Tanium Enforce User Guide

2026H2 Semiannual Release

Version 3.1

November 24, 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 servicesprovided 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

©2026 Tanium Inc. All Rights Reserved

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 atsupport@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 the irrespective owners.

Kubernetes®, K8s®, and the Kubernetes logo are registered trademarks of The Linux Foundation®.

Android, ChromeOS, and Google are trademarks of Google LLC.

iOS, iPad, iPadOS, iPhone, 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

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

© 2026 Tanium Inc. All rights reserved.

Table of contents

Overview 13
- Policies 13
- Device Actions 16
- Enforcements 17
- Interoperability with other Tanium products 19

Gaining organizational effectiveness 21

Requirements 28
- Core platform dependencies 28
- Solution dependencies 28
  - Tanium recommended installation 29
  - Import specific solutions 29
  - Required dependencies 29
  - Feature-specific dependencies 30
- Client extensions and endpoint tools 31
- Tanium™ Module Server 31
- Endpoints 31
- Host and network security requirements 38
  - Required ports 38
  - Ports for Enforce communication 38
  - Security exclusions 39
    - Enforce endpoint exclusions 40
    - Enforce server exclusions 42
  - Third-party internet URLs 43
- User role requirements 44
  - Create custom roles to only allow access to policies associated with a specific content set ... 63

Installing 65
- Before you begin 65

©2026 Tanium Inc. All Rights Reserved

Import Enforce with default settings 66
Default settings for Enforce 66
Import Enforce with custom settings 66
Manage solution dependencies 66
Upgrade Enforce 67
Verify Enforce version 67

Configuring 68
Manage solution configurations with Tanium Endpoint Configuration 68
Configure Enforce 69
Configure Enforce action group 69
Set up Enforce users 70

Getting started with policies 74
Configure Distribute Over Time settings for policies 74
Manage cluster policies 75
Install and configure Cloud Workloads 75
Configure settings for cluster policy enforcements 75
Manage anti-malware settings 76
Windows Defender platform updates 76
Enable Defender platform updates 78
Windows Defender definition updates 78
Action Lock Override 80
Distribute Over Time 80
Reissue Action Interval 81
Configure URLs for platform updates and definitions 81
Configure default rules for AppLocker 82
Create Default AppLocker rules 84
Configure endpoint encryption 88
Install Shared Services and endpoint tools 88
Manage Windows device classes and devices 89
Manage Stream profiles 91
Create a Stream profile 91
Prioritize Stream profiles 93
Take actions on Stream profiles 94
Next steps 94

©2026 Tanium Inc. All Rights Reserved

Create policies 94
Enforcements 94

Creating policies for Windows endpoints 96
AppLocker 98
BitLocker 103
Device Control - All Devices 110
Device Control - Removable Storage 113
Windows firewall management 114
Machine administrative template 117
SRP Management 124
Security Settings 125
Tanium Removable Storage Access Control 129
User Administrative Template 130

Creating policies for macOS endpoints 136

Creating policies for Linux endpoints 139

Creating policies for Kubernetes clusters 142
Create an Allow External Services by IP policy 142
Create an Allow Images by Registry policy 144
Create an Allow Ingress Actions by Hostname policy 146
Create a Block Images by Registry policy 148
Create a Block Images by Tag policy 150
Create a Block Resources by Version policy 152
Create a Block Rogue Containers policy 154
Create a Custom OPA policy 156

Managing policies 159
(Windows) Importing policies from a Group Policy backup 159
Import policies 160
Export policies 160
Prioritize policies 161

Enforcing policies 163
Applying policy settings on endpoints 163
Scheduled actions 165

©2026 Tanium Inc. All Rights Reserved

API or CLI 165
Create enforcements 165
Create an enforcement for a remediation policy 165
Create an enforcement for a cluster policy 165
Create an enforcement for all other types of policies 166
Create an enforcement from an individual policy 166
Complete the enforcement creation 167
Complete the enforcement creation for a cluster policy 169
View enforcements 171
Filter results 172
View endpoint details 173
Remove an enforcement 175

Managing device actions 176
Create a remediation policy 176
Remediation policy file pattern matching examples 178
Managing remediation policies 179
View remediation policies 179
Edit remediation policies 180
Delete remediation policies 180
Duplicate remediation policies 181
Export remediation policies 181
Import remediation policies 181
Viewing remediation policy details, results, and enforcements 182
Details 182
Results 183
Enforcements 185

Restricting policy visibility 187
Overview 187
Create a content set for a functional group 187
Create a role to assign to a user or user group 187
Create a policy 190

Using best practices with policies 191
Content sets 191

©2026 Tanium Inc. All Rights Reserved

Anti-malware policies 191
AppLocker policies workflow 191
Example workflow using default Allow List Rule Template 191
Firewall rules 192
SRP management rules 192
Role-based access control and configuration visibility 193

Scanning for anti-malware on-demand 194
Configure scans 194
View scan details 196
Required access rights 196
View the scan details 196
Filtering 197
View scan results 197
Required access rights 197
Merge 198
Drill down 198
Take action on a threat 199
Copy results 199
Export results 199
Manage quarantined files 200
View threats detected on endpoints 200
Restore all files quarantined at the same time for the same threat 201
Restore all quarantined files on a single endpoint 202
Restore all quarantined files on all endpoints 203
Check health 203

Maintaining 204
Enforce monthly maintenance 204
Monitor and troubleshoot Enforce coverage status (% of total) 204
Monitor and troubleshoot policy enforcement status (% of total) 205
Monitor and troubleshoot host firewall status on endpoints 205
Monitor and troubleshoot disk encryption status on endpoints 205
Monitor and troubleshoot antivirus status on endpoints 206

Troubleshooting 207
Collect logs 207

©2026 Tanium Inc. All Rights Reserved

Enforce Logs 207
Endpoint Logs 207
Update default log level 208
Review AppLocker event logs 208
Use Enforce sensors 209
Resolve Active Directory policy conflicts 211
Review policy settings when Windows Defender tamper protection is enabled 213
Review the status for policy settings on Windows endpoints 214
Regenerate the Key Encryption Key to align with security best practices 215
"Access is Denied" error when attempting to manually encrypt a removable drive 215
Translate encryption method values in an exported BitLocker policy 216
Verify endpoint tools 216
Identify and resolve issues with Client Extensions 216
Review the Extensions log for an endpoint 219
Remove Enforce tools from endpoints 219
Uninstall Enforce 221
Disable and remove Enforce firewall policies 221
Contact Tanium Support 222

Reference: Windows encryption management 223
Endpoint requirements 223
Configuration requirements 223
Generate the Key Encryption Key 224
Create a database to store the recovery keys 224
Install the End-User Notifications service and initialize endpoints 225
Install and configure Direct Connect 225
(Optional) Install and configure the encryption key recovery portal 225
Create and enforce the encryption management policy 225
Endpoint workflow 226
Prepare the drive for encryption 226
Configure the PIN or password 226
Encryption occurs 227
Behavior at subsequent starts or restarts 227
User forgets the PIN or password 227
Prompt the user to reset their PIN or password 227

©2026 Tanium Inc. All Rights Reserved

Suspend and resume BitLocker 228
Remove BitLocker encryption from an endpoint 228
Managing recovery keys 229
View BitLocker recovery keys 230
Retrieve a single recovery key 230
Export all recovery keys and the recovery keys access log 230
Rotate a recovery key 231
BitLocker encryption method values in exported policies 232
encryptionMethod 232
encryptionMethodNoDiffuser 232
encryptionMethodWithXtsOs 232

Reference: macOS encryption management 234
Endpoint requirements 234
Configuration requirements 234
Generate the Key Encryption Key 234
Create a database to store the recovery keys 235
Install the End-User Notifications service and initialize endpoints 235
Install and configure Direct Connect 236
(Optional) Install and configure the recovery portal 236
Create and enforce the encryption management policy 236
Endpoint workflow 236
Prepare the drive for encryption 236
Encryption occurs 237
User forgets the password 237
Remove FileVault encryption from an endpoint 237
Managing recovery keys 237
View FileVault recovery keys 238
Retrieve a single recovery key 238
Export all recovery keys and the recovery keys access log 239
Rotate a recovery key 239

Reference: Encryption key recovery portal 241
Requirements 241
Before you begin 243
Solution configuration 243

