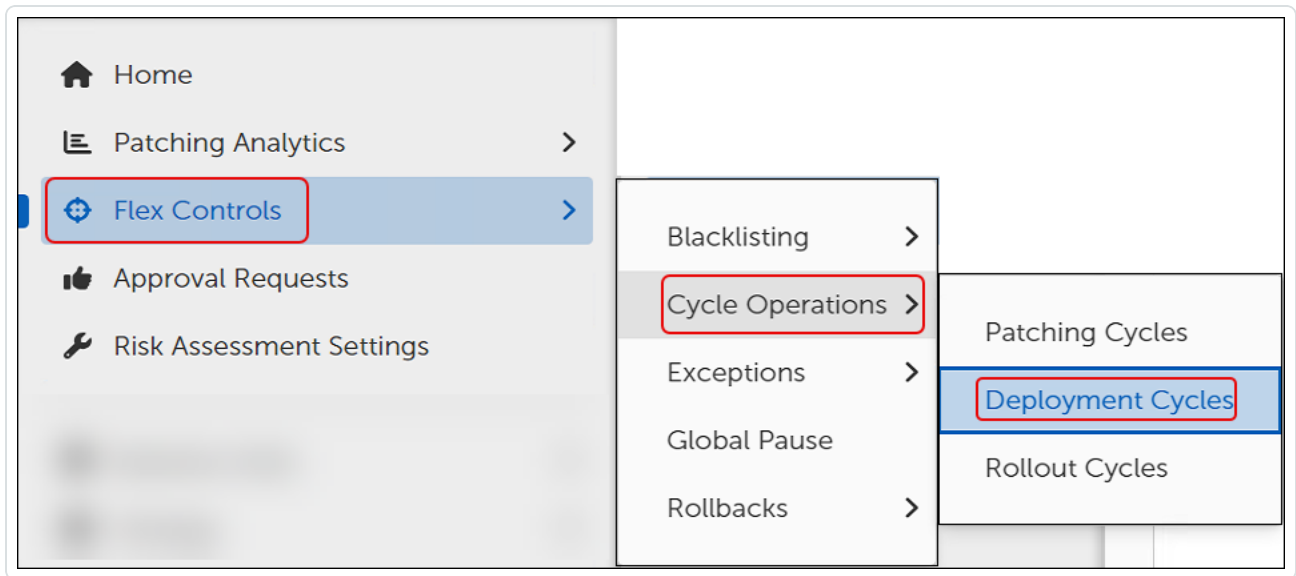
Deployment Cycles

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

View the Running Deployment Cycles

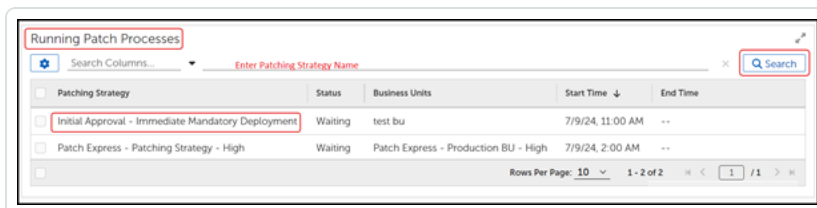


1. Mouse over or click **Flex Controls** in the **Home** menu, and then select **Cycle Operations > Deployment Cycles**.



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

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

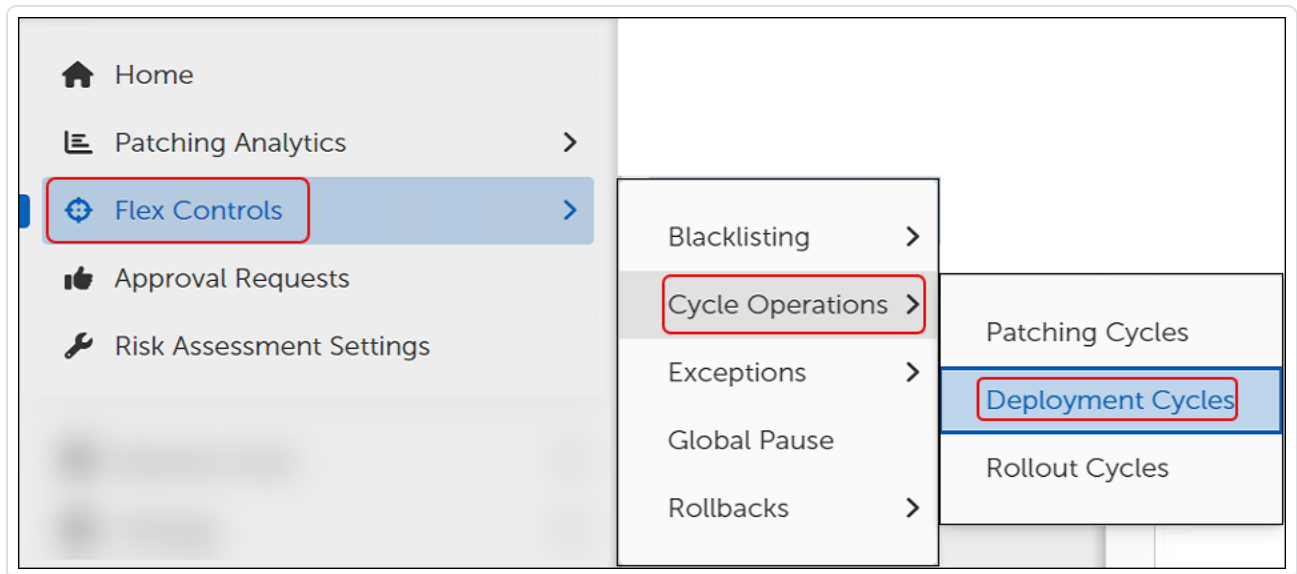


3. Select the **Deployment Strategy** name in the **Running Patch Processes** table to see specific details about that process.

View Deployment Cycle History



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



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

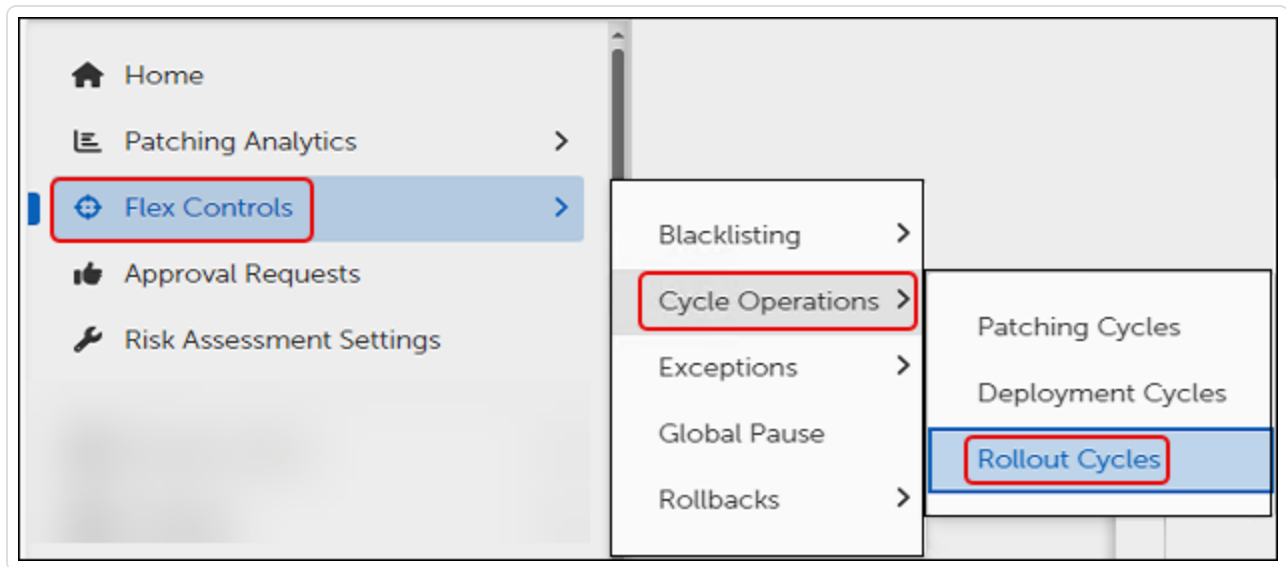
Rollout Cycles

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

View the Running Rollout Cycles



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



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

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

View Rollout Cycle History

1. Mouse over or click **Flex Controls** on the Home menu, and then select **Cycle Operations > Rollout Cycles**.
2. Select **History** on the upper left to change to the History tab:



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

Patching Exceptions

When Business Units require exemption from specific updates on certain products, or the entire enterprise must remain at a specific version of a product, Patching Exceptions provide a mechanism for creating and implementing the rules. Patching Exceptions provide version level patch support to give administrators 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

Tenable Patch Management 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 installation of a particular product.
- **Rollback:** Forces a rollback to a specific product version on a client device, when Tenable Patch Management 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 corner to open a Patching Exception template.
3. Name and describe the exception:
 - a. Enter a descriptive Name for this exception in the Name field.
 - b. Enter a detailed **Description** of the purpose for this exception.
4. Select **Save** on the upper left to save your new template:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.
5. Choose an Override Strategy:
 - If you choose **Override Desired States**, see [Set Override Details for Patch Exception](#).
 - If you choose **Select Last Allowed Versions**, see [Set Last Allowed Patch Versions](#).

Set Override Details for Patch Exceptions

Note: 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:
 - a. Enter a product name on the search line, and then click **Search**. This example uses Google Chrome.
 - b. Select the product from the list, and then click **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

4. Select **Save** on the upper-left corner of the dialog to save your changes:



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

5. Continue to 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 ⓘ

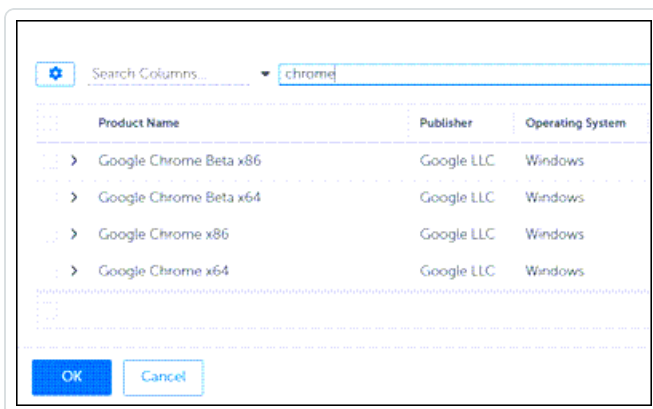
+ Browse

Target Business Units ⓘ *

+ Browse

2. Select **+Browse** to select the Last Allowed Version Patches.

- a. Enter a product name on the search line, and then click **Search**. This example uses Google Chrome.
- b. Select the product from the list, and then click **OK**.



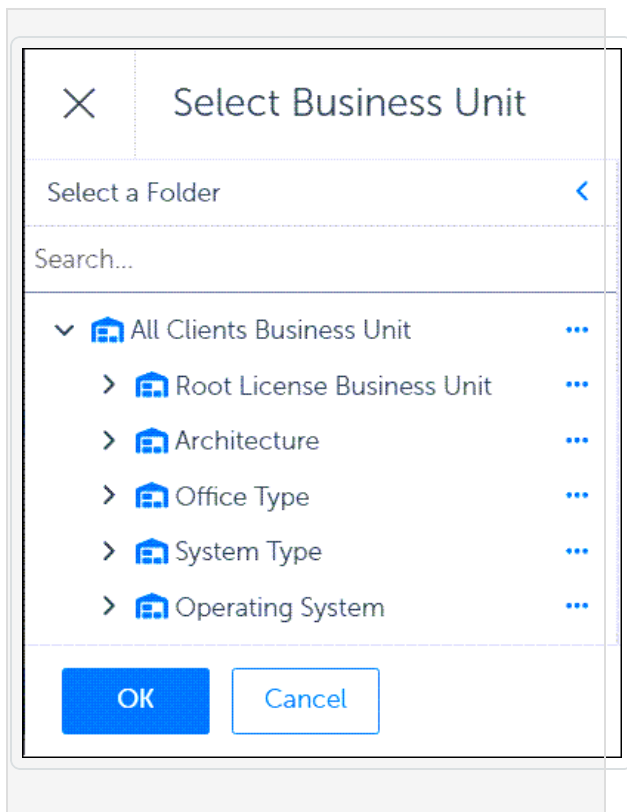


3. Select **Save** on the upper-left corner of the dialog to save your changes:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.
4. Continue to Target Business Units.

Add Target Business Units for Patch Exceptions

With **Select Last Allowed Versions** as your Override Strategy in 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 corner of the dialog.
4. Select **Save** on the upper left corner 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 Tenable Patch Management side, and the Tenable Patch Management pauses the deployment of patches identified in the pause settings.

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

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

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

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

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

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

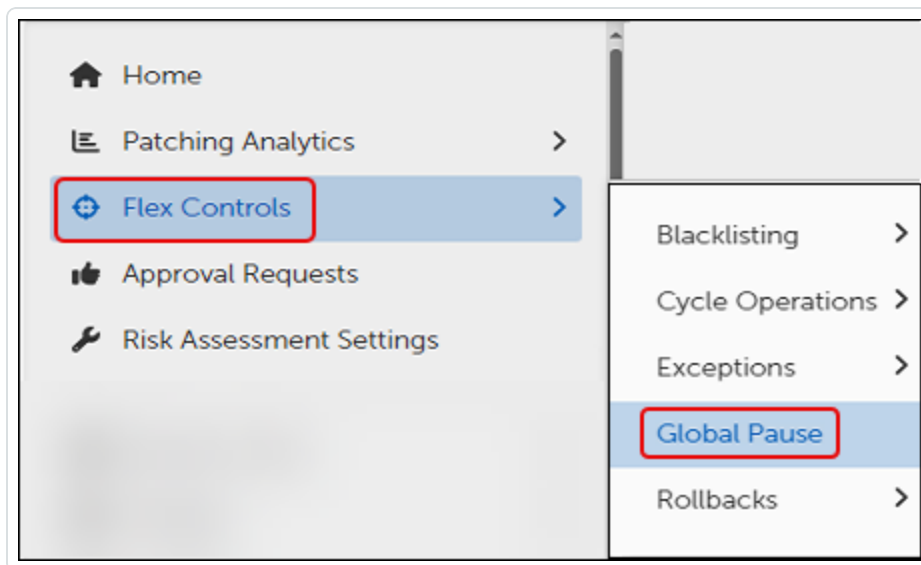
Paused Business Units : Pause all patches for specified Business Units.

Stop All Patching Activity Immediately

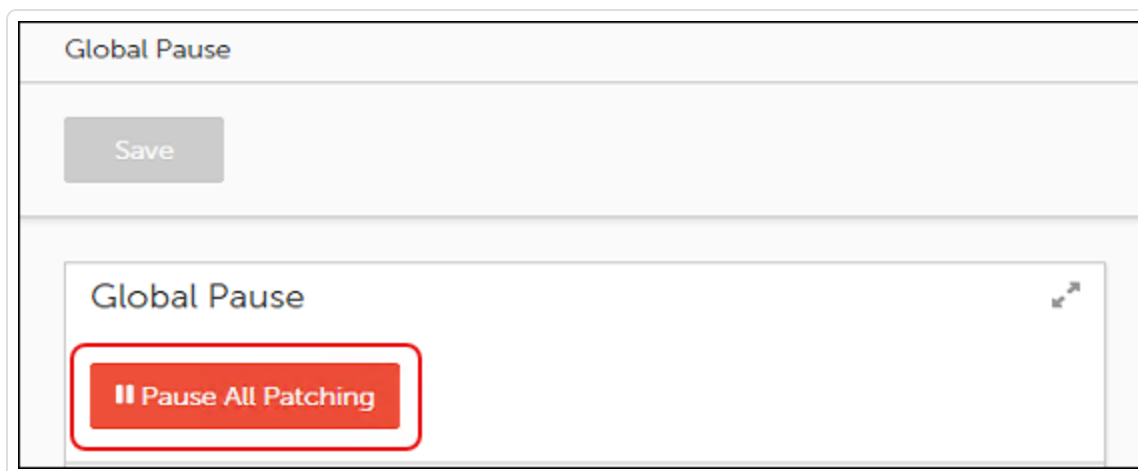
To stop all patching activity on all licensed clients in the estate, use the following steps to activate Global Pause.



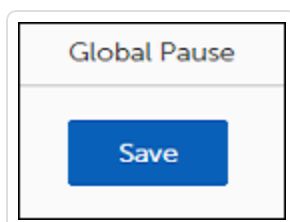
1. Select **Flex Controls** on the Home menu, and then select **Global Pause**.



This opens the Global Pause dialog:



2. Select **Pause All Patching**.



3. Select **Save** to activate Global Pause. This immediately stops all patch deployments across all licensed clients:

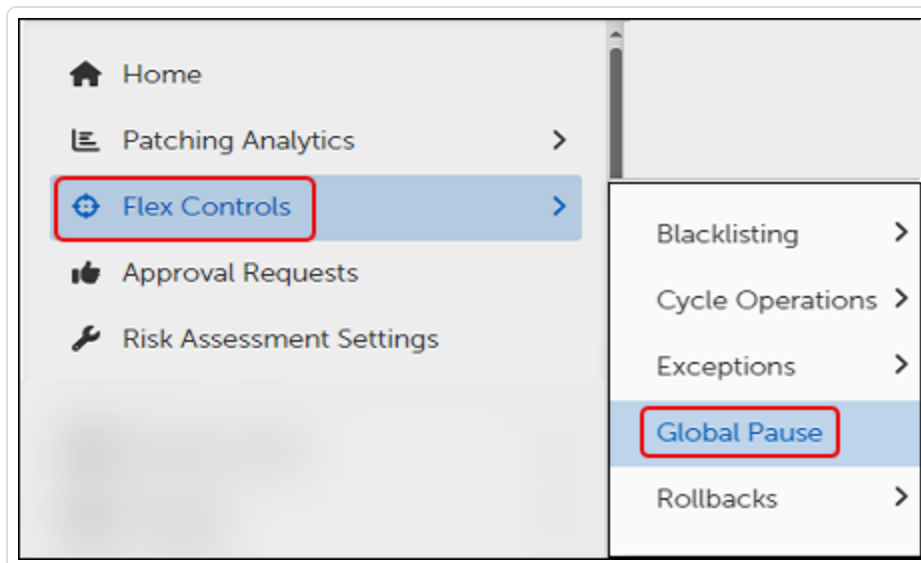


- All patch deployments in progress that have not reached an irreversible state are paused immediately.
- All newly initiated patch deployments are paused automatically.

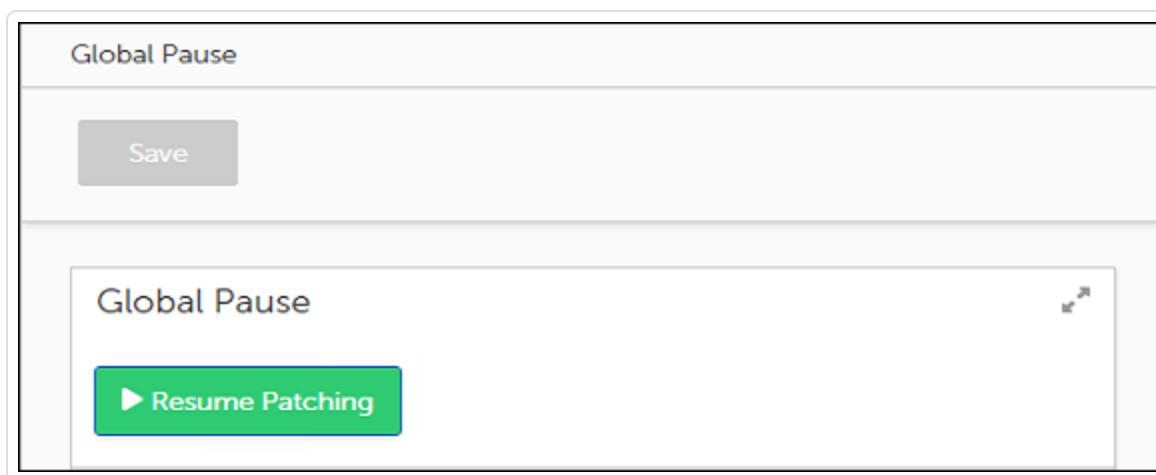
Resume All Paused Patching Activity Immediately

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**.

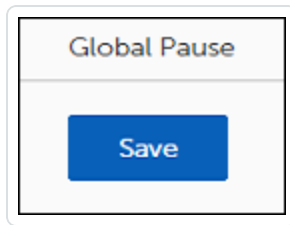


This opens the Global Pause dialog:





2. Select **Resume Patching**.

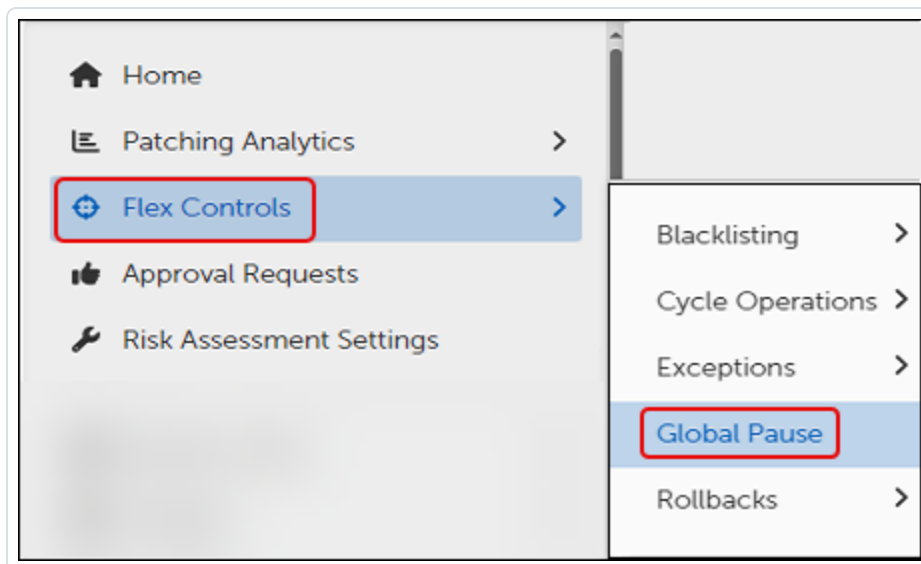


3. Select **Save** to revoke the Global Pause. This immediately revokes the Global Pause and allows patching activity to occur as configured.

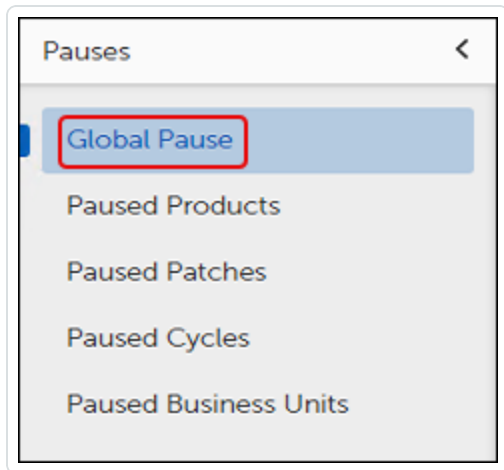
Pause Patching for Specific Objects

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.

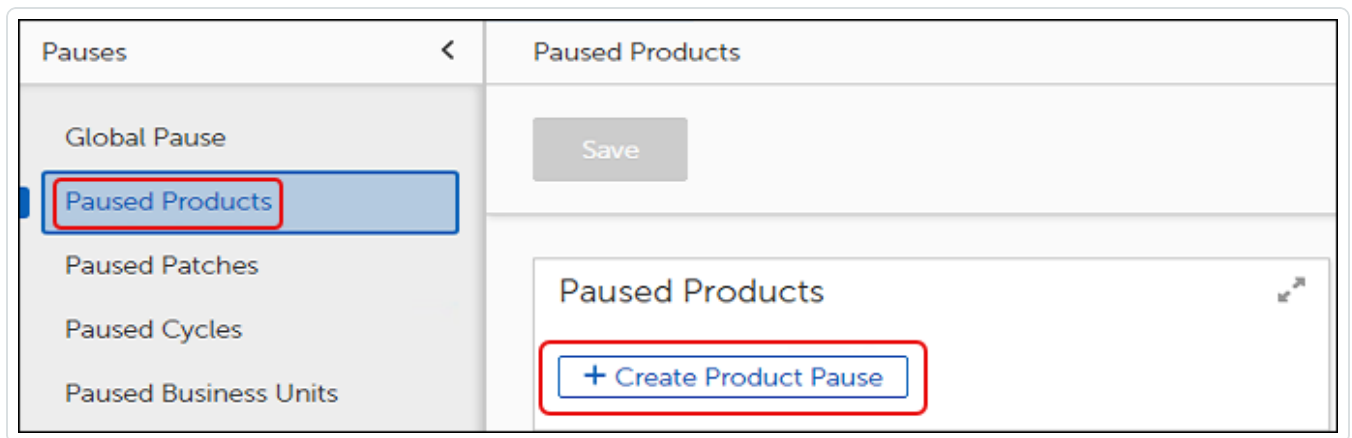
- **Global Pause:** Pause all patching activity immediately ([Stop All Patching Activity Immediately](#)).
- **Paused Products:** Pause patch deployments for one or more products ([Pause Deployment of a Specific Software Product](#)).
- **Pause Patches:** Pause deployment of a software patch or release 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

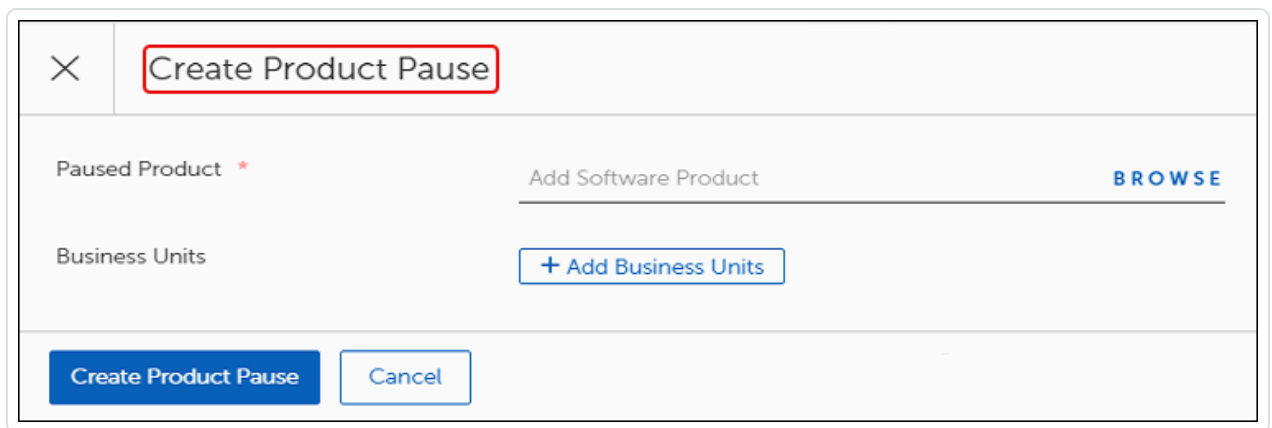
To stop patching activity for specific software products or patches, complete the following steps:

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

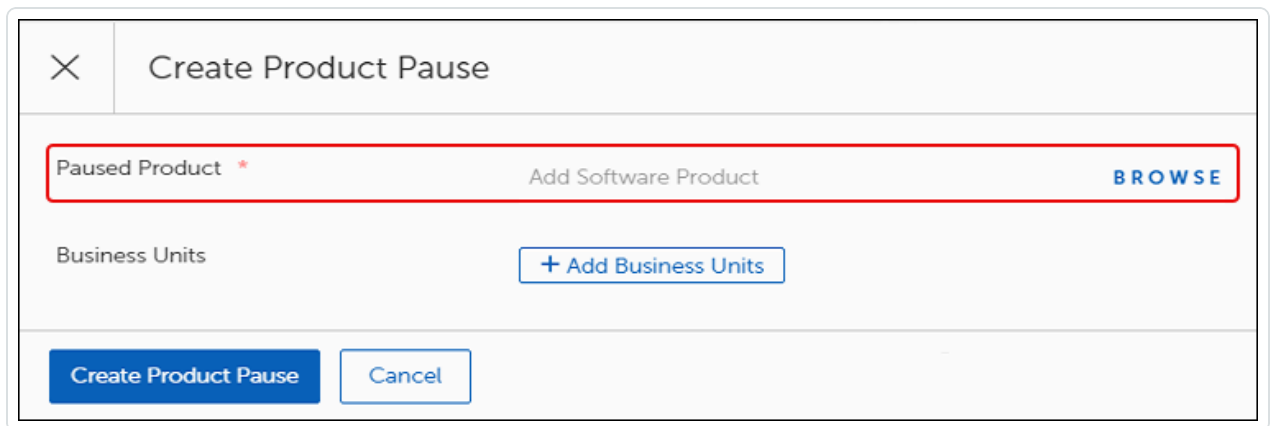
This opens the Paused Products dialog:



- 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:

Add Software Product

Software Products Show All

Search Columns... Search

☐	Name
☐	1Password x64
☐	3CX Call Flow Designer x64
☐	3Dconnexion 3DxWare 10 x64
☒	3Dconnexion 3DxWare 10 x86
☐	4K Video Downloader x64

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

Add Software Product Cancel

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

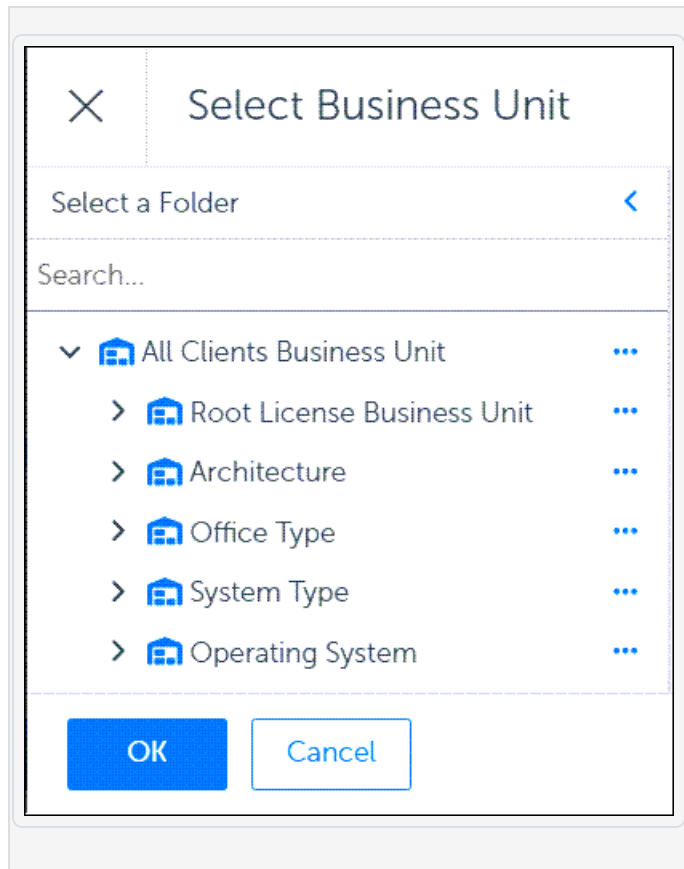
2. Select **Add Software Product** to return to the Create Product Pause dialog, and then choose one of the following methods to proceed:

- To create a Global Pause for the selected products, click **Create Product Pause**. This pauses the deployment of the selected software product on all devices in the estate.
- To specify a pause for specific devices, continue with the next step to **Add Business Units**.

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



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



- b. Select **OK**.

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

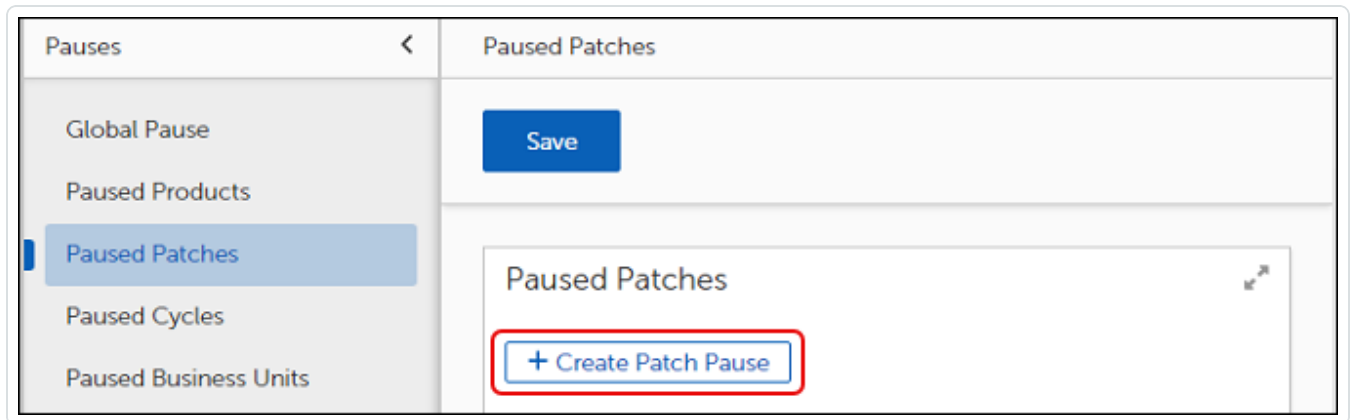
Pause Deployment of a Specific Patch

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

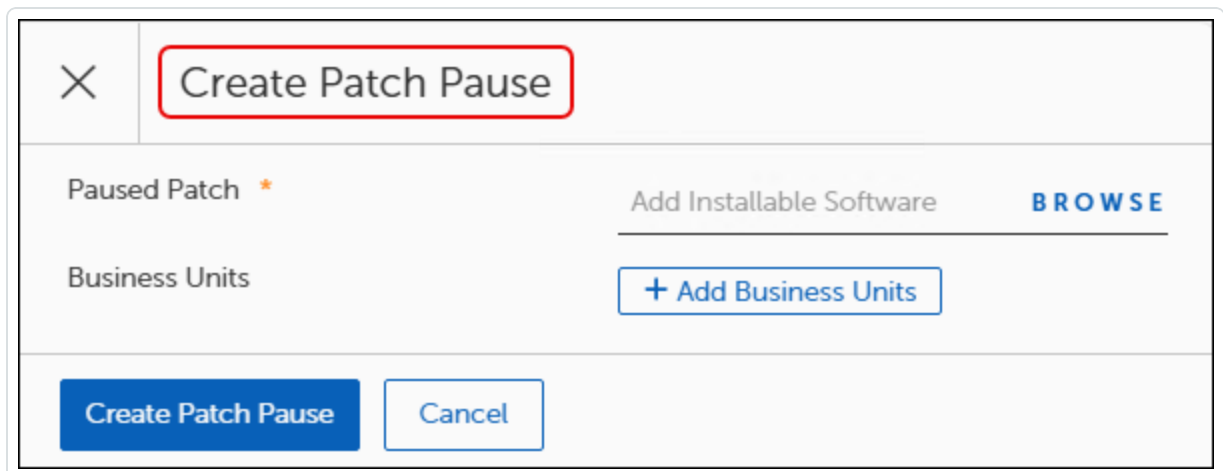


1. Navigate to the Pause menu (see [Pause Patching for Specific Objects](#)), and then select **Paused Patches**.

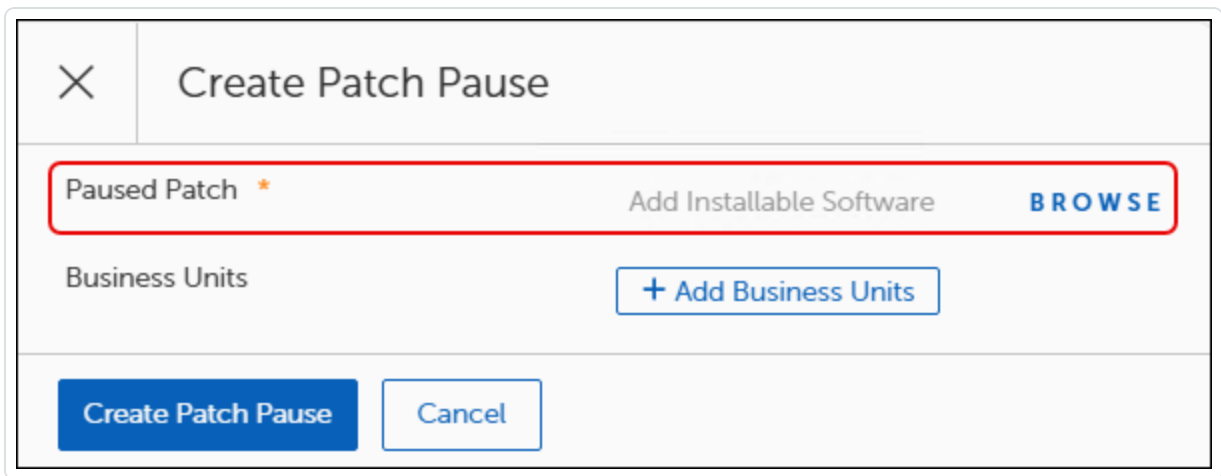
This opens the Paused Patches dialog:



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

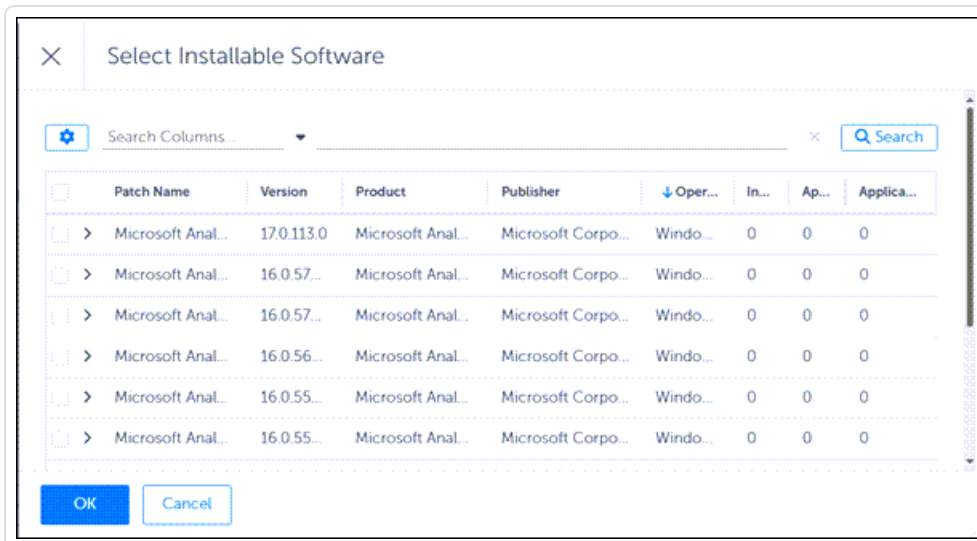


- b. Select **Browse** to find the Software Patch to pause:



The 'Create Patch Pause' dialog box features a close button (X) in the top left. The main title is 'Create Patch Pause'. Below the title bar, there is a section with a red border containing the text 'Paused Patch' followed by a star icon, the text 'Add Installable Software', and a blue 'BROWSE' button. Below this section is the label 'Business Units' and a blue button with a plus icon and the text '+ Add Business Units'. At the bottom of the dialog are two buttons: 'Create Patch Pause' (blue) and 'Cancel' (white with blue border).

c. Select the patch you want to pause:



The 'Select Installable Software' dialog box has a close button (X) and a title bar. Below the title bar is a search bar with a gear icon, the text 'Search Columns...', a dropdown arrow, a search icon, and the text 'Search'. Below the search bar is a table with the following columns: Patch Name, Version, Product, Publisher, Oper..., In..., Ap..., and Applica... (truncated). The table contains six rows of data, all from Microsoft Corporation. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Patch Name	Version	Product	Publisher	Oper...	In...	Ap...	Applica...
> Microsoft Anal...	17.0.113.0	Microsoft Anal...	Microsoft Corpo...	Windo...	0	0	0
> Microsoft Anal...	16.0.57...	Microsoft Anal...	Microsoft Corpo...	Windo...	0	0	0
> Microsoft Anal...	16.0.57...	Microsoft Anal...	Microsoft Corpo...	Windo...	0	0	0
> Microsoft Anal...	16.0.56...	Microsoft Anal...	Microsoft Corpo...	Windo...	0	0	0
> Microsoft Anal...	16.0.55...	Microsoft Anal...	Microsoft Corpo...	Windo...	0	0	0
> Microsoft Anal...	16.0.55...	Microsoft Anal...	Microsoft Corpo...	Windo...	0	0	0

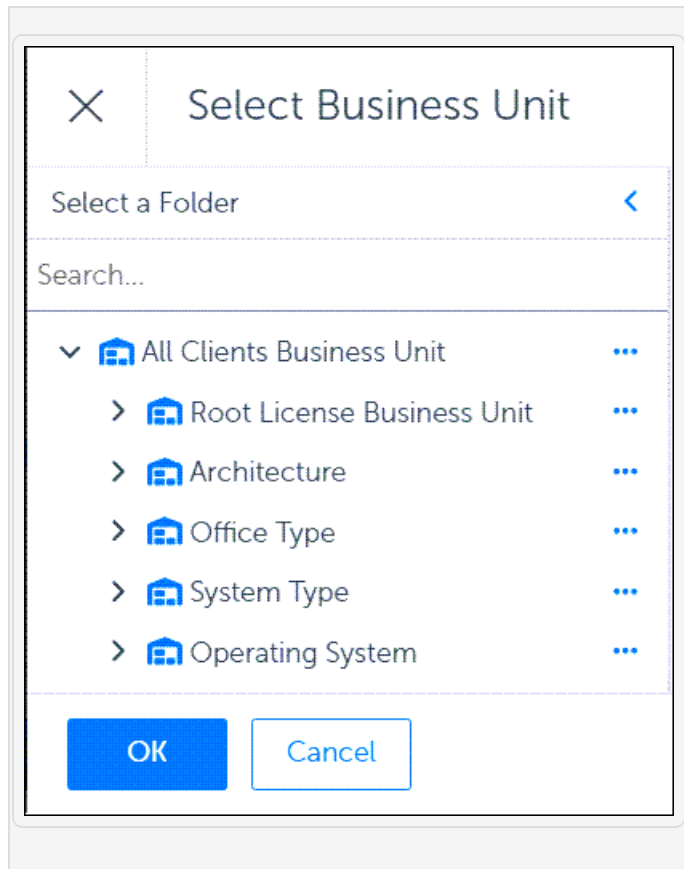
2. Select **Add Installable Software Product** to return to the Create Patch Pause dialog, and then choose one of the following methods to proceed:

- To create a Global Pause for the selected products, click **Create Patch Pause**. This pauses the deployment of the selected software patch on all devices in the estate.
- To specify a pause for specific devices, continue with the next step to **Add Business Units**.

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



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



- b. Select **OK**.

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

Pause Specific Cycles

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

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

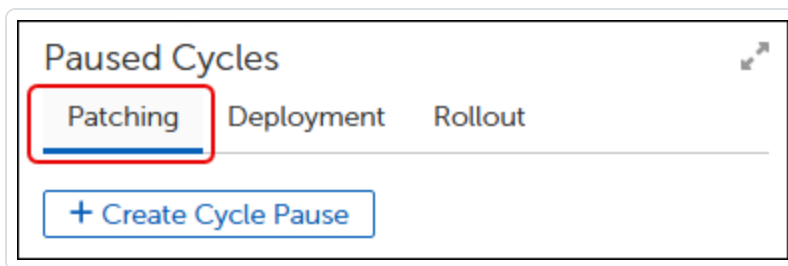
Note: Pausing a cycle that is currently in a WAITING state (has not run yet), prevents that cycle from running until you remove the pause. This is the only server-side behavior related to pausing.

Pause a Patching Cycle

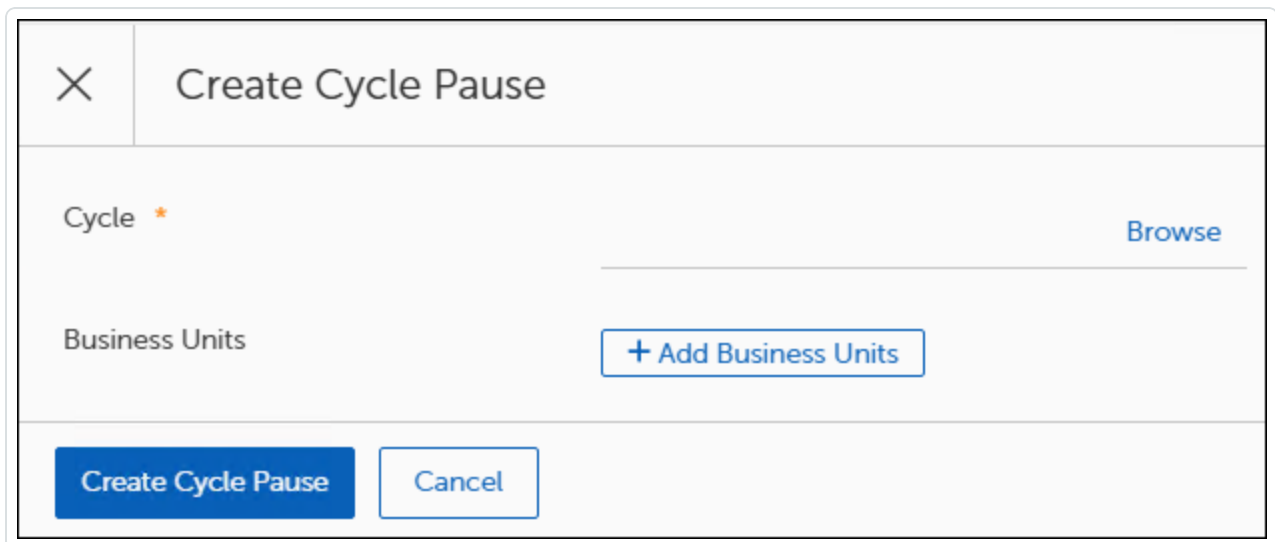
To stop patching activity for a specific patching cycle, complete the following steps:

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

This opens the Paused Cycles dialog to the Patching tab:



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





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

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

×

Select a Patching Cycle

⚙ Search Columns... × 🔍 Search

No data provided

OK Cancel

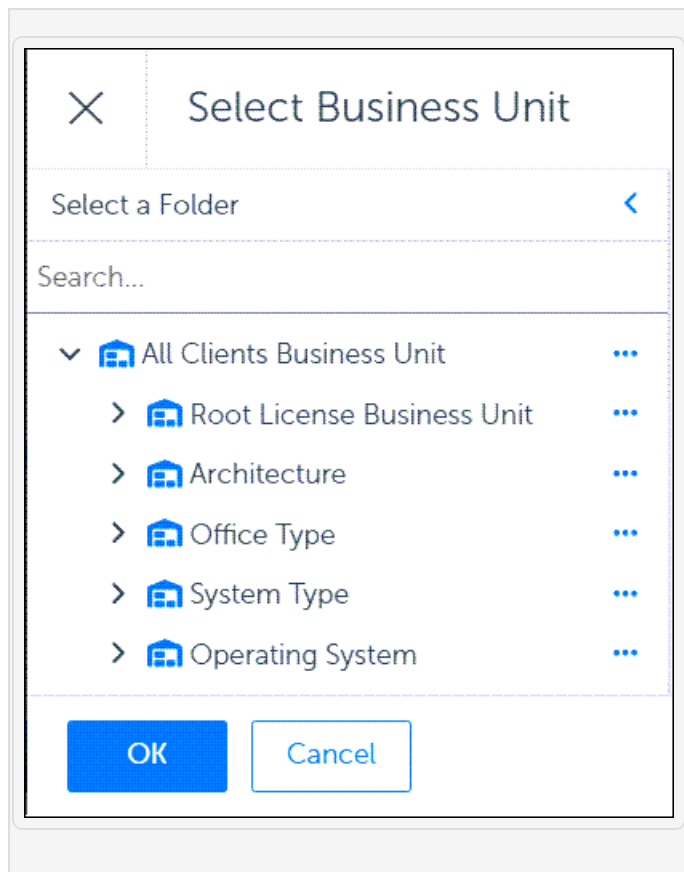
- Use the navigation tools on the bottom right to scroll through the pages to find and select a Patching Cycle from the table.
 - Enter a cycle name on the search line, and then click **Search** to find and select a specific cycle.
4. Select **OK**, and then choose one of the following options to proceed: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



- To specify a pause for specific devices, continue with the next step to **Add Business Units**.

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

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



- b. Select **OK**.

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

Pause a Deployment Cycle

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

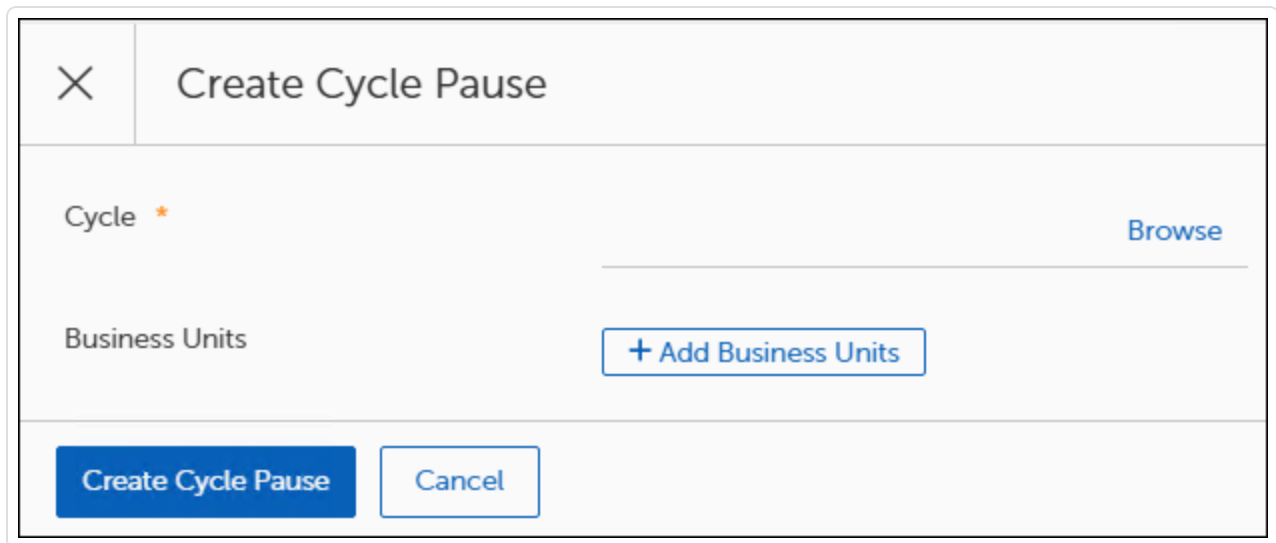


1. Navigate to the Pauses menu (see [Pause Patching for Specific Objects](#)), and then select **Paused Cycles**.

This opens the Paused Cycles dialog to the Deployment tab:



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



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

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



×

Select a Deployment Cycle

⚙

Search Columns...

▼

×

🔍

Search

No data provided

OK

Cancel

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

4. Select **OK** to save your entry, and then choose one of the following options to proceed:

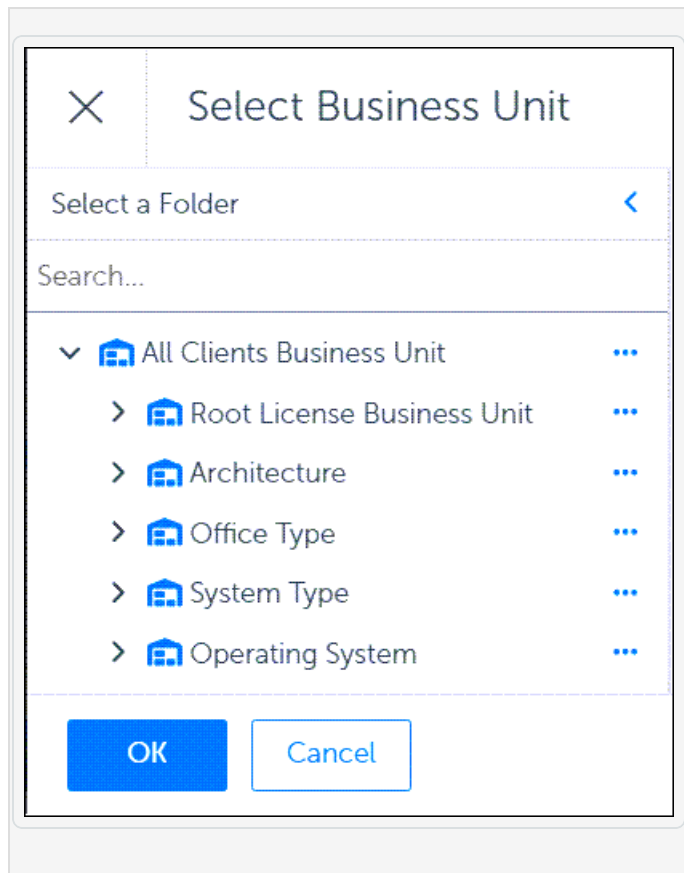
- To create a Global Pause for the selected cycle, skip to **Step 6**. This pauses the deployment of the selected software product on all devices in the estate.
- To specify a pause for specific devices, continue with the next step to **Add Business Units**.

