

Tanium™ Patch User Guide

Autonomous IT. Unstoppable Business.

2025H2 Semiannual Release

Version 3.28

April 06, 2026

The information in this document is subject to change without notice. Further, the information provided in this document is provided "as is" and is believed to be accurate, but is presented without any warranty of any kind, express or implied, except as provided in Tanium's customer sales terms and conditions. Unless so otherwise provided, Tanium assumes no liability whatsoever, and in no event shall Tanium or its suppliers be liable for any indirect, special, consequential, or incidental damages, including without limitation, lost profits or loss or damage to data arising out of the use or inability to use this document, even if Tanium Inc. has been advised of the possibility of such damages.

Any IP addresses used in this document are not intended to be actual addresses. Any examples, command display output, network topology diagrams, and other figures included in this document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Please visit https://help.tanium.com for the most current Tanium product documentation.

This documentation may provide access to or information about content, products (including hardware and software), and services provided by third parties ("Third Party Items"). With respect to such Third Party Items, Tanium Inc. and its affiliates (i) are not responsible for such items, and expressly disclaim all warranties and liability of any kind related to such Third Party Items and (ii) will not be responsible for any loss, costs, or damages incurred due to your access to or use of such Third Party Items unless expressly set forth otherwise in an applicable agreement between you and Tanium.

Further, this documentation does not require or contemplate the use of or combination with Tanium products with any particular Third Party Items and neither Tanium nor its affiliates shall have any responsibility for any infringement of intellectual property rights caused by any such combination. You, and not Tanium, are responsible for determining that any combination of Third Party Items with Tanium products is appropriate and will not cause infringement of any third party intellectual property rights.

Tanium is committed to the highest accessibility standards for our products. To date, Tanium has focused on compliance with U.S. Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. Tanium has conducted 3rd party accessibility assessments over the course of product development for many years. We certify against the WCAG 2.2 / VPAT 2.5 standards for all major product modules. Tanium performs ongoing reassessments as appropriate, given the scope and type of changes to the UI and product features from release to release. In the most recent testing, the Tanium Console UI achieved *supports* or *partially supports* for all applicable WCAG 2.2 criteria. Tanium can make available any VPAT reports on a module-by-module basis as part of a larger solution planning process for any customer or prospect.

As new products and features are continuously delivered, Tanium will conduct testing to identify potential gaps in compliance with accessibility guidelines. Tanium is committed to making commercially reasonable efforts to address any gaps as quickly as is feasible, given the severity of the issue and scope of the changes. Tanium factors these objectives into the ongoing delivery schedule of features and releases with our existing resources.

Tanium welcomes customer input on making solutions accessible based on your Tanium modules and assistive technology requirements. Accessibility requirements are important to the Tanium customer community and we are committed to prioritizing these compliance efforts as part of our overall product roadmap. Tanium maintains transparency on our progress and milestones and welcomes any further questions or discussion around this work. Contact your sales representative, Tanium Support at support@tanium.com, or email accessibility@tanium.com to make further inquiries.

Tanium is a trademark of Tanium, Inc. in the U.S. and other countries. Third-party trademarks mentioned are the property of their respective owners.

Mac and macOS are trademarks of Apple Inc., and registered in the U.S. and other countries and regions.

Patents: https://www.tanium.com/patents

© 2026 Tanium Inc. All Rights Reserved

Tanium Open Source Disclosure : https://tanium.github.io/opensource/

© 2026 Tanium Inc. All rights reserved.

Table of contents

Patch overview **13**

Patch scanning options for Windows and Linux endpoints 13

Available Patch scan methods for Windows endpoints 13

Available Patch scan methods for Linux endpoints 17

Patch lists and block lists for Windows and Linux endpoints 18

Superseded and superseding patches for Windows and Linux endpoints 18

Microsoft update and servicing details 19

Windows patch confidence score 19

Deployments for Windows and Linux endpoints 20

Maintenance windows for Windows and Linux endpoints 20

Linux repository snapshots 21

Self Service Client application for Windows endpoints 21

Tanium Autonomous IT Platform in Patch 21

Supported languages 22

Patch versus Deploy 22

Interoperability with other Tanium products 22

Tanium™ Automate 23

Tanium™ Comply 23

Tanium™ End-User Notifications 23

Tanium™ Endpoint Configuration 23

Tanium™ Reporting 23

Tanium™ Trends 23

Gaining organizational effectiveness with Patch **25**

Change management 25

RACI chart 25

Organizational alignment 29

Operational metrics 29

© 2026 Tanium Inc. All Rights Reserved

Patch maturity ... 29
Benchmark metrics for Windows and Linux endpoints ... 30
Patch requirements ... **34**
Core platform dependencies ... 34
Computer group dependencies ... 34
Solution dependencies ... 36
Tanium recommended installation ... 36
Import specific solutions ... 36
Required dependencies ... 36
Feature-specific dependencies ... 37
Client extensions and endpoint tools ... 37
Tanium Server and Module Server computer resources ... 37
Endpoints ... 38
Supported operating systems ... 38
Resource requirements ... 40
Third-party software ... 40
Host and network security requirements ... 40
Ports ... 40
Security exclusions ... 41
Third-party internet URLs ... 43
User role requirements ... 45
Installing Patch ... **52**
Before you begin ... 52
Import Patch with default settings ... 52
Import Patch with custom settings ... 53
Manage solution dependencies ... 54
Upgrade Patch ... 54
Verify Patch version ... 54
Configuring Patch ... **55**
Restricted targeting ... 55

© 2026 Tanium Inc. All Rights Reserved

Default settings ... 55
Configure advanced settings ... 56
Install and configure Tanium End-User Notifications for Windows endpoints ... 57
Disable Windows Update restart prompts ... 57
Install and configure Tanium Endpoint Configuration ... 57
Manage solution configurations with Tanium Endpoint Configuration ... 57
Configure Patch global settings ... 58
Configure the Patch action group for Windows and Linux endpoints ... 58
Next steps ... 59
Organize computer groups for Windows and Linux endpoints ... 59
Set up Patch users ... 63
Enable and configure Windows features ... 65
Enable and configure Tanium Scan for Windows ... 65
Configure WSUS server allowed URLs ... 66
Enable UUP Proxy ... 66
Enable manual synchronization ... 67
Enable direct patch downloads from Microsoft ... 67
Cautions and considerations ... 68
Tracking direct download status ... 68
Enable and configure Linux features ... 69
Migration of OS-based Linux configurations to Enhanced Linux configurations ... 69
Linux Endpoint Behavior Changes ... 69
Enable Patch for Enhanced Linux configurations ... 70
Add and target Linux repositories ... 70
(Red Hat endpoints) Configure Tanium Server to use certificate authentication ... 72
(Red Hat endpoints) Configure TDownloader to use certificate authentication (Tanium Server version 7.5.2.3552 and earlier) ... 72
Configure TDownloader on Tanium Server (Appliance) ... 72
Configure TDownloader on Tanium Server (Windows) ... 73
Next steps ... 78

© 2026 Tanium Inc. All Rights Reserved

Manage Linux repository snapshots ... 78
Before you begin ... 78
Procedure ... 78
Export a Linux repository ... 79
Import a Linux repository ... 79
Configure Patch behavior on action-locked endpoints ... 79
Initialize Patch ... 80
Select a language ... 80
Downloading Windows patches in an air-gapped environment ... 81
Before you begin ... 81
Patch air-gapped environments using Tanium Scan for Windows ... 81
Patch air-gapped environments using Offline CAB ... 83
Verify the Offline Cab configuration ... 85
Downloading Linux patches in an air-gapped environments ... 87
Download Linux CVE metadata ... 87
Modify the Patch - External File References – Linux package ... 88
Recreate the Required Files - Linux configuration ... 88
Add local repositories ... 89
Configure scans for air-gapped environments ... 89
What to do next ... 89
Enforcing scan configurations ... 90
Windows scan techniques ... 90
Windows scan techniques ... 90
Tanium Scan ... 90
Offline CAB File ... 91
Online Microsoft Windows Update ... 91
WSUS ... 92
Linux scan techniques ... 92
Repository Scan ... 93
Tanium Scan ... 93

© 2026 Tanium Inc. All Rights Reserved

Tanium Scan incompatibility with LibZypp Services Plugins ... 93
Create a scan configuration ... 94
Scan windows ... 96
View enforcement status ... 98
Prioritize scan configurations ... 98
Edit a scan configuration ... 99
Remove a scan enforcement ... 99
Delete a scan configuration ... 99
Managing patches ... **100**
Default patch lists ... 100
Patch list rules ... 100
Create a patch list ... 102
Exclude patches with block lists ... 104
yum.conf exclusions for Linux endpoints ... 104
Create lists from the Patches view ... 105
View confidence score of Windows patch ... 105
Edit a list ... 106
Check patch visibility ... 107
Manually synchronize patches ... 108
Synchronize patches from the Overview page ... 108
Synchronize a patch from the Patch details page ... 109
Copy a patch list ... 110
Export a list ... 111
Import a list ... 111
Delete a list ... 111
Add a custom Patch field ... 112
Example CSV ... 112
Deploying patches ... **113**
Before you begin ... 113
Create a deployment template ... 113

© 2026 Tanium Inc. All Rights Reserved

Set the default deployment template ... 116
Create a deployment to install patches ... 116
Endpoint restarts ... 120
Create a deployment to install patches on a single endpoint ... 121
Windows: Create a deployment to uninstall patches ... 122
Review deployment summary ... 125
Add targets to an existing deployment ... 126
Stop a deployment ... 126
Reissue a deployment ... 126
Delete old inactive deployments ... 127
Adjust the deployment retries ... 127
Reference: Patch status ... 127
Deployment status ... 127
Enforcement status ... 130
Setting maintenance windows ... 131
Maintenance window options ... 131
Create a maintenance window ... 132
Edit a maintenance window ... 134
Override a maintenance window ... 134
Delete a maintenance window ... 134
Managing End-User Self Service for Windows endpoints ... 135
Before you begin ... 135
Create a Self Service deployment to install patches ... 135
Create a Self Service deployment to uninstall patches ... 137
Use the Self Service Client application on endpoints ... 139
Maintaining Patch for Windows and Linux endpoints ... 142
Perform monthly maintenance ... 142
Review and remediate Patch coverage ... 142
Review and update scan configurations ... 142
Review and update deployments ... 143

© 2026 Tanium Inc. All Rights Reserved

Review and update maintenance windows ... 143
Perform quarterly maintenance ... 144
Perform as-needed maintenance ... 144
Check and update the Windows Update Agent ... 144
Check patch history on Windows endpoints ... 144
Monitor and troubleshoot Patch coverage ... 145
Monitor and troubleshoot endpoints missing critical or important patches ... 146
Monitor and troubleshoot mean time to patch ... 146
Troubleshooting Patch ... **148**
Collect a troubleshooting package ... 148
Download audit log ... 148
View job logs to troubleshoot job failed errors ... 148
Collect Patch troubleshooting information from Windows and Linux endpoints ... 149
Configure endpoint logging for Windows and Linux endpoints ... 150
Verify endpoint tools ... 150
Windows and Linux patches are not listed in the Patches view ... 150
Troubleshoot scan errors on Windows and Linux endpoints ... 150
Offline CAB scans fail for Windows 7 and Windows Server 2008 R2 ... 151
Scans are not completed on Linux endpoints ... 151
Red Hat Linux endpoints stuck in Waiting for Initial Scan status ... 152
Linux repository snapshots issues ... 152
Warning about a failed snapshot ... 152
Patch process is not running on Linux endpoints ... 152
OpenSUSE and SLES endpoints install later version of software ... 152
End user notifications are not displayed or endpoints have errors ... 152
Patch workbench slowly loads pages ... 153
Identify and resolve issues with Client Extensions ... 153
Review the Extensions log for an endpoint ... 156
Remove Patch tools from Windows and Linux endpoints ... 156
Uninstall Patch ... 157

© 2026 Tanium Inc. All Rights Reserved

Restore the state of the Patch database ... 159
Resolve UUP synchronization errors ... 159
Cannot use Tanium Patch to deploy Microsoft out-of-band updates ... 162
Contact Tanium Support ... 162
Reference: Common Patch errors ... 163
Client API connection failed. Unable to download file. Error #9 ... 163
Error creating Update Service Object - See C:\Windows\windowsupdate.log for more details. Error #9 ... 163
Patch <Patch UID>: WU_E_DM_INCORRECTFILEHASH. Error #-2145099774 ... 163
Patch <Patch UID>: ERROR_INSTALL_FAILURE. Error #-2147023293 ... 163
Patch <Patch UID>: WU_E_CALL_CANCELLED. Error #-2145124341 ... 164
-2147024784 ERROR_DISK_FULL ... 164
OfflSnc WARNING: failed to copy offline cab. hr = 0x80070070 ... 164
-2145124320 WU_E_NO_INTERACTIVE_USER ... 165
E_PROP_ID_UNSUPPORTED ... 165
Unable to Load PatchLib ... 165
Windows Update Error: -2145124338 WU_E_XML_INVALID ... 166
Unrestored registry snapshot found ... 166
Windows Update Error Code: 7 Out of Memory ... 166
Windows Update Manager timed out waiting for the Windows Update Service to reach a Stopped state ... 167
Windows Update Error: -2145107951 WU_E_PT_SUS_SERVER_NOT_SET ... 167
Linux: Could not get results ... 168
Linux: Failed to download repomd.xml ... 168
Linux: Repo URLs found but unable to snapshot metadata files, likely due to connectivity issue ... 168
Linux: Selected repo <repository_name> is missing required Yum variables ... 169
Linux: Repo URLs were found but the snapshot could not be created, likely due to a Yum variable mismatch ... 169
Reference: End-User Self Service sensors ... 170
Reference: Patch endpoint tools ... 171
Reference: Gateway examples for Patch ... 173
Patch query filter syntax ... 173
CVE ID ... 173

© 2026 Tanium Inc. All Rights Reserved

Classification ... 174
Has association with any CVE ... 176
Is superseded by another patch definition ... 177
Operating System platform ... 178
Product ... 179
Released on or before a date ... 181
Released on or after a date ... 182
Severity ... 183
Patch examples ... 184
Create a Patch install deployment for Linux (mutation.patchCreateDeployment) ... 185
Create a Linux patch deployment ... 185
Create a Patch install deployment for Windows (mutation.patchCreateDeployment) ... 191
Create a Windows patch deployment ... 191
Get Patch definitions (query.patchDefinitions) ... 199
Get multiple patch definitions ... 199
Get a Patch deployment by ID (query.patchDeployment) ... 201
Get a patch deployment by ID ... 201
Stop a Patch deployment by ID (mutation.patchStopDeployment) ... 205
Stop a patch deployment by ID ... 205
Upsert (create or update by ID) a Patch patch list (mutation.patchListUpsert) ... 210
Upsert (create or update by ID) a patch list ... 210

© 2026 Tanium Inc. All Rights Reserved

Patch overview

Use Patch to manage operating system patching across your enterprise at the speed and scale of Tanium. For Windows and Linux endpoints managed using Tanium Client, you can deploy a single patch to a computer group immediately. You can also perform more complex tasks, such as delivering groups of patches across your environment at specified times using advanced rule sets and maintenance windows.

For Windows and Linux endpoints, you can define custom workflows and schedule patches based on rules or exceptions built around patch lists, block lists, and maintenance windows. For example, you might always apply critical Microsoft patches to all machines except for datacenter servers, or always exclude .NET patches, or install patches during non-working hours.

Patch generates reports and returns current patch applicability results from every endpoint. For any patch or patch list deployment, the following details are provided:

- The patch details, such as severity, release date, applicable Common Vulnerabilities and Exposures (CVE), files, and links to knowledge base articles
- The status of the patch, split out by computer group
- The assigned patch lists or block lists for the patch



The Patch **Overview** page provides **Summary** and **Health** charts to monitor compliance. Unlike earlier versions of Patch, these charts currently only support Windows and Linux endpoints.

Patch scanning options for Windows and Linux endpoints

You can choose from several scan methods for Windows and Linux endpoints to determine the installed and missing patches across your network. *Scan configurations* define a scan method, scan frequency, and the computer groups that are being scanned, known as an *enforcement*. One scan configuration is applied to an endpoint. If an endpoint is included in multiple computer groups, the highest priority scan configuration is applied. For more information, see Enforcing scan configurations on page 90.

Review the following lists of scanning options for Windows and Linux endpoints to decide the best method to use for each computer group.

Available Patch scan methods for Windows endpoints

	Tanium Scan[1]	Offline CAB File[2]	Online Microsoft Windows Update	WSUS (Windows Server Update Services)[1,3]
Platform OS	Windows	Windows	Windows	Windows

© 2026 Tanium Inc. All Rights Reserved

	Tanium Scan[1]	Offline CAB File[2]	Online Microsoft Windows Update	WSUS (Windows Server Update Services)[1,3]
Updates included	Scanning and installing: • Critical Updates • Feature Packs • Security Updates • Service Packs • Tools • Update Rollups • Updates	Scanning and installing: • Security Updates • Service Packs • Update Rollups	Scanning: • Critical Updates • Definition Updates • Drivers IMPORTANT Tanium Patch can scan for drivers but cannot distribute or install the drivers. To install, use Tanium Deploy. For more information, see Tanium Deploy User Guide: Create a software package. • Feature Packs • Security Updates • Service Packs • Tools • Update Rollups • Updates • Upgrades Installing: • Critical Updates • Feature Packs • Security Updates • Service Packs • Tools • Update Rollups • Updates	Scanning: • Critical Updates • Definition Updates • Drivers IMPORTANT Tanium Patch can scan for drivers but cannot distribute or install the drivers. To install, use Tanium Deploy. For more information, see Tanium Deploy User Guide: Create a software package. • Feature Packs • Security Updates • Service Packs • Tools • Update Rollups • Updates • Upgrades Installing: • Critical Updates • Feature Packs • Security Updates • Service Packs • Tools • Update Rollups • Updates

	Tanium Scan[1]	Offline CAB File[2]	Online Microsoft Windows Update	WSUS (Windows Server Update Services)[1,3]
Client impact	• Initial scan: Moderate • Subsequent scans: Low	Initial and subsequent scans: Moderate	• Initial scan: Moderate • Subsequent scans: Low	Initial and subsequent scans: Low
Connectivity	• A client database file is stored locally by the Tanium Client. • With the direct download option for isolated endpoints, the endpoint contacts Microsoft directly.	• The CAB file is stored locally by the Tanium Client. • With the direct download option for isolated endpoints, the endpoint contacts Microsoft directly.	• The Tanium Client must contact Microsoft directly. • With the direct download option for isolated endpoints, the endpoint contacts Microsoft directly.	• The Tanium Client must contact the WSUS server. • With the direct download option for isolated endpoints, the endpoint contacts the location that is defined by the WSUS server directly. Depending on WSUS server configuration, the location is the WSUS server or Microsoft.
Support for direct download of patches on isolated endpoints	Yes	Yes	Yes	Yes

© 2026 Tanium Inc. All Rights Reserved

	Tanium Scan[1]	Offline CAB File[2]	Online Microsoft Windows Update	WSUS (Windows Server Update Services)[1,3]
Details	• The Patch service on the Module Server is configured to synchronize update metadata and detection rules directly from Microsoft. Alternatively, it can be configured to synchronize from WSUS in airgap scenarios where WSUS is available and already has approved and downloaded patches. • Supports direct patch downloads from Microsoft to isolated endpoints. • Supports using Tanium architecture to deliver cumulative updates for Windows 11, version 22H2 or later endpoints.	• Requires 600+ MB download of CAB file. • Does not include non-security updates, out-of-band fixes, hotfixes, and enhancements that are included with WSUS or Online to Microsoft scan methods. • Supports direct patch downloads from Microsoft to isolated endpoints.	• Requires additional network traffic to Microsoft directly. • Supports direct patch downloads from Microsoft to isolated endpoints.	• Must deploy and configure one or more WSUS servers. • Updates must be approved in WSUS prior to scanning or deployment. • Supports direct patch downloads from Microsoft or the WSUS server to isolated endpoints.

© 2026 Tanium Inc. All Rights Reserved

For more information, see Windows scan techniques on page 90.

Available Patch scan methods for Linux endpoints

	Tanium Scan[1]	Repository Scan
Platform OS	• Red Hat • CentOS • Oracle Linux • SUSE[2] • Ubuntu • Debian	• Red Hat • CentOS • Oracle Linux • Amazon Linux • SUSE[2] • Ubuntu • Debian
Updates included	All updates in the repositories[3]	All updates in the repositories
Client impact	Initial and subsequent scans: Moderate	Initial and subsequent scans: Moderate
Connectivity	The Tanium Client stores the repository scanning logic locally.	The Tanium Client must contact the repositories for scanning and patch downloads.
Support for direct download of patches on isolated endpoints	No	Yes
Details	• Internal or external repositories can be used. • Only the Tanium™ Server needs connectivity to the repositories.	• Must deploy and configure one or more repositories. • Updates must be maintained in the repositories.

[1]Tanium Scan for Linux is not compatible with LibZypp Service Plugins. Tanium Scan will scan repositories provided by the plugin, but will not have access to the metadata in these repositories, which leads to scan results with incomplete metadata. Patch list applicability reports packages with incomplete metadata, but Patch cannot install them. If possible, uninstall the plugin and create repositories using Tanium.

[2]SUSE 11.x Service Pack 3 support is limited to scanning only.

[3]When installing package dependencies for patches on Debian and Ubuntu endpoints, Tanium Patch includes only packages that are required dependencies. Recommended dependencies are not included.

For more information, see Core platform dependencies on page 34, Linux scan techniques on page 92, and Tanium Scan incompatibility with LibZypp Services Plugins on page 93.

© 2026 Tanium Inc. All Rights Reserved

Patch lists and block lists for Windows and Linux endpoints

A *patch list* is a set of patches that you want to deploy to a group of Windows and Linux endpoints. A *block list* is a set of patches that you want to exclude from deployments. Patch provides a baseline reporting patch list for Windows and Linux. You can compile lists by manually adding individual patches or by defining rules that add patches dynamically. Here are some examples of how you can utilize patch lists and block lists:

- Focus only on CVE issues.
- Create lists based on severity, prioritize the most critical and most recent updates first.
- Create lists based on the month or a specific release date.
- • Create a patch list that includes Servicing Stack Updates (SSUs) and Cumulative Updates (CUs).
- • Create a block list to block SQL server patches.

As new patches come out, you can use dynamic rules to automatically assess and populate patches to the appropriate lists. You can iteratively develop these lists by creating new versions. You can deploy any version of the list as needed. For more information, see Managing patches on page 100.



To manage Linux patching based on a current release date, use repository snapshots instead of patch lists. Snapshots reduce dependency mismatches and deployment failures. For more information, see Linux repository snapshots on page 21.

Superseded and superseding patches for Windows and Linux endpoints

Each patch for Windows and Linux endpoints includes a column that indicates if the patch has been superseded, or effectively replaced by a newer patch. A patch is marked as superseded when a single endpoint reports that the patch is superseded. For best results, include superseded patches in patch lists for visibility of non-compliance on endpoints. Superseded patches are automatically included in block lists.

The following example demonstrates the differing level of detail that an endpoint reports when a patch list includes or excludes superseded patches. The expanded detail with including superseded patches provides visibility to understand the scope of non-compliance on endpoints A and B.

Endpoint report detail when including and excluding superseded patches

Endpoint status	Patch list includes superseded patches	Patch list excludes superseded patches
Endpoint A has not installed any cumulative updates since January 2023.	Endpoint reports that it has not installed a cumulative update since January 2023.	Endpoint reports that it only needs the most recent cumulative update.
Endpoint B is only missing the most recent cumulative update.	Endpoint reports that it only needs the most recent cumulative update.	Endpoint reports that it only needs the most recent cumulative update.

© 2026 Tanium Inc. All Rights Reserved

For disk space and bandwidth efficiencies, if a deployment contains both a superseded patch and the patch that supersedes it, then Patch downloads only the superseding patch (the newer patch). If a superseding patch is included in multiple deployments, Patch downloads the patch only one time. After a deployment completes, Patch removes patch files that are no longer required by any deployment on the endpoint.

For more information, see Exclude patches with block lists on page 104.

Microsoft update and servicing details

Microsoft provides software patch updates in different ways depending on the operating system of the endpoint. Microsoft changes these terms occasionally, and it is important to understand how these policies affect your patching processes.

- **Windows 11 (22H2 and later), Windows Server 2025**
    - *2024-XX Cumulative Update*: Released monthly, a cumulative update supersedes any previous cumulative update for Windows. Contains all security and non-security fixes for the month and all previous months. Microsoft introduced the Unified Update Platform (UUP) method for delivering Windows updates. To patch endpoints on Windows Server 2025 or Windows 11 22H2 or later, you need to use Tanium Scan for Windows. Offline CAB is not supported.
- **Windows 10, Windows 11 (up to but not including 22H2), Windows Server 2016, and Windows Server 2019**
    - *Feature Updates*: Feature builds are essentially a new build of Windows 10. These upgrades are published twice a year with a target of March and September of each year (for example 1709, 1803, 1809, 1902, 1909). Consider the following Tanium capabilities when you select a solution for Windows feature updates.
        - Tanium Deploy provides out of the box capabilities that enable efficient assessment, reporting, and deployment of Windows feature updates. For more information, see Windows 10 Upgrades and Servicing Made Easy With Tanium.
        - Tanium Core with custom sensors and custom packages
    - *2019-XX Cumulative Update*: Released monthly, a cumulative update supersedes any previous cumulative update for Windows 10. Contains all security and non-security fixes for the month and all previous months.
- **Windows 7, 8.1, 2008, 2008R2, 2012, 2012R2**
    - *2019-XX Security Monthly Quality Rollup*: Package is a cumulative update for current and all previous months. Only the current month will be applicable. All previous versions are superseded.
    - *2019-XX Security Only Quality Update*: Security updates for the specified month only. Does not include updates from any previous month. Previous monthly updates will still be applicable and needed.

  Do not deploy both the Security Monthly Quality Rollup and the Security Only Quality Update for the same month at the same time. If both updates are targeted to an endpoint, the Windows Update Agent installs the Security Monthly Quality Rollup, and the Security Only update is ignored. The download size increases without any benefit.

Windows patch confidence score

Tanium assigns a confidence score to Windows patches that have been released within the last 365 days or are applicable in your environment. A patch is applicable in your environment if at least one endpoint is reporting `Not Installed` for the patch.

© 2026 Tanium Inc. All Rights Reserved

The confidence score rates the probability that a patch deployment will succeed and will not cause post-installation downtime. Tanium bases the score on execution success and performance metrics that endpoints across all Tanium environments returned for previous deployments of the patch. For more information, see View confidence score of Windows patch on page 105

Tanium does not calculate confidence scores for the following patches:

- Windows patches released over 365 days ago or that are not applicable in your environment
- Linux patches



Confidence score is available only if your Tanium instance is linked to your Tanium Account. For more information, see Tanium Account User Guide: Link an on-premises Tanium instance. It can take up to one hour for confidence scores to appear after linking your account. If you unlink your account, it can take up to five hours for confidence scores to disappear.

Deployments for Windows and Linux endpoints

Deployments compile patches, typically from lists, and then distribute Patch packages to the target Windows and Linux computers. You can configure deployment options to set when and how patches are installed or uninstalled, including allowing Windows endpoint users to manage patches using the Self Service Client application.

For example, you might want to restart an endpoint after patches are installed to apply the changes. If a patch comes out that would normally be blocked but is needed for some reason, you can override the block list for that specific deployment instead of making a new block list. In urgent situations, you can even override a closed maintenance window.

You can choose whether to restart the endpoint after patch installation, to inform the user about the restart, and to allow the user to postpone the restart. For more information, see Deploying patches on page 113.

Deployment templates can be used to save settings for a deployment that you can issue repeatedly. For more information, see Create a deployment template on page 113.

Maintenance windows for Windows and Linux endpoints

Maintenance windows for Windows and Linux endpoints designate the permitted times that the targeted computer groups are open for patches to be installed or uninstalled. You can have multiple maintenance windows, even with overlapping times. Maintenance windows do not interfere with each other. For a patch deployment to take effect, the deployment and maintenance window times must be met.

Consider establishing a maintenance cycle that keeps your endpoints as up-to-date as possible. You can avoid many security risks with good operational hygiene. Some considerations might include coordinating with the Microsoft Patch Tuesday releases, on weekends, or outside the core work hours for your network. For example, you might create a maintenance window that starts three days after Microsoft Patch Tuesday each month.

For more information, see Setting maintenance windows on page 131.

© 2026 Tanium Inc. All Rights Reserved

Linux repository snapshots

A *repository snapshot* captures point-in-time metadata that determine patch versions and their dependencies and provides control over dependencies for Linux endpoint patches. Using a repository snapshot can help ensure that your production systems are installing the same patches as your testing systems, which reduces deployments of untested patches on production systems.



Use repository snapshots, instead of patch lists, for patching based on a current release date.



Be aware that CentOS reached its end of life in June 2024.

For more information, see Manage Linux repository snapshots on page 78.

Self Service Client application for Windows endpoints

With the Self Service Client application, you can publish patches to Windows endpoints so that users can start a patch deployment early or completely control when patches are installed. For example, you might deploy the Self Service Client application to a manufacturing endpoint that can be patched only between manufacturing runs or an endpoint in an operating room that must be patched between surgeries.

Patch self-service deployments and the Self Service Client application are used in conjunction with End-User Notification configurations in Tanium™ End-User Notifications 1.11.38 or later. The Self Service Client application is installed on endpoints targeted in the End-User Notification configuration.

For more information, see Managing End-User Self Service for Windows endpoints on page 135.

Tanium Autonomous IT Platform in Patch

Tanium Autonomous IT Platform comprises a set of interrelated features across multiple Tanium solutions. The Autonomous IT Platform provides guided initial configuration for solutions, proactively collects intelligence about conditions in Tanium environments, provides guidance based on those conditions, and enables automated workflows to address issues. For more information, see Tanium Console User Guide: Working with the Autonomous IT Platform. Tanium Patch provides the following Autonomous IT Platform features:

- **Confidence score**: The confidence score rates the probability that a Windows patch deployment will succeed and not cause post-installation downtime. Tanium assigns confidence scores to Windows patches released within the last 365 days or that are applicable in your environment. Use the score to determine if a patch is reliable enough for deployment or if you must first edit the endpoint targeting in the deployment. For more information, see Windows patch confidence score on page 19 and Tanium Console User Guide: Confidence score.

© 2026 Tanium Inc. All Rights Reserved

Supported languages

You can select one of the languages in the following table for user interface (UI) text in the Patch workbench and Tanium documentation. The language that you select for the workbench also sets the date and time format:

- **Dates**: In the table, the letters `dd`, `mm`, and `yyyy` represent the digits for day, month, and year respectively.
- **Times**: English (United States) times use the 12-hour clock in the format `hh:mm:ss [AM|PM] <time zone>`, where `hh`, `mm`, and `ss` represent the hour, minute, and second respectively. Other times use the 24-hour clock, where `GMT-<#>` indicates the offset from Greenwich Mean Time (GMT). For example, `GMT-7` indicates a time zone that is 7 hours ahead of GMT.

Supported languages with associated date and time formats

Language	Locale code	Date and time format
English (United States)	en-US	mm/dd/yyyy [AM|PM] <*time zone*>
French (France)	fr-FR	dd/mm/yyyy GMT-<#>
German (Germany)	de-DE	dd/mm/yyyy GMT-<#>
Japanese (Japan)	ja-JP	yyyy/mm/dd GMT-<#>
Korean (Korea, Republic of)	ko-KR	yyyy.mm.dd GMT-<#>
Spanish (Latin American)	es-LA	dd/mm/yyyy GMT-<#>

For information about language support, which types of text are translated, and the steps to select a language, see Tanium Console User Guide: Reference: Language support.

Patch versus Deploy

The following table describes the Tanium Patch and Tanium Deploy modules, and differentiates between Patch deployments and Deploy deployments. For more information, see Deploy overview .

Patch versus Deploy

Module	Description
Patch	Use the Tanium Patch module to install operating system patches, such as Windows Cumulative Updates. Create Patch deployments to download and install patches on a set of targeted endpoints.
Deploy	Use the Tanium Deploy module to install, update, or remove software on endpoints. Create Deploy deployments to deploy software on a set of targeted endpoints.

Interoperability with other Tanium products

Patch works with other Tanium products to provide additional features and reporting.

© 2026 Tanium Inc. All Rights Reserved

Tanium™ Automate

From the Automate **Install Patch** step, you can deploy software to target endpoints. For more information, see Tanium Automate User Guide.

Tanium™ Comply

From Comply vulnerability report results, you can open Patch to view details about the patch that resolves a reported vulnerability. You can also quickly install the patch to endpoints directly from the patch details page. For more information, see vulnerability report results in Tanium Comply User Guide: Working with reports.

Tanium™ End-User Notifications

With the Tanium End-User Notifications solution, you can notify users about deployments to Windows endpoints and configure End-User Self Service capabilities. You can create a notification message with your deployment to notify the user that the system is going to restart, and give the user the option to postpone the restart. For more information, see Tanium End-User Notifications User Guide.

Tanium™ Endpoint Configuration

With the Tanium Endpoint Configuration solution, you can enable approvals for endpoint configuration changes. For more information, see Tanium Endpoint Configuration User Guide.

Tanium™ Reporting

If you have Tanium Reporting 1.12 or later, Patch uses Tanium Reporting to create the charts on the Patch **Overview** page. For more information, see Tanium Reporting.

Tanium™ Trends

Patch has built in integration with Trends for additional reporting of patch data for Windows and Linux endpoints. The **Patch** board shows information about missing patches, service-level-agreement (SLA) based compliance reports, time between a patch release and its installation, endpoint status, and scan errors. The following sections and panels are in the **Patch** board:

- Summary
    - Patch Coverage
    - Endpoints Missing Critical or Important Patches Released Over 30 Days Ago
    - Workstations - Mean Time to Patch
    - Servers - Mean Time to Patch

© 2026 Tanium Inc. All Rights Reserved

- Missing Patches
    - Missing Critical/Important Patches per Year
    - Operating Systems Missing Critical/Important Patches
    - Missing Patches by Severity - Latest
    - Missing Patches by Severity - Last 90 Days
- SLA Based Compliance Reporting
    - Online Endpoints - Patch Compliance
    - Historical - Patch Compliance
    - Online Endpoints - 30 Day SLA Compliance
    - Historical - 30 Day SLA Compliance
- Endpoint Status
    - Days Since Last Patch Scan
- Errors
    - Scan Errors - Last 7 Days

For more information, see Tanium Trends User Guide: Importing the initial gallery.

© 2026 Tanium Inc. All Rights Reserved

Gaining organizational effectiveness with Patch

The four key organizational governance steps to maximizing the value that is delivered by Patch are as follows:

- Develop a dedicated change management process. For more information, see Change management on page 25.
- Define distinct roles and responsibilities. For more information, see RACI chart on page 25.
- Validate cross-functional alignment. For more information, see Organizational alignment on page 29.
- Track operational maturity. For more information, see Operational metrics on page 29.

Change management

Develop a tailored, dedicated change management process for patch management, taking into account the new capabilities provided by Tanium.

- Update SLAs with elevated expectations, from patch identification to patch deployment. For example, if you are an organization that typically patches critical OS vulnerabilities within 15 days with legacy tooling, transition to a five-day SLA.
- Identify internal and external dependencies to your patch management process (example: contractors who are responsible for a subset of IT estate).
- Designate change or maintenance windows for various patch management scenarios (example: emergency patching versus general maintenance patching).
- Create a Tanium steering group (TSG) for patching activities, to expedite reviews and approvals of processes that align with SLAs.

RACI chart

A RACI chart identifies the team or resource who is **R**esponsible, **A**ccountable, **C**onsulted, and **I**nformed, and serves as a guideline to describe the key activities across the security, risk/compliance, and operations teams. Every organization has specific business processes and IT organization demands. The following table represents Tanium's point of view for how organizations should align functional resources against patch management. Use the following table as a baseline example.

Task	IT Security	IT Operations	IT Risk/Compliance	Executive	Rationale
Standard patch notification For more information, see Standard patch workflow on page 28.	I	A/R	I	-	Standard patch cycles, such as Patch Tuesday, are owned by the operations team and have predefined notifications so that the security and risk/compliance teams are informed.

© 2026 Tanium Inc. All Rights Reserved

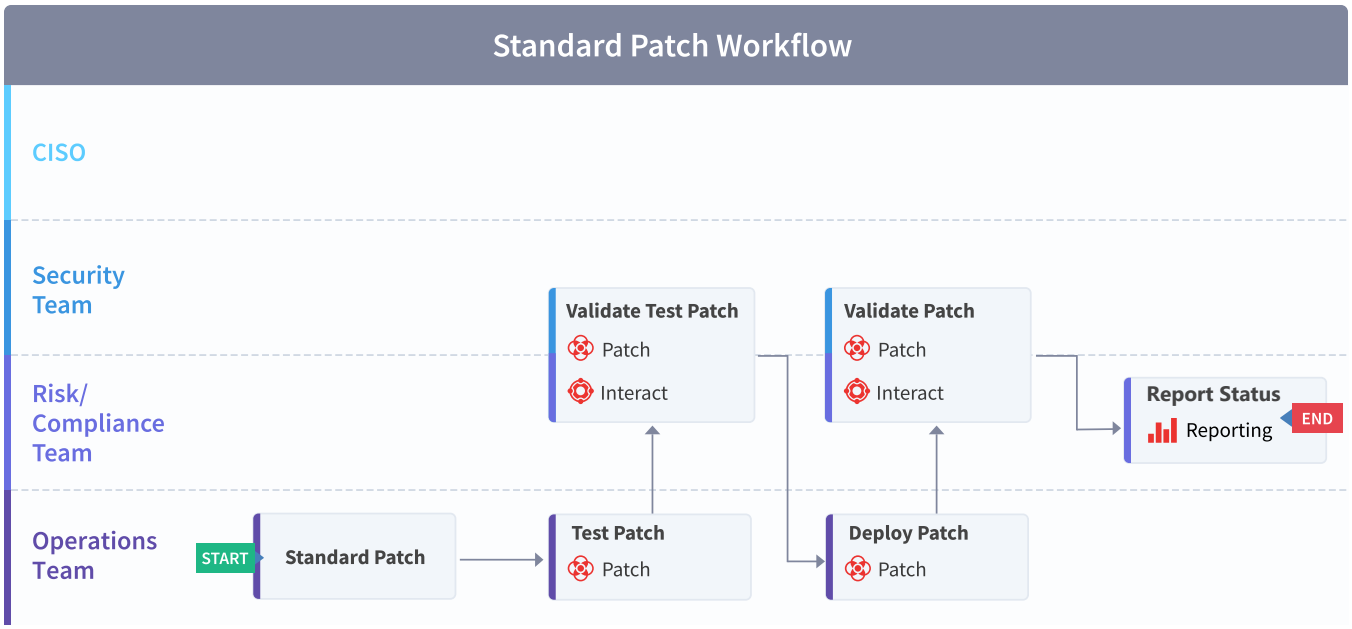
Task	IT Security	IT Operations	IT Risk/Compliance	Executive	Rationale
Zero-day/threat intel notification For more information, see Zero-day patch workflow on page 28.	A/R	I	I	C	Zero-days have a high security impact. The security team is accountable for informing the operations and risk/compliance teams, and consulting with the executive team.
Vulnerability scan patch notification For more information, see Vulnerability scan patch workflow on page 29.	A	I	R	C	The risk/compliance team identifies vulnerabilities based on tooling and notifies the security team. The security team is accountable and informs the operations team of the known threat.
Risk exposure scan	C	C	A/R	I	The risk/compliance team owns the tools that run the scan to understand risk and consults with the security and operations teams.
Deploy patches to test environment for user acceptance testing (UAT)	I	A/R	I	-	The operations team informs the security and risk/compliance teams when patching is completed so they can verify results.
Verification of remediation in test environment	C	C	A/R	-	The risk/compliance team owns the tools to verify that the systems are no longer vulnerable, and consults with the security and operations teams on the results.
Deploy patches to production environment	I	A/R	I	-	The operations team informs the security and risk/compliance teams when patching is completed so they can verify the results.

© 2026 Tanium Inc. All Rights Reserved

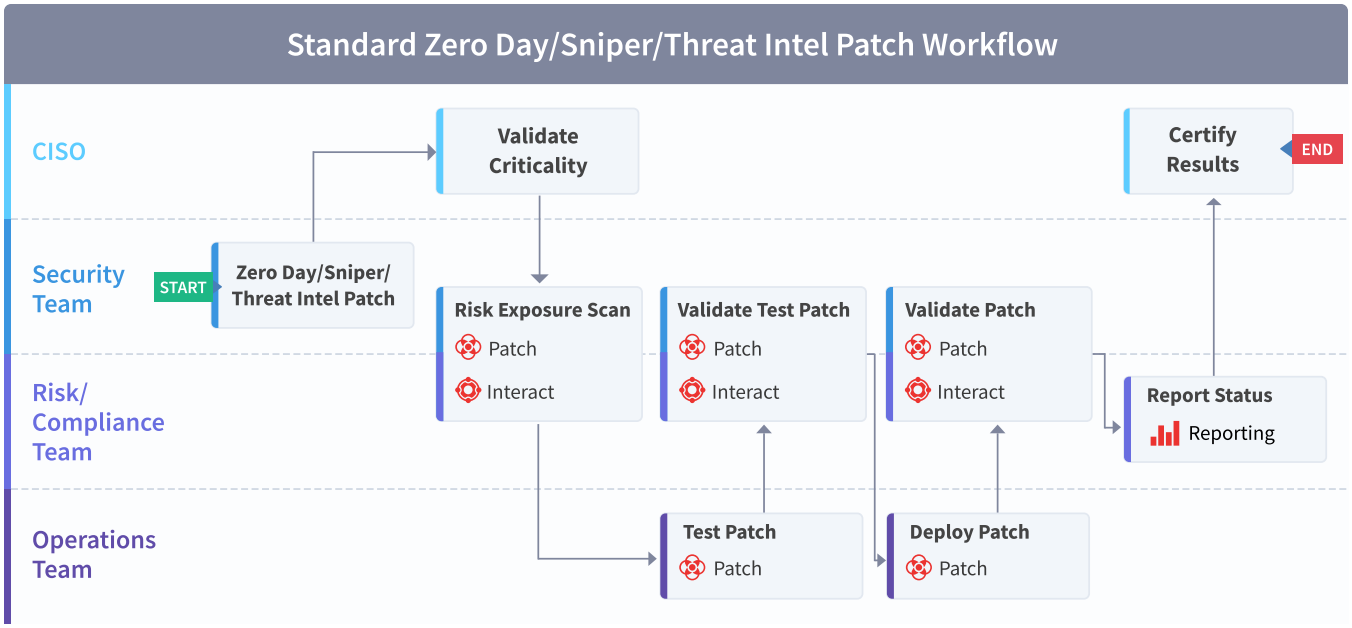
Task	IT Security	IT Operations	IT Risk/Compliance	Executive	Rationale
Verification of remediation in production environment	C	C	A/R	-	The risk/compliance team owns the tools to verify that the systems are no longer vulnerable, and consults with the security and operations teams on the results.
Track actions taken and escalation requests	C	A	R	I	The risk/compliance team is responsible for the vulnerabilities in the environment, informs the executive team, and consults with the security team. The operations team is accountable for taking any actions based on the escalation.
Reporting metrics/dashboard of remediation	A	A/R	I	I	The operations team is responsible and accountable for remediation reporting, consults with the security team on any questions, and informs the risk/compliance and executive team.
Reporting metrics/dashboard of risk	C	C	A/R	I	The risk/compliance team is responsible and accountable for risk reporting, consults with the security and operations teams on any questions, and informs the executive team.