©2026 Tanium Inc. All Rights Reserved

DNS configuration 243
Obtain or create SSL certificates 243
Create a Tanium persona or user and API token 244
Tanium persona or user 244
API token 244
Note details about your configuration 245
(Microsoft Entra) Create a Microsoft Entra enterprise application and configure an identity provider 245
Create an enterprise application 245
Assign users or groups to the enterprise application 247
Set up the Identity Provider and SSO 249
Part 1: Configure the initial IdP Settings in Enforce 249
Part 2: Configure the IdP settings in Microsoft Entra 250
Part 3: Complete the IdP settings in Enforce 251
(Other Identity Providers) Set up an identity provider and SSO 252
Prerequisites 252
Configure the recovery portal 252
(Windows) Install and configure the recovery portal 254
(Linux) Install and configure the recovery portal 255
Add or update IdP providers 257
Replace the SSL certificates 258
Windows 258
Linux 258
Update the recovery portal 259
Uninstall the recovery portal 259
End user self-service workflow 259

Reference: Creating a self-hosted database to store recovery keys 262
Step 1: Create the database 263
PostgreSQL 263
Microsoft SQL 264
Step 2: Configure the required permissions for the database service account 264
PostgreSQL 264
Option 1: Simplified permissions 264
Option 2: More restrictive permissions 265
Microsoft SQL 266

©2026 Tanium Inc. All Rights Reserved

Option 1: Simplified permissions (Database Owner SA Auth) 266
Option 2: Best practice - Windows Authentication (Domain Account) 266
Option 3: More restrictive specific permissions (SA Auth) 267
Step 3: Configure the database connection in Enforce 268

©2026 Tanium Inc. All Rights Reserved

Enforce Overview

Enforce enables unified endpoint management and security by providing centralized policy management across operating system, application, and security for Windows, Linux, and macOS endpoints regardless of the endpoint location: on-premises, remote, or cloud.

Policies

Configure policies to manage and secure endpoints across environments by providing control and visibility to all devices. Policies contain *policy settings*, which are specific settings and controls contained within the policy.

Policy types for Windows endpoints

You can configure one or more of the following policy types in a single policy for Windows endpoints.

AppLocker

Use AppLocker policies to prevent unwanted executables from running on your endpoints (Deny rules) or to allow only certain applications to run on endpoints (Allow rules).

BitLocker

Use BitLocker policies to encrypt drives on endpoints using Windows BitLocker Drive Encryption.

Device Control - All Devices

Use Device Control - All Devices policies to restrict the installation of new devices. With this policy type, the installation of any new device is blocked unless the device is explicitly allowed by either the device class or the hardware ID of the device.

Device Control - Removable Storage

Use Device Control - Removable Storage policies to control access permissions to specific removable media categories. The types of removable media predefined by Microsoft are CD-ROM and DVD drives, floppy disk drives, removable disk drives, tape drives, and Windows Portable Devices (WPD).

©2026 Tanium Inc. All Rights Reserved

Firewall Management - Windows

Use Firewall Management policies to configure rules that block or allow network traffic using the built-in operating system firewall.

Machine Administrative Templates

Use Machine Administrative Templates policies to target machine-based Active Directory administrative template (ADMX) group policy objects on Windows systems. With these policies, you can apply consistent rules to Windows devices regardless of the logged-in user.



Note: The following Microsoft packages are used in Windows administrative template policies: Windows 11 baseline, Windows Server 2025 ADMX templates (October 2025 release), Google Chrome, MS Office, Microsoft Edge, and Windows Security Baseline ADMX files (MSS-legacy and SecGuide).

Security Settings

Use Security Settings policies to protect endpoints from malicious threats using Windows operating system security settings.

Software Restriction Policy (SRP) Management

Use SRPs to configure rules created using the Windows SRP component that block the execution of applications.

Tanium Removable Storage Access Control

Use Tanium Removable Storage Access Control policies to block access for USB storage devices by default and provide configurable exception rules to allow access for specific devices.

User Administrative Templates

Use User Administrative Templates policies to target user-based Active Directory administrative template (ADMX) group policy objects on Windows systems. With these policies, you can apply consistent rules to Windows users. When a user signs in to an endpoint where a User Administrative Template policy is enforced, the settings in the policy apply to that user on that endpoint. The policy applies to every user that signs in to the endpoint where the policy is enforced.

©2026 Tanium Inc. All Rights Reserved

> **Note:** The following Microsoft packages are used in Windows administrative template policies: Windows 11 security baseline package (25H2), MS Office, Google Chrome (137.0.7151 build 120), Windows Security Baseline (MSS-legacy and SecGuide), Mozilla Firefox, OneDrive (build 20.201.1005.0009), and Microsoft Edge (Chromium) ADMX files.

For more information, see Creating policies for Windows endpoints on page 96.

Creating policies from a Group Policy backup

You can import a Windows Group Policy backup and automatically create a policy with the configuration required for endpoint compliance. This powerful migration toolset eliminates weeks of manual policy recreation and allows you to import industry standards like the Center for Information Security (CIS) Build Kits or the Microsoft Security Baselines. For more information, see (Windows) Importing policies from a Group Policy backup on page 159.

macOS policy types

FileVault Policy

Use FileVault policies to encrypt drives on endpoints using macOS FileVault Encryption. For more information, see Creating policies for macOS endpoints on page 136.

Linux policy types

Firewall Management - Windows and Linux

Use Firewall Management policies to configure rules that block or allow network traffic using the built-in operating system firewall. For more information, see Creating policies for Linux endpoints on page 139.

Kubernetes policy types

Use cluster policies to manage images and resources for Kubernetes clusters. Cluster policies are available only when Cloud Workloads is installed and configured and the Tanium Client images are deployed to the targeted cluster. For more information, see Manage cluster policies on page 75.

©2026 Tanium Inc. All Rights Reserved

Allow External Services by IP

Use **Allow External Services by IP** policies to allow external services that have any of the specified IP addresses.

Allow Images by Registry

Use **Allow Images by Registry** policies to select specific registries that should be allowed for use in the cluster.

Allow Ingress Actions by Hostname

Use **Allow ingress actions by Hostname** policies to specify the hostnames that are allowed when creating ingress resources in the cluster.

Block Images by Registry

Use **Block Images by Registry** policies to block images that are included in the set of selected registries.

Block Images by Tag

Use **Block Images by Tag** policies to block any images that have any of the specified image tags.

Block Resources by Version

Use **Block Resources by Version** policies to block the creation of out-of-date APIs.

Block Rogue Containers

Use **Block Rogue Containers** policies to block any images that are not from the list of trusted registries configured in Cloud Workloads.

Custom OPA

Use **Custom OPA** policies to provide a block of Rego code to configure custom Open Policy Agent (OPA) policies.

For more information, see Creating policies for Kubernetes clusters on page 142.

Device Actions

©2026 Tanium Inc. All Rights Reserved

Remediations

Use remediations to configure a set of tasks that run sequentially on endpoints. You can configure the following actions using a remediation:

- Windows
  - Delete file
  - Delete registry key
  - Edit registry data
  - Kill process
  - Run service action
  - Run service configuration
  - Update registry value
- macOS
  - Delete file
  - Kill process
  - Run service action
- Linux
  - Delete file
  - Kill process
  - Run service action

For more information, see Managing device actions on page 176.

Enforcements

Create an enforcement for a policy to apply it to a computer or user group. Policies can have one of

©2026 Tanium Inc. All Rights Reserved

these enforcement states:

Applied

The policy was successfully enforced. All rules and configurations of the policy are in effect on the targeted endpoint.

> **Note:** If *all* settings in one policy are duplicates of *all* settings in another policy, both policies are shown as applied even though only the policy with the lowest priority number is applied.

Partially applied

Some of the policy settings were enforced and some were not. This status can occur when similar policies with one or more duplicate settings take precedence. When some settings are duplicated across different policies, the settings from the policy with the highest priority are applied and the settings from policies with lower priorities are not applied. This scenario results in the enforcement of some settings from a policy while other settings in the same policy are not enforced. For more information about policy priorities, see Prioritize policies on page 161.

Superseded

The legacy policy is not in effect on the endpoint because an equivalent next-generation policy supersedes it. This status applies to legacy policies (BitLocker or Windows Firewall) when a next-generation policy of the same type is enforced on the same endpoint. Next-generation policies supersede legacy policies regardless of policy priority. Saved filters, audit reports, or sensor questions that match on **Not applied** for this scenario now match **Superseded** instead.