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

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



1. Select the Business Units.



2. Select **OK**.

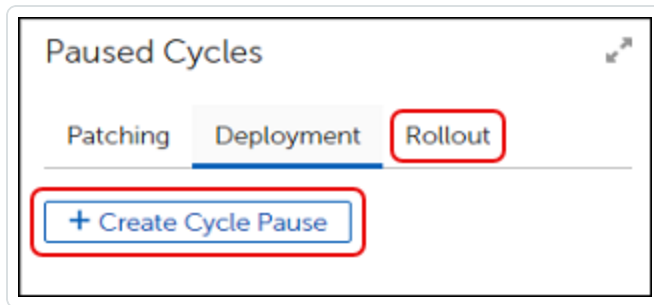
6. Select **Create Cycle Pause** and then click **Save** to create a pause for the selected cycle.

Pause a Rollout Cycle

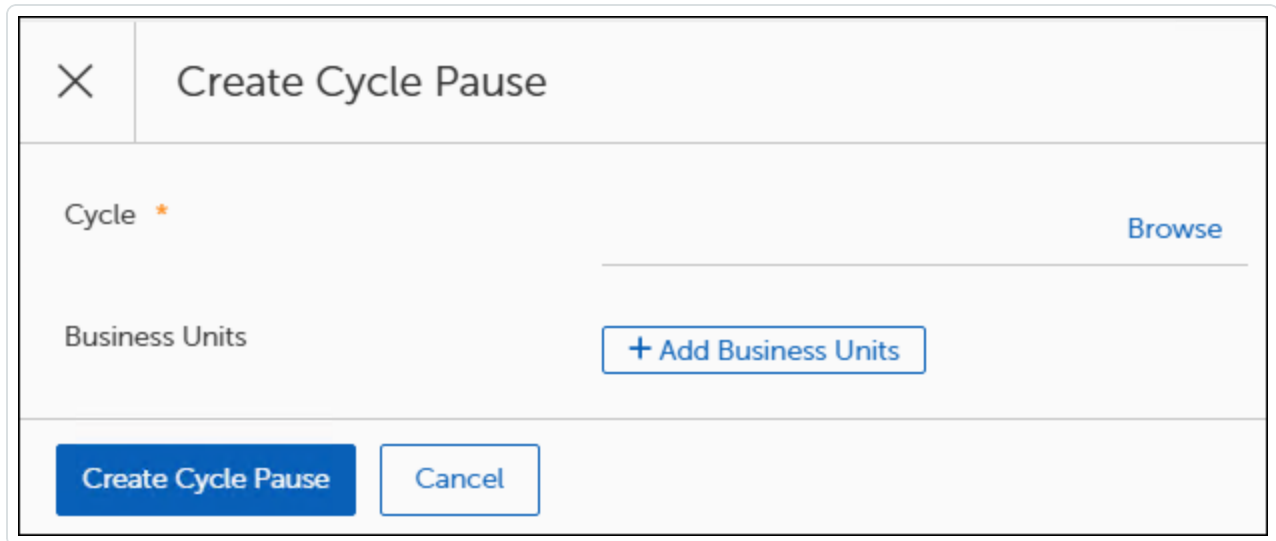
To stop all patching activity for a specific rollout cycle, complete the following steps:

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

This opens the Paused Cycles dialog to the Rollout tab:

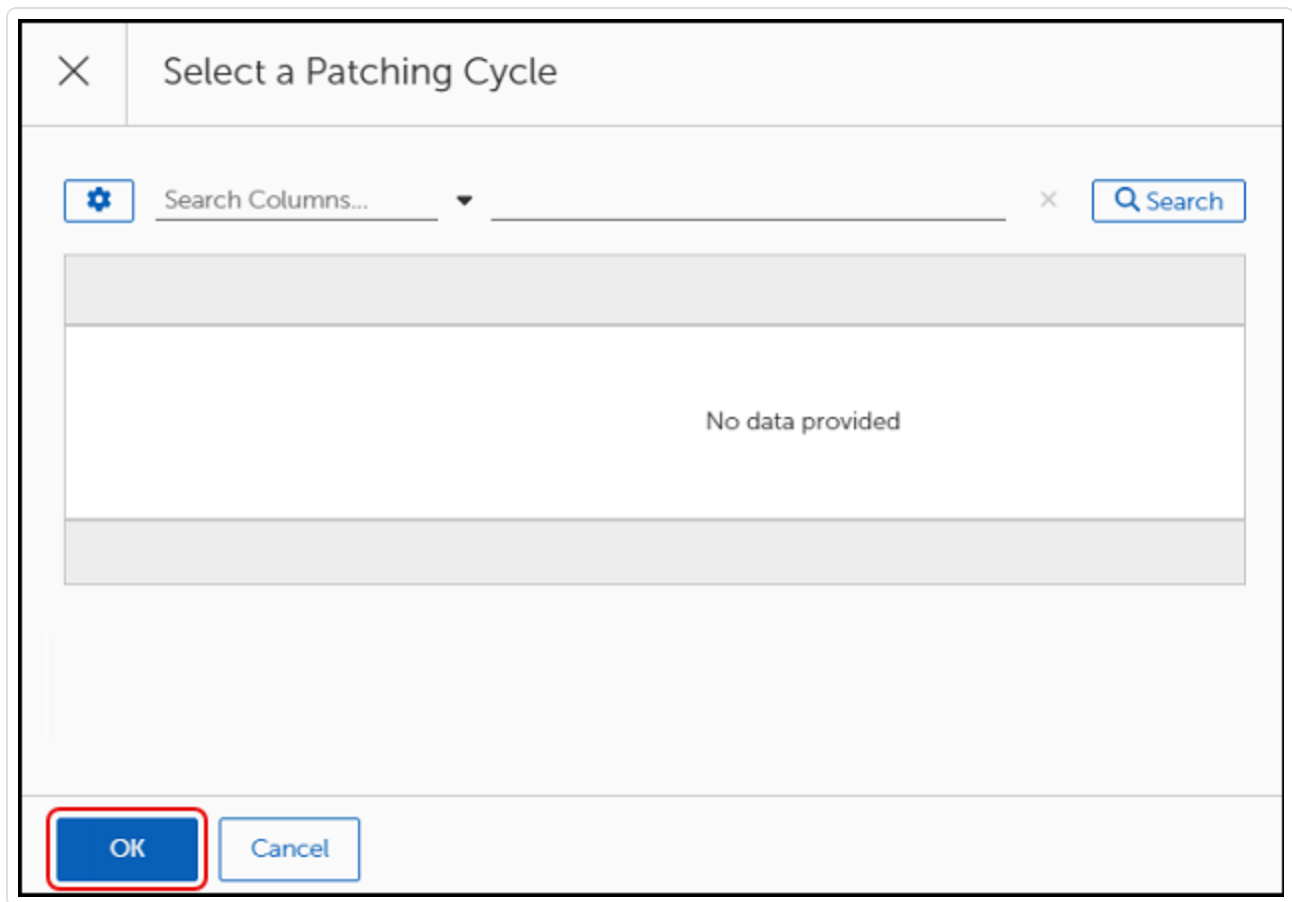


2. Select **+Create Cycle Pause**. This opens the Create Cycle Pause dialog:



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

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



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

4. Select **OK** , and then choose one of the following options to proceed:

- To create a Global Pause for the selected cycle, skip to **Step 6**. This pauses the deployment of the selected software product on all devices in the estate.
- To specify a pause for specific devices, continue with the next step to **Add Business Units**.

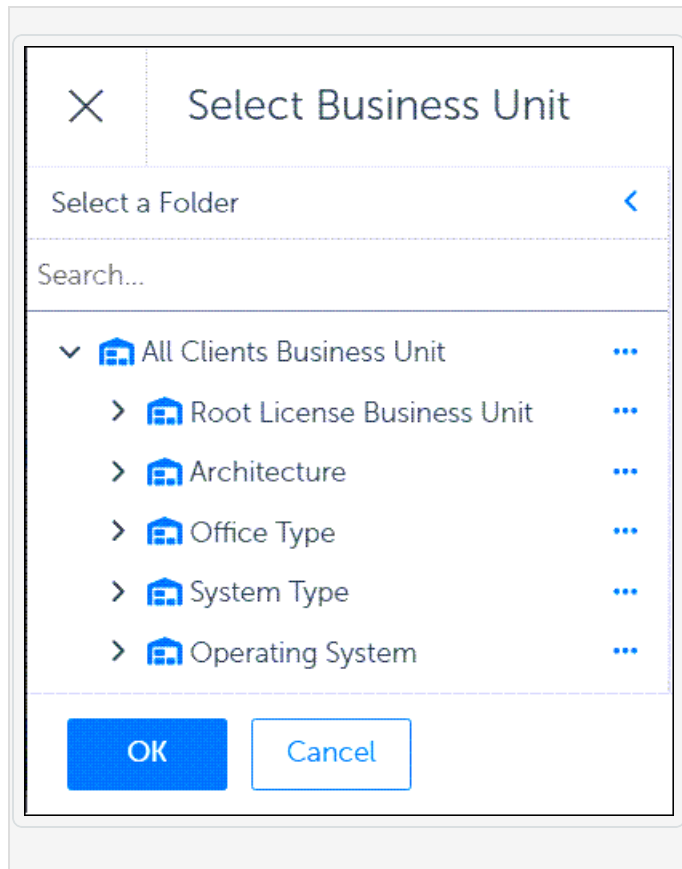
5. Add or remove **Business Units**:

- To remove existing Business Units, select the **ellipsis (...)** under Actions, and then select **Remove Row**.



- To add Business Units, complete the following steps:

1. Select the Business Units.



2. Select **OK**.

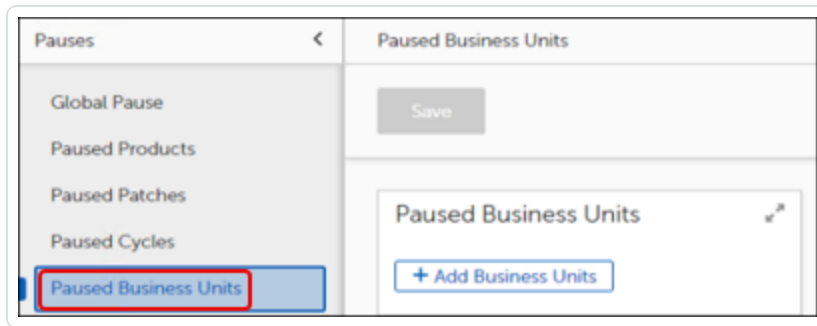
6. Select **Create Cycle Pause** and then click **Save** to create a pause for the selected rollout cycle.

Pause Deployment to a Business Unit

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

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

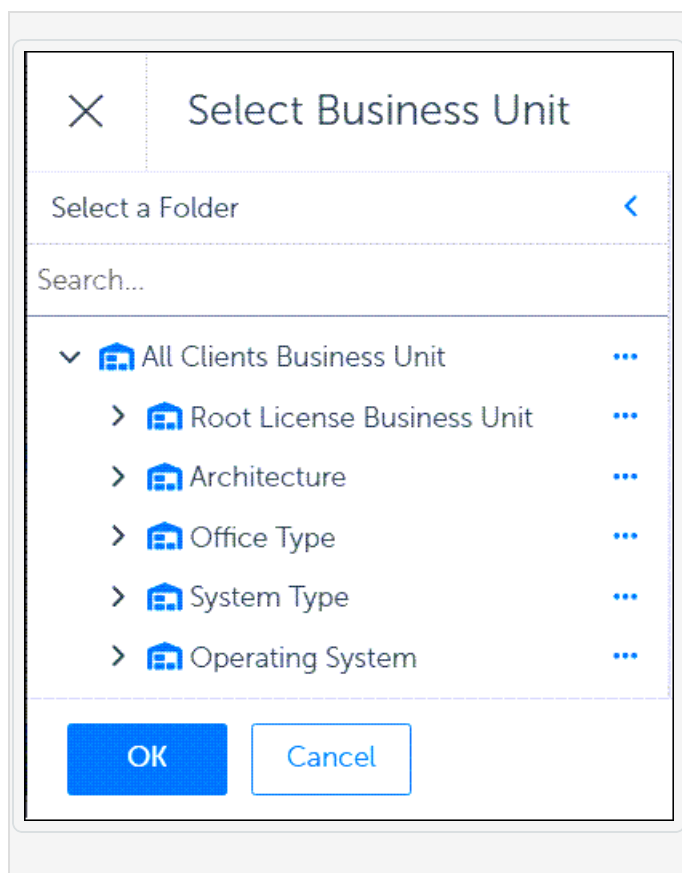
This opens the Paused Business Units dialog:



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

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

1. Select the Business Units.



2. Select **OK**.

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



Rollbacks Overview

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

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

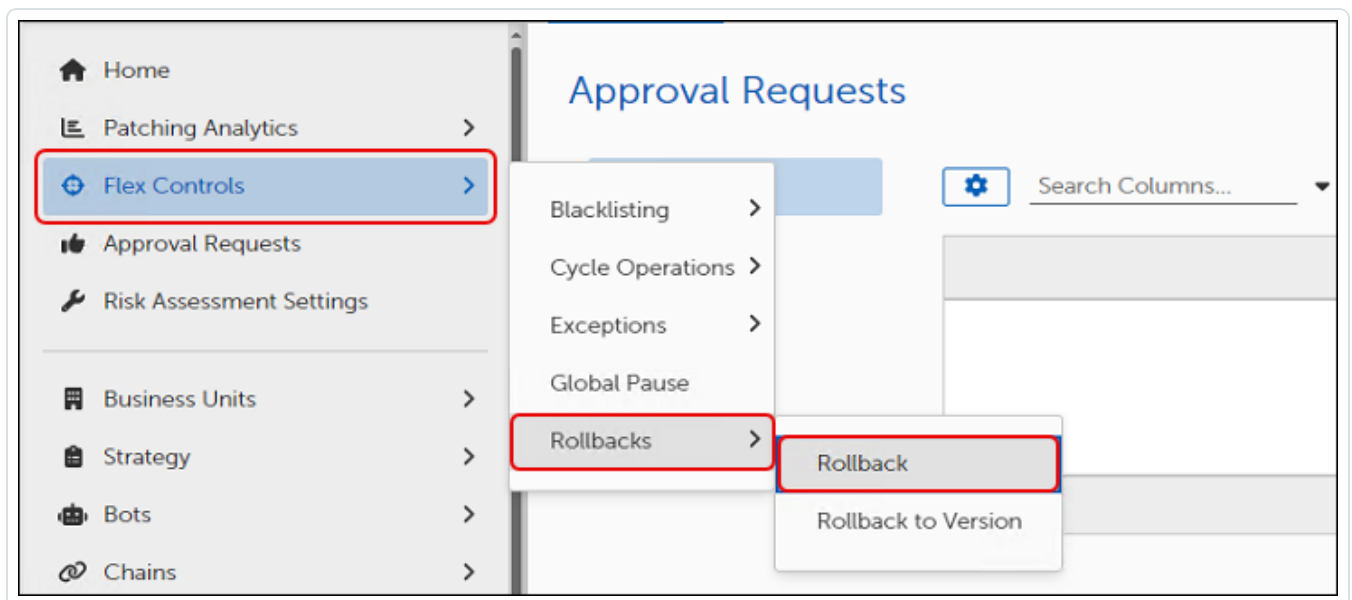
Rollback

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

Create a Rollback

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

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



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

Patching Rollbacks

Show All + New

Search Columns...

×

Search

No data provided

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

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

▼

General Settings

Name *

Name

Description

Description

Patch ⓘ *

Add Installable Software

BROWSE

Target Business Units ⓘ *

+ Add Business Units

- 341 -



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

Patch ⓘ ★ Add Installable Software **BROWSE**

4. Select a Software patch or release :

1. Enter a product name on the search line, and then click **Search**. This example uses Google Chrome.
2. Select the product from the list, and then click **OK**.

Search Columns... chrome

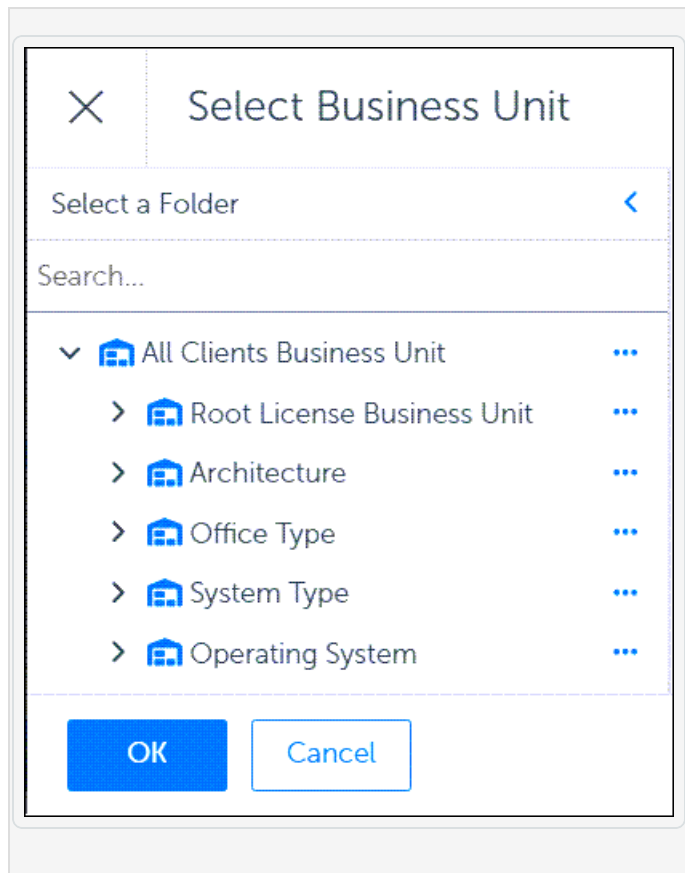
	Product Name	Publisher	Operating System
>	Google Chrome Beta x86	Google LLC	Windows
>	Google Chrome Beta x64	Google LLC	Windows
>	Google Chrome x86	Google LLC	Windows
>	Google Chrome x64	Google LLC	Windows

OK Cancel

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



1. Select the Business Units.



2. 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...

Search

	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 ...	...

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



Copy a Rollback

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

Patching Rollbacks

Show All + New

Search Columns...

Search

☐	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 ...	...

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

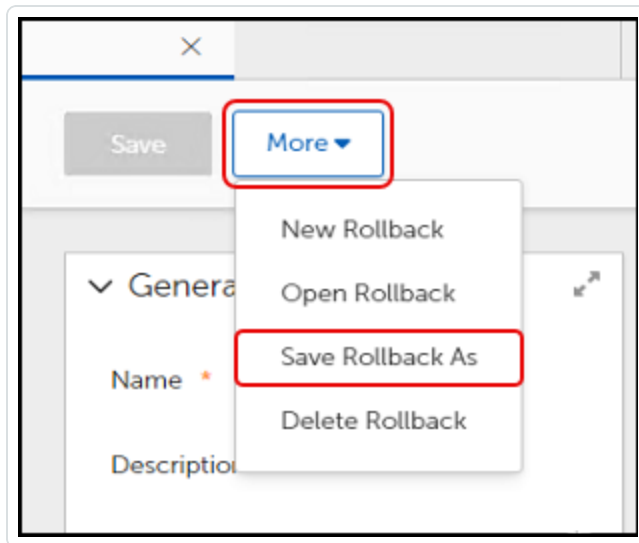
BROWSE X

Target Business Units ⓘ *

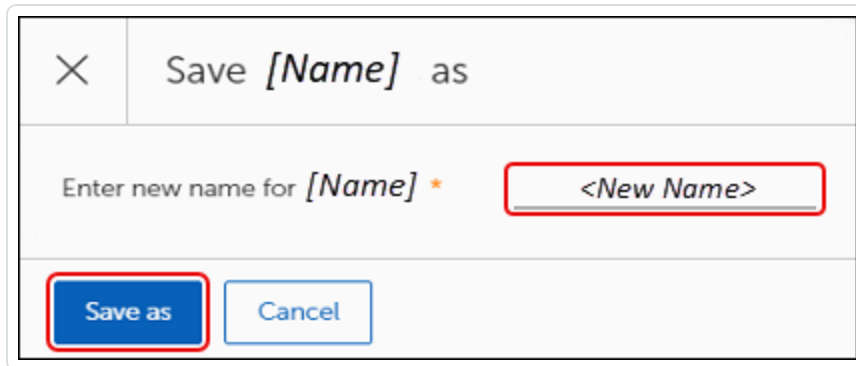
+ Add Business Units

☐	Name	Actions
☐	> Operating System	...

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



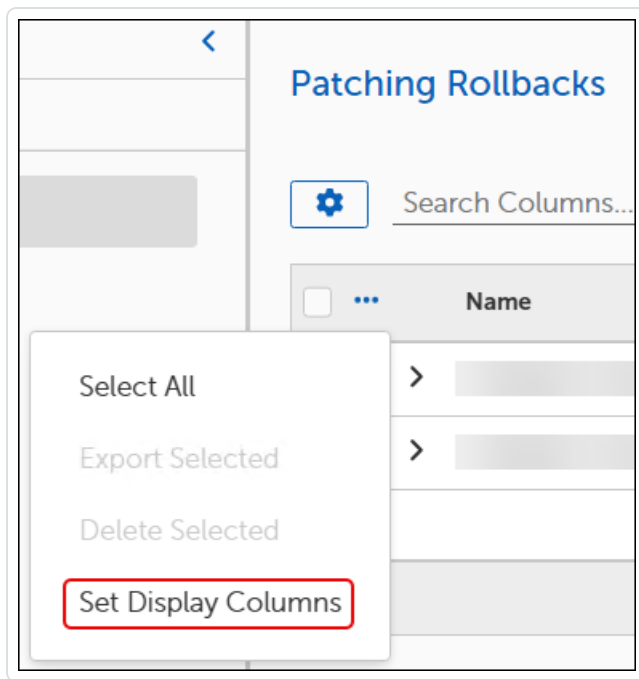
3. Enter a new **Name** for the template, and then click **Save as**.



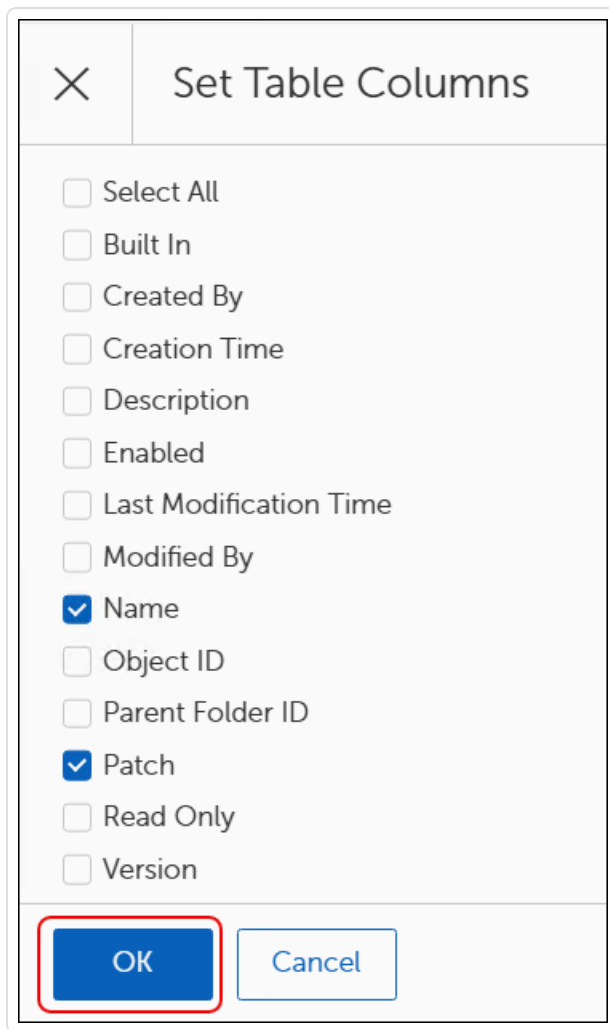
4. Revise the **Description** to reflect any changes needed for the copy, and then click **Save**.
5. Select **Back to Rollbacks** on the upper-left corner of the template to return to the Rollbacks table and view your changes.

Customize Patching Rollback Table Settings

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



This opens the Set Table Columns dialog.



Set Table Columns

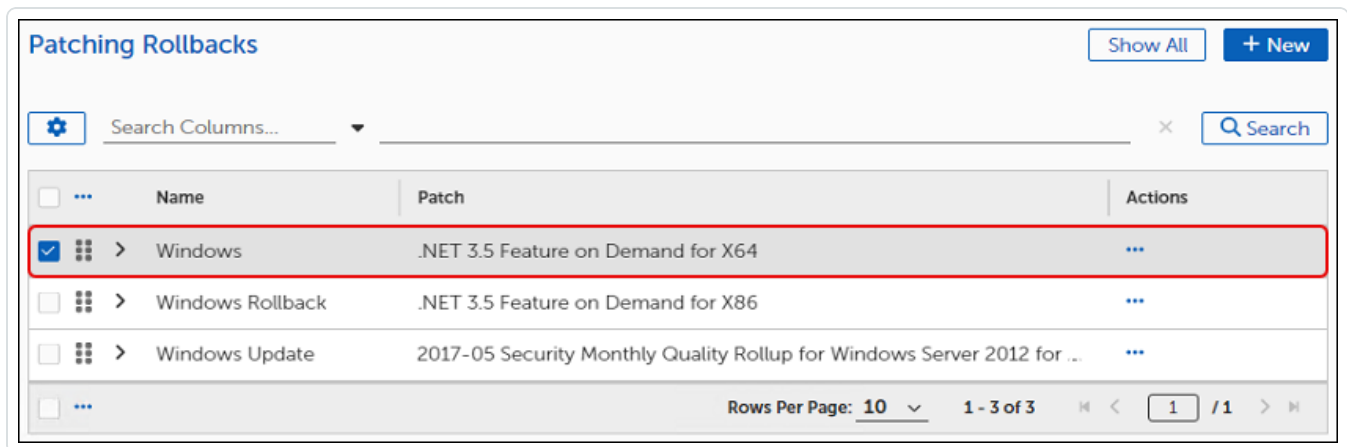
- ☐ Select All
- ☐ Built In
- ☐ Created By
- ☐ Creation Time
- ☐ Description
- ☐ Enabled
- ☐ Last Modification Time
- ☐ Modified By
- ☒ Name
- ☐ Object ID
- ☐ Parent Folder ID
- ☒ Patch
- ☐ Read Only
- ☐ Version

OK Cancel

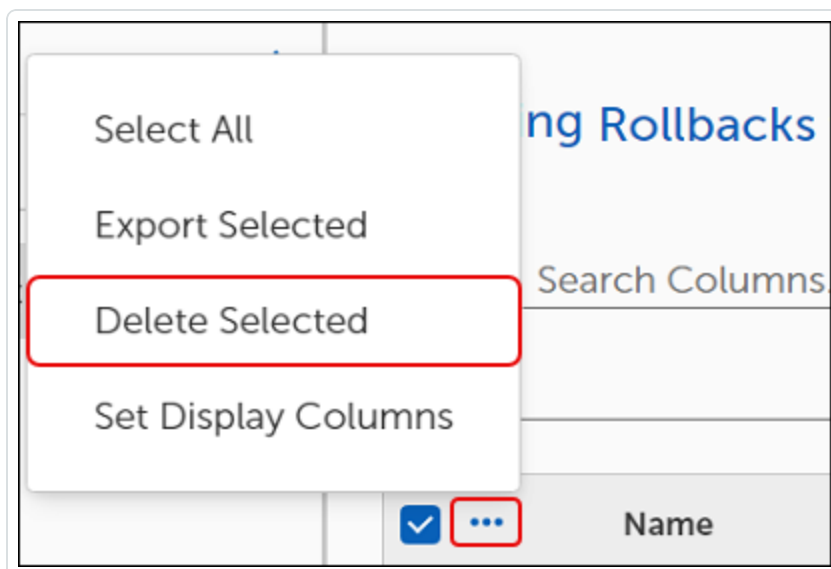
3. Select the **column names** you want the Patching Rollbacks table to display, and then click **OK**.

Delete a Rollback

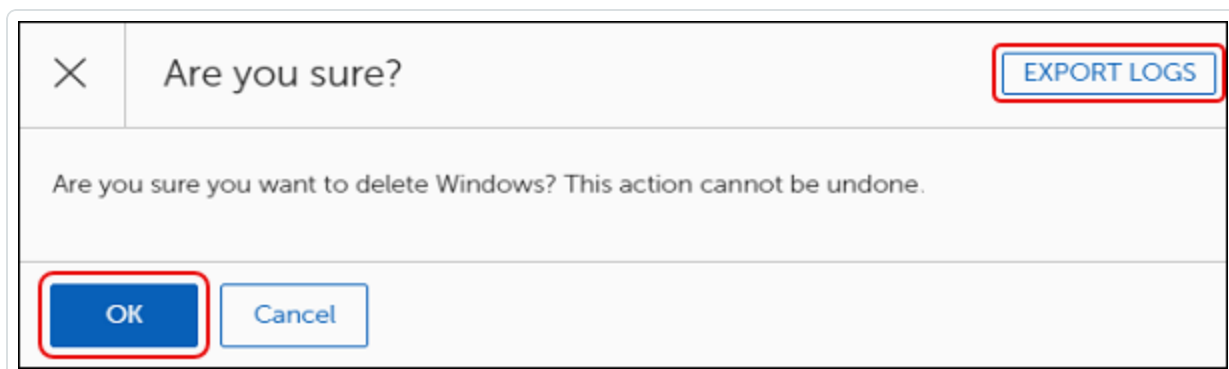
1. Select a **Rollback** template from the Patching Rollbacks table of an open [Patching Rollbacks](#) template.



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



3. Review the Are you sure? dialog:

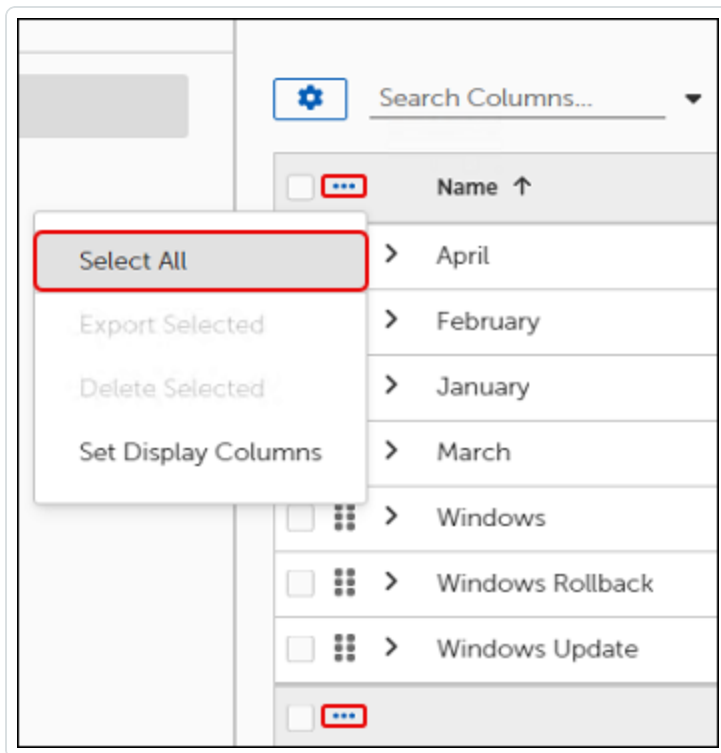




- a. Select **Export Logs** on the top-right corner of the Are you sure? dialog to export trace logs. The trace logs download to your device as a file with a .log extension.
 - b. Select **OK** to delete the Rollback.
4. Select **Back to Rollbacks** on the upper-left corner of the template to return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

Select All Rollbacks

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

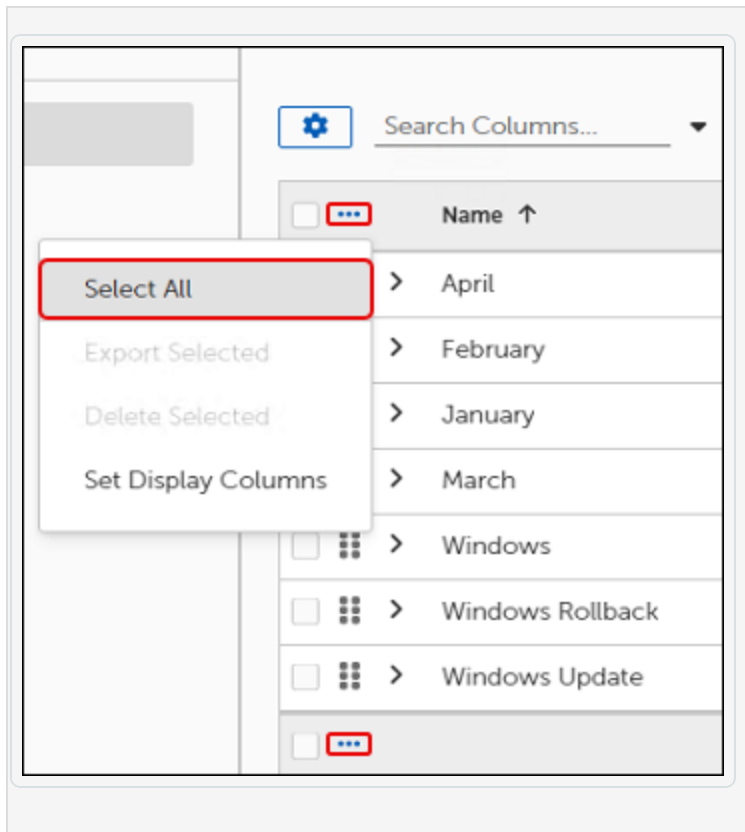


3. Select the ellipsis (...) again, and then choose what you want to do with the selected Rollbacks:
 - To export the selected Rollbacks, see [Select All Rollback to Version Objects](#).
 - To delete the Selected templates, see [Bulk Delete Rollbacks](#).
 - To customize the display columns of the Patching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

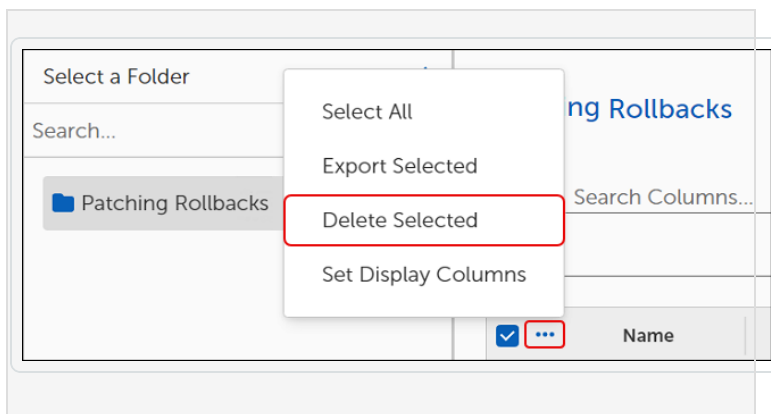
Bulk Delete Rollbacks



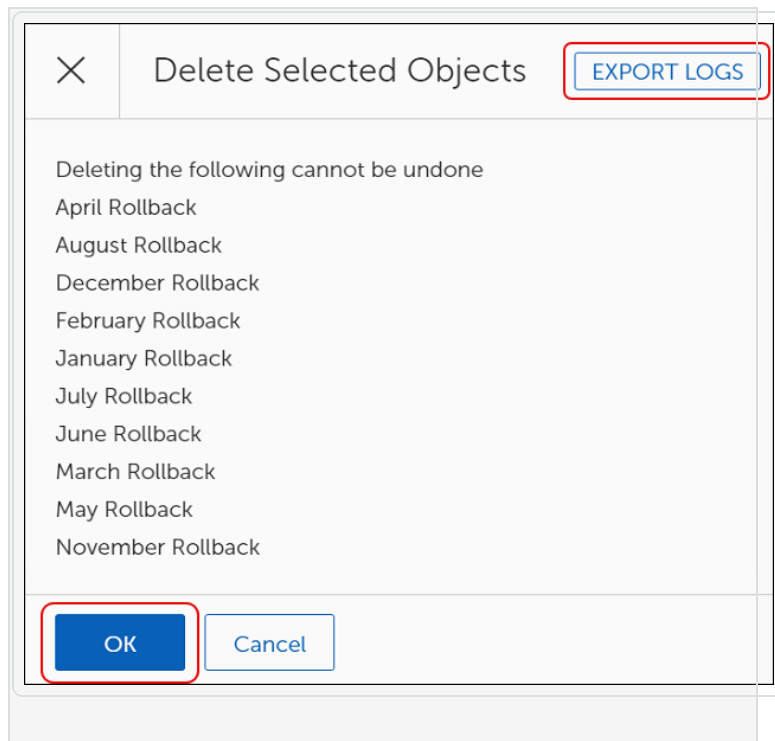
1. Open the **Patching Rollbacks** table (**Flex Controls > Rollbacks > Rollback**).
2. Select the **ellipsis (...)** next to Name, and then click **Select All**.



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



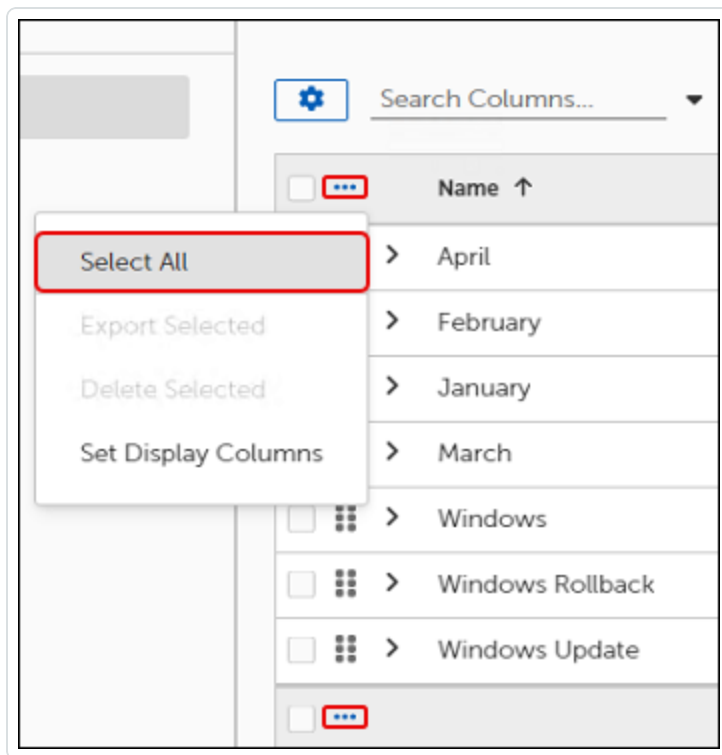
This opens the Delete Selected Objects dialog:



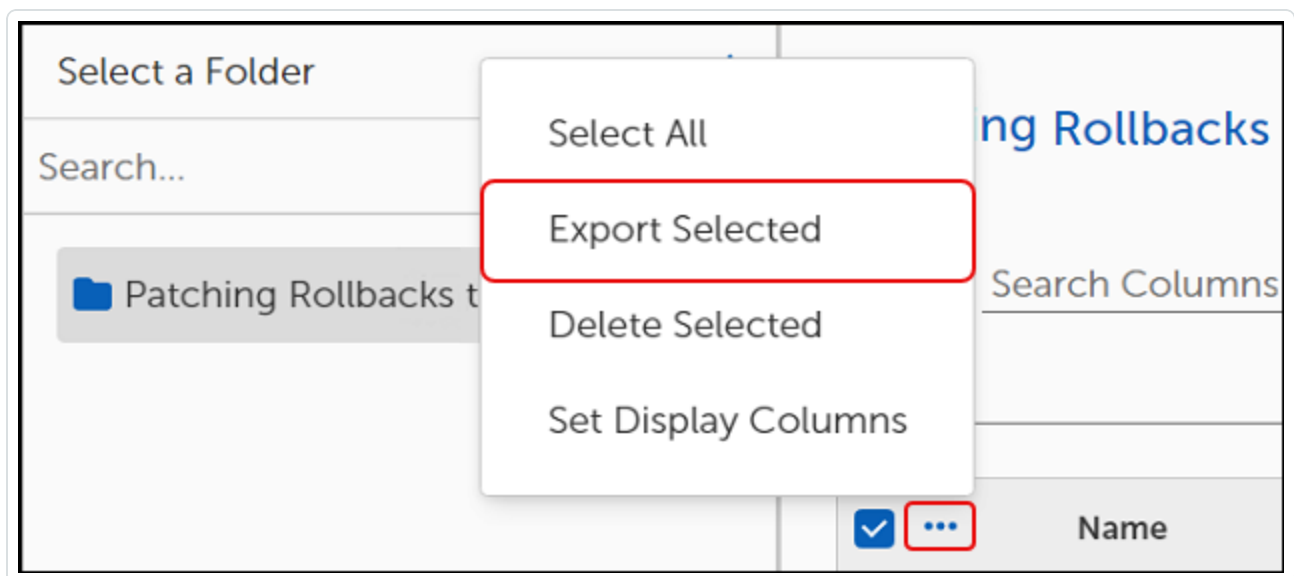
4. (Optional) Select **Export Logs** on the top-right corner of the Delete Selected Objects dialog to export trace logs. The trace logs download to your device as a file with a .log extension.
5. Select **OK** to delete the Rollbacks. This returns you to the **Patching Rollbacks** table where the deleted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

Export Rollbacks

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



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



This opens the Object Export Settings:

Object Export Settings

Exporting Organization

Exporting Organization Name

Description

Description

Export as JSON

Automatically Import Objects Into the Specified Folder

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

Errors (1)

Search Columns...

Search

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

Rows Per Page: 10

1 - 1 of 1

1 / 1

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

Configure Object Export Settings



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

The screenshot shows a dialog box titled "Object Export Settings" with a close button in the top right corner. The dialog is divided into two main sections. The top section has two labels: "Exporting Organization" and "Exporting Organization Name", with a horizontal line separating them. Below "Exporting Organization" is a label "Description" and a large text area containing the word "Description". The bottom section contains two toggle switches. The first is labeled "Export as JSON" and is currently turned off. The second is labeled "Automatically Import Objects Into the Specified Folder" and is also currently turned off.

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

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

Show Rollback References

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



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

Patching Rollbacks

Show All + New

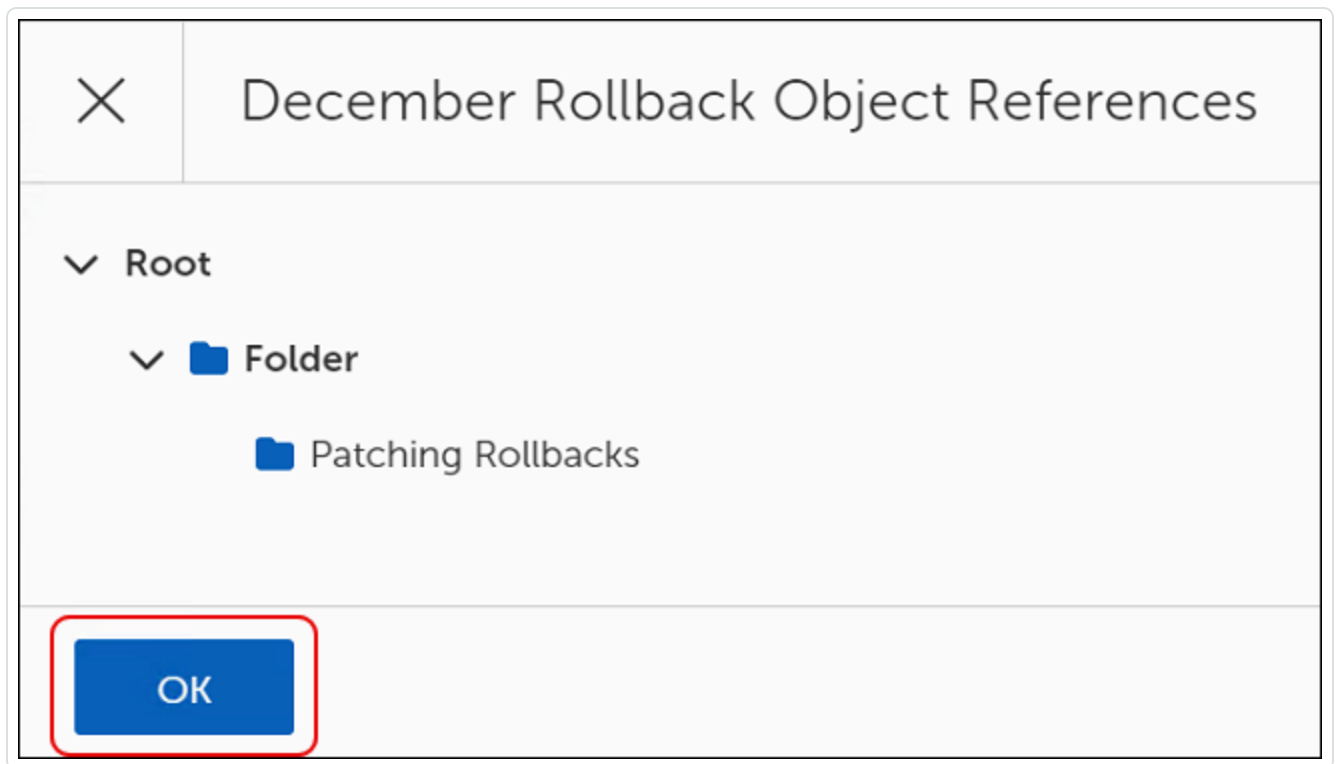
 Search Columns...    Search

☐	...	Name	Patch	Actions
☐		> April Rollback	.NET 3.5 F...	
☐		> August Rollback		
☐		> December Rollback		
☐		> February Rollback	.NET 3.5 F...	

Show References

Export

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.

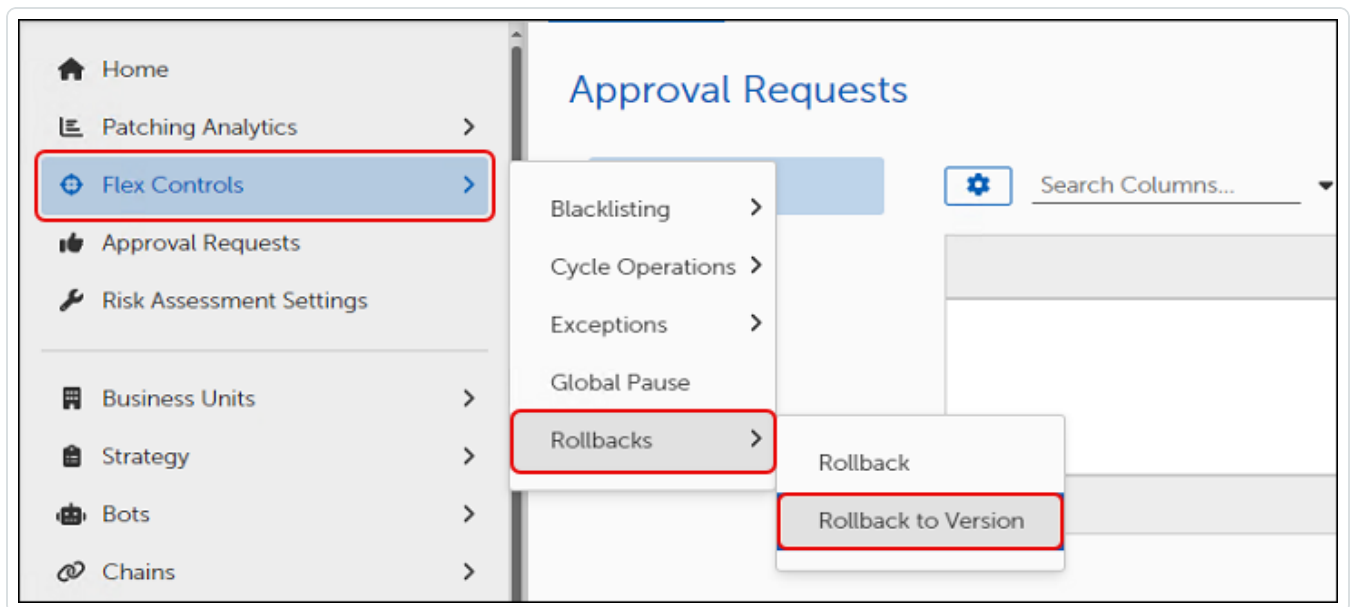
Rollback to Version

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](#).

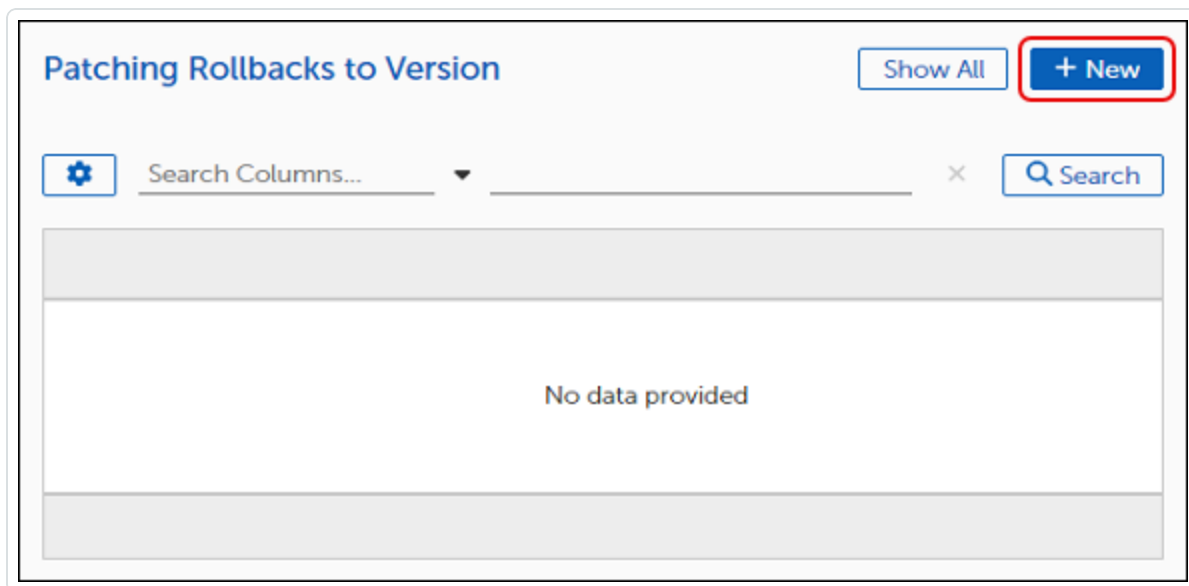
Create a Rollback to Version

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**.

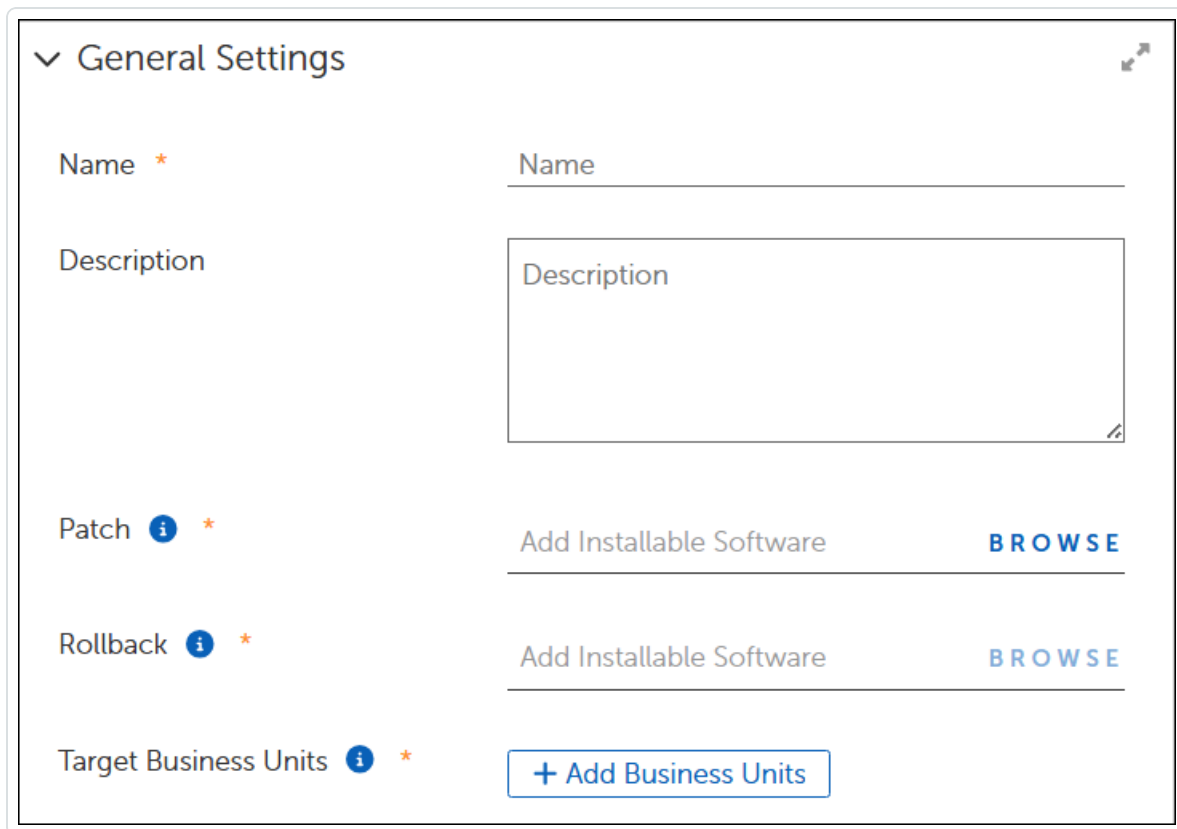


This opens the Patching Rollbacks to Version table. Until you create a rollback, the table is empty..