© 2026 Tanium Inc. All Rights Reserved

Standard patch workflow

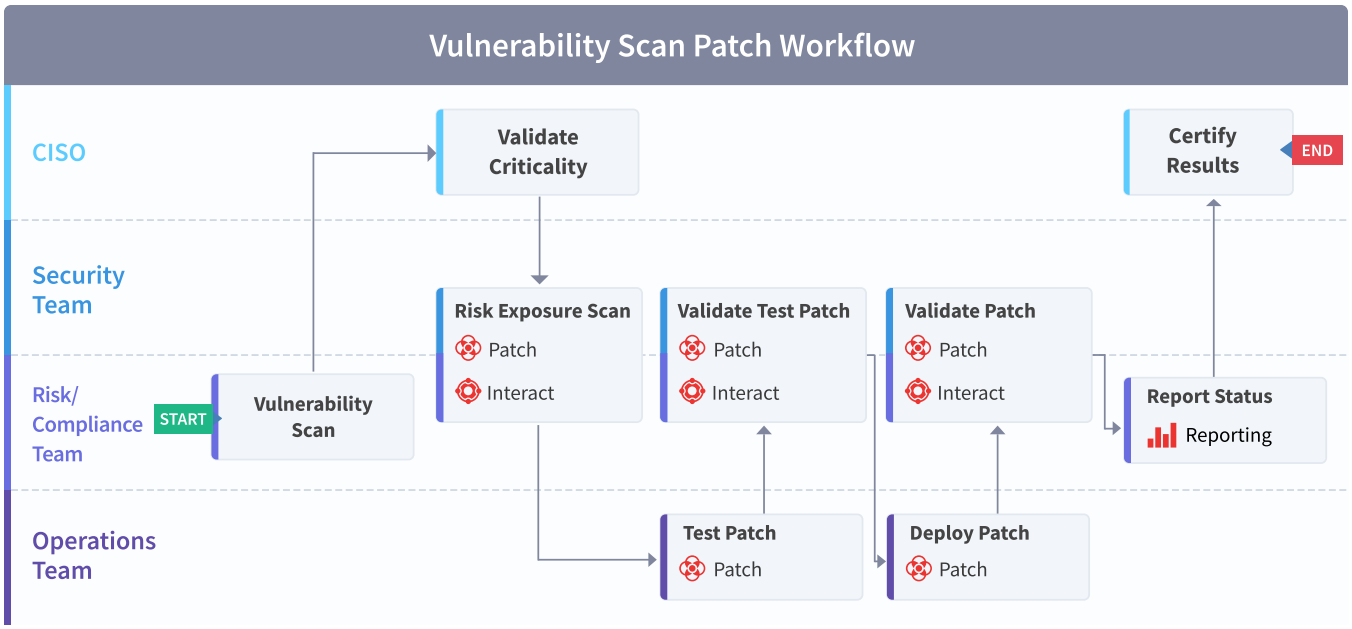


Zero-day patch workflow



© 2026 Tanium Inc. All Rights Reserved

Vulnerability scan patch workflow



Organizational alignment

Successful organizations use Tanium across functional silos as a common platform for high-fidelity endpoint data and unified endpoint management. Tanium provides a common data schema that enables security, operations, and risk/compliance teams to assure that they are acting on a common set of facts that are delivered by a unified platform.

In the absence of cross-functional alignment, functional silos often spend time and effort in litigating data quality instead of making decisions to improve patch management.

Operational metrics

Patch maturity

Managing a patching program successfully includes operationalization of the technology and measuring success through key benchmarking metrics. The four key processes to measure and guide operational maturity of your Tanium Patch program are as follows:

Process	Description
Usage	How and when Tanium Patch is used in your organization
Automation	How automated Tanium Patch is, across endpoints
Functional integration	How integrated Tanium Patch is, across IT security, IT operations, and IT risk/compliance teams
Reporting	How automated Tanium Patch is and who the audience of patch reporting is

© 2026 Tanium Inc. All Rights Reserved

Benchmark metrics for Windows and Linux endpoints

In addition to the key patch processes, the four key benchmark metrics that align to the operational maturity of the Tanium Patch program to achieve maximum value and success are as follows:

Executive Metrics	Patch Coverage	Endpoints Missing Critical or Important Patches Released Over 30 Days Ago	Workstations - Mean Time to Patch[1]	Servers - Mean Time to Patch
Description	Number of endpoints in each of these categories: • **Optimal**: Endpoints where Patch is operational • **Needs Attention**: Endpoints that do not have the Patch tools installed, are not targeted by a scan configuration, or do not have a supported version of the Tanium Client installed • **Unsupported**: Endpoints with an operating system version that is not supported by Patch	Percentage of endpoints that are missing critical or important patches released more than 30 days ago.	Average number of days between patch release date and patch application for workstations. Application includes installing the patch and restarting the workstation, if required. Calculation only considers installed patches and excludes missing patches.	Average number of days between patch release date and patch application for servers. Application includes installing the patch and restarting the workstation, if required.
Instrumentation	Number of endpoints with a patch scan age less than three days divided by total endpoints that are supported by Patch.	Number of endpoints that require critical or important patches that were released over 30 days ago divided by the number of endpoints with a scan configuration.	Number of days it takes for workstations to be fully patched and restarted after a patch is released, divided by the number of patches installed by Tanium. Calculation excludes patches installed by means other than Tanium Patch.	Number of days it takes for servers to be fully patched and restarted after a patch is released, divided by the number of patches installed by Tanium.

© 2026 Tanium Inc. All Rights Reserved

Executive Metrics	Patch Coverage	Endpoints Missing Critical or Important Patches Released Over 30 Days Ago	Workstations - Mean Time to Patch[1]	Servers - Mean Time to Patch
Why this metric matters	If you are not scanning all endpoints, then you are at risk. That risk must be highlighted and mitigated through other means (example: network isolation).	The sooner you know about an endpoint having an outstanding patch, the sooner you can deploy the patch or mitigate the risk until the patch is available.	If it takes you too long to deploy a patch and validate that it was applied, then you are at risk of being exploited by the vulnerabilities that are addressed by that patch.	If it takes you too long to deploy a patch and validate that it was applied, then you are at risk of being exploited by the vulnerabilities that are addressed by that patch.

[1] For Windows endpoints, the Mean Time to Patch sensor uses the OS installation date rather than patch release date for patches released before the OS was installed.

Use the following table to determine the maturity level for Tanium Patch in your organization.

© 2026 Tanium Inc. All Rights Reserved

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
Process	Usage	Patch configured	Patch used by exception (zero day or subset of environment)	Patch used to audit efficacy of legacy tooling	Patch used as default tooling for patch management; Legacy tooling used to audit patch efficacy	Patch used as default tooling for patch management
	Automation	Manual	Manual	Partially automated (>50% of patch deployment process automated)	Partially automated (>75% of patch deployment process automated)	Fully automated (>90% of patch deployment process automated)
	Functional integration	Functionally siloed	Consult with or take direction from peers in enterprise vulnerability management, and threat management	Consult with or provide direction for peers in enterprise vulnerability management, threat management, and asset management	Connect, Reporting, and Asset integrated into enterprise vulnerability management, threat management, and asset management tools	Connect, Reporting, and Asset integrated into enterprise vulnerability management, threat management, and asset management tools
	Reporting	Manual; Reporting for Operators only	Manual; Reporting for Operators and peer group only	Automated; Reporting for Operators and peer group only	Automated; Reporting tailored to stakeholders ranging from Operator to Executive	Automated; Reporting tailored to stakeholders ranging from Operator to Executive

© 2026 Tanium Inc. All Rights Reserved

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
(Windows and Linux) Metrics	Patch Coverage	< 93%	93-94%	95-96%	97-98%	99-100%
	Endpoints Missing Critical or Important Patches Released Over 30 Days Ago	> 15%	11-15%	6-10%	2-5%	0-1%
	Workstations - Mean Time to Patch	> 30 days	26-30 days	21-25 days	15-20 days	0-14 days
	Servers - Mean Time to Patch	> 60 days	46-60 days	31-45 days	21-30 days	0-20 days

© 2026 Tanium Inc. All Rights Reserved

Patch requirements

Review the requirements before you install and use Patch.

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium license that includes Patch. For more information about how to get Patch, see Tanium Solutions & Bundles.
- **Tanium™ Core Platform servers:**

  To support smart card authentication, including common access cards (CAC), see Tanium Core Platform User Guide for Windows Deployments: Configuring smart card authentication in a Windows deployment.
- **Tanium™ Client:** Any supported version of Tanium Client. For more information, see Tanium Client Management User Guide: Client version and host system requirements.

  If you use a Client version that is not listed, certain product features might not be available, or stability issues can occur that can only be resolved by upgrading to one of the listed Client versions.

Computer group dependencies

When you first sign in to Tanium Console after a fresh installation of Tanium Server, the server automatically imports the computer groups that Patch requires for managing endpoints:

- `All Alma Linux 8`
- `All Alma Linux 9`
- `All Amazon`
- `All Debian`
- `All Debian 8`
- `All Debian 9`
- `All Debian 10`
- `All Debian 11`
- `All Debian 12`
- `All CentOS 6`
- `All CentOS 7`
- `All CentOS 8`
- `All OpenSUSE 15`
- `All Oracle 6`

© 2026 Tanium Inc. All Rights Reserved

- `All Oracle 7`
- `All Oracle 8`
- `All Oracle 9`
- `All Red Hat 6`
- `All Red Hat 7`
- `All Red Hat 8`
- `All Red Hat 9`
- `All Rocky Linux 8`
- `All Rocky Linux 9`
- `All SLES 11`
- `All SLES 12`
- `All SLES 15`
- `All SUSE`
- `All Ubuntu 14.04 - amd64`
- `All Ubuntu 14.04 - i386`
- `All Ubuntu 14.04 - arm64`
- `All Ubuntu 16.04 - amd64`
- `All Ubuntu 16.04 - i386`
- `All Ubuntu 16.04 - arm64`
- `All Ubuntu 18.04 - amd64`
- `All Ubuntu 18.04 - i386`
- `All Ubuntu 18.04 - arm64`
- `All Ubuntu 20.04 - amd64`
- `All Ubuntu 20.04 - i386`
- `All Ubuntu 20.04 - arm64`
- `All Ubuntu 22.04 - amd64`
- `All Ubuntu 22.04 - i386`
- `All Ubuntu 22.04 - arm64`
- `All Ubuntu 24.04 - amd64`
- `All Ubuntu 24.04 - i386`

© 2026 Tanium Inc. All Rights Reserved

- `All Ubuntu 24.04 - arm64`
- `All Windows`
- `All Windows Servers`
- `Patch Supported Systems`

For earlier versions of the Tanium Server, or after upgrading from an earlier version, you must manually create the computer groups. For more information, see Tanium Console User Guide: Create a computer group.

Solution dependencies

Other Tanium solutions are required for Patch to function (required dependencies) or for specific Patch features to work (feature-specific dependencies). The installation method that you select determines if the Tanium Server automatically imports dependencies or if you must manually import them.



Some Patch dependencies have their own dependencies, which you can see by clicking the links in the lists of Required dependencies on page 36 and Feature-specific dependencies on page 37. Note that the links open the user guides for the latest version of each solution, not necessarily the minimum version that Patch requires.

Tanium recommended installation

If you select **Tanium Recommended Installation** when you import Patch, the Tanium Server automatically imports all your licensed solutions at the same time. For more information, see Tanium Console User Guide: Import all modules and services.

Import specific solutions

If you select only Patch to import and are using Tanium Core Platform 7.5.2.3531 or later with Tanium Console 3.0.72 or later, the Tanium Server automatically imports the latest available versions of any required dependencies that are missing. If some required dependencies are already imported but their versions are earlier than the minimum required for Patch, the server automatically updates those dependencies to the latest available versions.

If you select only Patch to import and you are using Tanium Core Platform 7.5.2.3503 or earlier with Tanium Console 3.0.64 or earlier, you must manually import or update required dependencies. For more information, see Tanium Console User Guide: Import, re-import, or update specific solutions.

Required dependencies

Patch has the following required dependencies:

- Tanium™ Endpoint Configuration
- Tanium™ Data Service (TDS)

© 2026 Tanium Inc. All Rights Reserved

- Tanium™ Trends
- Tanium™ End-User Notifications
- Tanium™ System User Service

Feature-specific dependencies

If you select only Patch to import, you must manually import or update its feature-specific dependencies regardless of Tanium Console or Tanium Core Platform versions. Patch has the following feature-specific dependencies:

- Tanium™ Reporting. Review charts on the **Overview** page. If Reporting is not installed, Trends creates the charts.
    - Tanium™ Blob Service
    - Reporting Content

Client extensions and endpoint tools

Tanium Endpoint Configuration installs Client Extensions and other tools for Patch on endpoints. Client extensions perform tasks that are common to certain Tanium solutions. Each Client Extension and tool might have recommended security exclusions to allow them to run without interference. For more information, see Security exclusions. For a list of Patch tools, see Reference: Patch endpoint tools on page 171. For a list of all Client Extensions and tools, see Tanium Client Management User Guide: Reference: Client extensions used for Tanium solutions.

Tanium Server and Module Server computer resources

Patch is installed and runs as a service on the Module Server host computer. The impact on the Module Server is minimal and depends on usage. You might need to tune the Tanium Server to set bandwidth limits for your environment. You can configure global throttles from **Administration > Configuration > Bandwidth Throttles**.

The Tanium Server needs an additional 500 GB of disk space as Tanium Patch downloads and distributes updates regularly. The Tanium Server stores these update packages within the `Downloads` directory.



If the UUP proxy feature is enabled, UUP might use up to 200 GB of the required 500 GB. The actual amount of disk space used depends on the size of the Windows update files. For more information, see Enable UUP Proxy on page 66.

For more information about other computer resources, see Tanium Core Platform User Guide for Windows Deployments: Reference: Host system resource guidelines and Tanium Appliance Deployment Guide: Reference: Tanium Appliance Specifications.

© 2026 Tanium Inc. All Rights Reserved

Endpoints

Supported operating systems

The following endpoint operating systems are supported with Patch. Specific version requirements depend on the version of Patch and components that you are using. For more information about Tanium Client versions, see Tanium Client Management User Guide: Client version and host system requirements.

Operating System	Version	Notes
Microsoft Windows Server	Windows Server 2012 or later	• Windows Server Core not supported for End-User Notifications functionality. • Windows Server 2012 R2 requires Microsoft KB2919394 or KB2919355 for End-User Self Service functionality.
Microsoft Windows Workstation	Windows 10 or later	• Patch supports Windows 11 endpoints with Arm processors. • For information about Windows 10 Home and Windows 11 Home support, see Available Patch scan methods for Windows endpoints on page 13.
Microsoft Windows Server (Legacy)	Windows Server 2008 R2 Service Pack 1[1]	• Windows Server Core not supported for End-User Notifications functionality. • Windows Server 2008 R2 Service Pack 1 requires Microsoft KB2758857. • Windows Server 2012 R2 requires Microsoft KB2919394 or KB2919355 for End-User Self Service functionality.
Microsoft Windows Workstation (Legacy)	Windows 7 Service Pack 1[1] Windows 8.1[1]	• Windows 7 Service Pack 1 requires Microsoft KB2758857. • Windows 8.1 requires Microsoft KB2919394 or KB2919355 for End-User Self Service functionality.

© 2026 Tanium Inc. All Rights Reserved

Operating System	Version	Notes
Linux	AlmaLinux 8.x, 9.x	
	Amazon Linux 1[1], 2, 2023	• Requires Yum version 3.2.29-22.el6 or later for systems using OS-based Linux distributions. • For deployments to Amazon Linux 2023 endpoints, you can only **Install All Updates** or **Install All Security Updates**. You cannot deploy using the **Choose Patch List** or **Manually Select Patches** options.
	CentOS 6.x[1], 7.x[1], 8.x[1]	• CentOS 6.x and 7.x require Yum version 3.2.29-22.el6 or later for systems using OS-based Linux distributions. • Cent OS 8.x requires DNF.
	Debian 8.x, 9.x, 10.x, 11.x, 12.x	• Requires APT.
	openSUSE Linux 11.x Service Pack 3 or later, 12.x[1], 15.x	• Requires Zypper. • SUSE 11.x Service Pack 3 support is limited to scanning only.
	Oracle Linux 6.x[1], 7.x, 8.x, 9.x	• Oracle Linux 6.x and 7.x require Yum version 3.2.29-22.el6 or later for systems using OS-based Linux distributions. • Oracle Linux 8.x and later requires DNF.
	Red Hat Enterprise Linux 6.x[1], 7.x, 8.x, 9.x	• Requires Yum version 3.2.29-22.el6 or later for systems using OS-based Linux distributions. • Red Hat endpoints must be registered to a Red Hat subscription. For more information, see Linux scan techniques on page 92. • Red Hat Enterprise Linux 8.x and 9.x requires DNF.
	Rocky Linux 8.x, 9.x	• Rocky Linux 8.x and 9.x requires DNF.
	SUSE Linux Enterprise Server 11.x Service Pack 3 or later, 12.x, 15.x	• Requires Zypper.
	Ubuntu 14.04, 16.04, 18.04, 20.04, 22.04, 24.04	• Requires APT.

[1] This operating system version has reached end of life. Tanium cannot guarantee Tanium Patch on operating system versions that have reached end of life.

© 2026 Tanium Inc. All Rights Reserved

Resource requirements

- The utilities that Patch uses for scanning use increased RAM for up to several minutes during endpoint scans. If an endpoint must also run other processes that use significant RAM during Patch scans, it might require more RAM than the minimum 2 GB. For more information, see Tanium Client Management User Guide: Hardware requirements.
- Endpoints must have at least 5 GB available in free disk space. For more information, see Tanium Client Management User Guide: Hardware requirements.
- Linux endpoints often use restricted volumes. The Tanium Client stores the repository scanning logic in the local Tanium Client directory. Package managers (for example, Yum, DNF, Zypper, and Apt) cache repository data in the `/var` partition. In most cases, the cache does not exceed 500 MB. If you use lean partitioning or have a high count of configured repositories, evaluate the available disk space and partition configurations to ensure `/var` has sufficient free space.
- On Tanium Console **Administration > Configuration > Settings > Advanced Settings** page, set the Tanium Client cache limit (**ClientCacheLimitInMB**) to 2048 MB. For more information, see Configure advanced settings on page 56 and Tanium Console User Guide: Managing Tanium Core Platform settings.
- If VDI is used in your environment, see the Tanium Client Management User Guide: Preparing the Tanium Client on a virtual desktop infrastructure (VDI) instance.

Third-party software

Patch requires that Windows endpoints have Windows Update Agent. If you are controlling all patch deployments through Tanium, disable the Windows Update Agent automatic functions at the domain level.

Host and network security requirements

Specific ports, processes, and URLs are needed to run Patch.

Ports

The following ports are required for Patch communication.

Source	Destination	Port	Protocol	Purpose
Module Server	Module Server (loopback)	17454	TCP	Internal purposes; not externally accessible



Configure firewall policies to open ports for Tanium traffic with TCP-based rules instead of application identity-based rules. For example, on a Palo Alto Networks firewall, configure the rules with service objects or service groups instead of application objects or application groups.

© 2026 Tanium Inc. All Rights Reserved

Security exclusions

If antivirus (AV) or other security software is in use in the environment to monitor and block unknown host system processes, Tanium requires that a security administrator create exclusions to allow the Tanium processes to run without interference. This software can include security applications that are included with an endpoint operating system, such as `fapolicyd` on some Linux distributions, or Microsoft Defender on Windows. The configuration of these exclusions varies depending on the security software. For more information about security exclusions to define across Tanium, see Tanium Client Management Guide: Reference: Endpoint security exclusions and for Windows-based Tanium Core Platform deployments, see Tanium Core Platform User Guide for Windows Deployments: Tanium Core Platform Server security exclusions.



If the required exclusions are not configured, or if Tanium suspects interference from AV or security software, Tanium might require you to remove or disable the AV or security software temporarily for the purposes of troubleshooting and restore it once troubleshooting is complete.

Patch security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\patch-service\node.exe`
	Required when Endpoint Configuration is installed	Process	`<Module Server>\services\endpoint-configuration-service\TaniumEndpointConfigService.exe`

The Tanium Client uses the Windows Update offline scan file, `Wsusscn2.cab`, to assess computers for installed or missing operating system and application security patches. If your endpoint security solutions scan archive files, refer to the Microsoft KB for information on how to configure those tools to interact appropriately with the `Wsusscn2.cab` file.

For Windows endpoints, review and follow the Microsoft antivirus security exclusion recommendations for enterprise computers. For more information, see Microsoft Support: Virus scanning recommendations for Enterprise computers that are running currently supported versions of Windows (KB822158).

© 2026 Tanium Inc. All Rights Reserved

Patch security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Process	<*Tanium Client*>\TaniumCX.exe
		File	<*Tanium Client*>\TaniumClientExtensions.dll
		File	<*Tanium Client*>\TaniumClientExtensions.dll.sig
		File	<*Tanium Client*>\Patch\lib\tanium-patch.min.vbs
		File	<*Tanium Client*>\Patch\scans\Wsusscn2.cab
		Process	<*Tanium Client*>\Patch\tools\active-user-sessions.exe
		File	<*Tanium Client*>\Patch\tools\run-patch-manager.min.vbs
		Process	<*Tanium Client*>\Patch\tools\TaniumExecWrapper.exe
		Process	<*Tanium Client*>\Patch\tools\TaniumFileInfo.exe
		Process	<*Tanium Client*>\Patch\tools\TaniumUpdateSearcher.exe
		Folder	<*Tanium Client*>\python312
		Process	<*Tanium Client*>\python312\TPython.exe
		File	<*Tanium Client*>\TPython\TPython.bat
		Folder	<*Tanium Client*>\TPython312
		Process	<*Tanium Client*>\Tools\Patch\7za.exe
		File	<*Tanium Client*>\extensions\TaniumSoftwareManager.dll
		File	<*Tanium Client*>\extensions\TaniumSoftwareManager.dll.sig
	Exclude from on-access or real-time scans	Folder	<*Tanium Client*>

© 2026 Tanium Inc. All Rights Reserved

Patch security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
Linux		File	`<Tanium Client>/libTaniumClientExtensions.so`
		File	`<Tanium Client>/libTaniumClientExtensions.so.sig`
		Process	`<Tanium Client>/python312/bin/pybin`
		Process	`<Tanium Client>/python312/python`
		Folder	`<Tanium Client>/python312`
		Process	`<Tanium Client>/TPython/TPython`
		Folder	`<Tanium Client>/TPython312`
		File	`<Tanium Client>/extensions/libTaniumSoftwareManager.so`
		File	`<Tanium Client>/extensions/libTaniumSoftwareManager.so.sig`

Third-party internet URLs

If security software is deployed in the environment to monitor and block unknown URLs, your security administrator must allow access to Internet URLs on the Tanium Server, Tanium Module Server, or endpoints, depending on the operating system of the endpoints and your Patch configuration. The complete list might vary based on your environment.

- Windows endpoints:
  - The Tanium Server needs access to the URLs if Patch is scanning Windows endpoints. For more information, see Windows scan techniques on page 90.
  - The Tanium Module Server needs access to `www.microsoft.com` when Patch uses the Tanium Scan technique. For more information, see Windows scan techniques on page 90.
  - The Windows endpoints need access to the URLs if you are using direct patch downloads. For more information, see Enable direct patch downloads from Microsoft on page 67.
- Linux endpoints:
  - The Tanium Server needs access to the URLs used by a scan configuration that uses the Tanium Scan technique. For more information, see Linux scan techniques on page 92.
  - The Linux endpoints need access to the URLs used by a scan configuration that uses the Repository Scan technique. For more information, see Linux scan techniques on page 92.

© 2026 Tanium Inc. All Rights Reserved

TIP

For a complete list of URLs needed in your environment, in Interact ask the question `Get Patch - Repositories from all machines with Is Linux equals True`. Review the URLs listed in the **Base URL** column.

Internet URLs to allow

Operating System	Source (Requestor)	URL
Windows	• Endpoints using direct download[1] • Windows 11, version 22H2 or later endpoints if not using Tanium architecture to deliver cumulative updates • Tanium Server[2]	`*.delivery.mp.microsoft.com`
		`*.prod.do.dsp.mp.microsoft.com`
		`*.update.microsoft.com`
		`*.windowsupdate.com`
		`*.windowsupdate.microsoft.com`
		`http://crl.microsoft.com`
		`http://emdl.ws.microsoft.com`
		`http://go.microsoft.com/fwlink/?linkid=74689`
		`http://ntservicepack.microsoft.com`
		`http://windowsupdate.microsoft.com`
		`http://wustat.windows.com`
		`https://download.microsoft.com`
		`https://sws.update.microsoft.com`
Windows	Tanium Module Server	`https://sws.update.microsoft.com`
		`*.microsoft.com` if using the Tanium Scan technique. For more information, see Windows scan techniques on page 90.

© 2026 Tanium Inc. All Rights Reserved

Internet URLs to allow (continued)

Operating System	Source (Requestor)	URL
Linux	• Tanium Server[3] • Tanium Module Server[4] • Endpoints[5]	`http://vault.centos.org/`
		`http://mirror.centos.org`
		`http://yum.oracle.com`
		`https://cdn.redhat.com`
		`http://download.opensuse.org`
		`http://deb.debian.org`
		`http://security.debian.org`
		`http://archive.ubuntu.com`
		`http://ports.ubuntu.com`
		`http://security.ubuntu.com`
		`http://dl.rockylinux.org`
		`https://repo.almalinux.org`
		`https://dl.suse.com`
		`https://dl-ipv4.suse.com`
		`https://public-dl.suse.com`
		`https://public-dl-ipv4.suse.com`
		`https://updates.suse.com`

[1] Enable direct patch downloads from Microsoft on page 67.

[2] Needed if Patch is scanning Windows endpoints.

[3] Needed if using a scan configuration that uses the Tanium Scan technique.

[4] Needed if using repository snapshots.

[5] Needed if using a scan configuration that uses the Repository Scan scan technique.

User role requirements

Predefined roles grant the following permissions, which are required to use Patch functionality:

© 2026 Tanium Inc. All Rights Reserved

- Patch solution permissions on page 46
- Provided Patch administration and platform content permissions on page 50: The solution permissions automatically provide some of these permissions.

To review a summary of the predefined roles, see Set up Patch users on page 63.

Some Patch solution permissions provide permissions that are associated with other solutions. Furthermore, all the platform content permissions and some solution permissions apply to content sets that might contain content for other solutions in addition to Patch. If you create custom roles for Patch users, be sure to assign all the solution permissions and content set permissions that are required for Patch functionality. If you are not sure which permissions are required for a custom role, view the permissions of the predefined roles. For more information, see the following sections of the Tanium Console User Guide:

- RBAC overview (provides an overview of roles, permissions, and content sets)
- Provided role permissions
- View effective role permissions
- Configure a custom role



Do not assign the **Patch Service Account** and **Patch Service Account - All Content Sets** roles to users. These roles are for internal purposes only.

Patch solution permissions

Permission	Patch Administrator[1]	Patch Configuration Author[1]	Patch Deployment Author[1]	Patch Endpoint Configuration Approver[1]	Patch Operator[1]	Patch Read Only User[1]	Patch Super User[1]
Linux Patch Access to the Linux Patch content	✓ USER	✓ USER	✓ USER	✗	✓ USER	✓ USER	✓ USER
Patch INITIALIZE: Set up Patch activities for the granted content sets SHOW: View the Patch workbench	✓ INITIALIZE SHOW	✓ SHOW	✓ SHOW	✗	✓ INITIALIZE SHOW	✓ SHOW	✓ INITIALIZE[2] SHOW

© 2026 Tanium Inc. All Rights Reserved

Patch solution permissions (continued)

Permission	Patch Administrator[1]	Patch Configuration Author[1]	Patch Deployment Author[1]	Patch Endpoint Configuration Approver[1]	Patch Operator[1]	Patch Read Only User[1]	Patch Super User[1]
Patch Block List Create, modify, and delete block lists for the granted content sets	✓[2,3] READ WRITE EXECUTE DELETE	✓[2] READ WRITE DELETE	✓[2] READ	✗	✓[2] READ WRITE EXECUTE DELETE	✓[2] READ	✓[2] READ WRITE EXECUTE DELETE
Patch Deployment Create, modify, and delete deployments for the granted content sets	✓[2,3] READ WRITE EXECUTE DELETE	✓[2] READ	✓[2] READ WRITE EXECUTE DELETE	✗	✓[2] READ WRITE EXECUTE DELETE	✓[2] READ	✓[2] READ WRITE EXECUTE DELETE
Patch Endpoint Configuration Approve changes to Patch endpoint configurations	✗	✗	✗	✓ APPROVER	✗	✗	✗
Patch Maintenance Window Create, modify, and delete enforcements in maintenance windows for the granted content sets	✓[2,3] READ WRITE EXECUTE DELETE	✓[2] READ WRITE DELETE	✓[2] READ	✗	✓[2] READ WRITE EXECUTE DELETE	✓[2] READ	✓[2] READ WRITE EXECUTE DELETE

© 2026 Tanium Inc. All Rights Reserved

Patch solution permissions (continued)

Permission	Patch Administrator[1]	Patch Configuration Author[1]	Patch Deployment Author[1]	Patch Endpoint Configuration Approver[1]	Patch Operator[1]	Patch Read Only User[1]	Patch Super User[1]
Patch MDM Configuration Create, modify, and delete MDM settings and enforcements	✓ READ WRITE DELETE	✗	✗	✗	✗	✗	✓ READ WRITE DELETE
Patch MDM Deployment Create, modify, and delete MDM deployments	✓ READ WRITE DELETE	✗	✗	✗	✗	✗	✓ READ WRITE DELETE
Patch MDM Enforcement Create, modify, and delete MDM enforcements	✓ READ WRITE DELETE	✗	✗	✗	✗	✗	✓ READ WRITE DELETE
Patch Operator Settings Write access to a subset of platform settings in the Patch module	✓ WRITE	✗	✗	✗	✓ WRITE	✗	✗
Patch Patchlist Create, modify, and delete enforcements in patch lists for the granted content sets	✓[2,3] READ WRITE EXECUTE DELETE	✓[2] READ WRITE EXECUTE DELETE	✓[2] READ	✗	✓[2] READ WRITE EXECUTE DELETE	✓[2] READ	✓[2] READ WRITE EXECUTE DELETE

© 2026 Tanium Inc. All Rights Reserved

Patch solution permissions (continued)

Permission	Patch Administrator[1]	Patch Configuration Author[1]	Patch Deployment Author[1]	Patch Endpoint Configuration Approver[1]	Patch Operator[1]	Patch Read Only User[1]	Patch Super User[1]
Patch Profile Create, modify, and delete profiles	✓ READ WRITE EXECUTE DELETE	✗	✗	✗	✓ WRITE EXECUTE DELETE	✓ READ	✓ WRITE EXECUTE DELETE
Patch Repository Create, modify, and delete repositories	✓ READ WRITE EXECUTE DELETE	✓ READ	✗	✗	✓ READ WRITE EXECUTE	✓ READ	✓ READ EXECUTE
Patch Repository Snapshot Create, edit, and delete repository snapshots	✓ READ WRITE DELETE	✓ READ WRITE DELETE	✗	✗	✓ READ WRITE DELETE	✓ READ	✓ READ WRITE DELETE
Patch Scan Configuration Create, modify, and delete scan configurations	✓ READ WRITE EXECUTE DELETE	✓ READ WRITE DELETE	✗	✗	✓ READ WRITE EXECUTE DELETE	✓ READ	✓ READ WRITE EXECUTE DELETE
Patch Settings Write access to all Patch settings	✓ READ WRITE	✓ READ	✓ READ	✗	✓ READ	✓ READ	✓ READ
Patch Solution Install or uninstall Patch	✓ UPGRADE	✗	✗	✗	✗	✗	✗

© 2026 Tanium Inc. All Rights Reserved

Patch solution permissions (continued)

Permission	Patch Administrator[1]	Patch Configuration Author[1]	Patch Deployment Author[1]	Patch Endpoint Configuration Approver[1]	Patch Operator[1]	Patch Read Only User[1]	Patch Super User[1]
Patch Statistics Access to the Patch statistics logs	✓ LOGS	✗	✗	✗	✗	✗	✗
Windows Patch Access to the Windows Patch content	✓ USER	✓ USER	✓ USER	✗	✓ USER	✓ USER	✓ USER

[1] The permissions for this role provide solution permissions for other solutions. To view the provided permissions, see Tanium Console User Guide: View effective role permissions.

[2] Grants access to content in the Patch Content Set content set.

Provided Patch administration and platform content permissions

Permission	Permission Type	Patch Administrator 1	Patch Configuration Author[1]	Patch Deployment Author[1]	Patch Endpoint Configuration Approver	Patch Operator 1	Patch Read Only User[1]	Patch Super User[1]
Action Group	Administration	✓ READ	✓ READ	✓ READ	✗	✓ READ	✓ READ	✓ READ
Allowed Urls	Administration	✓ READ WRITE	✗	✗	✗	✗	✗	✗
Action	Platform Content	✓ READ WRITE	✓ WRITE	✓ READ WRITE	✗	✓ READ WRITE	✗	✓ READ WRITE
Filter Group	Platform Content	✓ READ	✓ READ	✓ READ	✗	✓ READ	✓ READ	✓ READ
Own Action	Platform Content	✓ READ	✓ READ	✓ READ	✗	✓ READ	✗	✓ READ

© 2026 Tanium Inc. All Rights Reserved

Provided Patch administration and platform content permissions (continued)

Permission	Permission Type	Patch Administrator [1]	Patch Configuration Author[1]	Patch Deployment Author[1]	Patch Endpoint Configuration Approver	Patch Operator [1]	Patch Read Only User[1]	Patch Super User[1]
Package	Platform Content	✓ READ WRITE	✓ READ	✓ READ WRITE	✗	✓ READ WRITE	✗	✓ READ WRITE
Plugin	Platform Content	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE
Saved Question	Platform Content	✓ READ WRITE	✓ READ	✓ READ	✗	✓ READ WRITE	✓ READ	✓ READ WRITE
Sensor	Platform Content	✓ READ	✓ READ	✓ READ	✗	✓ READ	✓ READ	✓ READ

[1] The permissions for this role provide solution permissions for other solutions. To view the provided permissions, see Tanium Console User Guide: View effective role permissions.

© 2026 Tanium Inc. All Rights Reserved

Installing Patch

Use the **Solutions** page to install Patch and choose either automatic or manual configuration:

- **Automatic configuration with default settings**: Patch is installed with any required dependencies and other selected products. After installation, the Tanium Server automatically configures the recommended default settings. This option is the best practice for most deployments. For more information about the automatic configuration for Patch, see Import Patch with default settings on page 52.
- **Manual configuration with custom settings**: After installing Patch, you must manually configure required settings. Select this option only if Patch requires settings that differ from the recommended default settings. For more information, see Import Patch with custom settings on page 53.

Before you begin

- Read the release notes.
- Review the Patch requirements on page 34.
- If you are upgrading from a previous version, see Installing Patch on page 52.

Import Patch with default settings

You can set the Patch action group to target the **No Computers** filter group by enabling restricted targeting before importing Patch. This option enables you to control tools deployment through scheduled actions that are created during the import and that target the Tanium Patch action group. For example, you might want to test tools on a subset of endpoints before deploying the tools to all endpoints. In this case, you can manually deploy the tools to an action group that you configured to target only the subset. To configure an action group, see Tanium Console User Guide: Managing action groups. To enable or disable restricted targeting, see Tanium Console User Guide: Tools deployment and restricted targeting.

When you import Patch with automatic configuration, the following default settings for managing Windows and Linux endpoints are configured:

Setting	Default value
Action group	• Restricted targeting disabled (default): `Patch Supported Systems` computer group • Restricted targeting enabled: `No Computers` computer group
Advanced settings	The following advanced setting is configured for optimal delivery of larger payloads: • `ClientCacheLimitInMB` = 2048 For more information, see Configure advanced settings on page 56.
Patch computer groups	Computer groups that Patch requires are imported. For more information, see Computer group dependencies.

© 2026 Tanium Inc. All Rights Reserved

Setting	Default value
Patch scans	• Tanium Scan for Windows is configured and synchronized. • Default scan configurations are created for Windows and Linux and enforced by the recommended computer group. NOTE Tanium Scan does not include any Red Hat repositories because authentication for cdn.redhat.com must first be configured. For more information, see (Red Hat endpoints) Configure Tanium Server to use certificate authentication on page 72.
Patch lists	The following patch lists are automatically created: • **[Patch Baseline Deployment] - Windows** • **[Tanium Patch Baseline Reporting] - Windows** • **[Tanium Patch Baseline Reporting] - Linux** • **All Patches** • **[Tanium Patch Recommended Updates] - Windows** For more information, see Default patch lists on page 100.
Patch block lists	• The **[Global Block List] - Windows** block list is created and targets the `Patch Supported Systems` computer group. This block list excludes **Security Only** patches on Windows systems. For more information, see Microsoft update and servicing details on page 19. • A default block list is created for Linux but is not targeted.
Patch deployment templates	Default deployment templates are created for Windows and Linux.
Patch maintenance windows	• A **[Patch Tuesday] - Windows** default maintenance window is created for Patch Tuesday and is not enforced on any computer groups. • Default maintenance windows are created for Windows and Linux to block patch installations and reboots without first enabling another maintenance window. These maintenance windows are not enforced to any computer groups.

To import Patch and configure default settings, be sure to select the **Apply All Tanium recommended configurations** checkbox while performing the steps in Tanium Console User Guide: Import all modules and services. After the import, verify that the correct version is installed: see Verify Patch version on page 54.

Import Patch with custom settings

To import Patch without automatically configuring default settings, be sure to clear the **Apply All Tanium recommended configurations** checkbox while performing the steps in Tanium Console User Guide: Import or update specific solutions. After the import, verify that the correct version is installed: see Verify Patch version on page 54.

© 2026 Tanium Inc. All Rights Reserved

To organize computer groups, see Organize computer groups for Windows and Linux endpoints on page 59.

To configure the Patch action group, see Configuring Patch on page 55.

Manage solution dependencies

Other Tanium solutions are required for Patch to function (required dependencies) or for specific Patch features to work (feature-specific dependencies). For more information, see Solution dependencies on page 36.

Upgrade Patch

For the steps to upgrade Patch, see Tanium Console User Guide: Managing Tanium solutions. After the upgrade, verify that the correct version is installed: see Verify Patch version on page 54.

Verify Patch version

After you import or upgrade Patch, verify that the correct version is installed:

1. Refresh your browser.
2. From the Main menu, go to **Modules > Patch** to open the Patch **Overview** page.
3. To show version information, click Info .

© 2026 Tanium Inc. All Rights Reserved

Configuring Patch

If you did not install Patch with the **Apply All Tanium recommended configurations**, you must enable and configure certain features.

Configure Tanium Patch to ensure that you can effectively and accurately deploy patches to your targeted endpoints. Configurations include setting action groups, defining scan methods, and enabling features.

Restricted targeting

You can set the Patch action group to target the **No Computers** filter group by enabling restricted targeting before importing Patch. This option enables you to control tools deployment through scheduled actions that are created during the import and that target the Tanium Patch action group. For example, you might want to test tools on a subset of endpoints before deploying the tools to all endpoints. In this case, you can manually deploy the tools to an action group that you configured to target only the subset. To configure an action group, see Tanium Console User Guide: Managing action groups. To enable or disable restricted targeting, see Tanium Console User Guide: Tools deployment and restricted targeting.

Default settings

When you import Patch with automatic configuration, the following default settings for managing Windows and Linux endpoints are configured:

Setting	Default value
Action group	• Restricted targeting disabled (default): `Patch Supported Systems` computer group • Restricted targeting enabled: `No Computers` computer group
Advanced settings	The following advanced setting is configured for optimal delivery of larger payloads: • `ClientCacheLimitInMB` = 2048 For more information, see Configure advanced settings on page 56.
Patch computer groups	Computer groups that Patch requires are imported. For more information, see Computer group dependencies.
Patch scans	• Tanium Scan for Windows is configured and synchronized. • Default scan configurations are created for Windows and Linux and enforced by the recommended computer group. NOTE Tanium Scan does not include any Red Hat repositories because authentication for cdn.redhat.com must first be configured. For more information, see (Red Hat endpoints) Configure Tanium Server to use certificate authentication on page 72.

© 2026 Tanium Inc. All Rights Reserved

Setting	Default value
Patch lists	The following patch lists are automatically created: • **[Patch Baseline Deployment] - Windows** • **[Tanium Patch Baseline Reporting] - Windows** • **[Tanium Patch Baseline Reporting] - Linux** • **All Patches** • **[Tanium Patch Recommended Updates] - Windows** For more information, see Default patch lists on page 100.
Patch block lists	• The **[Global Block List] - Windows** block list is created and targets the `Patch Supported Systems` computer group. This block list excludes **Security Only** patches on Windows systems. For more information, see Microsoft update and servicing details on page 19. • A default block list is created for Linux but is not targeted.
Patch deployment templates	Default deployment templates are created for Windows and Linux.
Patch maintenance windows	• A **[Patch Tuesday] - Windows** default maintenance window is created for Patch Tuesday and is not enforced on any computer groups. • Default maintenance windows are created for Windows and Linux to block patch installations and reboots without first enabling another maintenance window. These maintenance windows are not enforced to any computer groups.

Configure advanced settings

You can configure the Tanium platform for optimal delivery of larger payloads, which are typically associated with patching activity.

1. From the Main menu, go to **Administration > Configuration > Settings > Advanced Settings**.
2. To increase the client cache size, click **Add Setting**, provide the following information, and click **Save**.
   Setting Type: `Client`
   Platform Setting Name: `ClientCacheLimitInMB`
   Value Type: `Numeric`
   Value : `2048`



Changes to platform settings can take up to five hours to propagate to clients.

© 2026 Tanium Inc. All Rights Reserved

Install and configure Tanium End-User Notifications for Windows endpoints

With the Tanium End-User Notifications solution, you can create a notification message with your deployment to notify the user that the Windows system is going to restart, and give the user the option to postpone the restart.

For more information, see Tanium End-User Notifications User Guide: End-User Notifications overview.

Disable Windows Update restart prompts

The Windows Update Agent automatically prompts users to restart their machine when an update is installed from any user or source. The following Windows Local/Group Policies should be configured to allow Tanium End-User Notifications to control endpoint restarts.

1. In the Windows Local Group Policy Editor, go to **Computer Configuration > Administrative Templates > Windows Components > Windows Update**.
2. Enable the **No auto-restart for scheduled Automatic Updates installations** parameter.
3. Disable the **Re-prompt for restart with scheduled installations** parameter.