Not applied

The policy is not in effect on the endpoint. This status can occur due to a timing issue if the policy was sent to the endpoint but not yet executed on that endpoint. See the enforcement state reason for more information.

Unsupported

An unsupported status might be due to a policy being applied to an operating system that does not support the policy settings.

©2026 Tanium Inc. All Rights Reserved

Error

All known and unknown errors.

Interoperability with other Tanium products

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

Tanium™ Cloud Workloads

Use Cloud Workloads to extend your visibility into Kubernetes clusters and create cluster policies in Enforce to manage the images and resources. For more information, see Cloud Workloads User Guide: Overview and Creating policies for Kubernetes clusters on page 142.

Tanium™ Guide

Tanium Guide can generate Enforce-related notifications for Tanium operators, which provide insight into Tanium, network, and endpoint performance.

For more information, see Tanium Guide User Guide: Overview.

Tanium™ Reporting

The **Enforce Overview** page uses charts to visualize data that Tanium™ Reporting provides through reports. For more information, see Tanium Reporting User Guide: Working with reports.

Enforce provides access to the Endpoint Details page in Tanium™ Reporting to view enhanced endpoint details in enforcements. In the **Endpoints** section on the enforcement details page, click Endpoint Details . Click **View Details** to open the endpoint details in Reporting. For more information, see View endpoint details on page 173 and Reporting User Guide: View endpoint details.

Tanium™ Threat Response

Use Threat Response findings to create process and network rule policies for Windows endpoints in Enforce to prevent future incidents across the network. Failing to identify and address fundamental vulnerabilities exploited during an incident leaves the organization with no net improvement to their security posture.

©2026 Tanium Inc. All Rights Reserved

For more information, see Tanium Threat Response User Guide: Remediate alerts in Tanium Protect or Tanium Enforce.

©2026 Tanium Inc. All Rights Reserved

Gaining organizational effectiveness with Enforce

There are four key organizational governance steps to maximizing the value delivered by Tanium Enforce to enable time to value:

- Develop a dedicated change management process. For more information, see Change management on page 21.
- Define distinct roles and responsibilities. For more information, see RACI chart on page 22.
- Validate cross-functional alignment. For more information, see Organizational alignment on page 23.
- Track operational maturity. For more information, see Benchmark metrics on page 24.

Change management

Develop a tailored, dedicated change management process to create a streamlined process around configuration and compliance policy management across endpoints with one console.

- Update SLAs and align activities to key resources for Tanium Enforce activities across configuration and compliance policy management processes. For more information, see RACI chart on page 22.
- Designate change or maintenance windows for various activities across configuration and compliance policy management scenarios. For example, implement a new firewall rule or endpoint hardening policy.
- Identify internal and external dependencies to your configuration and compliance policy management process. For example, compliance with standards such as SLAs or with PCI or HIPAA.
- Create a Tanium Steering Group (TSG) for discovery activities to expedite reviews and approvals of processes that align with SLAs.

©2026 Tanium Inc. All Rights Reserved

RACI chart

A RACI chart identifies the team or resource who is Responsible, Accountable, Consulted, and Informed, 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 the Tanium point of view for how organizations align functional resources across configuration and compliance policy management. Use the following table as a baseline example.

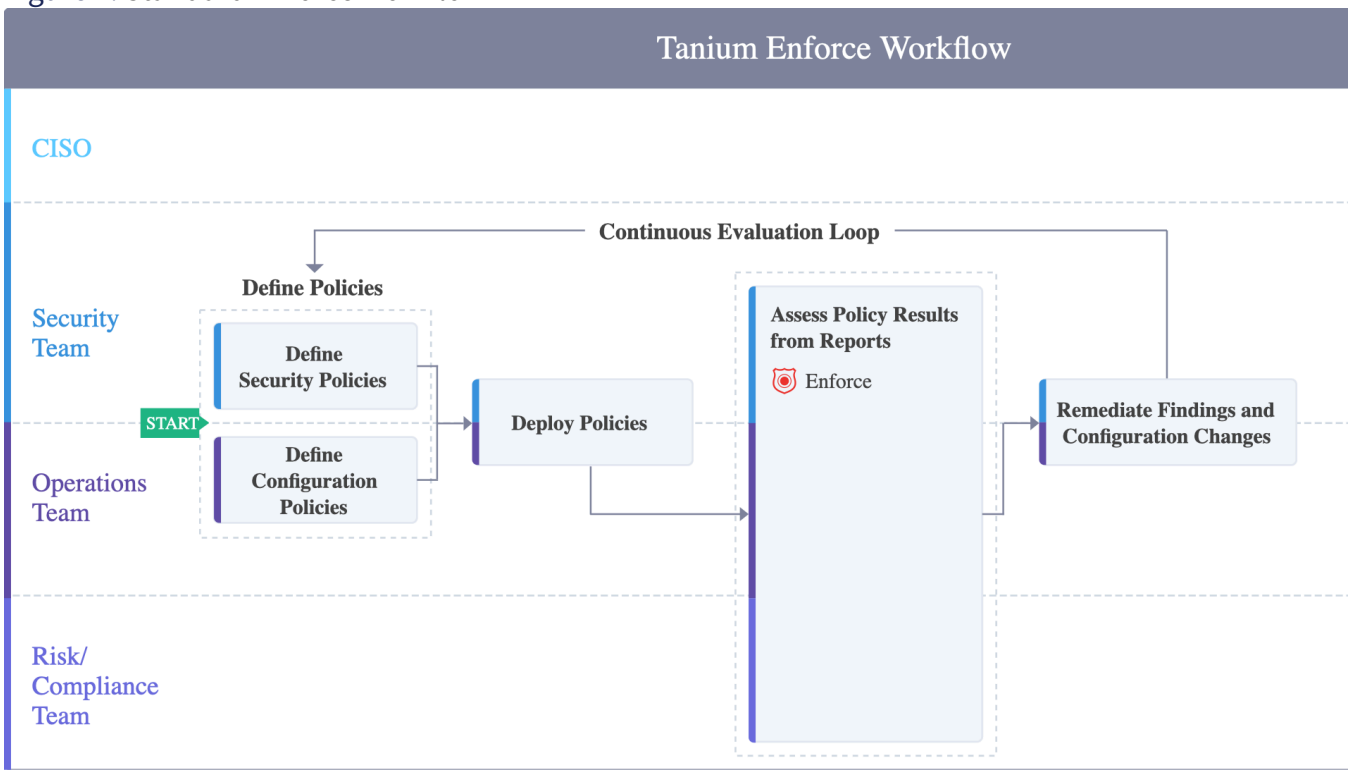
RACI chart for Enforce

Task	Security Team	Operations Team	Risk/ Compliance Team	Rationale
Define Policies: Define Security Policies	A/R	I	I	Security team creates security policies. For example, firewall policies, anti-malware policies, and end-state computer security settings.
Define Policies: Define Configuration Policies	I	A/R	I	Operations team creates configuration policies. For example, application settings, browser settings, operating system look-and-feel/system settings.
Deploy Policies	A/R	A/R	I	The targets created in the security and configuration policies are then configured in Tanium Enforce and policies are deployed to defined targets.
Assess Results of Policies Using Reports	A/R	A/R	A/R	Using Tanium Enforce, review the workbench/Reporting dashboards of policy results for assessment and remediation of any findings or need for configuration changes.
Remediate	A/R	A/R	I	Using the output of the results, action through remediation of

©2026 Tanium Inc. All Rights Reserved

Task	Security Team	Operations Team	Risk/ Compliance Team	Rationale
Findings and Configuration Changes				findings and configuration changes. For example, change targets, revise policy configuration errors, and then the workflow proceeds in a continuous loop.

Figure 1. Standard Enforce 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 on how to manage software and hardware assets.