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

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



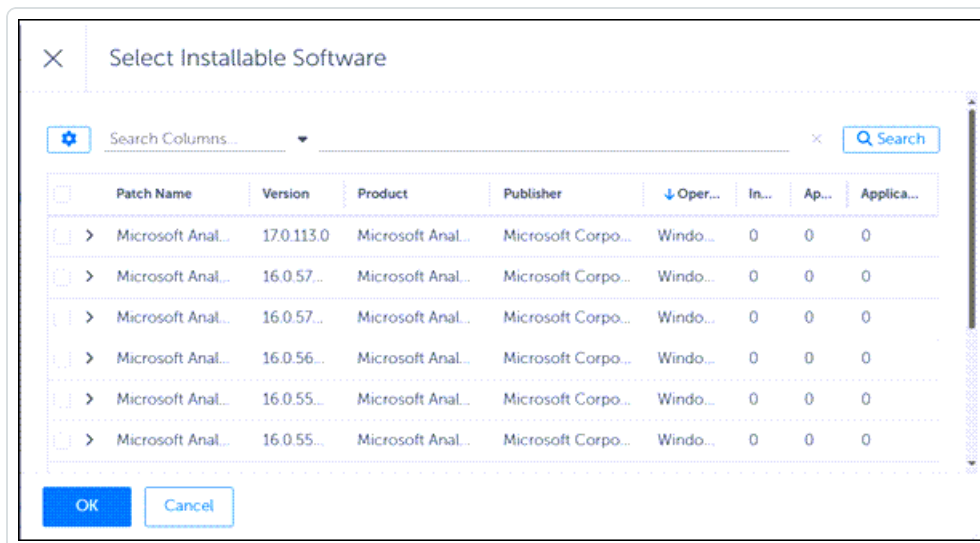
4. Add the patch or release to roll back from.

Choose the Software Patch or Release Version to Roll Back From

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

Patch ⓘ * Add Installable Software **BROWSE**

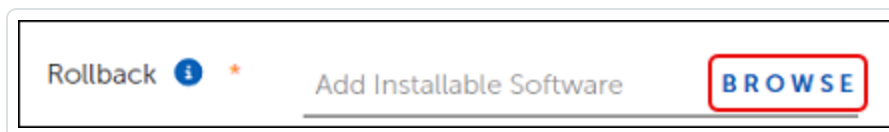
2. Choose the **Software Patch** or **Software Release** from the Add Installable Software table to roll back from. You can select only one Patch or Release to roll back from.



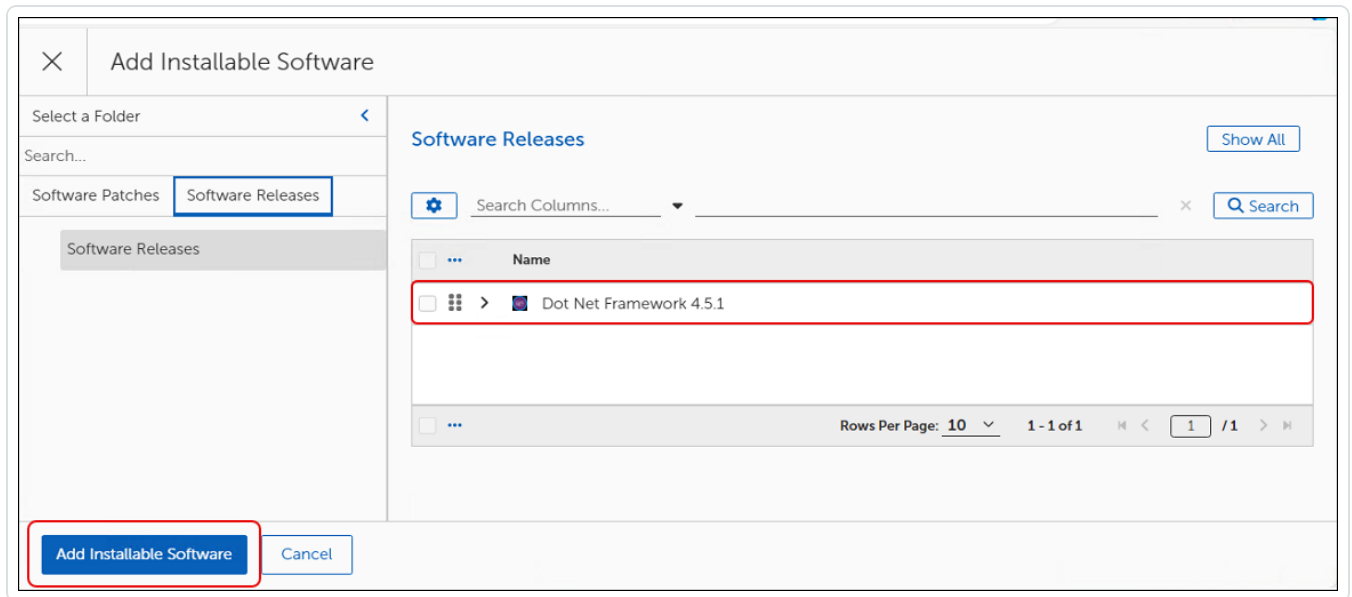
3. Select **Add Installable Software** to return to the Rollback to Version template.
4. [Choose the software patch or release version to roll back to.](#)

Choose the Software Patch or Release Version to Roll Back To

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



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



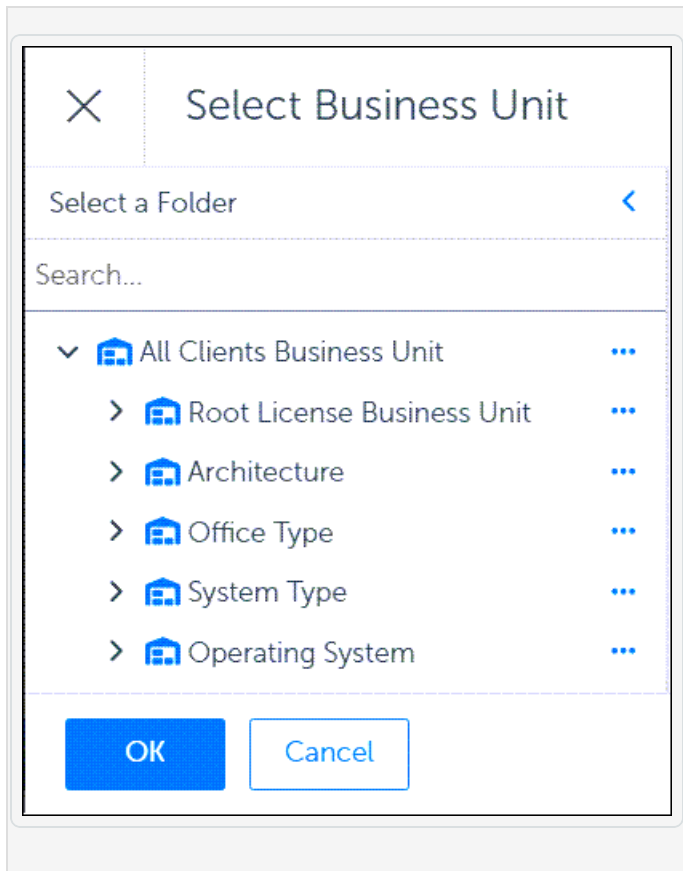
3. Select **Add Installable Software**.
4. [Add target Business Units for the Rollback to Version.](#)

Add Business Units for a Rollback to Version



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

1. Select the Business Units.



2. 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...

×

Search

☐	...	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 ...	...
☐	...			

Rows Per Page: 10

1 - 3 of 3

1 / 1

This opens the template.

▼ General Settings

Name *

Name

Description

Description

Patch ⓘ *

Add Installable Software

BROWSE

Rollback ⓘ *

Add Installable Software

BROWSE

Target Business Units ⓘ *

+ Add Business Units

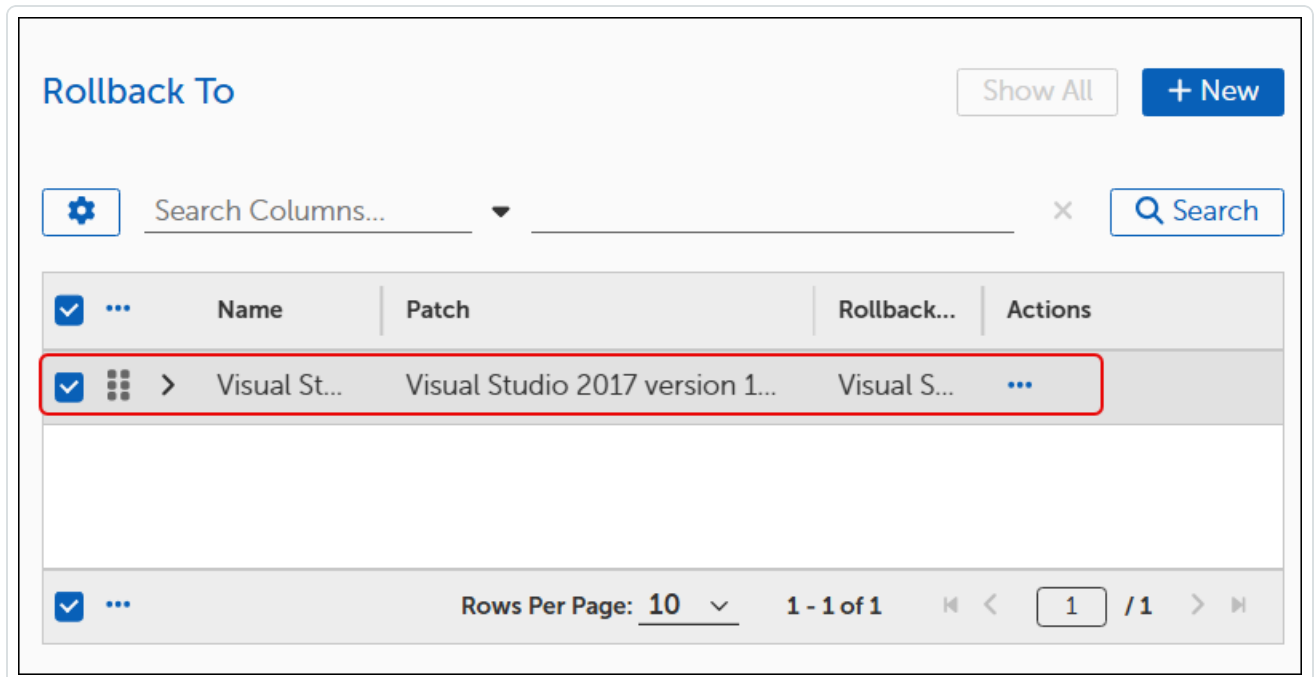
2. Modify the Rollback settings:



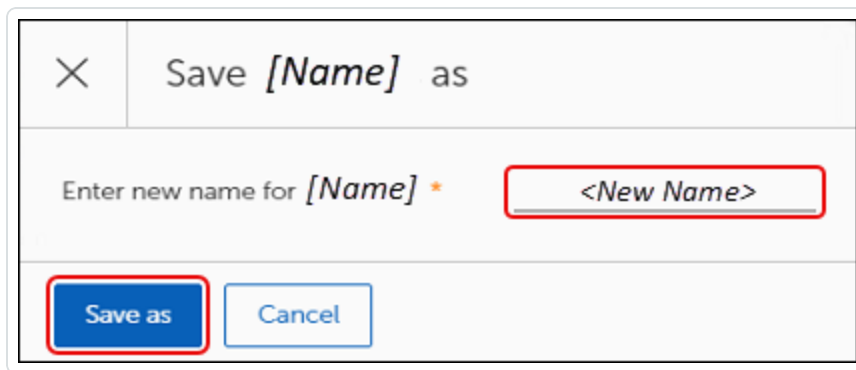
- a. Select **Browse** for Patch to choose a patch or release to roll back from.
 - b. Select **Browse** for Rollback to choose the version of the patch or release to roll back to.
 - c. Select **+Add Business Units** to add or remove target devices.
3. Select **Save** top-left corner of template to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

Copy a Rollback to Version Template

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



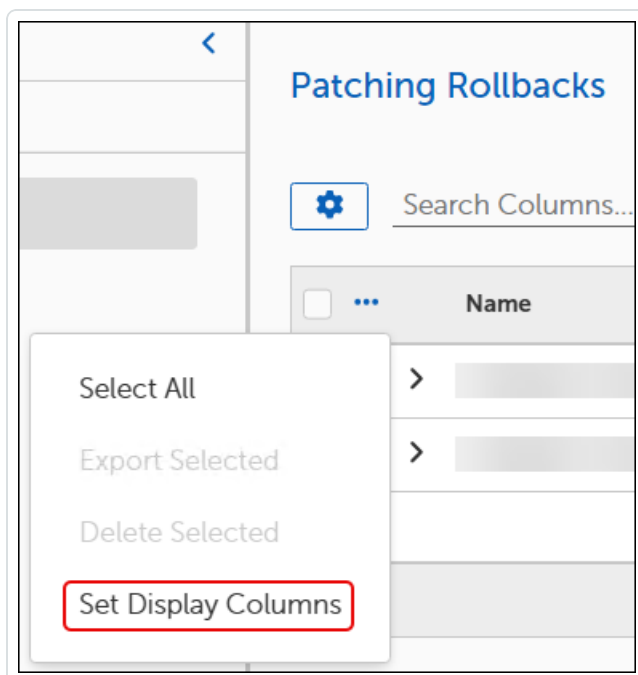
This opens the template.



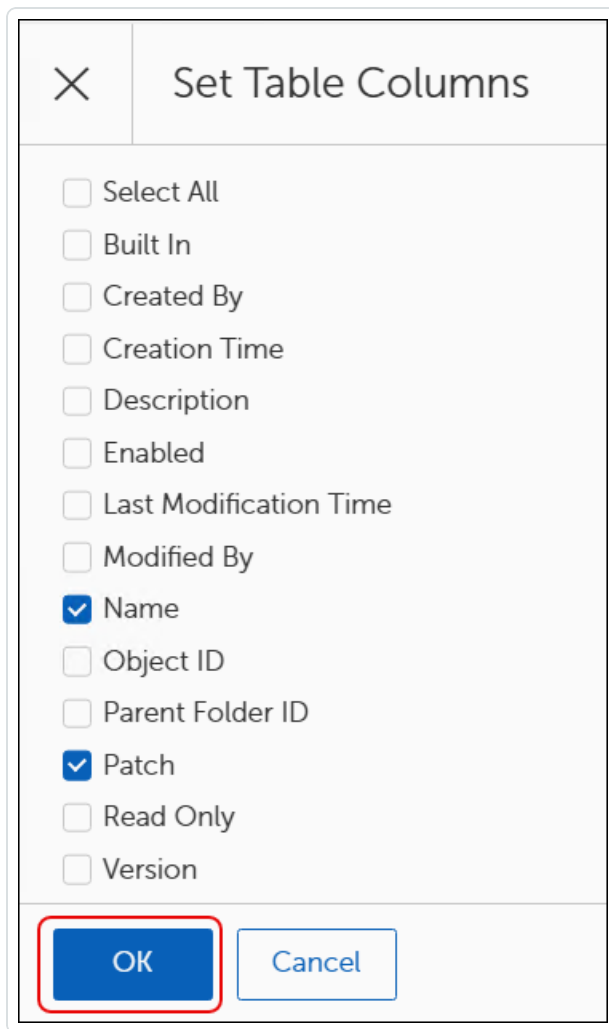
4. Revise the **Description** to reflect any changes needed for the copy, and then click **Save**.
5. Select **Back to Rollbacks** on the upper-left corner of the template to return to the Rollbacks table and view your changes.

Customize Patching Rollback Table Settings

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



This opens the Set Table Columns dialog.



Set Table Columns

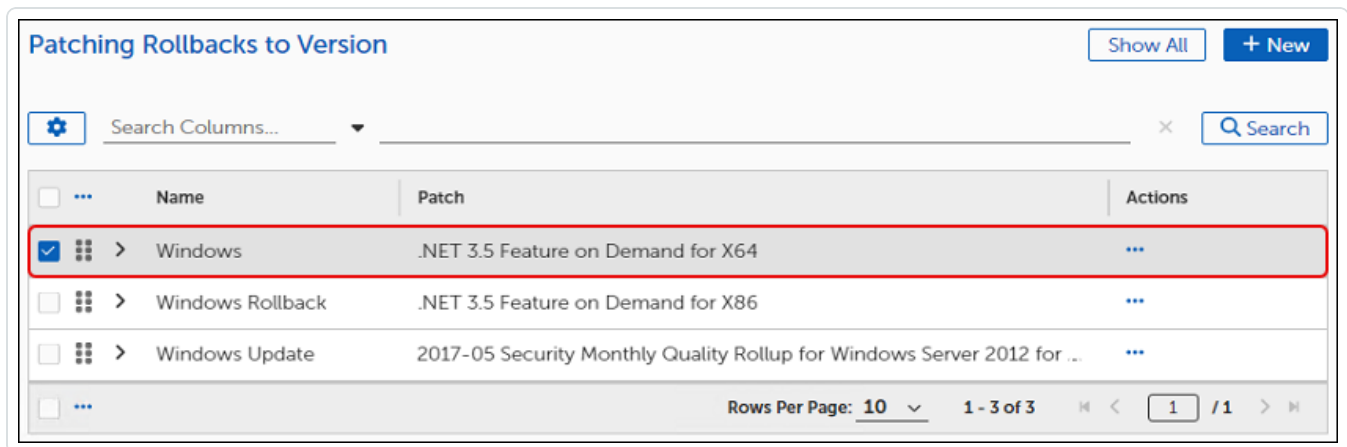
- ☐ Select All
- ☐ Built In
- ☐ Created By
- ☐ Creation Time
- ☐ Description
- ☐ Enabled
- ☐ Last Modification Time
- ☐ Modified By
- ☒ Name
- ☐ Object ID
- ☐ Parent Folder ID
- ☒ Patch
- ☐ Read Only
- ☐ Version

OK Cancel

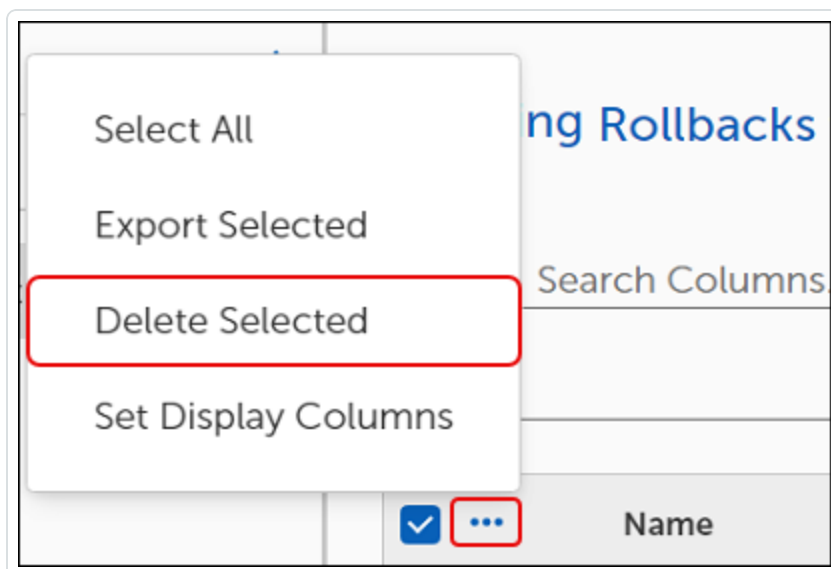
3. Select the **column names** you want the Patching Rollbacks table to display, and then click **OK**.

Delete a Rollback to Version

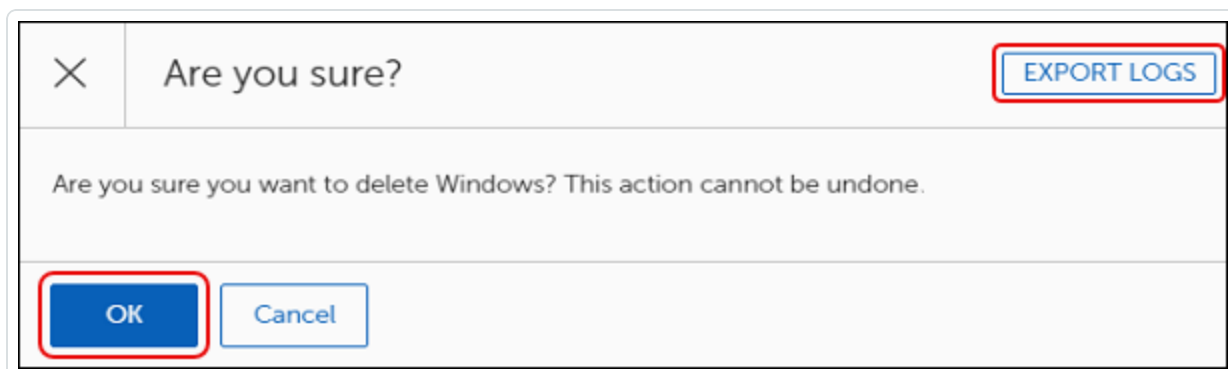
1. Select a **Rollback to Version** template from the Patching Rollbacks to Version table of an open [Patching Rollbacks](#) template.



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



- Review the Are you sure? dialog:

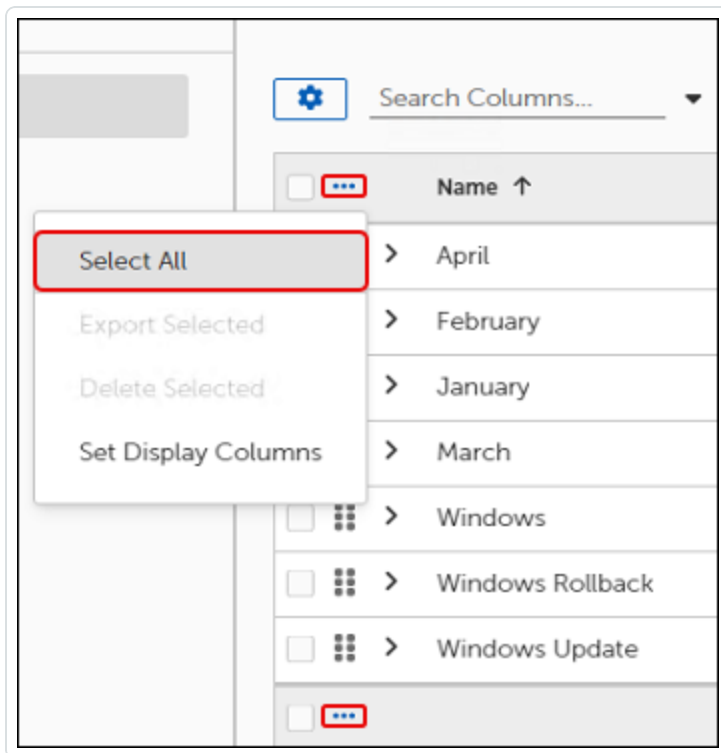




- a. Select **Export Logs** on the top-right corner of the Are you sure? dialog to export trace logs. The trace logs download to your device as a file with a .log extension.
 - b. Select **OK** to delete the Rollback.
4. Select **Back to Rollbacks** on the upper-left corner of the template to return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

Select All Rollback to Version Objects

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



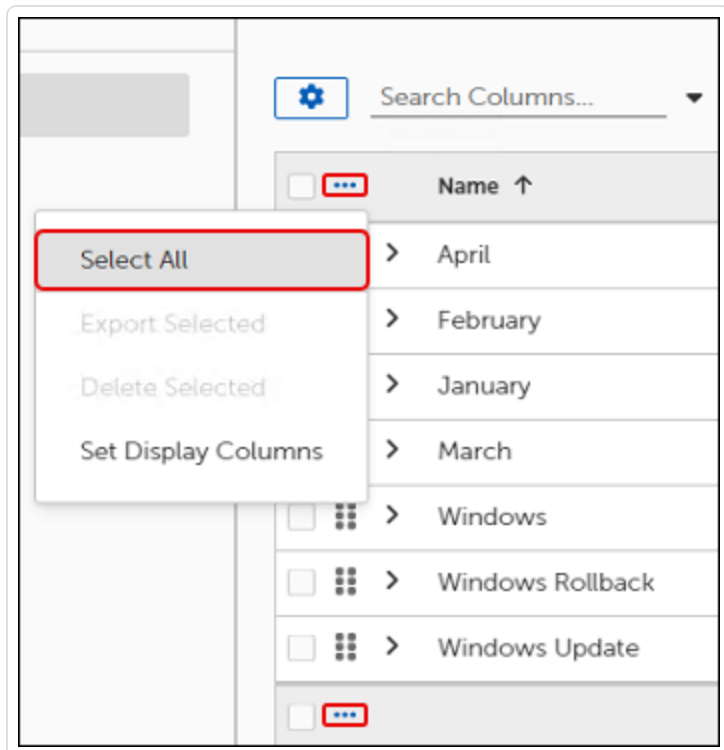
3. Select the ellipsis (...) again, and then choose what you want to do with the selected Rollbacks:
 - To export the selected Rollbacks, see [Select All Rollback to Version Objects](#).
 - To delete the Selected templates, see [Bulk Delete Rollbacks](#).
 - To customize the display columns of the Patching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

Bulk Delete Rollback to Version

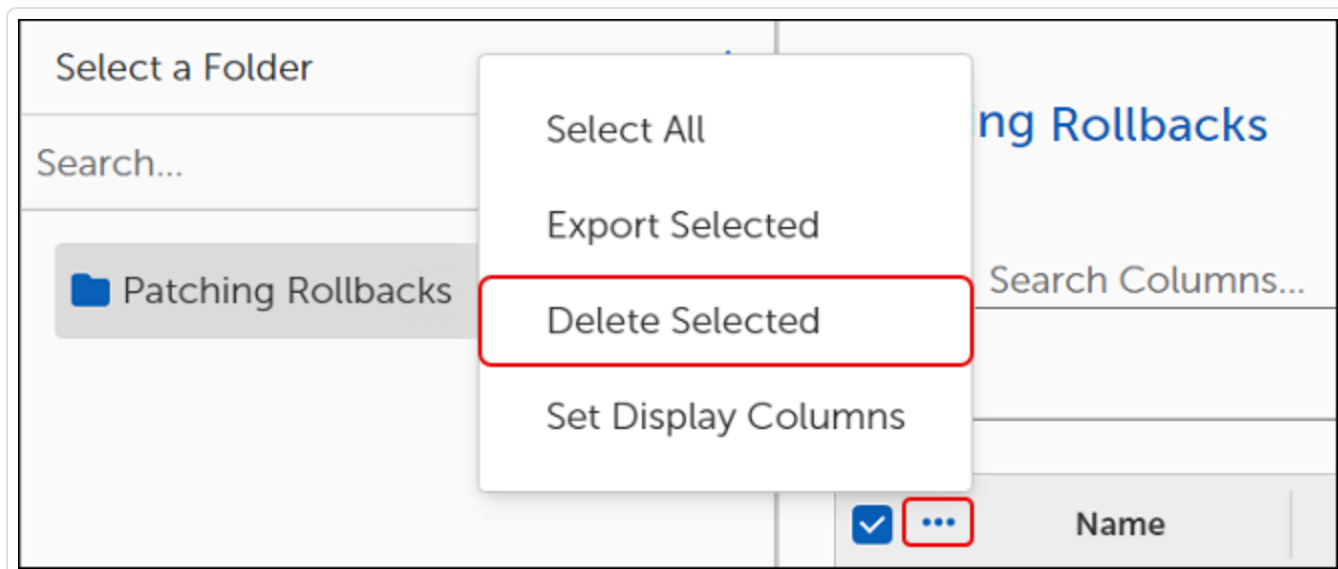


Use the following task to delete all Rollback to Version templates.

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

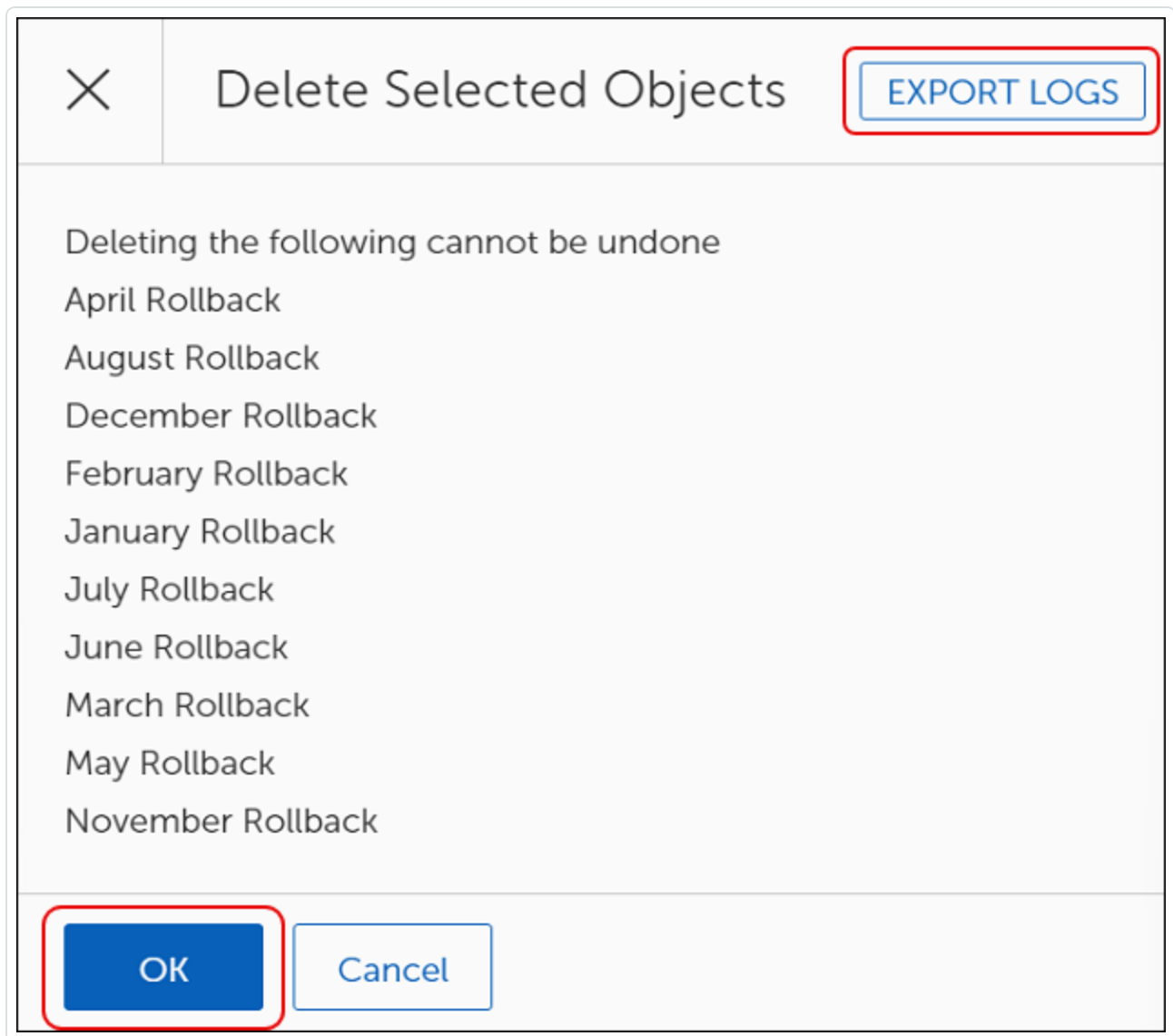


3. Select the **ellipsis (...)** next to Name, and then select **Delete Selected**.





This opens the Delete Selected Objects dialog:

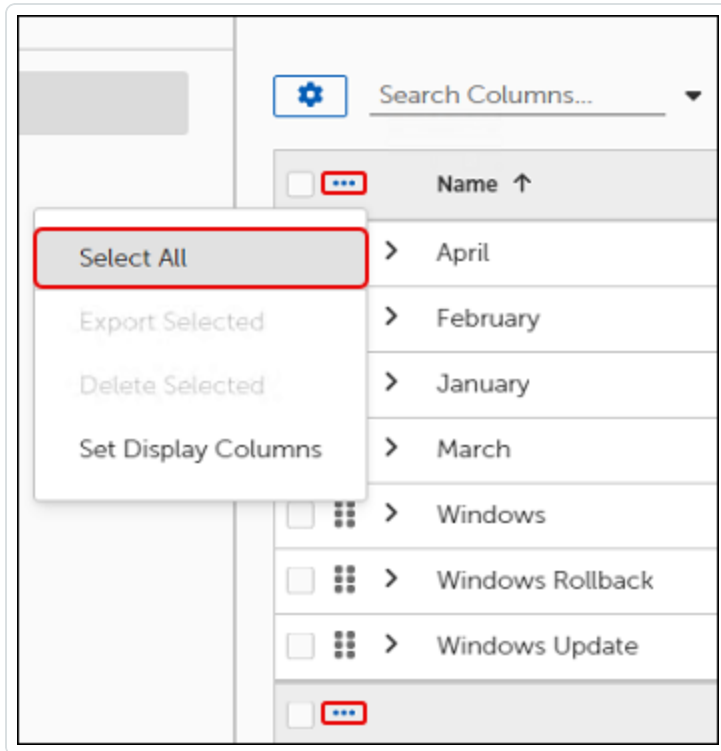


4. (Optional) Select **Export Logs** on the top-right corner of the Delete Selected Objects dialog to export trace logs. The trace logs download to your device as a file with a .log extension.
5. Select **OK** to delete the Rollbacks. This returns you to the **Patching Rollbacks to Version** table where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

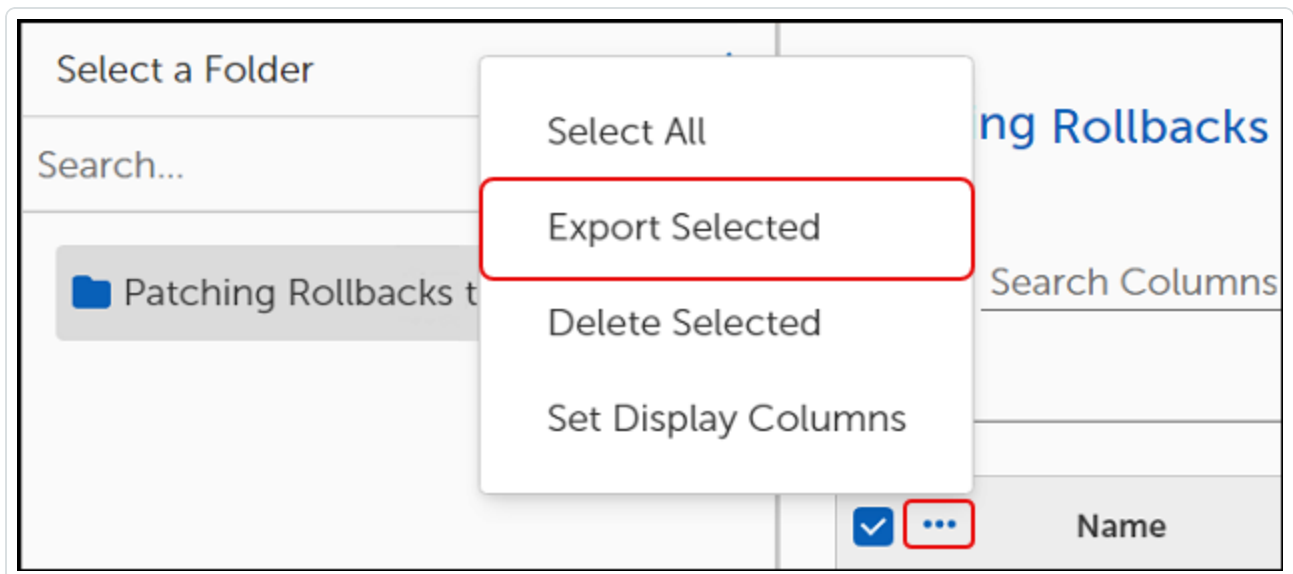
Export Rollback to Version



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



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



This opens the Object Export Settings:

Object Export Settings

Exporting Organization

Exporting Organization Name

Description

Description

Export as JSON

Automatically Import Objects Into the Specified Folder

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

Errors (1)

Search Columns...

Search

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

Rows Per Page: 10

1 - 1 of 1

1 / 1

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

Configure Object Export Settings



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

The screenshot shows a dialog box titled "Object Export Settings" with a close button in the top right corner. Inside the dialog, there are two columns. The left column contains labels: "Exporting Organization", "Description", "Export as JSON", "Automatically Import", and "Objects Into the Specified Folder". The right column contains a text input field labeled "Exporting Organization Name", a large text area labeled "Description", and two toggle switches for "Export as JSON" and "Automatically Import". The "Export as JSON" toggle is currently turned on, and the "Automatically Import" toggle is currently turned off.

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

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

Show Rollback to Version References

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



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

Patching Rollbacks to Version

Show All + New

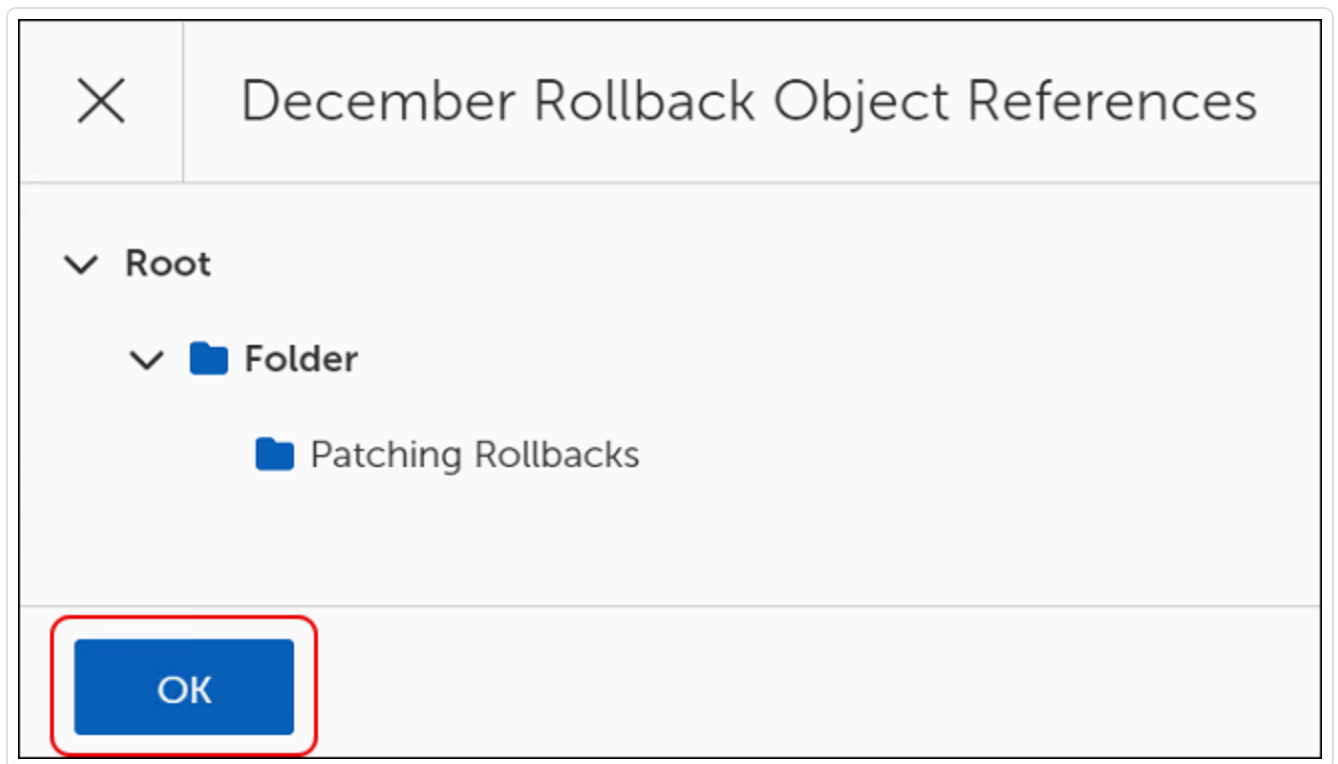
 Search Columns...    Search

☐	...	Name	Patch	Actions
☐		> April Rollback	.NET 3.5 F...	
☐		> August Rollback		
☐		> December Rollback		
☐		> February Rollback	.NET 3.5 F...	

Show References

Export

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.

Patching Strategies

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

Purpose of a Patching Strategy

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

Functionally, a Patch Strategy performs the following:

Automated handling of new patches



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

Customized targeting of patches

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

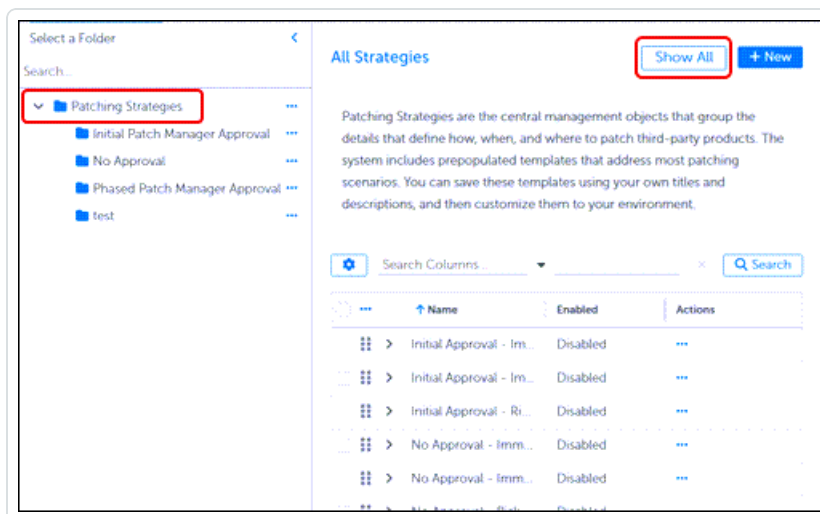
Reuse Intent Schema Objects

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

View built-in Patching Strategies

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

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



Appendices



Software Products

Tenable Patch Management 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

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

The metadata team receives automatic notification within 24 hours of an update release. The team uses Virus Total to scan all downloaded content in an isolated and secured environment. The Virus Total score for the content must be zero (0) before Tenable Patch Management publishes the content to the Tenable Patch Management Content Delivery Network (CDN). The Tenable Patch Management 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://www.adaptiva.com/OneSitePatch3rdPartyAppCatalog) for more information.

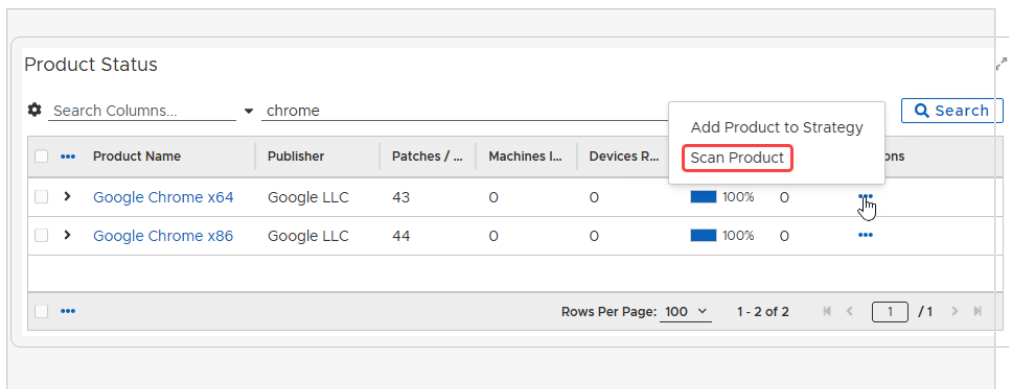
Endpoint Scans

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



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

×

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

	...	Name	Actions
☐	☰	> 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.

Menu Objects for Tenable Patch Management

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

Patch Content



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

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

Customer Extension Data

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

The screenshot shows a configuration window titled "Customer Extension Data" with a dropdown arrow on the left and a maximize icon on the right. Inside the window, there is a label "Customer Extension Data" followed by an information icon (i). To the right of this label are two input fields: "New Key" and "New Value". Below these fields is a button labeled "+ Add".

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

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

Deployment Channels and Deployment Channel Processes

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

Deployment Channel Processes are responsible for deploying patches to Business Units, and specifying the deployment schedule. When a patch is ready for deployment, it is queued and held



until the next scheduled execution. At that point, the Deployment Channel Process activates, processes all queued patches, and deploys them to the appropriate Business Units.

Deployment Channels

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

Understanding Channel Merging Rules

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

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

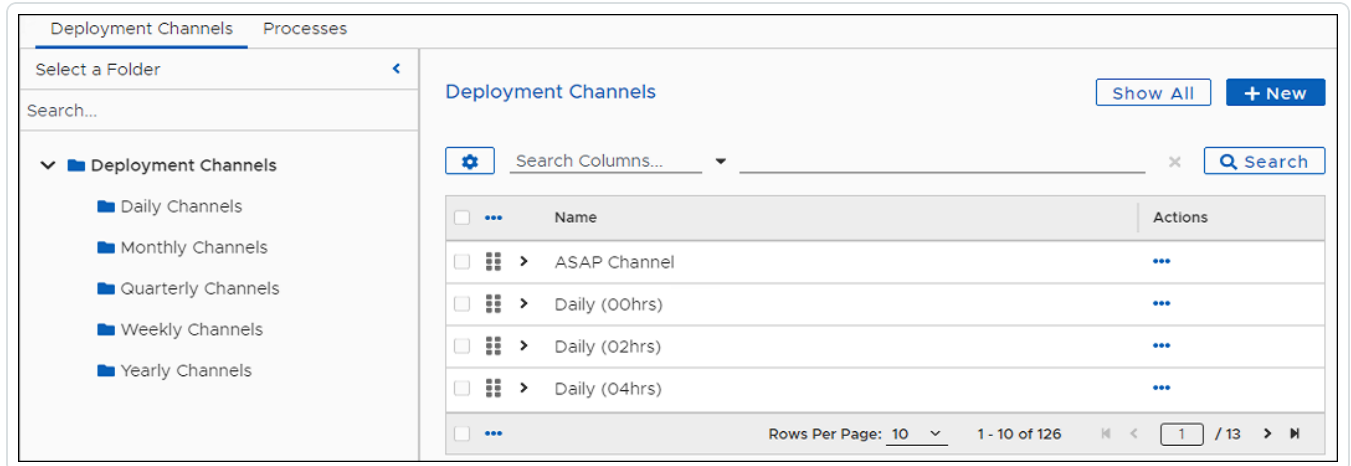
Creating a Deployment Channel

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

Open and Save a Deployment Channel Template



1. Hover over or select **Deployment Channels** in the left navigation menu of the [Patch Management Dashboard](#), and then select **Deployment Channels**. This opens the table of existing Deployment Channel templates.
2. [Create a New Folder for Objects](#) in the Deployment Channels Menu.
3. Select Show All to view the available templates.



4. Select the **Name** of an existing Deployment Channel template to open it.
5. Save the **template** with a new Name:
 - a. Select **More** in the upper-left corner of the dialog, and then select **Save As**.
 - b. Enter a new name for the template, and then click **Save as** on the lower-left corner of 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 corner of the dialog.
6. Move the new template to the folder you created, either now or when you complete your changes.

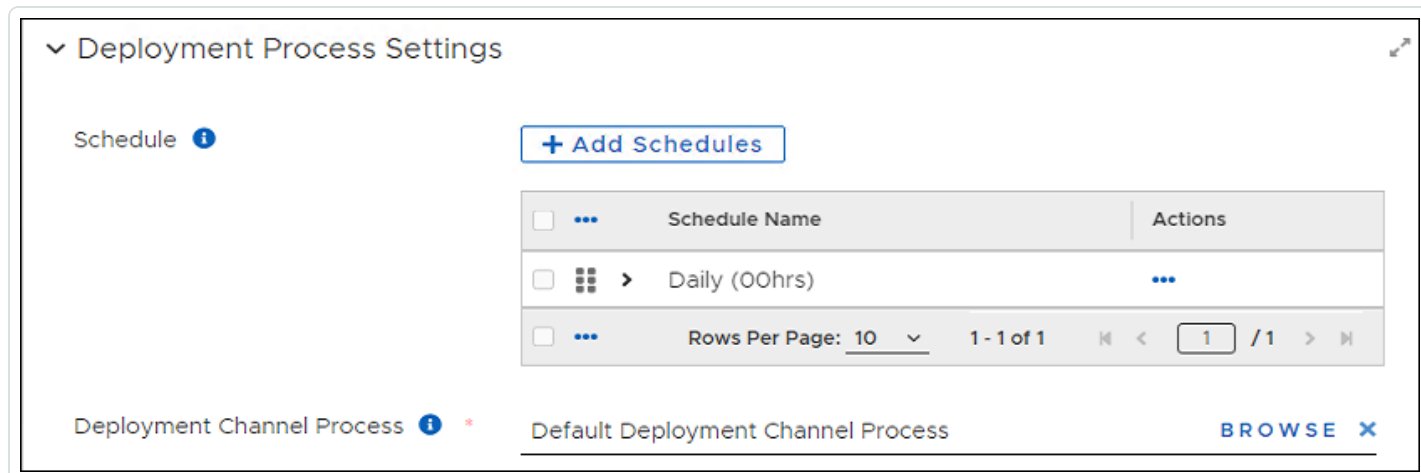
Deployment Process Settings

To add Deployment Process Settings to a Deployment Channel template:

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

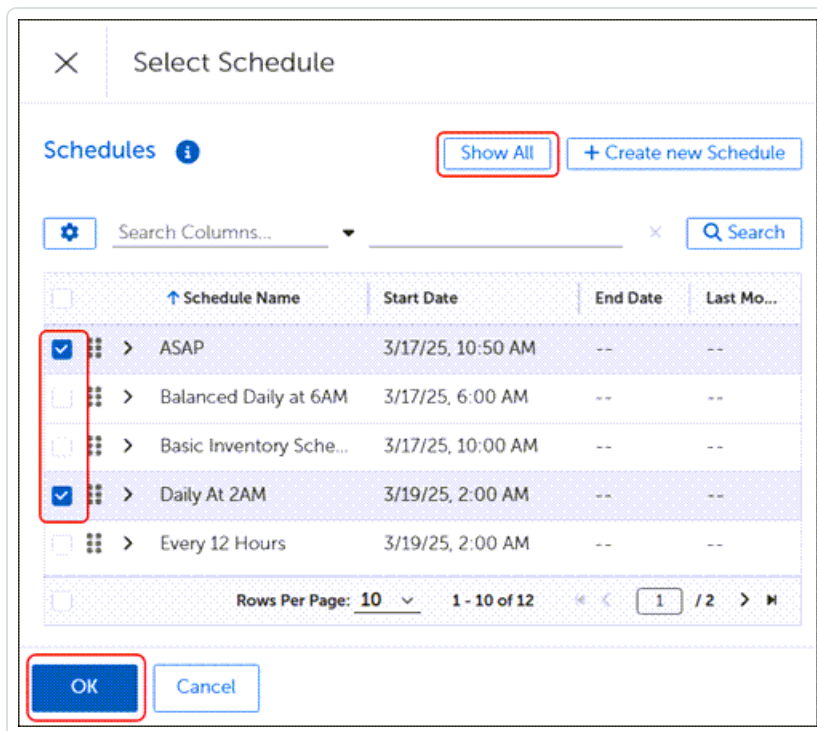


This opens the Deployment Process workspace.