Install and configure Tanium Endpoint Configuration

Manage solution configurations with Tanium Endpoint Configuration

Tanium Endpoint Configuration delivers configuration information and required tools for Tanium Solutions to endpoints. Endpoint Configuration consolidates the configuration actions that traditionally accompany additional Tanium functionality and eliminates the potential for timing errors that occur between when a solution configuration is made and the time that configuration reaches an endpoint. Managing configuration in this way greatly reduces the time to install, configure, and use Tanium functionality, and improves the flexibility to target specific configurations to groups of endpoints.



For information about how to install Endpoint Configuration, see Tanium Endpoint Configuration User Guide: Installing Endpoint Configuration.

Optionally, you can use Endpoint Configuration to require approval of configuration changes. When configuration approvals are enabled, Endpoint Configuration does not deploy a configuration change to endpoints until a user with approval permission approves the change. For information about the roles and permissions that are required to approve configuration changes for Patch, see User role requirements on page 45. For more information about how to enable and use configuration approvals in Endpoint Configuration, see Tanium Endpoint Configuration User Guide: Managing approvals.

© 2026 Tanium Inc. All Rights Reserved

IMPORTANT

For solutions to perform configuration changes or tool deployment through Endpoint Configuration on endpoints with action locks turned on, you must enable the **Manifest Package Ignore Action Lock** and **Deploy Client Configuration and Support Package Ignore Action Lock** settings. To access these settings, from the Endpoint Configuration **Overview** page, click Settings and select **Global**. For more information about action locks, see Tanium Console User Guide: Managing action locks.

For more information about Endpoint Configuration, see Tanium Endpoint Configuration User Guide.

If you enabled configuration approvals, the following configuration changes must be approved in Endpoint Configuration before they deploy to endpoints:

- Creating, updating, or deleting patch lists
- Adding or removing enforcements
- Removing all enforcements
- Updating scan configuration priorities
- Creating deployments
- Stopping deployments
- Adding targets to deployments
- User-initiated actions, such as initializing endpoints, uploading custom field files, enabling Linux

Configure Patch global settings

Configure the Patch action group for Windows and Linux endpoints

Use the Patch action group to define which managed endpoints are the targets for Patch deployments. Edit the computer groups in the Patch action group to specify which endpoints the deployments target.

Importing the Patch module automatically creates an action group to target specific endpoints. If you did not use automatic configuration or you enabled restricted targeting when you imported Patch, the action group targets **No Computers**.

If you used automatic configuration and restricted targeting was disabled when you imported Patch, configuring the Patch action group is optional.

Select the computer groups to include in the Patch action group.

BEST PRACTICE

Clear the selection for **No Computers** and make sure that all operating systems that are supported by Patch are included in the Patch action group.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Actions > Action Groups**.
2. Click **Patch**.
3. Select the computer groups that you want to include in the action group and click **Save**.
   If you select multiple computer groups, choose an operator (AND or OR) to combine the groups.

NEXT STEPS

Initialize Patch on page 80.

Organize computer groups for Windows and Linux endpoints

One way to apply Windows and Linux patches and view deployment results is by computer group. Create relevant computer groups to organize your endpoints. Some options include:

- Endpoint type, such as servers or employee workstations
- Endpoint location, such as by country or time zone
- Endpoint priority, such as business-critical machines
- Endpoint configuration needs, such as VDI machines



Organize computer groups by operating system generation for useful visibility and scan configuration targeting.

Computer group	Filter	Purpose
All Windows[1]	Is Windows equals True	• Visibility • Scan configuration targeting
All Windows Servers[1]	Windows OS Type equals Windows Server	• Visibility • Scan configuration targeting
All Windows Servers - Physical	Windows OS Type contains windows and Is Virtual equals no	Scan configuration targeting
All Windows Servers - Virtual	Windows OS Type contains windows and Is Virtual equals yes	Scan configuration targeting
All Windows Workstations	Windows OS Type equals Windows Workstation	Scan configuration targeting
All Windows Workstations - Physical	Windows OS Type contains windows workstation and Is Virtual equals no	Scan configuration targeting
All Windows Workstations - Virtual	Windows OS Type contains windows workstation and Is Virtual equals yes	Scan configuration targeting
All CentOS 6[1]	Operating System Generation equals CentOS 6	• Visibility • Scan configuration targeting

© 2026 Tanium Inc. All Rights Reserved

Computer group	Filter	Purpose
All CentOS 7[1]	Operating System Generation equals CentOS 7	• Visibility • Scan configuration targeting
All CentOS 8[1]	Operating System Generation equals CentOS 8	• Visibility • Scan configuration targeting
All Red Hat 6[1]	Operating System Generation equals Red Hat Enterprise Linux 6	• Visibility • Scan configuration targeting
All Red Hat 7[1]	Operating System Generation equals Red Hat Enterprise Linux 7	• Visibility • Scan configuration targeting
All Red Hat 8[1]	Operating System Generation equals Red Hat Enterprise Linux 8	• Visibility • Scan configuration targeting
All Red Hat 9[1]	Operating System Generation equals Red Hat Enterprise Linux 9	• Visibility • Scan configuration targeting
All Oracle 6[1]	Operating System Generation equals Oracle Linux Server 6	• Visibility • Scan configuration targeting
All Oracle 7[1]	Operating System Generation equals Oracle Linux Server 7	• Visibility • Scan configuration targeting
All Oracle 8[1]	Operating System Generation equals Oracle Linux Server 8	• Visibility • Scan configuration targeting
All Oracle 9[1]	Operating System Generation equals Oracle Linux Server 9	• Visibility • Scan configuration targeting
All Amazon[1]	Operating System Generation equals Amazon Linux	• Visibility • Scan configuration targeting
All Amazon Linux 1	Operating System Generation equals Amazon Linux 1	• Visibility • Scan configuration targeting
All Amazon Linux 2	Operating System Generation equals Amazon Linux 2	• Visibility • Scan configuration targeting

© 2026 Tanium Inc. All Rights Reserved

Computer group	Filter	Purpose
All SUSE[1]	Operating System contains SUSE	• Visibility • Scan configuration targeting
All SLES 11[1]	Operating System Generation contains SUSE Linux Enterprise Server 11	• Visibility • Scan configuration targeting
All SLES 12[1]	Operating System Generation contains SUSE Linux Enterprise Server 12	• Visibility • Scan configuration targeting
All SLES 15[1]	Operating System Generation contains SUSE Linux Enterprise Server 15	• Visibility • Scan configuration targeting
All Ubuntu	Operating System Generation contains Ubuntu	• Visibility • Scan configuration targeting
All Ubuntu 14.04 - amd64	Operating System Generation matches Ubuntu 14.04 and CPU Architecture matches amd64|x86_64	• Visibility • Scan configuration targeting
All Ubuntu 14.04 - i386	Operating System Generation matches Ubuntu 14.04 and CPU Architecture matches x86|i386	• Visibility • Scan configuration targeting
All Ubuntu 14.04 - arm64	Operating System Generation matches Ubuntu 14.04 and CPU Architecture matches arm64|aarch64	• Visibility • Scan configuration targeting
All Ubuntu 16.04 - amd64	Operating System Generation matches Ubuntu 16.04 and CPU Architecture matches amd64|x86_64	• Visibility • Scan configuration targeting
All Ubuntu 16.04 - i386	Operating System Generation matches Ubuntu 16.04 and CPU Architecture matches x86|i386	• Visibility • Scan configuration targeting
All Ubuntu 16.04 - arm64	Operating System Generation matches Ubuntu 16.04 and CPU Architecture matches arm64|aarch64	• Visibility • Scan configuration targeting
All Ubuntu 18.04 - amd64	Operating System Generation matches Ubuntu 18.04 and CPU Architecture matches amd64|x86_64	• Visibility • Scan configuration targeting
All Ubuntu 18.04 - i386	Operating System Generation matches Ubuntu 18.04 and CPU Architecture matches x86|i386	• Visibility • Scan configuration targeting

© 2026 Tanium Inc. All Rights Reserved

Computer group	Filter	Purpose
All Ubuntu 18.04 - arm64	Operating System Generation matches Ubuntu 18.04 and CPU Architecture matches arm64|aarch64	• Visibility • Scan configuration targeting
All Ubuntu 20.04 - amd64	Operating System Generation matches Ubuntu 20.04 and CPU Architecture matches amd64|x86_64	• Visibility • Scan configuration targeting
All Ubuntu 20.04 - i386	Operating System Generation matches Ubuntu 20.04 and CPU Architecture matches x86|i386	• Visibility • Scan configuration targeting
All Ubuntu 20.04 - arm64	Operating System Generation matches Ubuntu 20.04 and CPU Architecture matches arm64|aarch64	• Visibility • Scan configuration targeting
All Ubuntu 22.04 - amd64	Operating System Generation matches Ubuntu 22.04 and CPU Architecture matches amd64|x86_64	• Visibility • Scan configuration targeting
All Ubuntu 22.04 - i386	Operating System Generation matches Ubuntu 22.04 and CPU Architecture matches x86|i386	• Visibility • Scan configuration targeting
All Ubuntu 22.04 - arm64	Operating System Generation matches Ubuntu 22.04 and CPU Architecture matches arm64|aarch64	• Visibility • Scan configuration targeting
All Ubuntu 24.04 - amd64	Operating System Generation matches Ubuntu 24.04 and CPU Architecture matches amd64|x86_64	• Visibility • Scan configuration targeting
All Ubuntu 24.04 - i386	Operating System Generation matches Ubuntu 24.04 and CPU Architecture matches x86|i386	• Visibility • Scan configuration targeting
All Ubuntu 24.04 - arm64	Operating System Generation matches Ubuntu 24.04 and CPU Architecture matches arm64|aarch64	• Visibility • Scan configuration targeting
All Debian	Operating System Generation contains Debian	• Visibility • Scan configuration targeting
All Debian 8	Operating System Generation contains Debian 8	• Visibility • Scan configuration targeting
All Debian 9	Operating System Generation contains Debian 9	• Visibility • Scan configuration targeting

© 2026 Tanium Inc. All Rights Reserved

Computer group	Filter	Purpose
All Debian 10	Operating System Generation contains Debian 10	• Visibility • Scan configuration targeting
All Debian 11	Operating System Generation contains Debian 11	• Visibility • Scan configuration targeting
All Debian 12	Operating System Generation contains Debian 12	• Visibility • Scan configuration targeting
Tanium Scan Supported Windows	Windows OS Major Version > 6.0 and Tanium Client Version >= 7.2.314.3211	• Visibility • Scan configuration targeting
All Linux[1]	Operating System contains Linux	• Visibility • Scan configuration targeting
Patch Supported Systems[1]	Patch - Supported Scan Types matches ".*(Repo|Tanium|CAB|Online).*"	• Visibility • Patch action group

[1] Patch creates this computer group if you select the **Apply All Tanium recommended configurations** option during installation on Tanium Core Platform 7.4.2 or later.

Set up Patch users

You can use the following set of predefined user roles to set up Patch users.

To review specific permissions for each role, see User role requirements on page 45.



On installation, Patch creates a **Patch** user to automatically manage the Patch service account. Do not edit or delete the **Patch** user.

For more information about assigning user roles, see Tanium Core Platform User Guide: Manage role assignments for a user.

Patch Administrator

Assign the **Patch Administrator** role to users who manage the configuration and deployment of Patch functionality to endpoints.
This role can perform the following tasks:

- Configure all Patch settings
- Manage block lists, deployments, maintenance windows, patch lists, repositories, and scan configurations
- View the Patch statistics logs

© 2026 Tanium Inc. All Rights Reserved

- View all configurations, graphs, and reporting data in Patch

Patch Configuration Author

Assign the **Patch Configuration Author** role to users who manage Patch configurations.
This role can perform the following tasks:

- Manage block lists, maintenance windows, patch lists, and repository snapshots
- View deployments and repositories
- View Patch settings
- View all configurations, graphs, and reporting data in Patch

Patch Deployment Author

Assign the **Patch Deployment Author** role to users who manage Patch deployments.
This role can perform the following tasks:

- Manage deployments
- View block lists, maintenance windows, and patch lists
- View Patch settings
- View all configurations, graphs, and reporting data in Patch

Patch Endpoint Configuration Approver

Assign the **Patch Endpoint Configuration Approver** role to a user who approves or rejects Patch configuration items in Tanium Endpoint Configuration.
This role approves, rejects, or dismisses changes that target endpoints where Patch is installed.

Patch Operator

Assign the **Patch Operator** role to users who manage the configuration and deployment of Patch functionality to endpoints.
This role can perform the following tasks:

- Manage block lists, deployments, maintenance windows, patchlists, repositories, and scan configurations
- View all configurations, graphs, and reporting data in Patch

Patch Read Only User

Assign the **Patch Read Only User** role to users who need visibility into Patch data.
This role can view all configurations, graphs, and reporting data in Patch.

Patch Super User

Assign the **Patch Super User** role to users who manage the configuration and deployment of Patch functionality to endpoints.
This role can perform the following tasks:

© 2026 Tanium Inc. All Rights Reserved

- Manage block lists, deployments, maintenance windows, patchlists, repositories, and scan configurations
- View all configurations, graphs, and reporting data in Patch



Do not assign the **Patch Service Account** and **Patch Service Account - All Content Sets** roles to users. These roles are for internal purposes only.

Enable and configure Windows features

Before you can use the following Patch features for Windows endpoints, you must enable or configure them:

- Enable and configure Tanium Scan for Windows on page 65
- Configure WSUS server allowed URLs on page 66
- Enable UUP Proxy on page 66
- Enable manual synchronization on page 67
- Enable direct patch downloads from Microsoft on page 67

Enable and configure Tanium Scan for Windows

If you want to use Tanium Scan on page 90, configure the Tanium Scan settings.

1. From the Main menu, go to **Modules > Patch > Scan Management**.
2. Click **Tanium Scan for Windows** and then click **Edit**.
3. Select **Enable Tanium Scan for Windows** (if not already selected) and select a scan source.
4. In the **Tanium Scan Source** section, select where to retrieve information about available software patches.
    - **Microsoft Update Direct**: Synchronize update metadata and detection rules directly from Microsoft. Do not select this option if you have air-gapped environments.
    - **Local WSUS Server**: Synchronize update metadata and detection rules from a local WSUS server.
        a. Enter the **URL** and the **Content Download Port**. The content download port is the port from which the Tanium Server can download patch installation files. The Tanium Server then delivers the files as part of a Patch deployment.
        The default port may be 8530 or 80, depending on the WSUS server version. You can configure the WSUS server to use a custom port.
        b. Choose a PEM file containing the certificate authority for the WSUS server. The certificate should be the Base64-encoded ASCII, certificate chain format.
5. Click **Synchronize Now** to perform the required initial synchronization.
6. If you want to synchronize after Microsoft releases many significant patches, select **Enable Schedule Synchronization**.

© 2026 Tanium Inc. All Rights Reserved

7. Use the arrows to select products to include in scans.

   BEST PRACTICE

   Synchronize all products, regardless of which products are present in the environment. Selectively choosing products can cause gaps in critical or important patches.

8. Use the arrows to select update classifications to include in scans.

   BEST PRACTICE

   Select **Critical Updates**, **Security Updates**, **Service Packs**, and **Update Rollups**.

9. Click **Submit**.

   BEST PRACTICE

   Click **Synchronize Now** after you make any changes.

10. If you selected **Local WSUS Server** in the Tanium Scan Source option, then complete the steps in Configure WSUS server allowed URLs on page 66.

11. If you have endpoints running Windows 11 version 22H2 or later, see Enable UUP Proxy on page 66.

Configure WSUS server allowed URLs

If you enabled the **Local WSUS Server** option in Tanium Scan for Windows, add the server URL in the Patch settings to allow the Tanium Server to connect to the WSUS server.

1. Add the WSUS Server URL.

   a. From the Main menu, go to **Modules > Patch> Overview** and click Settings **> Configuration Settings** if needed.

   b. In the **WSUS Server Configuration** section, enter the URL and click **Submit**. A regular expression for the URL is generated and added.

   c. Click **View Allowed URLs**, or go to **Administration > Permissions > Allowed URLs** to view the entry that was added.

2. On the WSUS server, change the following settings:

   a. Set the intranet URL for detecting updates and the statistics server to `http://<WSUS server URL>:<port>`.

   b. Disable the **Configure Automatic Updates** setting.

Enable UUP Proxy

Starting with Windows 11 version 22H2 endpoints, Microsoft uses the Unified Update Platform (UUP) to deliver cumulative updates. If you configured Tanium Scan for Windows and want to use Tanium architecture to patch these endpoints, enable the UUP proxy. For some environments, the UUP proxy might be enabled by default. When enabled, patches are synchronized to the Tanium Server and then the Windows endpoints are patched using Tanium architecture.

© 2026 Tanium Inc. All Rights Reserved

NOTE

UUP might use up to 200 GB of the minimum required 500 GB disk space on the Tanium Server. The actual amount of disk space used depends on the size of the Windows update files.

NOTE

When UUP Proxy is not enabled, direct download is automatically enabled as the default patch delivery method for these endpoints. For more information see Enable direct patch downloads from Microsoft on page 67.

Complete the following steps to enable the UUP proxy:

1. From the Main menu, go to **Modules > Patch> Overview** and click Settings **> Configuration Settings** if needed.
2. In the **UUP Settings** section, select **Enable UUP Proxy**.
3. Click **Save**.
4. If you are using a local WSUS server to deliver patch data, see Enable manual synchronization on page 67.

Enable manual synchronization

Manual synchronization is only applicable when using Tanium Scan for Windows on Windows 11 version 22H2 or later endpoints.

NOTE

In airgap environments, manual synchronization is enabled by default.

If you are using a local WSUS server to deliver patch data to endpoints managed using Tanium Client, then enable **Manual Synchronization**. When **Manual Synchronization** is enabled, you need to manually run a synchronization job to synchronize the patches. If you do not enable **Manual Synchronization**, you might encounter synchronization failures when Tanium tries to automatically synchronize patches that are not yet approved on the WSUS server.

Complete the following steps to enable manual synchronization:

1. From the Main menu, go to **Modules > Patch> Overview** and click Settings **> Configuration Settings** if needed.
2. In the **UUP Settings** section, select **Enable Manual Synchronization**.
3. Click **Save**.

To manually start a synchronization after you prepare or approve patches for Windows version 11 22H2 or later, see Manually synchronize patches on page 108.

Enable direct patch downloads from Microsoft

For Windows scan configurations, you can enable *isolated endpoints* to download patch files directly from Microsoft instead of the Tanium Server to free network resources. An isolated endpoint is a Tanium Client that has no peer Tanium Clients. To download patches directly from Microsoft, an isolated endpoint must be connected to a user-configured list of Tanium Zone Servers or IP address ranges for split-tunnel VPN clients.

© 2026 Tanium Inc. All Rights Reserved

This option reduces the impact on network resources. If the direct download fails, the endpoint downloads patches from the Tanium Server.

CAUTIONS AND CONSIDERATIONS

Endpoints must be in a list of virtual private network (VPN) subnets or allowed Zone Servers that you configure. Configure VPN ranges only where clients have a direct path to the Microsoft URLs that are listed in Third-party internet URLs on page 43. The following configurations are recommended:

- Define the IP address ranges that are used by endpoints that connect to Tanium over a split-tunnel VPN. Use for split-tunnel VPN ranges with a separate route to download patches from the Internet. Isolated endpoints within the defined ranges attempt to download patches directly from Microsoft.
- Define the public IP addresses or Internet-resolvable fully qualified domain names of Internet-facing Zone Servers. Isolated Tanium Clients that are connected to these Zone Servers attempt to download patches directly from Microsoft.

Do not specify the following VPNs or Zone Servers:

- Split-tunnel VPNs where endpoints still send traffic bound for Microsoft URLs through the internal corporate network
- Full-tunnel VPNs
- Zone Servers that are used in an internal security zone

Clients that use WSUS scan configurations leverage the location that is defined by WSUS. Unless the WSUS server is configured to download patches from Microsoft instead of storing them locally, do not enable direct downloads for a WSUS Scan configuration. For more information about how to specify where updates are stored, see Microsoft article Update storage options.

1. From the Main menu, go to **Modules > Patch > Overview** and click Settings **> Configuration Settings** if needed.
2. In the **Patch Direct Downloads** section, specify network information:
   a. Select **VPN Networks**, **Zone Servers**, or both.
   b. Add one or more networks or servers, or, if previously created, choose from the list.
3. Click **Save**.

IMPORTANT

To enable remote endpoints to download patches directly from Microsoft, you must also enable direct downloads in each scan configuration. For more information, see Create a scan configuration on page 94.

TRACKING DIRECT DOWNLOAD STATUS

Review current and past patch downloads directly from Microsoft over the Internet.

1. In Interact, ask the `Get Patch - Direct Downloads Statuses from all machines` question.
2. Choose the time period in hours; for example, downloads in the last three hours.

© 2026 Tanium Inc. All Rights Reserved

3. Choose whether to include in-progress downloads in the results.
4. Choose whether to include failed downloads in the results.
5. Click **Ask Question**.

The results grid shows a row for each download attempt and its status.

Enable and configure Linux features

Before you can use the following Patch features for Linux endpoints, you must enable and configure them:

- Migration of OS-based Linux configurations to Enhanced Linux configurations on page 69
- Enable Patch for Enhanced Linux configurations on page 70
- Add and target Linux repositories on page 70
- (Red Hat endpoints) Configure Tanium Server to use certificate authentication on page 72
- Manage Linux repository snapshots on page 78

Migration of OS-based Linux configurations to Enhanced Linux configurations

After you enable support for Enhanced Linux distributions, Patch migrates any existing OS-based Linux configurations (scan configurations, patch lists, block lists, maintenance windows, and deployment templates) for Red Hat, CentOS, Ubuntu, Oracle, and Amazon to use Enhanced Linux distributions.

Targeting for migrated configurations continue to be filtered to the existing OS-based Linux configurations, so that the same endpoints remain targeted after migration. Migration does not add targeting for unenforced objects, nor does it create a configuration that supports multiple operating systems. You must create a configuration that supports multiple operating systems after migration.

Patch does not select a default deployment template for the new Linux platform. If you want to define a default deployment template, you define it after the automated portion of the migration completes.

LINUX ENDPOINT BEHAVIOR CHANGES

Linux endpoint behavior depends on your current configuration:

- If this is a new Patch module installation, Patch enables Enhanced Linux Support by default.
- If this is an existing Patch module installation, where Patch for Linux endpoints has never been enabled, Linux configurations remain disabled until you enable Enhanced Linux Support.
- If this is an existing Patch module installation, where Patch for Linux endpoints has been enabled, your OS-based Linux configurations remain the same until you enable Enhanced Linux Support.

After you migrate to Enhanced Linux Support, Patch no longer separates operating system selections for Linux. Instead, it creates a single category for all Linux operating systems. Scan configurations can have repositories for multiple Linux operating systems. You can add targets to repositories to ensure they are only used with the proper OS/version targets included in the scan configuration targets. If an endpoint does not meet the criteria for any repositories in a scan configuration, Patch continues to the next targeted scan configuration.

© 2026 Tanium Inc. All Rights Reserved

Enable Patch for Enhanced Linux configurations

Before you begin, ensure that you meet the prerequisites listed in Core platform dependencies on page 34.

> **NOTE** If this is a new Patch module installation, no action is required.

If this is an upgraded Patch module installation, complete the following steps:

1. From the Main menu, go to **Modules > Patch > Overview** page and click Settings.
2. In the **Operating Systems** tab, select **Enhanced Linux Support** and click **Save**.

   > **IMPORTANT** After you enable this option, you cannot disable it.

3. Review the **Migration of Linux Configurations** message and click **Acknowledge and Begin Migration**.
4. (Optional) Click **Set Default Template** to set a default deployment template for Enhanced Linux Support.

Add and target Linux repositories

To patch Linux endpoints, you must first add repositories that apply to those endpoints, and then use the repositories to target computer groups that contain the endpoints. SUSE Linux Enterprise Server (SLES) repositories use URLs that are unique for each customer, so the process for adding those repositories differs from other versions of Linux.

> **IMPORTANT** Before you begin patching SLES endpoints, make sure that at least one endpoint for each OS version that you want to support in Patch is registered with SUSE.

1. From the Main menu, go to **Modules > Patch > Scan Management** and then click **Repositories**.
2. Click **Add Repository**.

   > **TIP** You can also click Edit to edit existing repositories.

3. Add a name, and then select whether the repository contains RPM or DEB packages.
4. For RPM repositories, specify the following options as needed:
   a. Add a URL for the repository.

      > **TIP** If you are adding a SLES repository, use the following steps to more easily identify the names and URLs for the repositories that your endpoints use.

© 2026 Tanium Inc. All Rights Reserved

TIP

i. In a separate browser tab, go to **Modules > Interact**.

ii. Ask the following question:

```
Get Patch - Repositories from all machines with Operating System Generation contains SUSE
```

For more information, see Tanium Interact User Guide: Asking questions.

iii. For the repository that you want to add, hover over the **Name** cell, click Options, and then click Copy.

iv. In the original browser tab, in the **Add Repository** dialog, paste the cell contents into the **Name** field, and then select **RPM** from the **Type** dropdown list.

v. In the browser tab with the question results, hover over the **Base URL** cell, click Options, and then click Copy.

vi. In the original browser tab, in the **Add Repository** dialog, paste the cell contents into the **URL** field.

b. (Optional) Enable **GPG Check** and **Repo GPG Check** to confirm authenticity by verifying GPG signatures.

CAUTION

Red Hat operating systems do not support **Repo GPG Check**. If you specify that option in a Red Hat repository configuration, Tanium scans will not run.

5. For DEB repositories, specify the following options as needed:

   a. Add a URL for the repository.

   b. Specify the distribution and components for the release. You can add up to five components for the repository.

   c. (Optional) Enable **GPG Check** to confirm authenticity by verifying GPG signatures.

   d. In the **Release file signing** section, select **InRelease** if the release file is signed inline, or select **Release.gpg** if the release file has an accompanying GPG file.

   e. In the **GPG Key** section, select an option to confirm package authenticity and then enter additional information as needed.

6. Click **Submit**.

7. Expand the repository that you just created, and then click **Select Computer Groups**.

8. Select the computer groups that will use the repository, and then click **Save**.

9. (Optional) Create snapshots of repositories. For more information, see Manage Linux repository snapshots on page 78.

© 2026 Tanium Inc. All Rights Reserved

(Red Hat endpoints) Configure Tanium Server to use certificate authentication

To use Tanium Scan for Linux on Red Hat Linux endpoints, you must configure the Tanium Server (version 7.5.3.1249 and later) to use certificate authentication for downloads from the Red Hat Content Delivery Network (CDN), add the repositories to the Tanium Console, and edit the scan management technique to include the repositories.

1. Review the information and complete the steps in Knowledge Article: Create a Red Hat certificate for Tanium downloads (login required). The steps include confirming Red Hat Customer Portal configuration settings, obtaining certificates and a private key from an endpoint directly registered to the Red Hat CDN, and configuring the certificates in Tanium Console.
2. In the Tanium Console, add the repositories. For more information, see Add and target Linux repositories on page 70.
3. Edit the **[Tanium Scan] - Linux** scan management technique to include the Red Hat repositories. For more information, see Edit a scan configuration on page 99.

(Red Hat endpoints) Configure TDownloader to use certificate authentication (Tanium Server version 7.5.2.3552 and earlier)

To use Tanium Scan with Red Hat's patch content on Red Hat Linux endpoints, you must configure Tanium Downloader (TDownloader) to use certificate authentication for downloads from Red Hat's Content Delivery Network (CDN) or an internal Red Hat Satellite server. Obtain a valid client certificate and private key from the Red Hat Customer Portal or from the Satellite server. After you have acquired the client authentication certificate, complete the appropriate steps to configure the Tanium Server.

CONFIGURE TDOWNLOADER ON TANIUM SERVER (APPLIANCE)

If you are using an internal repository secured by a self-signed or an internal CA-signed certificate, Contact Tanium Support on page 162 to configure the Tanium Servers to trust this certificate.



In an active-active configuration, you must perform the following steps on both Tanium Servers.

1. Upload the SSL client private key and client certificate to your Tanium Appliance. Use SFTP with the `tancopy` account and copy the files to the `/incoming` folder.
2. Using the TanOS menu, verify that the Tanium Server can reach cdn.redhat.com or the Red Hat Satellite server by name:
   a. Enter `3` to go to the Tanium Support menu.
   b. Enter `4` to go to the Run Network Diagnostics menu.
   c. Enter `1` to select the Ping Remote System option.
3. Add the CA root certificate for the Red Hat CDN:
   a. Enter `2` to go to the Tanium Operations menu.
   b. Enter `2` to go to the Tanium Configuration Settings menu.

© 2026 Tanium Inc. All Rights Reserved

c. Enter `13` to go to the Control RedHat CA Cert menu.

d. Enter `1` to select the redhat-uep.pem option.

e. Enter `2` to install the redhat-uep.pem certificate.

4. Add the Red Hat Entitlement client certificate and key:

   a. Enter `2` to go to the Tanium Operations menu.

   b. Enter `2` to go to the Tanium Configuration Settings menu.

   c. Enter `4` to select the Add Tanium Server TDL Auth Cert option.

   d. Enter the URL (https://cdn.redhat.com or the Red Hat Satellite server), client certificate file name, and the SSL client private key file name at each prompt.

   e. At the #Line Content display, enter `R` to return to the previous menu.

For more information about authentication certificates, see Tanium Appliance User Guide: Manage additional authentication certificates.

CONFIGURE TDOWNLOADER ON TANIUM SERVER (WINDOWS)

1. Copy the SSL client private key, client certificate, and satellite server certificate to your Tanium Server.

2. Ensure that the Tanium Server can reach cdn.redhat.com or the Red Hat Satellite server by name.
   Example:
   `ping cdn.redhat.com`

3. On each Tanium Server, configure TDownloader to use certificate authentication for downloads to the Red Hat Satellite server.
   Example:
   `cmd-prompt>TDownloader.exe add-auth-cert --url https://cdn.redhat.com --cert C:\client-certificate.pem --key C:\client-key.pem`
   where:

   - `https://cdn.redhat.com` is the URL prefix for the satellite server download URLs
   - `C:\client-certficate.pem` is the client certificate
   - `C:\client-key.pem` is the client certificate private key

4. Check the TDownloader config to see that your certificate has been configured.

```
cmd-prompt>TDownloader.exe config list
Keys:
- Auth:
    - Auth.0:
      - Auth.0.Certificate: -----BEGIN CERTIFICATE-----
MIIFPTCCBCWgAwIBAgIIbY/mIdQbgMowDQYJKoZIhvcNAQEFBQAwgYwxCzAJBgNV
BAYTAlVTMRcwFQYDVQQIDA5Ob3J0aCBDYXJvbGluYTEQMA4GA1UEBwwHUmFsZWln
```

© 2026 Tanium Inc. All Rights Reserved

```
aDEQMA4GA1UECgwHS2F0ZWxsbzEUMBIGA1UECwwLU29tZU9yZ1VuaXQxKjAoBgNV
BAMMIXJoZWxwYXRjaHNhdGVsbGl0ZTAxLnByb2RxYS5sb2NhbDAeFw0xODA0MjAw
NDAwMDBaFw0xOTA0MjAwMzU5NTlaMEYxGTAXBgNVBAoMEHRhbml1bV9wYXRjaF9k
ZXYxKTAnBgNVBAMTIDBjYjk4NjcyZjBhNTQ0MDJhNzIzYmNjOGI5ODFjYTg3MIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtXPySC20fPzMreenmX+4mUhS
s/cdArQZOeeKliCdXI7Q/ZW0ZrhsgmMZTL+BNbZKUp72e0L3GF3yj0wx/8LWRLVC
S9AaZdbXmJRK7B5mwpQaLtfuE93bJIkmBbzKA49jiwFdDE0J6v+wj0NgBZ3hr0NH
V2O1hAwar2xkzz9fCTwyAR6d2I9Dpcfua8nH0ybO5kR8v1Epp70vw9/uMmGM3PCe
YFX81ll3wxStbHj/DznUzQ/vFE0SZxLXh9LyWy9Nq+obLaFeDxJ0DT7iXotwVqWs
Qow/upQ60vuYpAT57JM5tkrP+rKcct+TVVJNS/QmJC3yOwZWf8rIISRH4cb+GQID
AQABo4IB5jCCAeIwEQYJYIZIAYb4QgEBBAQDAgWgMAsGA1UdDwQEAwIEsDCBwQYD
VR0jBIG5MIG2gBRNdbtnITo9NxbcUdarkRIJv464dqGBkqSBjzCBjDELMAkGA1UE
BhMCVVMxFzAVBgNVBAgMDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHDAdSYWxlaWdo
MRAwDgYDVQQKDAdLYXRlbGxvMRQwEgYDVQQLDAtTb211lT3JnVW5pdDEqMCgGA1UE
AwwhcmhlbHBhdGNoc2F0ZWxsaXRlMDEucHJvZHFhLmxvY2FsggkAx2ndp2OhmcYw
HQYDVR0OBBYEFHX7IDsUYNAZdI5dBxckm5a8y60aMBMGA1UdJQQMMAoGCCsGAQUF
BwMCMBIGCSsGAQQBkggJBgQFDAMzLjMwFAYJKwYBBAGSCAkIBAcMBUJhc2ljMIGd
BgkrBgEEAZIICQcEgY8EgYx42i2MMQrDMBAE9zFukyYgfyJdHmDO8oIEis7cXYz9
e8ck1UwxjNM2GsbXj1bYsFQP6BpVuzRk7cEeSP8kYYRL3EK1OZ51NrED6f5ASK+f
97RK5DIt3KAO7mHiGIyN4rwGw/wVsVxwAp4aKvUSzZXb1epTaC96MJ25BX5rmucc
vyYlbSe9CpomkcWhADANBgkqhkiG9w0BAQUFAAOCAQEAubxqAqH/IQqIODQwaX9x
NrIuJp3qWIUFjxZ1Vby4lEg2xmwfBtvNKminJBWNwOMZjq40xrEz0C2sxqkr/npv
cbI4MMdQX1rdxMwsntgUZK8ApRR/pPwyxqAoa8IjahVBHNdFoA4+BBjcLcvzA1PB
PReiXo0GS2gQQAb8U7d/jBTG1gm3ZpJFBxv7NBM9tEey3DwzP5LWPnZZmstRrlfx
7sb5J/2zLvWuMG+dMJ5jkgUKTuNdccdBP9PEVrAKiDuoLCl4UqnP0YzMJd+e9Ktx
FC1QCICFUQLhZ/QVAhh8hIw0jSxIcGN+KVJF52BGdzUxvoidfqtMsjc/8NSTRk+T
/g==
-----END CERTIFICATE-----
- Auth.0.PrivateKey: (protected)
- Auth.0.URL: https://rhelpatchsatellite01.prodqa.local
- LogVerbosityLevel: 41
- ProxyPassword:
- ProxyPort:
- ProxyServer:
- ProxyType: NONE
- ProxyUserid:
- TrustedCertPath: C:\Program Files\Tanium\Tanium Server\Certs\installedcacert.crt
- TrustedHostList: localhost,tanium.local,win-2012-r2
```

5. To configure TDownloader to work with the Red Hat CDN, use a text editor to append the PEM-encoded certificate for cdn.redhat.com to the end of the certificate file as referenced by the *TrustedCertPath* value from the previous step (Example: `C:\Program Files\Tanium\Tanium Server\Certs\installedcacert.crt`).

© 2026 Tanium Inc. All Rights Reserved

```
-----BEGIN CERTIFICATE-----
MIIG/TCCBOWgAwIBAgIBNzANBgkqhkiG9w0BAQUFADCBsTELMAkGA1UEBhMCVVMx
FzAVBgNVBAgMDk5vcnRoIENhcm9saW5hMRYwFAYDVQQKDA1SZWQgSGF0LCBJbmMu
MRgwFgYDVQQLDA9SZWQgSGF0IE5ldHdvcmsxMTAvBgNVBAMMKFJlZCBIYXQgRW50
aXRsZW1lbnQgT3BlcmF0aW9ucyBBdXRob3JpdHkxJDAiBgkqhkiG9w0BCQEWFWNh
LXN1cHBvcnRAcmVkaGF0LmNvbTAeFw0xMDEwMDQxMzI3NDhaFw0zMDA5MjkxMzI3
NDhaMIGuMQswCQYDVQQGEwJVUzEXMBUGA1UECAwOTm9ydGggQ2Fyb2xpbmExFjAU
BgNVBAoMDVJlZCBIYXQsIEluYy4xGDAWBgNVBAsMD1JlZCBIYXQgTmV0d29yazEu
MCwGA1UEAwwlUmVkIEhhdCBFbnRpdGxlbWVudCBQcm9kdWN0IEF1dGhvcml0eTEk
MCIGCSqGSIb3DQEJARYVY2Etc3VwcG9ydEByZWRoYXQuY29tMIICIjANBgkqhkiG
9w0BAQEFAAOCAg8AMIICCgKCAgEA2QurMeAVnCHVsuZNQzciWMdpd4LAVk2eGugN
0cxmBpzoVI8lIsJOmJkpOAuFOQMX9CBr8RuQyg4r1/OH/rfhm6FgGIw8TGKZoWC/
1B9teZqTiM85k6/1GRNxdk6dUK77HVO0PMIKtNBHRxIsXcRzJ1q+u5WPBes9pEVG
nbidTNUkknrSIdynTJcqAI/I0VAsqLqX87XJSzXKvRilE+p/fLHmVTAffl1Cn/Dy
KULxna7ooyrKKnfqeQ5dK8aMr1ASQ1wphWohLjegly9V0amEi+HHWnOL8toxJy8v
WUTUzzAvZ4ZTtTV26xGetZZWEaNyv7YCv2AexjcBQ2x+ejrFJrVNo9jizHS06HK8
UgHVDKhmVcAe2/5yrJCjKDLwg1FJfjKwhzhLYdNVCejpy8CHQndwO0EX1hHv/AfP
RTAmr5qPhHFD+uuIrYrSLUpgMLmWa9dinJcGeKlA1KJvG5emGMM3k64Xr7dJToXo
5loGyZ6lvKPIKLmfeXMRW/4+BqyzwbO1i4aIHAZcSPDFGKWwuvF0iVUYUUVxw0nv
qPZA4roq5+j/YSz0q5XGVgiIt34htlvunLp/ICGYJBR6zEHcB9aZGJdDcJvoYZjw
7Gphw6lFF6Ta4imoyhGECWKjd1ips3opcN+DlU0yCUrcIXVIXAnkTwu5ocOgAkxr
f/6FjqcCAwEAAaOCAR8wggEbMB0GA1UdDgQWBBSW/bscQED/QIStsh8LJsHDam/W
fDCB5QYDVR0jBIHdMIHagBTESXhWRZ0eLGFgw2ZLWAU3LwMie6GBtqSBszCBsDEL
MAkGA1UEBhMCVVMxFzAVBgNVBAgMDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHDAdS
YWxlaWdoMRYwFAYDVQQKDA1SZWQgSGF0LCBJbmMuMRgwFgYDVQQLDA9SZWQgSGF0
IE5ldHdvcmsxHjAcBgNVBAMMFUVudGl0bGVtZW50IE1hc3RlciBDQTEkMCIGCSqG
SIb3DQEJARYVY2Etc3VwcG9ydEByZWRoYXQuY29tggkAkYrPyoUAAAAwEgYDVR0T
AQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQUFAAOCAgEArWBznYWKpY4LqAzhOSop
t30D2/UlCSr50l33uUCNYD4D4nTr/pyX3AR6P3JcOCz0t22pVCg8D3DZc5VlzY7y
P5RD3KbLxFNJTloclMG0n6aIN7baA4b8zwkduMQvKZnA/YNR5xE7V7J2WJHCEBBB
Z+ZFwGpGsoZpPZP4hHLVke3xHm6A5F5SzP1Ug0T9W80VLK4jtgyGs8l1R7rXiOIt
Nik8317KGq7DU8TI2Rw/9Gc8FKNfUYcVD7uC/MMQXJTRvkADmNLtZM63nhzpg1Hr
hA6U5YcDCBKsPA43/wsPOONYtrAlToD5hJhU+1Rhmwcw3qvWBO3NkdilqGFOTc2K
50PQrqoRTCZFS41nv2WqZFfbvSq4dZRJl8xpB4LAHSspsMrbr9WZHX5fbggf6ixw
S9KDqQbM7asP0FEKBFXJV1rE8P/oSK6yVWQyigTsNcdGR4AUzDsTO9udcwoM2Ed4
XdakVkF+dXm9ZBwv5UBf5ITSyMXL3qlusIOblJVGUQizumoq0LiSnjwbkxh2XHhd
XD/B/qax7FnaNg+TfujR/kk3kF1OpqWx/wC/qPR+zho1+35Al31gZOfNIn/sReoM
tcci9LFHGvijIy4VUDQK8HmGjIxJPrIIe1nB5BkiGyjwn00D5q+BwYVst1C68Rwx
iRZpyzOZmeineJvhrJZ4Tvs=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
```