©2026 Tanium Inc. All Rights Reserved

Operational metrics

Enforce maturity

Managing a configuration and compliance policy management 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 Enforce program are as follows:

Processes to measure Enforce maturity

Process	Description
Usage	How and when is Tanium Enforce used in your organization (for example, Is Tanium the sole tool or is it being supplemented by a legacy tool, such as Active Directory Group Policy?)
Automation	How automated is Tanium Enforce, and how well is it leveraged in automation of other systems
Functional Integration	How integrated Tanium Enforce is, across IT security, operations, compliance/risk, and asset management teams
Reporting	How is data from Tanium Enforce consumed by people and systems within the organization

Benchmark metrics

In addition to the key configuration and compliance policy management processes, the three key benchmark metrics that align to the operational maturity of the Tanium Enforce program to achieve maximum value and success are as follows:

Benchmark metrics for Enforce maturity

Value Metric	Value Metric #1	Value Metric #2	Value Metric #3	Value Metric #4	Value Metric #5
Metric Title	Enforce Coverage	Policy Enforcements (% of	Host firewall enabled	Disk Encryption Enabled	Antivirus Enabled

©2026 Tanium Inc. All Rights Reserved

Value Metric	Value Metric #1	Value Metric #2	Value Metric #3	Value Metric #4	Value Metric #5
	(% of total)	total)			
Why this metric matters	Provides visibility into the number of systems managed by Enforce	Provides visibility of policy health across enterprise. Enforcement errors or unenforced endpoints introduce risk to the environment.	Provides visibility of host firewall status across enterprise. Endpoints that do not have a host firewall installed and enabled introduce risk to the environment.	Provides visibility of hard drive encryption status across enterprise. Unencrypted endpoints introduce risk to the environment.	Provides visibility of Antivirus status across enterprise. Endpoints that do not have an antivirus agent installed and enabled introduce risk to the environment.
Instrumentation	Tools sensor	Enforce policy status (per policy type) / managed endpoints.	Enforce - Host firewall is enabled (Sensor)	View **Encryption Health** in Enforce. From the Main menu, go to **Modules** > **Enforce** > **Endpoint Encryption** > **Overview** .	Enforce - Antivirus Is Enabled (Sensor)

Maturity workflow

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

©2026 Tanium Inc. All Rights Reserved

Maturity levels for Enforce

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
Process	Usage	Enforce imported/ native OS, application, and security policies configured/ policies are enforced through legacy means	Policies are applied and verified	Policies for control group of desktops/ servers are implemented	For end user/ desktop endpoint, team is using Enforce to push policy configurations to endpoints and enforce them for all managed technologies	Implementation across all capable operating systems
	Automation	Manual	Policies are reapplied automatically	Policies are reapplied automatically	Policies are reapplied automatically	Policies are reapplied automatically; enforcement of the policies across all capable operating systems
	Functional integration	Native controls are integrated as applicable (for example, Defender, Firewall, AppLocker, BitLocker, FileVault and AD Group Policy)	Native controls are integrated as applicable (for example, Defender, Firewall, AppLocker, BitLocker, FileVault and AD Group Policy)	Native controls are integrated as applicable (for example, Defender, Firewall, AppLocker, BitLocker, FileVault and AD Group Policy/Remediation policies for file and service operations integrated)	Native controls are integrated as applicable (for example, Defender, Firewall, AppLocker, BitLocker, FileVault and AD Group/ Remediation policies for file and service operations	Remediation policies for file and service operations integrated

©2026 Tanium Inc. All Rights Reserved

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
					integrated)	
	Reporting	Manual; via Enforce workbench / for operators only	Manual; Enforce integration with native tools to export reports	Automated; Tanium Reporting for operators / peer group only	Automated; Tanium Reporting tailored to stakeholders ranging from Operator to Executive	Automated; Tanium Reporting tailored to stakeholders ranging from Operator to Executive
Metrics	Verified enforcement per policy (% of total enforcements vs. enforcement errors)	0-69%	70-79%	80-89%	90-98%	99-100%
	% of hosts with firewall enabled	0-69%	70-79%	80-89%	90-98%	99-100%
	% of hosts with disk encryption enabled	0-69%	70-79%	80-89%	90-98%	99-100%
	% of hosts with antivirus enabled	0-69%	70-79%	80-89%	90-98%	99-100%

©2026 Tanium Inc. All Rights Reserved

Enforce requirements

Review the requirements before you install and use Enforce.

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium license that includes Enforce. For more information about how to get Enforce, see Tanium Solutions & BundlesTanium Solutions & Bundles.
- Tanium™ Core Platform server
- Tanium™ Client: Any supported version of Tanium Client. For more information about the Tanium Client versions supported for each operating system, 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.

Solution dependencies

Other Tanium solutions are required for Enforce to function (required dependencies) or for specific Enforce 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.

©2026 Tanium Inc. All Rights Reserved

Note: Some Enforce dependencies have their own dependencies, which you can see in the lists of required and feature-specific dependencies below. Where a dependency links to its own user guide, that link opens the guide for the latest version of the solution, not necessarily the minimum version that Enforce requires.

Tanium recommended installation

If you select **Tanium Recommended Installation** when you import Enforce, 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 Enforce to import, 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 Enforce, the server automatically updates those dependencies to the latest available versions.

Required dependencies

Enforce has the following required dependencies:

- Tanium™ Data Service (TDS)
- Tanium™ Direct Connect
- Tanium™ Endpoint Configuration
- Tanium™ Interact
- Tanium™ RDB Service

©2026 Tanium Inc. All Rights Reserved

- (Windows endpoints) Tanium™ Client Recorder Extension*
- Tanium™ Secrets Service

*= This client extension includes the Tanium Driver.

Note:

If the Tanium Core Content version is missing or not up to date, this alert occurs: `Tanium Core Content solution is missing or minimum version is not satisfied. Install the Core Content solution and then restart the Enforce module service.`

After you install the latest version, restart the Enforce module service. For Windows, restart the service in the Service Manager on the Tanium Module Server. For more information about restarting services in TanOS, see Tanium Appliance User Guide: Start, stop, or restart Tanium services.

Feature-specific dependencies

Enforce has the following feature-specific dependencies:

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

- Tanium Cloud Workloads is required for cluster policies
- Tanium™ Core Content is required for BitLocker and FileVault policies

©2026 Tanium Inc. All Rights Reserved

- Tanium™ End-User Notifications is required for BitLocker and FileVault policies
- Tanium Reporting is required to view enhanced endpoint details for enforcements

Client extensions and endpoint tools

Tanium Endpoint Configuration installs Client Extensions and other tools for 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 a list of all Client Extensions and tools, see Reference: Client extensions used for Tanium solutions.

Note: The change management feature of Endpoint Configuration might affect the version of each endpoint tool installed on endpoints.

Tanium™ Module Server

Enforce is installed and runs as a service on the Tanium Module Server host computer. The impact on the Module Server is minimal and depends on usage.

Endpoints

Supported internet protocols

Enforce supports IPv4 and IPv6 addresses.

©2026 Tanium Inc. All Rights Reserved

Domain-joined Windows endpoints

For policy settings that are applied using Local Group Policy (LGPO), domain-joined endpoints must be able to connect to a domain controller so that Enforce can resolve conflicts and apply some settings. For more information, see Resolve Active Directory policy conflicts on page 211.

This requirement does not apply to Windows endpoints that are not joined to a domain or are Entra ID-joined, Security Policy settings, or configuration service providers (CSPs). For more information about using CSPs to apply settings, see Configuration service providers (CSPs) on page 163.

Supported operating systems

Enforce policies support the following endpoint operating systems:

Important: All Windows editions that support the Group Policy feature are supported for each of the following Windows versions, unless otherwise noted. Available Group Policy settings vary depending on Windows version and edition.

Supported operating systems for Enforce

Policy	Operating System	Notes
Anti-malware: Windows Defender	• Windows 10 or later, Enterprise or Pro[1] • Windows Server 2016 or later	
AppLocker	• Windows 10 or later[1] • Windows Server 2016 or later	• For more information about specific requirements, including supported editions and other required Microsoft KBs, see Microsoft: Requirements to use AppLocker - Operating System Requirements.