Add or Change a Deployment Process Schedule

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

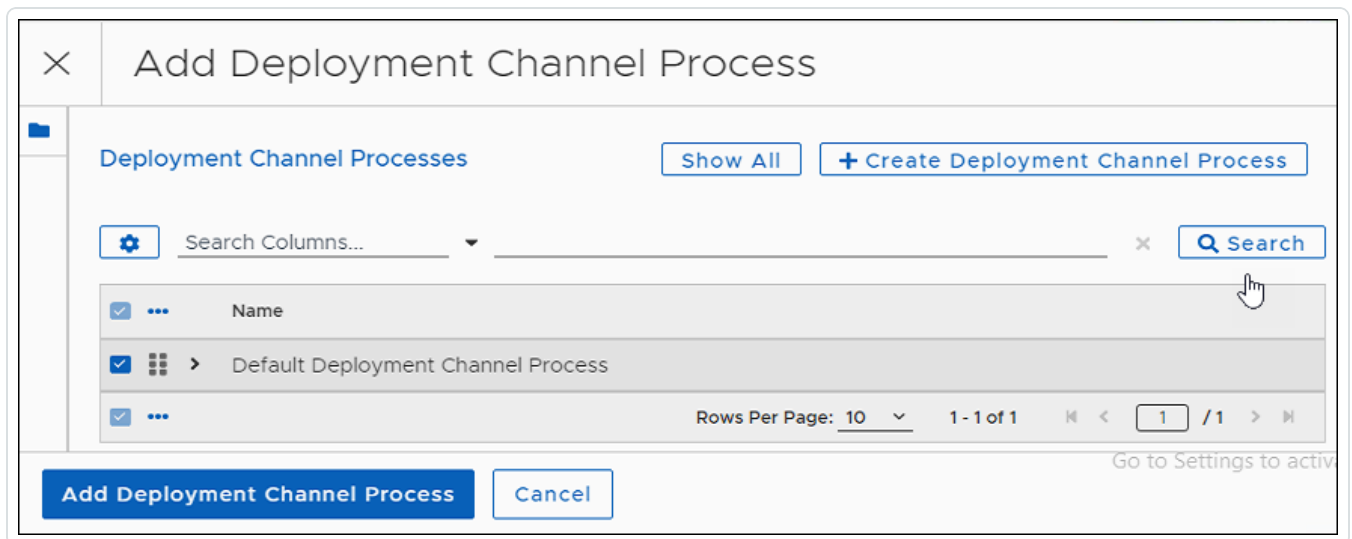


3. Select **Save** on the upper left to save your changes:

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

Add or Change a Deployment Channel Process

- Select **+ Add Schedules** from the Deployment Process Settings workspace of an open Deployment Channel template.
- Select **Show All** to see the available processes, and the select the **Process** to use for this Deployment Channel.



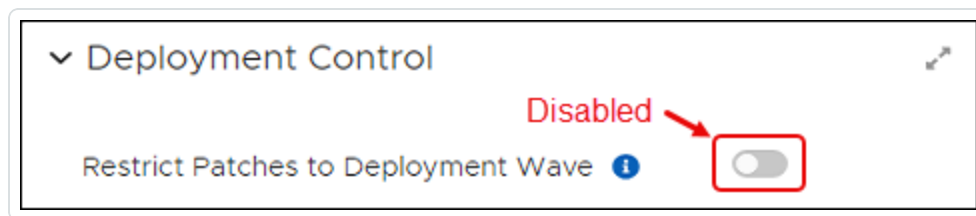
3. Select **Add Deployment Channel Process** on the bottom left to return to the template.

Deployment Control

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

To configure Deployment Control:

Open a [Deployment Channel template](#) , and then scroll down to the **Deployment Control** workspace.

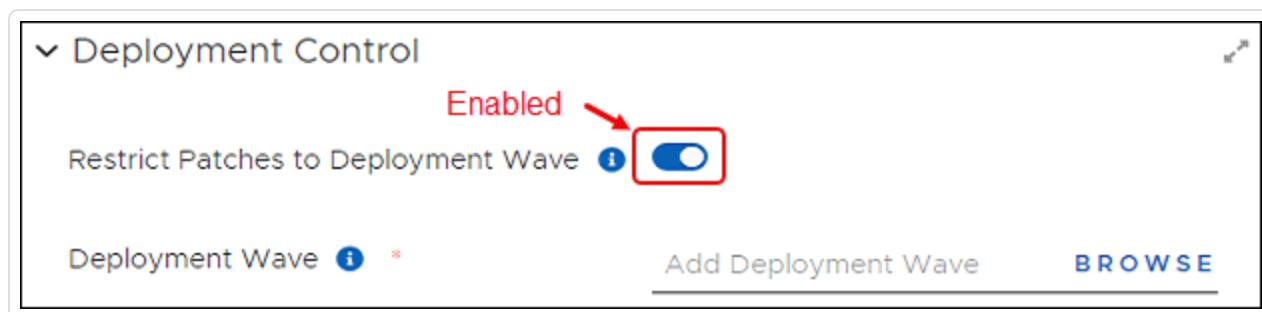


Enable Deployment Control

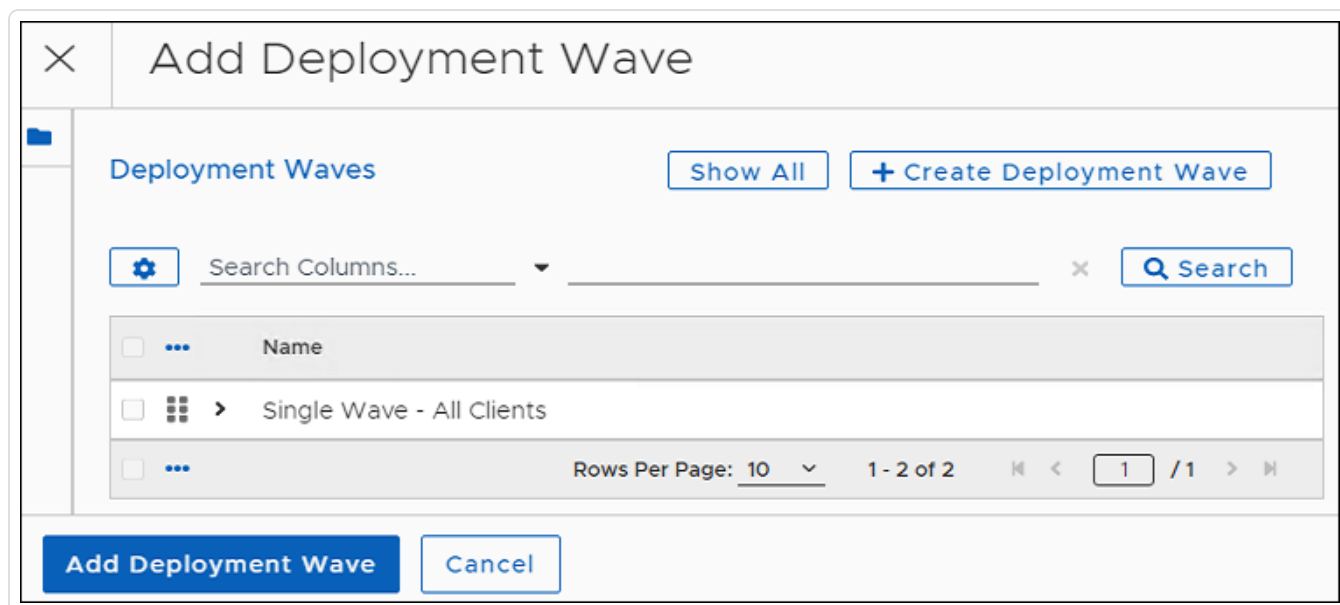
The Deployment Control setting defaults to disabled, which allows deployment of patches using this Deployment Channel to all Business Units.

To enable Deployment Control:

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



2. Select **Browse** next to Add Deployment Wave.
3. Select a **Deployment Wave**, and then click Add Deployment Wave on the bottom left of the dialog. To create a new Deployment Wave, see [Open and Save a Deployment Wave Template](#).



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

Disable Deployment Control



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

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



2. Select **Save** on the top left to save your changes:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.

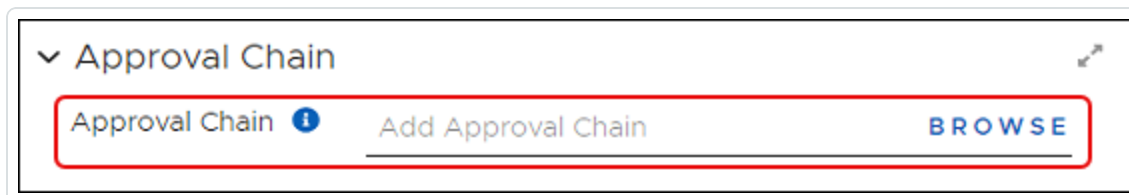
Approval Chains

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

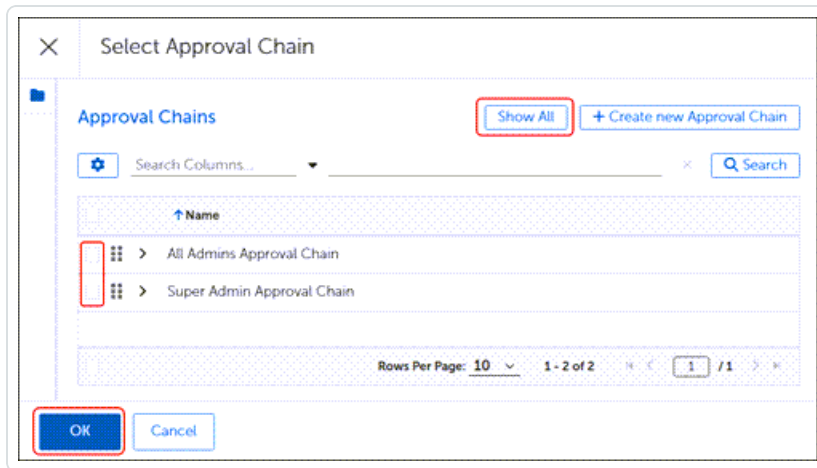
Add an Approval Chain

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

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



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



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

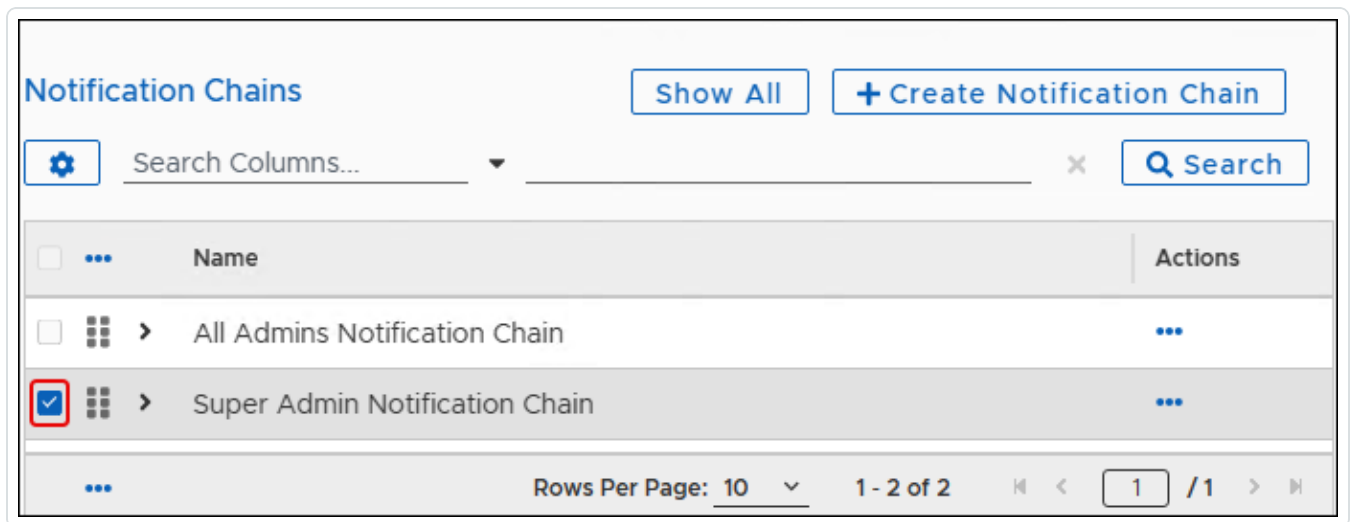
Notifications

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

Add a Notification Chain

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

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



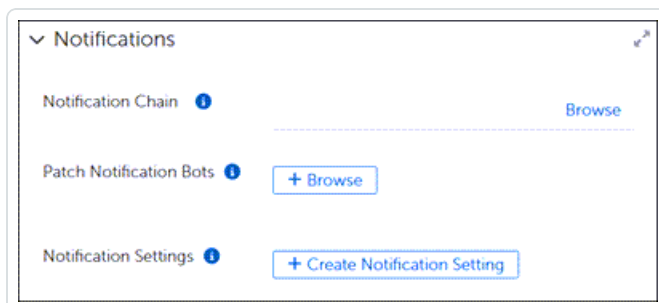
3. Select  **Notification Chains**, and then select **Show All** to see the available templates.
4. Select a **Notification Chain** from the table. To edit or create Notification Chains, see .
5. Continue editing the **Notification** settings or click OK on the bottom left corner to return to the template.

Create Notification Settings

Set Notification Urgency

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

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





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

×

Create Notification Setting

Notification Urgency ⓘ

Low ▾

Execution Schedules ⓘ

+ Add Schedules

Notify Patching Strategy Chains ⓘ

☐

Notify Business Unit Chains ⓘ

☐

Notification Cycle Workflow ⓘ

Add Workflow

BROWSE

Time Limit ⓘ

0 Hours 0 Minutes 0 Seconds

Create Notification Setting

Cancel

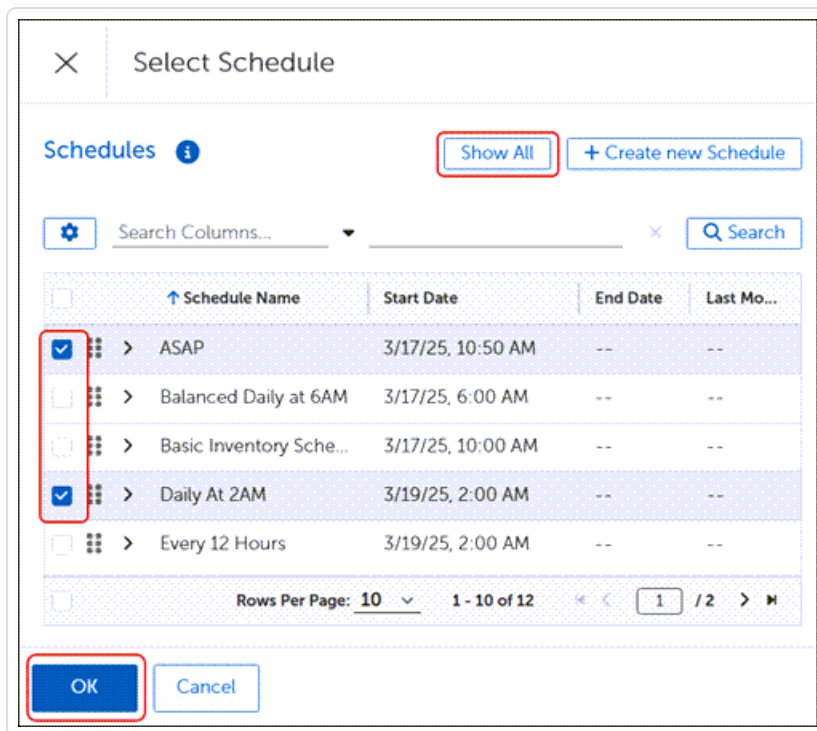
Windows.

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

Add Execution Schedules

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

1. Select **+ Create Notification Setting** from the Notifications workspace of a object template.
2. Select **+Browse** next to Execution Schedules to display the available schedules.
3. Select one or more schedules from the All Schedules table, and then select **OK** on the lower-left corner of the dialog.



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

Enable Notifications for Patching Strategy and Business Unit Chains

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

1. In the **+ Create Notification Setting** dialog in the Patching Strategy or Deployment Channel template, decide whether to enable notifications:
 - Select the **Notify Patching Strategy Chains** toggle to enable or disable (default) whether the notification cycle sends notifications to the chains included in the strategy.
 - Select the **Notify Business Unit Chains** toggle to enable or disable (default) whether the notification cycle sends notifications to Business Unit chains included in the strategy.
2. Continue editing the **Notifications** settings or click Create Notification Settings to return to the template.

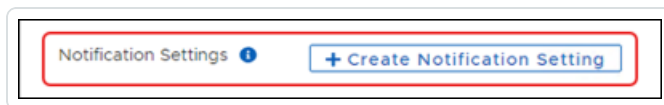
Choose a Notification Cycle Workflow



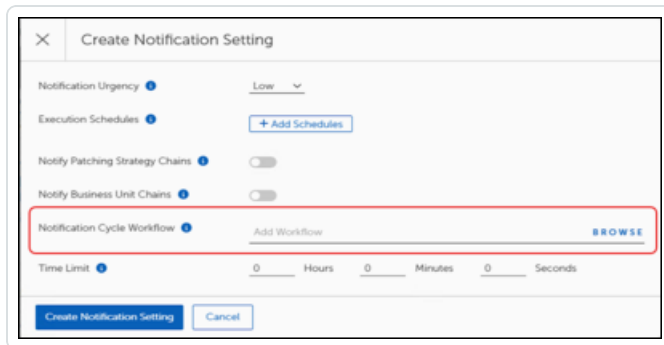
This setting names the Notification Cycle that processes the Notifications for the Patching Strategy or Deployment Channel. Notification Cycle workflows are customized for specific uses. Tenable Patch Management does not provide sample Notification Cycle templates. These templates exist only if you create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

Note: Contact Tenable Patch Management Customer Support for assistance with Notification Cycle templates

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



This opens the Create Notification Setting dialog.



2. Select **Browse** on the **Add Workflow** line. This opens the list of available workflows.
3. Select your custom workflow from the list, and then click **Add Workflow** on the lower-left corner of the dialog.
4. Continue editing the **Notification** settings or click Create Notification Settings to return to the template.

Set the Time Limit

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



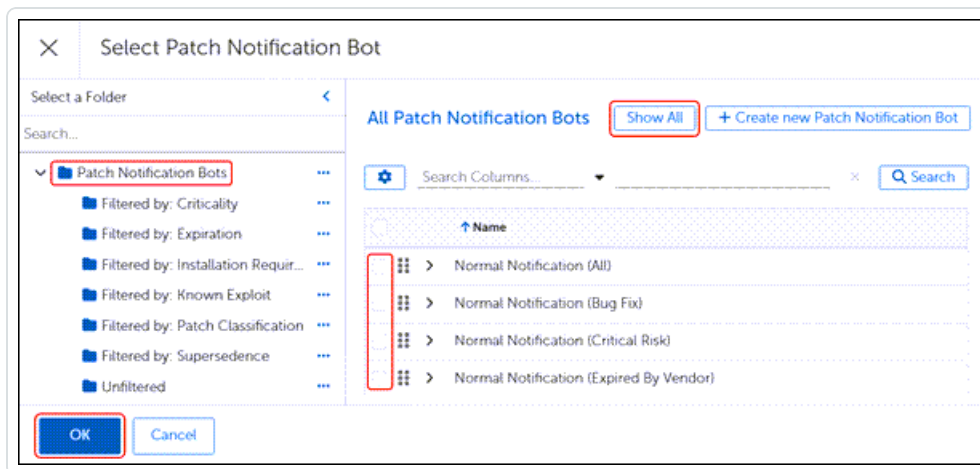
1. Select **+ Create Notification Setting** the Notification box of the object template.
2. Next to Time Limit, set the **Hours**, **Minutes**, or **Seconds** that the Notification Cycle will run, or leave the setting default at 0 for each item to allow the workflow to run indefinitely.
3. Continue editing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

Add Patch Notification Bots

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

1. Select **+ Browse** next to Patch Notification Bots in the **Notifications** workspace of the object template.

This opens the Select Patch Notification Bots dialog.



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

Create Channel Merging Rules



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

1. Select **Browse** next to **Add Deployment Channel**, and then select a **Deployment Channel**.
2. Select **+ Create Channel Merging Rule** from the Notification box of a Deployment Channel template.
3. Select **Add Deployment Channel** at the bottom left to return to the Channel Merging Rule template.
4. Set the **Merging Duration** to the number of hours, minutes, or seconds before this Deployment Channel executes.

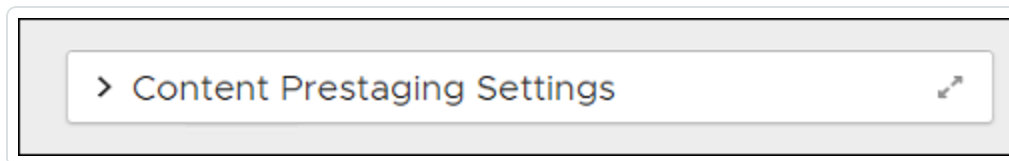
Content Prestaging Settings

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

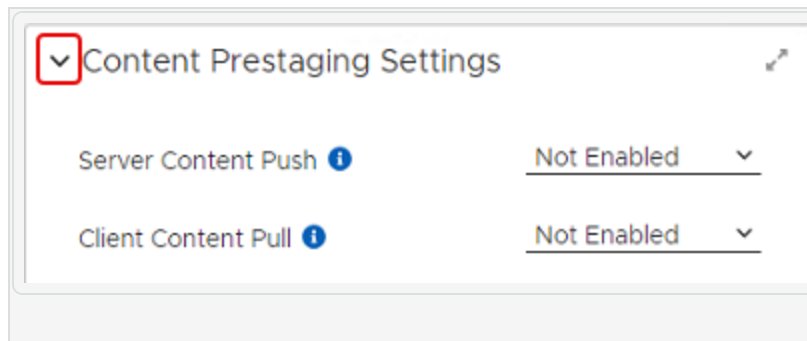
Set Content Prestaging Settings

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

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

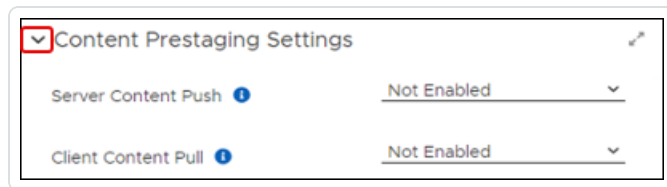


2. Expand the Content Prestaging Settings box to view the available settings.

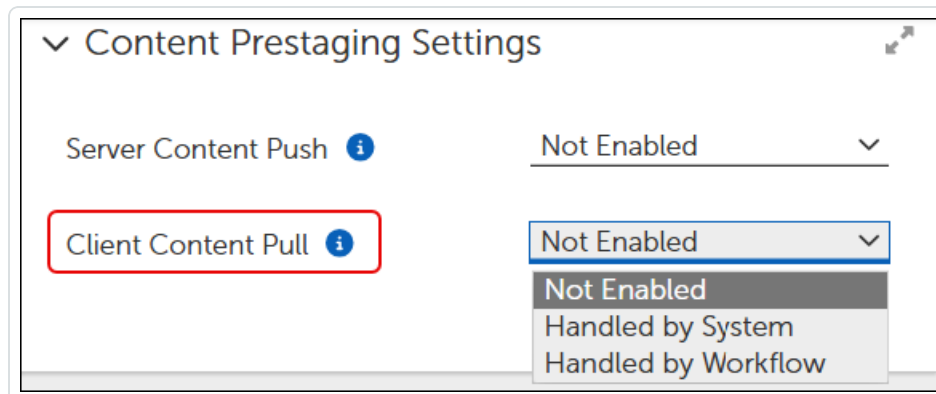


Enable Client Content Pull

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



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



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

Enable Server Content Push



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

Content Prestaging Settings

Server Content Push ⓘ Not Enabled

Client Content Pull ⓘ Not Enabled

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

Content Prestaging Settings

Server Content Push ⓘ Not Enabled

Client Content Pull ⓘ

Not Enabled

Not Enabled

Handled by System

Handled by Workflow

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

Customer Extension Data

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

Customer Extension Data ⓘ

New Key New Value

+ Add



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

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

Deployment Channel Processes

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

Creating Deployment Channel Processes

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

Integrate Tenable Vulnerability Manager

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

Minimum User Role Requirements for APIs

The Tenable API key you use or create for integration purposes inherits the same roles/permissions associated with the account you use to generate the key. The Tenable API account used for the integration requires minimum role access for either Tenable Vulnerability Manager or Tenable Security Center.

Before using a Tenable API key, make sure your account has asset export permissions as shown below. For more information, see Roles in the Tenable Vulnerability Management User Guide.



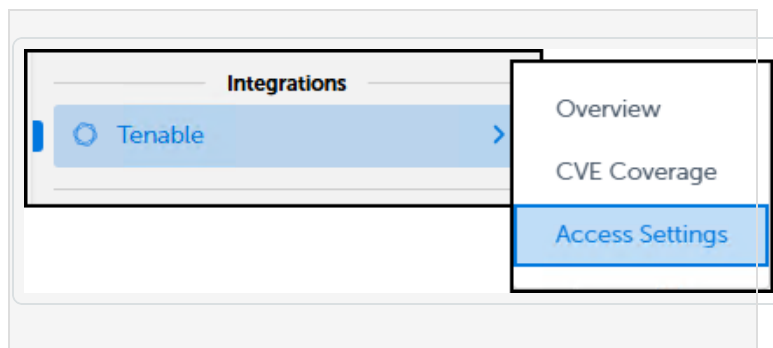
- BASIC [16] user role and **Can View** access control permissions for the All Assets object. The Administrator role does not require the **Can View** control permissions to export.
- ADMINISTRATOR [64] user role for Federal Risk and Authorization Management Program (FedRAMP) for using the GovCloud region.

For more information about roles, see [Tenable Vulnerability Manager roles](#) and [Tenable Security Center roles](#). For more information about API access, see [Tenable API Access](#).

Add Tenable Access Settings to Tenable Patch Management

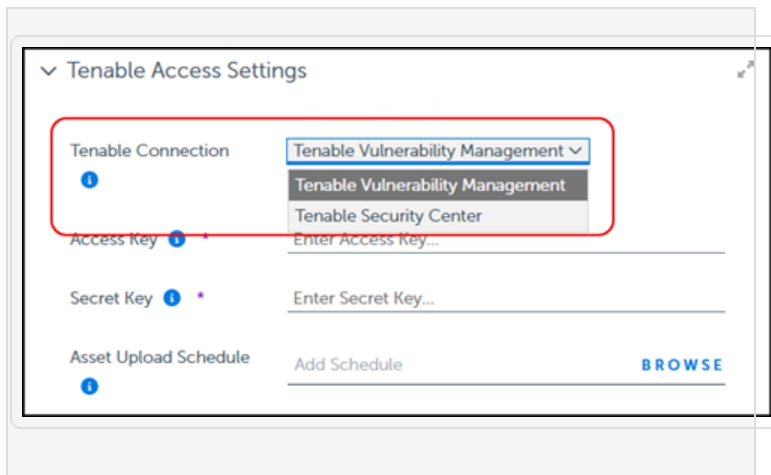
To integrate Tenable Vulnerability Management (cloud) or Tenable Security Center (server) details with Tenable Patch Management, complete the following steps:

1. Verify that the Tenable User Roles associated with your Tenable API account meet the [minimum roles and permission](#) requirements for integration and export of Tenable access objects.
2. Create **Tenable Access Keys** to use for Tenable Patch Management integration (see [Generate API Keys](#)).
3. Log on to the [Admin Portal](#) and open the [Patch Dashboard](#).
4. Select **Tenable** in the left navigation menu of the dashboard, and then select **Access Settings**



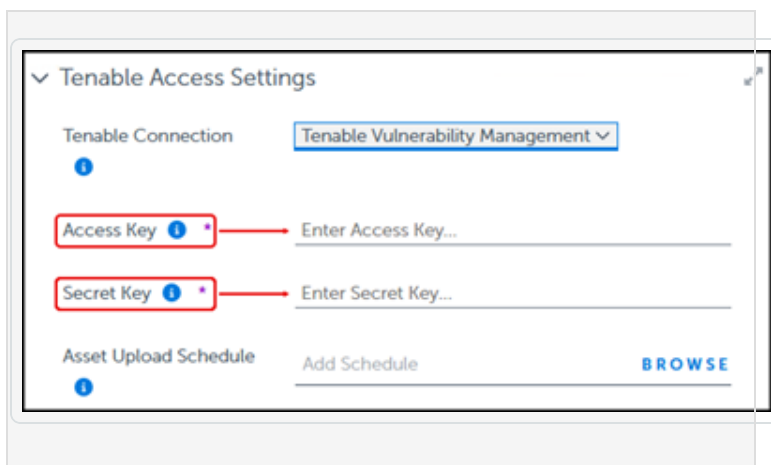
5. Select the Tenable Connection you want to create:
 - Select **Tenable Vulnerability Management**, and then see [Configure Tenable Vulnerability Management Settings](#).

- Select **Tenable Security Center**, and then see [Configure Tenable Security Center Settings](#).

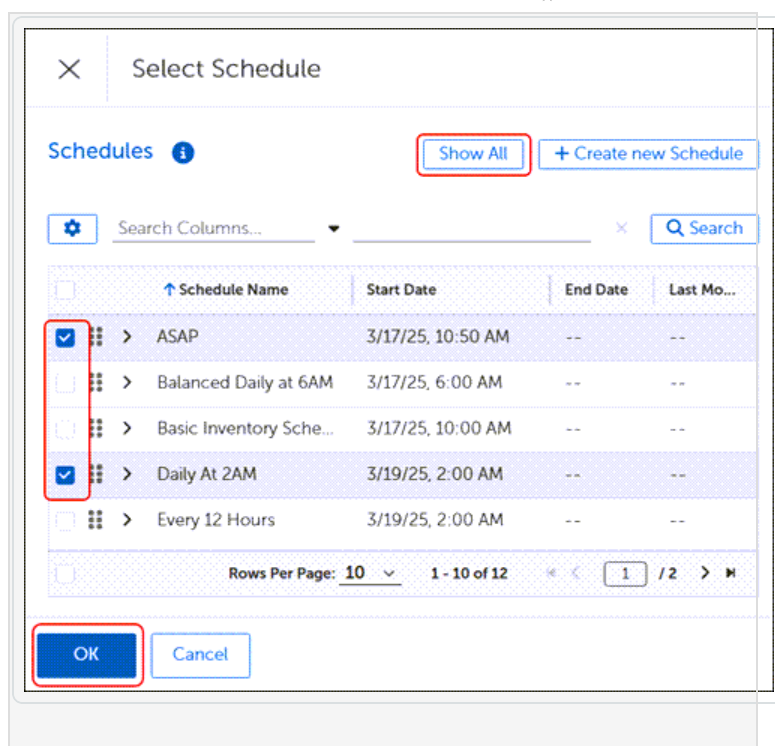


Configure Tenable Vulnerability Management Settings

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



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



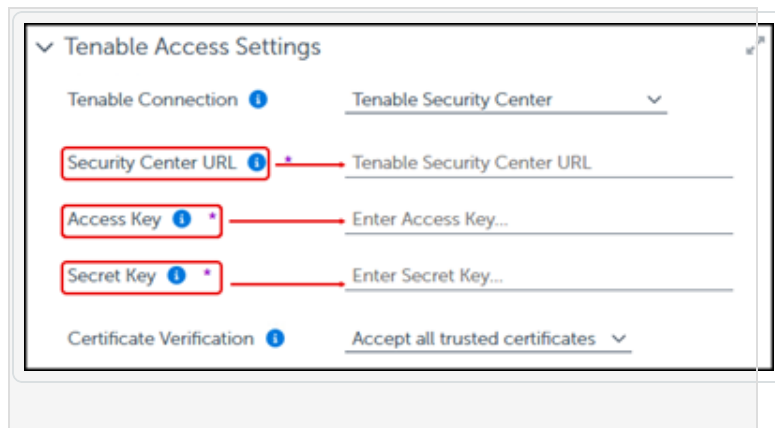
3. Select Save on the upper-left corner of the dialog:

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

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

Configure Tenable Security Center Settings

- Enter the **Security Center URL** (the host domain for the on-premise Tenable Security Center instance).



▼ Tenable Access Settings

Tenable Connection ⓘ Tenable Security Center ▼

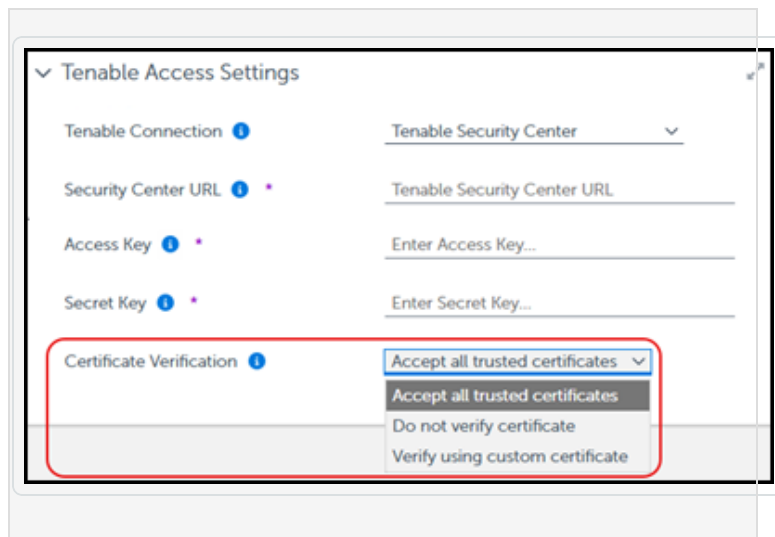
Security Center URL ⓘ * Tenable Security Center URL

Access Key ⓘ * Enter Access Key...

Secret Key ⓘ * Enter Secret Key...

Certificate Verification ⓘ Accept all trusted certificates ▼

2. Enter the **Access Key** and the **Secret Key** for Tenable Security Center.
3. Select a Certificate Verification to use for Tenable Security Center APIs:
 - Accept all trusted certificates
 - Do not verify certificate
 - Verify using custom certificate



▼ Tenable Access Settings

Tenable Connection ⓘ Tenable Security Center ▼

Security Center URL ⓘ * Tenable Security Center URL

Access Key ⓘ * Enter Access Key...

Secret Key ⓘ * Enter Secret Key...

Certificate Verification ⓘ Accept all trusted certificates ▼

Accept all trusted certificates

Do not verify certificate

Verify using custom certificate

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

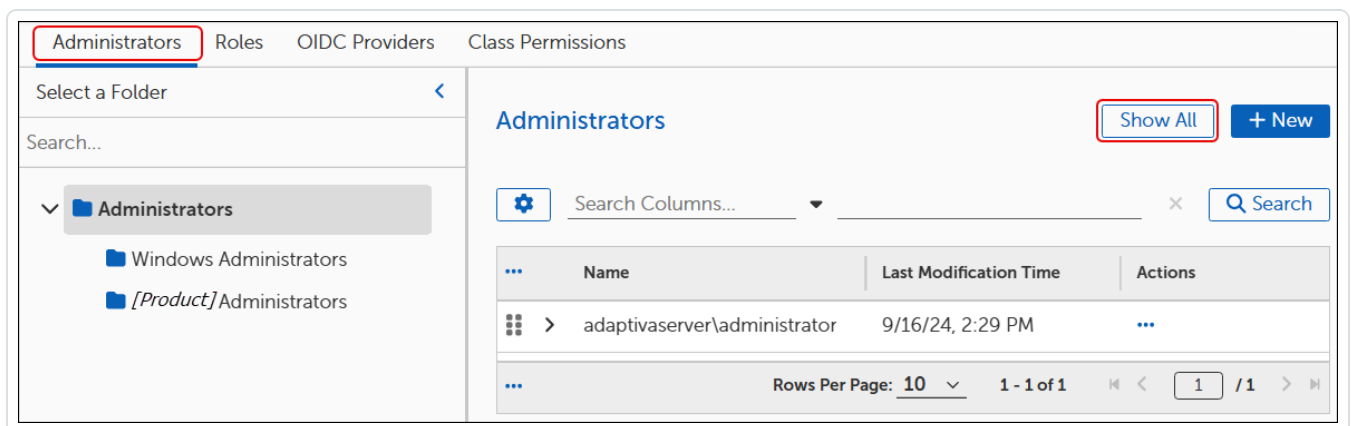


Administrators and Roles

View, create, or modify Administrators and Roles.

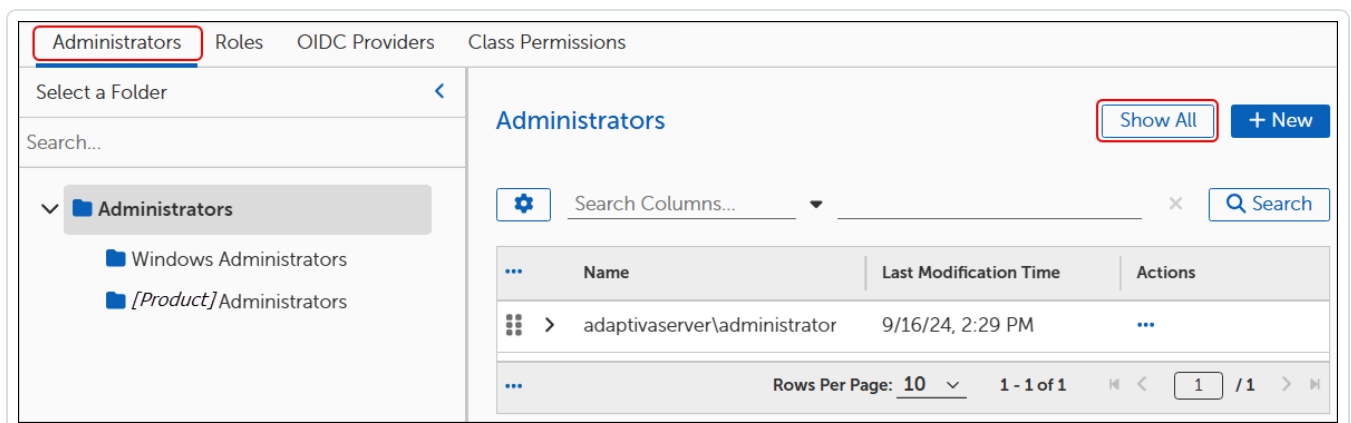
Access Security Settings

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



View Administrators

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

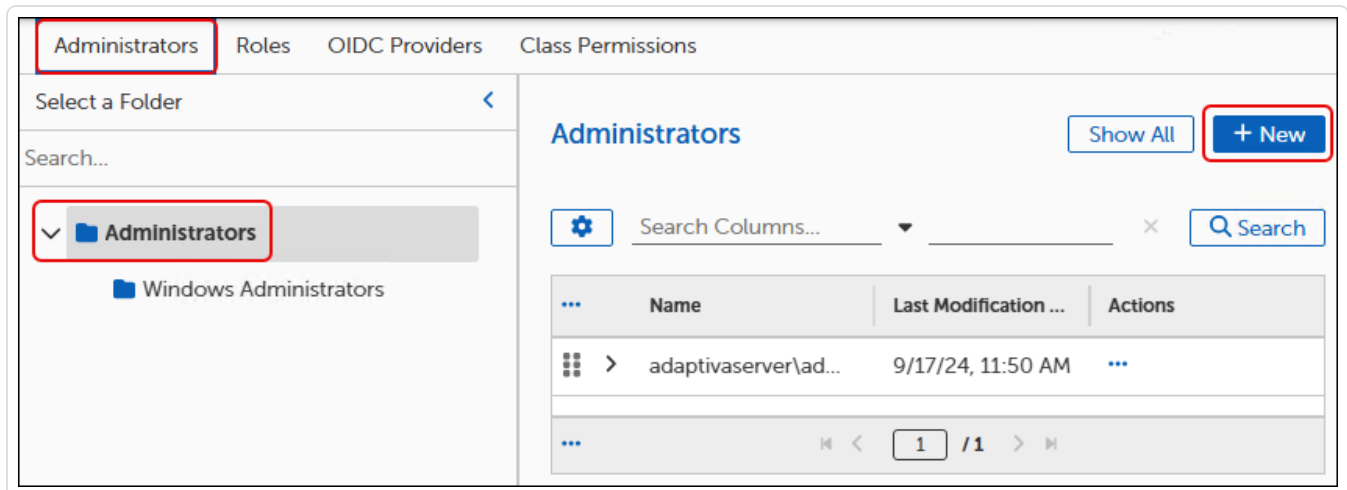


2. Select **Show All** to list all Administrators in the selected folder.

Create a New Administrator



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



2. Enter the **Administrator Details**:

- a. Select the **Admin Type** login from the list. Tenable Patch Management recommends using Windows Active Directory.
- b. Enter the email address and login details for the new administrator.

3. Enter the **User Details**:

- a. Add the **Name** and contact details for the new administrator.
- b. Choose country codes from the drop-down lists for phone numbers.

The screenshot shows the 'User Details' form. It contains fields for First Name, Last Name, Voice Phone Number, After Office Phone Number, Text Message Phone Number, WhatsApp Phone Number, and Teams Webhook URL. Each field has a dropdown menu for selecting a country code.

Field	Country Code
First Name	
Last Name	
Voice Phone Number	Phone Number
After Office Phone Number	After Office Phone Number
Text Message Phone Number	SMS Phone Number
WhatsApp Phone Number	WhatsApp Phone Number
Teams Webhook URL	Teams Webhook URL



- c. Add a **Teams Webhook URL**. If you need to create a Microsoft Teams Webhook URL see [Create a Microsoft Teams Webhook URL](#).

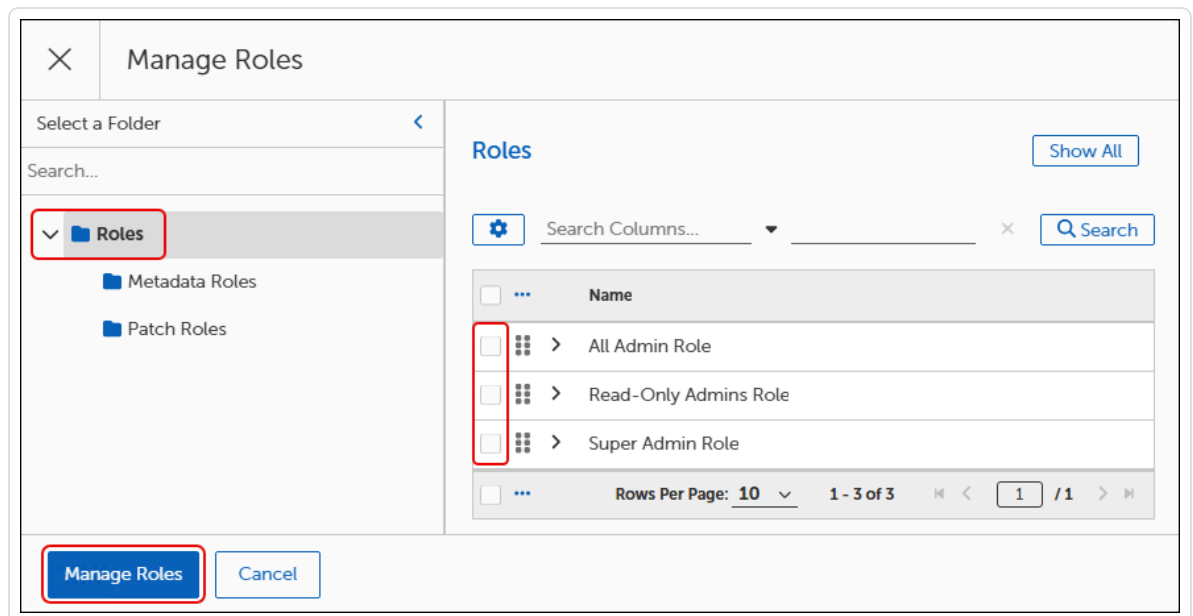
4. Assign **Direct Roles**:

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



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

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



- To create additional roles, see [Create a New Role](#).

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

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



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

Create a Microsoft Teams Webhook URL

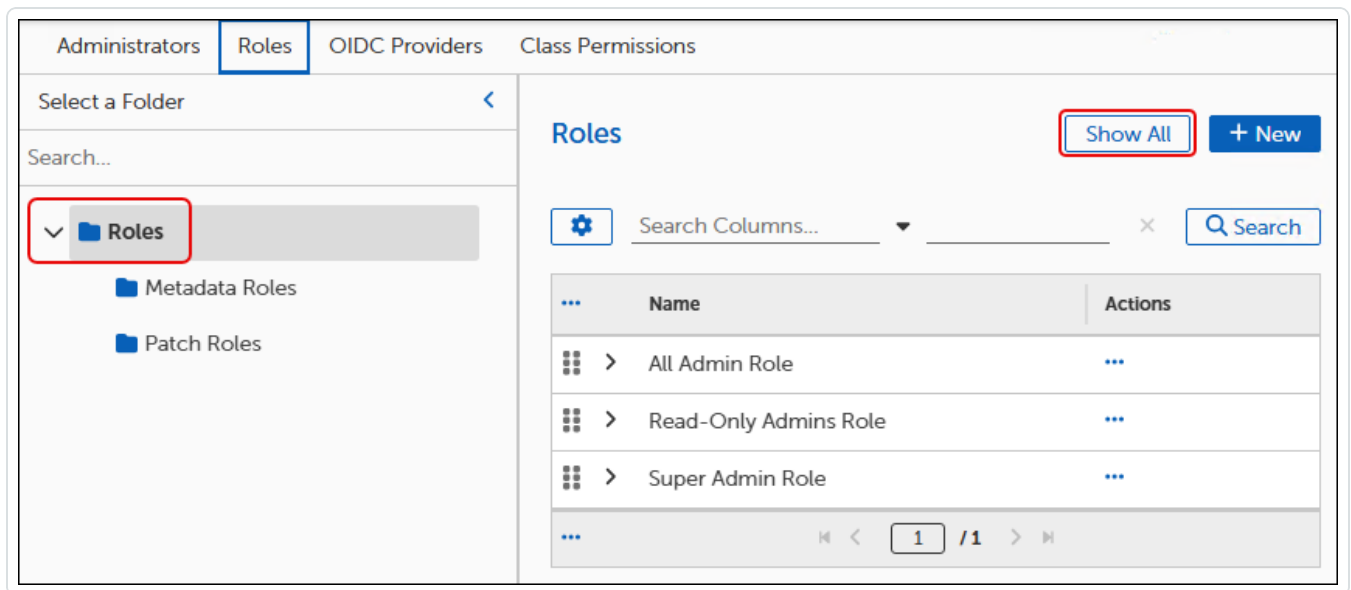
When adding a new administrator or modifying administrator details in Tenable Patch Management , add a Teams Webhook URL to post notices to a Teams channel, and then assign that URL to your administrators in Tenable Patch Management . Administrators can check the Teams channel for patch notifications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

1. Go to Microsoft.com for instructions on creating a Team and a Channel. The links below go to a third-party website outside of the Tenable Patch Management domain:
 - a. Go to [Microsoft Windows Team and Channel topics](#) to set up a new channel in an existing Team in Microsoft Teams, or create a new Team and add a channel for patch notification purposes.
 - b. Go to [Create an Incoming Webhook](#) to create the Webhook URL.
2. Open the **Admin Portal**, and then navigate to **Settings > Security > Administrators**.
3. Open an existing administrator or select **+NEW** to create a new Administrator.
4. Scroll down to **Teams Webhook URL** under User Details, and then paste the URL you generated in Step 1b into the associated text box.
5. Return to [Create a New Administrator](#) to complete any other administrator details.

View Roles



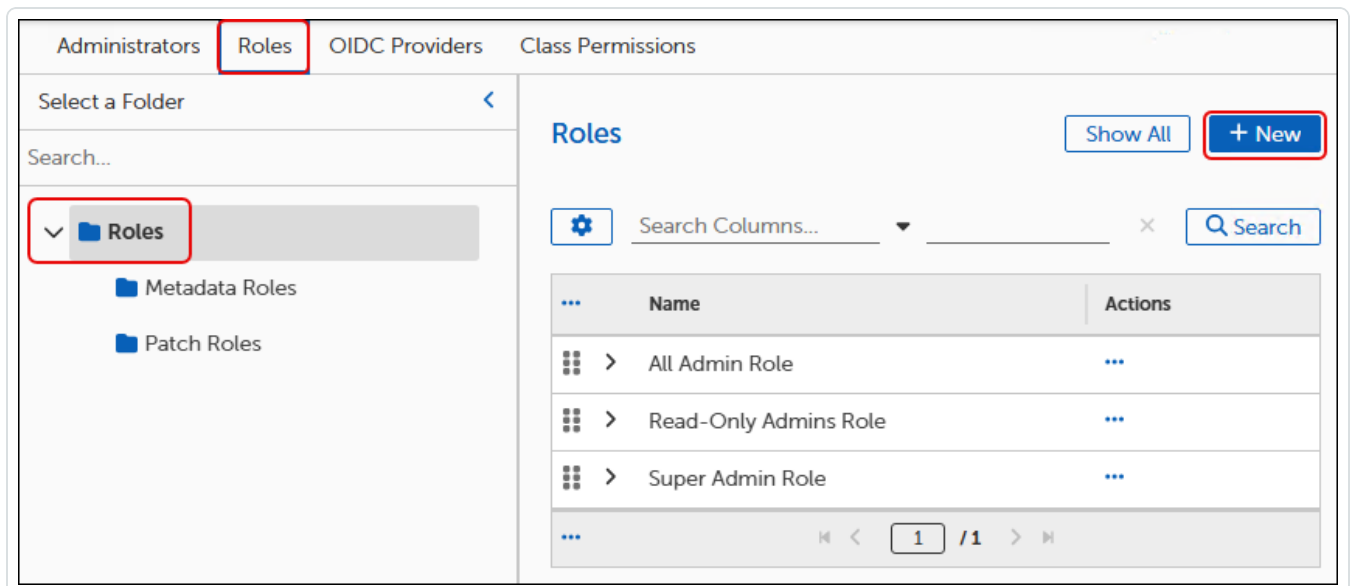
1. Select a **Roles** folder from the Roles tab of [Access Security Settings](#).



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

Create a New Role

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



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



▼ Role Properties

Role Name

Role Name

Role Description

Role Description

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

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

▼ Role Membership

Direct Administrators

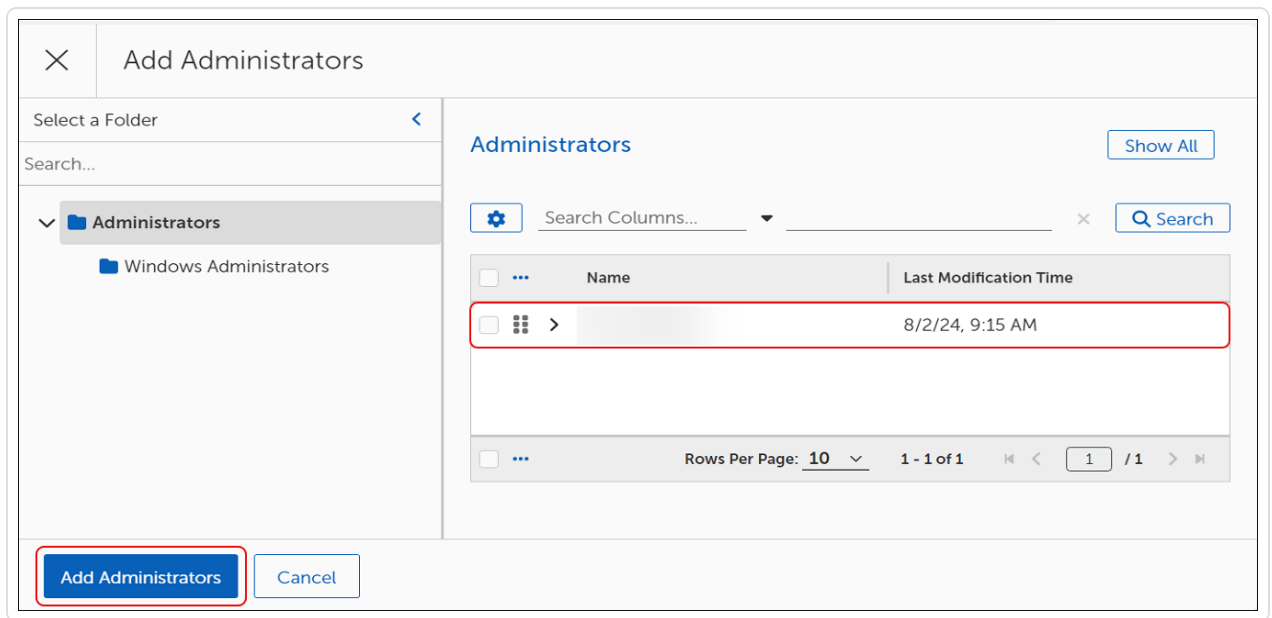
+ Add Administrators

Active Directory Groups

+ Add AD Group

No data provided

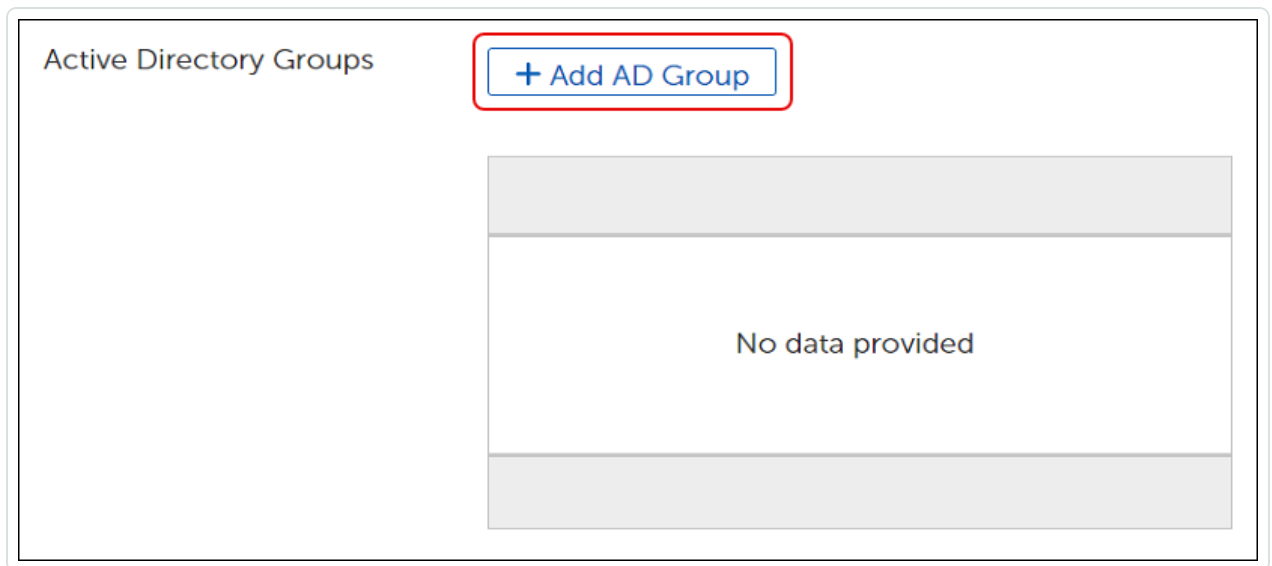
- Select one or more administrators from the table for the new role.