© 2026 Tanium Inc. All Rights Reserved

```
MIIHZTCCBU2gAwIBAgIJAJGKz8qFAAAAMA0GCSqGSIb3DQEBBQUAMIGwMQswCQYD
VQQGEwJVUzEXMBUGA1UECAwOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBAcMB1JhbGVp
Z2gxFjAUBgNVBAoMDVJlZCBIYXQsIEluYy4xGDAWBgNVBAsMD1JlZCBIYXQgTmV0
d29yazEeMBwGA1UEAwwVRW50aXRsZW1lbnQgTWFzdGVyIENBMSQwIgYJKoZIhvcN
AQkBFhVjYS1zdXBwb3J0QHJlZGhhdC5jb20wHhcNMTAwMzE4MTEyNDU0WhcNMzAw
MzEzMTEyNDU0WjCBsTELMAkGA1UEBhMCVVMxFzAVBgNVBAgMDk5vcnRoIENhcm9s
aW5hMRYwFAYDVQQKDA1SZWQgSGF0LCBJbmMuMRgwFgYDVQQLDA9SZWQgSGF0IE5l
dHdvcmsxMTAvBgNVBAMMKFJlZCBIYXQgRW50aXRsZW1lbnQgT3BlcmF0aW9ucyBB
dXRob3JpdHkxJDAiBgkqhkiG9w0BCQEWFWNhLXN1cHBvcnRAcmVkaGF0LmNvbTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBALsmiohDnNvIpBMZVJR5pbP6
GrE5B4doUmvTeR4XJ5C66uvFTwuGTVigNXAL+0UWf9r2AwxKEPCy65h7fLbyK4W7
/xEZPVsamQYDHpyBwlkPkJ3WhHneqQWC8bKkv8Iqu08V+86biCDDAh6uP0SiAz7a
NGaLEnOe5L9WNfsYyNwrG+2AfiLy/lLUtmmg5dc6Ln7R+uv0PZJ5J2iUbiT6lMz3
v73zAxuEjiDNurZzxzHSSEYzw0W1eO6zM4F26gcOuH2BHemPMjHi+c1OnheaafDE
HQJTNgECz5Xe7WGdZwOyn9a8GtMvm0PAhGVyp7RAWxxfoU1B794cBb66IKKjliJQ
5DKoqyxD9qJbMF8U4Kd1ZIVB0Iy2WEaaqCFMIi3xtlWVUNku5x21ewMmJvwjnWZA
tUeKQUFwIXqSjuOoZDu80H6NQb+4dnRSjWlx/m7HPk75m0zErshpB2HSKUnrs4wR
i7GsWDDcqBus7eLMwUZPvDNVcLQu/2Y4DUHNbJbn7+DwEqi5D0heC+dyY8iS45gp
I/yhVvq/GfKL+dqjaNaE4CorJJA5qJ9f383Ol/aub+aJeBahCBNuVa2daA9Bo3BA
dnL7KkILPFyCcEhQITnu70Qn9sQlwYcRoYF2LWAm9DtLrBT0Y0w7wQHh8vNhwEQ7
k5G87WpwzcC8y6ePR0vFAgMBAAGjggF9MIIBeTAdBgNVHQ4EFgQUxEl4VkWdHixh
YMNmS1gFNy8DInswgeUGA1UdIwSB3TCB2oAUiEumRcRG7I/Wz6b2Gs8mPJDMfxeh
gbakgbMwgbAxCzAJBgNVBAYTAlVTMRcwFQYDVQQIDA5Ob3J0aCBDYXJvbGluYTEQ
MA4GA1UEBwwHUmFsZWlnaDEWMBQGA1UECgwNUmVkIEhhdCwgSW5jLjEYMBYGA1UE
CwwPUmVkIEhhdCBOZXR3b3JrMR4wHAYDVQQDDBVFbnRpdGxlbWVudCBNYXN0ZXIg
Q0ExJDAiBgkqhkiG9w0BCQEWFWNhLXN1cHBvcnRAcmVkaGF0LmNvbYIJAOb+Qigl
yeZeMAwGA1UdEwQFMAMBAf8wCwYDVR0PBAQDAgEGMBEGCWCGSAGG+EIBAQQEAwIB
BjAgBgNVHREEGTAXgRVjYS1zdXBwb3J0QHJlZGhhdC5jb20wIAYDVR0SBBkwF4EV
Y2Etc3VwcG9ydEByZWRoYXQuY29tMA0GCSqGSIb3DQEBBQUAA4ICAQBbTSz+UIXP
AVIT0ZVL1flCHR113aj2j3UBZkaoDkSxtEfa1nqysmN0llpqh4NVBL3anEFYxokL
hQ2PB8mmuD5EuWaNxnXTc4Sr5dsOcjkFiU197lybaJK7w4OzQ2Qg/X/t4+R78cfM
ZK/qHpjuyT3NyHHvCug/WzkvU09pRr2aVHI+fn68u18TRzPJNKvegR4YeA3vsyQW
BgEc8sU7KrAvikFJ3mCTpAk+6SRgbGFLyZE637Qrzy2DDBw0V020dkTkC6YnEsZg
HwZWVmLtCgLlnimx6SRft+6zrXVHWZxod1GT/af7vizpmhrXt/Nu5Se7dpOhPayo
NwYCFNmfZeL4W/foSKNfaizZcc+tiNABRtT+tplfniv/yjr7sBAsFPhJqQB8CfsQ
8BVvKkHtixygyo+EO+NEotZGw3cn+/7soo9B1bWXk3PFSwEr+KwINACFGv2zcGLI
oeP4iK6DHZImWEV4tgMrQyXatEyPh2axPWU3SjY/fr1Ub5gEt+WpCtyYIN4ObBaN
eL3NPfTj79/VFZ22PhUInmGY/VK/ymvl/dkWyWi8zD8Aq55ofZ33FvQ46dcLp1pV
KWApIVqO27uhL6YxXDFi6n7RXACEIVz6JqDh5fGmOH1F+vfumZKzW78LlVD2QY15
rmCh0i9+AUCiUsNyYdJbSZDPiFPBwlwUoQ==
-----END CERTIFICATE-----
```

© 2026 Tanium Inc. All Rights Reserved

```
-----BEGIN CERTIFICATE-----
MIIHZDCCBUygAwIBAgIJAOb+QiglyeZeMA0GCSqGSIb3DQEBBQUAMIGwMQswCQYD
VQQGEwJVUzEXMBUGA1UECAwOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBAcMB1JhbGVp
Z2gxFjAUBgNVBAoMDVJlZCBIYXQsIEluYy4xGDAWBgNVBAsMD1JlZCBIYXQgTmV0
d29yazEeMBwGA1UEAwwVRW50aXRsZW1lbnQgTWFzdGVyIENBMSQwIgYJKoZIhvcN
AQkBFhVjYS1zdXBwb3J0QHJlZGhhdC5jb20wHhcNMTAwMzE3MTkwMDQ0WhcNMzAw
MzEyMTkwMDQ0WjCBsDELMAkGA1UEBhMCVVMxFzAVBgNVBAgMDk5vcnRoIENhcm9s
aW5hMRAwDgYDVQQHDAdSYWxlaWdoMRYwFAYDVQQKDA1SZWQgSGF0LCBJbmMuMRgw
FgYDVQQLDA9SZWQgSGF0IE5ldHdvcmsxHjAcBgNVBAMMFUVudGl0bGVtZW50IE1h
c3RlciBDQTEkMCIGCSqGSIb3DQEJARYVY2Etc3VwcG9ydEByZWRoYXQuY29tMIIC
IjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA2Z+mW7OYcBcGxWS+RSKG2GJ2
csMXiGGfEp36vKVsIvypmNS60SkicKENMYREalbdSjrgfXxPJygZWsVWJ5lHPfBV
o3WkFrFHTIXd/R6LxnaHD1m8Cx3GwEeuSlE/ASjc1ePtMnsHH7xqZ9wdl85b1C8O
scgO7fwuM192kvv/veI/BogIqUQugtG6szXpV8dp4ml029LXFoNIy2lfFoa2wKYw
MiUHwtYgAz7TDY63e8qGhd5PoqTv9XKQogo2ze9sF9y/npZjliNy5qf6bFE+24oW
E8pGsp3zqz8h5mvw4v+tfIx5uj7dwjDteFrrWD1tcT7UmNrBDWXjKMG81zchq3h4
etgF0iwMHEuYuixiJWNzKrLNVQbDmcLGNOvyJfq60tM8AUAd72OUQzivBegnWMit
CLcT5viCT1AIkYXt7l5zc/duQWLeAAR2FmpZFylSukknzzeiZpPclRziYTboDYHq
revM97eER1xsfoSYp4mJkBHfdlqMnf3CWPcNgru8NbEPeUGMI6+C0YvknPlqDDtU
ojfl4qNdf6nWL+YNXpR1YGKgWGWgTU6uaG8Sc6qGfAoLHh6oGwbuz102j84OgjAJ
DGv/S86svmZWSqZ5UoJOIEqFYrONcOSgztZ5tU+gP4fwRIkTRbTEWSgudVREOXhs
bfN1YGP7HYvS0OiBKZUCAwEAAaOCAX0wggF5MB0GA1UdDgQWBBSIS6ZFxEbsj9bP
pvYazyY8kMx/FzCB5QYDVR0jBIHdMIHagBSIS6ZFxEbsj9bPpvYazyY8kMx/F6GB
tqSBszCBsDELMAkGA1UEBhMCVVMxFzAVBgNVBAgMDk5vcnRoIENhcm9saW5hMRAw
DgYDVQQHDAdSYWxlaWdoMRYwFAYDVQQKDA1SZWQgSGF0LCBJbmMuMRgwFgYDVQQL
DA9SZWQgSGF0IE5ldHdvcmsxHjAcBgNVBAMMFUVudGl0bGVtZW50IE1hc3RlciBD
QTEkMCIGCSqGSIb3DQEJARYVY2Etc3VwcG9ydEByZWRoYXQuY29tggkA5v5CKCXJ
5l4wDAYDVR0TBAUwAwEB/zALBgNVHQ8EBAMCAQYwEQYJYIZIAYb4QgEBBAQDAgEG
MCAGA1UdEQQZMBeBFWNhLXN1cHBvcnRAcmVkaGF0LmNvbTAgBgNVHRIEGTAXgRVj
YS1zdXBwb3J0QHJlZGhhdC5jb20wDQYJKoZIhvcNAQEFBQADggIBAJ1hEdNBDTRr
6kI6W6stoogSUwjuiWPDY8DptwGhdpyIfbCoxvBR7F52DlwyXOpCunogfKMRklnE
gH1Wt66RYkgNuJcenKHAhR5xgSLoPCOVF9rDjMunyyBuxjIbctM21R7BswVpsEIE
OpV5nlJ6wkHsrn0/E+Zk5UJdCzM+Fp4hqHtEn/c97nvRspQcpWeDg6oUvaJSZTGM
8yFpzR90X8ZO4rOgpoERukvYutUfJUzZuDyS3LLc6ysamemH93rZXr52zc4B+C9G
Em8zemDgIPaH42ce3C3TdVysiq/yk+ir7pxW8toeavFv75l1UojFSjND+Q2AlNQn
pYkmRznbD5TZ3yDuPFQG2xYKnMPACepGgKZPyErtOIljQKCdgcvb9EqNdZaJFz1+
/iWKYBL077Y0CKwb+HGIDeYdzrYxbEd95YuVU0aStnf2Yii2tLcpQtK9cC2+DXjL
Yf3kQs4xzH4ZejhG9wzv8PGXOS8wHYnfVNA3+fclDEQ1mEBKWHHmenGI6QKZUP8f
g0SQ3PNRnSZu8R+rhABOEuVFIBRlaYijg2Pxe0NgL9FlHsNyRfo6EUrB2QFRKACW
3Mo6pZyDjQt7O8J7l9B9IIURoJ1niwygf7VSJTMl2w3fFleNJlZTGgdXw0V+5g+9
Kg6Ay0rrsi4nw1JHue2GvdjdfVOaWSWC
```

© 2026 Tanium Inc. All Rights Reserved

```
-----END CERTIFICATE-----
```

NEXT STEPS

(Red Hat) Edit the **[Tanium Scan] - Linux** scan management technique to include the Red Hat repositories. For more information, see Edit a scan configuration on page 99.

Manage Linux repository snapshots

You can create, rename, or delete snapshots.

BEFORE YOU BEGIN

Repository snapshots have the following requirements:

- Minimum Patch version:
  - For deployments to Red Hat and CentOS Linux endpoints, Patch 2.4.1.
  - For deployments to Oracle Linux endpoints, Patch 2.4.3.
  - For deployments to SUSE endpoints, Patch 3.2.160.
- The Patch process must be running on all Linux endpoints. For more information, see Patch process is not running on Linux endpoints on page 152.
- Patch must be enabled for Linux endpoints. For more information, see Enable Patch for Enhanced Linux configurations on page 70.
- You must use the Tanium Scan for Linux scan method. For more information, see Tanium Scan on page 93.
- You must create a scan configuration with the **Use repository snapshots for deployment** option enabled. For more information, see Create a scan configuration on page 94.
- For Red Hat endpoints, you must set up certificate authentication. For more information, see (Red Hat endpoints) Configure Tanium Server to use certificate authentication on page 72 or (Red Hat endpoints) Configure TDownloader to use certificate authentication (Tanium Server version 7.5.2.3552 and earlier) on page 72.
- To create snapshots for repositories that use variables, ensure that at least one endpoint has that operating system distribution and version deployed and that the endpoint has the Patch tools installed. To verify whether Patch tools is installed, see Linux: Could not get results on page 168.

PROCEDURE

1. From the Main menu, go to **Modules > Patch > Scan Management** and then click **Repositories**.
2. To create a snapshot, select a repository and then click **Create Snapshot**. Name the snapshot and click **Confirm**.
3. To rename a snapshot, expand a repository and then click Rename Snapshot . Provide a new name and click **Confirm**.

© 2026 Tanium Inc. All Rights Reserved

4. To permanently remove unneeded snapshots, click Delete Snapshot .
5. To remove failed snapshots across all repositories; for example, those for which the environment was not properly set up, click **Delete Failed Snapshots**.

Export a Linux repository

You can facilitate the migration of patch content by exporting repositories. The exported file includes all settings and definitions, except for repository snapshots. This is particularly useful in progressive deployment models where patches must be moved from a testing environment to a production environment.

1. From the Main menu, go to **Modules > Patch > Scan Management** and then click **Repositories**.
2. Select a repository and then click **Export**.

The JSON file is available in your downloads folder.

Import a Linux repository

You can import an exported repository into a new environment.

> NOTE
> You cannot import a repository with the same name as an existing repository.

1. From the Main menu, go to **Modules > Patch > Scan Management** and then click **Repositories**.
2. Click **Import Repository** and then click **Choose File**.
3. Browse to the list in .JSON extension and then click **Import**.

Configure Patch behavior on action-locked endpoints

Configure how Patch behaves on action-locked endpoints.

> NOTE
> The Patch action lock setting does not override the Endpoint Configuration action lock setting. If you do not select **Manifest package ignore action lock** in Endpoint Configuration settings, then action-locked endpoints do not receive changes to Patch configurations. For more information, see Tanium Endpoint Configuration User Guide: Reference: Settings and Tanium Console User Guide: Managing action locks.

1. From the Main menu, go to **Modules > Patch > Overview** and click Settings **> Configuration Settings** if needed.
2. In the **Action Lock Behavior** section, select an option. For best results, select either **Applicability Scanning Only** or **Ignore Action Lock** to ensure the accuracy of workbench data.

© 2026 Tanium Inc. All Rights Reserved

Initialize Patch

Patch installs a set of tools on each Windows and Linux endpoint that you have targeted. Initializing or reinitializing Patch is a common troubleshooting step.



Patch does not work on endpoints with action locks turned on. Be sure action locks are turned off on endpoints that you want to target with Patch. For more information, see Tanium Console User Guide: Managing action locks.

1. From the Main menu, go to **Modules > Patch > Overview**, click Help and then click **Support** if needed.
2. Click **Initialize Endpoints** to start the Patch service and begin distributing these tools to your endpoints.

Select a language

Select one of the supported languages for the Patch workbench and Patch user guide, as described in Tanium Console User Guide: Reference: Language support.

© 2026 Tanium Inc. All Rights Reserved

Downloading Windows patches in an air-gapped environment

When your Tanium Server is in an air-gapped environment, the server cannot download patches from the Internet. Instead, you must configure Tanium Patch to install patches from an alternate location. You have two options:

- Patch air-gapped environments using Tanium Scan for Windows on page 81
- Patch air-gapped environments using Offline CAB on page 83

> NOTE
>
> Offline CAB supports patching Windows versions earlier than Windows 11 version 22H2. For endpoints on Windows 11 version 22H2 or later, use Tanium Scan for Windows.

Before you begin

- If you want to configure a UNC share on a Tanium Appliance, you must add an authentication user for TDownloader as described in the Tanium Appliance User Guide: Add an authentication user for TDownloader.
- Review your firewall configuration to confirm that the necessary ports are open for remote sources. For more information, see Tanium Console User Guide: Manage remote systems.

Patch air-gapped environments using Tanium Scan for Windows

If you are using the Tanium Scan for Windows scan method, you must configure Tanium Scan to retrieve patches from a local WSUS server.

1. Ensure that your local WSUS server is configured to store updates locally. For more information, see Microsoft Documentation: Choose a WSUS storage strategy.
2. Configure Tanium Scan for Windows.
    a. From the Main menu, go to **Modules > Patch > Scan Management**.
    b. Click **Tanium Scan for Windows** and then click **Edit**.
    c. Select **Enable Tanium Scan for Windows** (if not already selected) and select a scan source.
    d. In the **Tanium Scan Source** section, select **Local WSUS Server** to retrieve patches from a local WSUS server.
        - Enter the **URL** and the **Content Download Port**. The content download port is the port from which the Tanium Server can download patch installation files. The Tanium Server then delivers the files as part of a Patch deployment.The default port may be 8530 or 80, depending on the WSUS server version. You can configure the

© 2026 Tanium Inc. All Rights Reserved

WSUS server to use a custom port.

- Choose a PEM file containing the certificate authority for the WSUS server. The certificate should be the Base64-encoded ASCII, certificate chain format.

e. If you want to synchronize after Microsoft releases many significant patches, select **Enable Schedule Synchronization**.

f. Use the arrows to select products to include in scans.

> BEST PRACTICE
>
> Synchronize all products, regardless of which products are present in the environment. Selectively choosing products can cause gaps in critical or important patches.

g. Use the arrows to select update classifications to include in scans.

> BEST PRACTICE
>
> Select **Critical Updates**, **Security Updates**, **Service Packs**, and **Update Rollups**.

h. Click **Submit**.

3. Configure WSUS server allowed URLs.

   a. Add the WSUS Server URL.

      i. From the Main menu, go to **Modules > Patch> Overview** and click Settings **> Configuration Settings** if needed.

      ii. In the **WSUS Server Configuration** section, enter the URL and click **Submit**. A regular expression for the URL is generated and added.

      iii. Click **View Allowed URLs**, or go to **Administration > Permissions > Allowed URLs** to view the entry that was added.

   b. On the WSUS server, change the following settings:

      i. Set the intranet URL for detecting updates and the statistics server to `http://<WSUS server URL>:<port>`.

      ii. Disable the **Configure Automatic Updates** setting.

4. Create a scan configuration that uses Tanium Scan.

   a. From the Main menu, go to **Modules > Patch > Scan Management**.

   b. Click **Create Scan Configuration**.

   c. Enter a name and description for the configuration.

   d. For the **Platform**, select **Windows**.

   e. For the **Configuration Technique**, select **Tanium Scan**.

© 2026 Tanium Inc. All Rights Reserved

f. In the **Frequency** field, enter a number and a time parameter.



Set this value to less than three days to improve the Patch coverage metric.

g. (Optional) Select **Enable Random Scan Delay** and enter a time to distribute the network activity.
The default is 120 minutes.

For VDI environments, set a longer scan delay, such as 480 minutes or higher, depending on the density and hardware performance of your VDI environment, to reduce the impact of the scan on the host system.

h. (Optional) Select **Scan only within defined window** to define the scan window options, such as browser time or local time on the endpoint, how often the window repeats, and override options. For more information, see Downloading Windows patches in an air-gapped environment on page 81.



The scan window specifies when a scan can start. If you enabled **Random Scan Delay**, scans can potentially start as late as the specified delay after the end of the scan window. For example, if a scan attempts to start one minute before the end of the scan window, but receives the full random scan delay of 120 minutes, the scan does not start until after that 120 minutes and continues to run until completion, even though the scan window is already closed.

i. Click **Create Scan Configuration**.

j. In the **Targeting** section, click **Select Computer Groups** to add one or more computer groups.

5. On the WSUS server, stage and approve the patches.
6. For patches that are applicable to Windows 11 version 22H2 or later endpoints, manually synchronize the patches. For more information, see Manually synchronize patches on page 108.
7. Deploy the patches.

Patch air-gapped environments using Offline CAB

If you are using the Offline CAB scan method, you must configure Patch to install patches from an alternate file location on an authorized local server that is accessible to the endpoints within the air-gapped environment.

1. Create a scan configuration with the **Offline CAB** configuration technique. For more information, see Create a scan configuration on page 94.
2. From the Main menu, go to **Modules > Patch > Scan Management** and then click **Airgap Configuration**.

© 2026 Tanium Inc. All Rights Reserved

3. Define the alternate location for patch files on the local network.

   a. Select **Enable Settings for Airgap - Windows**.

   b. Provide an **Alternate Patch File Location** where all air-gapped files are staged and then click **Save**.

   IMPORTANT

   - The network location that you specify must be accessible by the Tanium Server. To use a UNC path or a credential-protected URL, configure the settings based on the Tanium Server version and operating system.
     - **Tanium Server 7.5.3.3503 and later:** You must configure a downloads authentication entry for the UNC path or credential-protected URL. For information about configuring a downloads authentication entry, see Tanium Console User Guide: Managing remote authentication.
     - **(TanOS) Tanium Server earlier than 7.5.3.3503:** You must configure credentials in the TanOS Tanium Operations menu. For information, see Tanium Appliance User Guide: Add an authentication user for TDownloader
     - **(Windows) Tanium Server earlier than 7.5.3.3503:** You must configure the Tanium Server service account to run as a Windows user with sufficient permissions. For information, see Tanium Appliance User Guide: Add an authentication user for TDownloader
   - Tanium does not support hidden or administrative shares.

   c. From the Main menu, go to **Administration > Permissions > Allowed URLs** to verify that the configured alternate Patch file location is listed.

4. In the **Download Airgap Utility** section, click **Download Utility** to download the `airgap-downloader.exe` utility.

   NOTE

   You must run this utility on a Windows computer that can access the internet.

5. In the **Generate Download Manifest** section, select the **Include CAB File** and **Include MS-CVEs.dat File** options and then use the filters to create a list of patches to use in the air-gapped environment. For example, you can filter on a specific patch list, or you can filter only for Windows patches released during the past month that are applicable and have not been superseded.

6. In the list that you generate, select individual patches to include, or hold the Shift key and then select multiple patches.

© 2026 Tanium Inc. All Rights Reserved

7. Click **Download Manifest** to generate a file that contains a list of URLs for patch files that you will download and use to patch the air-gapped endpoints.

   A `urls.txt` file is downloaded to your computer. For example:

   ```
   http://download.windowsupdate.com/microsoftupdate/v6/wsusscan/wsusscn2.cab
   https://content.tanium.com/files/hosted_dats/MS-CVEs.dat
   https://content.tanium.com/files/windows-patch/wsusscn2.json
   ```

8. Use the `urls.txt` file that you generated from the Tanium Server to download files from a computer that is connected to the internet.

   a. Copy the `urls.txt` and `airgap-downloader.exe` files to a computer that is connected to the internet and open a command prompt to that directory.

   b. To download the package files from sources contained in `urls.txt`, run:

   ```
   airgap-downloader.exe download_files --no_rename
   ```

   > **NOTE** If the `urls.txt` and `airgap-downloader.exe` files are not in the same directory, you must also include the `--urls_source` option.

   The command downloads the files in the list and generates a `results.zip` archive that contains:

   - The downloaded files
   - A manifest `results.txt`

   c. Extract the contents of the `results.zip` file to the root of the alternate Patch file location that you defined on the local network.

Verify the Offline Cab configuration

To verify that Offline Cab for airgap was configured correctly, you can confirm the following:

1. Verify that the Tanium Server has the staged files:

   a. From the Main menu, go to **Administration > Content > Packages**.

   b. Select the **Patch - External File References - Windows** package and click Edit Selected.

   c. In the **Files** section, click **wsusscn2.cab** and verify that the **SHA-256** field has a non-empty hash value.

   d. Click **MS-CVEs.dat** and verify that the **SHA-256** field has a non-empty hash value.

© 2026 Tanium Inc. All Rights Reserved

2. Verify that the Windows endpoints can scan against the staged files:

    a. From the Main menu, go to **Modules > Patch**.

    b. In the **Scan Source Details** section, verify that the hash value in the **Microsoft Offline CAB File Information** matches the value in step 1c.

© 2026 Tanium Inc. All Rights Reserved

Downloading Linux patches in an air-gapped environments

When your Tanium Server is in an air-gapped environment, the server cannot download patches from the Internet. Instead, you must download patches to your local repository and configure Tanium Patch to scan and download using the repository.



Do not click **Initialize Endpoints** from the **Help > Support** page. Otherwise, all the changes that you make to the external packages in the following procedure are deleted. Also, do not send requests to the following routes:

- POST /v1/jobs/all
- POST /v1/jobs/sync-external-file-references

Download Linux CVE metadata

Use the **Download Airgap Utility** to download Linux CVE metadata. The Tanium Server uses this data to parse advisory details, CVE mappings, and package versions that resolve vulnerabilities.

1. From the Main menu, go to **Modules > Patch > Scan Management** and then click **Airgap Configuration**.
2. Download the Airgap Downloader utility. This utility is primarily used for Windows air-gapped environments but you can also use the utility to download Linux CVE metadata.
    - If you previously enabled **Airgap Configuration**, click **Download Utility** to download the `airgap-downloader.exe` utility.
    - If you do not see the **Download Utility** button, complete the following steps:
        a. Select **Enable Offline CAB** file.
        b. In the **Alternate Patch File Location** field, enter a dummy URL. This alternate location is used for Windows air-gapped environments and does not apply to Linux air-gapped environments. However, you still need to provide a value to continue to the next step.
        c. Click **Save**. The **Download Airgap Utility** section appears.
        d. Click **Download Utility**.
3. Populate a text file with the file addresses of the Linux patch metadata.
    a. Create a `urls.txt` file.
    b. From the Main menu, go to **Administration > Content > Packages**.
    c. Search for and select **Patch - External File References – Linux**.
    d. For each file that you want to include, copy the **File Address** field to the `urls.txt` text file; one address per line.

© 2026 Tanium Inc. All Rights Reserved

4. Download the Linux patch metadata.

    a. Copy the `urls.txt` and `airgap-downloader.exe` files to a Windows computer that can access the Internet.

    b. Open a command prompt to that directory.

    c. Run the following command to download the package files from sources contained in `urls.txt`:
    `airgap-downloader.exe download_files --no_rename`

    > NOTE
    > If the `urls.txt` and `airgap-downloader.exe` files are not in the same directory, you must also include the *--urls_source* option.

    The command downloads the files that are defined in the `urls.txt` and generates a `results.zip` archive that contains the following contents:

    - The downloaded files
    - A manifest `results.txt`

    d. Copy and extract the contents of the `results.zip` file to an air-gapped computer that can access the Tanium Console. For example, you can copy the contents to a flash drive, insert the drive into the air-gapped computer that is running the Tanium Server, and then transfer the files.

Modify the Patch - External File References – Linux package

By default, the **Patch - External File References – Linux** package contains external URL references to all the Linux patch metadata. Modify the **File Address** field for all the files in the package so that the fields do not point to an external URL.

1. On the air-gapped computer where you extracted the `results.zip` file, open Tanium Console.
2. From the Main menu, go to **Administration > Content > Packages**.
3. Search for and select **Patch - External File References – Linux**.
4. Click **Edit Mode**.
5. In the **Files** section, click Delete for every file.
6. Click **Add File > Local Files** and then click **Browse for Files**.
7. Select the Linux files that were extracted from the `results.zip`. After you upload the files, notice that the **File Address** field includes the file name only and does not include an external URL.
8. Click **Save**.

Recreate the Required Files - Linux configuration

Recreate the **Required Files – Linux** configuration to initialize the use of the updated **Patch - External File References – Linux** package.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Shared Services > Endpoint Configuration > Configurations**.
2. Search for and select **Required Files – Linux**.
3. Click **Delete**.

After a few minutes the file is recreated.

Add local repositories

Add your locally hosted repositories that the Tanium Server can contact and then target the computer groups with the air-gapped endpoints. Tanium Patch uses these repositories to scan for and download packages that you can use to patch Linux endpoints. For more information, see Add and target Linux repositories.

Configure scans for air-gapped environments

Create a scan configuration to target Linux endpoints that are air-gapped and ensure that these endpoints are not targeted by other scan configurations.

1. From the Main menu, go to **Modules > Patch > Scan Management > Scan Configurations**.
2. Click **Create Scan Configuration** and complete the fields with the following settings.
    - **Configuration Technique**: Select **Tanium Scan**.
    - **Repositories**: Add the local repositories that you previously configured.
3. Click **Create Scan Configuration**. The configuration is created, and the Scan Configuration details page appears.
4. In the **Targeting** section, click **Select Computer Groups** and target the group of air-gapped Linux endpoints.
5. Unenforce the default **[Tanium Scan] - Linux** scan configuration from Linux endpoints that are air-gapped.
    a. From the Main menu, go to **Modules > Patch > Scan Management > Scan Configurations**.
    b. Select **[Tanium Scan] - Linux**.
    c. In the **Targeting** section, remove the computer groups that include air-gapped Linux endpoints.

What to do next

Verify that you are getting scan results from endpoints and then create patch deployments as needed.

© 2026 Tanium Inc. All Rights Reserved

Enforcing scan configurations

Manage your scan configurations to select how and when scans are enforced. The list of available Windows and Linux patches comes from scanning the endpoints in your network. The *scan configuration* determines a scanning technique and frequency. A scan configuration is *enforced* by targeting computer groups.

Windows scan techniques

For Windows endpoints, the available scanning techniques include the offline CAB file, online Microsoft Windows Update, Windows Server Update Services (WSUS) Scan, and Tanium Scan.

For Windows scan configurations, you can enable *isolated endpoints* to download patch files directly from Microsoft instead of the Tanium Server to free network resources. An isolated endpoint is a Tanium Client that has no peer Tanium Clients. To download patches directly from Microsoft, an isolated endpoint must be connected to a user-configured list of Tanium Zone Servers or IP address ranges for split-tunnel VPN clients. For more information, see Enable direct patch downloads from Microsoft on page 67.

For Linux endpoints, the available scanning techniques include Repository Scan and Tanium Scan.

Windows scan techniques

Tanium Scan



If you are using Tanium Scan for Windows with a local WSUS server, you must approve updates on the WSUS server.

Tanium Scan for Windows allows Patch to assess all Microsoft Products (excluding Microsoft 365 Apps, Office 2019, and Office LTSC) and Update Classifications (excluding Drivers, Definition Updates, and Upgrades) on supported Windows 10 or later endpoints. The Patch service on the Module Server is configured to synchronize update metadata and detection rules directly from Microsoft. Alternatively, it can be configured to synchronize from WSUS in airgap scenarios where WSUS is available and already has approved and downloaded patches.

After the update metadata and detection rules are synchronized, the Patch service distributes portions of this data (in a client database file) to applicable machines on the network. The Windows Update Agent performs the scan against selected products and classifications and return data in the form of applicable and not applicable patches.

Tanium Scan for Windows is much less resource intensive than the offline CAB file scan method and provides more robust scan results. Tanium Scan does not rely on each endpoint having network access to Microsoft Update or a local WSUS server. For more information about Tanium Client requirements, see Core platform dependencies on page 34.

To enable and configure Tanium Scan for Windows, see Enable and configure Tanium Scan for Windows on page 65.

© 2026 Tanium Inc. All Rights Reserved

NOTE

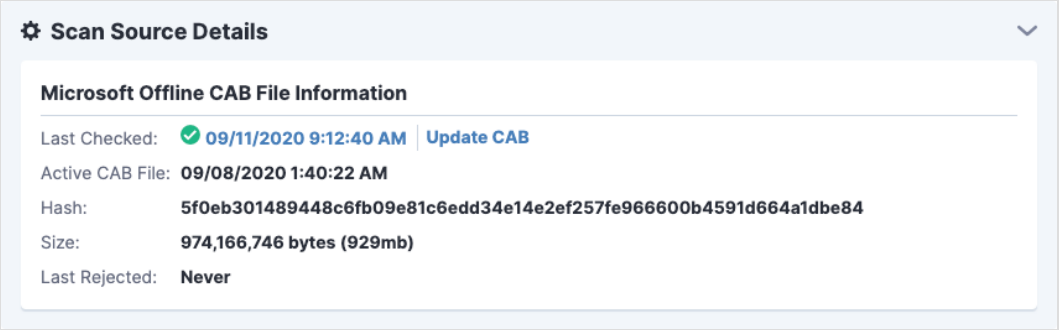
If you want to use Tanium architecture to deliver cumulative updates for Windows 11 version 22H2 or later endpoint, you must use Tanium Scan.

If enabled in **Configuration Settings**, the Online Microsoft Windows Update scan technique supports direct download of patches from Microsoft to isolated endpoints. For more information, see Enable direct patch downloads from Microsoft on page 67.

Offline CAB File

The Windows Cabinet (CAB) file is stored locally by the Tanium Client and contains security updates, update rollups, and service packs for all products in the Microsoft Update Catalog, including Windows and Office. On the Patch **Overview** page, the latest status of the offline CAB file is available. The active CAB file is the most recent, verified file published by Microsoft. Patch uses only the active CAB file for scan configurations. A rejected CAB is not pushed to a computer group. Patch checks for an updated CAB file every 15 minutes. You can click **Update CAB** to force a new download outside of the normal schedule.

Example CAB file status



NOTE

Offline CAB File includes only Security Updates, Service Packs, and Update Rollups updates. Because other scan methods include more updates than **Offline CAB File** includes, if you change the scan configuration technique on an active deployment from **Offline CAB File** to another technique, additional patches might be installed on endpoints.

Online Microsoft Windows Update

The Online Microsoft Windows Update option creates additional network traffic between the Tanium Client and Microsoft and is for Microsoft updates in Windows operating systems only. The full range of patches in the following list are available for scanning in the Windows operating system:

© 2026 Tanium Inc. All Rights Reserved

- Critical patches
- Cumulative security and quality patches

  The Microsoft online APIs do not always provide the required URLs to download and install cumulative update patches. Use this option in situations where Tanium Patch is being used only for auditing patch compliance.

- Non-security and optional updates

If enabled in **Configuration Settings**, the Online Microsoft Windows Update scan technique supports direct download of patches from Microsoft to isolated endpoints. For more information, see Enable direct patch downloads from Microsoft on page 67.

WSUS



If you are using Microsoft System Center Configuration Manager (SCCM) with your WSUS server, do not use Tanium for WSUS scanning with the same server.

Using WSUS servers for patching activities gives the option for the full range of patch types for all products in the Microsoft Update Catalog, including Windows and Office. However, some additional configuration is required. The Tanium Client must be able to contact the WSUS server, and patches must be approved before they can be downloaded.

The guidelines about how many clients a WSUS server can support are similar to the Microsoft guidelines for SCCM: up to 150,000 clients per WSUS server. For more information, see Microsoft Docs: Size and scale numbers for System Center Configuration Manager.

If enabled in **Configuration Settings**, the Online Microsoft Windows Update scan technique supports direct download of patches from Microsoft to isolated endpoints. For more information, see Enable direct patch downloads from Microsoft on page 67.

Linux scan techniques

For Linux endpoints, the available scanning techniques include Repository Scan and Tanium Scan.



To simplify Linux scanning, enable **Enhanced Linux Support** in the Patch **Configuration Settings**. This setting lets you create a single scan technique that applies to multiple Linux distributions, instead of having to create separate OS-based scan techniques. For more information, see Enable Patch for Enhanced Linux configurations on page 70.

© 2026 Tanium Inc. All Rights Reserved

Repository Scan

Using repositories for patching activities gives the option for the full range of patch types for all updates in the repositories. However, you must configure one or more repositories, and updates must be maintained in the repositories. The Tanium Client must be able to contact the repositories for scanning as well as patch downloads.

For the Repository Scan technique, you can use all repositories from which an endpoint can pull.



When using the Repository Scan technique with Red Hat distributions, endpoints must be directly registered with Red Hat or a Red Hat Satellite server.

Tanium Scan



For best results, create a single scan configuration for Tanium Scan for Linux targeting the Patch Supported Systems computer group with each included repository targeted to the proper operating systems. For more information, see Red Hat Linux endpoints stuck in Waiting for Initial Scan status on page 152.

Tanium Scan for Linux can use both internal or external repositories, but only the Tanium Server needs connectivity to the repositories. The Tanium Client stores the repository scanning logic in the local Tanium Client directory. Package managers (for example, Yum, DNF, Zypper, and Apt) cache repository data in the `/var` partition. In most cases, the cache does not exceed 500 MB. If you use lean partitioning or have a high count of configured repositories, evaluate the available disk space and partition configurations to ensure `/var` has sufficient free space. If you patch from repository snapshots, ensure that the `/var` partition has at least two times the needed free disk space, as both the snapshot and non-snapshot repository data occupy this space.

Tanium Scan supports AlmaLinux, CentOS, Debian, openSUSE, Oracle Linux, Red Hat, Rocky Linux, SUSE, and Ubuntu distributions. With Tanium Scan for Linux, you can create and use repository snapshots for deployments. For more information, see Linux repository snapshots on page 21.



When using the Tanium Scan technique with Red Hat distributions, you must use Red Hat Content Delivery Network, Red Hat Satellite 6 or later, or custom repositories. For more information, see (Red Hat endpoints) Configure Tanium Server to use certificate authentication on page 72.

TANIUM SCAN INCOMPATIBILITY WITH LIBZYPP SERVICES PLUGINS

Tanium Scan for Linux is not compatible with LibZypp Service Plugins, such as Spacewalk. LibZypp Service Plugins provide a client a list of repositories. This method conflicts with Tanium Scan being the sole source of repositories.

If a LibZypp Service Plugin is in use when attempting to run Tanium Scan, Patch displays scan and deployment error messages as this configuration is unsupported.

To determine if there are any LibZypp Service Plugins on an endpoint, review the `/usr/lib/zypp/plugins/services` directory, where all LibZypp Service Plugins are listed. If the `/usr/lib/zypp/plugins/services` directory is not empty, Tanium Scan is not supported.

© 2026 Tanium Inc. All Rights Reserved

You cannot disable LibZypp Service Plugins during a Tanium Scan. If possible, uninstall the plugin and create repositories using Tanium. If the plugin package cannot be uninstalled, use Repository Scan instead of Tanium Scan.

Create a scan configuration

You can create multiple scan configurations and add computer group enforcements as needed.

BEST PRACTICE

Any endpoint that is supported by Patch should be targeted by at least one scan configuration.

1. From the Main menu, go to **Modules > Patch > Scan Management** and then click **Create Scan Configuration**.
2. Provide a name, an optional description, and select an operating system.
3. Choose the scan configuration options.
   a. (Windows and Linux) Select a **Configuration Technique** and applicable options.

   CAUTION

   For Red Hat, Ubuntu, and SUSE Linux Enterprise Server (SLES) endpoints, if you choose **Repository Scan**, you must also select **Use repositories configured on endpoint**.

   (Windows) If you choose **Offline CAB File**, select **Download and scan immediately upon new CAB release** to ensure that the endpoints are scanned when a new CAB file is published. Similarly, if you choose **Tanium Scan**, select **Scan when new patches are available** to ensure that the endpoints are scanned when a new patch is released. Selecting either of these settings overrides the frequency settings, but scans still wait for the scan window, if configured.

   BEST PRACTICE

   - (Windows endpoints) Choose **Tanium Scan**. If you use other products that use WSUS technology on the same endpoints, such as SCCM, select **Enable Managed Compatibility** to enable an additional scan to ensure compatibility.
   - (CentOS, Debian, Oracle Linux, Red Hat, SUSE, and Ubuntu endpoints) To use repository snapshots for Linux deployments, choose **Tanium Scan**.
   - (Amazon endpoints) You must use **Repository Scan**.

   (Optional, Windows) If you choose **WSUS**, select **Enable audit only mode** if you want Tanium to scan for all patches synchronized in WSUS, including patches that are not available to be installed because they are unapproved. This setting lets you use a WSUS server to audit systems for missing patches. If you do not select this option, then Tanium will scan only for approved patches.

   b. In the **Frequency** field, enter a number and a time parameter.

   BEST PRACTICE

   Set this value to less than three days to improve the Patch coverage metric.

© 2026 Tanium Inc. All Rights Reserved

c. (Optional) Select **Enable Random Scan Delay** and enter a time to distribute the network activity.
The default is 120 minutes.

For VDI environments, set a longer scan delay, such as 480 minutes or higher, depending on the density and hardware performance of your VDI environment, to reduce the impact of the scan on the host system.

d. (Optional, Windows) To enable remote endpoints to download patches directly from Microsoft, select **Enable Patch direct downloads from Microsoft**.



- To download patches directly from Microsoft, you must also enable direct downloads in the Patch **Configuration Settings**. Click **View Settings for Direct Download** to access those settings. For more information, see Enable direct patch downloads from Microsoft on page 67.
- The **Enable Patch direct downloads from Microsoft** option will not appear if your administrator has disabled it.

e. (Optional, Linux) To use repository snapshots for Linux deployments, select **Deployment Snapshots** and choose the repository name and the snapshot in the **Repositories** section.



If you use this feature, be aware that the snapshot files uses additional disk space in the `/opt/Tanium/TaniumClient/Tools/Patch/data/repos` and `/var/cache` directories. For example, the directories might contain `repo-42` and `repo-42-snapshot-1` files.

4. (Optional) Select **Scan only within defined window** to define the scan window options, such as browser time or local time on the endpoint, how often the window repeats, and override options. For more information, see Scan windows on page 96.



The scan window specifies when a scan can start. If you enabled **Random Scan Delay**, scans can potentially start as late as the specified delay after the end of the scan window. For example, if a scan attempts to start one minute before the end of the scan window, but receives the full random scan delay of 120 minutes, the scan does not start until after that 120 minutes and continues to run until completion, even though the scan window is already closed.

5. Click **Create Scan Configuration**.

6. In the **Targeting** section, click **Select Computer Groups** to add one or more computer groups.
Enabling the patch applicability results provides a refined aggregation for the specific computer group.

The list of available patches might appear within 15-30 minutes. Longer scan delays might result in patches appearing slowly. If no data appears after the scan delay, Contact Tanium Support on page 162. If an endpoint cannot be scanned, for example if it is offline, it is scanned at the earliest opportunity.

© 2026 Tanium Inc. All Rights Reserved

Scan windows

You can set a scan window to restrict scans to a certain time of day or day of the week. For example, you can create a scan configuration to scan your endpoints daily, but restrict the scans to run during non-business hours, such as from 6:30 PM to 11:30 PM. Additionally, if some of your endpoints are offline during the scan window, you can choose the **Override** option to scan any endpoints that have a scan age older than a specified amount of time, in hours or days.

NOTE

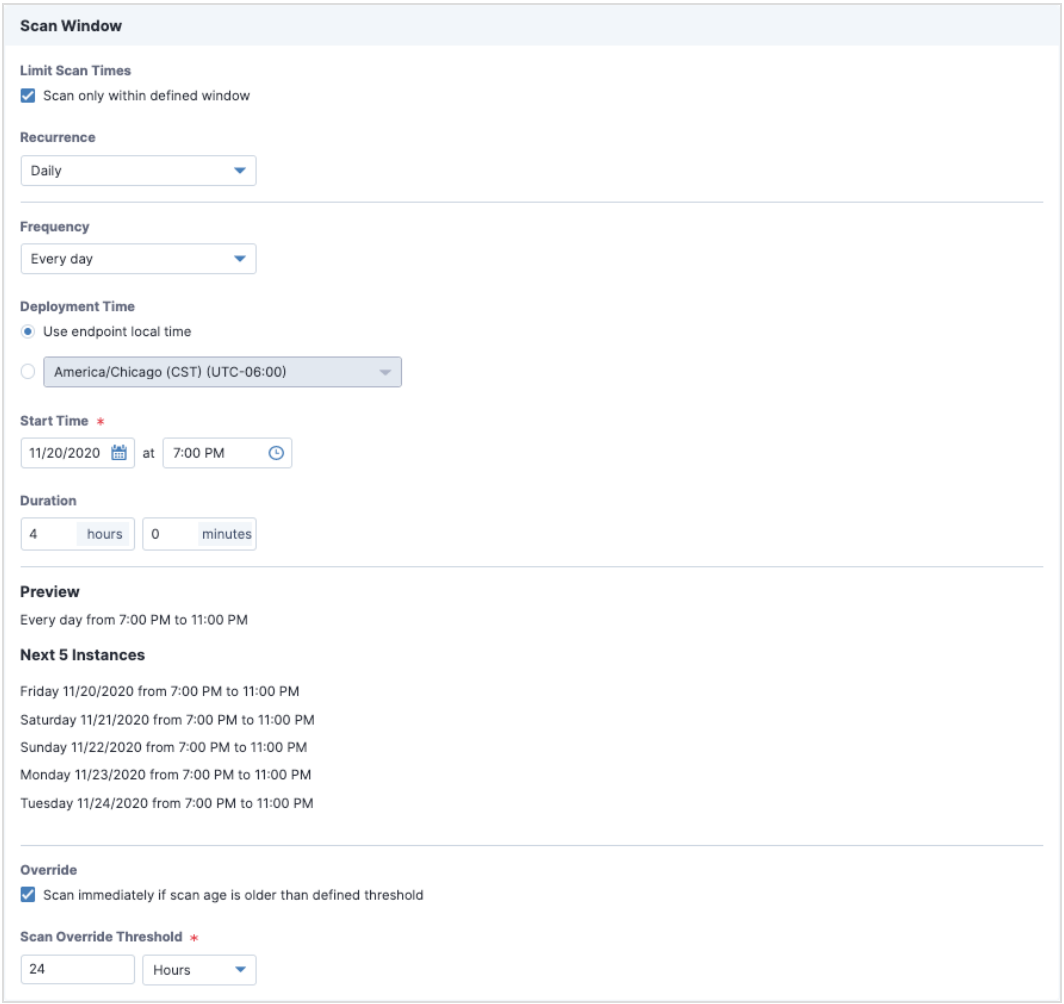
A maintenance window is different from a scan window. Maintenance windows are mandatory, one-time or repeating time frames that define when Windows and Linux patches can be applied to a computer group. Scan windows are optional restrictions that define when endpoints are scanned. For more information, see Setting maintenance windows on page 131.