©2026 Tanium Inc. All Rights Reserved

Policy	Operating System	Notes
		Enforce supports the versions that list **Yes** in the **Can be enforced** column in the Microsoft document. **Note:** Packaged app rules are not supported for any operating system.
BitLocker	• Windows 10 Education, Pro Education, Enterprise, or Pro • Windows 11 Enterprise or Pro[1] • Windows Server 2019 and later	• Application of policy settings using a configuration service provider (CSP) requires specific versions of Windows. To determine the earliest supported operating system version for a specific setting, hover over next to the setting.
Cluster policies	• Support for the same container orchestrators and registry providers as Cloud Workloads. For more information, see Cloud Workloads User Guide: Requirements	
Device Control - Windows	• Windows 10 or later[1] • Windows Server 2016 or later	
FileVault	• macOS 10.13 High Sierra • macOS 10.14 Mojave • macOS 10.15 Catalina • macOS 11 Big Sur • macOS 12 Monterey	

©2026 Tanium Inc. All Rights Reserved

Policy	Operating System	Notes
	• macOS 13 Ventura • macOS 14 Sonoma • macOS 15 Sequoia • macOS 26 Tahoe	
Firewall Management - Linux	• Amazon Linux 2023, Amazon Linux 2 LTS, Amazon Linux 1 AMI • CentOS 6, 7, or 8 • Debian 12 • Oracle Linux (OEL) 6, 7, 8, or 9 • Red Hat Enterprise Linux (RHEL) 6, 7, 8, or 9 • SUSE Linux Enterprise Server (SLES) 12.x, 15.x • Ubuntu 16.04 LTS, 18.04 LTS, 20.04 LTS, 22.04 LTS, or 24.04 LTS	• ARM architecture is supported with Enforce 2.1.287 or later and only for OEL 8, 9 and RHEL 8,9. For more information about the versions of the Tanium Client that support this architecture, see Tanium Client Management User Guide: Client version and host system requirements. Supported firewalls: • **Iptables** is supported for use with these distributions: • AlmaLinux • Amazon Linux • CentOS • Oracle Linux (OEL) • Red Hat Enterprise Linux (RHEL) • Rocky Linux

©2026 Tanium Inc. All Rights Reserved

Policy	Operating System	Notes
		• SUSE Linux Enterprise Server (SLES) • **Firewalld** is supported for use with these distributions: • AlmaLinux • Amazon Linux • CentOS • Debian • Oracle Linux (OEL) • Red Hat Enterprise Linux (RHEL) • Rocky Linux • SUSE Linux Enterprise Server (SLES) • **Debian Uncomplicated Firewall (ufw)** is supported for use with these distributions:

©2026 Tanium Inc. All Rights Reserved

Policy	Operating System	Notes
		• Debian • Ubuntu
Firewall Management - Windows	• Windows 10 or later[1] • Windows Server 2016 or later	
Machine Administrative Templates	• Windows 10 or later, Enterprise or Pro[1] • Windows Server 2016 or later	• Application of policy settings using a configuration service provider (CSP) requires specific versions of Windows. To determine the earliest supported operating system version for a specific setting, hover over  next to the setting.
Remediation - Linux	• Amazon Linux 2023, Amazon Linux 2 LTS, Amazon Linux 1 AMI • CentOS 6, 7, or 8 • Debian 12 • Oracle Linux (OEL) 8 or 9 • Red Hat Enterprise Linux (RHEL) 6, 7, 8, or 9 • SUSE Linux Enterprise Server (SLES) 12.x, 15.x • Ubuntu 16.04 LTS, 18.04 LTS, 20.04 LTS, 22.04 LTS, or 24.04 LTS	• ARM architecture is supported with Enforce 2.1.287 or later and only for OEL 8, 9 and RHEL 8,9. For more information about the versions of the Tanium Client that support this architecture, see Tanium Client Management User Guide: Client version and host system requirements.
Remediation -	• macOS 10.13 High Sierra	

©2026 Tanium Inc. All Rights Reserved

Policy	Operating System	Notes
Mac	• macOS 10.14 Mojave • macOS 10.15 Catalina • macOS 11 Big Sur • macOS 12 Monterey • macOS 13 Ventura • macOS 14 Sonoma • macOS 15 Sequoia • macOS 26 Tahoe	
Remediation - Windows	• Windows 10 or later, Enterprise or Pro[1] • Windows Server 2016 or later	
SRP Management	• Windows 10 or later, Enterprise or Pro[1] • Windows Server 2016 or later	
Security Settings	• Windows 10 or later[1]	• Application of policy settings using a configuration service provider (CSP) requires specific versions of Windows. To determine the earliest supported operating system version for a specific setting, hover over  next to the setting.
Tanium Removable Storage Access	• Windows 10, build 1607 or later[1] • Windows Server 2016 or later	• Same Windows endpoint requirements as Client Recorder Extension. For more information, see Client Recorder Extension User Guide: Endpoints.

©2026 Tanium Inc. All Rights Reserved

Policy	Operating System	Notes
User Administrative Templates	• Windows 10 or later, Enterprise or Pro[1] • Windows Server 2016 or later	• Application of policy settings using a configuration service provider (CSP) requires specific versions of Windows. To determine the earliest supported operating system version for a specific setting, hover over next to the setting.

[1] Windows 11 endpoints with Arm processors are supported with Enforce 2.4.213 or later. For more information about the versions of the Tanium Client that support this architecture, see Tanium Client Management User Guide: Client version and host system requirements.

Host and network security requirements

Specific ports and processes are needed to run Enforce.

Required ports

The following ports are required for Enforce communication.

Best Practice: 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.

Ports for Enforce communication

©2026 Tanium Inc. All Rights Reserved

Required ports for Enforce communication

Component	Direction	Port	Protocol	Purpose
Module Server	Inbound	17475	TCP	Required only when you use disk encryption policies. Allows communication between the Module Server and endpoints for Direct Connect.
	Module Server (Loopback)	17476	TCP	Required only when you use disk encryption policies. Allows notifications on endpoints from the End-User Notifications shared service.
	Module Server (Loopback)	17497	TCP	Internal purposes; not externally accessible.
	Module Server (Loopback)	17512	TCP	Required only when you use BitLocker and when the BitLocker recovery database is hosted on the Module Server.
Recovery portal server	Inbound	443	TCP	Required only when you use the recovery portal with disk encryption policies. Allows users to access the recovery portal.
	Outbound	443	TCP	Required only when you use the recovery portal with disk encryption policies. Allows the recovery portal to access the Tanium Server.
Zone Server	Inbound	17486	TCP	Required only when you use disk encryption policies for external endpoints that connect through a Zone Server.

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

©2026 Tanium Inc. All Rights Reserved

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 Reference: Endpoint security exclusions. For Windows-based Tanium Core Platform deployments, see Tanium Core Platform Server security exclusions.

Note: 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.

ENFORCE ENDPOINT EXCLUSIONS

Enforce security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Process	*<Tanium Client>* \Tools\StdUtils\7za.exe
	x86 endpoints	Process	*<Tanium Client>* \Tools\Enforce\devcon32.exe
	x64 endpoints	Process	*<Tanium Client>* \Tools\Enforce\devcon64.exe
		Process	*<Tanium Client>* \Tools\Enforce\LocalPolicyTool.exe
		Folder	*<Tanium Client>* \python312
		File	*<Tanium Client>* \TPython\TPython.bat
		Folder	*<Tanium Client>* \TPython312

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	*<Tanium Client>* \python312\TPython.exe
		Process	*<Tanium Client>* \TaniumClient.exe
		Process	*<Tanium Client>* \TaniumCX.exe
		Process	*<Tanium Client>* \Tools\recorder\TaniumRecorderCtl.exe
		File	*<Tanium Client>* \extensions\TaniumRecorder.dll
		File	*<Tanium Client>* \extensions\TaniumRecorder.dll.sig
		File	*<Tanium Client>* \extensions\recorder\proc.bin
		File	*<Tanium Client>* \extensions\recorder\recorder.db
		File	*<Tanium Client>* \extensions\recorder\recorder.db-shm
		File	*<Tanium Client>* \extensions\recorder\recorder.db-wal
		File	C:\Windows\System32\drivers\TaniumRecorderDrv.sys
		Process	*<Tanium Client>* \tools\driver\service\TaniumDriverSvc.exe
	x86 endpoints	Process	*<Tanium Client>* \tools\driver\TaniumDriverCtl.exe
	x86 endpoints	Process	*<Tanium Client>* \tools\driver\TaniumDriverSvc.exe
	x86 endpoints	File	*<Tanium Client>* \tools\driver\TaniumProcessMonitor.dll