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

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

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



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

×

Active Directory Group

Domain Name

Group Name

Check Group

No data provided

Add AD Group Cancel

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

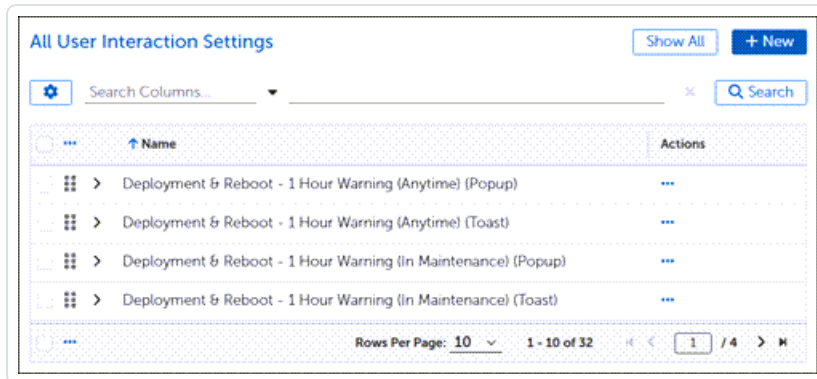
User Interaction Settings

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



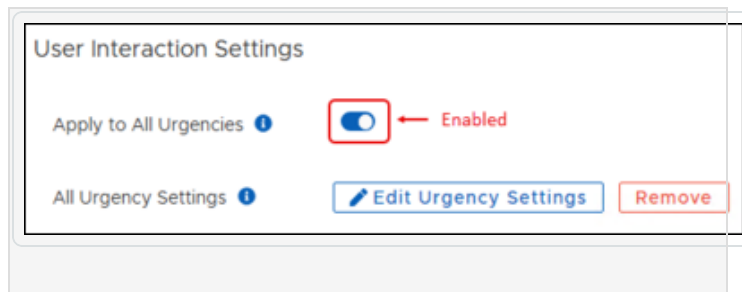
1. Select  **User Interaction Settings** in the left navigation menu of the [Patch Dashboard](#), and then select **Show All**.



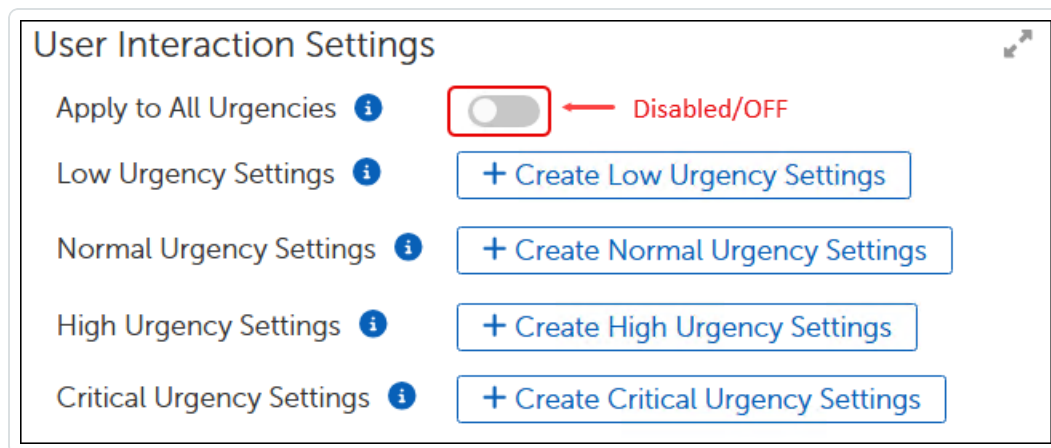
2. Select the Name of an existing template to open it. This example uses the Deployment & Reboot - 1 Hour Warning (Anytime)(Toast) template.
3. Save the template with a new name:
 - a. Select **More** in the upper-left corner of the dialog, and then select **Save As**.
 - b. Enter a new name for the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

Choose Urgency Settings

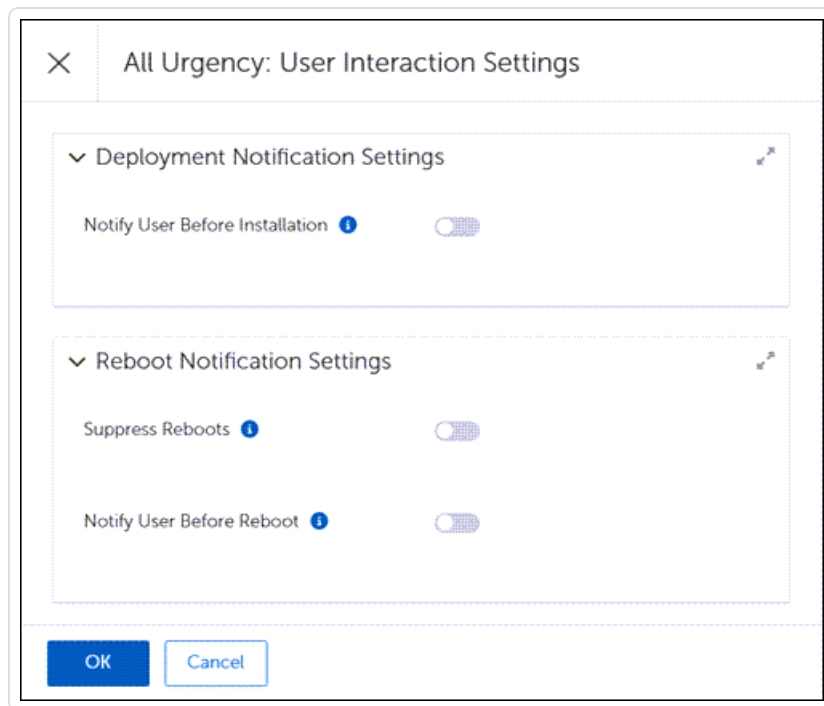
1. Scroll down to User Interaction Settings in an [open User Interaction Settings](#) template:
 - When working from an existing template, these settings reflect the needs of the template you chose to modify. With Apply to All Urgencies enabled, you have the option to create a single set of urgency settings 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.



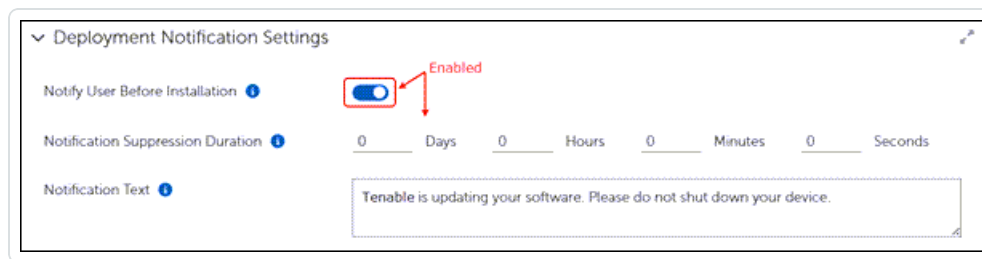
2. Select the **Apply to All Urgencies** toggle to enable or disable setting urgencies for all levels:
 - Each setting, including Apply to All Urgencies, uses the same template layout and fields.
 - This example uses the Apply to All Urgencies setting. The example below shows all settings disabled.



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.

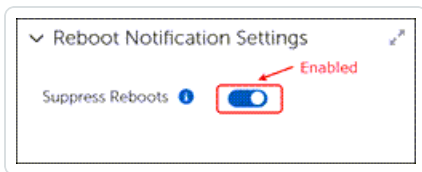


3. Enter **Notification Text** in the text box. The user sees this text when the notification arrives on their device.
4. Next, see [Reboot Notification Settings](#).

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.



▼ Reboot Notification Settings

Suppress Reboots ☐ ← Disabled

Notify User Before Reboot ☒ ← Enabled

Notification Title Reboot Notification

Notification Text System reboot required

Prevent Notification Dismissal ☐

Perform Reboot Only During Maintenance Window ☐

Reboot Deadline 0 Days 0 Hours 0 Minutes 0 Seconds

OK Cancel

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, Tenable Patch Management provides no warning to the user.

4. [Configure snooze settings.](#)

Managing Snooze Settings

When defining User Interaction Settings, Tenable Patch Management 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.

Allow Snooze ⓘ	☒ ← Enabled							
Maximum Snooze Duration ⓘ	0	Days	8	Hours	0	Minutes	0	Seconds
Snooze Reminder ⓘ	0	Days	6	Hours	0	Minutes	0	Seconds
Snooze Durations ⓘ	0	Days	0	Hours	0	Minutes	0	Seconds
+ Add								

- 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).

Snooze Durations 1								
0	Days	4	Hours	0	Minutes	0	Seconds	X
0	Days	2	Hours	0	Minutes	0	Seconds	X
0	Days	1	Hours	0	Minutes	0	Seconds	X
0	Days	0	Hours	15	Minutes	0	Seconds	X
0	Days	0	Hours	0	Minutes	0	Seconds	
+ Add								

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

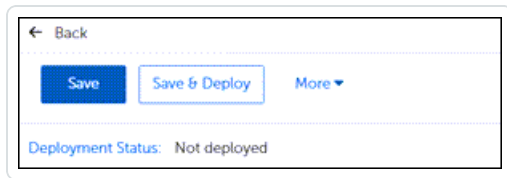
After creating and configuring or editing User Interaction Settings, you must deploy them. Otherwise, the User Interaction Settings are not available in the list of templates when you add **User Interaction Settings** to a Business Unit.

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.

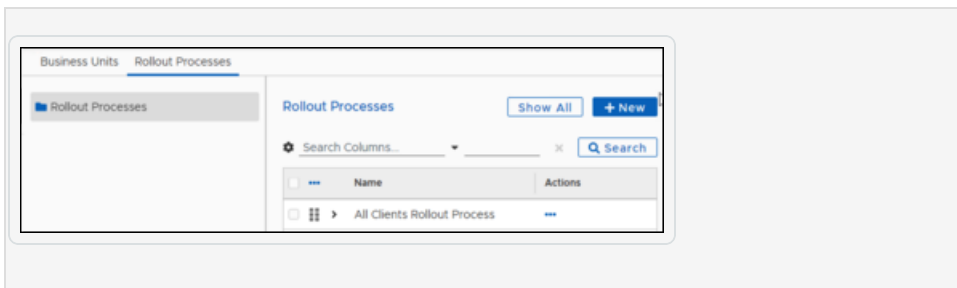


Rollout Processes

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

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

Before creating a custom Rollout Processes, enter a support ticket and request help from



Including Rollouts in Business Units

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

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

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



Business Units and Rollout Processes

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

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

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

Creating a Patching Strategy

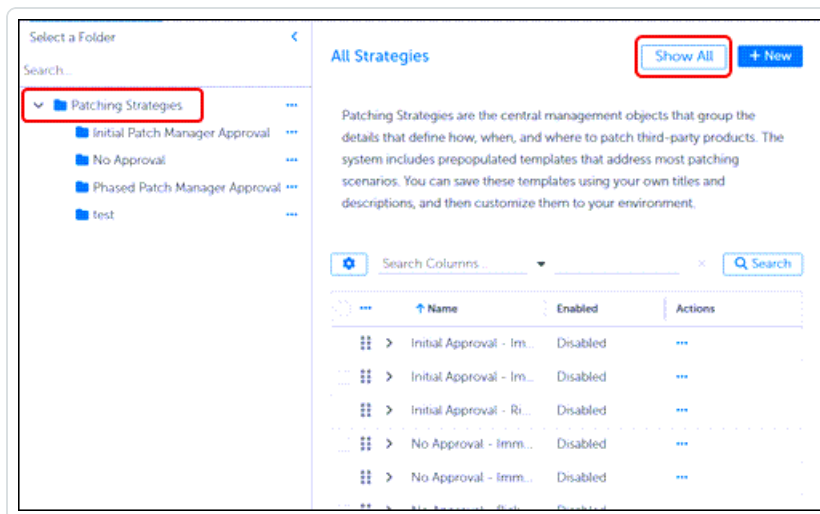
A Patching Strategy template contains specific fields that you can configure to make a unique Patching Strategy for your environment. Tenable Patch Management recommends opening an existing strategy that contains most of the configuration items you want, and then saving it with a new name and description.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

Open and Save a Patching Strategy Template

1. Follow the instructions in [Create a New Folder for Objects](#).
2. Hover over or click **Strategy** in the left navigation menu of the [Patch Management Dashboard](#), and then select **Patching Strategies**.



3. Select **Patching Strategies**, and then select **Show All** to see all available Patching Strategies.



For descriptions of each template type, see [Patching Strategy Templates](#).

4. Select the **Name** of a strategy to open it.
5. Select **More** in the upper left corner of the template, and then select **Save As**:
 - a. Enter a unique name that reflects what the strategy does conceptually. For example, ITS Immediate Daily Product Patching.
 - b. Select **Save as** on the bottom left corner of the dialog. This opens your strategy template with all the default entries for the built-in strategy, including a detailed description.
 - c. Enter a detailed **Description** of your new template or keep the existing detail, and then click **Save** on the upper-left corner of the dialog.

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

Managing Software Product Selections

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

For more information about the products available with Tenable Patch Management, see [Software Products](#).



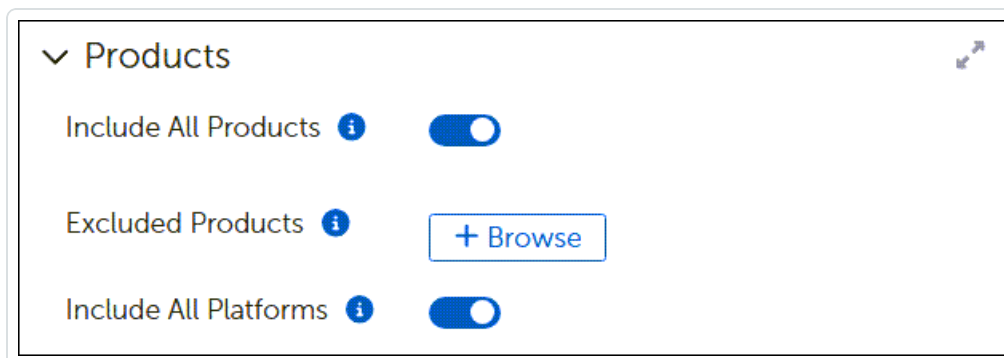
Include All Software Products

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



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

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



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

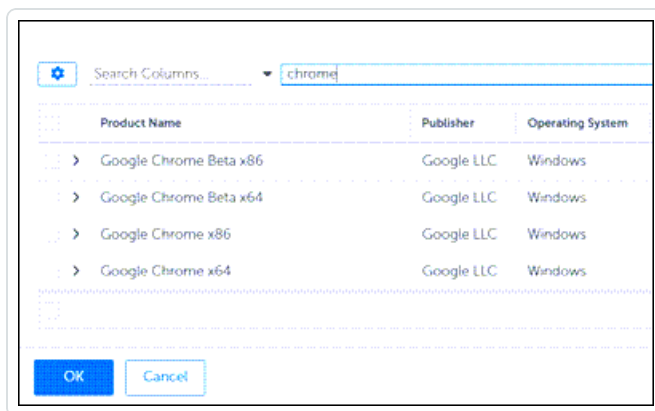
Include Specific Software Products



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



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



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

Exclude Products from a Patching Strategy

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



Products

Include All Products

Excluded Products

+ Browse

Include All Platforms

Note: When you add Business Units to a Strategy, the [Patching Exceptions](#) set for the Business Unit take precedence over the Product settings in the Patching Strategy.

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

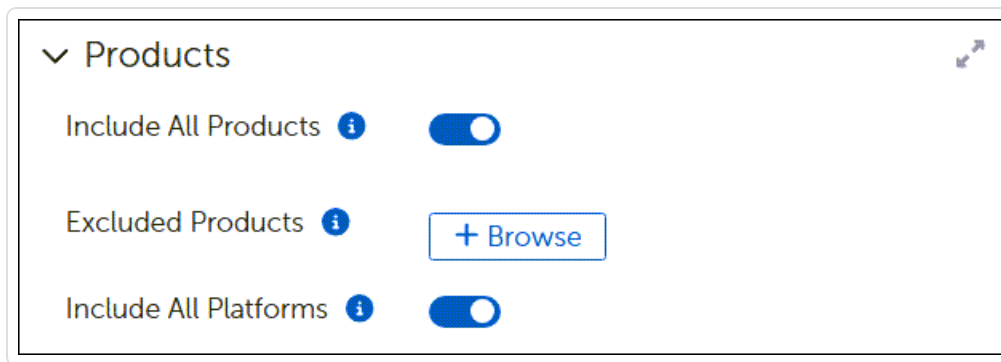
2. Select **Save** on the upper left of the strategy to keep your changes:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.

Include or Exclude Platforms in a Patching Strategy

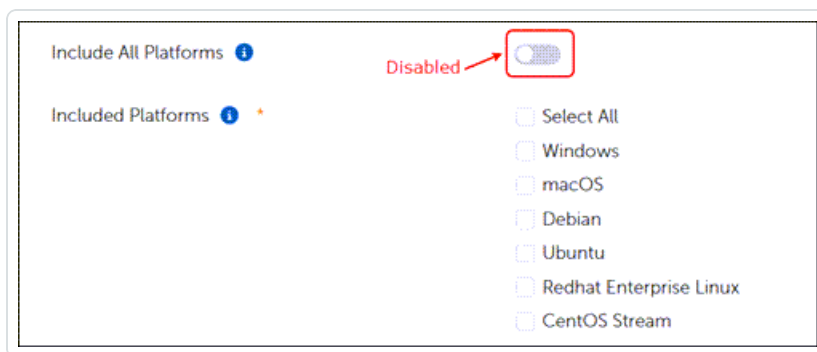
When you enable Include All Products from the Products workspace in an open Patching Strategy, you also include all platforms by default.



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



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



3. Decide which platforms to include:
 - To include all Platforms, either **Select All** or select the **Include All Platforms** toggle to enable it.
 - To include specific Platforms, select those you want to include.
4. Select **Save** on the upper left corner to keep your changes:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.

Manage Trigger Metadata Properties

Tenable Patch Management provides several Trigger Metadata Properties..

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



The changed patch must:

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

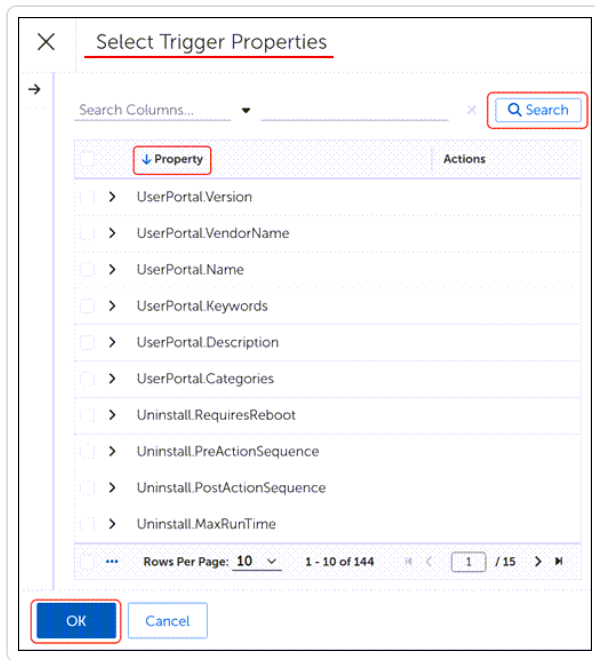
View All Trigger Metadata Properties

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

Select from all Trigger Properties

The first table you see shows all available trigger properties.

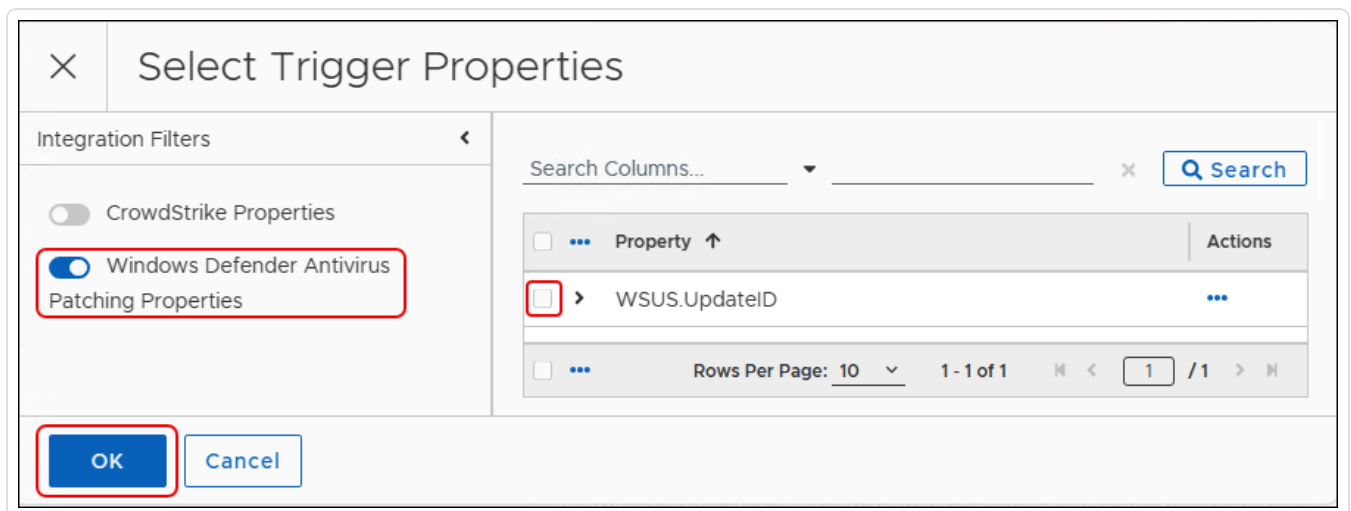
1. In the **Select Trigger Properties** table of the **Trigger Metadata Properties** dialog, select one or more properties to use as triggers:
 - To find a specific trigger, enter a trigger name on the **Search** line, and then select **Search**.
 - To sort the list of Trigger Properties, click **Property**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



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

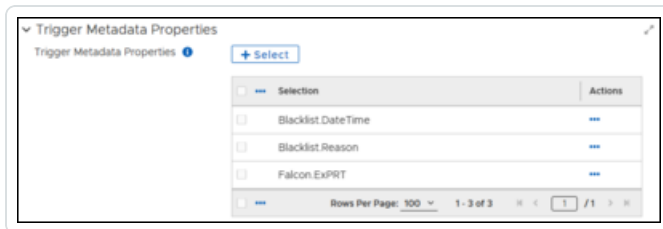
Select Only Windows Defender Antivirus Trigger Properties

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





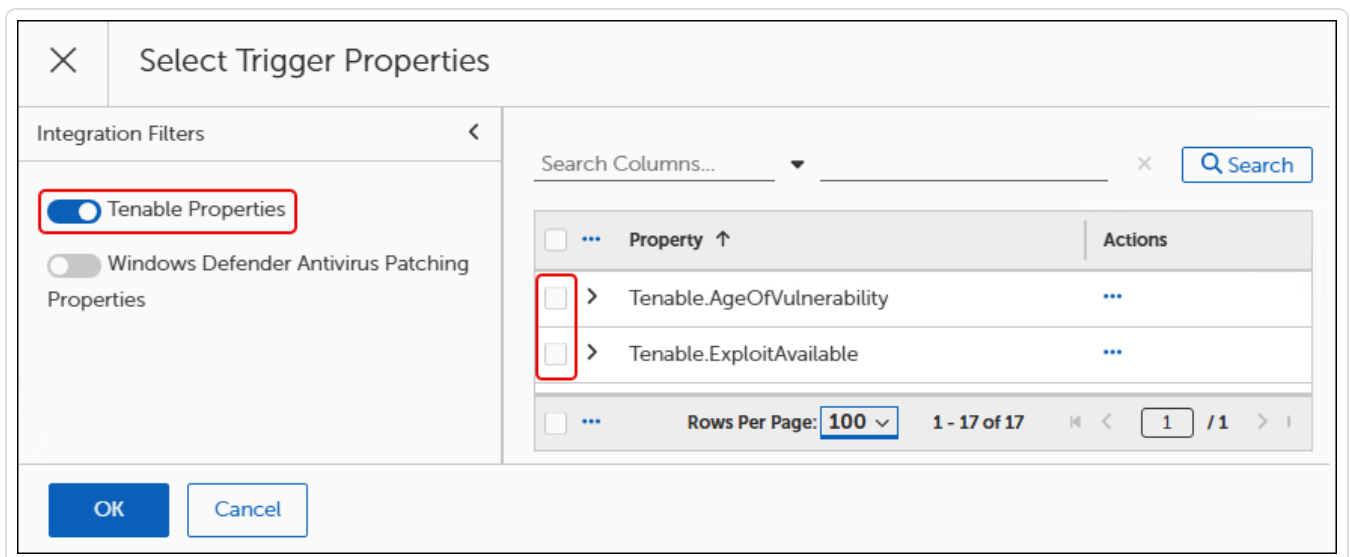
3. Select **OK** at the bottom left of the dialog to save your selections and return to the Patching Strategy template.



Select Only Tenable Trigger Properties

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

1. Select the **Tenable Properties** toggle to enable or disable (default) Tenable trigger properties.
2. Select one or more **Tenable** properties from Properties column of the table.

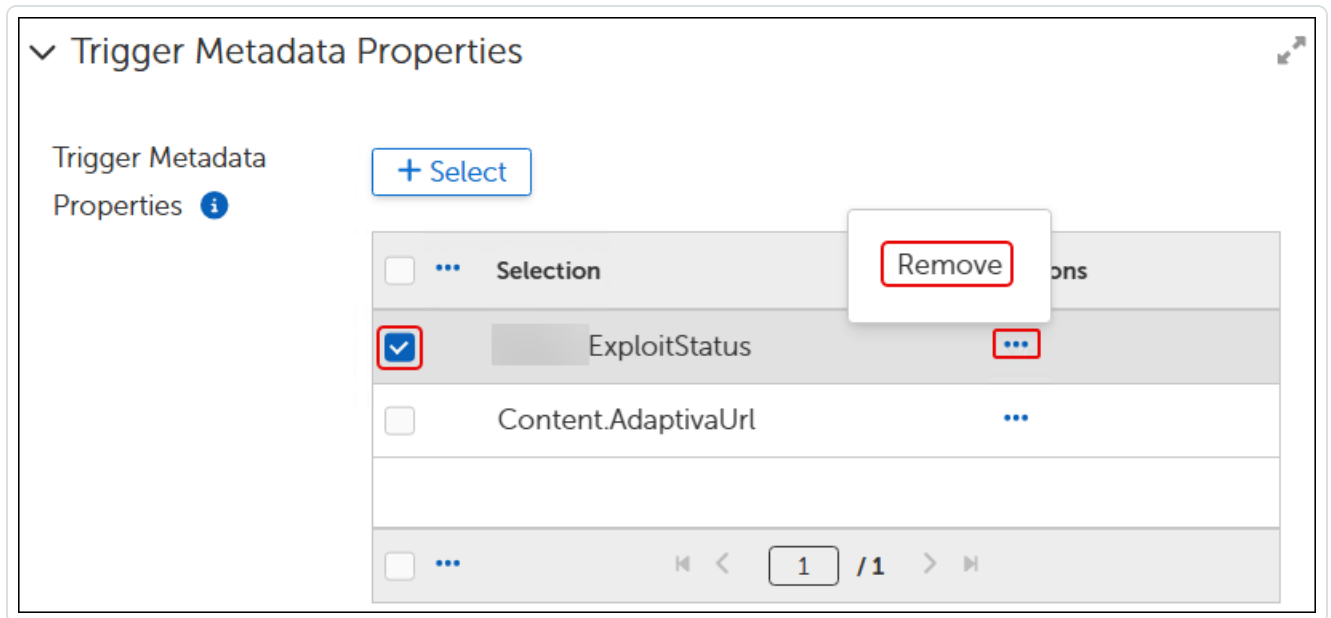


3. Select **OK** on the bottom-left corner of the dialog to save your selections and return to the Patching Strategy template.

Remove Trigger Metadata Properties



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



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

Deployment Settings

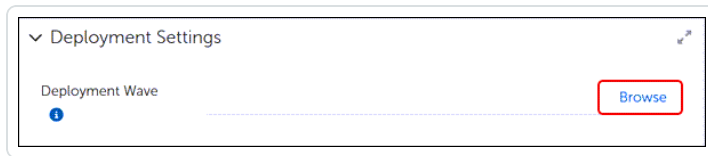
Deployment settings in a Patching Strategy include choosing a Deployment Wave, Creating a Deployment Bot Runtime configuration, and choosing whether to present each patch to the first matching Deployment bot only (defaults to disabled). When [customizing an existing Patching Strategy](#) (recommended),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

Begin by [adding a Deployment Wave](#).

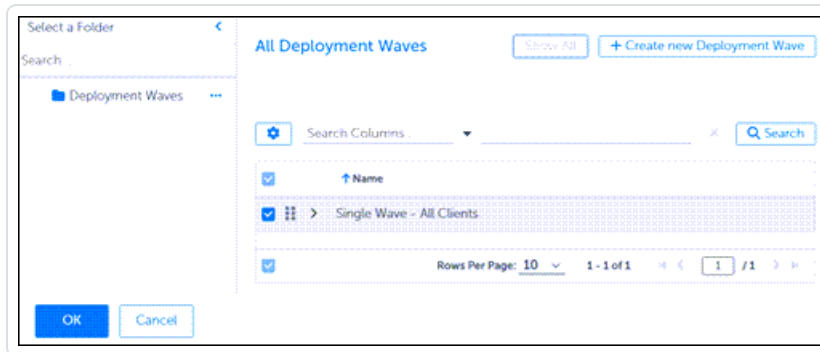
Add a Deployment Wave



1. Select **Browse** next to Deployment Wave in the Deployment Settings workspace of an open [Patching Strategy](#) template.



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



2. Select a **Deployment Wave** from the list.
 - Tenable Patch Management provides a **Single Wave-All Clients** Deployment Wave, which includes a Business Unit called **All Clients Business Unit**.
 - If you are following the tasks in **Introduction to Patching Strategies**, choose **Single Wave-All Clients**.
3. Select **OK** on the bottom left of the dialog to return to the Patching Strategy.

Note: When updating an existing Patching Strategy with a new Deployment Wave, the system prompts you with a recommendation to specify Business Unit Addition Settings.

4. Select **OK** to close the recommendation. The system returns you to the Patching Strategy at the Business Unit Addition Settings workspace:
 - If you are following the tasks in **Introduction to Patching Strategies**, skip to [Add Software Products](#). There is no need to modify the Deployment Bot Runtime settings for purposes of this exercise.



- If you are creating or modifying a Patching Strategy for ongoing use, continue with the next step.
5. Choose whether to specify Business Unit Addition Settings (recommended), if prompted by the system.
- To continue with Deployment Settings, see [Deployment Bot Runtime Settings](#). You may configure Business Unit Addition Settings later in the template.
 - To complete Business Unit Addition Settings now, see [Business Unit Addition Settings](#).

Deployment Bot Runtime Settings

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

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

See also:

[Bots - Patch Deployment and Notification Bots](#)

[Patching Processes](#)

[Deployment Channels and Deployment Channel Processes](#)

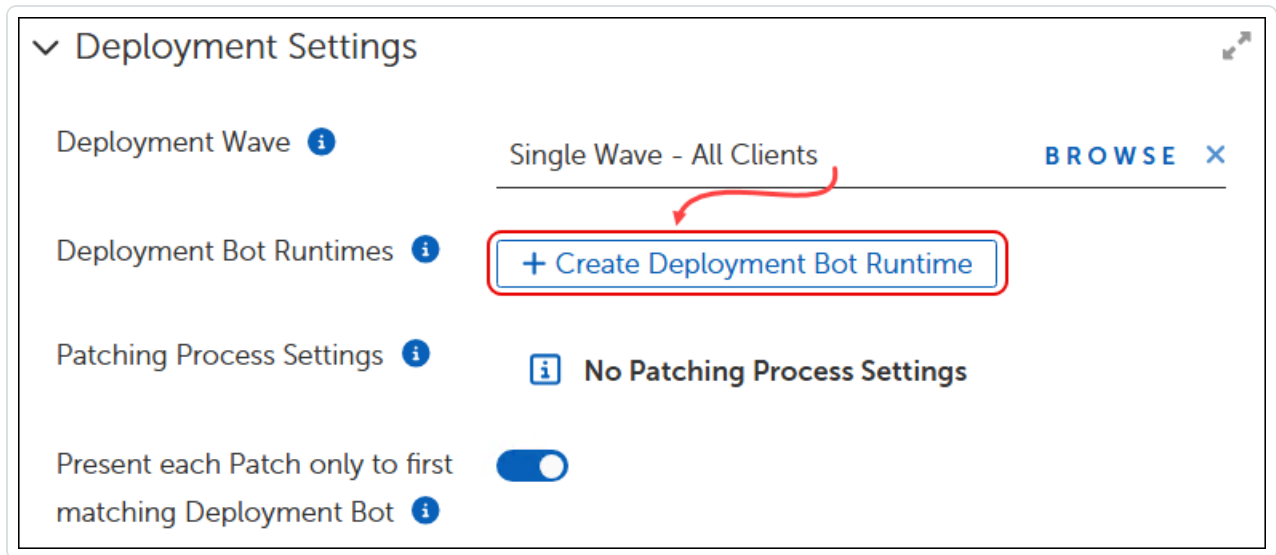
[Business Units and Rollout Processes](#)

Create Deployment Bot Runtime Scenarios

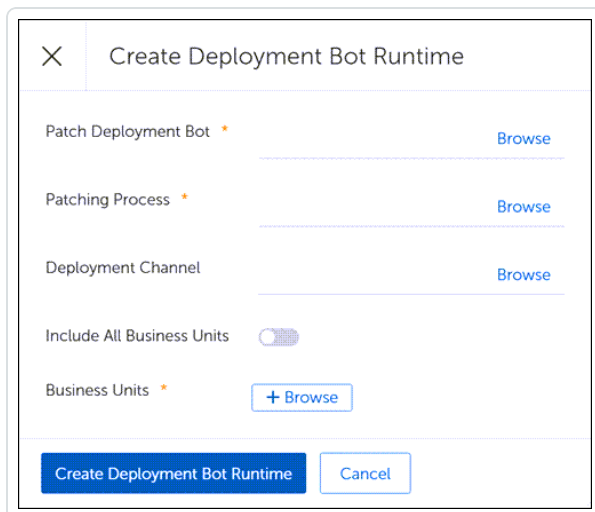
Before creating a Deployment Bot Runtime, [select a Deployment Wave](#) to enable the Create Deployment Bot Runtime selection.



1. Select **+ Create Deployment Bot Runtime** from the Deployment Settings workspace of an open [Patching Strategy](#) template.



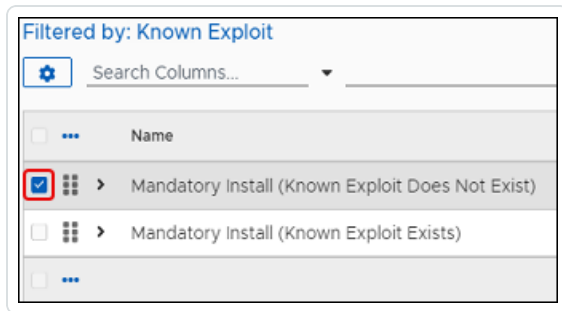
This opens the Create Deployment Bot Runtime dialog:



2. Begin by [adding a Patch Deployment Bot](#).

Add a Patch Deployment Bot (Required)

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

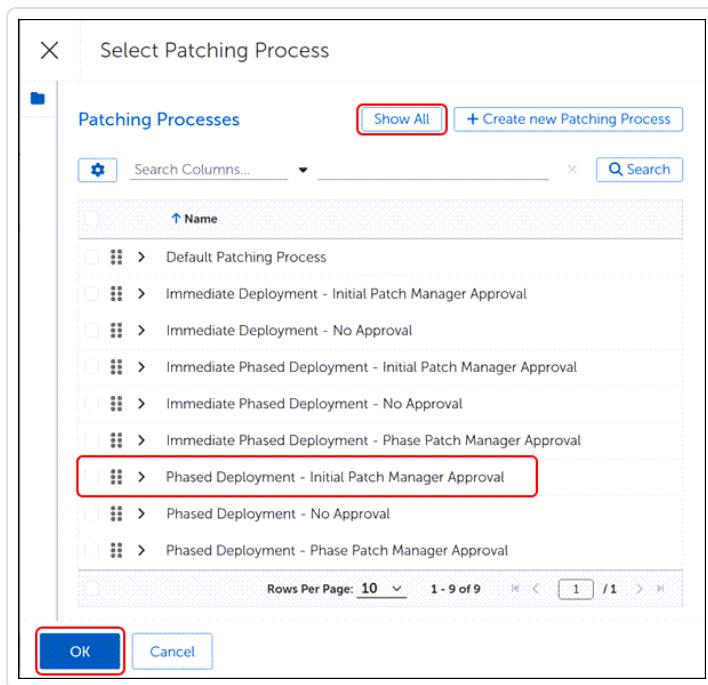


- Select  **Patch Deployment Bots**, and then select **Show All** to see the available choices.
 - Select a **Filtered by:** setting beneath  **Patch Deployment Bots** to see only the items associated with that filter.
3. Select the template you want to use. For example, in **Filtered by: Known Exploit**, select **Mandatory Install (Known Exploit Exists)**.
 4. Select **OK** on the bottom left of the dialog to return to the Create Deployment Bot Runtime template.

Add a Patching Process (Required)

1. Select **Browse** next to **Add Patching Process** in the Create Deployment Runtime dialog.
2. Select  **Patching Processes**, and then select **Show All** to see the available processes.
3. Select the process you want to use. For example, select **Immediate Phased Deployment - Initial Patch Manager Approval**.

4. Select **OK** on the bottom left of the dialog.



Add a Deployment Channel (Optional)

1. Select **Browse** next to **Add Deployment Channel**.
2. Select  **Deployment Channels**, and then select **Show All** to see the available channels.
3. Select the channel you want to use. For example, select **Daily (13hrs)** to run the Deployment Channel at 1:00 pm every day.
4. Select OK on the bottom left of the dialog.

Add Business Units (Optional)

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



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

×

Create Deployment Bot Runtime

Patch Deployment Bot * [Browse](#)

Patching Process * [Browse](#)

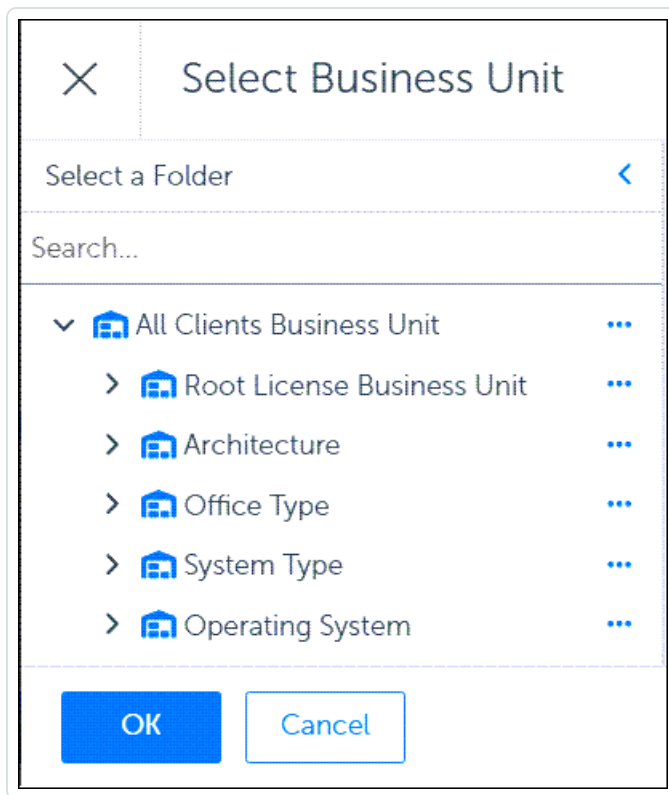
Deployment Channel [Browse](#)

Include All Business Units ☐ Disabled

Business Units * [+ Browse](#)

Create Deployment Bot Runtime Cancel

- To choose specific Business Units for this Runtime, click **+ Browse**, and then continue with the next step.
2. Select one or more **Business Units** to add to this Runtime. For example, to use this Runtime on all Windows 11 systems using a Wi-Fi connection, select **Operating System - Windows 11** and **Office Type - WiFi**.

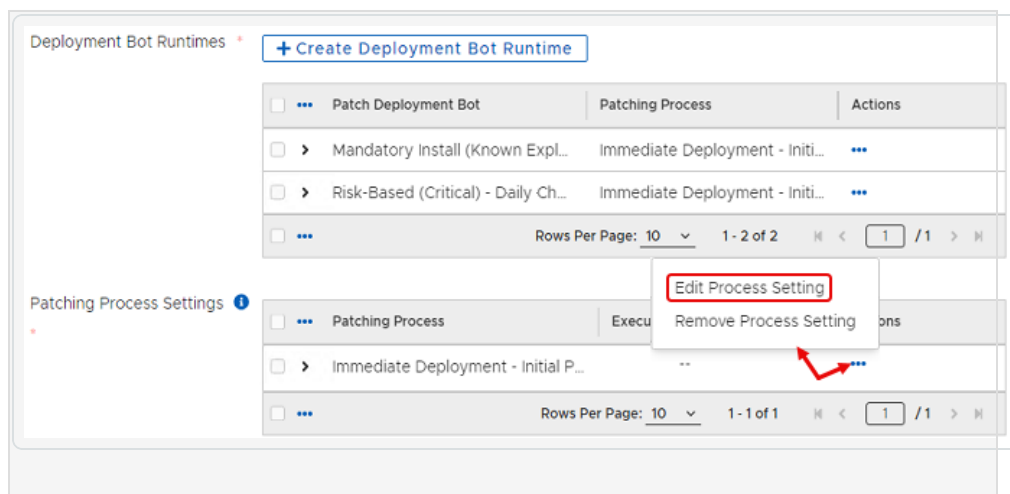


3. Select **OK** on the bottom left of the dialog to view the completed Runtime Bot.
4. Select **Create Deployment Bot Runtime** on the bottom-left corner of the dialog to return to the Patching Strategy.
5. Return to [Create Deployment Bot Runtime Scenarios](#) to add more Deployment Bot/Patching Process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

Set the Patching Process Runtime

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

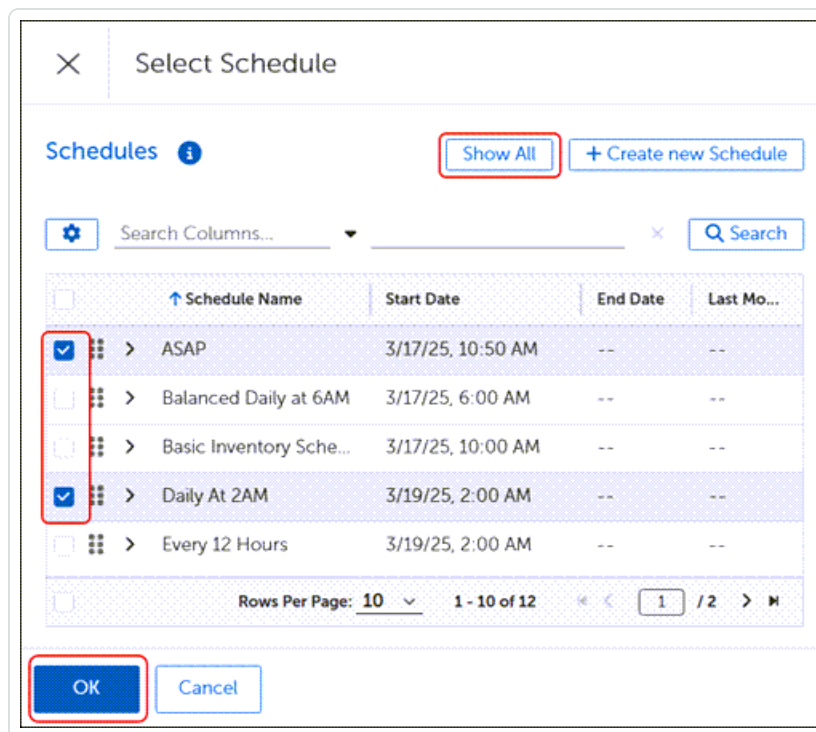
1. Select the **ellipsis (...)** under **Actions** in the **Patching Process Settings** table of an open Patching Strategy template, and then select **Edit Process Setting**.



2. Add one or more schedules for the process:

a. Select **+ Browse** next to Execution Schedules.

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



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



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

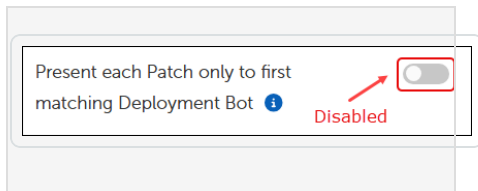
- d. Enter the number of **Hours**, **Minutes**, and **Seconds** that the patching process may run before timing out. Zero indicates no time limit.

3. Select **OK**, to return to the Patching Strategy workspace.

Present Patches to the First Matching Deployment Bot

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

1. Scroll down to the bottom of the **Deployment Settings** workspace of an open [Patching Strategy](#).



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

Add Approval Chains to a Patching Strategy

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



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

6. Select **Save** at the upper left to save your progress:

- a. Check the **Error View** and resolve any errors.
- b. Select **Save** again if you make any changes.

Managing Notification Settings

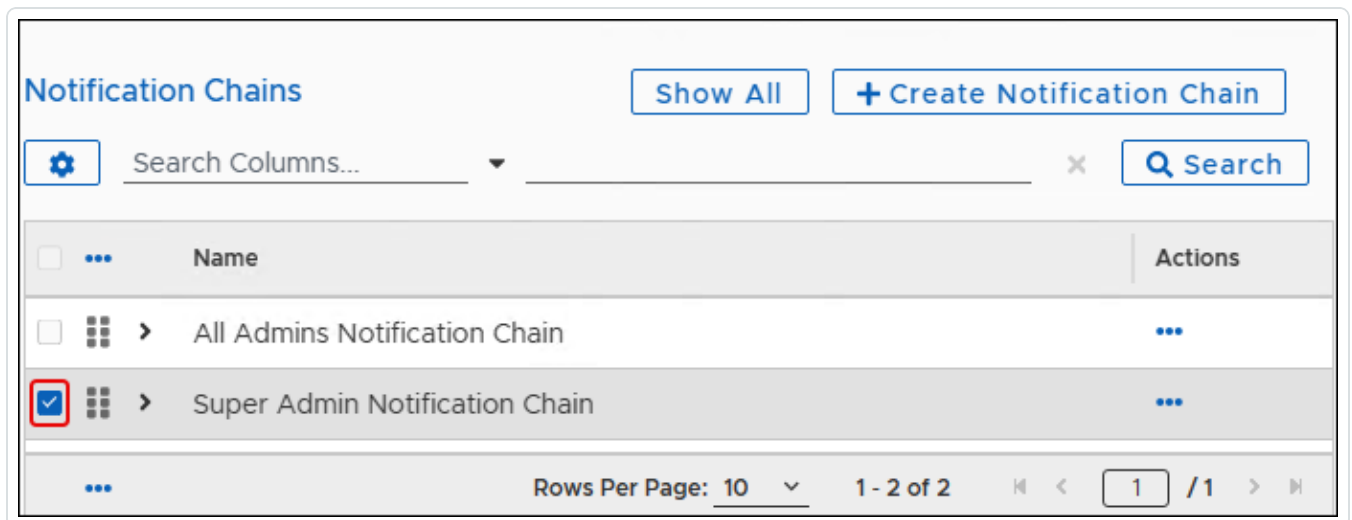
Patching Strategy, Deployment Channel, and Business Unit objects include a **Notifications** dialog where you can configure notification details. The configuration choices differ slightly for each object.

Note: This configuration requires selecting a specific type of Notification Cycle template. Contact Tenable Patch Management Customer Support for assistance with this configuration and for information about choosing the correct template.

Add a Notification Chain

Notification Chain settings exist in the object templates for Patching Strategies, Deployment Channels, and Business Units.

1. Expand the **Notifications** box in an open object template to show the available configuration options.
2. Select **Browse** next to **Notification Chain**. This opens the Notifications Chain dialog.



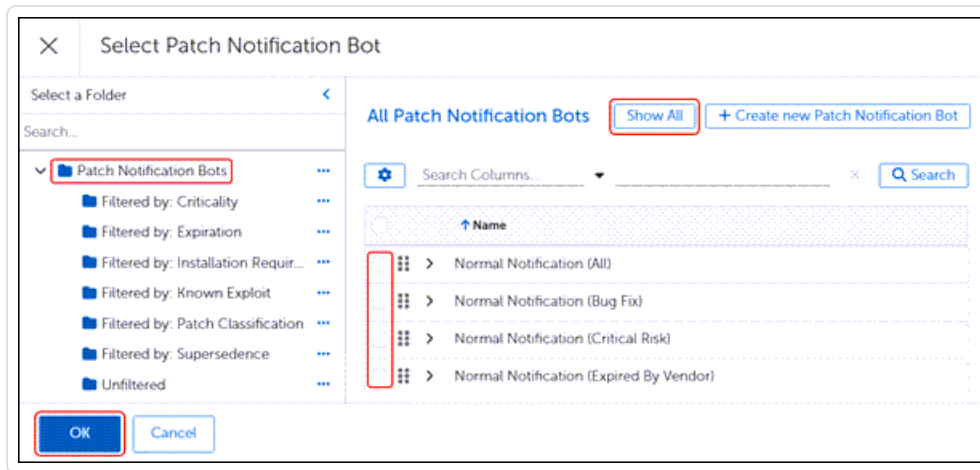
3. Select  **Notification Chains**, and then select **Show All** to see the available templates.
4. Select a **Notification Chain** from the table. To edit or create Notification Chains, see .
5. Continue editing the **Notification** settings or click OK on the bottom left corner to return to the template.

Add Patch Notification Bots

Both Patching Strategies and Deployment Channel templates have an option to Add Patch Notification Bots.

1. Select **+ Browse** next to Patch Notification Bots in the **Notifications** workspace of the object template.

This opens the Select Patch Notification Bots dialog.



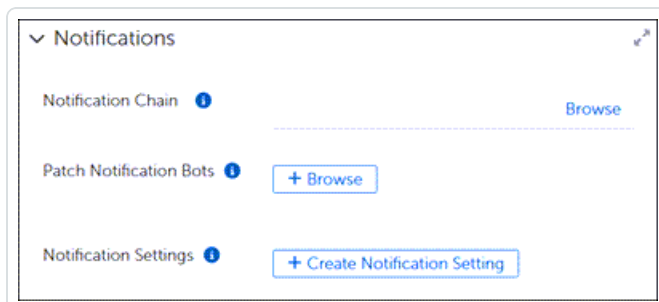
2. Select  **Patch Notification Bots**, and then select **Show All** to list all available Patch Notification Bots or click any **Filtered by:** folder to see the Bots associated with that filter.
3. Choose one or more **Notification Bots** to set requirements for this template. To create more Notification Bots, see [Creating Notification Bots](#).
4. Select **OK** on the bottom left of the dialog to return to the starting template.

Create Notification Settings

Set Notification Urgency

These values must match the corresponding values defined in the Notification Bots. Otherwise, the Notification Cycle does not send a notification.

1. Select **+ Create Notification Setting** in the Notifications box of the object template.





2. Expand the list of options next to **Notification Urgency**, and then select the urgency setting that matches the Notification Bot.