BEST PRACTICE

Scan windows are optional. If you decide to use them, the **Override** option should be set to less than two days to increase the Patch coverage metric.

© 2026 Tanium Inc. All Rights Reserved

1. In the **Scan Window** section, select **Scan only within defined window**.
2. Configure your preferences:



   a. (Optional) Choose whether to repeat the scan window daily or weekly.
   b. Set additional frequency options.
   c. Select between the local time on the endpoint or UTC time.
   d. Use the date and time pickers to set the start time of the window.
   e. Set the duration of the scan window.

© 2026 Tanium Inc. All Rights Reserved

f. (Optional) Select **Scan immediately if scan age is older than defined threshold** and specify how many hours or days can elapse before triggering an immediate scan.

> NOTE
>
> This setting overrides the **Scan Window** settings and can control the timing of scans on endpoints depending on the **Scan Override Threshold** and **Scan Configuration Options Frequency** values. For example, an endpoint does not complete a scan during a daily four-hour scan window, the **Scan Configuration Options Frequency** is 24 hours and the **Scan Override Threshold** value is 25 hours. After 25 hours, the **Scan Override Threshold** value forces a scan on the endpoint. During the next daily four-hour scan window, the endpoint does not scan because it has scanned within 24 hours. After 25 hours, the **Scan Override Threshold** value forces a scan again.

> BEST PRACTICE
>
> Set this value to less than two days.

View enforcement status

By reviewing a scan configuration, you can see which endpoints in the computer group contain the enforced configuration.

1. From the Main menu, go to **Modules > Patch > Scan Management** and then click the name of a scan configuration.
2. In the **Enforcements** section, click the links for any of the enforcement statuses to open the question results for each endpoint.
   The Interact results grid shows the endpoint status and the reason, if it is not enforced.

> BEST PRACTICE
>
> Investigate endpoints with scan errors that have scan results older than two days and resolve the errors for each endpoint. For more information, see Troubleshoot scan errors on Windows and Linux endpoints on page 150.

Prioritize scan configurations

You can create multiple scan configurations with multiple computer groups. The order of the configuration in the **Scan Configurations** list decides its priority. If an endpoint is in multiple computer groups with conflicting configurations, only the highest priority configuration in the list is applied to the endpoint.

> NOTE
>
> The highest priority configuration has a **Priority** of `1`.

1. From the Main menu, go to **Modules > Patch > Scan Management**.
2. On the **Scan Configurations** tab, click **Prioritize**.
3. Move the scan configuration by dragging and dropping it into the order that you want and then click **Confirm**.

© 2026 Tanium Inc. All Rights Reserved

Edit a scan configuration

1. From the Main menu, go to **Modules > Patch > Scan Management** and then click the name of a scan configuration.
2. Click **Edit** and make your changes.

   NOTE

   You cannot edit a scan configuration if the **Allow Scan Configuration Editing** option is disabled in the Patch Settings.

3. Click **Update Scan Configuration**.

Remove a scan enforcement

Removing a computer group from a scan configuration removes the enforcement.

1. From the Main menu, go to **Modules > Patch > Scan Management** and then click the name of a scan configuration.
2. In the **Targeting** section, delete the computer group.

Delete a scan configuration

After the enforcements are removed, you can delete a scan configuration.

1. From the Main menu, go to **Modules > Patch > Scan Management** and then click the name of a scan configuration.
2. If the scan configuration is enforced against Computer Groups, remove all groups.
3. Click Delete .

© 2026 Tanium Inc. All Rights Reserved

Managing patches

You can manage Windows and Linux patches with patch lists and block lists. *Patch lists* are groups of patches that can be applied on the targeted computer groups. *Block lists* are groups of patches that are specifically excluded from being downloaded or deployed to the targeted computer groups.

Default patch lists

Patch automatically includes the following patch lists. If a patch list is marked as **Tanium Managed** in the **Patch Lists** page, you cannot edit or delete it.

Patch list	Description
[Patch Baseline Deployment] - Windows for Windows endpoints	Includes security updates, update rollups, and service packs for Windows endpoints. This is a basic Windows patch list that you can use as a good starting point. NOTE If you import Patch with default settings, this patch list is automatically created.
• **[Tanium Patch Baseline Reporting] - Windows** • **[Tanium Patch Baseline Reporting] - Linux**	Tanium managed. Used in the **Patch** section of the **IT Operations Metrics** board in Trends. • The Windows patch list includes patches that are associated with security updates, update rollups, and service packs. • The Linux patch list includes security patches, patches with a severity that is greater than none, or patches that are associated with a CVE.
All Patches	Tanium managed. Used in the **Patch** board in Trends. Includes all patches for all operating systems.
Tanium Patch Recommended Updates] - Windows for Windows endpoint	Tanium managed. Includes all critical, high, and important patches released 30 or more days ago. Patch updates the items in this patch list each time the list is used in a deployment.

Patch list rules

Although you can manually select patches to include in a patch list, it is more efficient to use rules to dynamically populate lists of patches. As patches are added to the Available Patches list, Tanium assesses those patches for inclusion on a list by comparing them to rules. You can create rules from customized conditions that define which part of the patch description to examine.

Consider the following example rules and conditions:

© 2026 Tanium Inc. All Rights Reserved

Rule	Explanation
Condition: **Classification equals** `Security Updates` AND Condition: **Release Date is on or before** `8/12/2022`	The rule includes security updates released on or before August 12, 2022. You must update the date in this rule at a regular interval to include future security updates.
Condition: **Classification equals** `Security Updates` AND Condition: **Release Date is equal to or older than** `30 days`	The rule includes security updates released 30 or more days ago. Each time the patch list that contains this rule is used, Patch updates the security updates in the list. You do not need to update the rule at a regular interval to include future security updates.
Condition:**Classification equals**`Service Packs` AND Condition: **Release Date is equal to or older than**`14 days`	The rule waits 14 days until after a service pack is released to include it in the patch list. Each time the patch list that contains this rule is used, Patch updates the service packs in the list. You do not need to update the rule at a regular interval to include future service packs. You might use this rule to defer installation to allow time for testing.



- Include patches for the current month.
- Avoid waiting longer than two weeks after a patch release to start patching production systems.
- Expand endpoint diversity in patch testing groups to increase the chances of identifying newly-released problematic patches for deploying patches to production.

You can include the following options in rule conditions.

© 2026 Tanium Inc. All Rights Reserved

Rule condition options

Condition	Available options
Column	• Title • Severity • Release Date • Bulletins • KB Articles • CVE • Custom Field • Product • Classification
Type	• Contains • Equals • Does not contain • (Release Date only) On or after (date) • (Release Date only) On or before (date) • (Release Date only) Equal to or newer than (age) • (Release Date only) Equal to or older than (age)
Expression	The search criteria used in the expression.

Create a patch list

Sort patches into manageable patch lists for use in deployments or reporting. For example, you might create a patch list that includes security updates to use in a deployment for Windows endpoints or to generate a report for the security team. Or you might have a 30-day service level agreement (SLA) on patch installation, so you create a patch list that includes the **is equal to or older than 30 days** option to track your alignment with the SLA and deploy any needed patches.

You can add individual patches to the list or populate the list dynamically with rules.



For testing environments, create a patch list to deploy the latest patches. For production environments, create a patch list using the options **Release Date is equal to or older than 30 days**, so you can reuse this patch list each month without making any changes.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules > Patch > Patch Lists**.
2. Click **Create Patch List**, name the list, select an operating system, and select a content set.
3. Add patches.

Adding patches dynamically

a. Select **Include superseded patches when applying rules** to include these patches in your patch list.

> BEST PRACTICE
>
> Although including superseded patches is not selected by default, select this option to provide visibility of all applicable patches, including superseded patches. This visibility provides data to understand the scope of non-compliance on endpoints. For more information, see Superseded and superseding patches for Windows and Linux endpoints on page 18.

b. Click **Add Rule**.

c. Name the rule.

d. Select a **Condition** and an **Operator**.

e. Type in the expression to search. Searches are not case sensitive. Click **Apply**.

f. (Optional) Add additional conditions.

> IMPORTANT
>
> When a rule has more than one condition, the conditions are connected with the AND operator. Patches must meet both conditions to be included. When a list has multiple rules, the rules are connected with the OR operator, so patches that meet either rule are included on the list.

Add patches manually

a. Expand **Add Patches Manually**.

b. Select the patches that you want.

c. (Optional) Click the patch title to see the details in a new browser tab.

> BEST PRACTICE
>
> Avoid choosing specific patches based on vulnerability reports. Instead, use dynamic, rule-based patch lists. These lists should be cumulative. For example, do not create any rules that prevent patches that are older than a specific date from being included in a patch list.

You can get details about the patch, visibility into the results by computer group, and the associated lists.

4. Preview the changes and then click **Create Patch List**.

To distribute the patches to endpoints, see Create a deployment to install patches on page 116.

© 2026 Tanium Inc. All Rights Reserved

Exclude patches with block lists

A block list is a collection of patches that are prohibited from downloading or deploying to the targeted computer groups. You can add individual patches to the list or populate the list dynamically with rules. Unlike patch lists, you do not need to create a deployment to enforce a block list. For best results, use block lists only for patches that are never deployed to one or more computer groups.

A block list excludes patches from the results of the sensors **Patch - Patch List Applicability** and **Patch - Patch List Compliance** for any patch list other than **ID 1**. You can still review applicable patch list reports through the patch list **ID 1** or the **Applicable Patches** sensor.

Block patches with the Title containing either "Quality Rollup" or "Security Only" to avoid redundant patch deployments.

1. From the Main menu, go to **Modules > Patch > Block Lists** and then click **Create Block List**.
2. Name the list, select an operating system, and select a content set.
3. Add patches.

Adding patches dynamically	Adding patches manually
a. Superseded patches are automatically included in block lists. b. Click **Add Rule**. c. Name the rule. d. Select a **Condition** and then an **Operator**. e. Type in the expression to search against and then click **Apply**. Searches are case-insensitive.	a. Expand **Add Patches Manually**. b. Select the patches that you want. c. (Optional) Click the patch title to see the details in a new browser tab.  If a patch is known to cause issues for a subset of endpoints, create a block list with the patch KB number and target only the computer group that contains the endpoints that are adversely affected by that patch.

   You can get details about the patch, visibility into the results by computer group, and the associated lists.
4. Preview the changes and then click **Create Block List**.
5. On the Block List Details page, select the targeted computer groups.

The block list is distributed to the selected endpoints, blocking those patches. However, if an endpoint comes online with a blocked patch already installed, the patch remains until it is uninstalled.

`yum.conf` exclusions for Linux endpoints

If a Linux endpoint has excluded packages in the `yum.conf` file, Patch honors those exclusions and will not install them.

© 2026 Tanium Inc. All Rights Reserved

NOTE

Tanium Patch blocking occurs on an Advisory basis. Because a Linux Advisory consists of a list of packages that need to be installed on Linux, a non-blocked Advisory might not be installed if it includes packages that are associated with a blocked Advisory.

Create lists from the Patches view

In addition to creating a list from the Patch Lists or Block Lists page, you can also select individual patches to build lists.

1. From the Main menu, go to **Modules > Patch > Patches**.
2. Select one or more patches.
3. From the **More** dropdown list, select the list type.
4. Complete the list.

View confidence score of Windows patch

You can view the confidence scores of Windows patches. The confidence score rates the probability that a patch deployment will succeed in the future and will not cause post-installation downtime. For more information, see Windows patch confidence score on page 19.

Tanium does not calculate confidence scores for Linux patches. These patches have a confidence score of **N/A**.

NOTE

Confidence score is available only if your Tanium instance is linked to your Tanium Account. For more information, see Tanium Account User Guide: Link an on-premises Tanium instance. It can take up to one hour for confidence scores to appear after linking your account. If you unlink your account, it can take up to five hours for confidence scores to disappear.

NOTE

Confidence score is not available in Tanium Cloud for U.S. Government. For more information, see Patch overview on page 13.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules > Patch > Patches**.
2. Click the patch for which you want to review the confidence score.

Patch confidence score values

Score	Description
High	A score of 80 or higher indicates a patch had positive deployments in the sense of having high installation success and low uninstall rate.
Moderate	A score of 60 to 79 conveys caution because the patch deployments had a moderate number of installation failures and a moderate uninstall rate.
Low	A score of 59 or lower constitutes an alert due to a critical number of installation failures and a critical uninstall rate.
Calculating	The Tanium Server has not yet collected the minimum number of reported outcomes (20) that is required for a valid score.

3. In the **Confidence Score Breakdown** section, review the values for the individual metrics that Tanium uses to calculate the score.



The value of each metric indicates the affected endpoints as a percentage of all the reporting endpoints. **Sample Size** is the number of endpoints included in the **Installation Status** metric. **Uninstall Rate** mentions the number of endpoints included in the metric. The confidence score is the weighted average value of the following metrics:

Patch confidence score metrics

Metric	Description
Installation Status	Percentage of endpoints that successfully deployed the Windows patch in prior deployments.
Uninstall Rate	Percentage of endpoints that have uninstalled the Windows patch after a successful installation.

Edit a list

When a user changes an existing list, the changes become a new version of the list. With some basic changes, such as adding a rule for each new month, you can refine your patch testing and roll up changes without creating a new list.

1. From the Main menu, go to **Modules > Patch** and click **Patch Lists** or **Block Lists**.
2. Click the list name and then click **Edit**.
3. Make your changes.
4. Preview the changes and then click **Update Patch List** or **Update Block List**.

© 2026 Tanium Inc. All Rights Reserved

Check patch visibility

You can get details about the patch, the installation results by computer group, and the associated lists.

1. From the Main menu, go to **Modules > Patch > Patches**. To see only patches that are not installed, click **Applicable** from the **Applicability** section of the **Filters**.
2. Click the patch name.

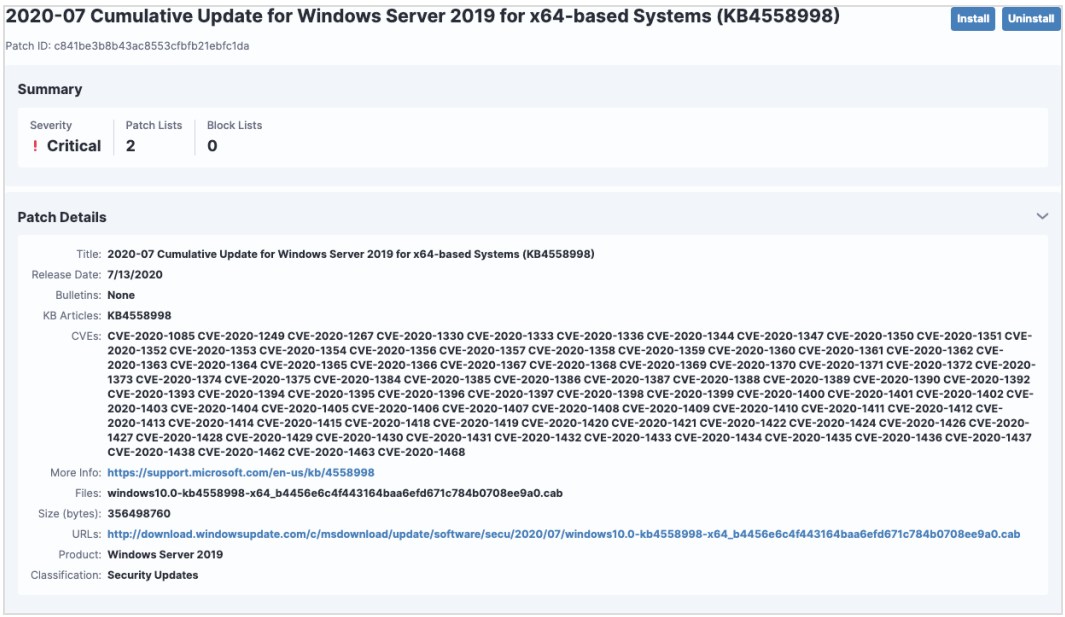
   TIP You can also click Expand next to the patch name to view additional information.

3. Review the sections.

   - **Summary** shows the severity and the associated lists.

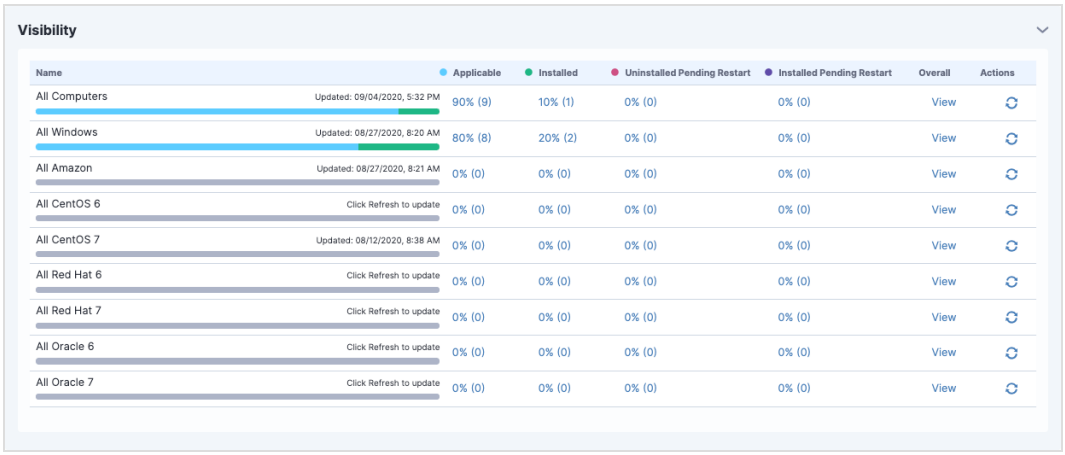
     For patches targeted to endpoints on Windows 11 version 22H2 or later, the summary also shows the UUP synchronization status. For more information, see UUP Synchronization Status.

   - **Patch Details** has the patch title, release date, bulletins, KB articles, CVEs, files, size, URLs, and the product and classification types.

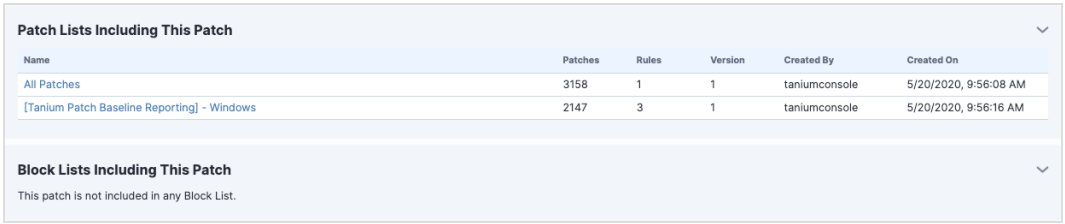


© 2026 Tanium Inc. All Rights Reserved

- **Visibility** splits out the patch results by computer group. To filter the list of computer groups, update the selected computer groups in the **Computer Groups for Patch Visibility** section in the **Configuration Settings** tab of the Patch Settings. Only users with the **Patch Settings write** permission can make changes to the Patch Settings.



- **Patch Lists Including This Patch** and **Block Lists Including This Patch** are summaries that include the number of patches on the list, rules, version, and creation details.



Manually synchronize patches

If you are using Tanium Scan for Windows to deliver cumulative updates to Windows 11 version 22H2 or later endpoints, Tanium must first synchronize the patches to the Tanium Server. If you are using a local WSUS server, the patch files need to be approved on the WSUS server before Tanium can successfully download the necessary files.

1. On the WSUS server, approve the patches that you want to apply to the endpoints.
2. Go to the Patch workbench.
3. Ensure that the manual synchronization option is enabled.
4. Synchronize the patches. Use the Overview page to synchronize all patches at once or use the Patch details page to synchronize a specific patch.

Synchronize patches from the Overview page

Use the Overview page to synchronize all patches that failed.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules > Patch > Overview**.
2. Expand the **UUP Synchronization Management** section and click **Synchronize All Patches** to synchronize all the approved patches to the Tanium Server.
3. Review the status of the patches.

   TIP

   If Tanium encounters any synchronization errors, the errors appear immediately in the **Synchronization Errors** table. You can attempt to resolve issues and retry the failed synchronizations at any time, even if a synchronization is in progress.

   UUP Synchronization Status descriptions

UUP Synchronization Status	Description
Synchronization pending	The next synchronization job is queued.
Synchronization in progress	Patches are synchronizing to the Tanium Server.
Last synchronized on *<date and time>*	Synchronization completed on the specified date and time.
Last synchronized with errors on *<date and time>*	Synchronization failed due to errors downloading patch files or creating packages. Review the errors in the **Synchronization Errors** table.
Job failed: Sync Windows UUP Updates	Synchronization job failed. Click **Retry Job**. If the problem persists, contact Tanium Support.

4. If the **Synchronization Errors** table appears, expand the patches and review the errors. For more information about how to troubleshoot the problems, see Resolve UUP synchronization errors on page 159.
5. If the troubleshooting solution requires you to retry the synchronization, use any of the following methods:
   - In the Actions column, click Retry for the specific patch that you want to synchronize.
   - Select the patches that you want to synchronize and click **Retry** in the grid header.
   - Click **Retry All Failed Patches**.
6. After the synchronization completes successfully, deploy the synchronized patches.

   NOTE

   Do not deploy patches that appear in the **Synchronization Errors** table.

Synchronize a patch from the Patch details page

Use the Patch details page to synchronize a specific patch.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules > Patch> Patches**.
2. Click the name of a UUP patch. UUP patches generally contain the following characteristics:
    - Are Cumulative Updates
    - Are approximately 10GB in size
    - Contain at least one `.wim` file and at least one `.psf` file.
    - Have at least 10 files

    You can click Expand next to the patch name to view additional information.
3. Review the **Summary** section, which shows the UUP synchronization status.

    UUP Synchronization Status descriptions

UUP Synchronization Status	Description
Sync required	Patch not available on Tanium Server. Click **Sync**.
Waiting for sync	The next synchronization job is queued
Synchronization in progress	Patches are synchronizing to Tanium Server.
Sync completed. *<date and time>*	Synchronization completed on the specified date and time.
Sync errors	Synchronization job failed. Review the error details.

4. If the **Sync errors** message appears, review the error details. For more information about how to troubleshoot the problems, see Resolve UUP synchronization errors on page 159.
5. If the troubleshooting solution requires you to retry the synchronization, click **Re-Sync**.
6. After the synchronization completes successfully, deploy the patch.

Copy a patch list

You can copy a patch list to use as a starting point for a new patch list. You cannot copy Tanium Managed patch lists.

1. From the Main menu, go to **Modules > Patch > Patch Lists**.
2. Click the list to copy and click **Save As**.
3. Make any necessary changes, preview the changes, and then click **Create Patch List**.

© 2026 Tanium Inc. All Rights Reserved

Export a list

You can facilitate the migration of patch content by exporting lists. The exported file includes rules manually added patches. This is particularly useful in progressive deployment models where patches must be moved from a testing environment to a production environment.

1. From the Main menu, go to **Modules > Patch** and click **Patch Lists** or **Block Lists**.
2. Click the list name.
3. (Optional) Select the version.
4. Click Options and then click **Export Patch or Block List**.

The JSON file is available in your downloads folder. The file name is the list identifier, the actual list name appears after import.

Import a list

You can import an exported list into a new environment. The import contains the latest version of the list and the version is set to 1 in the new environment.

> NOTE
> You cannot import a list with the same name as an existing list.

1. From the Main menu, go to **Modules > Patch** and click **Patch Lists** or **Block Lists**.

   > IMPORTANT
   > Take care to only import the list as the right type.

2. Click **Import Patch List** or **Import Block List** and then click **Choose File**.
3. Browse to the list in .JSON extension and then click **Import**.

Delete a list

Deleting a list does not delete patches, it only deletes the assembled list and any previous versions.

> NOTE
> Remove computer group enforcements before deleting a block list.

1. From the Main menu, go to **Modules > Patch** and click **Patch Lists** or **Block Lists**.
2. Select the list name.
3. Click Delete.

© 2026 Tanium Inc. All Rights Reserved

Add a custom Patch field

You can add a custom field to your patches based on the KB mapping that you provide in a CSV file. You might use this custom field to override the severity of a patch.

1. From the Main menu, go to **Modules > Patch > Overview**, click Settings  and then click **Custom Field** if needed.
2. Click **Upload CSV** for any of the OS types and add the CSV file.
3. The custom column shows up in your patch list views.

Example CSV

The following example maps the Vendor KB value to a new custom value.

```
KB,IAVM
KB829438,1234-A-0016
KB822362,1234-A-0016
kb828037,1234-A-0017
```

© 2026 Tanium Inc. All Rights Reserved

Deploying patches

Create deployments to download and install Windows and Linux patches on a set of target computers. You can also use deployments to uninstall Windows patches. Deployments can run once, be ongoing to maintain operational hygiene for computers that come online after being offline, or be managed by end users with the End-User Self Service Client application.

BEST PRACTICE

- Use ongoing deployments for general patch management and manual deployments for exigent circumstances.
- Do not stagger deployments in an attempt to distribute the load on your network or Tanium. The more endpoints that are being patched simultaneously, the more efficient Tanium becomes with overall WAN usage. For bandwidth-constrained locations, you can implement site throttles. For more information, see Tanium Console User Guide: Configure site throttles.

BEST PRACTICE

Tanium Automate implements install deployments in playbook steps. You can configure reusable playbooks with various steps and run a playbook multiple times to streamline and simplify your business processes. For more information on building a playbook, see Tanium Automate User Guide: Building playbooks. For more information on the available playbook steps, see Tanium Automate User Guide: Reference: Steps.

Before you begin

- Organize the available patches into lists. For more information, see Create a patch list on page 102.
- If you want to notify the end users of your endpoints about the restarts that occur after patch installations, install the Tanium End-User Notifications solution. For more information, see Tanium End-User Notifications User Guide: Installing End-User Notifications and Endpoint restarts on page 120.

TIP

It is recommended that endpoints have around three to five times more free disk space than the size of the Patch deployment.

Create a deployment template

You can create an install or uninstall deployment template. This template saves basic settings for a deployment that you can issue repeatedly. You can either create a deployment template from the **Deployment Templates** menu item, or you can select an option when you create a deployment to save the options as a template.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules > Patch > Deployment Templates**.
2. Click either **Create Deployment Template > Create Install Template** or **Create Deployment Template > Create Uninstall Template**.
3. Name the deployment template, select an operating system, and select a content set. For more information, see Tanium Console User Guide: Managing content sets.
4. Select deployment options.
   a. Specify a deployment frequency. You can do an ongoing deployment that does not have an end time, a single deployment with a specific start and end time, or a self service deployment to allow end users to manage the deployment in the Self Service Client application.

      NOTE

      After patch installation starts, it continues even if you stop the deployment, the deployment ends, or the maintenance window closes.

      NOTE

      After the deployment ends or the maintenance window closes, restarts do not occur and End-User Notification messages do not appear.

   b. Select **Use endpoint local time** to use the local time on the endpoint for the deployment. If you do not select this option, then you can specify the UTC time when you create a deployment from the template.
   c. If you select an ongoing or single deployment, configure the Self Service settings.
      - **Hide from Self Service Client**: Hide this deployment from the Self Service Client application
      - **Make available before Start Time**: Allow the end user to start this deployment in the Self Service Client application before the scheduled **Start Time** and outside of maintenance windows.
   d. If you want the endpoints to download the patch content before the installation time, select the option for **Download Immediately**.

      BEST PRACTICE

      Select this option for future deployments. If you find that endpoints are not completing patch installations within the specified windows, schedule the deployments even further in advance.

   e. If you select an ongoing or single deployment, you can protect shared resources by selecting **Enabled** for the **Distribute Over Time** option and indicating an amount of time. The value you indicate for **Distribute Over Time** must be less than the deployment duration.

      Distribute Over Time randomizes the deployment start time on each endpoint by an amount of time up to the value configured. This option reduces concurrent consumption of shared compute resources in a virtual environment, network bandwidth on the WSUS server when using **WSUS** scan configuration technique, and network bandwidth on the repository server when using the **Repository Scan** scan configuration technique.

© 2026 Tanium Inc. All Rights Reserved

BEST PRACTICE

Specify a **Distribute Over Time** value that is at least two hours less than the length of the deployment window and any maintenance windows. If the value exceeds deployment and maintenance windows, some endpoints will not be able to run the deployment or will install the patches outside of the maintenance window.

f. If you want to ignore patching restrictions, select **Override Maintenance Windows** or **Override Block Lists**.

g. Select whether to restart the endpoint.

NOTE

Windows endpoints restart when this option is configured, regardless of which patches are installed. Linux endpoints restart only when installing patches that require restart, such as Linux kernel updates.

h. (Windows endpoints only) If you enabled endpoint restarts, you can enable end user notifications about the restarts. Select **Notify User After Deployment Activity** and configure the following settings. For more information, see Endpoint restarts on page 120.

NOTE

For endpoints with multiple users, notifications appear for the user with the lowest active session ID. For example, when two users are logged in at the same time, User1 gets the notification but User2 does not. If User1 logs off and User3 logs in, User2 gets the notification because User2 now has the lowest active session ID.

- (Optional) Configure settings that allow the end user to postpone the restart.
- Specify the **Message Content** that informs the user about the restart.
- (Optional) Select additional languages and provide translated title and body text for endpoints that are configured for other languages. To view the preview in additional languages, toggle the language dropdown list in the preview. You can also use the dropdown list to preview the notification in light or dark theme.

BEST PRACTICE

Ensure that the **Duration of Notification Period** value is less than a few days. To decrease the endpoints missing critical or important patches metric, the optimal value for this setting depends on your patching cycle. For best results, set the **Duration of Notification Period** value to less than three days.

5. Click **Save**.

© 2026 Tanium Inc. All Rights Reserved

Set the default deployment template

The default deployment template is applied when you create new deployments. Importing Patch with automatic configuration creates a default installation deployment template for each supported operating system. You can change the default installation template. After you create an uninstallation deployment template, you can set it as the default template.

1. From the Main menu, go to **Modules > Patch > Deployment Templates**.
2. To set a default deployment template, select a deployment template and then click **Set as Default**.
3. To remove the default designation, select a deployment template and then click **Remove as Default**.

Create a deployment to install patches

BEST PRACTICE

- Use single deployments with a defined start and end time instead of continuously creating new deployments and manually stopping them after the patch window ends.
- Avoid creating multiple deployments with the same patches to the same or overlapping endpoints.
- Start with older patches first.

1. From the Main menu, go to **Modules > Patch > Deployments** and then click **Create Deployment > Create Install Deployment**.

   TIP

   You can also create a deployment from the **Patches** page or from the **Patch Lists** page. From the **Patches** page, select a group of patches and click **Install**; from the **Patch Lists** page, select a patch list and click **Install**. If you use either of these methods to create a deployment, then the patches or patch list that you select will already be populated in the **Deployment Details** section.

2. (Optional) Click **Apply Deployment Template** to select an existing template upon which to base this deployment.
3. In the **Deployment Overview** section, accept the default name or provide a name for the deployment, add an optional description, select an operating system, and select a content set. For more information, see Tanium Console User Guide: Managing content sets.
4. In the **Deployment Details** section, complete the following steps as needed for the operating system of the deployment:
   - (Windows) Add one or more patch lists, including version, or add patches manually. Review the confidence scores for applicable patches. For more information, see Windows patch confidence score on page 19. If you select a patch list or multiple patches, you can view the confidence score of each patch after you select the endpoints to target.

© 2026 Tanium Inc. All Rights Reserved

- (Linux) Select whether you want to **Install All Updates**; **Install All Security Updates**; **Choose Patch List**, including version; or **Manually Select Patches**.

  BEST PRACTICE

  Avoid choosing specific patches based on vulnerability reports. Instead, use dynamic, rule-based patch lists. These lists should be cumulative. For example, do not create any rules that prevent patches that are older than a specific date from being included in a patch list.

  CAUTION

  For deployments to Amazon Linux 2023 endpoints, you can only **Install All Updates** or **Install All Security Updates**. You cannot deploy using the **Choose Patch List** or **Manually Select Patches** options.

5. In the **Endpoints to target** section, add targeting criteria for endpoints.

   Select the following targeting methods and complete the fields as needed:

   - **Computer Groups** provides a list of computer groups. You can later use these groups to refine patch applicability results, as needed.
   - **Question Criteria** filters on all endpoints with a specific set of criteria and within the limiting groups selected from the list of available groups. Limiting groups are available after you add question criteria. For example, you can type `Operating System contains win` in the **Filter Bar** or use the **Filter Builder** to target all Windows endpoints within those groups. The deployment is applied to all endpoints that meet the criteria. Individual rows cannot be selected. If you define multiple limiting groups, they are evaluated with an `OR` operator.
   - **Computer Names** lets you use exact names, such as the fully qualified domain name (FQDN) registered with Tanium. Use the **Manual Names** field to manually type in computer names, separated by commas. To upload as a CSV file, click **Names by CSV File** and then click **Upload Names**. Then filter within the limiting groups selected from the list of available groups. Limiting groups are available after you add computer names.

     BEST PRACTICE

     Target fewer than 100 computer names to reduce the impact on the **All Computers** group.

6. Review the **Deployment type and schedule** section and click Edit to make changes as needed.

   a. Specify a deployment frequency. You can do an ongoing deployment that does not have an end time, a single deployment with a specific start and end time, or a self service deployment to allow end users to manage the deployment in the Self Service Client application.

      NOTE

      After patch installation starts, it continues even if you stop the deployment, the deployment ends, or the maintenance window closes.

© 2026 Tanium Inc. All Rights Reserved

> NOTE
>
> After the deployment ends or the maintenance window closes, restarts do not occur and End-User Notification messages do not appear.

b. Designate the deployment time zone.

   Choose the local time on the endpoint or UTC time.

c. Specify the window of time during which the deployment will be effective.

d. If you select an ongoing or single deployment, you can protect shared resources by selecting **Enabled** for the **Distribute Over Time** option and indicating an amount of time. The value you indicate for **Distribute Over Time** must be less than the deployment duration.

   Distribute Over Time randomizes the deployment start time on each endpoint by an amount of time up to the value configured. This option reduces concurrent consumption of shared compute resources in a virtual environment, network bandwidth on the WSUS server when using **WSUS** scan configuration technique, and network bandwidth on the repository server when using the **Repository Scan** scan configuration technique.

   > BEST PRACTICE
   >
   > Specify a **Distribute Over Time** value that is at least two hours less than the length of the deployment window and any maintenance windows. If the value exceeds deployment and maintenance windows, some endpoints will not be able to run the deployment or will install the patches outside of the maintenance window.

e. If you want the endpoints to download the patch content before the installation time, select the option for **Download Immediately**.

   > BEST PRACTICE
   >
   > Select this option for future deployments. If you find that endpoints are not completing patch installations within the specified windows, schedule the deployments even further in advance.

   > TIP
   >
   > To schedule a download time, leave this option cleared and create a maintenance window after the start time for this deployment. With this configuration, endpoints begin downloading software at the start time for the deployment and begin installing downloaded software at the start time for the maintenance window.

f. If you want to ignore patching restrictions, select **Override Maintenance Windows** or **Override Block Lists**.

g. If you select an ongoing or single deployment, configure the End-User Self Service settings.

   - **Hide from Self Service Client**: Hide this deployment from the Self Service Client application
   - **Make available before Start Time**: Allow the end user to start this deployment in the Self Service Client application before the scheduled **Start Time** and outside of maintenance windows.

© 2026 Tanium Inc. All Rights Reserved

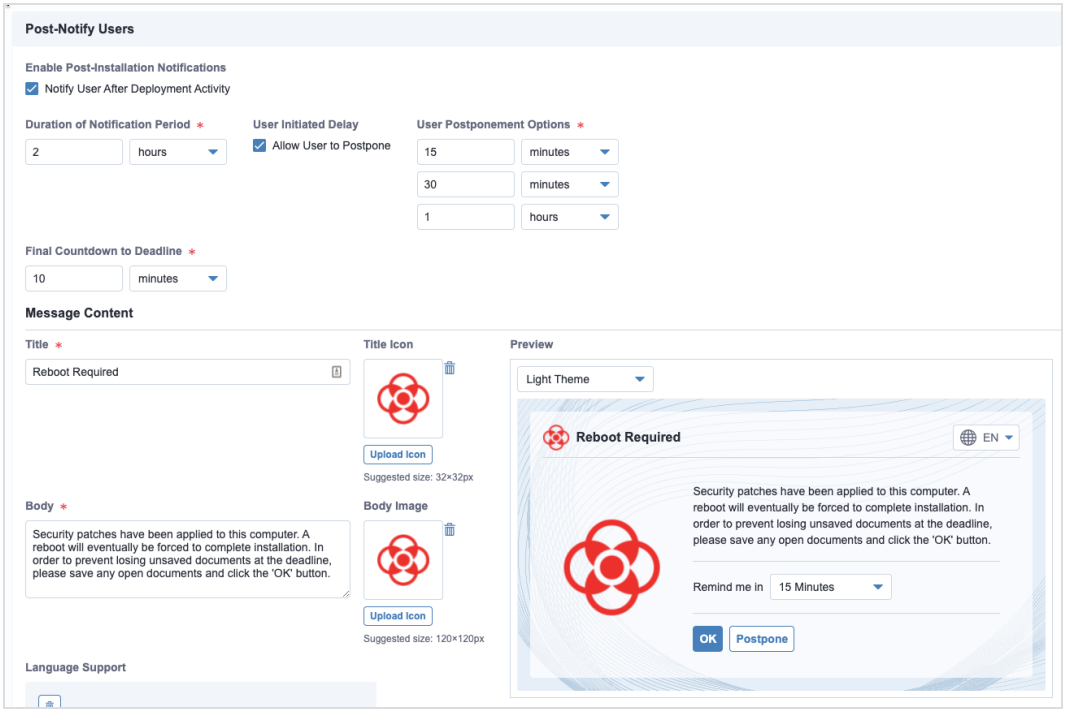
h. Select whether to restart the endpoint.

> **NOTE** Windows endpoints restart when this option is configured, regardless of which patches are installed. Linux endpoints restart only when installing patches that require restart, such as Linux kernel updates.

7. (Windows endpoints) If you enabled endpoint restarts, you can enable end user notifications about the restarts. If necessary, click Edit and then select **Notify User After Deployment Activity** to configure the following settings. For more information, see Endpoint restarts on page 120.

> **NOTE** For endpoints with multiple users, notifications appear for the user with the lowest active session ID. For example, when two users are logged in at the same time, User1 gets the notification but User2 does not. If User1 logs off and User3 logs in, User2 gets the notification because User2 now has the lowest active session ID.

   - (Optional) Configure settings that allow the end user to postpone the restart.
   - Specify the **Message Content** that informs the user about the restart.
   - (Optional) Select additional languages and provide translated title and body text for endpoints that are configured for other languages. To view the preview in additional languages, toggle the language drop-down menu in the preview. You can also use the drop-down menu to preview the notification in light or dark theme.



© 2026 Tanium Inc. All Rights Reserved

BEST PRACTICE

Ensure that the **Duration of Notification Period** value is less than a few days. To decrease the endpoints missing critical or important patches metric, the optimal value for this setting depends on your patching cycle. For best results, set the **Duration of Notification Period** value to less than three days.

8. (Optional) To create a new template based on this deployment, click **Save Settings as New Template**, specify a name for the template, and then click **Save**. For more information, see Create a deployment template on page 113.
9. Click **Preview to Continue**.
10. Review the deployment details for the applicable patches, and then click **Deploy**.

To change the number of retries for each phase of a deployment, see Adjust the deployment retries on page 127.

Endpoint restarts

Patch can trigger a restart of any system after updates have been installed. You can choose between the following options for the restart:

- (Windows and Linux endpoints) Restart silently and immediately after deployment. This option is typically used for servers and production machines in conjunction with maintenance windows and change control processes.
- (Windows endpoints) Notify the system user about the pending restart and give the system user the option to hide the notification for a specified amount of time. Configure the following options:

  Final Countdown to Deadline

  Specify the amount of time in minutes, hours, or days to show the final notification before restarting the endpoint. This notification also shows a countdown until restart. If end users dismiss the notification and a restart is required, the notification will reappear in the last minute of the final countdown to deadline before the computer restarts. Set a low value because this option is meant to signal a forced restart that cannot be postponed.

  Allow User to Postpone

  If you want to give the user an option to hide the notification for a specified amount of time, select this option. A user cannot postpone beyond the deadline.

  Duration of Notification Period

  Specify the amount of time in minutes, hours, or days before the endpoint must be restarted. The deadline is calculated by adding this value to the time the deployment completed for each endpoint.

  User Postponement Options

  Specify the amount of time in minutes, hours, or days that a user can hide the notification.

  Appearance

  Specify the appearance of the notification. **Allow user to minimize** displays the notification with a title bar that includes the minimize option. **Do not allow user to minimize** displays the notification without a title bar. **Do not allow user to minimize** is the default.

© 2026 Tanium Inc. All Rights Reserved

Message Content

Specify the title and body of the notification message. Upload optional icon and body images for branding to avoid confusing users and to limit support calls. Enable additional languages and provide translated title and body text. By default, the notification displays content in the system language on the endpoints. If you enable additional languages, the user can select other languages to display.

Show Countdown

Select this option to show the final countdown to deadline in the preview. You can use the slider to adjust the time remaining in the countdown.

End user notifications can be added to existing deployments by stopping, reconfiguring, and reissuing the deployment.



If your deployment is configured for a notification, but the endpoint does NOT have the End User Notifications Tools installed, the endpoint installs the updates, but does NOT restart. A status message is displayed in the Patch workbench about the missing tools.



If no user is logged into an endpoint, the endpoint restarts immediately after a deployment completion even if the deployment is configured for a notification.

Create a deployment to install patches on a single endpoint

You can quickly create a deployment to install patches on a single endpoint through the Endpoint Details page in Tanium Reporting. To create a deployment, you must have the **Patch Deployment write** permission.



You can also install a patch on a single endpoint by following the steps in Create a deployment to install patches on page 116.