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	x64 endpoints	Process	*<Tanium Client>* \tools\driver\TaniumDriverCtl64.exe
	x64 endpoints	Process	*<Tanium Client>* \tools\driver\TaniumDriverSvc64.exe
	x64 endpoints	File	*<Tanium Client>* \tools\driver\TaniumProcessMonitor64.dll
	x64 endpoints	File	C:\Windows\SysWOW64\TaniumProcessMonitor.dll
		Folder	*<Tanium Client>* \extensions\stream
macOS and Linux x86 and x64		Folder	*<Tanium Client>* /python312
		Process	*<Tanium Client>* /TPython/TPython
		Folder	*<Tanium Client>* /TPython312
		Process	*<Tanium Client>* /python312/python
		Process	*<Tanium Client>* /python312/bin/pybin
		Process	*<Tanium Client>* /TaniumClient
		Process	*<Tanium Client>* /TaniumCX

ENFORCE SERVER EXCLUSIONS

©2026 Tanium Inc. All Rights Reserved

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

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	*<Module Server>* \services\enforce-service\node.exe
Zone Server		Process	<Tanium Installation Directory>\Tanium Direct Connect Zone Proxy\node.exe
		Process	<Tanium Installation Directory>\Tanium Direct Connect Zone Proxy\twsm.exe

Third-party internet URLs

For anti-malware policy settings, allow outbound communication from the Tanium Module Server to the following Microsoft download URLs. For more information about configuration details, see Configure URLs for platform updates and definitions on page 81.

Internet URLs required for Enforce communication

Architecture	URL
Windows x86 endpoints	https://go.microsoft.com/fwlink/?LinkID=121721&arch=x86
	https://go.microsoft.com/fwlink/?LinkId=211053
	https://definitionupdates.microsoft.com
	http://catalog.update.microsoft.com [1]
	http://catalog.s.download.windowsupdate.com [1]
Windows x64 endpoints	https://go.microsoft.com/fwlink/?LinkID=121721&arch=x64
	https://go.microsoft.com/fwlink/?LinkId=211054
	https://definitionupdates.microsoft.com

©2026 Tanium Inc. All Rights Reserved

Architecture	URL
	http://catalog.update.microsoft.com [1]
	http://catalog.s.download.windowsupdate.com [1]

[1] Required for Microsoft Defender Platform updates. For more information, see Windows Defender platform updates on page 76 .

User role requirements

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

- Table 10. Enforce Global solution permissions on page 45
- Enforce administration, platform content, and global permissions on page 45: The solution permissions automatically provide some of these permissions.

To review a summary of the predefined roles, see Set up Enforce users on page 70.

Optional roles for Enforce are required to enable optional Enforce functionality.

Some Enforce 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 Enforce. If you create custom roles for Enforce users, be sure to assign all the solution permissions and content set permissions that are required for Enforce 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)

©2026 Tanium Inc. All Rights Reserved

- Provided role permissions
- View effective role permissions
- Configure a custom role

Important: The **Enforce service account** role is for internal use only. It is automatically managed by the **Enforce** user. Do not assign the **Enforce service account** role to users.

Enforce Global solution permissions

Permission	Enforce Administrator	Enforce Defender Scan User	Enforce Defender Scan Viewer	Enforce Endpoint Configuration Approver	Enforce Operator	Enforce Policy Administrator (Global)	Enforce Policy User (Global)	Enforce Policy Viewer (Global)	Enforce Quarantine Administrator	Enforce Write Content Wipe Action
Disk Encryption Recovery Keys Read, rotate, export, or delete recovery keys for disk encryption in given content sets	✓ EXPORT ROTATE READ DELETE	✗	✗	✗	✓ EXPORT ROTATE READ DELETE	✗	✗	✗	✗	✗
Enforce SHOW: View the Enforce workbench	✓ SHOW OPERATOR	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW OPERATOR	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW

©2026 Tanium Inc. All Rights Reserved

Permission	Enforce Admin-istrator	Enforce Defender Scan User	Enforce Defender Scan Viewer	Enforce Endpoint Config-uration Approver	Enforce Operator	Enforce Policy Admin-istrator (Global)	Enforce Policy User (Global)	Enforce Policy Viewer (Global)	Enforce Quar-antine Admin-istrator	Enforce Write Content Wipe Action
OPERATOR: Read, edit, and delete most Enforce objects (except edit access to Enforce settings)										
Enforce Administrator Unrestricted access to Enforce	✓ ADMINISTER	✗	✗	✗	✗	✗	✗	✗	✗	✗
Enforce Create Enforce policies in given content sets	✓ ENFORCE-MENT	✗	✗	✗	✓ ENFORCE-MENT	✓ ENFORCE-MENT	✓ ENFORCE-MENT	✗	✗	✗
Enforce Defender Scan View, create,	✓ READ	✓ READ	✓ READ	✗	✓ READ	✗	✗	✗	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Enforce Admin-istrator	Enforce Defender Scan User	Enforce Defender Scan Viewer	Enforce Endpoint Config-uration Approver	Enforce Operator	Enforce Policy Admin-istrator (Global)	Enforce Policy User (Global)	Enforce Policy Viewer (Global)	Enforce Quar-antine Admin-istrator	Enforce Write Content Wipe Action
or delete Defender scans	WRITE	WRITE			WRITE					
Enforce Edit Any Edit available policy enforcements. Users always have access to enforcements that they created.	✓ ENFORCE-MENT	✗	✗	✗	✓ ENFORCE-MENT	✓ ENFORCE-MENT	✓ ENFORCE-MENT	✗	✗	✗
Enforce Endpoint Configuration Approve Enforce items in Endpoint Configuration	✗	✗	✗	✓ APPROVER	✗	✗	✗	✗	✗	✗
Enforce Endpoint Configuration	✓ WRITE	✗	✗	✗	✓ WRITE	✓ WRITE	✓ WRITE	✓ READ	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Enforce Administrator	Enforce Defender Scan User	Enforce Defender Scan Viewer	Enforce Endpoint Configuration Approver	Enforce Operator	Enforce Policy Administrator (Global)	Enforce Policy User (Global)	Enforce Policy Viewer (Global)	Enforce Quarantine Administrator	Enforce Write Content Wipe Action
All View or create Endpoint Configuration items for Enforce										
Enforce Endpoint Wipe Issue Windows Remediation actions that wipe, freeze, or recover endpoints	✗	✗	✗	✗	✗	✓ ACTION	✗	✗	✗	✓ ACTION
Enforce Operator Settings Globally read or edit most Enforce settings	✓ READ WRITE	✗	✗	✗	✓ READ WRITE	✗	✗	✗	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Enforce Admin-istrator	Enforce Defender Scan User	Enforce Defender Scan Viewer	Enforce Endpoint Config-uration Approver	Enforce Operator	Enforce Policy Admin-istrator (Global)	Enforce Policy User (Global)	Enforce Policy Viewer (Global)	Enforce Quar-antine Admin-istrator	Enforce Write Content Wipe Action
Enforce Policy Prioritize, view, create, or edit Enforce policy priorities in given content sets	✓ PRIORITIZE READ WRITE	✗	✗	✗	✓ PRIORITIZE READ WRITE	✓ PRIORITIZE READ WRITE	✓ READ WRITE	✓ READ	✗	✗
Enforce Recovery Portal View recovery portal configuration and status, or write recovery portal configuration and download the installer	✓ READ WRITE	✗	✗	✗	✗	✗	✗	✗	✗	✗
Enforce Settings Globally read or edit all	✓ READ	✗	✗	✗	✗	✗	✗	✗	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Enforce Admin-istrator	Enforce Defender Scan User	Enforce Defender Scan Viewer	Enforce Endpoint Config-uration Approver	Enforce Operator	Enforce Policy Admin-istrator (Global)	Enforce Policy User (Global)	Enforce Policy Viewer (Global)	Enforce Quar-antine Admin-istrator	Enforce Write Content Wipe Action
Enforce settings	WRITE									
Enforce Write Policy Create policy packages for enforcements	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Policy Template Read, edit, or delete policy templates in given content sets	✓ READ WRITE DELETE	✗	✗	✗	✓ READ WRITE DELETE	✓ READ WRITE DELETE	✓ READ	✓ READ	✗	✗
Policy Type Read or edit policy types in given content sets	✓ READ WRITE	✗	✗	✗	✓ READ WRITE	✓ READ WRITE DELETE	✓ READ WRITE	✓ READ	✗	✗
Reports Read, edit, or delete reports	✓ READ	✗	✗	✗	✓ READ	✓ READ	✓ READ	✓ READ	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Enforce Admin-istrator	Enforce Defender Scan User	Enforce Defender Scan Viewer	Enforce Endpoint Config-uration Approver	Enforce Operator	Enforce Policy Admin-istrator (Global)	Enforce Policy User (Global)	Enforce Policy Viewer (Global)	Enforce Quar-antine Admin-istrator	Enforce Write Content Wipe Action
in given content sets	WRITE DELETE				WRITE DELETE	WRITE DELETE	WRITE DELETE			
Restore from Quarantine Restore files quarantined by Microsoft Defender.	✓ ADMINISTER	✗	✗	✗	✓ ADMINISTER	✗	✗	✗	✓ ADMINISTER	✗

The permissions for these roles provide solution permissions for other solutions. To view the provided permissions, see Tanium Console User Guide: View effective role permissions .