Create Notification Setting

Notification Urgency ⓘ Low ▼

Execution Schedules ⓘ [+ Add Schedules](#)

Notify Patching Strategy Chains ⓘ ☐

Notify Business Unit Chains ⓘ ☐

Notification Cycle Workflow ⓘ [Add Workflow](#) [BROWSE](#)

Time Limit ⓘ 0 Hours 0 Minutes 0 Seconds

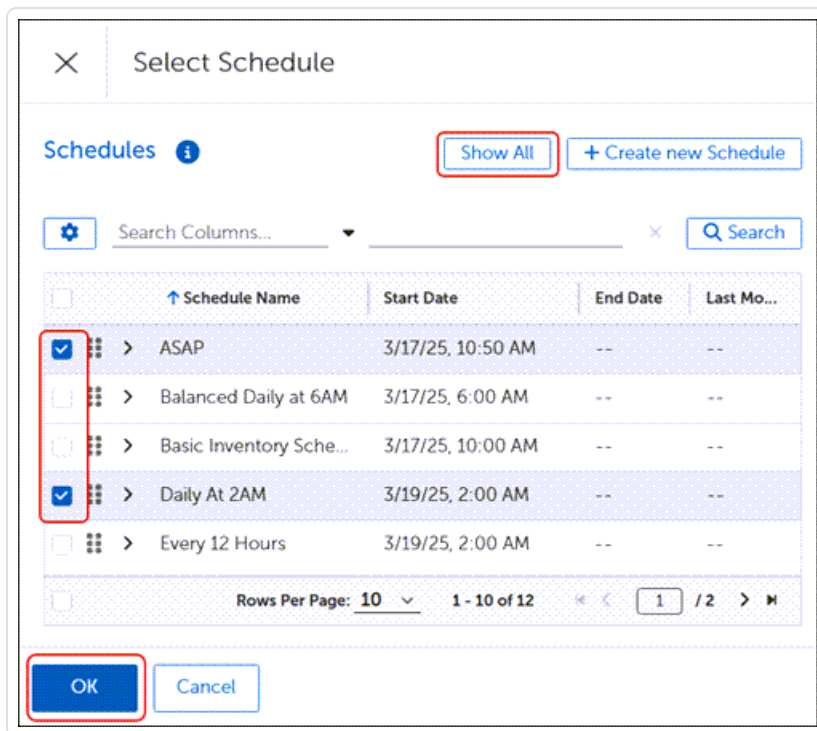
[Create Notification Setting](#) [Cancel](#) Windows.

3. Continue editing the **Notification** settings or click Create Notification Settings to return to the template.

Add Execution Schedules

Execution Schedules control when and how often a Notification Cycle sends notifications. Choose schedules based on when and how often receiving parties require notification.

1. Select **+ Create Notification Setting** from the Notifications workspace of a object template.
2. Select **+Browse** next to Execution Schedules to display the available schedules.
3. Select one or more schedules from the All Schedules table, and then select **OK** on the lower-left corner of the dialog.



4. Continue editing the notification settings or click Create Notification Settings to return to the template.

Enable Notifications for Patching Strategy and Business Unit Chains

When enabled, sends notifications to the Roles shown in the Notification Chain associated with the Patching Strategy or Deployment Channel template. Defaults to disabled.

1. In the **+ Create Notification Setting** dialog in the Patching Strategy or Deployment Channel template, decide whether to enable notifications:
 - Select the **Notify Patching Strategy Chains** toggle to enable or disable (default) whether the notification cycle sends notifications to the chains included in the strategy.
 - Select the **Notify Business Unit Chains** toggle to enable or disable (default) whether the notification cycle sends notifications to Business Unit chains included in the strategy.
2. Continue editing the **Notifications** settings or click Create Notification Settings to return to the template.

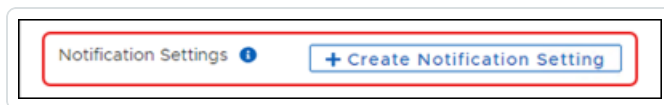
Choose a Notification Cycle Workflow



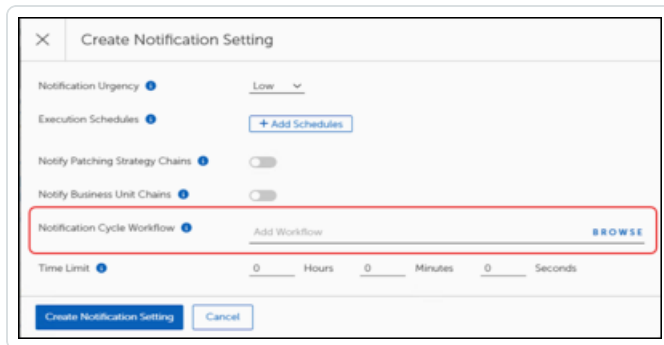
This setting names the Notification Cycle that processes the Notifications for the Patching Strategy or Deployment Channel. Notification Cycle workflows are customized for specific uses. Tenable Patch Management does not provide sample Notification Cycle templates. These templates exist only if you create them for your environment.

Note: Contact Tenable Patch Management Customer Support for assistance with Notification Cycle templates

1. Select **+ Create Notification Setting** from the Notifications box in the object template.



This opens the Create Notification Setting dialog.



2. Select **Browse** on the **Add Workflow** line. This opens the list of available workflows.
3. Select your custom workflow from the list, and then click **Add Workflow** on the lower-left corner of the dialog.
4. Continue editing the **Notification** settings or click Create Notification Settings to return to the template.

Set the Time Limit

Specifies the maximum length of time that the Notification Cycle Workflow runs before timing out. If set to all zeros (default) the workflow may run indefinitely. Choose this setting with care. If the notification times out before sending all notifications, the next cycle triggers the notifications again.



1. Select **+ Create Notification Setting** the Notification box of the object template.
2. Next to Time Limit, set the **Hours**, **Minutes**, or **Seconds** that the Notification Cycle will run, or leave the setting default at 0 for each item to allow the workflow to run indefinitely.
3. Continue editing the **Notification** settings or click Create Notification Settings to return to the template.

Customer Extension Data

Customer Extension Data is an advanced feature of Tenable Patch Management . The Customer Extension Data fields allow advanced users to specify different key/value pairs for use in customized Patching Strategies, Deployment Chains, or Business Units when necessary to achieve different results.

The screenshot shows a configuration window titled "Customer Extension Data" with a dropdown arrow on the left and a refresh icon on the right. Inside the window, there is a header "Customer Extension Data" followed by an information icon (i). Below this, there are two input fields: "New Key" and "New Value". At the bottom center, there is a button labeled "+ Add".

Customer Extension Data fields relate directly to fields in a customized template. If you do not have customized templates with key/value pairs you can modify, you do not need to configure or use this feature.

If you want to create customized templates that use key/value pairs for some settings, contact Tenable Patch Management Customer Support .

Content Prestaging Settings

The Content Prestaging feature deploys content to devices ahead of the scheduled deployment, either pushing content to a location or allowing a client to pull content. Prestaging content makes the content available on the device locally when the deployment time arrives. This reduces the deployment time and minimizes the chances of missing service windows or having devices going offline before a content download finishes.

You can create Content Prestaging Settings within the Patching Strategy, Business Unit, or Deployment Channel templates.



Defining Content Prestaging Settings

The templates for Patching Strategies, Deployment Channels, and Business Units include the choice to set Content Prestaging settings. Settings default to **Not Enabled**.

Content Prestaging settings include two options:

- **Server Content Push (Recommended)** - The Tenable Patch Management pushes the content to the best-suited sources in all locations that require the content. Tenable Patch Management recommends this type of prestaging when the Deployment Strategy targets only a subset of devices. High-availability machines receive the content and function as local sources during discovery and deployment.
- **Client Content Pull** - This option enables any client that requires the content to download and cache it before deployment. Suitable when a Deployment Strategy targets all clients that need the updated content.

Push Content

- **Not Enabled** -- Disables any prestaging as part of the Patching Process workflow or Patching Strategy.
- **Handled by System** - The Tenable Patch Management system handles the prestaging automatically and pushes content to three automatically chosen devices within the office that require the content.

This push occurs at once when the metadata updates include the latest content that meets patching requirements.

- **Handled by Workflow** - When enabled as part of a Patching Process, Deployment Channel, or Business Unit template, pushes the content upon deployment of the Patching Process.

Pull Content

- **Not Enabled** -- Disables any prestaging as part of the Patching Process workflow or Patching Strategy.
- **Handled by System** - The Tenable Patch Management system handles the prestaging automatically. The Client pulls content from the Server and instructs all Clients that require the content to download and cache it ahead of any deployment.

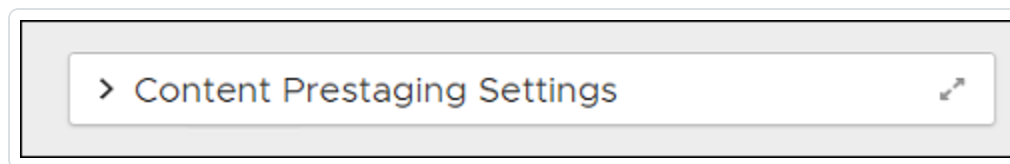


- **Handled by Workflow** - When enabled as part of a Patching Process, Deployment Channel, or Business Unit template, the Client pulls the content upon deployment.

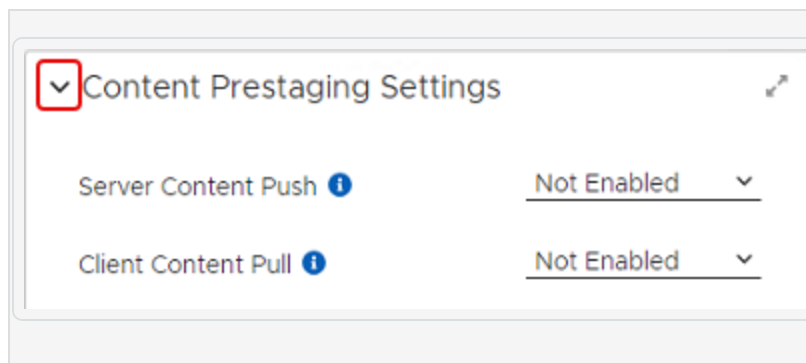
Set Content Prestaging Settings

Use this procedure to add or change Content Prestaging Settings in Patching Strategy, Business Unit, or Deployment Channel templates.

1. Expand the **Notifications** box in an open object template, and then scroll down to the Content Prestaging Settings.

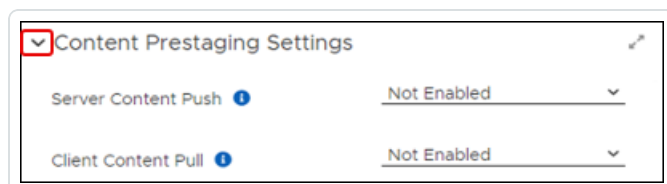


2. Expand the Content Prestaging Settings box to view the available settings.



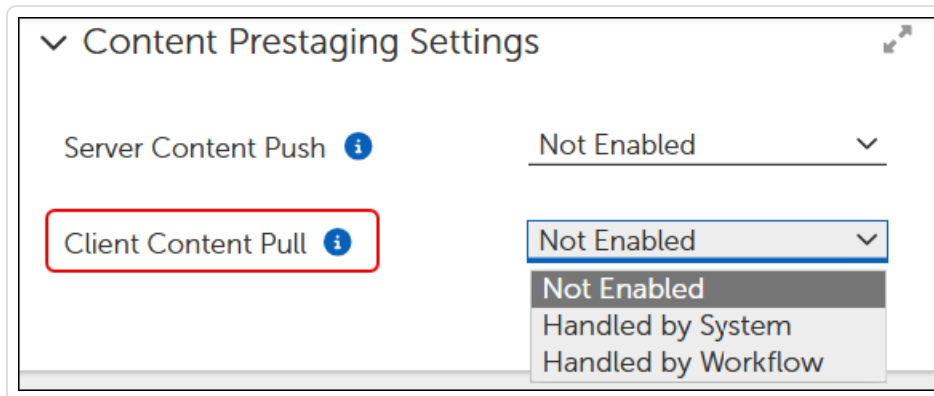
Enable Client Content Pull

Client Content Pull defaults to Not Enabled. To enable pull settings, complete the following steps in the Content Prestaging Settings of a Patching Strategy, Business Unit, or Deployment Channel template:





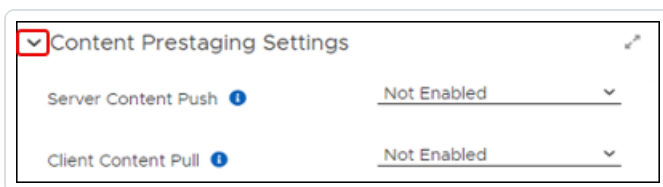
1. Select the arrow to the right of **Client Content Pull** to expand the menu of available options.



2. Select the option you need for the object template you are using. For definitions of push options, see [Defining Content Prestaging Settings](#).
3. Select **Save** on the upper left to save your changes:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.

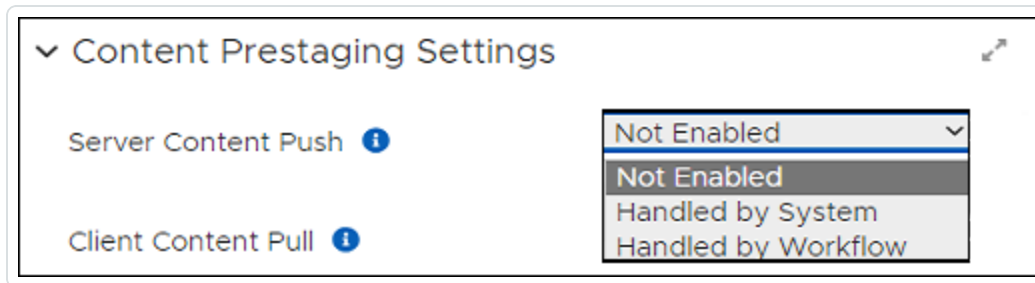
Enable Server Content Push

Server Content Push defaults to Not Enabled. To enable push settings, complete the following steps in the Content Prestaging Settings of a Patching Strategy, Business Unit, or Deployment Channel template, complete the following steps:





1. Select the arrow to the right of **Server Content Push** to expand the menu of available options.



2. Select the option you need for the object template you are using. For definitions of push options, see [Defining Content Prestaging Settings](#).
3. Select **Save** on the upper left to save your changes:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.

Business Unit Addition Settings

Business Unit Addition Settings do not have a separate menu item. Configure these settings from the Business Unit Addition Settings dialog in a Patching Strategies template.

Business Unit Addition Settings in Patching Strategies

When you have added a new Business Unit to an enabled Patching Strategy that has already completed the current patching cycle, you must use the Business Unit Addition Settings to add the parent Business Unit that contains the details, such as Patches and Patch Approval Settings, any Business Unit added to the Strategy will inherit.

The Business Unit you specify here includes the patch approvals the Patching Strategy will use for any Business Units you add to the Strategy after the Strategy has run.

The Patching Process you select here is the same process you identified in the Deployment Bot Runtime configuration of the Patching Strategy.



Business Unit Addition Settings

Template Business Unit

Add Business Unit

BROWSE

Patching Process

Add Patching Process

BROWSE

Configure Business Unit Addition Settings

1. Select **Strategy > Patching Strategies** from the left navigation menu of the [Patch Dashboard](#).
2. Scroll down to **Business Unit Addition Settings** and then click the **right arrow** to expand the box.

Business Unit Addition Settings

Template Business Unit

Add Business Unit

BROWSE

Patching Process

Add Patching Process

BROWSE

Select a Business Unit

Specify the parent Business Unit for this strategy so that when new Business Units become part of the strategy after it has already run, the new Business Units inherit settings from the same parent.

1. Select **Browse** next to Template Business Unit in the Business Unit Addition Settings dialog of an open Patching Strategy template.
2. Select the **Business Unit** that has the parent settings for any future Business Units added to the Strategy.
3. Click **OK** to return to the template.
4. Select **Save** on the upper left to save your changes:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.



Note: If you came to this procedure while you were configuring Deployment Settings in a Patching Strategy, return to [Deployment Settings](#) to continue the Strategy configuration.

Select a Patching Process

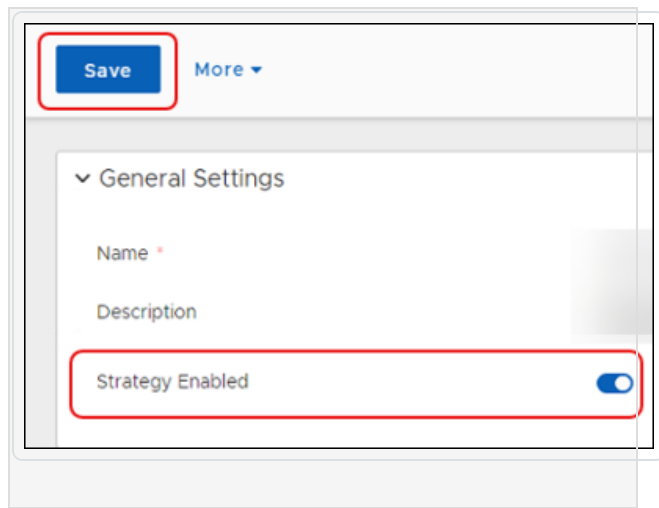
Identify the Patching Process that controls the approval and deployment logic for the existing Business Units in this strategy. This is the same Patching Process identified in the Deployment Bot Runtime, which is the only Patching Process you can choose here. This ensures that any Business Units added after initial creation of this strategy use the same Patching Process as the existing Business Units.

1. Verify that the **Deployment Bot Runtime** details are accurate. The Patching Process settings needed for Business Unit Addition settings are the same as those used in the Deployment Bot Runtime.
2. Select **Browse** next to **Patching Process** in the Business Unit Additions dialog of an open Patching Strategy. If Browse is disabled, check the [Deployment Bot Runtime Settings](#).
3. Select the available Patching Process, and then click **OK**.
4. Select **Save** on the upper left corner to save your changes:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.

Enable the Patching Strategy

After completing the Patching Strategy configuration, including [Add Software Products](#), you must enable the Patching Strategy. When enabled, the strategy runs according to the configured schedules.

1. In **General Settings** at the top of the Patching Strategy template, click the **Strategy Enabled** toggle to enable the strategy and make it available for use.



2. Select **Save** on the upper-left corner of the workflow to save the strategy:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.
3. [Move the saved template to your folder](#) .

Maintenance Windows

A Maintenance Window defines a period during which system maintenance occurs on a device. Business Unit configurations include Maintenance Window settings so administrators can schedule maintenance activities. Tenable Patch Management installs patches only during the defined Maintenance Window.

Maintenance Windows can include one or more schedules that deploy based on urgency settings (Low, Normal, High, and Critical). Urgency settings are cumulative, so higher urgencies inherit any settings specified at lower urgencies.

Overlapping time settings do not have a restrictive effect, but Tenable Patch Management recommends keeping your Maintenance Window time settings simple. When a patch encounters multiple time settings for Maintenance Windows, it reviews one after another until it finds a match.

Tenable Patch Management provides built-in Start Time objects, available from the following path:

Schedules\Patching Schedules\Window Start

Open and Save a Maintenance Window Template



1. Select **Maintenance Windows** in the left navigation menu of the [Patch Dashboard](#).

Note: 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 corner of the dialog, and then select **Save As**.
 - b. Enter a new name for the template, and then click **Save as** on the lower-left corner of 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 corner 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 Tenable Patch Management 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 click **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 ⓘ [+ Create Maintenance Window](#)

Start Time Schedule	Duration	Actions
02:00	2h	⋮

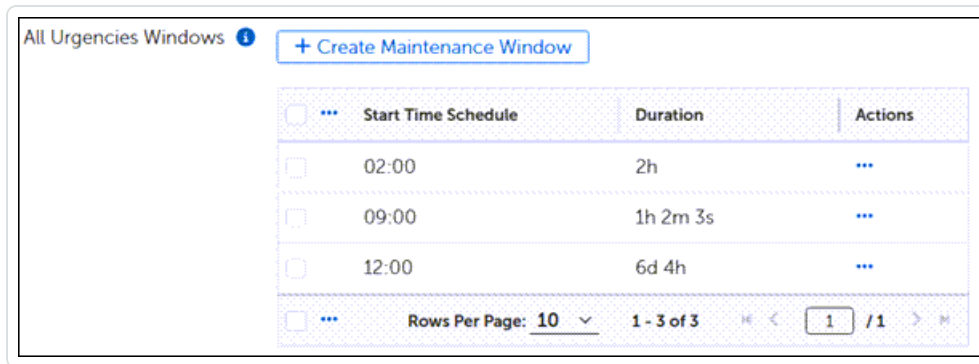
Rows Per Page: 10 1 - 1 of 1 < 1 / 1 >

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.



The screenshot shows a web interface titled "All Urgencies Windows" with a "+ Create Maintenance Window" button. Below the button is a table with the following columns: "Start Time Schedule", "Duration", and "Actions". The table contains three rows of data:

	Start Time Schedule	Duration	Actions
☐	02:00	2h	...
☐	09:00	1h 2m 3s	...
☐	12:00	6d 4h	...

At the bottom of the table, there is a pagination bar showing "Rows Per Page: 10", "1 - 3 of 3", and a page number "1 / 1".

3. Set an All Urgencies Override Duration.

These settings override any non-zero duration values set in 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

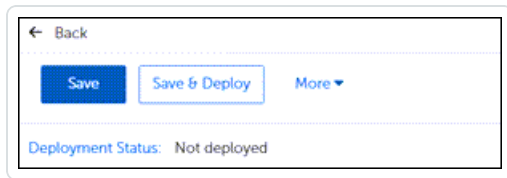
Deploy a Maintenance Window to make it available for use in a template. If you update a Maintenance Window template that was previously deployed, you must save and deploy it again for the changes to take effect.

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.

A screenshot of a web interface showing deployment options. At the top left is a 'Back' button with a left arrow. Below it are three buttons: 'Save' (solid blue), 'Save & Deploy' (outlined blue), and 'More' (outlined blue with a dropdown arrow). At the bottom, it says 'Deployment Status: Not deployed'.

Customized Products

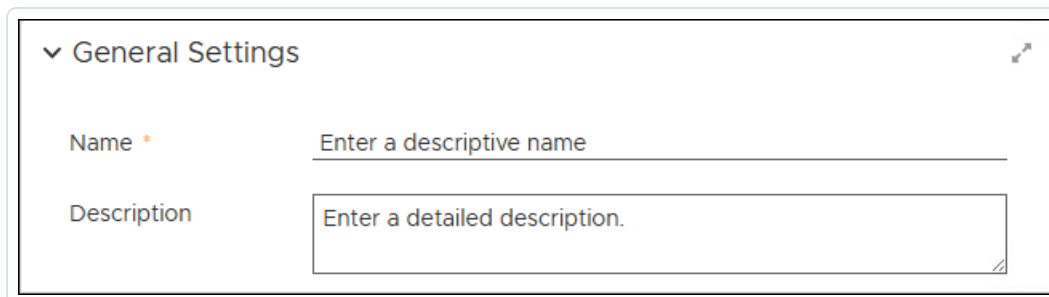
Software products and patches sometimes require user interaction when installing. Users enter details such as license information or request to show a menu at startup. Other default settings include auto update, or desktop shortcuts.

Tenable Patch Management uses Customized Product settings to include information or change defaults when installing products on managed devices.

Manage Settings for Customized Products

Open and Save a Customized Product Template

1. Select **Customized Products** on the left navigation menu of the [Patch Dashboard](#).
2. Select **+ New** in the upper-right corner to open a new template:

A screenshot of a 'General Settings' form. The title 'General Settings' is at the top left with a dropdown arrow. In the top right corner is a small icon with a left arrow and a plus sign. The form has two main sections: 'Name' with a red asterisk and a text input field containing the placeholder 'Enter a descriptive name'; and 'Description' with a text area containing the placeholder 'Enter a detailed description.'.

- a. Enter a **Name** that identifies your template.
 - b. Enter a detailed **Description**, and then click **Save** on the upper left corner.
3. Continue with [Add a Deployment Wave](#).

Add a Deployment Wave to a Customized Product Template

The Deployment Wave contains the Business Units that use the product you intend to target.



1. Select **Browse** next to **Add Deployment Wave** in an open [Customized Product Template](#) .

General Settings

Name *

Description

Deployment Wave ⓘ * **BROWSE**

Target Product ⓘ * **BROWSE**

2. Select the **Deployment Wave** to which these Customized Product settings apply on the Deployment Waves dialog. See [Deployment Waves](#) for details.
3. Select **Add Deployment Wave** on the lower-left corner of the Deployment Waves dialog.
4. Select **Save** on the upper-left corner of the template to save your changes and continue editing.
5. Continue with [Add a Target Product](#).

Add a Target Product

1. Select **Browse** next to Add Software Product in an open [Customized Product Template](#) .
2. Enter the Name of the product you want to customize in the search field, and then click **Search**.

Software Products Show All

☐	Name	Actions
☒	Google Chrome x64	...
☐	Google Chrome x86	...

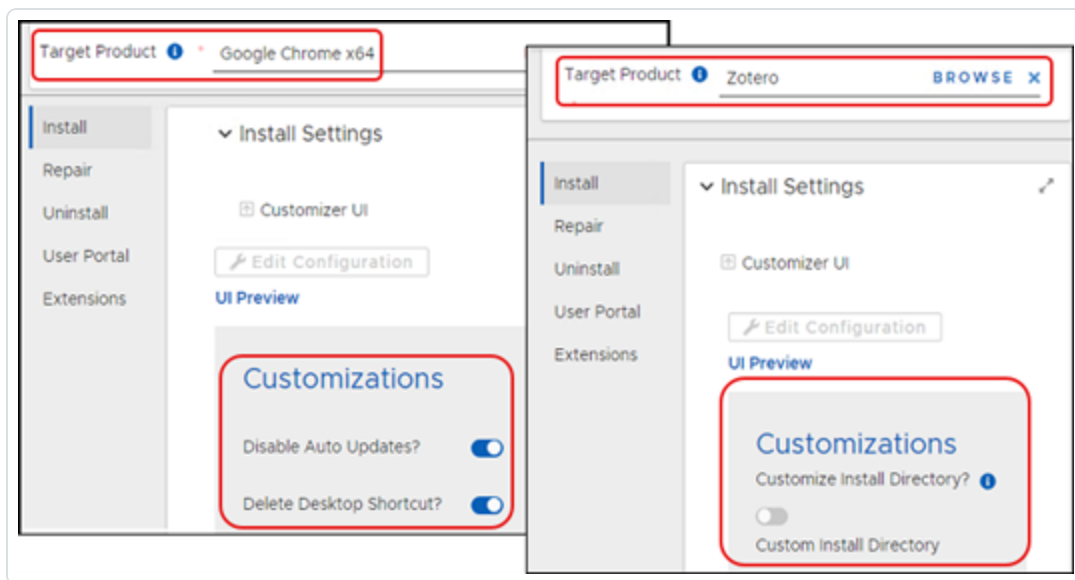
3. Select the **Software Product** you want to customize. You can target only one Software Product in each Customized Product entry.



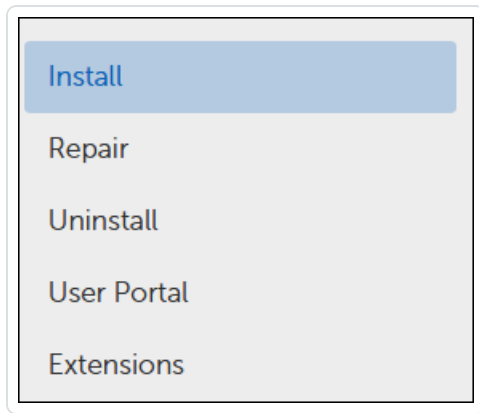
4. Select **Add Software Product** to populate the configurable items in the static list of **Install Settings**. Settings change depending on the Target Product.
5. Select **Save** in the upper-left corner of the template to save your changes.
6. Continue with [Configure Software Install Settings](#).

Configure Software Install Settings

1. Select **Install** in the left column of **Install Settings**.
 - 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 chose allows changes or input for any of these settings, review and create the responses you need.



3. Select **Save** at the upper left to save your progress:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.
4. Select <-- **Back to Customized Products** above the **General Settings** box. The changes you have made take effect the next time the associated Deployment Wave runs.

Deployment Waves

Deployment Waves allow deployment of patches progressively to devices contained in different Business Units. Because Waves execute in top-to-bottom order, less Critical Business Units appear higher in the priority. This prioritizes deployment to non-mission critical business units or smaller groups of endpoints first, followed by more critical or larger groupings of endpoints.

Using Deployment Waves

Entries for Deployment Wave settings exist in the object templates for Business Units, Deployment Channels, and Customized Products templates. All methods use the same process.

Open and Save a Deployment Wave Template

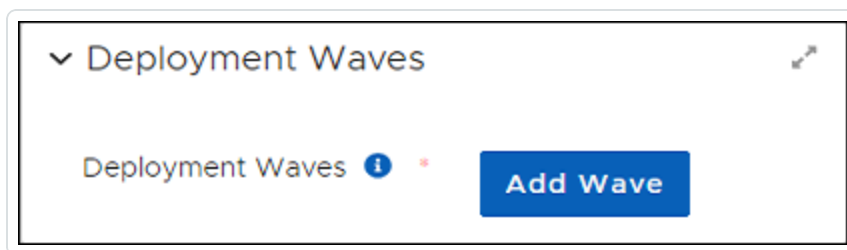
1. Select **Deployment Waves** in the left navigation menu of the [Patch Management Dashboard](#).
2. Select the **Name** of a template to open it, and then save the template with a new title:



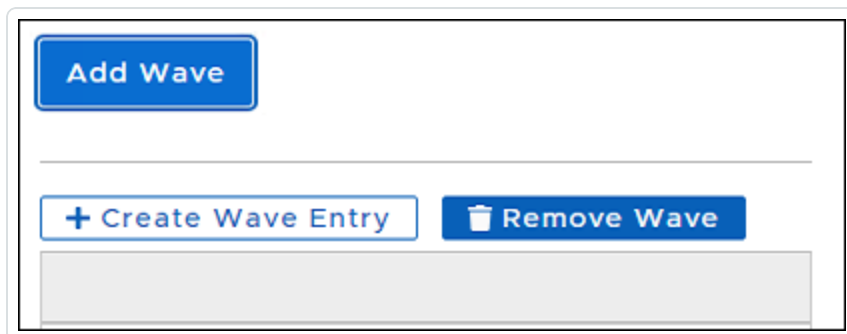
- a. Select **More** in the upper-left corner of the dialog, and then select **Save As**.
- b. Enter a new name for the template, and then click **Save as** on the lower-left corner of dialog. This returns you to a copy of the template with the new name.
- c. Enter a detailed **Description** of the process 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 corner of the dialog.

Add a Deployment Wave Entry

1. Scroll down to **Deployment Waves** in an open [Deployment Wave](#) template.
2. Select **Add Wave**. This creates a new table to hold another Wave in the template.



3. Select **+ Create Wave Entry** to open the **Wave Entry** dialog.



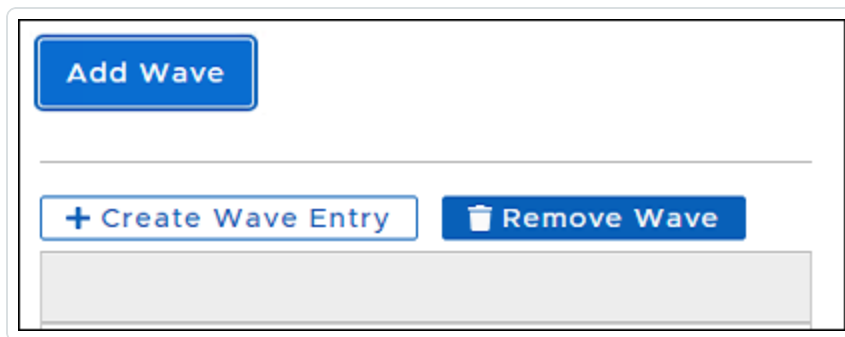
4. Select **Browse** next to **Add Business Unit**:
 - a. Navigate to and select the Business Unit to which the Wave Entry applies.
 - b. Expand the **Include Child Business Units** menu to include one or more child Business Units of the selected parent.



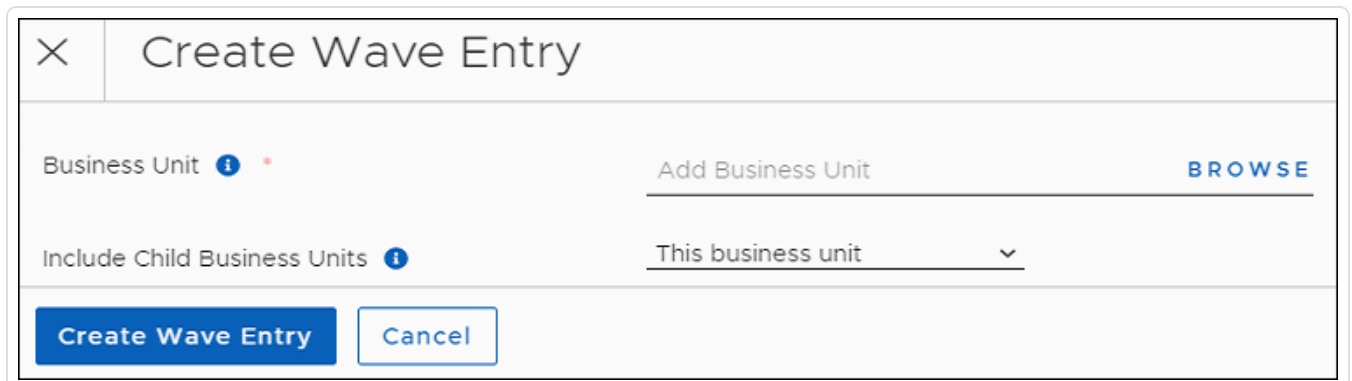
- c. Select the **item** that best describes how you want this wave to manage this deployment to child Business Units.
5. Select **Create Wave Entry** to return to the **Deployment Wave** template.
6. Select **Save** at the upper left to save your progress:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.

Create a Wave Entry

1. Scroll down to **Deployment Waves** in an open Deployment Wave template:



2. Select **Add Wave**, and then select **+ Create Wave Entry**. This opens the **Create Wave Entry** dialog.



3. Select **Browse** next to **Add Business Unit**:



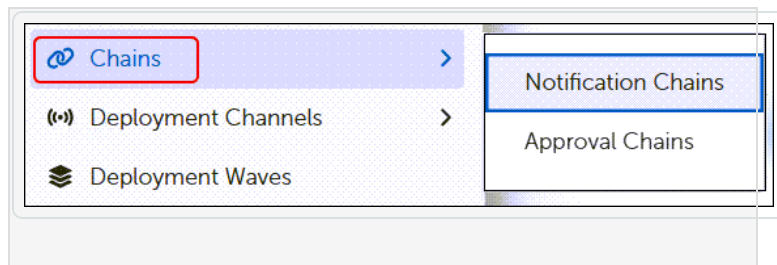
- a. Navigate to and select the **Business Unit** to which the Wave Entry applies.
 - m. Select **Add Business Unit** on the bottom left.
4. Expand the **Include Child Business Units** menu to include one or more child Business Units of the selected parent.
5. Select **Create Wave Entry** to return to the Deployment Wave template.
6. Select **Save** at the upper left to save your progress:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.

Edit or Remove a Wave Entry

1. Select **Deployment Waves** in the left navigation menu of the Tenable Patch Management dashboard, and then click **Show All** on the upper right.
2. Open the **Deployment Wave template** you want to change.
3. Scroll down to the Deployment Waves table that shows the Wave Entry you want to edit or remove.
4. Select the **ellipsis (...)** in the **Actions** column, and then choose an option:
 - To remove the Wave, select **Remove Wave Entry**.
 - To Edit the Wave, select **Edit the Remote Wave Entry**, and then make any necessary changes.
5. Select **Save** at the upper left to save your progress:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.

Chains

Tenable Patch Management uses Approval Chains and Notification Chains to manage communication about, and seek approvals for, patch updates and installations.



Approval Chains: Include details such as approval layers, backup roles, reminder intervals, and more.

Notification Chains: Include details about which parties to notify for what kinds of activities and business units, as well as identifying carrier services.

After you have created Approval Chains and Notification Chains using the Chains workspace, you can assign the chains to a Patching Strategy, a Business Unit, or a Deployment Channel.

Approval Chains

Using Approval Chains

Approval Chains allow the administrator to specify users who will receive patch approval requests for Patching Strategies or Business Units.

Tenable Patch Management includes suggested Approval Chain personas, such as Product Owner, Patch Management, Security, Test Lab, and Change Management. You can customize and layer these roles to model the natural approval structure in your environment, including backup approvers and timeout settings to allow for automatic escalation. You can also omit layers based on patch criticality/urgency.

Open and Save an Approval Chain Template

1. Mouse over or click **Chains** in the left navigation menu of the [Patch Management Dashboard](#), and then select **Approval Chains**.



2. Select the **Name** of a template to open it, and then save the template with new information:
 - a. Select **More** in the upper-left corner of the dialog, and then select **Save As**.
 - b. Enter a new name for the template, and then click **Save as** on the lower-left corner of 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 corner of the dialog.

Managing Approval Chain Settings

Approval Chain management choices include approval of timed out patches, reapproval of modified approvals, setting approval layers, and choosing communication providers.

Each of these tasks assumes you have opened and saved an Approval Chain template and you are ready to complete the General Settings configuration.



General Settings

Name *

[Enter name]

Description

[Enter Detailed Description]

Automatically Approve Timed Out Patches

Reapprove Modified Approvals

Approval Layers

+ Create Approval Layer

☐ ...	Approver Roles	Number of Approvals Needed	Actions
☐ >	All Admin Role	1	...

☐ ...

Rows Per Page: 10

1 - 1 of 1

< 1 / 1 >

Communication Providers

+ Add Communication Providers

☐ ...	Name	Actions
☐ >	HTMLEmailCommunicationProvider	...
☐ >	SimpleEmailCommunicationProvider	...
☐ >	TeamsCommunicationProvider	...
☐ >	TextCommunicationProvider	...
☐ >	WhatsAppCommunicationProvider	...

☐ ...

Rows Per Page: 10

1 - 5 of 5

< 1 / 1 >

Enable or Disable Automatic Approval of Timed Out Patches

When enabled, this setting automatically approves patches when reviewers do not respond within the timeout duration specified in the Approval Layer.



General Settings

Name *

Description

Automatically Approve Timed Out Patches ⓘ ☒ Disabled

Reapprove Modified Approvals ⓘ ☐

Approval Layers ⓘ [+ Create Approval Layer](#)

Communication Providers ⓘ [+ Add Communication Providers](#)

Select the **Automatically Approve Timed Out Patches** toggle to enable or disable (default) this feature.

Enable or Disable Reapproval for Modifications after Approval

When enabled, this setting resends an approval request to earlier approvers if a later approver makes modifications.

General Settings

Name *

Description

Automatically Approve Timed Out Patches ⓘ ☐

Reapprove Modified Approvals ⓘ ☒ Disabled

Approval Layers ⓘ [+ Create Approval Layer](#)

Communication Providers ⓘ [+ Add Communication Providers](#)

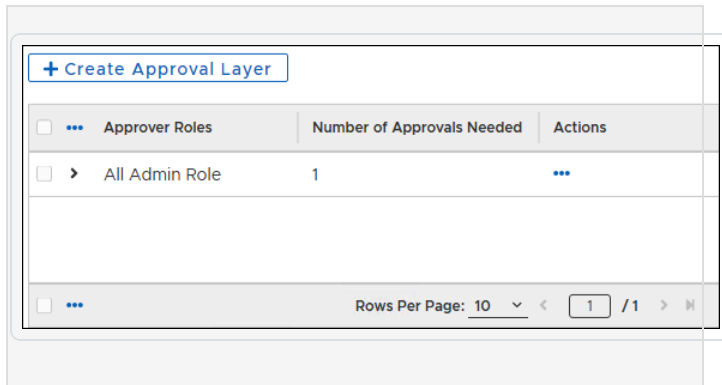
Select the **Reapprove Modified Approvals** toggle to enable or disable (default) this feature.

Create an Approval Layer

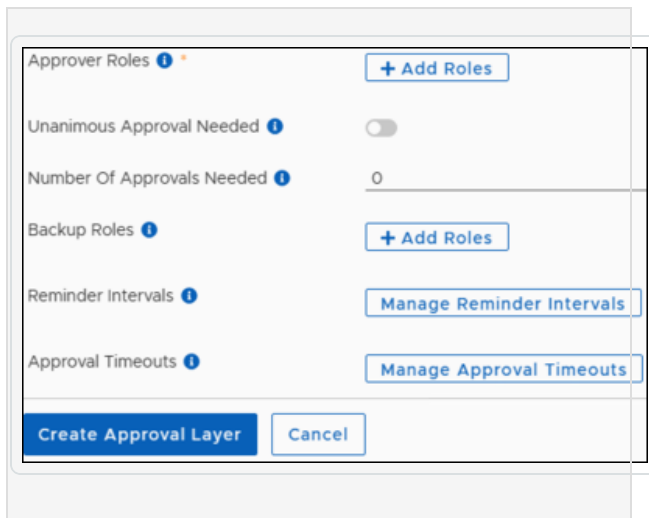
Any object that uses this Approval Chain will process approvals top to bottom in the order listed in the approval layers.



1. Scroll down to **Approval Layers** in an Approval Chain template.
 - For a new approval Layer, click **+ Create Approval Layer**.
 - To change an existing Approval Layer, click the **ellipsis (...)** in the Actions column for the role you want to change, and then select **Edit Approval Layer**.



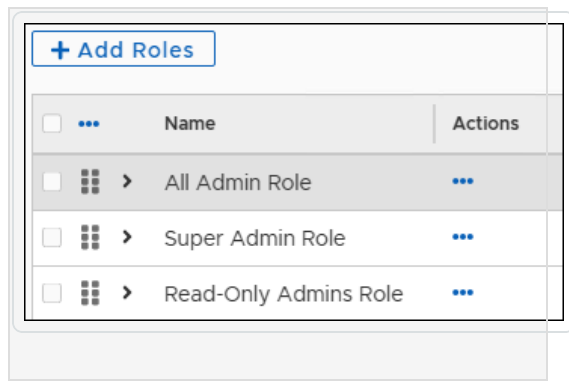
2. This opens the **Create Approval Layer** dialog.



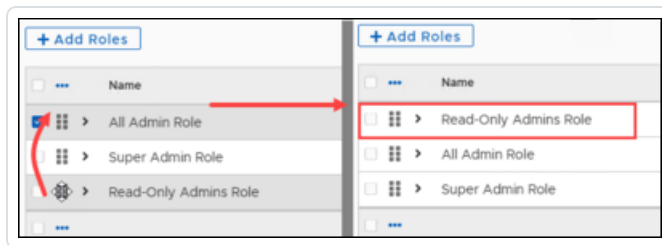
Add and Order Approval Roles

The processing order sends approvals from the top to bottom based on the order of the listed roles.

1. Select **+ Add Roles** on the Approval Layer page.
2. Select one or more existing **Names** from the Roles table, and then click **Add Roles** at the bottom left of the page. This returns you to the Approval Layer dialog.



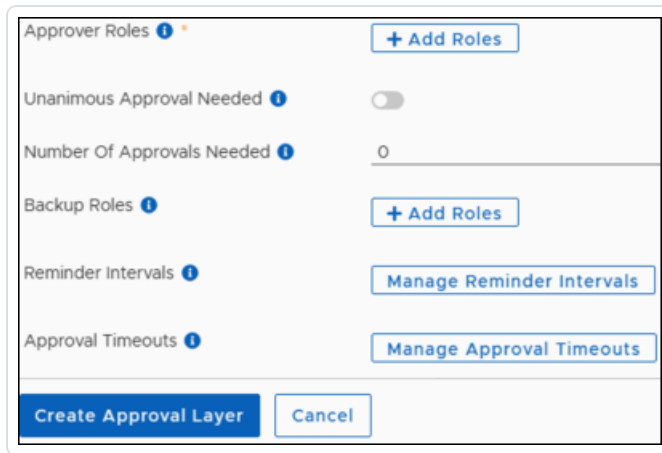
3. Reorder the roles to reflect the processing order you want the strategy to use:
 - a. Select and hold the **stacked dots** for the role you want to move.
 - b. Drag the **role** up or down to move it in the list.



Add Approval Roles to an Approval Layer

Tenable Patch Management includes templates for commonly required roles. You can add these existing roles to the Chains you create by creating approval layers.

1. Select **+ Create Approval Layer** in an open Approval Chain template. This opens the Create Approval Layer dialog.



Approver Roles ⓘ * [+ Add Roles](#)

Unanimous Approval Needed ⓘ ☐

Number Of Approvals Needed ⓘ 0

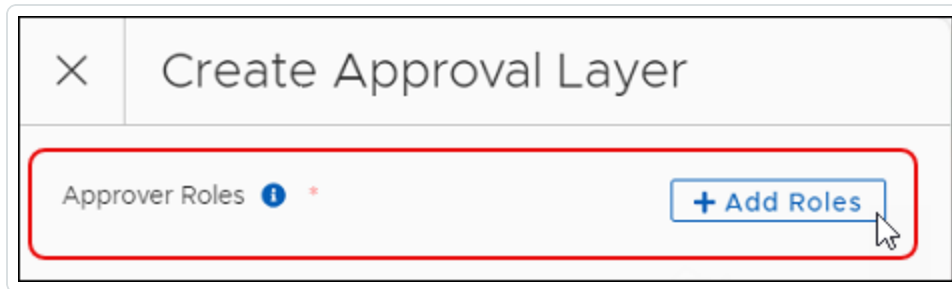
Backup Roles ⓘ [+ Add Roles](#)

Reminder Intervals ⓘ [Manage Reminder Intervals](#)

Approval Timeouts ⓘ [Manage Approval Timeouts](#)

[Create Approval Layer](#) [Cancel](#)

2. Select **Add Roles** next to Approver Roles.



×

Create Approval Layer

Approver Roles ⓘ * [+ Add Roles](#)

3. Select the **Show All** on the upper right to view the available Roles.
4. Select one or more **Roles** to add to the **Approval Layer**.

×

Add Roles

Select a Folder <

Search...

> Roles

Roles

Show All

⚙️

Search Columns...

×

🔍 Search

☐	...	Name
☐	⋮	> All Admin Role
☐	⋮	> Read-Only Admins Role
☐	⋮	> Super Admin Role

☐
...
Rows Per Page: 10
1 - 3 of 3
1 / 1

Add Roles

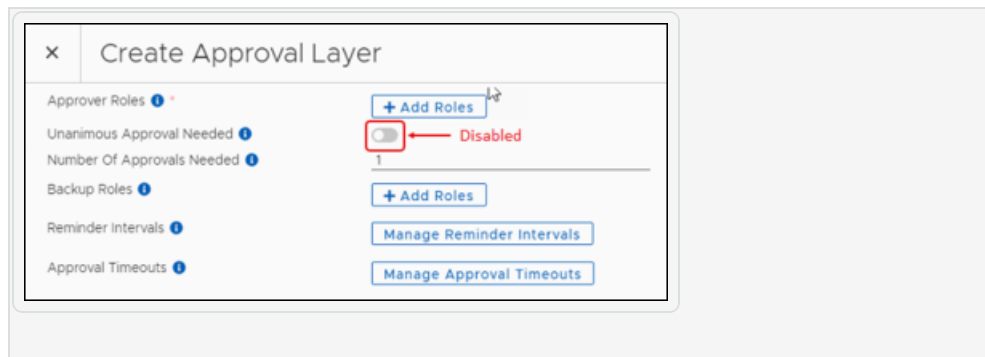
Cancel

5. Select **Add Roles** at the bottom left of the page.

Set Unanimous Approval or Number of Approvals Needed

Choose the number of approvers who must approve patches to satisfy this Approval Layer:

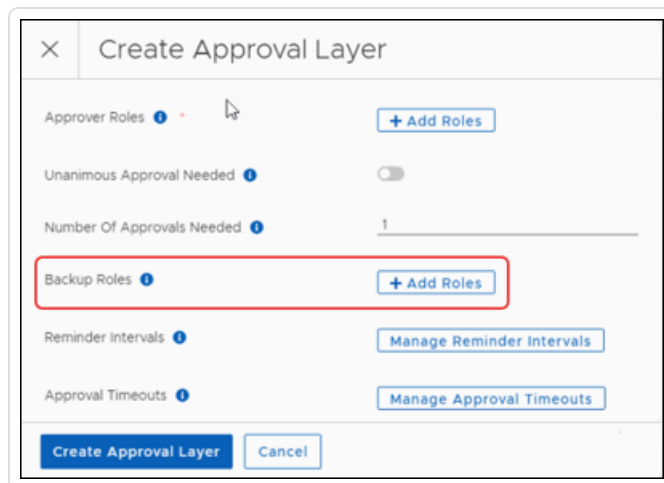
- **Enable Unanimous Approval:** Select the **Unanimous Approval Needed** toggle to enable the unanimous approval requirement. All approvers must approve before deployment continues. Defaults to disabled.
- **Disable Unanimous Approval:** If you choose not to enable this feature, you must enter the Minimal Number of Approvals Needed.



Add Backup Roles to an Approval Layer

Select backup approvers for this approval chain layer. If backup approvers do not approve within the approval timeout duration, the approval request fails.

1. Select **+ Add Roles** next to Backup Roles in the Create Approval Layer dialog.



2. Select **Show All** on the upper right to view all available Roles.
3. Select one or more **Roles** to add.

×

Add Roles

Select a Folder <

Search...

>

Roles

Roles

Show All

⚙

Search Columns...

×

🔍

Search

☐	...	Name
☐	⋮ >	All Admin Role
☐	⋮ >	Read-Only Admins Role
☐	⋮ >	Super Admin Role

☐
...
Rows Per Page: 10
1 - 3 of 3
1 / 1

Add Roles

Cancel

4. Select **Add Roles** at the bottom left of the page.

Set Reminder Intervals

These settings define when to send approval reminders to approvers who have not responded. You can specify different reminder intervals for each urgency level. A setting of zero (0) sends no reminders.



1. Select **Manage Reminder Intervals** below to **Approver Roles**.

Urgency Level	Hours	Minutes	Seconds
Low Urgency Reminder Interval	0	0	0
Normal Urgency Reminder Interval	0	0	0
High Urgency Reminder Interval	0	0	0
Critical Urgency Reminder Interval	0	0	0

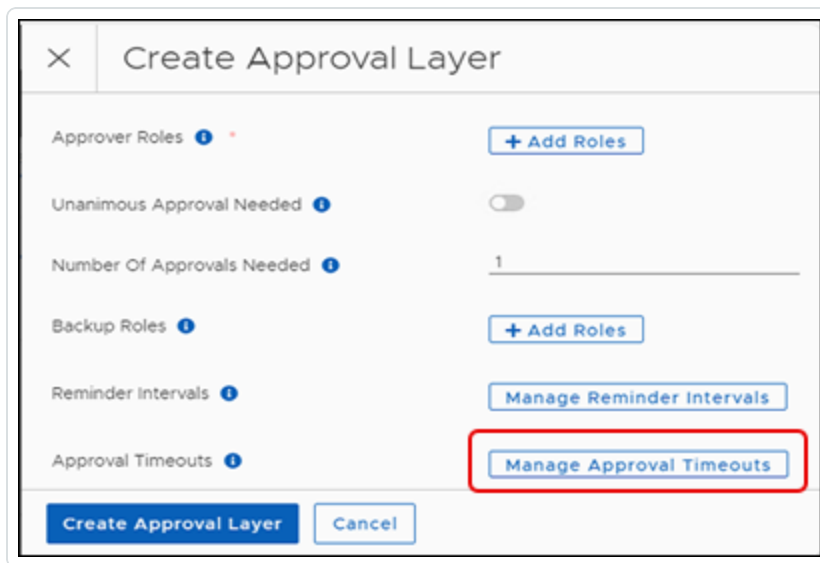
Buttons: OK, Cancel

2. Enter a number for the **Urgency Reminder Interval** (Low, Normal, High, Critical).
 - At zero (0) the strategy sends no reminder.
 - When the request times out, the approval request fails.
3. Select **OK** at the bottom left of the page.

Set Approval Timeouts

These settings define the time out variables for the approval request . You can specify different reminder intervals for each urgency level. A setting of zero (0) sends no reminders.