1. Open the Endpoint Details page for the endpoint that requires a deployment. For more information, see Tanium Reporting User Guide: View endpoint details.
2. Select the **Endpoint Management** tab.
3. In the **OS Patch Applicability** section, select up to 50 patches, click **Install**, and complete the deployment.

© 2026 Tanium Inc. All Rights Reserved

Windows: Create a deployment to uninstall patches

You can uninstall patches that appear in scan results; however, operating system limitations prevent some patches from being uninstalled.

1. From the Main menu, go to **Modules > Patch > Deployments** and then click **Create Deployment > Create Uninstall Deployment**.
2. (Optional) Click **Apply Deployment Template** to select an existing template upon which to base this deployment.
3. Review the **Deployment Overview** section and click Edit to make changes as needed. Accept the default name or provide a name for the deployment, add an optional description, and select a content set. For more information, see Tanium Console User Guide: Managing content sets.
4. In the **Content to deploy** section, expand the **Add Patches Manually** section and add one or more patches. Review the confidence scores for applicable patches. For more information, see Windows patch confidence score on page 19. If you select a patch list or multiple patches, you can view the confidence score of each patch after you select the endpoints to target.

   NOTE

   The applicability count in the grid is for endpoints that do not have the patch installed.

5. In the **Endpoints to target** section, add targeting criteria for endpoints.
   Select the following targeting methods and complete the fields as needed:

   - **Computer Groups** provides a list of computer groups. You can later use these groups to refine patch applicability results, as needed.
   - **Question Criteria** filters on all endpoints with a specific set of criteria and within the limiting groups selected from the list of available groups. Limiting groups are available after you add question criteria. For example, you can type `Operating System contains win` in the **Filter Bar** or use the **Filter Builder** to target all Windows endpoints within those groups. The deployment is applied to all endpoints that meet the criteria. Individual rows cannot be selected. If you define multiple limiting groups, they are evaluated with an `OR` operator.
   - **Computer Names** lets you use exact names, such as the fully qualified domain name (FQDN) registered with Tanium. Use the **Manual Names** field to manually type in computer names, separated by commas. To upload as a CSV file, click **Names by CSV File** and then click **Upload Names**. Then filter within the limiting groups selected from the list of available groups. Limiting groups are available after you add computer names.

     BEST PRACTICE

     Target fewer than 100 computer names to reduce the impact on the **All Computers** group.

6. Review the **Deployment type and schedule** section and click Edit to make changes as needed.

   a. Specify a deployment frequency. You can do an ongoing deployment that does not have an end time, a single deployment with a specific start and end time, or a self service deployment to allow end users to manage the deployment in the Self Service Client application.

© 2026 Tanium Inc. All Rights Reserved

> **NOTE** After patch uninstallation starts, it continues even if you stop the deployment, the deployment ends, or the maintenance window closes.

> **NOTE** After the deployment ends or the maintenance window closes, restarts do not occur and End-User Notification messages do not appear.

b. Designate the deployment time zone.

   Choose the local time on the endpoint or UTC time.

c. Specify the window of time during which the deployment will be effective.

d. If you select an ongoing or single deployment, you can protect shared resources by selecting **Enabled** for the **Distribute Over Time** option and indicating an amount of time. The value you indicate for **Distribute Over Time** must be less than the deployment duration.

   Distribute Over Time randomizes the deployment start time on each endpoint by an amount of time up to the value configured. This option reduces concurrent consumption of shared compute resources in a virtual environment, network bandwidth on the WSUS server when using **WSUS** scan configuration technique, and network bandwidth on the repository server when using the **Repository Scan** scan configuration technique.

> **BEST PRACTICE** Specify a **Distribute Over Time** value that is at least two hours less than the length of the deployment window and any maintenance windows. If the value exceeds deployment and maintenance windows, some endpoints will not be able to run the deployment or will install the patches outside of the maintenance window.

e. If you want the endpoints to download the patch content before the deployment start time, select the option for **Download Immediately**.

> **BEST PRACTICE** Select this option for future deployments. If you find that endpoints are not completing patch installations within the specified windows, schedule the deployments even further in advance.

f. If you want to ignore patching restrictions, select **Override Maintenance Windows** or **Override Block Lists**.

g. If you select an ongoing or single deployment, configure the End-User Self Service settings.

   - **Hide from Self Service Client**: Hide this deployment from the Self Service Client application
   - **Make available before Start Time**: Allow the end user to start this deployment in the Self Service Client application before the scheduled **Start Time** and outside of maintenance windows.

© 2026 Tanium Inc. All Rights Reserved

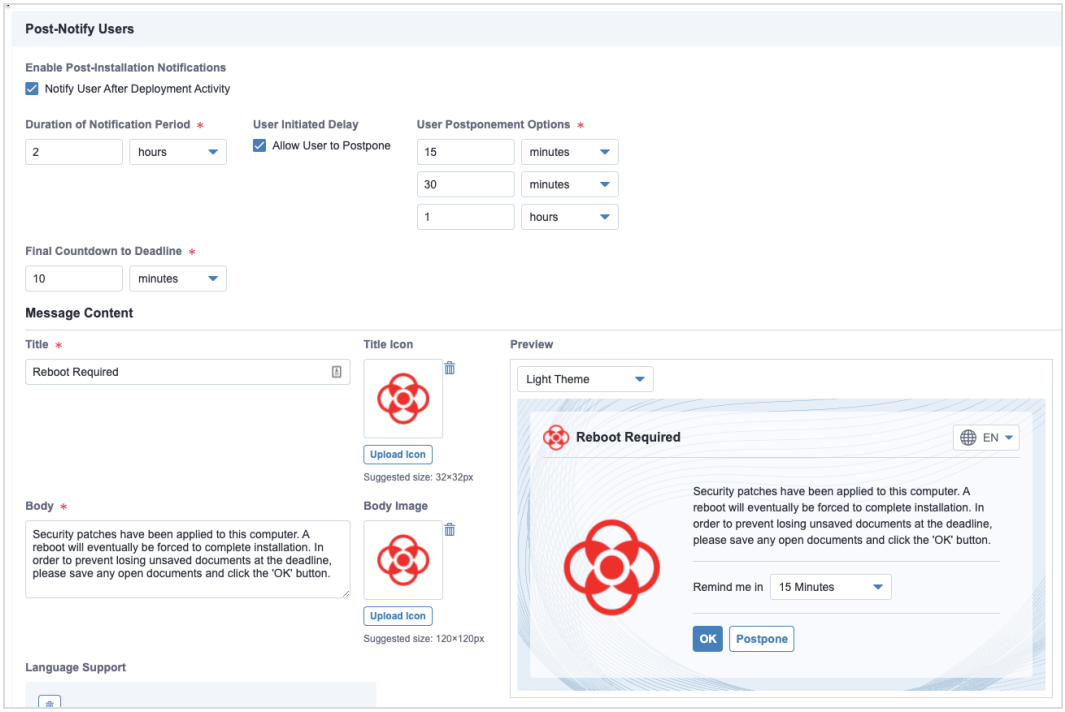
h. Select whether to restart the endpoint.

> NOTE
>
> Linux endpoints will restart only when patches that require restart are installed.

7. (Windows endpoints) If you enabled endpoint restarts, you can enable end user notifications about the restarts. If necessary, click Edit and then select **Notify User After Deployment Activity** to configure the following settings. For more information, see Endpoint restarts on page 120.

> NOTE
>
> For endpoints with multiple users, notifications appear for the user with the lowest active session ID. For example, when two users are logged in at the same time, User1 gets the notification but User2 does not. If User1 logs off and User3 logs in, User2 gets the notification because User2 now has the lowest active session ID.

- (Optional) Configure settings that allow the end user to postpone the restart.
- Specify the **Message Content** that informs the user about the restart.
- (Optional) Select additional languages and provide translated title and body text for endpoints that are configured for other languages. To view the preview in additional languages, toggle the language drop-down menu in the preview. You can also use the drop-down menu to preview the notification in light or dark theme.



© 2026 Tanium Inc. All Rights Reserved

BEST PRACTICE

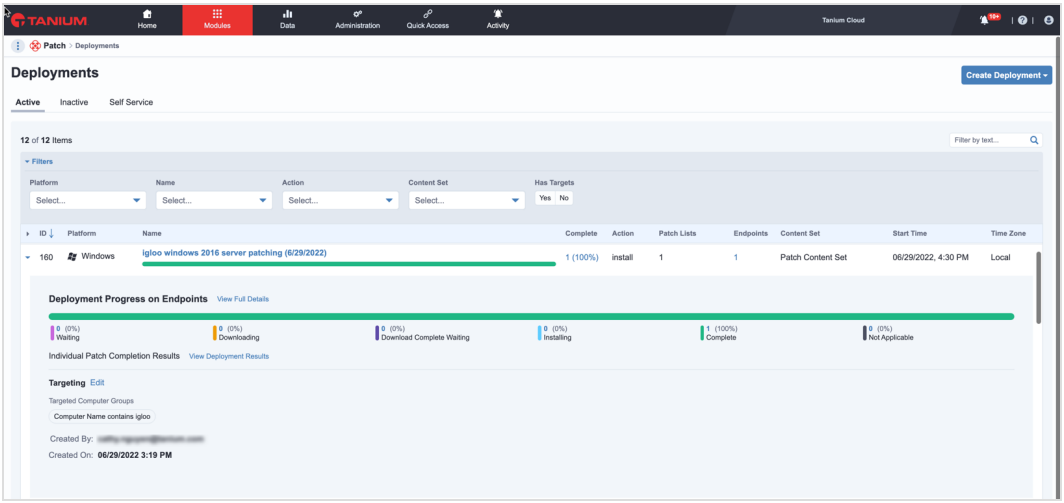
Ensure that the **Duration of Notification Period** value is less than a few days. To decrease the endpoints missing critical or important patches metric, the optimal value for this setting depends on your patching cycle. For best results, set the **Duration of Notification Period** value to less than three days.

8. (Optional) To create a new deployment template based on this template, click **Save Settings as New Template**, specify a name for the template, and then click **Save**. For more information, see Create a deployment template on page 113.
9. Click **Preview to Continue**.
10. Review the deployment details for the applicable patches, and then click **Deploy**.

Review deployment summary

You can get the deployment results by status, any error messages, and the deployment configuration details.

1. From the Main menu, go to **Modules > Patch > Deployments**.
2. Select the **Active**, **Inactive**, or **Self Service** tab.
   Expand the sections to see summary information about the deployment, such as targeted groups and schedule.



3. Click the deployment name. The **Status** section shows the status and substatus, links to deployment results, OS, online endpoints, information about the last time the status or initialization was updated, and any error messages.
4. In the Deployment Details area, expand the section you want to see, or click **Expand All** to expand all sections.
   - **Content to deploy** provides all the configuration information, including installation details, execution information, installation workflow and notifications, patch lists, patches, and confidence score.
   - **Endpoints to target** lists the targeted endpoints for the deployment.
   - **Deployment type and schedule** shows the deployment frequency, time zone, and schedule.
   - **User notifications** has the information about any end user notifications associated with the deployment.

© 2026 Tanium Inc. All Rights Reserved

Add targets to an existing deployment

You can add more targets to a deployment. For example, you can limit patch testing to a select computer group and then roll it out to more groups after it has been validated. All other deployment options remain the same and deployment results from the previous installation deployments are preserved.

1. From the Main menu, go to **Modules > Patch > Deployments**.
2. Click the deployment name and then click **Edit**.
3. In the **Endpoints to target** section, click **Computer Groups**, **Question Criteria**, or **Computer Names**.

   IMPORTANT

   You cannot remove targets from active deployments. To remove a target from a deployment, you must stop the deployment and create a new deployment without that target.

4. Click **Preview to Continue**.
5. Review the deployment details, and then click **Deploy**.

Stop a deployment

You can stop a patch deployment. Stopping changes the deployment end time to now. It does not remove patches that have already completed installation.

1. From the Main menu, go to **Modules > Patch > Deployments**.
2. Click the deployment name and then click **Stop**.
3. Go to the **Inactive** tab and click the deployment name to verify the status.

Reissue a deployment

You can restart a stopped deployment or reissue a one-time deployment. Reissuing a deployment creates a new deployment with the same configuration and targets.

1. From the Main menu, go to **Modules > Patch > Deployments** and then click **Inactive**.
2. Click the deployment name and then click **Reissue**.
3. (Optional) Make any necessary changes.
4. Click **Preview to Continue**.
5. Review the deployment details, and then click **Deploy**.

© 2026 Tanium Inc. All Rights Reserved

Delete old inactive deployments

You can delete stopped or ended deployments that are older than a specified interval to help improve the performance of the Patch workbench.

1. From the Main menu, go to **Modules > Patch > Overview**, click Settings and then click **Configuration Settings** if needed.
2. In the **Inactive Deployment Removal Settings** section, select **Enable Inactive Deployments Removal**.
3. In the **Inactive Deployment Removal Frequency** field, enter the number of days and then click **Save**. The minimum is 30 days. The maximum and default is 180 days.

Adjust the deployment retries

You can change how many times Patch attempts a deployment status within a specified time period. For example, with the default of five retries and 24 hours, Patch tries to download patches five times before stopping for 24 hours. Patch then tries again five times in the next 24 hours, as long as there is an active or ongoing deployment and an active maintenance window.

> NOTE
>
> When you adjust the **Deployment Retry Settings**, Patch applies the new values to new deployments. To apply the new values to an existing deployment, re-create the deployment.

1. From the Main menu, go to **Modules > Patch > Overview**, click Settings and then click **Configuration Settings** if needed.
2. In the **Deployment Retry Settings** section, select the number of retries from the **Retry Limit** dropdown list.
3. In the **Reset Frequency** field, type in the number of hours and then click **Save**.

Reference: Patch status

Deployment status

The following is a list of all possible deployment status groups and the sub-statuses.

If there has been more than one attempt, the status might be appended with `- Retry #`, for example `Downloading - Retry 2`. For more information on retries, see Adjust the deployment retries on page 127.

© 2026 Tanium Inc. All Rights Reserved

Status group	Sub-status
Needs Attention	• Complete, Missing Download URLs • Complete, Some Patches Applied (if you have exhausted your retries) • Complete, Some Patches Removed (if you have exhausted your retries) • Download Complete, Waiting for Block List Configuration File • Download Complete, Waiting for Maintenance Window Configuration File • Download Failed, Download retry limit exceeded • Error, No Patches Removed • Error, Install Aborted • Error, Uninstall Aborted • Error, Deployment Ended Before Any Action Was Taken • Error, No Patches Applied • Has Scan Errors • Missing Scan Results • Pending Restart, End-User Notification Unsupported • Pending Restart, Missing End-User Notification Tools • Pending Restart, Waiting for Maintenance Window Configuration File • Stale Scan Results (results older than three days) • Unable to Download • Waiting for Deployment Configuration File • Waiting for Scan Configuration File • Waiting for Block List Configuration File
Waiting	• Waiting for Deployment Start Time • Waiting for Maintenance Window • Waiting for User Input • Waiting for Required UUP Metadata

© 2026 Tanium Inc. All Rights Reserved

Status group	Sub-status
Downloading	• Downloading
Download Complete Waiting	• Download Complete, Waiting for Deployment Start Time • Download Complete, Waiting for Maintenance Window • Download Complete, Waiting for User Input
Installing	• Pre-Install Random Delay • Pre-Install Scan • Installing • Post-Install Scan
Uninstalling	• Pre-Uninstall Random Delay • Uninstalling • Pending Restart, Waiting for Maintenance Window • Post-Uninstall Scan
Pending Restart	• Pending Restart, Awaiting User Acceptance (this includes user has postponed)[3] • Pending Restart, Restart Required to Complete the Install • Pending Restart, Waiting for Maintenance Window
Complete	• Complete, All Patches Applied • Complete, All Patches Removed
Not Applicable	• Not Applicable[1,2] • Not Targeted[2] • Deployment Configuration File Received (applicability has not yet been determined) • Not Applicable, No longer targeted

[1] Windows endpoints return deployment statuses only for targeted endpoints. If a Windows endpoint returns the `Not Applicable` status, then the deployment is targeted to the endpoint and has no applicable patches.

[2] Linux endpoints return the `Not Applicable` status when the deployment has no applicable patches for that endpoint. If a Linux endpoint returns the `Not Targeted` status, then the endpoint is not targeted by the deployment.

© 2026 Tanium Inc. All Rights Reserved

Enforcement status

Status group	Sub-status
Block lists and maintenance windows	• Enforced • Unenforced
Scan configurations	• Unenforced • Waiting For Initial Scan • Complete, Waiting For Next Scan • Downloading • Scanning

© 2026 Tanium Inc. All Rights Reserved

Setting maintenance windows

Maintenance windows control when Windows and Linux patches can be applied to a computer group. A maintenance window is separate from the deployment start and end time. After a maintenance window is applied to an endpoint, that endpoint does not install patches or restart to complete patch installation, unless it is currently in an open maintenance window. To install a patch, the maintenance window must be open during the configured deployment time.

Maintenance windows do not control when endpoints download patch content. Endpoints start downloading patch content based on the settings in the Patch deployment. For more information, see the Download Immediately option.

A maintenance window is different from a scan window. For more information about limiting scan activity to a designated scan window, see Scan windows on page 96.



If endpoints do not have a maintenance window assigned, you might unintentionally install patches on those endpoints when there is an active deployment. To prevent endpoints from being patched accidentally, you can set a blocking maintenance window that never occurs for the computer group that contains the endpoints. To set a blocking maintenance window, create a maintenance window that does not repeat, with start and end dates in the past. With the blocking maintenance window in place, the endpoint computer group will be patched only during active maintenance windows. This type of setup is useful if you want to prevent servers from being patched on the same schedule as end-user machines. For more information about the different options available to prevent server patching, see Improve Your Automated Patch Workflow: Preventing Server Patching.



Ensure that maintenance windows are at least four hours long, repeat at least once each month, and properly overlap with deployment times and change control process timelines.

Maintenance window options

You can configure maintenance windows for the times that are best for your environment. Apply maintenance windows by enforcing them against computer groups. Multiple maintenance windows can affect a computer group, creating several times that patch activity is permitted.

If you want . . .	After the date and time, select . . .
A one-time window	**Does Not Repeat**
A window that repeats every few days	**Daily** and the number of days between windows
A window that repeats on the same days of the week	**Weekly**, the number of weeks between windows, and which days of the week it opens on

© 2026 Tanium Inc. All Rights Reserved

If you want . . .	After the date and time, select . . .
A window that repeats on the same date each month	**Monthly**, the number of months between windows, and **Day of the Month**
A window that repeats on the same day each month	**Monthly**, the number of months between windows, and **Day of the Week**
A window that repeats relative to a specified day each month For example, a window that repeats three days after the second Tuesday of each month	**Monthly, relative to another day**, the week number (for example, second), the day of the week, **+** or **-**, and the number of days offset from the specified day
A window that repeats on the same day of the year	**Yearly** and the number of years between windows



If a maintenance window does not repeat and it is the only one enforced against a computer group, patches cannot be applied after the window closes. However, if endpoints do not have a maintenance window assigned, you might unintentionally install patches on those endpoints when there is an active deployment. To prevent accidental patching, you can apply a blocking maintenance window to a computer group.

Create a maintenance window

You can open multiple maintenance windows to customize when patches are applied to your endpoints. For example, you can create windows that allow deployments to install patches during periods of low network activity or outside of core working hours.

1. From the Main menu, go to **Modules > Patch > Maintenance Windows** and then click **Create Window**.
2. Set the windows details: **Name**, **Description**, **Operating System**, and Content set.
3. Configure the window options.
    - (Optional) **Recurrence**: Select a recurrence time frame. If you chose a repeating window, set additional options, such as **Frequency**, **Days of the week**, or **Day of the month**. The additional options appear dynamically based on your Recurrence selection. For more information, see Maintenance window options on page 131.
    - **Window Time**: Choose from endpoint local time or UTC time.
    - **Effective Date and Start Time**: Use the date and time pickers to set the maintenance window start time.



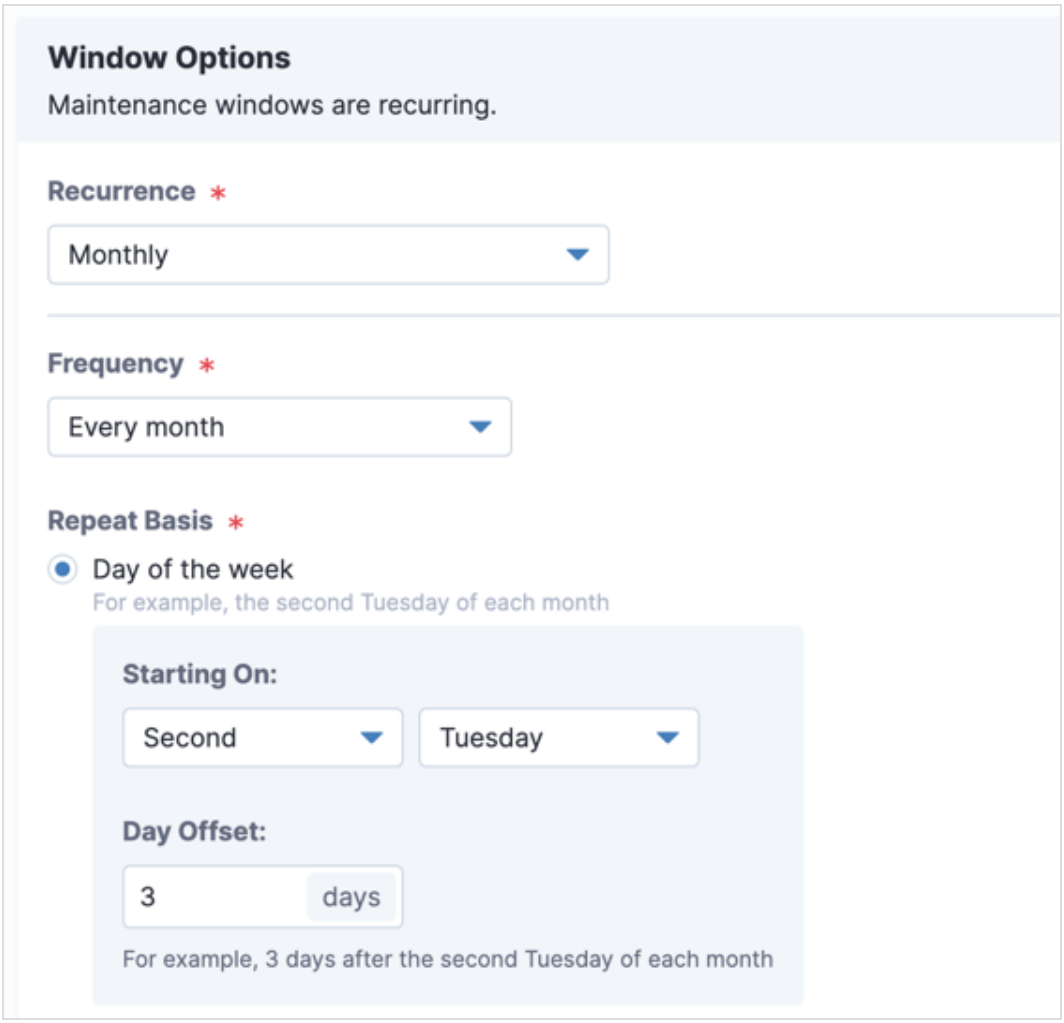
If you are using the **Monthly, Day of the week** frequency, select a start date that is at least one day in the future. A **Monthly, Day of the week** maintenance window cannot be enforced on the same day that it is created because some endpoints may have already passed the start time, depending on endpoint time. Review the **Next 5 Instances** before continuing.

© 2026 Tanium Inc. All Rights Reserved

> NOTE
>
> Repeating maintenance windows do not have an end date. You must remove the enforcement against the target computer groups to stop the maintenance window.

- **End Time**: (Non-repeating windows) Use the date and time pickers to set the window end time.
- **Duration**: (Repeating windows) Set the duration of the window.

For example, to account for Patch Tuesday, you could use these settings for three days after patch updates are typically released by Microsoft.



4. Click **Create Window**. Review any informational messages that appear and perform any updates that are necessary to the maintenance window. Click **Create Window**.
5. Add one or more target computer groups. Maintenance windows can only target management-rights enabled computer groups. Filter groups and targeting filters are not supported. If you add more than one computer group, the computer groups are joined by an OR operator. Click **Save**.

© 2026 Tanium Inc. All Rights Reserved

NOTE

Maintenance window computer groups must be assigned RBAC permissions for the user or group to appear in the list. For more information, see Tanium Console User Guide: RBAC overview.

Edit a maintenance window

1. From the Main menu, go to **Modules > Patch > Maintenance Windows**.
2. Click the name of a window and click **Edit**.
3. Make your changes and click **Update Window**.

Override a maintenance window

You can apply a patch outside of a maintenance window by configuring the **Override Maintenance Windows** option during a patch deployment. For more information, see Deploying patches on page 113. Note that if you also choose to restart the endpoint in the deployment options, the endpoint restarts immediately after the patch is installed.

Delete a maintenance window

After the enforcements have been removed, you can delete a maintenance window.

1. From the Main menu, go to **Modules > Patch > Maintenance Windows**.
2. Click the name of a window.
3. If the window is enforced against computer groups, remove all groups.
4. Click Delete .

© 2026 Tanium Inc. All Rights Reserved

Managing End-User Self Service for Windows endpoints

With the Self Service Client application, you can publish patches to Windows endpoints so that users can start a patch deployment early or completely control when patches are installed. For example, you might deploy the Self Service Client application to a manufacturing endpoint that can be patched only between manufacturing runs or an endpoint in an operating room that must be patched between surgeries. To use the Self Service Client application on your Windows endpoints, you must create a self service deployment in Patch version 3.12 or later.

Before you begin

Create an End-User Notifications configuration that enables End-User Self Service and specifies other options, such as logo, title, greeting text, additional language support, and shortcut options. For more information, see End-User Notifications User Guide: Customizing the End-User Self Service interface.

Create a Self Service deployment to install patches

1. From the Main menu, go to **Modules > Patch > Deployments** and click **Create Deployment > Create Install Deployment**.
2. In the **Deployment Overview** section, accept the default name or provide a name for the deployment, add an optional description, select the **Windows** platform, and select a content set. For more information, see Tanium Console User Guide: Managing content sets.
3. In the **Deployment Details** section, add one or more patch lists, including version, or add patches manually. Review the confidence scores for applicable patches. For more information on confidence scores for Windows patches, see Windows patch confidence score on page 19. If you select a patch list or multiple patches, you can view the confidence score of each patch after you select the endpoints to target.
4. In the **Endpoints to target** section, add targeting criteria for endpoints.
   Select the following targeting methods and complete the fields as needed:
   - **Computer Groups** provides a list of computer groups. You can later use these groups to refine patch applicability results, as needed.
   - **Question Criteria** filters on all endpoints with a specific set of criteria and within the limiting groups selected from the list of available groups. Limiting groups are available after you add question criteria. For example, you can type `Operating System contains win` in the **Filter Bar** or use the **Filter Builder** to target all Windows endpoints within those groups. The deployment is applied to all endpoints that meet the criteria. Individual rows cannot be selected. If you define multiple limiting groups, they are evaluated with an `OR` operator.
   - **Computer Names** lets you use exact names, such as the fully qualified domain name (FQDN) registered with Tanium. Use the **Manual Names** field to manually type in computer names, separated by commas. To upload as a CSV file, click **Names by CSV File** and then click **Upload Names**. Then filter within the limiting groups selected from the list of

© 2026 Tanium Inc. All Rights Reserved

available groups. Limiting groups are available after you add computer names.



Target fewer than 100 computer names to reduce the impact on the **All Computers** group.

5. In the **Deployment type and schedule** section, click Edit to make changes as needed.

   a. Select the **Self Service** deployment type.

   b. If you want the endpoints to download the patch content before the installation time, select the option for **Download Immediately**.



Select this option for future deployments. If you find that endpoints are not completing patch installations within the specified windows, schedule the deployments even further in advance.

   c. If you want to ignore patching restrictions, select **Override Block Lists**.

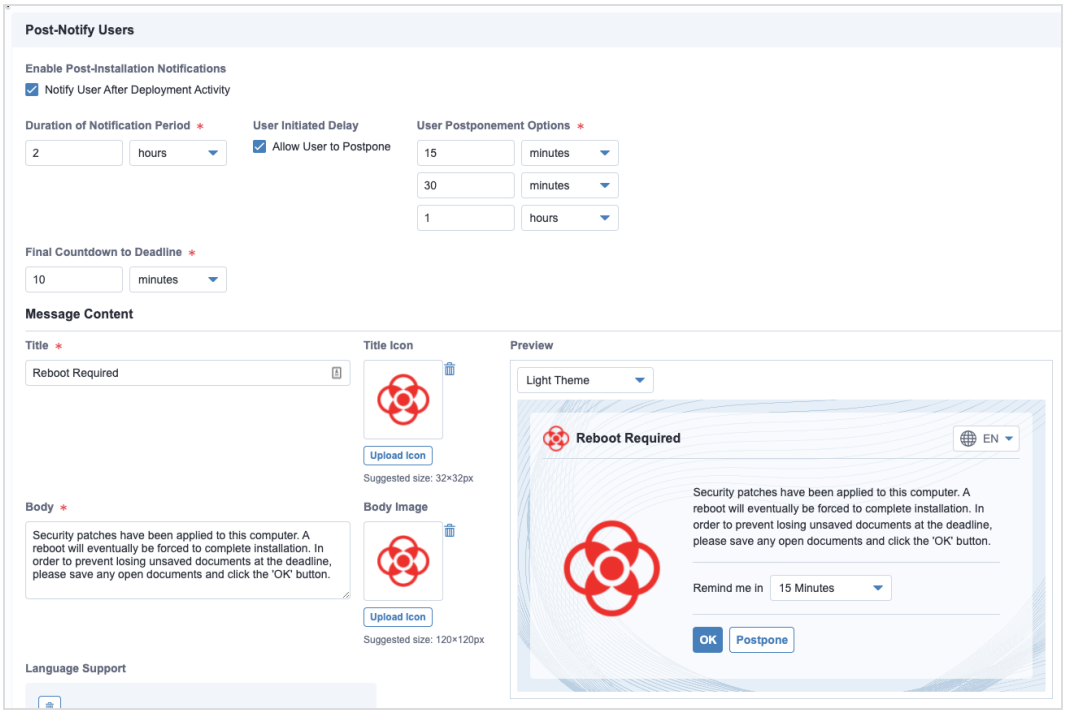
   d. Select whether to restart the endpoint.

6. If you enabled endpoint restarts, you can enable end user notifications about the restarts. If necessary, click Edit and then select **Notify User After Deployment Activity** to configure the following settings. For more information, see Endpoint restarts on page 120.

   - (Optional) Configure settings that allow the end user to postpone the restart.
   - Specify the **Message Content** that informs the user about the restart.

© 2026 Tanium Inc. All Rights Reserved

- (Optional) Select additional languages and provide translated title and body text for endpoints that are configured for other languages. To view the preview in additional languages, toggle the language dropdown list in the preview. You can also use the dropdown list to preview the notification in light or dark theme.



BEST PRACTICE

Ensure that the **Duration of Notification Period** value is less than a few days. To decrease the endpoints missing critical or important patches metric, the optimal value for this setting depends on your patching cycle. For best results, set the **Duration of Notification Period** value to less than three days.

7. Click **Preview to Continue**.
8. Review the deployment details, and then click **Deploy**.

Create a Self Service deployment to uninstall patches

1. From the Main menu, go to **Modules > Patch > Deployments** and then click **Create Deployment > Create Uninstall Deployment**.
2. Review the **Deployment Overview** section and click Edit to make changes as needed. Accept the default name or provide a name for the deployment, add an optional description, select the **Windows** platform, and select a content set. For more information, see Tanium Console User Guide: Managing content sets.

© 2026 Tanium Inc. All Rights Reserved

3. In the **Content to deploy** section, expand the **Add Patches Manually** section and add one or more patches. For more information on confidence scores for Windows patches, see Windows patch confidence score on page 19.

   NOTE

   The applicability count in the grid is for endpoints that do not have the patch installed.

4. In the **Endpoints to target** section, add targeting criteria for endpoints.
   Select the following targeting methods and complete the fields as needed:

   - **Computer Groups** provides a list of computer groups. You can later use these groups to refine patch applicability results, as needed.
   - **Question Criteria** filters on all endpoints with a specific set of criteria and within the limiting groups selected from the list of available groups. Limiting groups are available after you add question criteria. For example, you can type `Operating System contains win` in the **Filter Bar** or use the **Filter Builder** to target all Windows endpoints within those groups. The deployment is applied to all endpoints that meet the criteria. Individual rows cannot be selected. If you define multiple limiting groups, they are evaluated with an `OR` operator.
   - **Computer Names** lets you use exact names, such as the fully qualified domain name (FQDN) registered with Tanium. Use the **Manual Names** field to manually type in computer names, separated by commas. To upload as a CSV file, click **Names by CSV File** and then click **Upload Names**. Then filter within the limiting groups selected from the list of available groups. Limiting groups are available after you add computer names.

     BEST PRACTICE

     Target fewer than 100 computer names to reduce the impact on the **All Computers** group.

5. Review the **Deployment type and schedule** section and click Edit to make changes as needed.

   a. Select the **Self Service** deployment type.

   b. If you want the endpoints to download the patch content before the installation time, select the option for **Download Immediately**.

      BEST PRACTICE

      Select this option for future deployments. If you find that endpoints are not completing patch installations within the specified windows, schedule the deployments even further in advance.

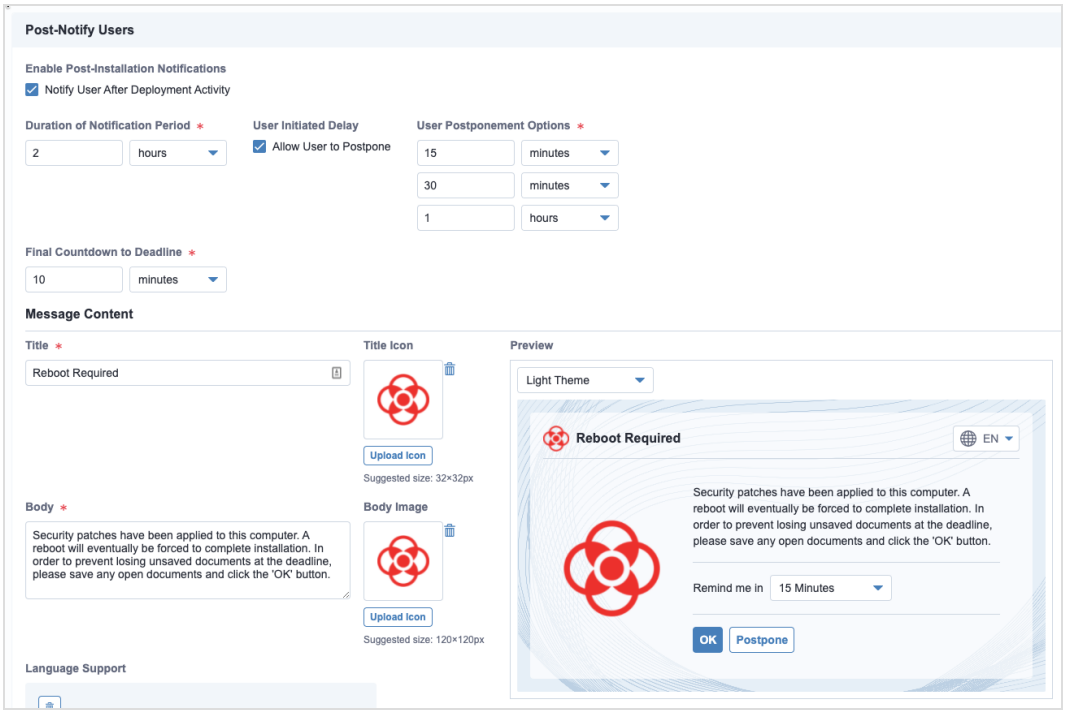
   c. If you want to ignore patching restrictions, select **Override Maintenance Windows** or **Override Block Lists**.

   d. Select whether to restart the endpoint.

6. If you enabled endpoint restarts, you can enable end user notifications about the restarts. If necessary, click Edit and then select **Notify User After Deployment Activity** to configure the following settings. For more information, see Endpoint restarts on page 120.

© 2026 Tanium Inc. All Rights Reserved

- (Optional) Configure settings that allow the end user to postpone the restart.
- Specify the **Message Content** that informs the user about the restart.
- (Optional) Select additional languages and provide translated title and body text for endpoints that are configured for other languages. To view the preview in additional languages, toggle the language dropdown list in the preview. You can also use the dropdown list to preview the notification in light or dark theme.



BEST PRACTICE

Ensure that the **Duration of Notification Period** value is less than a few days. To decrease the endpoints missing critical or important patches metric, the optimal value for this setting depends on your patching cycle. For best results, set the **Duration of Notification Period** value to less than three days.

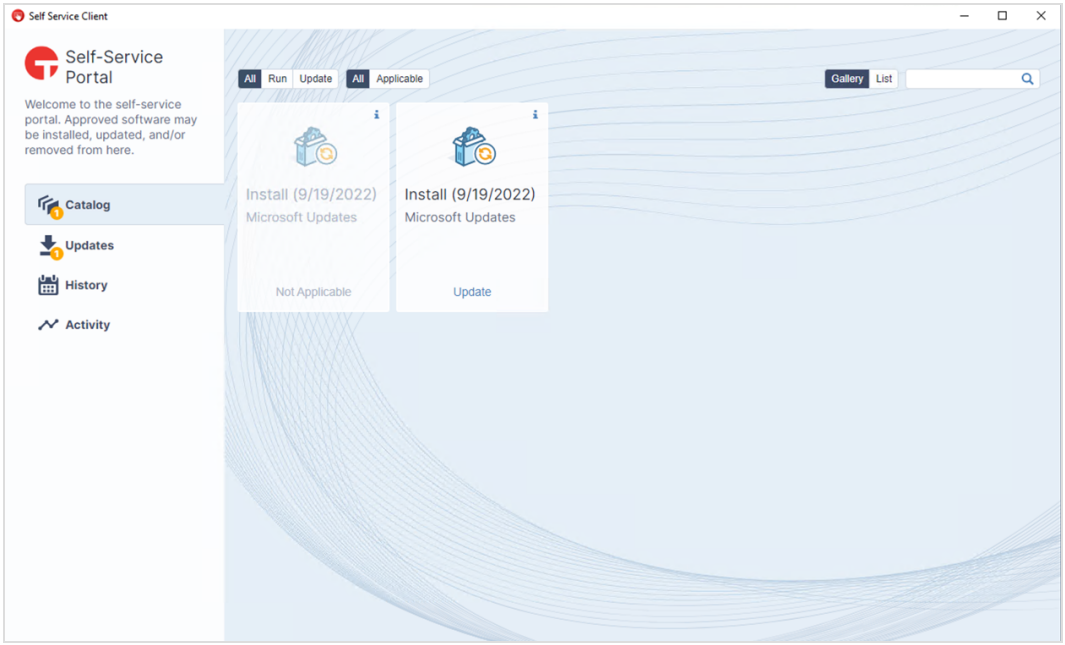
7. Click **Preview to Continue**.
8. Review the deployment details, and then click **Deploy**.

Use the Self Service Client application on endpoints

The Self Service Client application lets users install, update, or remove patches on endpoints.

© 2026 Tanium Inc. All Rights Reserved

The Self Service Client application displays only patches that are applicable on an endpoint. For example, if a deployment uses a patch list that includes patches released 30 or more days ago, the Self Service Client application displays patches when they become available.



The Self Service Client application includes the following tabs:

Catalog

On the **Catalog** tab, you can perform the following actions:

- See a list of all available deployments in the catalog. You can filter to show deployments to install, remove, or update, or to show only the deployments available to the endpoint. You can also select a gallery or list view and that view automatically adjusts based on the resolution set on the endpoint.
- See all active deployments, until the install, update, or removal is complete.
- Select additional languages that you have enabled in the End User Notifications settings. For more information, see Tanium End User Notifications User Guide: Customizing the End-User Self Service interface.
- See additional details about each available deployment. Hover your mouse over the information icon to see the list of patches included in the deployment.

Updates

On the **Updates** tab, you can see updates that are available for installed patches.

History

On the **History** tab, you can see any completed activities that occurred on the system, as well as who initiated the activity. You can filter results by deployment type, as well as by time period.

© 2026 Tanium Inc. All Rights Reserved

Activity

On the **Activity** tab, you can see current and upcoming deployment activity. You can also select **Install** to start the deployment before its scheduled start time.

© 2026 Tanium Inc. All Rights Reserved

Maintaining Patch for Windows and Linux endpoints

Perform regular maintenance tasks to ensure that Patch successfully performs scheduled activities on all the targeted Windows and Linux endpoints and does not overuse endpoint or network resources. If Patch is not performing as expected, you might need to troubleshoot issues or change settings. For more information, see Troubleshooting Patch on page 148 for related procedures.

Perform monthly maintenance

Review Patch coverage, scan configurations, deployments, and maintenance windows. Update the configurations if necessary.

Review and remediate Patch coverage

1. From the Main menu, go to **Modules > Patch > Overview**.
2. Go to the **Health** dashboard to verify that the Patch process is running on all endpoints.
3. To investigate endpoints that are not running the process, click the number above **No** or **Error** in the **Running Patch** panel. The Tanium Server issues a question that returns the computer name, operating system, IP address, and Patch process status for the affected endpoints.
4. To investigate Patch coverage issues, click the number above **Needs Attention** in the **Patch Coverage** panel. The Tanium Server issues a question that returns the computer name, operating system, IP address, and Patch coverage status details for the affected endpoints.

   You can also see this information in the predefined **Patch Coverage Status** report, which is available in the Tanium Reporting workbench.
5. To troubleshoot issues related to the Patch process or coverage, see Monitor and troubleshoot Patch coverage on page 145.

Review and update scan configurations

1. From the Main menu, go to **Modules > Patch > Scan Management**.
2. Review the **Scan Configurations** for each operating system (OS) to verify that they conform to the practices of your organization.
3. Select the **Tanium Scan for Windows** tab and click **Edit**.
4. Review the **Products to Include in Scan**, add any products that you want to include, and click **Submit**.
5. From the Main menu, go to **Modules > Trends > Boards** and click the **Patch** board.
6. Review the **Days Since Last Patch Scan** and **Scan Errors - Last 7 Days** panels for any errors. Click a panel name to see more details.

© 2026 Tanium Inc. All Rights Reserved

7. Troubleshoot scan errors if necessary. For more information, see Troubleshooting Patch on page 148.
8. Edit scan configurations if necessary to resolve errors. For more information, see Edit a scan configuration on page 99.
9. Delete scan configurations if any are no longer useful. For more information, see Delete a scan configuration on page 99.

Review and update deployments

1. From the Patch menu, go to **Deployments**.
2. Review the deployments to determine if any are misconfigured, no longer useful, or do not comply with the practices of your organization.
   For example, if the number of targeted endpoints is low relative to the number of deployments, you might be able to make the patching process more efficient by configuring fewer deployments to target more endpoints.
3. Check the deployment summaries for error messages. For more information, see Review deployment summary on page 125.
4. From the Main menu, go to **Modules > Trends > Boards** and click the **Patch** board.
5. Review the panels in the **Summary**, **Missing Patches**, and **SLA Based Compliance Reporting** sections for any errors. Click a panel name to see more details.
6. Troubleshoot deployments if necessary. For more information, see Troubleshooting Patch on page 148.
7. Add targets to the deployments if necessary to resolve errors. For more information, see Add targets to an existing deployment on page 126.