Global Template (Permissions restricted by operating system content sets: Windows, macOS, or Linux) solution permissions

Permission	Enforce Policy Administrator (Template)	Enforce Policy User (Template)	Enforce Policy Viewer (Template)	Enforce Quarantine Administrator	Enforce Recovery Key Administrator (Template) Enforce Recovery Key User (Template)	Enforce Recovery Key Viewer (Template)	Enforce Recovery Portal (Template)	Enforce Recovery Portal Administrator (Template)	Enforce Recovery Portal Viewer (Template)
Disk Encryption	✗	✗	✗	✗	✓	✓	✗	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Enforce Policy Administrator (Template)	Enforce Policy User (Template)	Enforce Policy Viewer (Template)	Enforce Quarantine Administrator	Enforce Recovery Key Administrator (Template) Enforce Recovery Key User (Template)	Enforce Recovery Key Viewer (Template)	Enforce Recovery Portal (Template)	Enforce Recovery Portal Administrator (Template)	Enforce Recovery Portal Viewer (Template)
Recovery Keys Read, rotate, or delete recovery keys for disk encryption in given content sets					ROTATE READ DELETE	READ			
Disk Encryption Recovery Keys Portal Read recovery keys for disk encryption in given content sets	✗	✗	✗	✗	✓ READ	✓ READ	✓ READ	✗	✗
Enforce SHOW: View the Enforce	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW	✗	✓ SHOW	✓ SHOW

©2026 Tanium Inc. All Rights Reserved

Permission	Enforce Policy Administrator (Template)	Enforce Policy User (Template)	Enforce Policy Viewer (Template)	Enforce Quarantine Administrator	Enforce Recovery Key Administrator (Template) Enforce Recovery Key User (Template)	Enforce Recovery Key Viewer (Template)	Enforce Recovery Portal (Template)	Enforce Recovery Portal Administrator (Template)	Enforce Recovery Portal Viewer (Template)
workbench OPERATOR: Read, edit, and delete most Enforce objects (except edit access to Enforce settings)									
Enforce Create Enforce policies in given content sets	✓ ENFORCE-MENT	✓ ENFORCE-MENT	✗	✗	✗	✗	✗	✗	✗
Enforce Edit Any Edit available	✓ ENFORCE-MENT	✗	✗	✗	✗	✗	✗	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Enforce Policy Administrator (Template)	Enforce Policy User (Template)	Enforce Policy Viewer (Template)	Enforce Quarantine Administrator	Enforce Recovery Key Administrator (Template) Enforce Recovery Key User (Template)	Enforce Recovery Key Viewer (Template)	Enforce Recovery Portal (Template)	Enforce Recovery Portal Administrator (Template)	Enforce Recovery Portal Viewer (Template)
policy enforcements. Users always have access to enforcements that they created.									
Enforce Endpoint Configuration (Template) View or create Endpoint Configuration items for OS	✓ WRITE	✓ WRITE	✓ READ	✗	✗	✗	✗	✗	✗
Enforce Policy Prioritize, view, create, or edit	✓ READ WRITE	✓ READ WRITE	✓ READ	✗	✗	✗	✗	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Enforce Policy Administrator (Template)	Enforce Policy User (Template)	Enforce Policy Viewer (Template)	Enforce Quarantine Administrator	Enforce Recovery Key Administrator (Template) Enforce Recovery Key User (Template)	Enforce Recovery Key Viewer (Template)	Enforce Recovery Portal (Template)	Enforce Recovery Portal Administrator (Template)	Enforce Recovery Portal Viewer (Template)
Enforce policy priorities in given content sets									
Enforce Recovery Allows the user to be used as the Enforce Recovery Portal	✗	✗	✗	✗	✗	✗	✓ PORTAL	✗	✗
Enforce Recovery Portal View recovery portal configuration and status, or	✗	✗	✗	✗	✗	✗	✗	✓ READ WRITE	✓ READ

©2026 Tanium Inc. All Rights Reserved

Permission	Enforce Policy Administrator (Template)	Enforce Policy User (Template)	Enforce Policy Viewer (Template)	Enforce Quarantine Administrator	Enforce Recovery Key Administrator (Template) Enforce Recovery Key User (Template)	Enforce Recovery Key Viewer (Template)	Enforce Recovery Portal (Template)	Enforce Recovery Portal Administrator (Template)	Enforce Recovery Portal Viewer (Template)
write recovery portal configuration and download the installer									
Policy Template Read, edit, or delete policy templates in given content sets	✓ READ WRITE DELETE	✓ READ	✓ READ	✗	✗	✗	✗	✗	✗
Policy Type Read or edit policy types in given content sets	✓ READ WRITE	✓ READ WRITE	✓ READ	✗	✗	✗	✗	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Enforce Policy Administrator (Template)	Enforce Policy User (Template)	Enforce Policy Viewer (Template)	Enforce Quarantine Administrator	Enforce Recovery Key Administrator (Template) Enforce Recovery Key User (Template)	Enforce Recovery Key Viewer (Template)	Enforce Recovery Portal (Template)	Enforce Recovery Portal Administrator (Template)	Enforce Recovery Portal Viewer (Template)
Quarantine Restore files quarantined by Microsoft Defender	✓ ADMINISTER	✗	✗	✓ ADMINISTER	✗	✗	✗	✗	✗
Reports Read, edit, or delete reports in given content sets	✓ READ WRITE DELETE	✓ READ WRITE DELETE	✓ READ	✗	✗	✗	✗	✗	✗

The permissions for these roles provide solution permissions for other solutions. To view the provided permissions, see Tanium Console User Guide: View effective role permissions .

Module Objects with Access Control by Content Sets

Access Control Type	Policy Definition	Policy Type	Policy Templates	Policy Item	Managed Definition Files	Reports	Disk Encryption Recovery Keys
Global	✗	✗	✗	✓	✓	✗	✓

©2026 Tanium Inc. All Rights Reserved

Access Control Type	Policy Definition	Policy Type	Policy Templates	Policy Item	Managed Definition Files	Reports	Disk Encryption Recovery Keys
Content Set	✓	✓	✓	✗	✗	✓	✗

Administration and platform content permissions

Permission	Permission Type	Enforce Administrator	Enforce Defender Scan User	Enforce Defender Scan Viewer Enforce Endpoint Configuration Approver	Enforce Operator Enforce Policy Administrator Enforce Policy User	Enforce Policy Viewer	Enforce Quarantine Administrator	Enforce Recovery Key Administrator Enforce Recovery Key User Enforce Recovery Key Viewer Enforce Recovery Portal Administrator Enforce Recovery Portal Viewer	Enforce Recovery Portal	Enforce Write Content Wipe Action
Action Group	Administration	✓ READ	✗	✗	✓ READ	✗	✗	✗	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Permission Type	Enforce Administrator	Enforce Defender Scan User	Enforce Defender Scan Viewer Enforce Endpoint Configuration Approver	Enforce Operator Enforce Policy Administrator Enforce Policy User	Enforce Policy Viewer	Enforce Quarantine Administrator	Enforce Recovery Key Administrator Enforce Recovery Key User Enforce Recovery Key Viewer Enforce Recovery Portal Administrator Enforce Recovery Portal Viewer	Enforce Recovery Portal	Enforce Write Content Wipe Action
Token - Use	Administration	✗	✗	✗	✗	✗	✗	✗	✓ SPECIAL	✗
Token - View	Administration	✗	✗	✗	✗	✗	✗	✗	✓ SPECIAL	✗
Action	Platform Content	✓ WRITE	✓ WRITE	✗	✓ WRITE	✗	✓ WRITE	✗	✗	✓ WRITE