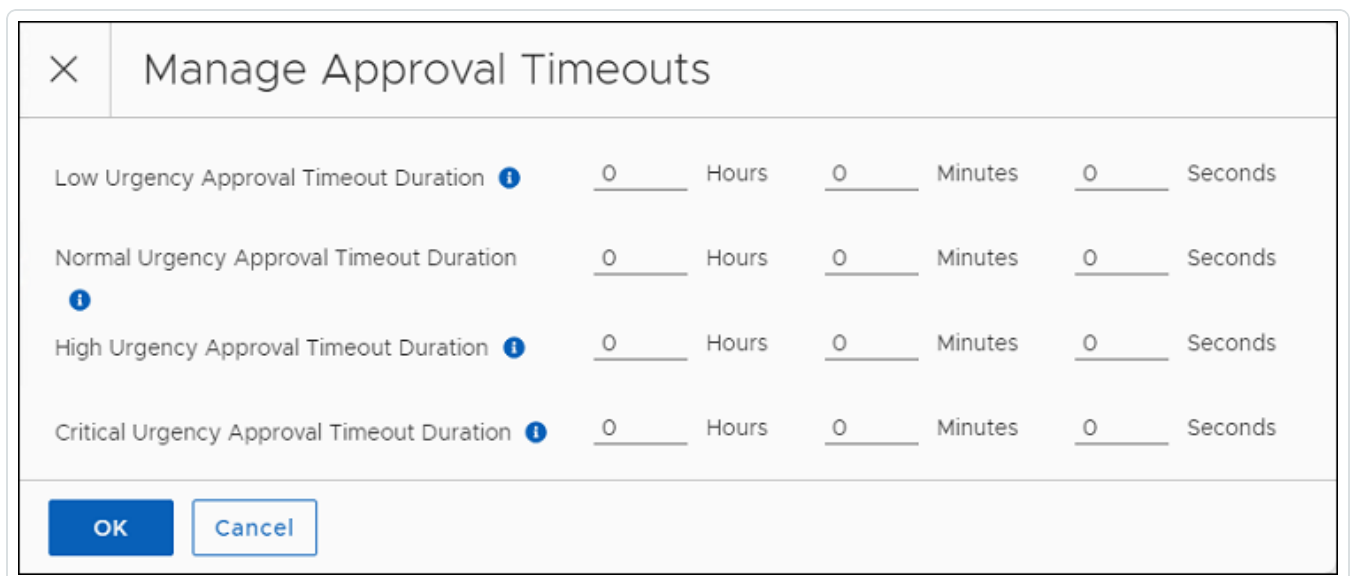
1. Select **Manage Approval Timeouts** in the Create Approval Layer dialog of the Approval Chain template.



The 'Create Approval Layer' dialog box contains the following elements:

- Approver Roles:** A label with an information icon and a red asterisk, followed by a '+ Add Roles' button.
- Unanimous Approval Needed:** A label with an information icon and a toggle switch.
- Number Of Approvals Needed:** A label with an information icon and a text input field containing the number '1'.
- Backup Roles:** A label with an information icon and a '+ Add Roles' button.
- Reminder Intervals:** A label with an information icon and a 'Manage Reminder Intervals' button.
- Approval Timeouts:** A label with an information icon and a 'Manage Approval Timeouts' button, which is highlighted with a red rectangular border.
- Buttons:** 'Create Approval Layer' and 'Cancel' buttons at the bottom.

2. Enter a number for the Urgency Approval Timeout Duration (Hours, Minutes, or Seconds) of the urgency level required:
 - At zero (0) the strategy sends no reminder.
 - If the request times out, the approval request fails.



The 'Manage Approval Timeouts' dialog box contains the following elements:

- Low Urgency Approval Timeout Duration:** A label with an information icon, followed by three input fields for 'Hours', 'Minutes', and 'Seconds', each containing the value '0'.
- Normal Urgency Approval Timeout Duration:** A label with an information icon, followed by three input fields for 'Hours', 'Minutes', and 'Seconds', each containing the value '0'.
- High Urgency Approval Timeout Duration:** A label with an information icon, followed by three input fields for 'Hours', 'Minutes', and 'Seconds', each containing the value '0'.
- Critical Urgency Approval Timeout Duration:** A label with an information icon, followed by three input fields for 'Hours', 'Minutes', and 'Seconds', each containing the value '0'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom left.

3. Select OK on the bottom left of the Manage Approval Time Outs dialog.
4. Select Create Approval Layer to save your changes and return to the Approval Chains template.

Add Communication Providers to an Approval Layer



Tenable Patch Management supplies default Communication Providers that you can use here, or you can create your own. To create new Communication Providers that you can choose when creating Chains, see [Communication Providers](#).

1. Select **+ Add Communication Providers** to open the Add Communication Providers dialog.
2. Select one or more providers to add to the Approval Chain.
3. Select **Add Communication Providers** at the bottom left of the page.
4. Select **Save** at the upper left to save your progress:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.

Managing Approval Settings in Object Templates

Patching Strategy and Business Unit object templates include an **Approval Chains** dialog so you can define administrative approval details as part of the object. To see links to other settings for Patching Strategies, see .

Use this procedure to assign existing **Approval Chains** to a Patching Strategy or Business Unit template. This procedure assumes you have opened and saved an object template and are ready to configure the Approval Chains.

Add Approval Chains to a Patching Strategy

1. Select **Approval Chains** to open the Approval Chains workspace.
2. Select **Browse** next to the type of Approval chain you want to add (Product Owner, Patch Management, Security, and so on).



- Skip any groups that do not apply to your situation.
- When each group from which you need an approval contains an approval chain, continue with the next step.

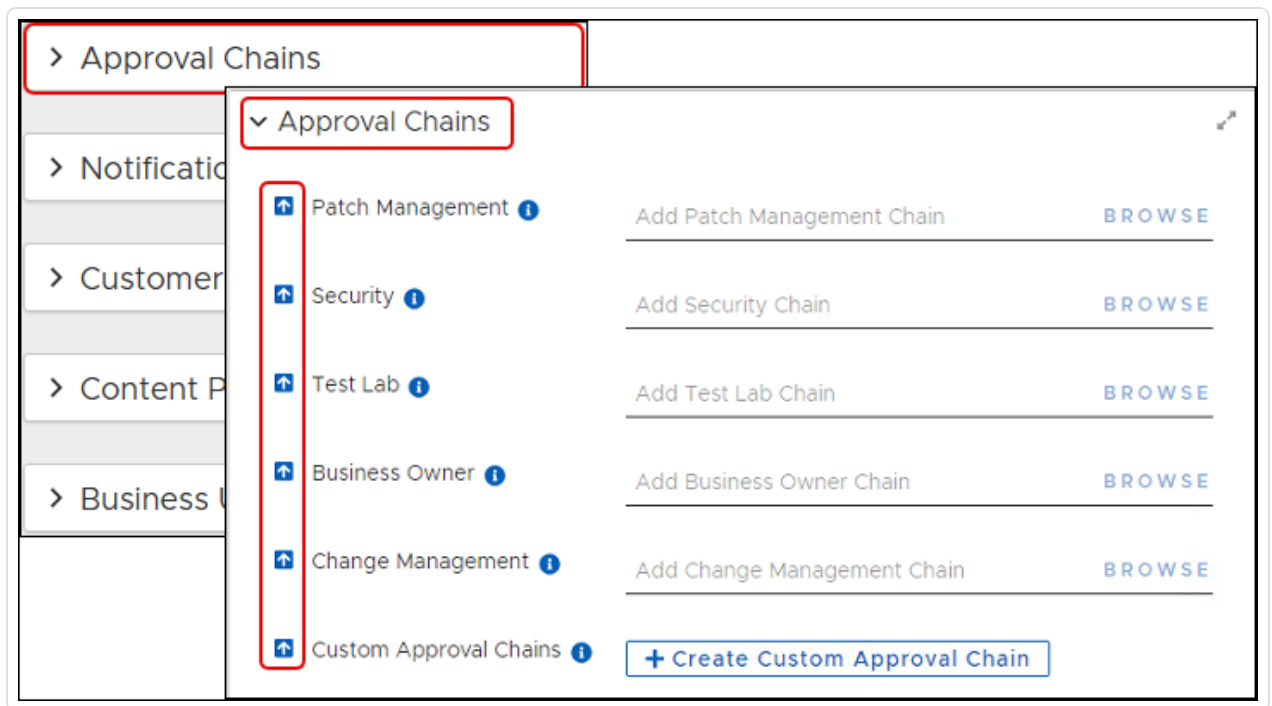
6. Select **Save** at the upper left to save your progress:

- a. Check the **Error View** and resolve any errors.
- b. Select **Save** again if you make any changes.

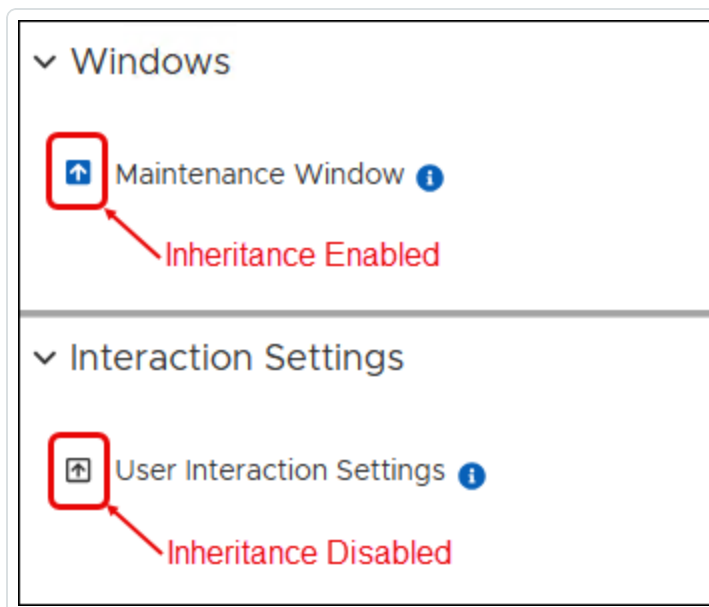
Add Approval Chains to a Business Unit

Adding Approval Chains to a Business Unit is an advanced feature. The Approval Chains fields allow advanced users to specify details for use in customized Patching Strategies, Deployment Chains, or Business Units when necessary to achieve different results.

1. In an open Business Unit template, click **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 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.

The screenshot shows a web interface titled "All Approval Chains". At the top right, there are buttons for "Show All" and "+ Create new Approval Chain". Below the title is a search bar with a "Search Columns..." dropdown and a "Search" button. The table below has a header row with "Name" and a sort icon. It contains two rows: "All Admins Approval Chain" and "Super Admin Approval Chain". The first row is selected, with a red box around its checkbox. At the bottom left, there are "OK" and "Cancel" buttons, with the "OK" button highlighted by a red box. The bottom right of the table shows pagination: "Rows Per Page: 10", "1 - 2 of 2", and a page number "1 / 1".

4. Select OK on the bottom left to return to the Approval Chains workspace.
5. Repeat Steps 2 through 4 for each of the groups listed in the Approval Chains workspace:
 - Skip any groups that do not apply to your situation.
 - When each group from which you need an approval contains an approval chain, continue with the next step.
6. Select **Save** at the upper left to save your progress:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.

Notification Chains

Using Notification Chains

Notification Chains send notifications to the administrator roles you specify to inform them about pending deployments. In addition to creating Notifications Chains here, you can also view and



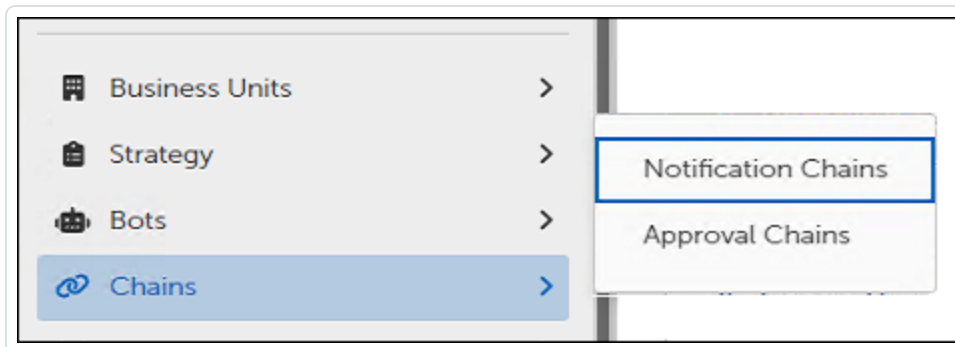
create them in object templates for Patching Strategies and Business Units (see [Managing Notification Settings](#), and for Deployment Channels (see something else).

Notification Chains allow administrators to specify who will receive notifications about patches and deployments and by what method, such as email, Teams, SMS text, or WhatsApp.

Name	Actions
All Admin Role	...

Open and Save a Notification Chain Template

1. Mouse over **Chains** or click the right arrow next to **Chains** in the left navigation menu of the [Patch dashboard](#), and then select **Notification Chains**.



2. Select the title of a template to open the template, and then save the template with a new title:
 - a. Select **More** in the upper-left corner of the dialog, and then select **Save As**.
 - b. Enter a new name for the template, and then click **Save as** on the lower-left corner of 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 corner of the dialog.

Manage Notification Chain Settings



Notification management configuration means identifying the Roles that require notification for the associated patches.

Each of these tasks assumes you have opened and saved a Notification Chain template and you are ready to complete the General Settings configuration.

▼ General Settings

Name *

All Admins Notification Chain

Description

Description

Roles To Notify ⓘ *

+ Add Roles

☐	...	Name	Actions
☐	⋮	> All Admin Role	...

Add Roles to Notify

Add existing Roles to a Notification Chain.

1. Scroll down to **Roles to Notify**. If a table appears, check to see whether the existing roles apply:
 - To remove a Role from the table, click the **ellipsis (...)** in the **Actions** column, and then click **Remove**.
 - To add Roles to the table, click **+ Add Roles**, and then continue with the next step.
2. Select one or more **Roles** from the Roles table, and then click **Add Roles** at the bottom left of the dialog.
3. Select **Save** to save your progress and check for errors:



- a. Check the **Error View** and resolve any errors.
- b. Select **Save** again if you make any changes.

Managing Notification Settings

Patching Strategy, Deployment Channel, and Business Unit objects include a **Notifications** dialog where you can configure notification details. The configuration choices differ slightly for each object.

Note: This configuration requires selecting a specific type of Notification Cycle template. Contact Tenable Patch Management Customer Support for assistance with this configuration and for information about choosing the correct template.

Add a Notification Chain

Notification Chain settings exist in the object templates for Patching Strategies, Deployment Channels, and Business Units.

1. Expand the **Notifications** box in an open object template to show the available configuration options.
2. Select **Browse** next to **Notification Chain**. This opens the Notifications Chain dialog.

Notification Chains		Show All	+ Create Notification Chain
Search Columns...		Search	
☐	Name	Actions	
☐	All Admins Notification Chain	...	
☒	Super Admin Notification Chain	...	

Rows Per Page: 10 1 - 2 of 2 1 / 1



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 .



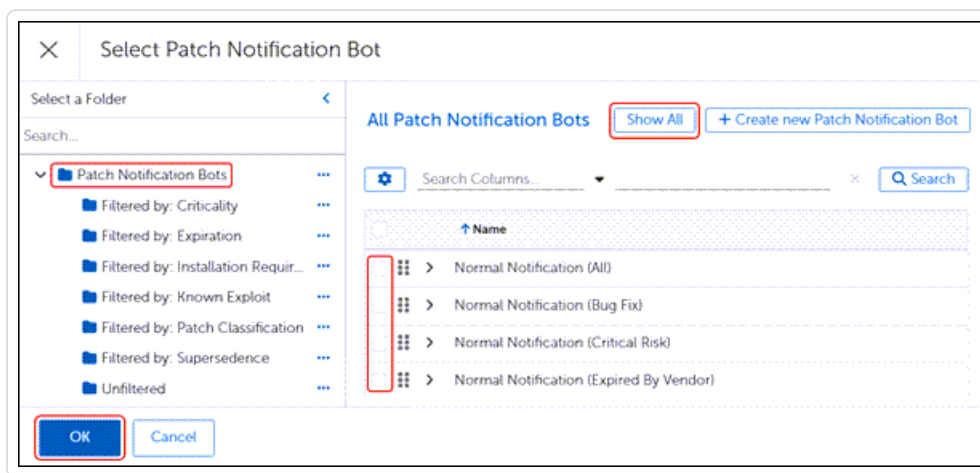
5. Continue editing the **Notification** settings or click OK on the bottom left corner to return to the template.

Add Patch Notification Bots

Both Patching Strategies and Deployment Channel templates have an option to Add Patch Notification Bots.

1. Select **+ Browse** next to Patch Notification Bots in the **Notifications** workspace of the object template.

This opens the Select Patch Notification Bots dialog.



2. Select  **Patch Notification Bots**, and then select **Show All** to list all available Patch Notification Bots or click any **Filtered by:** folder to see the Bots associated with that filter.
3. Choose one or more **Notification Bots** to set requirements for this template. To create more Notification Bots, see [Creating Notification Bots](#).
4. Select **OK** on the bottom left of the dialog to return to the starting template.

Create Notification Settings

Set Notification Urgency

These values must match the corresponding values defined in the Notification Bots. Otherwise, the Notification Cycle does not send a notification.



1. Select **+ Create Notification Setting** in the Notifications box of the object template.

The screenshot shows a 'Notifications' section with a dropdown arrow on the left. It contains three items: 'Notification Chain' with an information icon and a 'Browse' link; 'Patch Notification Bots' with an information icon and a '+ Browse' button; and 'Notification Settings' with an information icon and a '+ Create Notification Setting' button.

2. Expand the list of options next to **Notification Urgency**, and then select the urgency setting that matches the Notification Bot.

The screenshot shows the 'Create Notification Setting' dialog box. The 'Notification Urgency' dropdown is highlighted with a red box and set to 'Low'. Below it are 'Execution Schedules' with a '+ Add Schedules' button, 'Notify Patching Strategy Chains' and 'Notify Business Unit Chains' with toggle switches, and 'Notification Cycle Workflow' with an 'Add Workflow' link and a 'BROWSE' button. At the bottom, there is a 'Time Limit' section with input fields for '0' Hours, '0' Minutes, and '0' Seconds. The dialog has 'Create Notification Setting' and 'Cancel' buttons at the bottom left, and a 'Windows.' label at the bottom right.

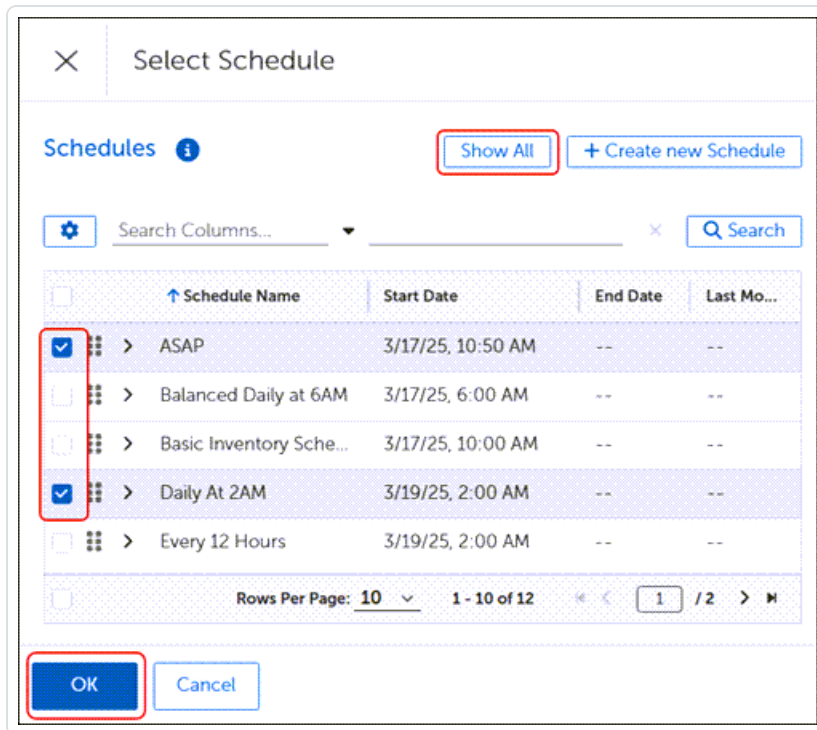
3. Continue editing the **Notification** settings or click Create Notification Settings to return to the template.

Add Execution Schedules

Execution Schedules control when and how often a Notification Cycle sends notifications. Choose schedules based on when and how often receiving parties require notification.



1. Select **+ Create Notification Setting** from the Notifications workspace of a object template.
2. Select **+Browse** next to Execution Schedules to display the available schedules.
3. Select one or more schedules from the All Schedules table, and then select **OK** on the lower-left corner of the dialog.



4. Continue editing the notification settings or click **Create Notification Settings** to return to the template.

Enable Notifications for Patching Strategy and Business Unit Chains

When enabled, sends notifications to the Roles shown in the Notification Chain associated with the Patching Strategy or Deployment Channel template. Defaults to disabled.

1. In the **+ Create Notification Setting** dialog in the Patching Strategy or Deployment Channel template, decide whether to enable notifications:
 - Select the **Notify Patching Strategy Chains** toggle to enable or disable (default) whether the notification cycle sends notifications to the chains included in the strategy.



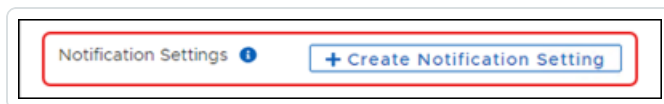
- Select the **Notify Business Unit Chains** toggle to enable or disable (default) whether the notification cycle sends notifications to Business Unit chains included in the strategy.
2. Continue editing the **Notifications** settings or click Create Notification Settings to return to the template.

Choose a Notification Cycle Workflow

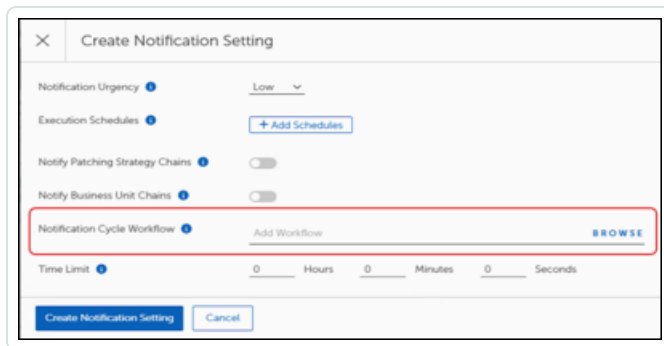
This setting names the Notification Cycle that processes the Notifications for the Patching Strategy or Deployment Channel. Notification Cycle workflows are customized for specific uses. Tenable Patch Management does not provide sample Notification Cycle templates. These templates exist only if you create them for your environment.

Note: Contact Tenable Patch Management Customer Support for assistance with Notification Cycle templates.

1. Select **+ Create Notification Setting** from the Notifications box in the object template.



This opens the Create Notification Setting dialog.



2. Select **Browse** on the **Add Workflow** line. This opens the list of available workflows.
3. Select your custom workflow from the list, and then click **Add Workflow** on the lower-left corner of the dialog.
4. Continue editing the **Notification** settings or click Create Notification Settings to return to the template.

Set the Time Limit



Specifies the maximum length of time that the Notification Cycle Workflow runs before timing out. If set to all zeros (default) the workflow may run indefinitely. Choose this setting with care. If the notification times out before sending all notifications, the next cycle triggers the notifications again.

1. Select **+ Create Notification Setting** the Notification box of the object template.
2. Next to Time Limit, set the **Hours**, **Minutes**, or **Seconds** that the Notification Cycle will run, or leave the setting default at 0 for each item to allow the workflow to run indefinitely.
3. Continue editing the **Notification** settings or click Create Notification Settings to return to the template.

Tenable Patch Management Enterprise

Table of Contents

[New in this Tenable Patch Management Release](#)

[Getting Started with Tenable Patch Management](#)

[Prerequisites](#)

[Supported Platforms and Distributions](#)

[Supported Browsers](#)

[Logs for Server and Client](#)

[Customer Support](#)

[Tenable Patch Management Admin Portal](#)

[Resolve Mozilla Firefox Active Directory Login Issue](#)

[Licensing Tenable Patch Management](#)

[Patch Management Dashboard](#)

[Integrate Tenable Vulnerability Manager](#)

[Minimum User Role Requirements for APIs](#)

[Add Tenable Access Settings to Tenable Patch Management](#)

[Administrators and Roles](#)

[Administrators and Roles](#)

[Access Security Settings](#)

[View Administrators](#)



[Create a New Administrator](#)

[Create a Microsoft Teams Webhook URL](#)

[View Roles](#)

[Create a New Role](#)

[Introduction to Patching Strategies](#)

[Patching Strategy Use Case](#)

[Open and Save a Patching Strategy Template](#)

[Configure Deployment Settings](#)

[Add Software Products](#)

[Enable the Patching Strategy](#)

[View a Staged Patching Strategy](#)

[Start the Patching Strategy Manually](#)

[Optional Objects in Patching Strategy Templates](#)

[Organize New Patch Objects](#)

[Create a New Folder for Objects](#)

[Move an Object Template Between Folders](#)

[Menu Objects for Tenable Patch Management](#)

[Business Units and Rollout Processes](#)

[Business Units](#)

[Rollout Processes](#)

[Patching Strategies](#)

[Purpose of a Patching Strategy](#)

[View built-in Patching Strategies](#)

[Patching Strategy Templates](#)

[Creating a Patching Strategy](#)

[View a Staged Patching Strategy](#)

[Start the Patching Strategy Manually](#)

[Managing Enabled Patching Strategies](#)

[Delete an Enabled Patching Strategy](#)

[Submit Patches to an Enabled Patching Strategy](#)



[Approvals for Adding Patches](#)
[Resubmit an Enabled Strategy](#)

[Patching Processes](#)

[Creating Patching Processes](#)
[Patching Process Templates](#)

[Bots - Patch Deployment and Notification Bots](#)

[Deployment Bots](#)
[Notification Bots](#)

[Chains](#)

[Approval Chains](#)
[Notification Chains](#)

[Deployment Channels and Deployment Channel Processes](#)

[Deployment Channels](#)
[Deployment Channel Processes](#)

[Deployment Waves](#)

[Using Deployment Waves](#)
[Open and Save a Deployment Wave Template](#)
[Add a Deployment Wave Entry](#)
[Create a Wave Entry](#)
[Edit or Remove a Wave Entry](#)

[Maintenance Windows](#)

[Open and Save a Maintenance Window Template](#)
[Dynamic Settings](#)
[Add Dynamic Detection Workflow \(Optional\)](#)
[Maintenance Windows by Urgency](#)
[Apply a Maintenance Window to All Urgencies](#)
[Save and Deploy the Maintenance Window](#)

[Communication Providers](#)



[Using Communication Providers](#)

[Open and Save a Communication Provider Template](#)

[User Interaction Settings](#)

[Open and Save a User Interaction Template](#)

[Choose Urgency Settings](#)

[Configure Deployment Notification Settings](#)

[Reboot Notification Settings](#)

[Managing Snooze Settings](#)

[Configure Snooze Settings](#)

[Save and Deploy User Interaction Settings](#)

[Customized Products](#)

[Manage Settings for Customized Products](#)

[Patch Content](#)

[Schedules](#)

[View Available Schedules](#)

[Create a Custom Schedule](#)

[Patching Analytics Dashboards](#)

[Using Search in Tenable Patch Management](#)

[Patching Analytics Overview](#)

[Products View](#)

[Patches View](#)

[Devices View](#)

[Flex Controls](#)

[Blocklisting](#)

[Cycle Operations](#)

[Patching Exceptions](#)

[Global Pause](#)

[Rollbacks Overview](#)

[Approval Requests](#)



[Approve or Reject a Patch Request](#)

[Risk Assessment Settings](#)

[Risk Score Settings](#)

[Custom Risk Settings](#)

[Content Prestaging Settings](#)

[Defining Content Prestaging Settings](#)

[Set Content Prestaging Settings](#)

[Customer Extension Data](#)

[Navigating the Tenable Patch Management Dashboard](#)

[Date Settings, Export, and Refresh](#)

[Tenable Patch Management Patch Menus](#)

[Tenable Patch Management Dashboard and Performance Widgets](#)

[Appendices](#)

[Software Products](#)

[Endpoint Scans](#)

Organize New Patch Objects

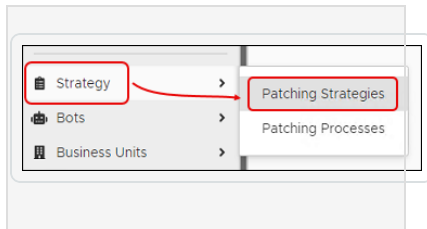
Throughout your patch management journey, you will customize object templates to meet the needs of your business environment. Tenable Patch Management recommends setting up your own folder to hold object templates that you customize or create, to keep them separate from those provided by Tenable Patch Management.

Create a New Folder for Objects

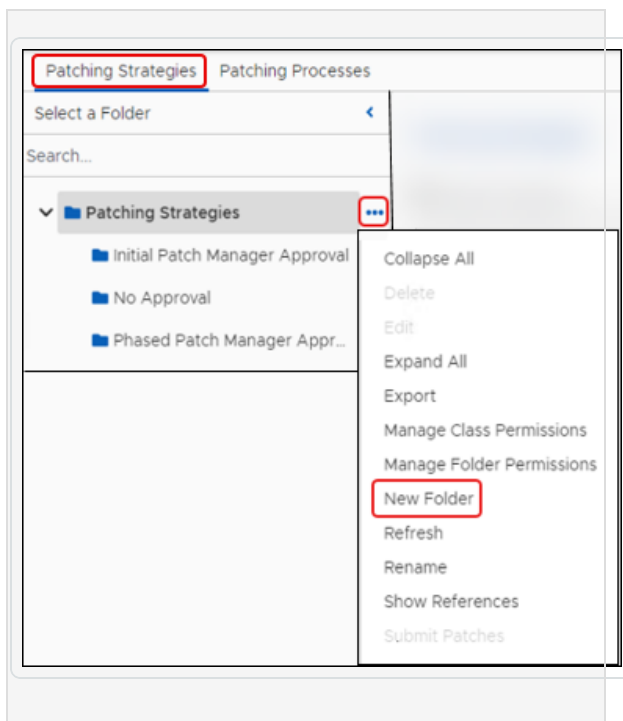
When creating new templates for most objects, or when customizing (save as) existing templates, create a location under each object to hold your templates separately from those provided by Tenable Patch Management.



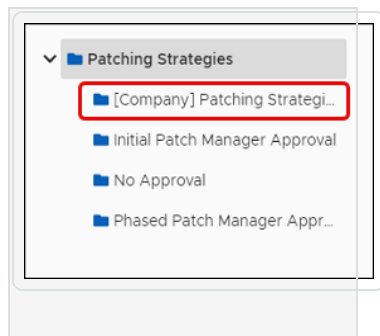
1. Select an object on the left navigation menu of the Tenable Patch Management dashboard.
This example uses **Strategy > Patching Strategies**.



2. Create a new folder to hold your Patching Strategies:
 - a. Select the **ellipsis (...)** to the right of the Patching Strategies Folder, and then select **New Folder**.



- b. Enter a descriptive **Name** for the folder, and then click **OK** on the bottom-left corner of the dialog.
 - This creates the new folder structure showing both your folder and the Patching Strategies folder.

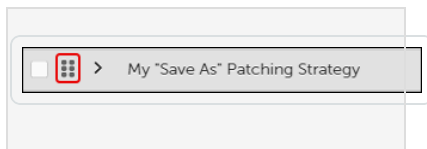


- When you create new strategies or modify existing strategies, move them to your folder location (see [Move an Object Template Between Folders](#)).

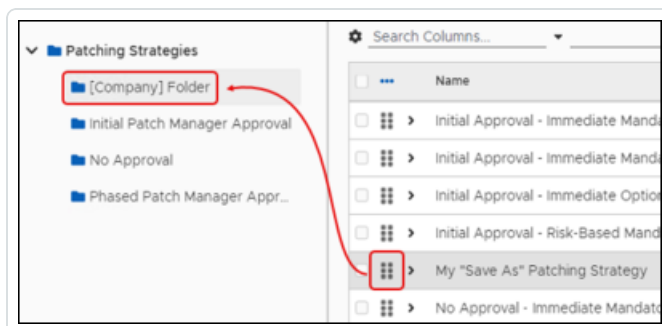
Move an Object Template Between Folders

After [creating a new folder](#) to hold your object templates, use the following procedure to move saved templates from one folder to another. This example uses **Strategy > Patching Strategies**.

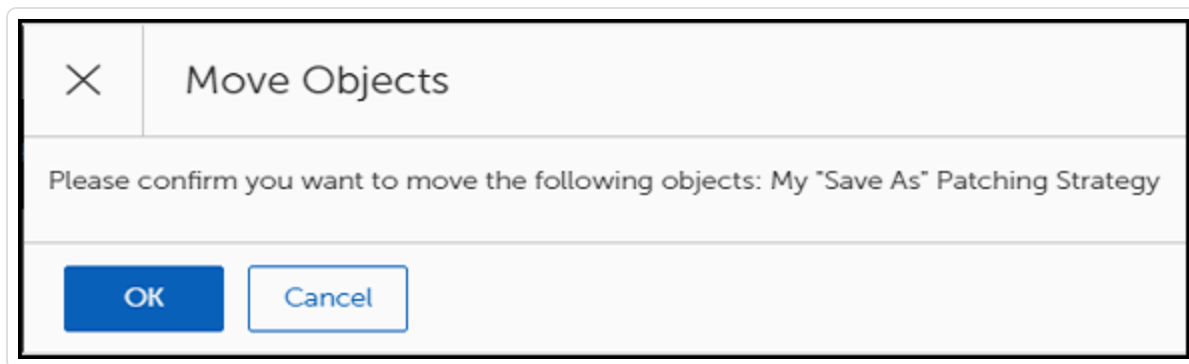
1. Select and hold the **stacked icon** next to the template you want to drag and drop to the new folder.



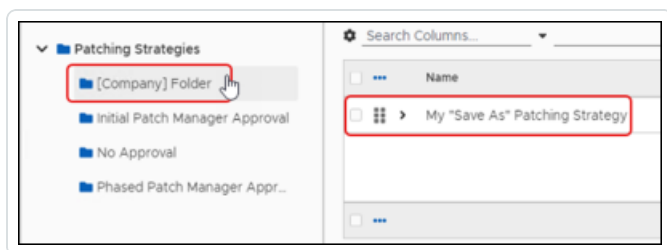
2. Drag the **stacked icon** over the folder, and then release it.



This opens the **Move Objects** dialog.



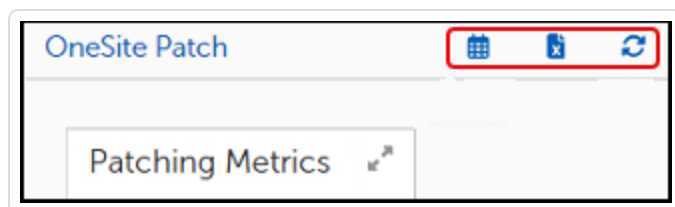
3. Select **OK** to confirm the move.
4. Select the designated folder to view its content and verify that the list includes the template you moved.



Navigating the Tenable Patch Management Dashboard

Date Settings, Export, and Refresh

The three small icons (Calendar, Export and Refresh) on the upper right of the Tenable Patch Management Home page and on any of the Patching Analytics pages (Overview, Products, Patches, or Devices) provide options to customize the date settings to a particular date range, choose some or all widgets on the page for exporting data, and refresh the data shown on the page.

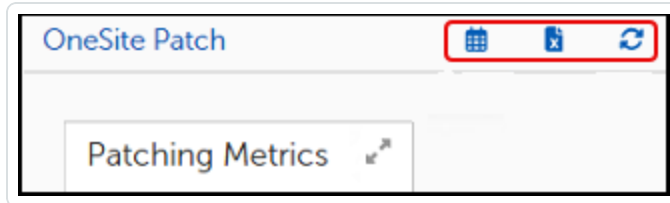


Set Dates for Status Views



The dashboard Date Settings default to the current day. Use the following steps to change the date settings:

1. Select  on the upper-right corner of the Home page or from any Patching Analytics page.



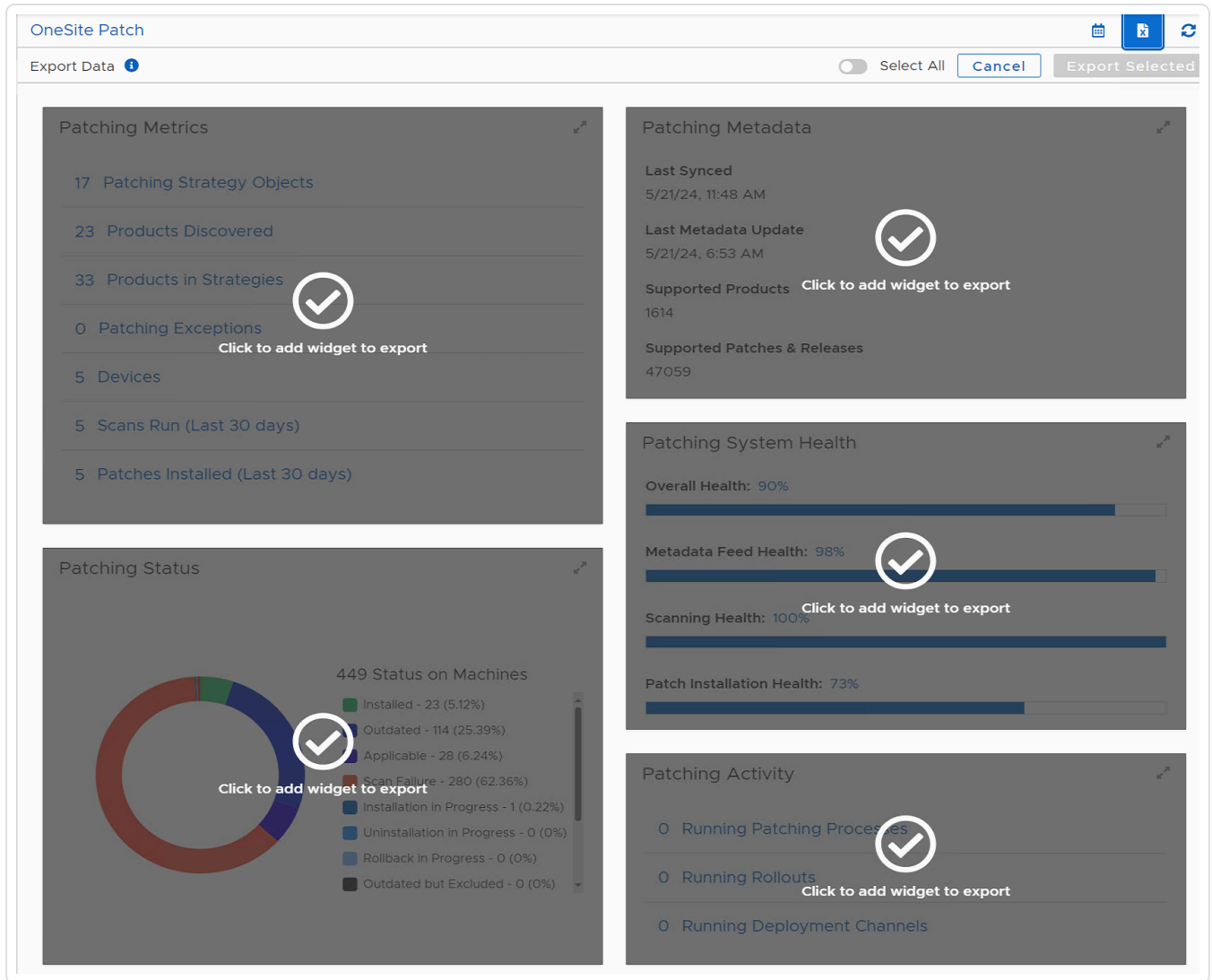
2. Enter the **starting and ending dates** for the range you want to view or use the calendar icon to the right of each date field to choose a date from the calendar.

3. Select the **Window Type** setting, and then select whether to view data by **Day**, **Week**, **Month**, **Quarter**, or **Year** from the dropdown menu.
4. Select **Update** to save the settings. The view details update automatically for the date range you entered.

Export Widget Data



1. Select the Export icon  on the upper-right corner of the Home page or on any Patching Analytics page. This changes the view to an Export Data page, which highlights in gray the widgets you can export.



OneSite Patch

Export Data

Select All Cancel Export Selected

Patching Metrics

- 17 Patching Strategy Objects
- 23 Products Discovered
- 33 Products in Strategies
- 0 Patching Exceptions
- 5 Devices
- 5 Scans Run (Last 30 days)
- 5 Patches Installed (Last 30 days)

Patching Metadata

- Last Synced: 5/21/24, 11:48 AM
- Last Metadata Update: 5/21/24, 6:53 AM
- Supported Products: 1614
- Supported Patches & Releases: 47059

Patching System Health

- Overall Health: 90%
- Metadata Feed Health: 98%
- Scanning Health: 100%
- Patch Installation Health: 73%

Patching Activity

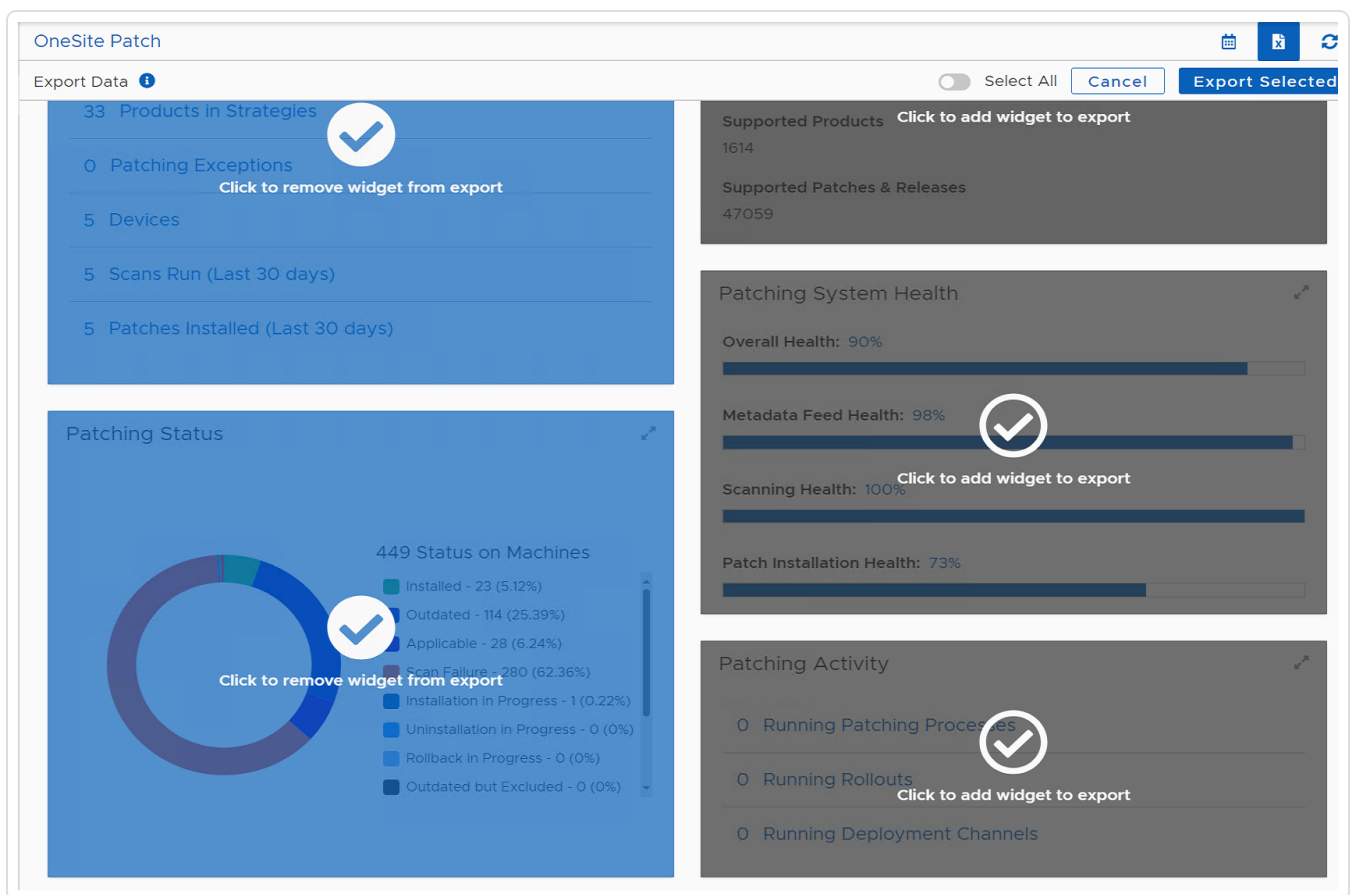
- Running Patching Processes
- Running Rollouts
- Running Deployment Channels

Patching Status

449 Status on Machines

- Installed - 23 (5.12%)
- Outdated - 114 (25.39%)
- Applicable - 28 (6.24%)
- Scan Failure - 280 (62.36%)
- Installation In Progress - 1 (0.22%)
- Uninstallation In Progress - 0 (0%)
- Rollback In Progress - 0 (0%)
- Outdated but Excluded - 0 (0%)

2. Choose which widgets to export:
 - Select **Select All** at the top of the page to export all widgets.
 - Select an individual widget to export a single widget, or click multiple widgets to export.



3. Select **Export Selected** on the upper-right corner. The system downloads the export to the server with an .xlsx extension.

Refresh the Status View

Select the Refresh icon  on the upper-right corner of the Home page or on any Patching Analytics page. This refreshes the data on the status pages to reflect the most current information if your customized date range includes the current date.

Tenable Patch Management Patch Menus

The left navigation menu lists the object available for configuring or monitoring in the Tenable Patch Management product. Those items with additional choices include a pop-out menu indicated by a right-angle bracket (>).

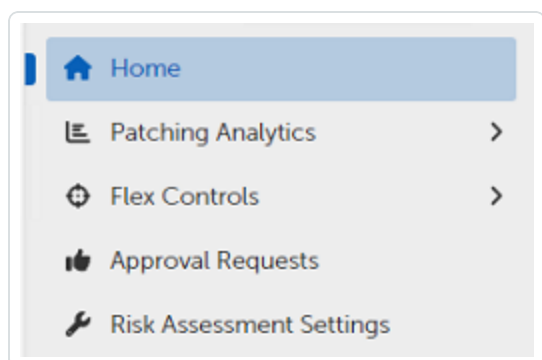
The left pane stays the same, regardless of which object you choose, and consists of three sections.

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 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 Tenable Patch Management , 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

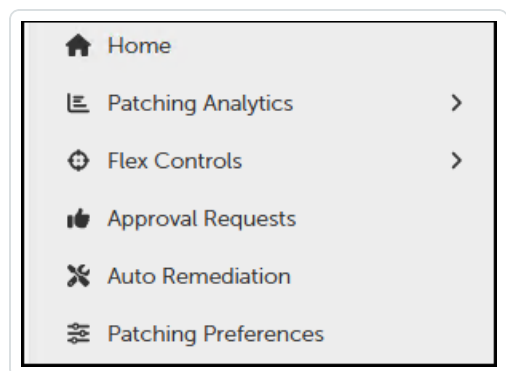
Object	Purpose
Home	Opens the Home page to view the overall status, metric, and compliance for patching in your environment. See Tenable Patch Management EnterpriseDashboard and Performance Widgets .
Patching Analytics	Shows the status of patches and products in the environment. Change tabs to view metrics 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	View all approval requests and check the status of pending and completed



Object	Purpose
Requests	.
Risk Assessment Settings	Customize risk calculations and display risks in other dashboards. See Risk Assessment Settings .

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 Tenable Patch Management functionality.



From any location within Tenable Patch Management , 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

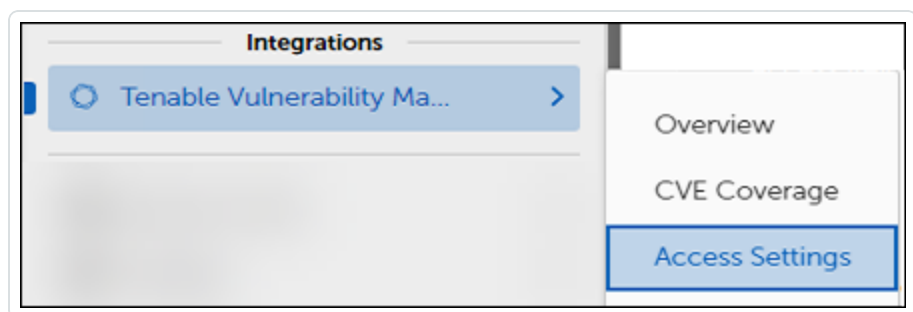
Object	Purpose
Home	Opens the Home page to view the overall status, metric, and compliance for patching in your environment. See Tenable Patch Management EnterpriseDashboard and Performance Widgets .
Patching Analytics	Shows the status of patches and products in the environment. Change tabs to view metrics for Products, Patches, or Devices. See Patching Analytics Dashboards . Sub menus include Overview, Products, Patches, and Devices.



Object	Purpose
Flex Controls	Review and manage settings for Blocklisting, Exceptions, Global Pause, and Rollbacks. Review Patching Cycle statistics (Cycle Operations), and view both running and historic cycles for Patching, Deployment, and Rollout. For details on each selection, see Flex Controls
Approval Requests	View all approval requests and check the status of pending and completed requests. See Approval Requests .
Auto Remediation	Use this menu to enable and configure Auto Remediation details for security issues based on level of criticality (Critical, High, Medium, Low). Configure and test production deployment settings.
Patching Preferences	Create patching preferences based on target Business Unit including assignment of a Maintenance Window and User Interaction settings.

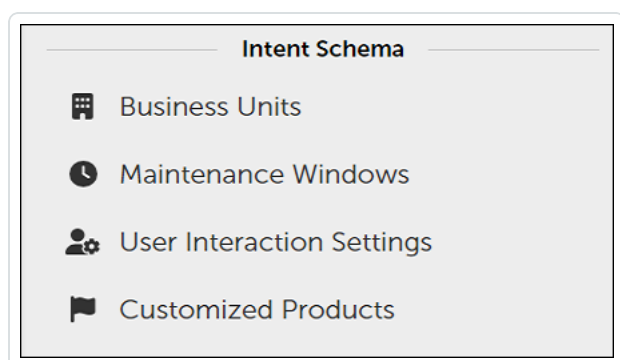
Integration Menu

The Integrations menu provides access to available integrations based on licensing.



Intent Schema Menu

The Intent Schema Menu refers to the menu items administrators use to customize and manage patching policies for Business Units.

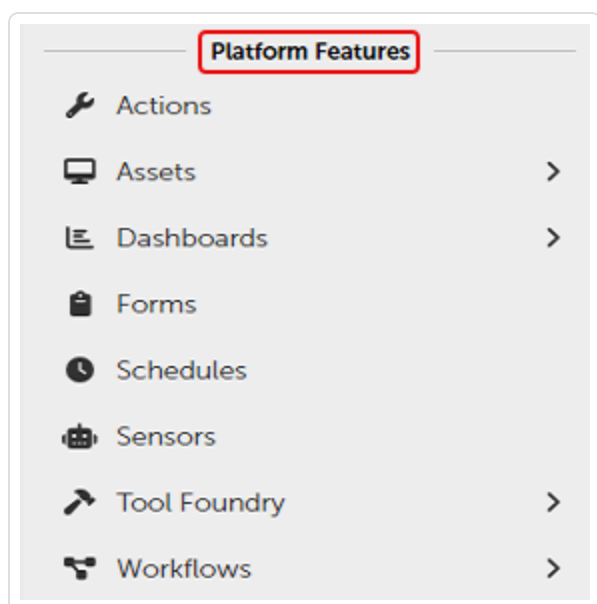


Intent Schema Object Descriptions

Object	Purpose
Business Units	Logically group and manage devices, settings, and other resources within a hierarchy. See Business Units
Maintenance Windows	Define maintenance and reboot windows. Primarily associated with Business Unit configurations. See Maintenance Windows .
User Interaction Settings	Control what the endpoint user sees and what options they have for interacting with patching notifications and required reboots. See User Interaction Settings .
Customized Products	Customization of installation for products with specific actions needed, such as license key entry or custom installation locations, before or after an installation. See Customized Products .

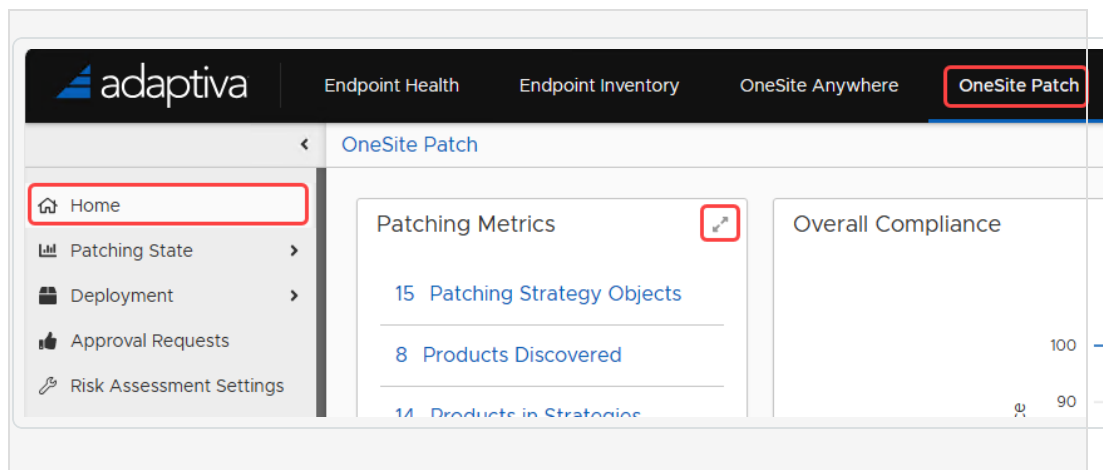
Platform Features Menu

These are common features available from every menu in Tenable Patch Management.