   For an existing deployment, you cannot perform edits other than adding targets.
8. Stop any deployments that are no longer useful. For more information, see Stop a deployment on page 126.

Review and update maintenance windows

1. From the Main menu, go to **Modules > Patch > Deployments**.
2. Review the maintenance windows to determine if any are misconfigured or no longer useful.
   For example, maintenance windows that have end dates in the past are useful only as blocking maintenance windows. For more information, see Setting maintenance windows on page 131.

   Deployments can run anytime if no maintenance windows are configured. If you imported Patch with default settings, it provides predefined maintenance windows that are not enforced on any computer groups. For more information, see Configuring Patch on page 55.
3. From the Main menu, go to **Modules > Trends > Boards** and click the **Patch** board.
4. If the **Endpoints Missing Critical or Important Patches Released Over 30 Days Ago** panel shows a higher than expected number, check whether maintenance windows are a contributing factor. For more information, see Monitor and troubleshoot mean time to patch on page 146.

© 2026 Tanium Inc. All Rights Reserved

5. Edit maintenance windows if necessary to resolve issues. For more information, see Setting maintenance windows on page 131.
6. Remove any maintenance windows that are no longer useful. For more information, see Delete a maintenance window on page 134.

Perform quarterly maintenance

If you install Patch with default settings, it includes the **Patch** action group, to which the **Patch Supported Systems** computer group is assigned. If you changed computer group assignments for the **Patch** action group, or if you created custom action groups for Patch, review those action groups and, if necessary, update them. For example, if you discover that the Patch process is not starting on all the necessary endpoints, you might have to change the computer group assignments in the action group that is specified for **Patch - Start Patch Process** actions.

1. From the Main menu, go to **Administration > Actions > Action Groups**.
2. Use the filters to list only the groups that are for Patch operations. For more information, see Tanium Console User Guide: View action groups.
   For example, if the custom action groups all have the string "Patch" in their names, enter `Patch` in the **Filter items** field.
3. Edit, create, or delete action groups if necessary to ensure Patch targets the correct computer groups. For more information, see Tanium Console User Guide: Managing action groups.

Perform as-needed maintenance

Review Patch block lists and, if necessary, update them:

1. Go to **Modules > Patch > Block Lists** and review the block lists.
2. Expand  each block list that has one or more **Targets** (computer groups) and verify that the list is **Enforced**. If a list is **Unenforced** on endpoints or some endpoints have an **Old Version**, click the percentage (number) of affected endpoints to analyze the data in Interact.
3. Edit, create, or delete block lists if necessary to resolve issues. For more information, see Managing patches on page 100.

Check and update the Windows Update Agent

You can use Tanium to check which Windows Update Agent versions are installed on your Windows endpoints.

1. In Interact, ask the `Get File Version["C:\Windows\System32\wuaueng.dll"] from all machines` question.
2. Update any endpoints that have a version earlier than 6.1.0022.4. For more information, see the Microsoft article Updating the Windows Update Agent.

Check patch history on Windows endpoints

Use the following resources to check patch history on Windows endpoints:

© 2026 Tanium Inc. All Rights Reserved

1. Ask questions in Interact using the Tanium sensors, specifically the **Patch Installation History** sensor. The **Patch Installation History** sensor returns a list of patches that were installed along with the date and the tool that installed them. AV Definition updates and Windows Store updates are excluded.

   IMPORTANT

   The **Patch Installation History** sensor queries and returns the data in `C:\Windows\SoftwareDistribution\ReportingEvents.log`. Be aware that if you have modified or deleted `ReportingEvents.log` or the `SoftwareDistribution` folder (for example, for troubleshooting), this sensor does not return comprehensive patch history on the endpoint.

2. Use the Powershell **Get-Hotfix** cmdlet, which returns the hotfixes that are installed on local or remote computers.

   NOTE

   Get-Hotfix is supplied by the Component Based Servicing **Win32_QuickFixEngineering** WMI class. Updates supplied by the Microsoft Windows Installer (MSI) or the Windows update site are not returned by **Get-Hotfix**. For more information, see Microsoft Ignite: Get-Hotfix not returning all installed KBs.

Monitor and troubleshoot Patch coverage

The following table lists contributing factors into why the Patch coverage metric might report endpoints as **Needs Attention** or **Unsupported**, and corrective actions you can make.

Contributing factor	Corrective action
Gaps in Patch action group membership	Ensure all operating systems that are supported by Patch are included in the Patch action group.
Gaps in scan configuration coverage	Review each scan configuration and which computer groups are targeted by each configuration. Ensure that every endpoint that is supported by Patch is targeted by at least one scan configuration.
Scan frequency value is set too high	Review each scan configuration to ensure that the **Frequency** value is set to less than three days for all scan configurations.
Scan windows are too restrictive	Scan windows are optional. If you decide to use them, the **Override** option should be set to less than two days.
Unmitigated scan failures	Investigate endpoints with scan errors in scan results that are older than two days. Remediate the error conditions on each endpoint. For more information, see Maintaining Patch for Windows and Linux endpoints on page 142.
Patch process is not running	Ensure that there are no conditions that could prevent the Patch process from running on endpoints that are included in the Patch action group.

© 2026 Tanium Inc. All Rights Reserved

Monitor and troubleshoot endpoints missing critical or important patches

The following table lists contributing factors into why the endpoints missing critical or important patches metric might be higher than expected, and corrective actions you can make.

Contributing factor	Corrective action
Selective patching as a practice	Avoid choosing specific patches based on vulnerability reports. Instead, use dynamic, rule-based patch lists. These lists should be cumulative. For example, do not create any rules that prevent patches that are older than a specific date from being included in a patch list.
Patches are deployed only for the current month	Use dynamic, rule-based patch lists. These lists should be cumulative. For example, do not create any rules that prevent patches that are older than a specific date from being included in a patch list.
Having an n-1 patching policy	Include patches for the current month. Expand endpoint diversity in patch testing groups to increase the changes of identifying newly-released problematic patches for deploying patches to production.
Not enforcing post-deployment restarts	Use the **Restart** option within deployments. (Windows) Use the **Notify User** option and set the **Deadline for restart** value to less than a few days. To decrease both the endpoints missing critical or important patches and the mean time to patch metrics, the optimal value for this setting depends on your patching cycle. Successful customers find that setting the **Deadline for restart** value to less than three days is optimal.

Monitor and troubleshoot mean time to patch

The following table lists contributing factors into why the mean time to patch metric might be higher than expected for endpoints and corrective actions you can make.

Contributing factor	Corrective action
Delayed testing cycle	Begin the process of testing new monthly patches the day they are released, typically Patch Tuesday (second Tuesday of each month).
Delayed start of production cycle	Avoid waiting longer than two weeks after a patch release to start patching production systems. The longer you wait to start patching production systems, the more aggressive the subsequent deployments need to be to complete the patching cycle in a reasonable time.
Staggering deployments to distribute the load on the network	Do not stagger deployments in an attempt to distribute the load on your network or Tanium. The more endpoints that are being patched simultaneously, the more efficient Tanium becomes with overall WAN usage. For bandwidth-constrained locations, you can implement site throttles. For more information, see Tanium Console User Guide: Configure site throttles.

© 2026 Tanium Inc. All Rights Reserved

Contributing factor	Corrective action
Staggering deployments to distribute the load on the Tanium Server or Patch	Do not stagger deployments in an attempt to distribute the load on your network or Tanium.
Endpoints do not have enough time to install patches	Ensure that deployment windows are at least four hours and properly overlap with maintenance window times. Ensure that maintenance windows are at least four hours long, repeat at least once each month, and properly overlap with deployment times and change control process timelines. For deployments that are scheduled for the future, select the **Download immediately** option. If you find that endpoints are not completing patch installations within the specified windows, schedule the deployments even further in advance.
Attempting to minimize disruption to users with maintenance windows	Use Tanium End-User Notifications instead of restrictive maintenance windows.
Not enforcing post-deployment restarts	Use the **Restart** option within deployments. (Windows) Use the **Notify User** option and set the **Deadline for restart** value to less than a few days. To decrease both the endpoints missing critical or important patches and the mean time to patch metrics, the optimal value for this setting depends on your patching cycle. Successful customers find that setting the **Deadline for restart** value to less than three days is optimal.
Unmitigated installation failures	Identify endpoints with patch installation failures. Investigate the specific error codes. Remediate the conditions that caused the failures.
Endpoint health issues	Ensure that endpoints have at least 5 GB of free space, a healthy Windows Update Agent, and an up-time of less than 90 days.

© 2026 Tanium Inc. All Rights Reserved

Troubleshooting Patch

If Patch is not performing as expected, you might need to do some troubleshooting or change settings. For information about specific error messages, see Reference: Common Patch errors on page 163.

BEST PRACTICE

To prevent issues that might occur due to endpoint health issues, ensure that endpoints have:

- At least 5 GB of free space
- A healthy Windows Update Agent
- An up-time of less than 90 days

Collect a troubleshooting package

For your own review or to assist support, you can compile Patch logs and files that are relevant for troubleshooting. The ZIP file is also known as a support bundle.

1. From the Main menu, go to **Modules > Patch > Overview** and click Help.
2. Click the **Support** tab and click **Collect**.
3. When the **Status:** is updated, click **Download**.
   The log ZIP file might take a few moments to download. The files have a timestamp with a Patch-*YYYY-MM-DD*T*HH-MM-SS.mmm*Z format.

Download audit log

You can download an audit log for a single object (for example, a deployment) or multiple objects (for example, all deployments). The audit log contains all creation, modification, and deletion events for the object or objects. For example, you can download the audit log for a deployment to view the details of when it was stopped.

To download an audit log, on a Patch page, click Options > **Download <*Object*> Audit Logs**. The CSV file is available in your downloads folder.

View job logs to troubleshoot `job failed` errors

You can download job logs to troubleshoot "job failed" errors.

1. From the Main menu, go to **Modules > Patch > Overview** and click Help.
2. Click the **Support** tab and click **View Job Status**.
3. In the **Job Detail** window, click **Download Logs** to download a `job-logs.txt` file with more details about recent jobs.

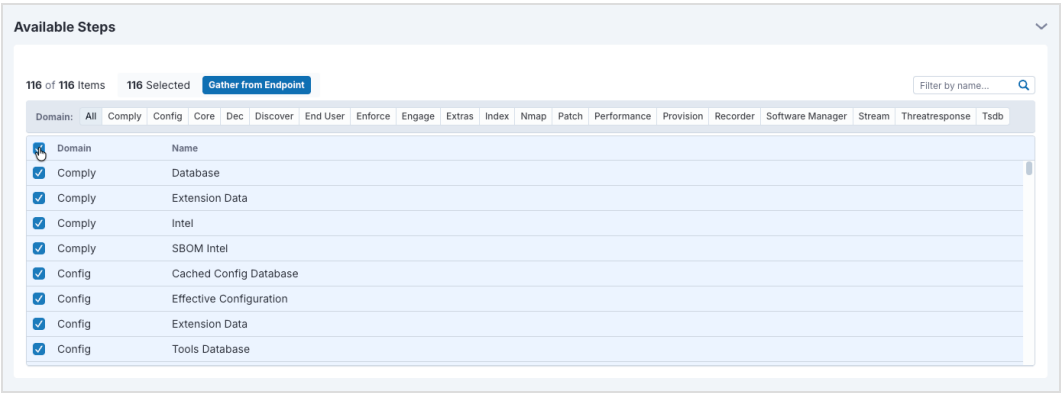
© 2026 Tanium Inc. All Rights Reserved

Collect Patch troubleshooting information from Windows and Linux endpoints

You can collect and review endpoint artifacts to troubleshoot Patch issues on Windows and Linux endpoints.

You can use Client Management to directly connect to an endpoint and collect a bundle of logs and other artifacts, sometimes referred to as an *Endpoint Must Gather* (EMG).

1. From the Main menu, go to **Shared Services > Client Management**.
2. From the Client Management menu, click **Client Health**.
3. In the **Direct Connect** search box, enter all or part of an IP address or a computer name.
   Matching results appear after the search completes.
4. From the search results, click the computer name to connect to the endpoint.
5. Click the **Gather** tab. For the **Domain** filter, select the domain and category names for which you want to gather troubleshooting information. You can optionally filter the category list by domain, and you can select the check box in the header row to toggle the selection of all categories in the current filter.

   For Patch information, select the **Patch** domain.
6. Click **Gather from Endpoint**.
   The selected logs and artifacts are gathered from the endpoint. The package appears in the **Must Gathers** section, and the name of the package corresponds with its time stamp.
7. When **Finished** appears in the **Run State** column, select the package and click **Download** to download a ZIP file that contains the troubleshooting information.

For more information about how to connect directly to endpoints, see Tanium Direct Connect User Guide.

For more information about Client health features in Client Management, see Tanium Client Management User Guide: Monitor the Client health overview in Client Management and Tanium Client Management User Guide: Access detailed Client health and troubleshooting information on an endpoint.

© 2026 Tanium Inc. All Rights Reserved

Configure endpoint logging for Windows and Linux endpoints

Distribute the **Patch - Set Patch Process Options** package to your Windows and Linux endpoints to change the default logging type and log rotation settings.

1. In Interact, target the endpoints on which you want to configure logging. For example, `Get Operating System from all machines`.
2. Click **Deploy Action**. Choose the **Patch - Set Patch Process Options** package and specify the log level, log size, and number of logs to keep.
3. Click **Preview** and then click **Deploy Action**.

Verify endpoint tools

If you are experiencing issues such as a feature not working on an endpoint or seeing incorrect data in the workbench, confirm that your endpoints have the latest toolset version. For more information, see Tanium Endpoint Configuration User Guide: Identify and resolve issues with endpoint tools or Client Extensions. For more information about Patch tools, see Reference: Patch endpoint tools on page 171.

Windows and Linux patches are not listed in the Patches view

If you are having difficulty getting Windows and Linux patches to appear:

1. Verify that the **Patch - Is Process Running** sensor returns `Yes` for your endpoints.
2. Ensure that the expected endpoints are in the action group.
3. Verify that the expected endpoints are targeted by a scan configuration.
4. Check for scan errors on the endpoints targeted by a scan configuration.

Troubleshoot scan errors on Windows and Linux endpoints

Investigate Windows and Linux endpoints with scan errors that have scan results older than two days and resolve the errors for each endpoint. If Patch is unable to successfully scan an endpoint for its applicable patches, Patch does not know what patches to deliver to the endpoint during a patch deployment.

1. From the Main menu, go to **Modules > Patch > Scan Management** and then click **Scan Errors**.
2. Review any scan errors.
3. Review Reference: Common Patch errors on page 163 and implement solutions for applicable errors.
4. For other errors, complete the following general troubleshooting steps.
    a. (Windows) Review the Windows Update log on the endpoint. Search for key errors and then search the internet for solutions for the identified error. To get the Windows Update log, see Collect Patch troubleshooting information from Windows and Linux endpoints on page 149.

© 2026 Tanium Inc. All Rights Reserved

b. Review the Tanium Patch logs for information on why the scan did not start or complete successfully on an endpoint. To get the Tanium Patch logs, see Collect a troubleshooting package on page 148.

5. Confirm that routine scan error remediation is done before your routine patching cycle. To help identify errors, create a report from a saved question that identifies endpoints with scan errors.

   For example, you might use the following saved question:

   ```
   Get Computer Name and Operating System and Patch - Scan Errors and Patch - Scan Age and Patch - Has Enforced Scan Configuration and Patch - Is Process Running from all machines with ( Patch - Scan Errors matches "^[1-9]\d+\|.*$" or ( Patch - Has Enforced Scan Configuration equals No or ( Patch - Scan Age matches "^(?!([0-2] Day|N\/A|Could not get results).*).*$" and Uptime matches "^\d+ [Dd]ays$" ) ) )
   ```

   For more information on saved questions and reporting, see Tanium Console User Guide: Managing saved questions in Console and Interact.

Offline CAB scans fail for Windows 7 and Windows Server 2008 R2

If offline CAB scans fail for Windows 7 and Windows Server 2008 R2 with the error:

```
Error creating Update Service Object - See C:\Windows\windowsupdate.log for more details
```

Check the Windows Update log for the following errors:

```
WARNING: Digital Signatures on file C:\Windows\SoftwareDistribution\ScanFile\f6f0081a-1e6e-4e64-a804-58cf334a1f48\Source.cab are not trusted: Error 0x800b0109
```

```
WARNING: Digital Signatures on file C:\Windows\SoftwareDistribution\ScanFile\f6f0081a-1e6e-4e64-a804-58cf334a1f48\Source.cab are not trusted: Error 0x800b0109
```

If you see these errors, then prerequisite patches might not be installed on the endpoints. To resolve this issue, use either Tanium Scan or a method outside of Patch to install updates for SHA2 signing and Extended Security Update on the endpoints. For more information, see Tanium Scan on page 90 and Knowledge Article: Enabling and Delivering Microsoft Extended Security Updates with Tanium.

Scans are not completed on Linux endpoints

Patch 2.3.5 supports Red Hat and CentOS Linux endpoints. Patch 2.4.3 also supports Oracle and Amazon Linux endpoints. Patch 3.2.160 also supports SUSE endpoints.If you are having difficulty getting scans to run on Linux endpoints:

1. From the Main menu, go to **Modules > Patch > Overview**, click Settings and then click **Operating Systems** to verify that the **Enhanced Linux Support** option is enabled.
2. Verify that the **Patch - Is Process Running** sensor returns `Yes` for your Linux endpoints.
3. Verifythat the Tanium Server can reach the `repomd.xml` file by appending `/repodata/repomd.xml` to the configured **baseurl** value.
4. Check the endpoint log at `/opt/Tanium/TaniumClient/Tools/Patch/logs/patch-process.log` for errors.

© 2026 Tanium Inc. All Rights Reserved

Red Hat Linux endpoints stuck in `Waiting for Initial Scan` status

If you configure a repository that includes both **Red Hat Enterprise Linux 6 Server (RPMs)** and **Red Hat Enterprise Linux 7 Server (RPMs)** endpoints, your targeted endpoints might appear to be stuck in the `Waiting for Initial Scan` status.

1. Verify that each major operating system is targeted in repositories.
2. Target Linux endpoints by major operating systems.

Linux repository snapshots issues

If you encounter issues creating or using snapshots, review the following solutions. For information about specific snapshot errors, see Reference: Common Patch errors on page 163.

Warning about a failed snapshot

A warning message appears, to indicate that a snapshot failed. To modify the snapshot, click **Manage Repository Snapshots**. To remove the warning, click **Dismiss warning**.

Patch process is not running on Linux endpoints

Start the Patch process:

1. In Interact, ask the `Get Operating System from all machines` question.
2. From the grid, select the Linux operating systems.
3. Click **Deploy Action**. Choose the **Patch - Start Patch Process [Non-Windows]** package.
4. Click **Preview** and then click **Deploy Action**.

OpenSUSE and SLES endpoints install later version of software

OpenSUSE and SUSE Linux Enterprise Server (SLES) endpoints might install a later version of software than specified in a deployment. Zypper, which manages software packages on those endpoints, automatically selects the latest available version of software for installation. If you create a deployment to install version 1.0.1 of software and the latest available version of the software is 1.0.2, when the endpoint receives the deployment, Zypper installs version 1.0.2.

To workaround this Zypper behavior, use repository snapshots. For more information, see Manage Linux repository snapshots on page 78.

End user notifications are not displayed or endpoints have errors

End user notifications are supported for Windows endpoints only. If end user notifications are not being displayed on the endpoints or the endpoints have errors (for example, their statuses are **Non-compliant**):

© 2026 Tanium Inc. All Rights Reserved

1. Confirm that the endpoints have the latest versions of the tools. For more information, see Tanium Endpoint Configuration User Guide: Manage toolset versions in the upgrade rings.
2. Verify that the Tanium End-User Notifications solution is installed. For more information, see Tanium End-User Notifications User Guide: Installing End-User Notifications.
3. Ask the question: `Get Endpoint Configuration - Tools Status from all machines` to check if your endpoints have the end user notification tools.
4. Verify that any security software exclusions include the `\Tanium\Tanium End User Notification Tools` directory. For more information, see Security exclusions on page 41.
5. Uninstall the End-User Notifications tools on the endpoints. For more information, see Tanium End-User Notifications User Guide: Remove End-User Notifications tools from endpoints. Then wait up to 10 minutes for the tools to automatically reinstall.

   You can also reinstall the End-User Notifications tools with the **Endpoint Configuration - Reinstall Tool** package.

Patch workbench slowly loads pages

If the Patch workbench slowly loads pages, confirm that you have enabled the **Inactive Deployments Removal** option to remove old inactive deployments. The deployment cleanup helps improve the performance of the Patch workbench. For more information, see Delete old inactive deployments on page 127.

Identify and resolve issues with Client Extensions

Use the following steps to troubleshoot issues with the Client Extensions that Patch installs and uses. During troubleshooting, consider environmental factors such as security exclusions, file locks, CPU usage, RAM usage, and disk failures.

For more information about the Client Extensions that Patch installs and uses, see Client Extensions.

1. If endpoints have Client Extension shared process mode enabled and you need to troubleshoot resource usage or crashes in the combined `TaniumCX.exe` or `TaniumCX` process, disable shared process mode on the affected endpoints, and then reproduce the issue if possible. For more information, see Endpoint Configuration User Guide: Manage Client Extension shared process mode.
2. To review the health of Client Extensions or to start an investigation into an existing error, ask a question using the `Client Extensions - Status` sensor.
   The results of these questions help to identify endpoints with errors and provide a starting point to deploy actions that might help correct the issue. Filter the results and drill down as necessary to investigate results that indicate errors.

© 2026 Tanium Inc. All Rights Reserved

Consider whether endpoints with errors share common characteristics, such as operating system, domain or organization unit, or the antivirus software that is installed.

3. Target one or more endpoints with errors, and uninstall tools that report errors without blocking reinstallation. For more information, see Remove Patch tools from endpoints and Endpoint Configuration User Guide: Uninstall a tool installed by Endpoint Configuration.



When you perform a hard uninstallation of some tools, the uninstallation also removes data that is associated with the tool from the endpoint. This data might include important historical or environmental data. If data that you want to keep is associated with the tool, make sure you perform only a soft uninstallation of the tool.

Wait for automatic reinstallation of the tool. If the reinstallation does not resolve the issue, continue to the next step.

4. Ask a question using the `Endpoint Configuration - Tools Status Details` sensor, and include filters to limit the results to the tool that you are investigating. For example:

`Get Endpoint Configuration - Tools Status Details having Endpoint Configuration - Tools Status Details:Tool Name contains Patch from all machines with Endpoint Configuration - Tools Status:Tool Name contains Patch`

Review the columns in the results for specific information about errors. The following table provides guidance for some common error conditions:

© 2026 Tanium Inc. All Rights Reserved

Potential errors returned by the Ednpoint Configuration - Tools Status Details sensor

Error Condition	Possible Resolution
No error appears, but an available new version has not been installed	Review the **Targeted Version** column to make sure that the endpoint has received the latest manifest. If the targeted version does not yet show the updated version, the Endpoint Configuration manifest has not updated on the endpoint, usually for one of the following reasons: • The manifest update is still pending. Either wait for the manifest to update and then review the results again, or follow the steps in Endpoint Configuration User Guide: Verify and manually update the Endpoint Configuration manifest. • Action lock is enabled on the endpoint. Follow the steps in Endpoint Configuration User Guide: Verify and manually update the Endpoint Configuration manifest to identify endpoints with action lock turned on. • Patch is no longer installed, or it is no longer targeting the endpoint. In some cases, Patch might stop targeting an endpoint because it no longer needs the endpoint for a particular workload. Consider whether Patch should still target the endpoint: ◦ If it is expected or intentional that Patch no longer targets the endpoint, you can optionally uninstall Patch tools and dependencies. For more information, see Remove Patch tools from endpoints. ◦ If Patch should still target the endpoint, make sure that the Patch action group includes the endpoint, and make sure Patch targets the endpoint in any expected configurations or profiles. Then, either wait for the manifest to update and then review the results again, or follow the steps in Endpoint Configuration User Guide: Verify and manually update the Endpoint Configuration manifest.
Installation Blocker:`Unmet Dependencies: [Tool name]`	If no **Failure Message** or **Failure Step** appears, the endpoint might be waiting for the dependencies to install. Wait to see if the condition resolves on its own. If this condition remains for an extended period, ask the question again and review any error information in other columns, especially the **Failing Dependency** column.
Failing Dependency: *`[Tool name]`*	Ask the question: `Endpoint Configuration - Tools Status Details having Endpoint Configuration - Tools Status Details:Tool Name contains [Tool name] from all machines with Endpoint Configuration - Tools Status:Tool Name contains [Tool name]` Investigate further errors with the tool. If the dependency has not been installed on an endpoint, ask the question: `Get Endpoint Configuration - Tools Retry Status from all machines with Computer Name equals Computer_Name` to review the retry status for the tool installation. For more information, see Endpoint Configuration User Guide: Review tool installations that are scheduled for a retry.
Manually Blocked:`blocked`	The tool was previously blocked, either manually or during a previous uninstallation. Unblock the tool. For more information, see Endpoint Configuration User Guide: Block or unblock tools from installing on an endpoint.

5. Review the Extensions logs on the endpoint. Take note of entries that include `fail` or `error`. For more information, see Review the Extensions log for an endpoint on page 156.

For additional help, collect all logs for Tanium Patch, and contact Tanium Support.

© 2026 Tanium Inc. All Rights Reserved

Review the Extensions log for an endpoint

Use Client Management to directly connect to an endpoint and view and download extension logs.

1. From the Main menu, go to **Shared Services > Client Management**.
2. From the Client Management menu, click **Client Health**.
3. In the **Direct Connect** search box, enter all or part of an IP address or a computer name.
   Matching results are displayed after the search completes.
4. From the search results, click the computer name to connect to the endpoint.
5. Click the **Logs** tab, and select an **extensions*[#]*.log** file.
6. (Optional) To download the log, click **Download**.

For additional help, collect all logs for Tanium Patch, and contact Tanium Support.

Remove Patch tools from Windows and Linux endpoints

You can deploy an action to remove Patch tools from an endpoint or computer group. Separate actions are available for Windows and non-Windows endpoints.

1. Prevent Patch tools from installing on endpoints and scheduled actions from running.
   a. From the Main menu, go to **Administration > Actions > Action Groups**.
   b. Click the **Patch** action group, change the **Computer Groups**, and click **Save**.
      - To prevent Patch actions on select endpoints, change the computer groups to no longer target the endpoint or computer group.
      - To prevent Patch actions on all endpoints, change the computer groups to **No Computers**.
2. In Interact, target the endpoints from which you want to remove the tools. For example, ask a question that targets a specific operating system:
   `Get Endpoint Configuration - Tools Status from all machines with Is Windows equals true`
3. In the results, select the row for **Patch**, drill down as necessary, and select the targets from which you want to remove Patch tools. For more information, see Tanium Interact User Guide: Drill Down.
4. Click **Deploy Action**.
5. For the **Deployment Package**, select **Endpoint Configuration - Uninstall Tool [Windows]** or **Endpoint Configuration - Uninstall Tool [Non-Windows]**, depending on the endpoints you are targeting.
6. For **Tool Name**, select **Patch**.

© 2026 Tanium Inc. All Rights Reserved

7. (Optional) By default, after the tools are removed they cannot be reinstalled. To allow tools to be automatically reinstalled, clear the selection for **Block reinstallation**. Re-installation occurs almost immediately.

   NOTE

   If reinstallation is blocked, you must unblock it manually:

   - To allow Patch to reinstall tools, deploy the **Endpoint Configuration - Unblock Tool [Windows]** or **Endpoint Configuration - Unblock Tool [Non-Windows]** package (depending on the targeted endpoints).
   - If you reinstall tools manually, select **Unblock Tool** when you deploy the **Endpoint Configuration - Reinstall Tool [Windows]** or **Endpoint Configuration - Reinstall Tool [Non-Windows]** package.

8. (Optional) To remove all Patch databases and logs from the endpoints, clear the selection for **Soft uninstall**.

   CAUTION

   When you perform a hard uninstallation of some tools, the uninstallation also removes data that is associated with the tool from the endpoint. This data might include important historical or environmental data. If data that you want to keep is associated with the tool, make sure you perform only a soft uninstallation of the tool.

9. (Optional) To also remove any tools that were dependencies of the Patch tools that are not dependencies for tools from other solutions, select **Remove unreferenced dependencies**.

10. (Optional) In the **Deployment Schedule** section, configure a schedule for the action.

    BEST PRACTICE

    If some target endpoints might be offline when you initially deploy the action, select **Recurring Deployment** and set a reissue interval.

11. Click **Show preview to continue**.

12. A results grid appears at the bottom of the page showing you the targeted endpoints for your action. If you are satisfied with the results, click **Deploy Action**.

NOTE

If you have enabled Endpoint Configuration approval, tool removal must be approved in Endpoint Configuration before tools are removed from endpoints.

Uninstall Patch

If you need to uninstall Patch, first clean up the Patch artifacts on the endpoint and then uninstall Patch from the server.

© 2026 Tanium Inc. All Rights Reserved

1. Remove the Patch solution from the Tanium Module Server. From the Main menu, go to **Administration > Configuration > Solutions**.
    a. In the Patch section, select **Patch**, click **Uninstall**, and follow the process.
    b. Click **Proceed with Uninstall**.
    The uninstaller disables any actions.
    c. Return to the Solutions page and verify that the **Import** button is available for Patch.
    If the Patch module has not updated in the console, refresh your browser.
2. Delete any remaining files in the `<Module Server>\services\patch-service` and `Tanium Module Server\services\patch-files` directories.
3. Unregister all Patch-related sensors.
    a. Go to the Interact **Overview** page and click Settings.
    b. Filter the **Registration & Collection** tab to find the Patch-related sensors.
    c. For each sensor, select **Actions > Release** to unregister.
4. Delete all Patch-related Endpoint Configuration items.
    a. From the Main menu, go to **Shared Services > Endpoint Configuration > Configurations**.
    b. Select **Patch Toolset** and all items in the **Patch** domain, and click **Delete**.
5. Delete all scheduled actions under the Patch action group.
    a. From the Main menu, go to **Administration > Actions > Scheduled Actions**.
    b. Select the **Patch** action group.
    c. Select the scheduled actions and click **More > Delete**.
6. Delete the Patch action group.
    a. From the Main menu, go to **Administration > Actions > Action Groups**.
    b. Select the **Patch** action group, click **Migrate and Delete**, and complete the process.
7. Delete all Patch-related saved questions.
    a. From the Main menu, go to **Administration > Content > Saved Questions**.
    b. Select all Patch-related questions and click Delete.
8. Delete all sensors prefixed with **Patch -** .
    a. From the Main menu, go to **Administration > Content > Sensors**.
    b. Select all sensors prefixed with **Patch -** and click Delete.

© 2026 Tanium Inc. All Rights Reserved

9. Delete all packages prefixed with **Patch -** .
    a. From the Main menu, go to **Administration > Content > Packages**.
    b. Select all packages prefixed with **Patch -** and click Delete .

Restore the state of the Patch database

You can import the `patch.db` file to restore the Patch configuration.

1. Stop the Patch service on the Tanium Module Server.
2. Copy your `patch.db` file into the `<Module Server>\services\patch-service\` directory, replacing the existing file.
3. Restart the Patch service.
4. In Tanium Console, refresh the Patch workbench.
5. Configuring Patch on page 55.
   Any existing data, including patch lists, deployments, and associated patches and actions appear in the Patch workbench.

   
   NOTE

   If a deployment scheduled action is missing, you might need to wait up to 5 minutes for it to show up.

Resolve UUP synchronization errors

If Tanium encounters problems synchronizing patches for Windows 11 22H2 or later endpoints, errors appear in the **UUP Synchronization Management** section of the **Overview** page or in the **Summary** section of a **Patch details** page.

© 2026 Tanium Inc. All Rights Reserved

UUP synchronization errors and resolutions

Error message	Problem	Solution
Not enough disk space on the Tanium Server	Synchronization will result in less than 10% total disk space remaining on the Tanium Server so the process does not progress.	To resolve the error you can do one of the following actions: • Get more disk space and then retry the failed synchronization. • In time-sensitive emergency situations, configure the **BypassUUPStorageLimit** advanced setting, which allows synchronization to fill the disk to 95% disk usage. 1. From the Main menu, go to **Modules > Patch > Overview > Settings**. 2. In the **Advanced Settings** section, click **Add Setting** and then set `BypassUUPStorageLimit = 1` 3. Click **Save**. 4. Retry the failed synchronization. For more information, see Manually synchronize patches on page 108. 5. After synchronization is successful, set `BypassUUPStorageLimit = 0` to disable the setting.
Failed to upload data to Tanium Server	Potential `System User Service` error or some internal error within the Tanium Server.	This error often self-resolves after the sync retries. If the problem persists, contact Tanium Support.

© 2026 Tanium Inc. All Rights Reserved

UUP synchronization errors and resolutions (continued)

Error message	Problem	Solution
All known urls failed to respond	Tanium could not reach any of the URLs on patch.	• If you are using are using a local WSUS server: 1. Confirm that the WSUS server is reachable from the Tanium Module Server. 2. On the WSUS server, verify whether the update is approved. 3. If the update is approved, verify that making a head request from the Tanium Module Server to the URL of the associated metadata file responds with a 200 status. If the response is a 404, proceed with troubleshooting any proxy settings that might be present in the environment. 4. If the update is not approved, approve the update and then manually synchronize patches. • If you are not using a local WSUS server: 1. Go to the Patch details page and confirm whether the patch URLs have any of the following domains: ○ windowsupdate.microsoft.com ○ *.windowsupdate.microsoft.com ○ *.update.microsoft.com ○ *.windowsupdate.com ○ download.windowsupdate.com ○ download.microsoft.com ○ *.download.windowsupdate.com ○ dl.delivery.mp.microsoft.com ○ *.delivery.mp.microsoft.com 2. If a patch URL domain is not on the list: a. Use Tanium to target the endpoints that have this patch marked as applicable. b. Deploy the **Patch - Reset Windows Update Client** package to perform a Windows Update Agent reset. c. Wait for a re-scan. 3. If the issue is not resolved, check the proxy configuration of the environment and confirm whether the Tanium Module Server can reach any of the patch URLs that have errors. Resolve any proxy issues.

© 2026 Tanium Inc. All Rights Reserved

UUP synchronization errors and resolutions (continued)

Error message	Problem	Solution
All reachable urls responded with 404	The update is revoked or proxy settings are causing issues.	• If you are using a local WSUS server, see the solution for **All known urls failed to respond**. • If you are not using a local WSUS server, the patch is likely a revoked update. No action is needed. If the patch is not a revoked update, retry the failed synchronization. For more information, see Manually synchronize patches on page 108.
Hash mismatch	Incorrect files might have been staged on the WSUS server.	1. On the third-party patching tool or WSUS server, approve the patches that failed to synchronize. 2. Retry the failed synchronization. For more information, see Manually synchronize patches on page 108. 3. If the problem persists, deploy the **Patch - Reset Windows Update Client** package to all endpoints to perform a Windows Update Agent reset. If the problem persists, contact Tanium Support to help investigate the issue.
Failed to sync update with endpoint config	Patch files were downloaded successfully, and packages were created, but Endpoint Configuration failed to register the necessary metadata for endpoints.	1. Collect a troubleshooting package. 2. In the logs, search for the root cause of the Endpoint Configuration errors and resolve the issues 3. Retry the failed synchronization. For more information, see Manually synchronize patches on page 108.

Cannot use Tanium Patch to deploy Microsoft out-of-band updates

Tanium Scan for Windows synchronizes with the Microsoft Windows Server Update Services (WSUS) catalog. Only updates which Microsoft publishes to the Server Update Services release channel are visible to endpoints scanned with the Tanium Scan method. Microsoft typically does not release out-of-band updates to the Server Update Services channel.

To deploy out-of-band updates, use Tanium Deploy to install the Latest Cumulative Update (LCU) package that includes the out-of-band update. For more information, see Knowledge Article: Deploying Out-of-Band Microsoft Updates with Tanium. If the out-of-band update is not included in an LCU, download the update from Microsoft and then create a software package in Tanium Deploy. For more information, see Tanium Deploy User Guide: Create a software package.

Contact Tanium Support

To contact Tanium Support for help, sign in to the Tanium Customer Community.

For more information about how to submit a support case, see Case Submission Form.

© 2026 Tanium Inc. All Rights Reserved

Reference: Common Patch errors

Review common Patch error messages and possible solutions. For information about general errors in Patch, see Troubleshooting Patch on page 148.

Client API connection failed. Unable to download file. Error #9

Cause

An endpoint performed a client reset while downloading a patch.

Solution

This error message can typically be ignored. After the client reset is complete, the endpoint typically continues downloading the patch within minutes. If you continue to see this error message, Contact Tanium Support on page 162.

Error creating Update Service Object - See C:\Windows\windowsupdate.log for more details. Error #9

Cause

Patch is unable to establish communication with the local Windows Update API.

Solution

Review the Windows Update log for errors, and then consult the Microsoft documentation for information about each error.

Patch <Patch UID>: WU_E_DM_INCORRECTFILEHASH. Error #-2145099774

Cause

A patch file becomes corrupted in transit from Microsoft to the Tanium Server.

Solution

For help with this error message, Contact Tanium Support on page 162.

Patch <Patch UID>: ERROR_INSTALL_FAILURE. Error #-2147023293

Cause

This error can have various causes, but it is likely caused either by a third-party application or by corruption in the Windows update.

© 2026 Tanium Inc. All Rights Reserved

Solutions

- Review your Host and network security requirements on page 40 and make sure you have added the necessary security exclusions so that antivirus software is not blocking Tanium processes.
- Use Tanium to target the endpoint and deploy the **Patch - Reset Windows Update Client** package to perform a Windows Update Agent reset.

Patch <Patch UID>: WU_E_CALL_CANCELLED. Error #-2145124341

Cause

This error is likely caused by interference from anti-virus software on an endpoint.

Solution

Review your Host and network security requirements on page 40 and make sure you have added the necessary security exclusions so that antivirus software is not blocking Tanium processes.

-2147024784 ERROR_DISK_FULL

Cause

The installation drive on an endpoint is full.

Solution

Check the system drive and the drive on which the Tanium Client is installed and provide more disk space. Use the **Disk Free Space**, **System Disk Free Space**, **Low Disk Space**, or **Low System Disk Free Space** Tanium sensors to identify systems with low amounts of free disk space.

OfflSnc WARNING: failed to copy offline cab. hr = 0x80070070

Cause

The drive that contains the Tanium Client does not have enough disk space to download the offline CAB file.

Solution

Increase the amount of space available on the drive. Use the **Disk Free Space**, **System Disk Free Space**, **Low Disk Space**, or **Low System Disk Free Space** Tanium sensors to identify systems with low amounts of free disk space.

© 2026 Tanium Inc. All Rights Reserved

-2145124320 WU_E_NO_INTERACTIVE_USER

Cause

The patch cannot be installed silently, and a user must sign in and interact with the installation. Typically, this error occurs when conducting server patching.

Solution

Add the update to a block list or remove it from your deployment patch list. For more information, see Exclude patches with block lists on page 104 and Edit a list on page 106.

E_PROP_ID_UNSUPPORTED

Cause

This error is triggered by the Windows Update Agent, and usually indicates that the endpoint needs to be restarted.

Solutions

- Use the **Uptime** sensor to verify the uptime of the endpoint. For more information, see Tanium Console User Guide: Managing Sensors.
- If the endpoint was configured to reboot but did not reboot after receiving a patch, this error is the result of conflicting files running on the endpoint. Verify that End-User Notifications and reboot settings are properly configured for the endpoint. For more information, see Install and Configure Tanium End-User Notifications.
- Restart the endpoint and reissue the deployment. For more information, see Reissue a deployment on page 126.

Unable to Load PatchLib

Cause

This error is likely caused either by an endpoint not being part of a Patch action group, or by an incorrect version of Patch on the endpoint.

Solutions

- Verify that the affected endpoint is in the Patch action group so that it is within scope of operations. For more information, see Configuring Patch on page 55.
- Verify that asking **Get Endpoint Configuration – Tools Status contains Patch** in Interact shows the correct version of Patch is installed.

© 2026 Tanium Inc. All Rights Reserved

Windows Update Error: -2145124338 WU_E_XML_INVALID

Cause

The Windows Update Agent found invalid information in the XML data for the update.

Solution

Make sure that the endpoint is using the latest version of Windows Update Agent.

Unrestored registry snapshot found

Cause

The Patch Manager process was interrupted during a scan. This issue can happen if the endpoint restarts during a scan.

Solution

This issue is usually transient and no longer appears after the next scheduled scan. If you continue to see this error message, Contact Tanium Support on page 162.

Windows Update Error Code: 7 Out of Memory

Cause

The system has reached the system commit limit and is unable to complete scanning operations. Patch automatically performs batching operations to try to reduce the overall memory utilization of `svchost` during scans.

When Windows Update Service (`wuauserv`) builds the `datastore.edb` cache database, several gigabytes of memory need to be available to be committed. If not, this error can occur.



Systems running earlier versions of Windows Server 2016 are more prone to this error.

Solutions

- Set the page file to system managed.
  Review Microsoft documentation: How to determine the appropriate page file size for 64-bit versions of Windows. When using a dedicated logical disk for a system-managed paging file, the page file does not automatically grow beyond the size of the volume ÷ 8. For example, if a system is mounted with a 16 GB volume and a system-managed page file, the page file only expands to approximately 2 GB. In this situation, consider using a static page file or increasing the volume size to allow the page file to dynamically grow.
- If the system is undersized, increase the installed RAM or reduce memory from other applications.

© 2026 Tanium Inc. All Rights Reserved

Windows Update Manager timed out waiting for the Windows Update Service to reach a Stopped state

Cause

Tanium attempted to restart the Windows Update service prior to executing a Tanium Scan for Windows scan. This attempt timed out if the Windows Update service was busy performing an operation (likely unrelated to Tanium Patch) at the time Tanium attempted to restart the service.

Solutions

- Check the following Windows Update Agent logs to determine what invoked the operation (for example, automatic updates scan or WSUS):
  - `C:\Windows\Logs\WindowsUpdate`
  - `C:\Windows\WindowsUpdate.log`
- Use the **Patch - Reset Windows Update Client** package to reset Windows Update Agent.

Windows Update Error: -2145107951 WU_E_PT_SUS_SERVER_NOT_SET

Cause

Either the endpoint is running Windows 10 Home Edition, or else the registry value is not set for a WSUS scan.

Solutions

- Windows 10 Home Edition does not support Tanium Scan or WSUS scan. Contact Tanium Support on page 162 if you see this error in your environment.
- Use the **Registry Value Data** Tanium sensor to identify the values set on the endpoint. WSUS scans require the following registry values:
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\WUServer` with a value of *URL:port*. For example, `http://192.168.1.10:8530`
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU\UseWUServer` with a value of `1`

  To update the values on the endpoint, use the **Registry - Set Value** Tanium package. To add the key on the endpoint, use the **Registry - Create Key** Tanium package. Specify the `WUServer` registry value as a **REG_SZ** value type and the `UseWUServer` as a **REG_DWORD** value type. For more information, see Tanium Console User Guide: Managing packages.