Tenable Patch Management Dashboard and Performance Widgets

The Tenable Patch Management Home page shows several widgets that provide patching details for the environment. You can expand each widget to a full page using the  icon at the upper-right corner of each widget.



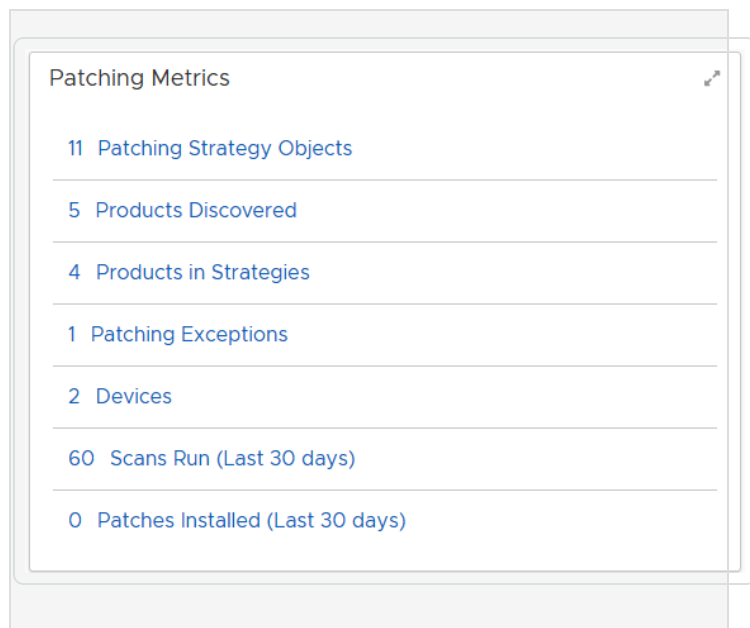
The layout of these widgets depends on the size of your computer monitor.

Collectively, these widgets supply information about the overall state of patches in your environment based on Tenable Patch Management system scans. The Patching Analytics menus show more detail about specific products, patches, and devices.

Patching Metrics

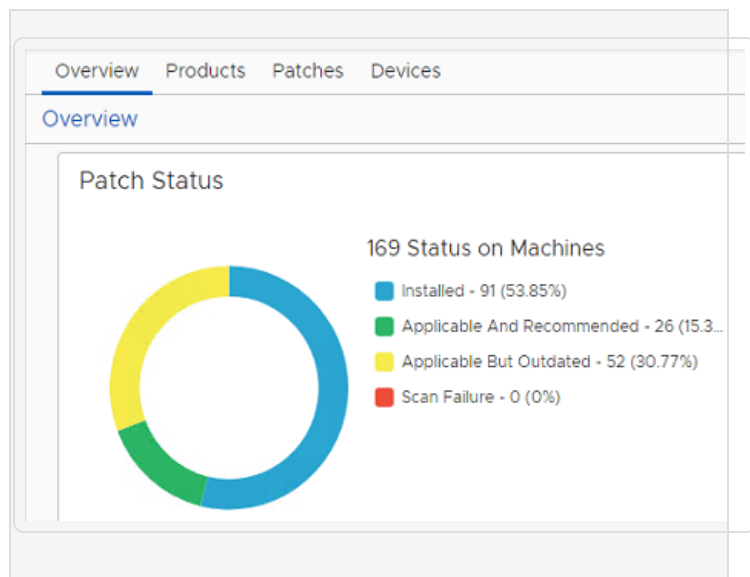


Accessed from the Home screen, Patching Metrics show basic patch related information specific to your environment based on scanning requirements. Details include a quantitative summary of the item within the environment. Each item links to the **Patching Analytics Overview**, which includes a separate and detailed view for Products, Patches, or Devices.



Patching Status

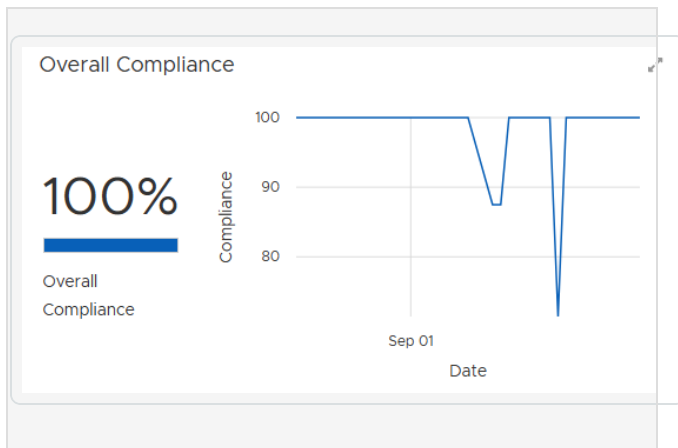
Provides an aggregate view of patching statuses reported in the environment including the combined total of statuses from all machines. The percentages that follow show what percentage of the reported statuses fall into each category.



Overall Compliance

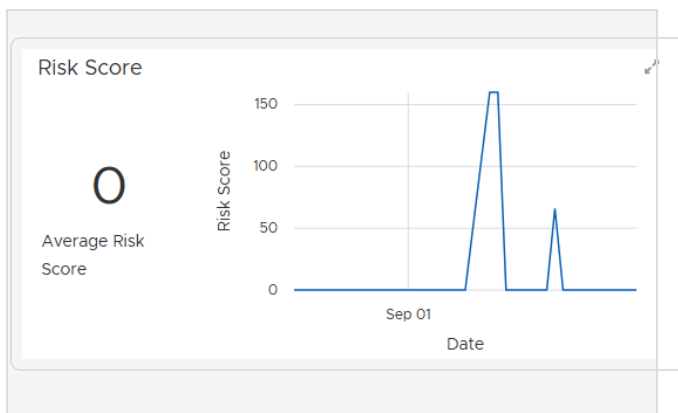


Graphs the overall compliance of devices in the environment with the patch requirements.



Risk Score

Returns the average risk score for all products identified in the metadata, and shows the average Risk Score. Depending on the dates chosen for the dashboard reporting, the administrator can see the changes in risk over time. See [Date Settings for Status Views](#) for more information.



The average number reported here reflects a customized risk assessment for each product based on patch status, applicability, and weight of risk. See [Risk Assessment Settings](#) for more information.

Patching Metadata

Summarizes the status of the latest endpoint scans and client product inventory updates. Metadata includes details about the products, patches, and updates approved by the company for installation. The Patch Metadata summary tells the administrator when the Tenable Patch Management and Tenable Patch Management last synchronized with the Metadata Server and when the last sync resulted in an update to the clients.

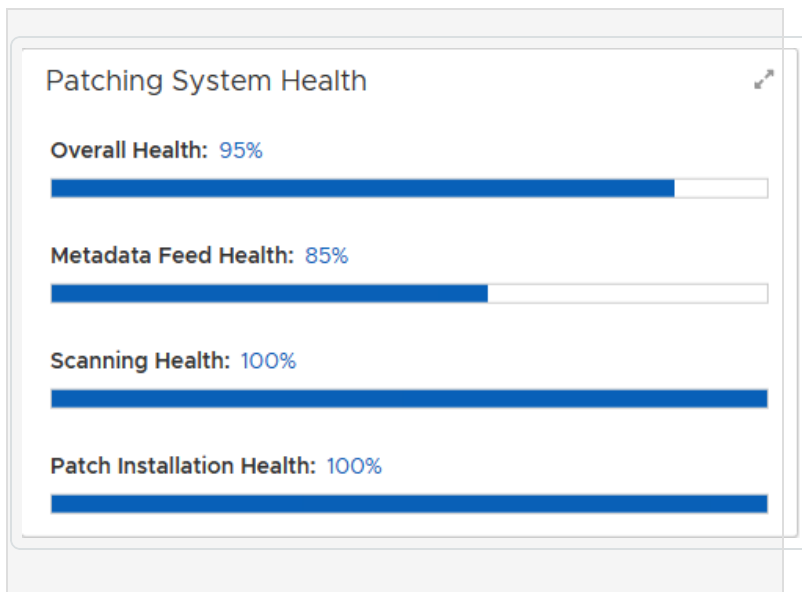


Patching Metadata	
Last Synced	9/29/23, 2:16 PM
Last Metadata Update	9/26/23, 7:06 AM
Supported Products	818
Supported Patches & Releases	18670

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

☐ ...	Product Name	Compliance Status	Actions
☐	Microsoft Analysis Services OLE DB Provider ...	0%	...
☐	Microsoft Orca	0%	...
☐	Microsoft Visual C++ 2015-2022 Redistribut...	0%	...
☐	Microsoft Visual C++ 2015-2022 Redistribut...	0%	...
☐	SQL Server Management Studio x64	0%	...
☐ ...	Rows Per Page: 1 - 5 of 5 1 / 1		

Top 5 Missing Patches

Displays the most critical patches contributing to the Risk Score and by what percentage (highest to lowest). Scanning compares the risk score of missing patches and reports these top five as those contributing most to the [Risk Score](#).



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.

Introduction to Patching Strategies

Creating a Patching Strategy is a great way to start using Tenable Patch Management . Start with a common scenario, and then build a Patching Strategy to distribute a patch to active clients.

Patching Strategy Use Case

An administrator wants to build a Patching Strategy to update devices every day based on devices that have the following characteristics:

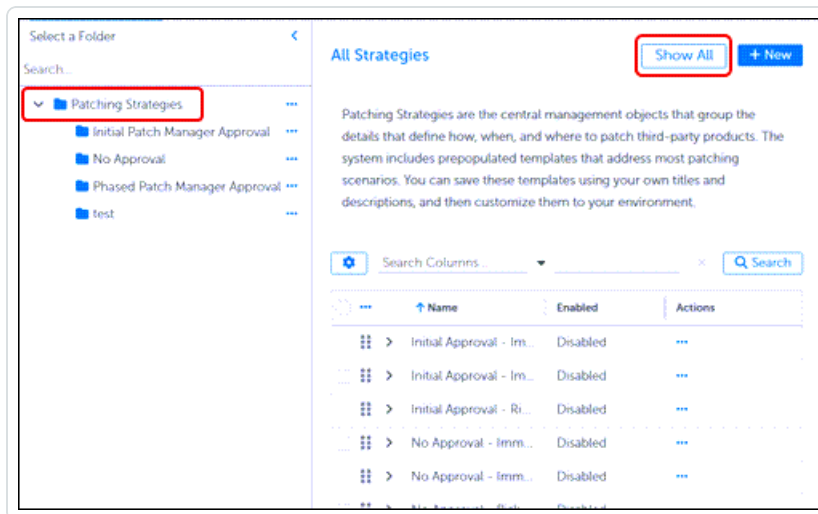
- Company wide (all Clients).
- Within a Tenable Business Unit.
- Running a version of Google Chrome Enterprise other than the internally approved version.
- Initial approval needed.
- Immediate, mandatory update to approved version.

Open and Save a Patching Strategy Template



1. Follow the instructions in [Create a New Folder for Objects](#).
2. Hover over or click **Strategy** in the left navigation menu of the [Patch Management Dashboard](#), and then select **Patching Strategies**.

3. Select  **Patching Strategies**, and then select **Show All** to see all available Patching Strategies.



For descriptions of each template type, see [Patching Strategy Templates](#).

4. Select the **Name** of a strategy to open it.
5. Select **More** in the upper left corner of the template, and then select **Save As**:
 - a. Enter a unique name that reflects what the strategy does conceptually. For example, ITS Immediate Daily Product Patching.
 - b. Select **Save as** on the bottom left corner of the dialog. This opens your strategy template with all the default entries for the built-in strategy, including a detailed description.
 - c. Enter a detailed **Description** of your new template or keep the existing detail, and then click **Save** on the upper-left corner of the dialog.

Tip: Remember to click **Save** on the upper left corner to save your progress as you make changes. After completing the Patching Strategy configuration, you must save and enable the completed strategy to make it available for use.

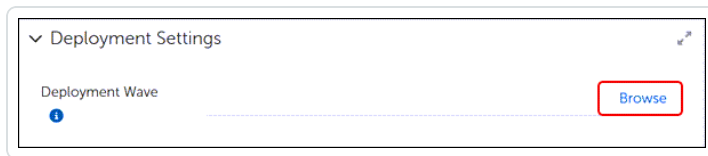
Configure Deployment Settings



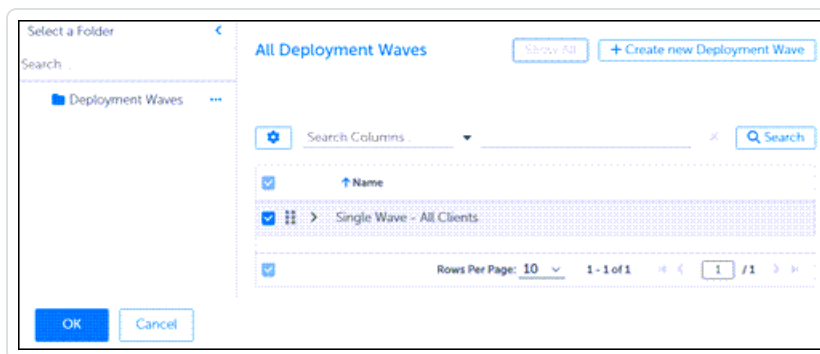
Deployment Settings for quick start purposes include selecting a built-in Deployment Wave, which already includes a Business Unit. For details on Deployment Waves, see [Deployment Waves](#). When customizing an existing template, process and deployment fields may include tables with existing configuration selections.

Add a Deployment Wave

1. Select **Browse** next to Deployment Wave in the Deployment Settings workspace of an open [Patching Strategy](#) template.



This opens the **All Deployment Wave** dialog.



2. Select a **Deployment Wave** from the list.
 - Tenable Patch Management provides a **Single Wave-All Clients** Deployment Wave, which includes a Business Unit called **All Clients Business Unit**.
 - If you are following the tasks in **Introduction to Patching Strategies**, choose **Single Wave-All Clients**.
3. Select **OK** on the bottom left of the dialog to return to the Patching Strategy.



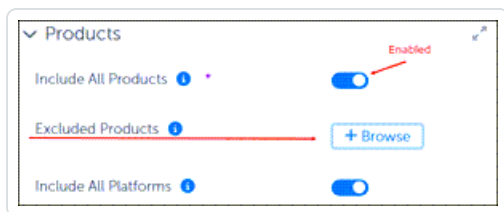
Important

When updating an existing Patching Strategy with a new Deployment Wave, the system prompts you with a recommendation to specify Business Unit Addition Settings.

4. Select **OK** to close the recommendation. The system returns you to the Patching Strategy at the Business Unit Addition Settings workspace:
 - If you are following the tasks in **Introduction to Patching Strategies**, skip to [Add Software Products](#). There is no need to modify the Deployment Bot Runtime settings for purposes of this exercise.
 - If you are creating or modifying a Patching Strategy for ongoing use, continue with the next step.
5. Choose whether to specify Business Unit Addition Settings (recommended), if prompted by the system.
 - To continue with Deployment Settings, see [Deployment Bot Runtime Settings](#). You may configure Business Unit Addition Settings later in the template.
 - To complete Business Unit Addition Settings now, see [Business Unit Addition Settings](#).

Add Software Products

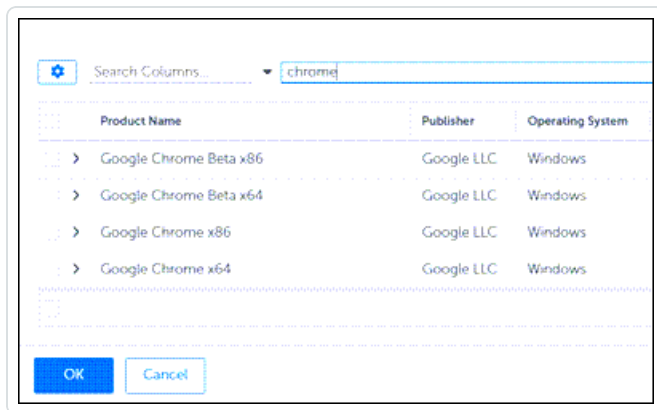
1. Select **+ Browse** in the **Products** workspace of an open [Patching Strategy](#) template. The following image shows the default settings for this dialog.



2. Select the **Include All Products** toggle to disable inclusion of all products. This changes the next item to Included Products.



3. Select **Browse** to open the Select Software Product dialog.
4. Enter **Chrome** on the search line, and then click **Search**.
5. Select **Google Chrome x64**, and then click **OK** on the lower-left corner of the dialog.



6. Scroll up to **General Settings** to enable the strategy.

Enable the Patching Strategy

After completing the Patching Strategy configuration, including [Add Software Products](#), you must enable the Patching Strategy. When enabled, the strategy runs according to the configured schedules.

1. In **General Settings** at the top of the Patching Strategy template, click the **Strategy Enabled** toggle to enable the strategy and make it available for use.

Save More ▾

▼ General Settings

Name *

Description

Strategy Enabled ☒

2. Select **Save** on the upper-left corner of the workflow to save the strategy:
 - a. Check the **Error View** and resolve any errors.
 - b. Select **Save** again if you make any changes.
3. [Move the saved template to your folder](#) .

View a Staged Patching Strategy

After you [Enable the Patching Strategy](#), you can view the pending approval request.

1. Select the **Approval Requests** in the left navigation menu of the [Patch Management Dashboard](#).

My Requests All Requests

Approval Requests

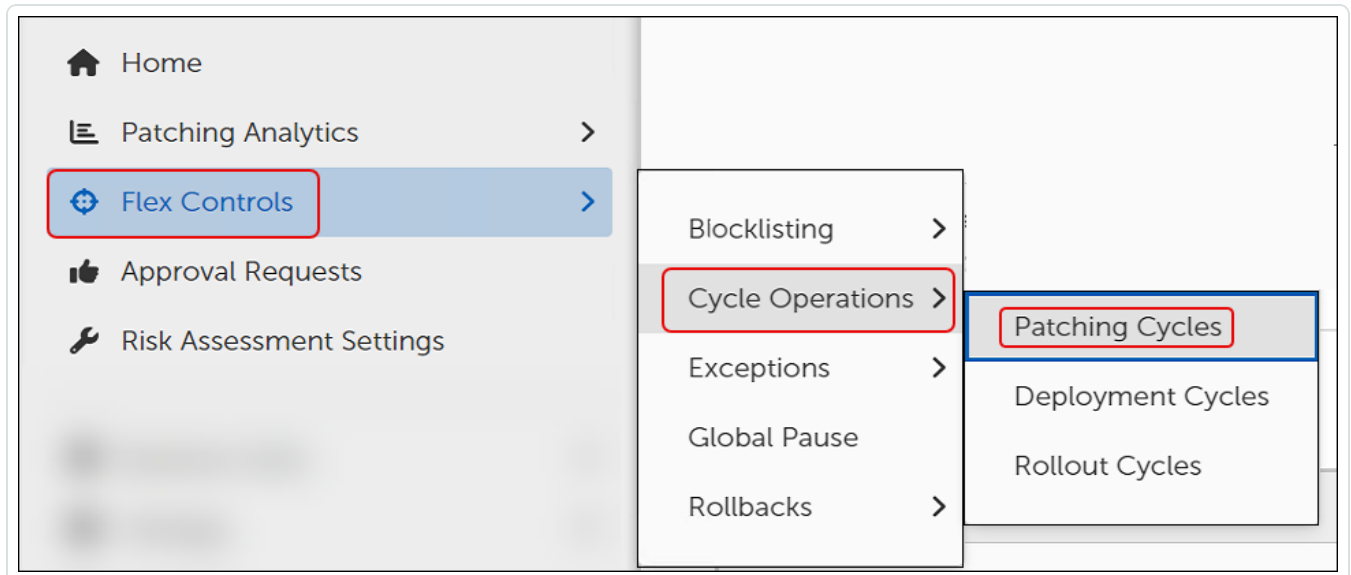
All Pending Completed

Search Columns...

Approval Summary	Request Send Time ↓
▶ Patching Process Approval	4/10/24, 1:07 AM

- The view defaults to All requests, which includes pending and completed.
- The Patching Strategy you just enabled appears in the Approval Summary table with a Request Status of In Progress and Awaiting Response.

2. Select **Flex Controls > Cycle Operations > Patching Cycles** from the left navigation menu of the [Patch Management Dashboard](#).



3. Check the **Running Patch Processes** table, which lists the status of the Patching Strategy as Waiting.

Patching Strategy	Status	Business Units	Start Time ↓
964 patching strategy	Waiting	All Clients Business Unit	4/19/24, 11:00 AM

4. Select **Approval Requests** in the left navigation menu, and then click the **Patching Strategy** in the table.
5. Select **Approve**, and then click **Back to Approval Requests**. You can wait until the patch time passes, or you can start the deployment manually.



Note: When you add a new endpoint device to your network after this strategy has scanned and updated all associated devices, Tenable Patch Management automatically adds any new devices to the strategy if the next scan detects an earlier version of Chrome.

Start the Patching Strategy Manually

After the Patching Strategy approval process status shows Completed, you can wait until the time setting for patch deployment, or you can start the deployment immediately.

1. Select **Flex Controls > Patching Cycles**, and then click the name of the Patching Strategy to open the Cycle Information.

The screenshot shows a table titled 'Running Patch Processes'. It has a search bar at the top with a 'Search Columns...' dropdown and a 'Search' button. The table has four columns: 'Patching Strategy', 'Status', 'Business Units', and 'Start Time'. The 'Status' column is highlighted with a red box. The table contains one row with the following data: '964 patching strategy', 'Waiting', 'All Clients Business Unit', and '4/19/24, 11:00 AM'. At the bottom, there is a pagination bar showing 'Rows Per Page: 10', '1 - 1 of 1', and a page number '1 / 1'.

Patching Strategy	Status	Business Units	Start Time
964 patching strategy	Waiting	All Clients Business Unit	4/19/24, 11:00 AM

2. Select Play  under Cycle Information, and then click **Close**. This returns you to the Patching Cycles workspace where you can view Running Patch Processes.

The screenshot shows the same 'Running Patch Processes' table as before, but the 'Status' column now shows 'In Progress' instead of 'Waiting'. The 'Status' column is still highlighted with a red box. The other data in the table remains the same: '964 patching strategy', 'All Clients Business Unit', and '4/18/24, 1:24 PM'. The pagination bar at the bottom shows 'Rows Per Page: 10', '1 - 1 of 1', and '1 / 1'.

Patching Strategy	Status	Business Units	Start Time
964 patching strategy	In Progress	All Clients Business Unit	4/18/24, 1:24 PM

3. Select the **Patching Strategy** name to view details about the patching process.

Optional Objects in Patching Strategy Templates

The exercise in [Introduction to Patching Strategies](#) uses the minimum requirements for a Patching Strategy.



Additional settings in the Patching Strategy template include those listed below, though you do not need them for quick start purposes. [Creating a Patching Strategy](#) documents the configuration steps.

- [Chains](#)(Approval and Notification)
- [Customer Extension Data](#)
- [Content Prestaging Settings](#)
- [Business Unit Addition Settings](#)

> Approval Chains

> Notifications

> Customer Extension Data

> Content Prestaging Settings

> Business Unit Addition Settings

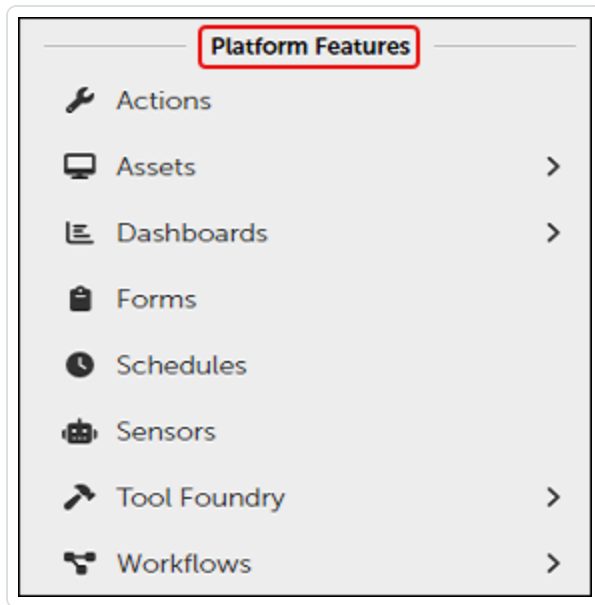
Schedules

Tenable Patch Management uses schedules throughout the product to automate patching processes that include content push, updating custom groups, setting maintenance windows, and more. Tenable Patch Management provides several default schedules you can customize for your environment, or you can create new schedules.

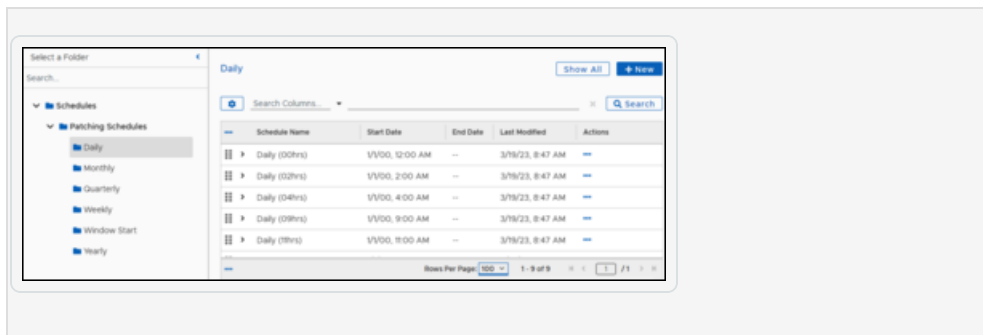
View Available Schedules



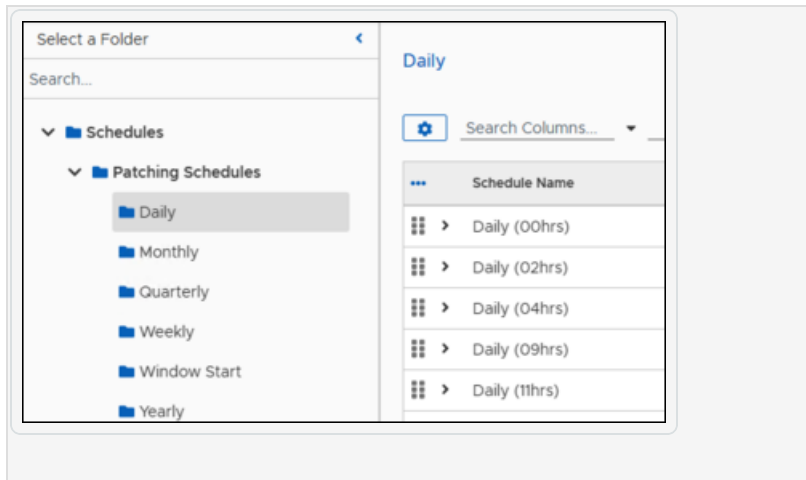
1. Select **Schedules** in the Platform Features menu of the [Patch Management Dashboard](#).



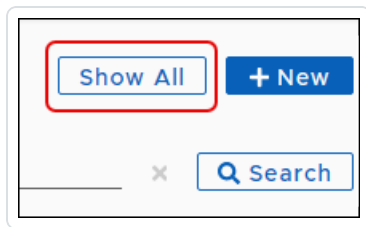
This opens the list of available schedules.



2. Choose how you want to view schedules:
 - Select one of the **Patching Schedule** folders listed in the left navigation pane. These choices list the available schedules for each category.
 - Select the **Schedule Name** to open it and view the details.



3. Select **Show All** at the upper right to view all available schedules. This list contains over 100 available schedules.



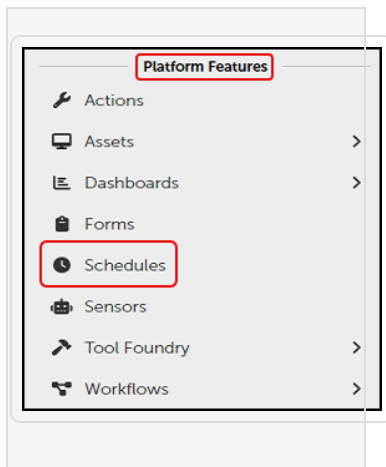
Create a Custom Schedule

This example customizes an existing schedule template. You can also create a new schedule template under **+ New**. The template layout for either includes the same choices and fields.

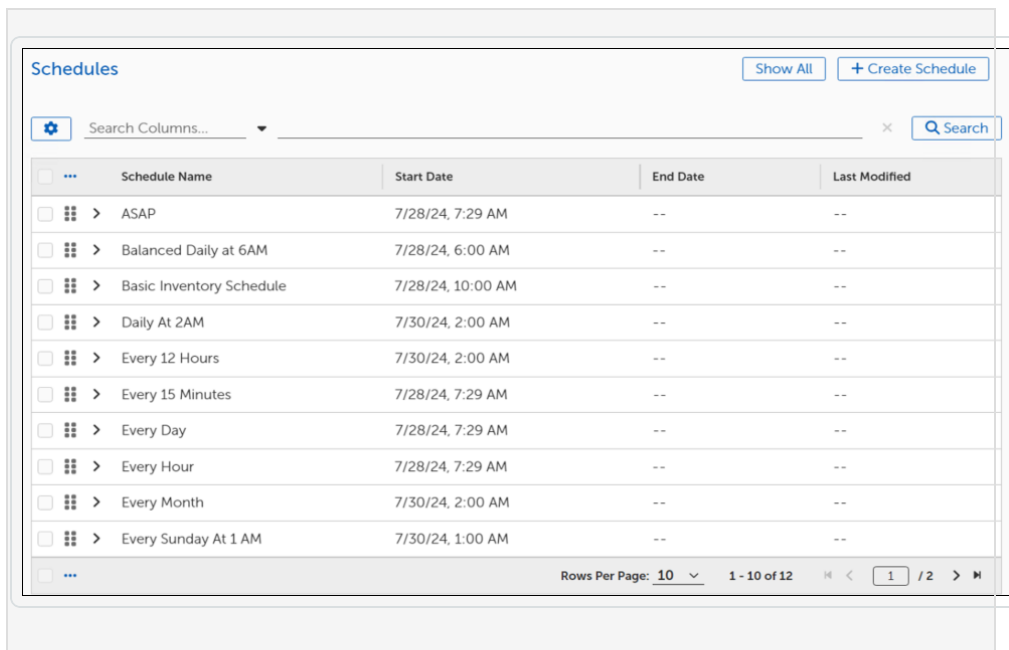
Open and Save a Schedule Template



1. Select **Schedules** in the **Platform Features** menu of the [Patch Management Dashboard](#).



This opens the list of available schedules.



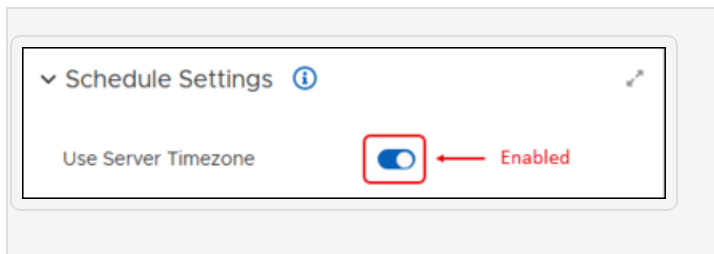
2. Select a **ScheduleName** from the table to open that scheduling template.
3. Save the template with a new **Name**:
 - a. Select **More** in the upper-left corner of the dialog, and then select **Save As**.
 - b. Enter a new name for the template, and then click **Save as** on the lower-left corner of 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 corner of the dialog.

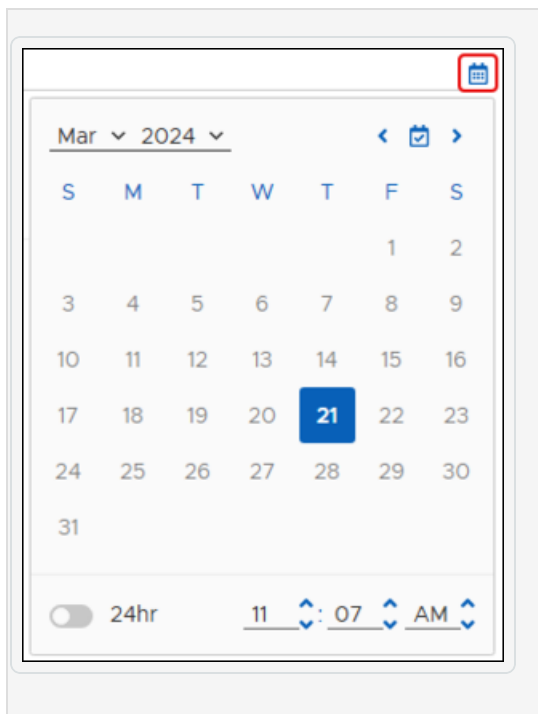
Create Schedule Settings

1. Scroll down to **Schedule Settings** in an open schedule template.
2. Select the **Use Server Timezone** toggle to enable or disable using the time zone of the Tenable Patch Management server running this schedule.



Set Start Time (Required) and End Time (Optional)

1. Select the **calendar icon** to the right of Start Time to choose the starting day and time for the schedule.





2. Navigate through the open calendar to change the start day and time:
 - a. Select the **calendar icon** with the check mark to move to the current day and time, and then use the left and right arrows to change the month.
 - b. Select a **month** using the down arrow next to the month.
 - c. Select any **date** in the calendar to select that day.
 - d. Select the **24hr** toggle to display the time using the 24 hour clock.
 - e. Select a **year** using the down arrow next to the year.
 - f. Change the **start time** for the schedule using the up and down arrows next to the time settings.
3. Select the **Enable End Time** toggle to enable or disable setting an end time.



Set Repeat and Recurrence Intervals

Select a **Schedule Repeat** setting from the list. Options include the following:

Non-Recurring

- **ASAP:** Run the process immediately using this schedule. One time only.
- **Not Recurring:** Run the process on the set schedule one time only.

Recurring

- **Recurring Interval:** Set the number of recurrences and whether they repeat by Minute (up to 60), Hours (up to 24), or Days (up to 100).
- **Recurring By Day:** Set the schedule to run one or more days per week, or to run the schedule every day.
- **Recurring By Week:** Run the schedule on a specific day of the week and set the schedule to run again on the same day for up to 127 weeks.

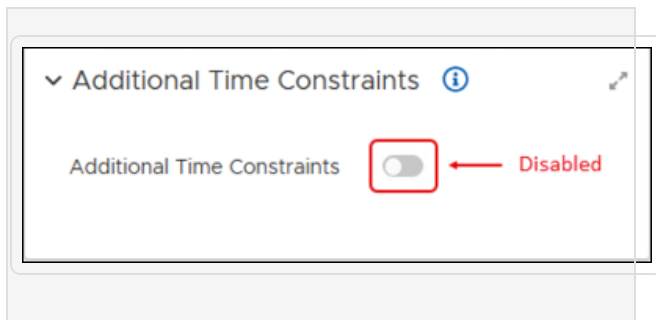


- **Recurring Monthly by Date:** Run the schedule on a specific day of the month and set the schedule to run again on the same day every month (up to 127).
- **Recurring Monthly By Last Day:** Run the schedule on the last day of the month and set the schedule to run for one or more months (up to 127).
- **Recurring Monthly By Day of Week:** Choose whether to run the schedule on a specific day of the week every month, a specific week of any month (up to 4), or run the schedule during the last week of the month. Set the Recurring Interval in Months (up to 127).

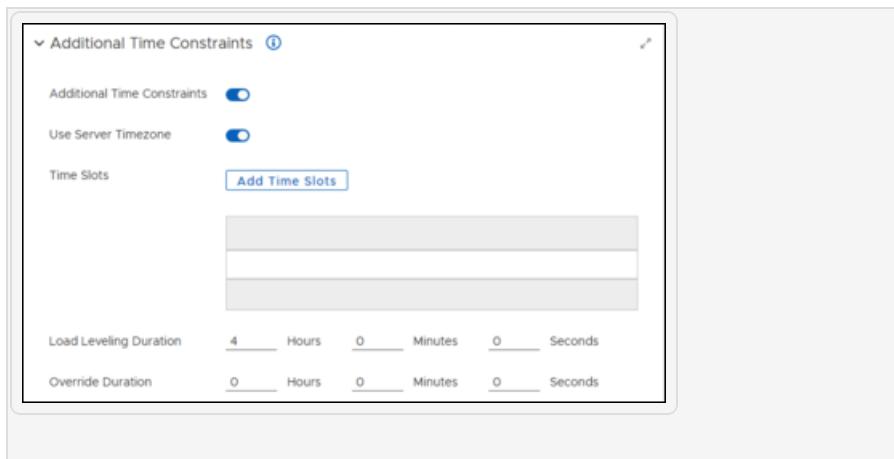
Set Additional Time Constraints

Configuring a constraint means that the schedule settings in this template run only within the time range provided in this constraint.

1. Scroll down to **Schedule Settings** in an [open schedule template](#) .
2. Select the **Additional Time Constraints** toggle to enable or disable their use.



3. Select the **Use Server Timezone** toggle to enable or disable using the timezone of the Server running the schedule.



Additional Time Constraints ⓘ

Additional Time Constraints ☒

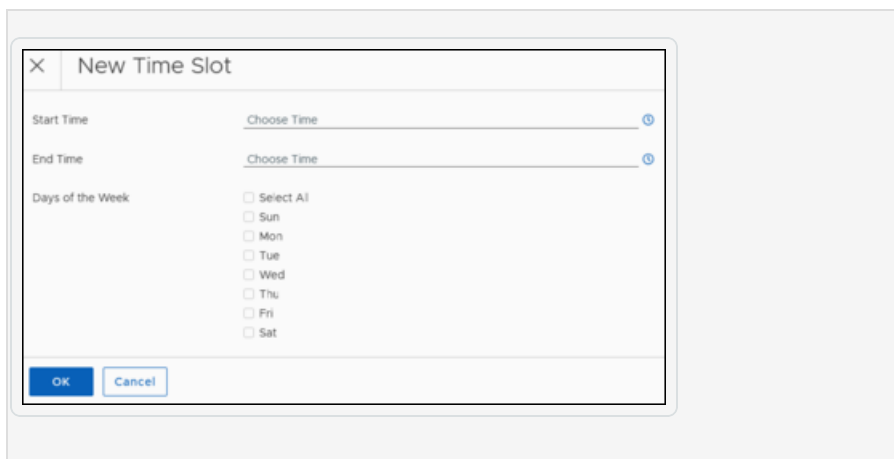
Use Server Timezone ☒

Time Slots [Add Time Slots](#)

Load Leveling Duration 4 Hours 0 Minutes 0 Seconds

Override Duration 0 Hours 0 Minutes 0 Seconds

4. Select **Add Time Slots** to define a time slot for this schedule. This opens the New Time Slot dialog.



X New Time Slot

Start Time Choose Time ⓘ

End Time Choose Time ⓘ

Days of the Week

☐ Select All

☐ Sun

☐ Mon

☐ Tue

☐ Wed

☐ Thu

☐ Fri

☐ Sat

[OK](#) [Cancel](#)

5. Enter a **Start Time** and an **End Time** in the specified field or click the clock icon to customize the clock and time settings for each field.
6. Select **OK** to save the settings and return to the **Additional Time Constraints** configuration.

Set Load Leveling Duration

Set the Load Leveling Duration in days, hours, or minutes. Tenable Patch Management balances the target of list of devices using this schedule across the time interval you set here.

Set Override Duration

Set the Override Duration in days, hours, or minutes. When the Override Duration expires, schedules start immediately.

Deploy Schedules



After saving the changes to the schedule template, you must deploy it. Deploying the schedule makes it available for use in any object that requires selecting a schedule.

1. Select **Deploy** or click **Save & Deploy** in an open Schedule template.
2. Verify that **Deployment Status** shows **Deployed**, and then click **Back to Schedules** or select another object from the left navigation menu of the dashboard.

Delete a Schedule

If you have created a schedule that you no longer need, you can delete it from the list of schedules. You cannot delete any schedules provided by Tenable Patch Management.

1. Select **Schedules** in the **Platform Features** menu of the [Patch Dashboard](#).
2. Set **Rows Per Page** at the bottom right to a larger number to see all available schedules, and then scroll down the table to the schedule you want to delete.
3. Enter a search term on the search line, and then click **Search**.
4. Locate the schedule you want to delete:
 - a. Select the **ellipsis (...)** under **Actions** for the schedule you want to delete.
 - b. Select **Delete** from the list.
5. When prompted, click **OK** to delete the schedule. You may not undo this action.

Risk Assessment Settings

Use Risk Assessment settings to customize risk calculations and display risks in other dashboards. The weight and formula information listed below is also available from the **Risk Assessment Settings** dialog under **Risk Assessment Info** in the upper right corner.

- Exposure Level Weight:
 - Low = 0
 - Medium = 33
 - High = 66



- Critical = 100
- Exploit Exists Weight
 - False = 0 (exploit does not exist)
 - True = 100 (exploit exists)
- Product Criticality Rating Weight

Use the default setting or set custom criticality by product. See Custom Risk Settings.

The Risk Assessment Score calculation uses the following formula:

$$\frac{((\text{ExposureLevelValue} * \text{ExposureLevelWeight}) + (\text{ExploitExistsValue} * \text{ExploitExistsWeight}) + (\text{CriticalityValue} * \text{CriticalityWeight}))}{(\text{ExposureLevelWeight} + \text{ExploitExistsWeight} + \text{CriticalityWeight})}$$

Risk Score Settings

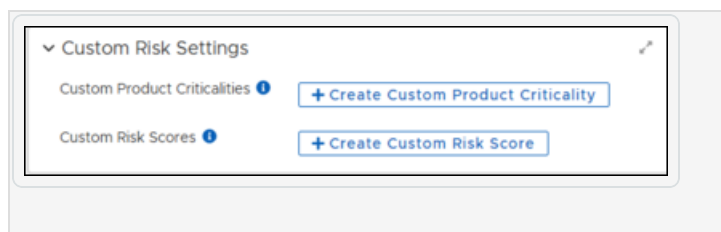
The Risk Assessment Score calculation uses a weighted average of three aspects of software security listed below. Each uses an assigned weight between 0 - 100. The default value for each weight is 50.

▼ Risk Score Settings ⓘ

Exposure Level Weight ⓘ	50
Exploit Exists Weight ⓘ	50
Product Criticality Rating Weight ⓘ	50

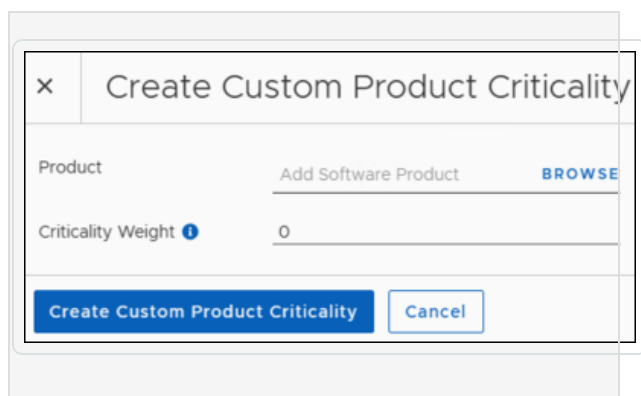
Custom Risk Settings

Use these settings to create settings that override the default settings defined in the metadata for Product Criticality settings or to create Custom Risk Scores.

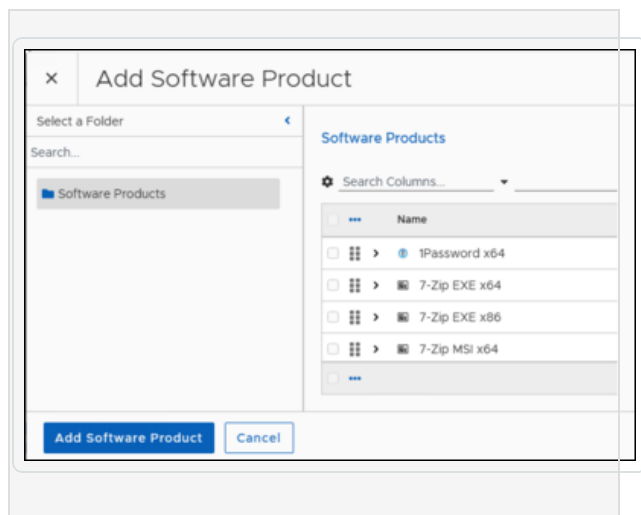


Create Custom Product Criticalities

1. Select **+ Create Custom Product Criticality** in the **Custom Risk Settings** box. This opens the **Create Custom Product Criticality** dialog.



2. Select **Browse** to search for the product you want to customize.



3. Select the product to modify, and then click **Add Software Product**.
 - This adds a table to **Custom Product Criticalities**.
 - Each time you add another product, the added information appears in this tabl



4. Enter the number that corresponds to the criticality weight you want to set for this product, and then click **Create Custom Product Criticality**.

Create Custom Risk Scores

1. Select **+ Create Custom Risk Score** in the **Custom Risk Settings** box of Risk Assessment Settings. This opens the **Create Custom Risk Score** dialog.

2. Select **Browse** to open the **Add Installable Software** dialog.
 1. Enter a product name on the search line, and then click **Search**. This example uses Google Chrome.
- 3.



2. Select the product from the list, and then click **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

4. Enter the number that corresponds to the risk score you want to set for this product, and then click **Create Custom Risk Score**.
 - This adds a table to **Custom Risk Scores**.
 - Each time you add another product, the added information appears in this table.
5. Select **Save Settings**.

Approval Requests

Some Patching Strategies require patch manager approval before beginning a patch cycle. The Patching Process looks for an Approval Chain to use when processing approvals and sends notification based on the communication process configured for each approver.

These approval communications include a link that takes the approver to the Admin Portal, which prompts the approver for authentication.

Administrators may see all pending and completed Approvals using the Tenable Patch Management dashboard.

Approve or Reject a Patch Request

1. Select **Approval Requests** from the left navigation menu of the Patch dashboard 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 awaiting 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:

Approval Summary	Request Sent To	Scope Object	Request Status	Your Response	Actions
Patching Process Appr...	3/23/25, 1:58 PM	Enabled Patching Strategy Ch...	In Progress	Awaiting response	...
Patching Process Appr...	3/21/25, 8:32 AM	Enabled Patching Strategy Ch...	Completed, Approv...	Approved	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.

Patching Strategy Templates

Effective management and deployment of software patches is crucial for maintaining the security and stability of an IT infrastructure. The Patching Strategies included in Tenable Patch Management address various deployment scenarios and considerations.

Recommended Use

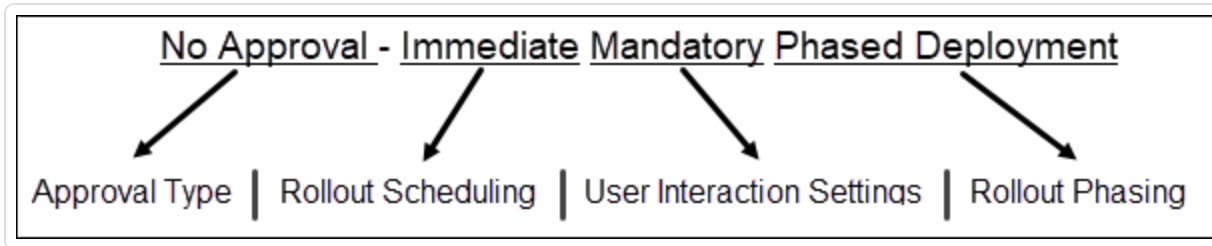
You can choose a Patching Strategy template, save it under a descriptive local naming convention, and then customize it as needed. Tenable Patch Management Patching Strategy templates reference objects that include the minimum requirements for a successful patching strategy: Deployment Wave, Deployment Bot, and Patching Process.

recommends creating a folder to hold all new or customized strategies. This separates them from the strategies provided with the product.



Patching Strategy Template Naming Conventions

Tenable Patch Management Patching Strategy templates cater to four specific use cases: Approval Types, Rollout Scheduling, User Interaction Settings, and Rollout Phasing. When deciding which Patching Strategy to choose, consider the following example to understand naming:



By offering various combinations of these parameters, the templates are a versatile framework that can accommodate a wide range of patching scenarios.

Minimal customization includes adding the products to patch and a schedule. This flexibility allows for efficient patch management without the need for extensive customization or the creation of new strategies.

- **Approval Type:** Level of approval needed prior to deployment:
 - **No Approval:** Deploys at once.
 - **Initial Approval:** Requires approval prior to deploying.
 - **Phased Approval:** Requires approval between each wave in the Deployment Waves object.
- **Rollout Scheduling:** Defines the schedule and impact of a deployment.
 - **Immediate:** All product patches deploy at once.
 - **RiskBased:** Targeted and controlled deployment based on specific risk levels (low, medium, high, critical). Schedule and run patch deployments based on risk levels. Uses Deployment Channels.
- **User Interaction:** Defines permitted user actions related to the patch installation.
 - **Mandatory:** Alerts the end user who can postpone depending on [User Interaction Settings](#) but cannot decline. All product patches deploy at once.



- **Options:** Alerts the end user. Otherwise, functionality not available in this release.
- **Rollout Phasing:** Deploys in separate phases to allow a review before continuing.
 - Minimal customization includes adding the products to patch and a schedule.
 - This flexibility allows for efficient patch management without the need for extensive customization or the creation of new strategies.

Initial Patch Manager Approval Strategies

Each of these strategies requires an approval step before deploying updates. Except for Risk Based Mandatory Deployment, the Patching Process within these strategies manages the deployment process exclusively and does not use Deployment Channels.

Similarly, the Deployment Bot does not apply any filtering mechanism, so the Patching Process manages all updates related to the products included in the non-risk strategies.

- **Initial Approval - Immediate Mandatory Deployment**

Approval required prior to deployment, then deploys at once with no user interaction.

- **Initial Approval - Immediate Mandatory Phased Deployment**

Approval required prior to deployment, then deploys at once in a phased manner, rolling out to each wave of business units sequentially with no user interaction control.

- **Initial Approval - Immediate Optional Deployment**

Approval required prior to deployment, then deploys at once in a phased manner, rolling out to each wave of business units sequentially. User interaction allowed.

- **Initial Approval - Risk-Based Mandatory Deployment**

Approval required prior to deployment, and then deploys at once to all devices in the targeted business units based on the patch risk levels.

Uses both Deployment Waves and Deployment Channels. Higher-risk updates have priority in high-frequency Deployment Channels. Lower-risk updates belong to lower-frequency Channels.



Also uses Deployment Bot to filter patches based on risk level, and then sends the final wave to the proper Deployment Channels.

Ensures processing and deployment of the final wave through the most suitable Deployment Channel and adds a layer of control and customization to the deployment process.

No Approval Strategies

Each of these strategies requires no approval before deploying updates. Except for Risk Based Mandatory Deployment, the Patching Process within these strategies manages the deployment process exclusively and they do not use Deployment Channels.

Additionally, the Deployment Bot does not apply any filtering mechanism, so the Patching Process manages all updates related to the products included in the non-risk strategies.

- **No Approval - Immediate Mandatory Deployment**

No approval needed prior to deployment. Deploys at once with no user interaction.

- **No Approval - Immediate Mandatory Phased Deployment**

No approval needed prior to deployment. Deploys at once in a phased manner, rolling out to each wave of Business Units sequentially. No user interaction.

- **No Approval - Immediate Optional Deployment**

No approval needed prior to deployment. Deploys at once to all devices in the targeted business unit. User interaction allowed.

- **No Approval - Risk-Based Mandatory Deployment**

No approval needed prior to deployment. Deploys at once to all devices in the targeted business units based on the patch risk levels. No user interaction.

Uses both Deployment Waves and Deployment Channels. Higher-risk updates have priority in high-frequency Deployment Channels. Lower-risk updates belong to lower-frequency Channels.

Also uses Deployment Bot to filter patches based on risk level, and then sends the final wave to the proper Deployment Channels.



Ensures processing and deployment of the final wave through the most suitable Deployment Channel and adds a layer of control and customization to the deployment process.

Phase Approval Strategies

Each of these strategies requires phased approvals before deploying updates. Except for Risk Based Mandatory Deployment, the Patching Process within these strategies manages the deployment process exclusively without using Deployment Channels.

Similarly, the Deployment Bot does not apply any filtering mechanism, so the Patching Process manages all updates related to the products included in the non-risk strategies.

- **Phase Approval - Immediate Mandatory Phased Deployment**

Approval required between each wave of the deployment, and then deploys the updates in a phased manner, rolling out to each wave of business units sequentially. No user interaction.

- **Phase Approval - Risk-Based Mandatory Deployment**

Approval step required between each wave of the deployment, and then deploys the updates at once to all devices in the targeted business units based on risk levels. No user interaction.