  After the values are added to the endpoints, restart the Windows Update service for the changes to take effect.

© 2026 Tanium Inc. All Rights Reserved



Windows Group Policies overwrites these registry changes if a Group Policy object specifies an intranet server to host updates from Microsoft Update. For more information, see Microsoft Documentation: Configure Group Policy settings for automatic updates.

Linux: Could not get results

Cause

This error is likely caused by Patch tools not being installed on endpoints.

Solution

Verify that the Patch tools are installed on your Linux endpoints.

1. From the Main menu, go to **Modules > Patch > Overview**, click Settings and then click **Operating Systems** to verify that the **Enhanced Linux Support** option is enabled.
2. Verify that the Patch tools are installed on your Linux endpoints.
   If the Patch tools are not installed on your Linux endpoints, the **Endpoint Configuration - Tools Status** sensor returns `Not Installed for Patch`.

Linux: Failed to download `repomd.xml`

Cause

This error indicates that the Tanium Server cannot download the `repomd.xml` metadata file from the repository. The `repomd.xml` file is required for patch scanning.

Solution

Check for the following issues:

- For Red Hat endpoints, the Red Hat certificate has been improperly configured or has rotated or the subscription has expired. For more information, see Knowledge Article: Create a Red Hat certificate for Tanium downloads (login required).
- The repository has been decommissioned by the vendor (for example, CentOS 6).
- A firewall or proxy is interfering with communication between the Tanium Server and the remote repository.

Linux: Repo URLs found but unable to snapshot metadata files, likely due to connectivity issue

Cause

This error indicates that the Tanium Server cannot access the source repository for download.

© 2026 Tanium Inc. All Rights Reserved

Solutions

- Ensure that the Tanium Server can access the repository upstream URL.
- For Red Hat Enterprise Linux repositories, ensure that you have properly configured the Red Hat certificate. For more information, see (Red Hat endpoints) Configure Tanium Server to use certificate authentication on page 72.
- If the problem persists, Contact Tanium Support on page 162 for assistance. Provide logs from the time period during which the problem occurred. For more information, see Collect a troubleshooting package on page 148.

Linux: Selected repo <*repository_name*> is missing required Yum variables

Cause

This error indicates that Patch could not gather Yum variables for the operating system type of the selected repository. This issue might occur after you import a new version of Patch.

Solution

1. Ensure that the process is running on Linux endpoints. For more information, see Patch process is not running on Linux endpoints on page 152.
2. Re-create the Yum variables by clicking the Interact icon in the message.

Linux: Repo URLs were found but the snapshot could not be created, likely due to a Yum variable mismatch

Cause

This issue indicates that Patch could not resolve the listed Yum variables in the repository upstream URL.

Solution

1. Ensure that the Patch process is running on Linux endpoints. For more information, see Patch process is not running on Linux endpoints on page 152.
2. Ensure that custom Yum variables in the URL are accurate.
3. Ensure that you have defined the custom Yum variables on your Linux endpoints.
4. Reinitialize Patch, which runs the `Patch - Repository variables` sensor to gather Yum variables from Linux endpoints. For more information, see Initialize Patch on page 80. Alternatively, wait up to three hours for normal processing to gather the variables.

© 2026 Tanium Inc. All Rights Reserved

Reference: End-User Self Service sensors

Patch uses the following sensors for End-User Self Service activity. Use these sensors to help troubleshoot End-User Self Service issues.

Patch End-User Self Service sensors

Sensor	Description

Patch - Patch Downloads	Returns the status for Tanium file downloads initiated by Patch deployments, including deployments visible in the Self Service Client application.
	Example: `Deployment IDs|Tanium UID|Patch URL|Status`
	`1|09fa665904c554959b822222c203d444|https://path/to/patch/file|Complete`
	`2|fe320b179031f7b18942d0b4af98180f|https://path/to/patch/file|Requested`
	
	NOTE
	This sensor is also used by Patch for deployments that do not use the Self Service Client application.

Patch - Self Service Activity	Return the self service activity for deployments. By default, registered with Tanium Data Service.
Patch - Self Service Deployments	Return Patch self service deployments. By default, registered with Tanium Data Service.

© 2026 Tanium Inc. All Rights Reserved

Reference: Patch endpoint tools

Endpoint Configuration installs the following Patch tools on endpoints. Patch endpoint tools extend the functionality of Tanium Patch. You can check the status of these tools with the **Get Endpoint Configuration - Tools Status** sensor.

Patch endpoint tools

Tool	Description
7za	`<Tanium Client>\Tools\Patch` File archiver used for compressing patches.
active-user-sessions	`<Tanium Client>\Patch\tools` A utility used to detect if there is an active user session. If there is an active user session, End-User Notifications notifies the user or immediately reboots, depending on deployment configuration.
index-cx	`<Tanium Client>\extensions\index` Tanium Client Extension that runs Tanium Index. If an endpoint uses both Asset and Patch, Index must be installed for Patch on the endpoint. Index is not used by Patch but is a dependency of **swmgr-cx**. You can disable but not uninstall Index on Patch endpoints.
Patch	`<Tanium Client>\Patch\lib` The long-running Python Patch process.
Patch - Euss Tool Wrapper and **Tanium EUSS**	• `<Tanium Client>\Tools\EussToolWrapper` Euss Tool Wrapper installs End-User Self Service (EUSS) for Patch on Windows endpoints. The `version` file in this directory indicates the current version of EUSS required by Patch. NOTE Deploy and End-User Notifications use unique Euss Tool Wrappers to indicate the required EUSS versions for the solutions. Separate tool wrappers for each solution allow for independent solution installations and upgrades. • `<Tanium Client>\Tools\euss` EUSS code. When a user runs the Self Service Client, Tanium writes logs to `%localappdata%\tanium-end-user-self-service`.When a user clicks a Patch tile or deployment in Self Service, Tanium generates an activity file in `%localappdata%\tanium-end-user-self-service`. If you are uninstalling or reinstalling EUSS, generally target Tanium EUSS and not the wrapper. If you are using End-User Self Service and notifications, Patch also uses the **End-User Notifications** tool. For more information, see Tanium End-User Notifications User Guide: Reference: End-User Notifications tool.

© 2026 Tanium Inc. All Rights Reserved

Patch endpoint tools (continued)

Tool	Description
python38	`<Tanium Client>\python38` Provides TPython binary and libraries for endpoints with a toolset version earlier than 2.7. NOTE **python38** is also used by other Tanium solutions and is commonly found on endpoints managed using Tanium Client.
python312	`<Tanium Client>\python312` Provides TPython binary and libraries for endpoints with toolset 2.7 or later. NOTE **python312** is also used by other Tanium solutions and is commonly found on endpoints managed using Tanium Client.
TaniumExecWrapper	`<Tanium Client>\Patch\tools` Wrapper used to invoke child processes to enforce process timeouts and logging levels.
TaniumFileInfo	`<Tanium Client>\Patch\tools` Executable used to calculate the hashes of files on disk.
TaniumUpdateSearcher	`<Tanium Client>\Patch\tools` A utility to extract patch file download URLs from Windows Update Agent (WUA) results. This utility addresses Microsoft changes to the WUA API introduced in Windows 10, version 2004.
swmgr-cx (or Software Manager)	`<Tanium Client>\extensions\software_manager` Tanium Client extension that starts the Patch process. Software Manager is also used for Client Management Endpoint Must Gathers. NOTE Software Manager is also used by Deploy and Asset.

© 2026 Tanium Inc. All Rights Reserved

Reference: Gateway examples for Patch

Tanium™ Gateway provides a GraphQL API integration point for Tanium solutions. The following example query and mutation requests pertain to Patchfunctionality. You can use these examples as a reference to create custom GraphQL API requests for Patch integrations, data exports, and other related work. For additional Gateway example syntax, see Tanium Gateway User Guide: Reference: Filter syntax and Tanium Gateway User Guide: Reference: Gateway examples.

Patch query filter syntax

Patch queries to retrieve patch definitions support the following filter field:

- `cveIds`
- `classification`
- `hasCve`
- `isSuperseded`
- `platform`
- `product`
- `releasedOnOrBeforeDate`
- `releasedOnOrAfterDate`
- `severity`

For more information on syntax, see `patchDefinitionFieldFilter` in the **Documentation Explorer** pane of the query explorer.

CVE ID

You can filter patch definitions based on an associated CVE ID. Define a filter object using the syntax:

```
{cveIds: [cve-id]}
```



The filter supports one, and only one, CVE ID to filter the returned patch definitions.

For example, the following request filters and returns only patch definitions with a CVE ID of `CVE-2014-123456`:

```
query exampleGetPatchDefinitions ($first: Int, $filter: PatchDefinitionFieldFilter,
$sort:PatchDefinitionFieldSort) {
```

© 2026 Tanium Inc. All Rights Reserved

```
  patchDefinitions (first: $first, filter: $filter, sort: $sort) {
    edges {
      node {
        id
        createdDate
        cveIds
        isSuperseded
        platform
        releaseDate
        severity
        sizeInBytes
        title
      }
    }
    pageInfo {
      hasNextPage
      hasPreviousPage
      startCursor
      endCursor
    },
    totalRecords
  }
}
```

Include the pagination and filter variables in the **Variables** panel or in your variables dictionary:

```
{
  "first": 1,
  "filter": {"cveIds": ["CVE-2014-123456"]},
  "sort": {"field": "releaseDate", "order": "desc"}
}
```

Classification

You can filter patch definitions based on a patch definition classification. Define a filter object using the syntax:

© 2026 Tanium Inc. All Rights Reserved

```
{classification: classification-type}
```

For example, the following request filters and returns only patch definitions with a classification of `Security Updates`:

```
query exampleGetPatchDefinitions ($filter: PatchDefinitionFieldFilter,
$sort:PatchDefinitionFieldSort) {
  patchDefinitions (filter: $filter, sort: $sort) {
    edges {
      node {
        id
        createdDate
        classification
        cveIds
        isSuperseded
        platform
        releaseDate
        severity
        sizeInBytes
        title
      }
    }
    pageInfo {
      hasNextPage
      hasPreviousPage
      startCursor
      endCursor
    },
    totalRecords
  }
}
```

Include the pagination and filter variables in the **Variables** panel or in your variables dictionary:

```
{
  "filter": {"classification": ["Security Updates"]},
```

© 2026 Tanium Inc. All Rights Reserved

```
  "sort": {"field": "releaseDate", "order": "desc"}
}
```

Has association with any CVE

You can filter patch definitions based on whether the patch definition is associated with any CVE. Define a filter object using the syntax:

```
{hasCve: boolean-value}
```

For example, the following request filters and returns only patch definitions associated with any CVE:

```
query exampleGetPatchDefinitions ($filter: PatchDefinitionFieldFilter,
$sort:PatchDefinitionFieldSort) {
  patchDefinitions (filter: $filter, sort: $sort) {
    edges {
      node {
        id
        createdDate
        classification
        cveIds
        isSuperseded
        platform
        releaseDate
        severity
        sizeInBytes
        title
      }
    }
    pageInfo {
      hasNextPage
      hasPreviousPage
      startCursor
      endCursor
```

© 2026 Tanium Inc. All Rights Reserved

```
    },
    totalRecords
  }
}
```

Include the pagination and filter variables in the **Variables** panel or in your variables dictionary:

```
{
  "filter": {"hasCve": true},
  "sort": {"field": "releaseDate", "order": "desc"}
}
```

Is superseded by another patch definition

You can filter patch definitions based on whether the patch definition is superseded by another patch definition. Define a filter object using the syntax:

```
{isSuperseded: boolean-value}
```

For example, the following request filters and returns only patch definitions superseded by another patch definition:

```
query exampleGetPatchDefinitions ($filter: PatchDefinitionFieldFilter,
$sort:PatchDefinitionFieldSort) {
  patchDefinitions (filter: $filter, sort: $sort) {
    edges {
      node {
        id
        createdDate
        classification
        cveIds
        isSuperseded
        platform
        releaseDate
        severity
```

© 2026 Tanium Inc. All Rights Reserved

```
        sizeInBytes
        title
      }
    }
    pageInfo {
      hasNextPage
      hasPreviousPage
      startCursor
      endCursor
    },
    totalRecords
  }
}
```

Include the pagination and filter variables in the **Variables** panel or in your variables dictionary:

```
{
  "filter": {"isSuperseded": true},
  "sort": {"field": "releaseDate", "order": "desc"}
}
```

Operating System platform

You can filter patch definitions based on whether the patch definition applies to an operating system. Define a filter object using the syntax:

```
{platform: PatchEndpointPlatform-enum-value}
```

Supported values include `MACOS`, `LINUX`, and `WINDOWS`.

For example, the following request filters and returns only patch definitions that apply to Linux operating systems:

```
query exampleGetPatchDefinitions ($filter: PatchDefinitionFieldFilter,
$sort:PatchDefinitionFieldSort) {
  patchDefinitions (filter: $filter, sort: $sort) {
```

© 2026 Tanium Inc. All Rights Reserved

```
    edges {
      node {
        id
        createdDate
        classification
        cveIds
        isSuperseded
        platform
        releaseDate
        severity
        sizeInBytes
        title
      }
    }
    pageInfo {
      hasNextPage
      hasPreviousPage
      startCursor
      endCursor
    },
    totalRecords
  }
}
```

Include the pagination and filter variables in the **Variables** panel or in your variables dictionary:

```
{
  "filter": {"platform": "LINUX"},
  "sort": {"field": "releaseDate", "order": "desc"}
}
```

Product

You can filter patch definitions based on the product to which the patch definition applies to an operating system. Define a filter object using the syntax:

© 2026 Tanium Inc. All Rights Reserved

```
{product: product-name}
```

For example, the following request filters and returns only patch definitions for Windows Server 2019:

```
query exampleGetPatchDefinitions ($filter: PatchDefinitionFieldFilter,
$sort:PatchDefinitionFieldSort) {
  patchDefinitions (filter: $filter, sort: $sort) {
    edges {
      node {
        id
        createdDate
        classification
        cveIds
        isSuperseded
        platform
        releaseDate
        severity
        sizeInBytes
        title
      }
    }
    pageInfo {
      hasNextPage
      hasPreviousPage
      startCursor
      endCursor
    },
    totalRecords
  }
}
```

Include the pagination and filter variables in the **Variables** panel or in your variables dictionary:

```
{
  "filter": {"product": "Windows Server 2019"},
```

© 2026 Tanium Inc. All Rights Reserved

```
  "sort": {"field": "releaseDate", "order": "desc"}
}
```

Released on or before a date

You can filter patch definitions based on the patch definition release date occurring prior to or equal to a date in ISO 8601 format. Define a filter object using the syntax:

```
{releasedOnOrBeforeDate: iso-8601-date}
```

For example, the following request filters and returns only patch definitions released before or on December 31, 2020:

```
query exampleGetPatchDefinitions ($filter: PatchDefinitionFieldFilter,
$sort:PatchDefinitionFieldSort) {
  patchDefinitions (filter: $filter, sort: $sort) {
    edges {
      node {
        id
        createdDate
        classification
        cveIds
        isSuperseded
        platform
        releaseDate
        severity
        sizeInBytes
        title
      }
    }
    pageInfo {
      hasNextPage
      hasPreviousPage
      startCursor
      endCursor
```

© 2026 Tanium Inc. All Rights Reserved

```
    },
    totalRecords
  }
}
```

Include the pagination and filter variables in the **Variables** panel or in your variables dictionary:

```
{
  "filter": {"releasedOnOrBeforeDate": "2020-12-31"},
  "sort": {"field": "releaseDate", "order": "desc"}
}
```

Released on or after a date

You can filter patch definitions based on the patch definition release date occurring on or after a date in ISO 8601 format. Define a filter object using the syntax:

```
{releasedOnOrAfterDate: iso-8601-date}
```

For example, the following request filters and returns only patch definitions released on or after December 31, 2023:

```
query exampleGetPatchDefinitions ($filter: PatchDefinitionFieldFilter,
$sort:PatchDefinitionFieldSort) {
  patchDefinitions (filter: $filter, sort: $sort) {
    edges {
      node {
        id
        createdDate
        classification
        cveIds
        isSuperseded
        platform
        releaseDate
        severity
```

© 2026 Tanium Inc. All Rights Reserved

```
        sizeInBytes
        title
      }
    }
    pageInfo {
      hasNextPage
      hasPreviousPage
      startCursor
      endCursor
    },
    totalRecords
  }
}
```

Include the pagination and filter variables in the **Variables** panel or in your variables dictionary:

```
{
  "filter": {"releasedOnOrAfterDate": "2023-12-31"},
  "sort": {"field": "releaseDate", "order": "desc"}
}
```

Severity

You can filter patch definitions based on the patch definition severity. Define a filter object using the syntax:

```
{severity: severity-value}
```

The filter comparison is case-insensitive. Supported severity values include `critical`, `important`, `low`, `medium`, `moderate`, and `none`

For example, the following request filters and returns only patch definitions assigned a `medium` severity:

```
query exampleGetPatchDefinitions ($filter: PatchDefinitionFieldFilter,
$sort:PatchDefinitionFieldSort) {
  patchDefinitions (filter: $filter, sort: $sort) {
```

© 2026 Tanium Inc. All Rights Reserved

```
    edges {
      node {
        id
        createdDate
        classification
        cveIds
        isSuperseded
        platform
        releaseDate
        severity
        sizeInBytes
        title
      }
    }
    pageInfo {
      hasNextPage
      hasPreviousPage
      startCursor
      endCursor
    },
    totalRecords
  }
}
```

Include the pagination and filter variables in the **Variables** panel or in your variables dictionary:

```
{
  "filter": {"severity": "medium"},
  "sort": {"field": "releaseDate", "order": "desc"}
}
```

Patch examples

The following requests require Patch 3.16.191 or later and create, retrieve, and stop Patch deployments.

© 2026 Tanium Inc. All Rights Reserved

Create a Patch install deployment for Linux (`mutation.patchCreateDeployment`)

CREATE A LINUX PATCH DEPLOYMENT

The `patchCreateDeployment` mutation requires Patch 3.16.191 or later and the **Patch Deployment Write** and **Patch Deployment Execute** permissions.

> **NOTE**
>
> The `patchCreateDeployment` mutation does not support uploading images to pre-install and post-install user notifications.

The following mutation creates a new deployment for installing Linux patches on targeted endpoints.

```
mutation exampleCreateLinuxPatchDeployment($input: PatchCreateDeploymentInput!) {
  patchCreateDeployment(input: $input) {
    deployment {
      id
      author {
        id
        displayName
        username
      }
      contentDeploymentType
      contentSet {
        id
      }
      createdTime
      description
      downloadImmediately
      name
      notifications {
        postDeployment {
          body
          countdownToDeadline {
            nanoseconds
            seconds
          }
          notificationPeriodDuration {
```

© 2026 Tanium Inc. All Rights Reserved

```
            nanoseconds
            seconds
          }
          postponeOptions {
            durationOne {
              nanoseconds
              seconds
            }
            durationTwo {
              nanoseconds
              seconds
            }
            durationThree {
              nanoseconds
              seconds
            }
          }
          title
          translations {
            body
            languageCode
            title
          }
        }
      }
      overrideBlocklists
      patches {
        id
      }
      patchLists {
        id
        version
      }
      platform
```

© 2026 Tanium Inc. All Rights Reserved

```
      restart
      schedule {
        distributeOver {
          nanoseconds
          seconds
        }
        endTime
        eussAvailableBeforeStart
        eussHideFromActivity
        overrideMaintenanceWindows
        startTime
        timeZone
        type
      }
      status
      stoppedTime
      targets {
        computerGroups {
          id
        }
      }
      type
      updatedTime
    }
    error {
      message
      retryable
      timedOut
    }
  }
}

```

Include the input variables in the **Variables** panel or in your variables dictionary:

© 2026 Tanium Inc. All Rights Reserved

```
{
  "input": {
    "contentDeploymentType": "ALL_UPDATES",
    "contentSet": {
      "id": "123"
    },
    "description": "example Patch deployment for Linux",
    "downloadImmediately": true,
    "name": "example_deployment_linux",
    "overrideBlocklists": false,
    "patches": null,
    "patchLists": [
      {
        "id": "234",
        "version": 1
      }
    ],
    "platform": "LINUX",
    "restart": false,
    "schedule": {
      "distributeOver": {
        "seconds": 600
      },
      "endTime": "2025-02-01",
      "eussAvailableBeforeStart": false,
      "eussHideFromActivity": false,
      "overrideMaintenanceWindows": false,
      "startTime": "2025-01-01",
      "timeZone": "EST",
      "type": "SINGLE"
    },
    "targets": {
      "computerGroups": [
        {
```

© 2026 Tanium Inc. All Rights Reserved

```
          "id": "123"
        }
      ]
    },
    "type": "INSTALL"
  }
}
```

Example response:

```
{
  "data": {
    "patchCreateDeployment": {
      "deployment": {
        "id": "123",
        "author": {
          "id": "1",
          "displayName": null,
          "username": "Administrator"
        },
        "contentDeploymentType": "ALL_UPDATES",
        "contentSet": {
          "id": "123"
        },
        "createdTime": "2023-10-18T18:48:43.515Z",
        "description": "example Patch deployment for Linux",
        "downloadImmediately": true,
        "name": "example_deployment_linux",
        "notifications": null,
        "overrideBlocklists": false,
        "patches": [],
        "patchLists": [
          {
            "id": "234",
```

© 2026 Tanium Inc. All Rights Reserved

```
            "version": 1
          }
        ],
        "platform": "LINUX",
        "restart": false,
        "schedule": {
          "distributeOver": {
            "nanoseconds": 0,
            "seconds": 600
          },
          "endTime": "2025-02-01T00:00:00.000Z",
          "eussAvailableBeforeStart": false,
          "eussHideFromActivity": false,
          "overrideMaintenanceWindows": false,
          "startTime": "2025-01-01T00:00:00.000Z",
          "timeZone": "EST",
          "type": "SINGLE"
        },
        "status": "INACTIVE",
        "stoppedTime": null,
        "targets": {
          "computerGroups": [
            {
              "id": "123"
            }
          ]
        },
        "type": "INSTALL",
        "updatedTime": "2023-10-18T18:48:43.515Z"
      },
      "error": null
    }
  }
}
```


© 2026 Tanium Inc. All Rights Reserved

Create a Patch install deployment for Windows (`mutation.patchCreateDeployment`)

CREATE A WINDOWS PATCH DEPLOYMENT

The `patchCreateDeployment` mutation requires Patch 3.16.191 or later and the **Patch Deployment Write** and **Patch Deployment Execute** permissions.

> NOTE
>
> The `patchCreateDeployment` mutation does not support uploading images to pre-install and post-install user notifications.

The following mutation creates a new deployment for installing Windows patches on targeted endpoints.

> NOTE
>
> Set `mutation.patchCreateDeployment (input.type)` equal to `INSTALL` for a Windows patch install deployment, or `UNINSTALL` for a Windows patch uninstall deployment.

```
mutation exampleCreateWindowsPatchDeployment($input: PatchCreateDeploymentInput!) {
  patchCreateDeployment(input: $input) {
    deployment {
      id
      author {
        id
        displayName
        username
      }
      contentDeploymentType
      contentSet {
        id
      }
      createdTime
      description
      downloadImmediately
      name
      notifications {
        postDeployment {
          body
```

© 2026 Tanium Inc. All Rights Reserved

```
            countdownToDeadline {
              nanoseconds
              seconds
            }
            notificationPeriodDuration {
              nanoseconds
              seconds
            }
            postponeOptions {
              durationOne {
                nanoseconds
                seconds
              }
              durationTwo {
                nanoseconds
                seconds
              }
              durationThree {
                nanoseconds
                seconds
              }
            }
            title
            translations {
              body
              languageCode
              title
            }
          }
        }
        overrideBlocklists
        patches {
          id
        }
```

© 2026 Tanium Inc. All Rights Reserved

```
      patchLists {
        id
        version
      }
      platform
      restart
      schedule {
        distributeOver {
          nanoseconds
          seconds
        }
        endTime
        eussAvailableBeforeStart
        eussHideFromActivity
        overrideMaintenanceWindows
        startTime
        timeZone
        type
      }
      status
      stoppedTime
      targets {
        computerGroups {
          id
        }
      }
      type
      updatedTime
    }
    error {
      message
      retryable
      timedOut
    }
```

© 2026 Tanium Inc. All Rights Reserved

```
  }
}
```

Include the input variables in the **Variables** panel or in your variables dictionary:

```
{
  "input": {
    "contentDeploymentType": "MANUAL_SELECTION",
    "contentSet": {
      "id": "123"
    },
    "description": "example Patch deployment for Windows",
    "downloadImmediately": true,
    "name": "example_deployment_windows",
    "notifications": {
      "postDeployment": {
        "body": "example text display",
        "countdownToDeadline": {
          "seconds": 15
        },
        "notificationPeriodDuration": {
          "seconds": 1440
        },
        "postponeOptions": {
          "durationOne": {
            "seconds": 60
          },
          "durationTwo": {
            "seconds": 120
          },
          "durationThree": {
            "seconds": 240
          }
        },
```

© 2026 Tanium Inc. All Rights Reserved

```
        "title": "example title",
        "translations": [
          {
            "body": "ejemplo",
            "languageCode": "es",
            "title": "texto"
          }
        ]
      }
    },
    "overrideBlocklists": false,
    "patches": null,
    "patchLists": [
      {
        "id": "234",
        "version": 1
      }
    ],
    "platform": "WINDOWS",
    "restart": true,
    "schedule": {
      "distributeOver": {
        "seconds": 600
      },
      "endTime": null,
      "eussAvailableBeforeStart": false,
      "eussHideFromActivity": false,
      "overrideMaintenanceWindows": false,
      "startTime": "2025-01-01",
      "timeZone": "EST",
      "type": "ONGOING"
    },
    "targets": {
      "computerGroups": [
```

© 2026 Tanium Inc. All Rights Reserved

```
        {
          "id": "345"
        }
      ]
    },
    "type": "INSTALL"
  }
}
```

Example response:

```
{
  "data": {
    "patchCreateDeployment": {
      "deployment": {
        "id": "123",
        "author": {
          "id": "1",
          "displayName": null,
          "username": "admin"
        },
        "contentDeploymentType": "MANUAL_SELECTION",
        "contentSet": {
          "id": "123"
        },
        "createdTime": "2023-10-24T17:59:00.274Z",
        "description": "example Patch deployment for Windows",
        "downloadImmediately": true,
        "name": "example_deployment_windows",
        "notifications": {
          "postDeployment": {
            "body": "example text display",
            "countdownToDeadline": {
              "nanoseconds": 0,
```

© 2026 Tanium Inc. All Rights Reserved

```
            "seconds": 0
          },
          "notificationPeriodDuration": {
            "nanoseconds": 0,
            "seconds": 1440
          },
          "postponeOptions": {
            "durationOne": {
              "nanoseconds": 0,
              "seconds": 60
            },
            "durationTwo": {
              "nanoseconds": 0,
              "seconds": 120
            },
            "durationThree": {
              "nanoseconds": 0,
              "seconds": 240
            }
          },
          "title": "example title",
          "translations": [
            {
              "body": "ejemplo",
              "languageCode": "es",
              "title": "texto"
            }
          ]
        }
      },
      "overrideBlocklists": false,
      "patches": [],
      "patchLists": [
        {
```

© 2026 Tanium Inc. All Rights Reserved

```
            "id": "234",
            "version": 1
          }
        ],
        "platform": "WINDOWS",
        "restart": true,
        "schedule": {
          "distributeOver": {
            "nanoseconds": 0,
            "seconds": 600
          },
          "endTime": null,
          "eussAvailableBeforeStart": false,
          "eussHideFromActivity": false,
          "overrideMaintenanceWindows": false,
          "startTime": "2025-01-01T00:00:00.000Z",
          "timeZone": "EST",
          "type": "ONGOING"
        },
        "status": "INACTIVE",
        "stoppedTime": null,
        "targets": {
          "computerGroups": [
            {
              "id": "345"
            }
          ]
        },
        "type": "INSTALL",
        "updatedTime": "2023-10-24T17:59:00.274Z"
      },
      "error": null
    }
  }
}
```


© 2026 Tanium Inc. All Rights Reserved

Get Patch definitions (`query.patchDefinitions`)

GET MULTIPLE PATCH DEFINITIONS

The `patchDefinition` query requires Patch 3.17.175 or later and the **Patch Show** permission.

The following query retrieves the first patch definition that matches the specified CVE ID.



The filter supports one, and only one, CVE ID to filter the returned patch definitions.

```
query exampleGetPatchDefinitions($first: Int, $filter: PatchDefinitionFieldFilter,
$sort:PatchDefinitionFieldSort) {
  patchDefinitions(first: $first, filter: $filter, sort: $sort) {
    edges {
      node {
        id
        createdDate
        cveIds
        isSuperseded
        platform
        releaseDate
        severity
        sizeInBytes
        title
      }
    }
    pageInfo {
      hasNextPage
      hasPreviousPage
      startCursor
      endCursor
    },
    totalRecords
  }
}
```

Include the pagination and filter variables in the **Variables** panel or in your variables dictionary:

© 2026 Tanium Inc. All Rights Reserved

```
{
  "first": 1,
  "filter": {"cveIds": ["CVE-2014-123456"]},
  "sort": {"field": "releaseDate", "order": "desc"}
}
```

Example response:


```
{
  "data": {
    "patchDefinitions": {
      "edges": [
        {
          "node": {
            "id": "1234567890abcdef1234567890abcdef",
            "createdDate": "2021-04-20",
            "cveIds": [
              "CVE-2014-123456"
            ],
            "isSuperseded": false,
            "platform": "LINUX",
            "releaseDate": "2020-01-01",
            "severity": "Important",
            "sizeInBytes": 12345678,
            "title": "example patch definition"
          }
        }
      ],
      "pageInfo": {
        "hasNextPage": false,
        "hasPreviousPage": false,
        "startCursor":
"eyJpZCI6ImE4OWE0ZGFkZWY2YWU0YTAzZDBjYzY5NGFhZjg4MzMzIiwiY3JlYXRlZERhdGUiOiIyMDIxLTA0LTIwVDA
2OjAxOjQ2Ljg1MloiLCJyZWxlYXNlRGF0ZSI6IjIwMTItMDYtMThUMDA6MDA6MDAuMDAwWiJ9",
```


© 2026 Tanium Inc. All Rights Reserved

```
        "endCursor":
"eyJpZCI6ImE4OWE0ZGFkZWY2YWU0YTAzZDBjYzY5NGFhZjg4MzMzIiwiY3JlYXRlZERhdGUiOiIyMDIxLTA0LTIwVDA
2OjAxOjQ2Ljg1MloiLCJyZWxlYXNlRGF0ZSI6IjIwMTItMDYtMThUMDA6MDA6MDAuMDAwWiJ9"
      },
      "totalRecords": 1
    }
  }
}
```

Get a Patch deployment by ID (`query.patchDeployment`)

GET A PATCH DEPLOYMENT BY ID

The `patchDeployment` query requires Patch 3.16.191 or later and the **Patch Deployment Read** permission.

The following query retrieves the Patch deployment that matches the specified ID.

```
query examplgeGetPatchDeployment($id: ID!) {
  patchDeployment(ref: {id: $id}) {
    id
    author {
      id
      displayName
      username
    }
    contentDeploymentType
    contentSet {
      id
    }
    createdTime
    description
    downloadImmediately
    name
    notifications {
      postDeployment {
```

© 2026 Tanium Inc. All Rights Reserved

```
        body
        countdownToDeadline {
          nanoseconds
          seconds
        }
        notificationPeriodDuration {
          nanoseconds
          seconds
        }
        postponeOptions {
          durationOne {
            nanoseconds
            seconds
          }
          durationTwo {
            nanoseconds
            seconds
          }
          durationThree {
            nanoseconds
            seconds
          }
        }
        title
        translations {
          body
          languageCode
          title
        }
      }
    }
    overrideBlocklists
    patches {
      id
```

© 2026 Tanium Inc. All Rights Reserved

```
    }
    patchLists {
      id
      version
    }
    platform
    restart
    schedule {
      distributeOver {
        nanoseconds
        seconds
      }
      endTime
      eussAvailableBeforeStart
      eussHideFromActivity
      overrideMaintenanceWindows
      startTime
      timeZone
      type
    }
    status
    stoppedTime
    targets {
      computerGroups {
        id
      }
    }
    type
    updatedTime
  }
}
```

Include the ID variable in the **Variables** panel or in your variables dictionary:

© 2026 Tanium Inc. All Rights Reserved

```
{
  "id": "123"
}
```

Example response:

```
{
  "data": {
    "patchDeployment": {
      "id": "123",
      "author": {
        "id": "1",
        "displayName": null,
        "username": "Administrator"
      },
      "contentDeploymentType": "ALL_UPDATES",
      "contentSet": {
        "id": "123"
      },
      "createdTime": "2023-10-18T18:48:43.515Z",
      "description": "example Patch deployment for Linux",
      "downloadImmediately": true,
      "name": "example_deployment_linux",
      "notifications": null,
      "overrideBlocklists": false,
      "patches": [],
      "patchLists": [
        {
          "id": "234",
          "version": 1
        }
      ],
      "platform": "LINUX",
      "restart": false,
```

© 2026 Tanium Inc. All Rights Reserved

```
      "schedule": {
        "distributeOver": {
          "nanoseconds": 0,
          "seconds": 600
        },
        "endTime": "2025-02-01T00:00:00.000Z",
        "eussAvailableBeforeStart": false,
        "eussHideFromActivity": false,
        "overrideMaintenanceWindows": false,
        "startTime": "2025-01-01T00:00:00.000Z",
        "timeZone": "EST",
        "type": "SINGLE"
      },
      "status": "INACTIVE",
      "stoppedTime": null,
      "targets": {
        "computerGroups": [
          {
            "id": "1"
          }
        ]
      },
      "type": "INSTALL",
      "updatedTime": "2023-10-18T18:48:44.693Z"
    }
  }
}
```


Stop a Patch deployment by ID (`mutation.patchStopDeployment`)

STOP A PATCH DEPLOYMENT BY ID

The `patchStopDeployment` mutation requires Patch 3.16.191 or later and the **Patch Deployment** write and **Patch Deployment** execute permissions.

The following mutation updates a deployment that matches the ID `123`.

© 2026 Tanium Inc. All Rights Reserved

```
mutation exampleStopPatchDeployment($id: ID!) {
  patchStopDeployment(ref: {id: $id}) {
    deployment {
      id
      author {
        id
        displayName
        username
      }
      contentDeploymentType
      contentSet {
        id
      }
      createdTime
      description
      downloadImmediately
      name
      notifications {
        postDeployment {
          body
          countdownToDeadline {
            nanoseconds
            seconds
          }
          notificationPeriodDuration {
            nanoseconds
            seconds
          }
          postponeOptions {
            durationOne {
              nanoseconds
              seconds
            }
            durationTwo {
```

© 2026 Tanium Inc. All Rights Reserved

```
            nanoseconds
            seconds
          }
          durationThree {
            nanoseconds
            seconds
          }
        }
        title
        translations {
          body
          languageCode
          title
        }
      }
    }
    overrideBlocklists
    patches {
      id
    }
    patchLists {
      id
      version
    }
    platform
    restart
    schedule {
      distributeOver {
        nanoseconds
        seconds
      }
      endTime
      eussAvailableBeforeStart
      eussHideFromActivity
```

© 2026 Tanium Inc. All Rights Reserved

```
        overrideMaintenanceWindows
        startTime
        timeZone
        type
      }
      status
      stoppedTime
      targets {
        computerGroups {
          id
        }
      }
      type
      updatedTime
    }
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Include the ID variable in the **Variables** panel or in your variables dictionary:

```
{
  "id": "123"
}
```

Example response:

```
{
  "data": {
```

© 2026 Tanium Inc. All Rights Reserved

```
    "patchStopDeployment": {
      "deployment": {
        "id": "123",
        "author": {
          "id": "1",
          "displayName": null,
          "username": "Administrator"
        },
        "contentDeploymentType": "ALL_UPDATES",
        "contentSet": {
          "id": "123"
        },
        "createdTime": "2023-10-18T18:48:43.515Z",
        "description": "example Patch deployment for Linux",
        "downloadImmediately": true,
        "name": "example_deployment_linux",
        "notifications": null,
        "overrideBlocklists": false,
        "patches": null,
        "patchLists": [
          {
            "id": "234",
            "version": 1
          }
        ],
        "platform": "LINUX",
        "restart": false,
        "schedule": {
          "distributeOver": {
            "nanoseconds": 0,
            "seconds": 600
          },
          "endTime": "2025-02-01T00:00:00.000Z",
          "eussAvailableBeforeStart": false,
```


© 2026 Tanium Inc. All Rights Reserved

```
            "eussHideFromActivity": false,
            "overrideMaintenanceWindows": false,
            "startTime": "2025-01-01T00:00:00.000Z",
            "timeZone": "EST",
            "type": "SINGLE"
          },
          "status": "STOPPED",
          "stoppedTime": "2023-10-18T19:16:28.105Z",
          "targets": {
            "computerGroups": [
              {
                "id": "1"
              }
            ]
          },
          "type": "INSTALL",
          "updatedTime": "2023-10-18T19:16:28.123Z"
        },
        "error": null
      }
    }
}
```


Upsert (create or update by ID) a Patch patch list (`mutation.patchListUpsert`)

UPSERT (CREATE OR UPDATE BY ID) A PATCH LIST

The `patchListUpsert` mutation requires Patch 3.24.83 or later and the **Patch Patchlist execute** and **Patch Patchlist write** permissions.

The `patchListUpsert` mutation either creates a new patch list or updates the existing patch list that matches an ID.



Although you can manually select patches to include in a patch list, it is more efficient to use rules to dynamically populate lists of patches.

The following mutation creates a new Linux patch list. The list defines two rules:

© 2026 Tanium Inc. All Rights Reserved

- include all patches with "example" in the title
- include all critical severity patches released in the past seven days

```
mutation examplePatchListCreate($input: PatchListUpsertInput!) {
  patchListUpsert(input: $input) {
    patchList {
      id
      name
      author {
        id
        displayName
        username
      }
      contentSet {
        id
        description
        name
      }
      createdTime
      includeSupersededPatches
      isTaniumManaged
      patchDefinitionIDs
      platform
      rules {
        name
        conditions {
          comparisonOperator
          fieldName
          fieldValue
        }
      }
      updatedTime
      version
    }
    error {
```

© 2026 Tanium Inc. All Rights Reserved

```
      message
      retryable
      timedOut
    }
  }
}

```

Include the input variables in the **Variables** panel or in your variables dictionary:

```
{
  "input": {
    "name": "example_patch_list",
    "platform": "LINUX",
    "contentSet": {
      "id": "234"
    },
    "patchDefinitionIDs": [],
    "includeSupersededPatches": false,
    "rules": [
      {
        "name": "example_rule_1",
        "conditions": [
          {
            "fieldName": "TITLE",
            "comparisonOperator": "CONTAINS",
            "fieldValue": {
              "value": "example"
            }
          }
        ]
      },
      {
        "name": "example_rule_2",
```

© 2026 Tanium Inc. All Rights Reserved

```
        "conditions": [
          {
            "fieldName": "RELEASE_DATE",
            "comparisonOperator": "ON_OR_BEFORE_RELATIVE_DAYS",
            "fieldValue": {
              "releaseDateDaysAgo": 7
            }
          },
          {
            "fieldName": "SEVERITY",
            "comparisonOperator": "EQUALS",
            "fieldValue": {
              "severity": "CRITICAL"
            }
          }
        ]
      }
    ]
  }
}
```

Example response:

```
{
  "data": {
    "patchListUpsert": {
      "patchList": {
        "id": "123",
        "name": "example_patch_list",
        "author": {
          "id": "1",
          "displayName": null,
          "username": "admin"
        },
```

© 2026 Tanium Inc. All Rights Reserved

```
        "contentSet": {
          "id": "53",
          "description": "Default container for objects.",
          "name": "Patch Content Set"
        },
        "createdTime": "2025-02-03T14:24:43.327Z",
        "includeSupersededPatches": false,
        "isTaniumManaged": false,
        "patchDefinitionIDs": [],
        "platform": "LINUX",
        "rules": [
          {
            "name": "example_rule_1",
            "conditions": [
              {
                "comparisonOperator": "CONTAINS",
                "fieldName": "TITLE",
                "fieldValue": "example"
              }
            ]
          },
          {
            "name": "example_rule_2",
            "conditions": [
              {
                "comparisonOperator": "ON_OR_BEFORE_RELATIVE_DAYS",
                "fieldName": "RELEASE_DATE",
                "fieldValue": "7"
              },
              {
                "comparisonOperator": "EQUALS",
                "fieldName": "SEVERITY",
                "fieldValue": "CRITICAL"
              }
```


© 2026 Tanium Inc. All Rights Reserved

```
            ]
          }
        ],
        "updatedTime": "2025-02-03T14:24:43.370Z",
        "version": 1
      },
      "error": null
    }
  }
}
```

The following mutation updates the patch list with the ID `123`.

```
mutation examplePatchListUpdate($input: PatchListUpsertInput!) {
  patchListUpsert(input: $input) {
    patchList {
      id
      name
      author {
        id
        displayName
        username
      }
      contentSet {
        id
        description
        name
      }
      createdTime
      includeSupersededPatches
      isTaniumManaged
      patchDefinitionIDs
      platform
      rules {
```

© 2026 Tanium Inc. All Rights Reserved

```
        name
        conditions {
          comparisonOperator
          fieldName
          fieldValue
        }
      }
      updatedTime
      version
    }
    error {
      message
      retryable
      timedOut
    }
  }
}

```

Include the input variables in the **Variables** panel or in your variables dictionary:

```
{
  "input": {
    "id": "123",
    "name": "example_patch_list",
    "platform": "LINUX",
    "contentSet": {
      "id": "234"
    },
    "patchDefinitionIDs": [],
    "includeSupersededPatches": false,
    "rules": [
      {
        "name": "example_rule_1",
```

© 2026 Tanium Inc. All Rights Reserved

```
        "conditions": [
          {
            "fieldName": "TITLE",
            "comparisonOperator": "CONTAINS",
            "fieldValue": {
              "value": "example"
            }
          }
        ]
      }
    ]
  }
}
```

Example response:

```
{
  "data": {
    "patchListUpsert": {
      "patchList": {
        "id": "123",
        "name": "example_patch_list",
        "author": {
          "id": "1",
          "displayName": null,
          "username": "admin"
        },
        "contentSet": {
          "id": "53",
          "description": "Default container for objects.",
          "name": "Patch Content Set"
        },
        "createdTime": "2025-02-03T14:24:43.327Z",
        "includeSupersededPatches": false,
```

© 2026 Tanium Inc. All Rights Reserved

```
          "isTaniumManaged": false,
          "patchDefinitionIDs": [],
          "platform": "LINUX",
          "rules": [
            {
              "name": "example_rule_1",
              "conditions": [
                {
                  "comparisonOperator": "CONTAINS",
                  "fieldName": "TITLE",
                  "fieldValue": "example"
                }
              ]
            }
          ],
          "updatedTime": "2025-02-03T14:24:43.370Z",
          "version": 1
        },
        "error": null
      }
    }
}
```


© 2026 Tanium Inc. All Rights Reserved