©2026 Tanium Inc. All Rights Reserved

Permission	Permission Type	Enforce Administrator	Enforce Defender Scan User	Enforce Defender Scan Viewer Enforce Endpoint Configuration Approver	Enforce Operator Enforce Policy Administrator Enforce Policy User	Enforce Policy Viewer	Enforce Quarantine Administrator	Enforce Recovery Key Administrator Enforce Recovery Key User Enforce Recovery Key Viewer Enforce Recovery Portal Administrator Enforce Recovery Portal Viewer	Enforce Recovery Portal	Enforce Write Content Wipe Action
Action for Saved Question	Platform Content	✓ WRITE	✗	✗	✓ WRITE	✗	✗	✗	✗	✗
Filter Group	Platform Content	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ	✗	✓ READ
Own Action	Platform Content	✓ READ	✓ READ	✗	✓ READ	✗	✓ READ	✗	✗	✓ READ

©2026 Tanium Inc. All Rights Reserved

Permission	Permission Type	Enforce Administrator	Enforce Defender Scan User	Enforce Defender Scan Viewer Enforce Endpoint Configuration Approver	Enforce Operator Enforce Policy Administrator Enforce Policy User	Enforce Policy Viewer	Enforce Quarantine Administrator	Enforce Recovery Key Administrator Enforce Recovery Key User Enforce Recovery Key Viewer Enforce Recovery Portal Administrator Enforce Recovery Portal Viewer	Enforce Recovery Portal	Enforce Write Content Wipe Action
Package	Platform Content	READ	READ		READ		READ			READ
Plugin	Platform Content	READ EXECUTE	READ EXECUTE	READ EXECUTE	READ EXECUTE	READ EXECUTE	READ EXECUTE	READ EXECUTE		READ EXECUTE
Saved Question	Platform Content									

©2026 Tanium Inc. All Rights Reserved

Permission	Permission Type	Enforce Administrator	Enforce Defender Scan User	Enforce Defender Scan Viewer Enforce Endpoint Configuration Approver	Enforce Operator Enforce Policy Administrator Enforce Policy User	Enforce Policy Viewer	Enforce Quarantine Administrator	Enforce Recovery Key Administrator Enforce Recovery Key User Enforce Recovery Key Viewer Enforce Recovery Portal Administrator Enforce Recovery Portal Viewer	Enforce Recovery Portal	Enforce Write Content Wipe Action
		READ WRITE	READ WRITE		READ WRITE					
Sensor	Platform Content	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ	✗	✓ READ

The permissions for this role provide solution permissions for other solutions. To view the provided permissions, see View effective role permissions .

©2026 Tanium Inc. All Rights Reserved

Note:

Tanium Guide observations and guidance display for users based on user permissions.

- Assign the **Token - Use** administration permission to enable receiving observations and guidance.
- Assign the **Benchmark show** permission to view Risk Score-related observations.
- Assign the **Enforce Operator Settings write** permission to view Windows Defender automatic platform update guidance.
- Assign the **Enforce show** permission to view endpoint security software-related observations.

For more information, see Tanium Guide User Guide: Viewing and managing notifications.

Optional Enforce roles for Guide observations and guidance

Role	Enables
A custom role that includes the **Enforce show** and **Token - Use** permissions	Access to Enforce observations. For more information, see Tanium Console User Guide: Configure a custom role .
A custom role that includes the **Enforce Operator Settings write** and **Token - Use** permissions	Access to Enforce guidance. For more information, see Tanium Console User Guide: Configure a custom role .

Create custom roles to only allow access to policies associated with a specific content set

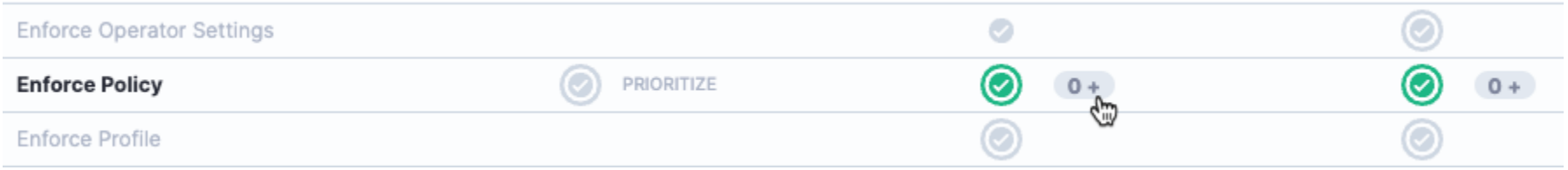
If you want to limit access for a user to policies for a specific operating system or a specific policy type, you can create a custom role with

©2026 Tanium Inc. All Rights Reserved

access only to the associated content set.

For example, you can create a custom role that includes the Enforce - Show, Enforce Policy - Write, and Enforce - Policy Type permissions. When you add the policy permissions, click **0+** in the permission column, select the content sets for the operating systems or policy types that you want the user to be able to access, such as **Enforce Windows** (to allow access to all Windows policy types, but not Linux or Mac policy types) or **Enforce Windows BitLocker** (to allow access only to Windows BitLocker policy types) and click **Select**.

Figure 2. Add a permission to a role



For more information about creating custom roles, see Tanium Console User Guide: Configure a custom role.

CAUTION: Thoroughly test all custom roles in a lab or test environment to ensure that access levels are as expected before you use the role in a production environment.

©2026 Tanium Inc. All Rights Reserved

Installing Enforce

About this task

Use the **Solutions** page to install Enforce and select either automatic or manual configuration:

- Automatic configuration with default settings: Enforce 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 Enforce, see Import Enforce with default settings on page 66.
- Manual configuration with custom settings: After installing Enforce, you must manually configure required settings. Select this option only if Enforce requires settings that differ from the recommended default settings. For more information, see Import Enforce with custom settings on page 66.

Before you begin

- Read the release notes.
- Review the Enforce requirements on page 28.
- If you are upgrading from a previous version, see Upgrade Enforce on page 67.
- Assign the correct roles to users for Enforce. Review the User role requirements on page 44.
    - To import the Enforce solution, you must be assigned the Administrator reserved role.
    - To configure the Enforce action group, you must be assigned the Administrator reserved role, Content Administrator reserved role, or a role that has the **Write Action Group** permission.

©2026 Tanium Inc. All Rights Reserved

Import Enforce with default settings

Use default settings to get started with installing Enforce without extra configuration steps.

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

To import Enforce and configure default settings, see Tanium Console User Guide: Import all modules and services. To verify that the correct version is installed after the import, see Verify Enforce version on page 67.

Default settings for Enforce

When you import Enforce with automatic configuration, the following default settings are configured:

Default settings for Enforce

Setting	Default value
Action group	• Restricted targeting disabled (default): `All Computers` computer group • Restricted targeting enabled: `No Computers` computer group
Computer groups	The Enforce tools group is set to `All Computers` .

Import Enforce with custom settings

To import Enforce without automatically configuring default settings, be sure to clear the **Apply All Tanium recommended configurations** option while performing the steps in Tanium Console User Guide: Import or update specific solutions. When you import with custom settings, default settings are not configured.

Manage solution dependencies

©2026 Tanium Inc. All Rights Reserved

When you start the Enforce workbench for the first time, the Tanium Server checks whether all the Tanium modules and shared services (solutions) that are required for Enforce are installed at the required versions. The Enforce workbench cannot load unless all required dependencies are installed. If you selected **Tanium Recommended Installation** when you imported Enforce , the Tanium Server automatically imported all your licensed solutions at the same time. Otherwise, if you manually imported Enforce and did not import all its dependencies, Tanium Console displays a banner that lists the dependencies and the required versions.

1. Install the dependencies as described in Import or update specific solutions.
2. Open the **Enforce Overview** page. From the Main menu, go to **Shared Services** > **Enforce**. Verify that the Console no longer displays a banner to list missing dependencies.

Upgrade Enforce

To upgrade Enforce , see Tanium Console User Guide: Install a Tanium release update. To verify that the correct version is installed after the upgrade, see Verify Enforce version on page 67.

Verify Enforce version

After you import or upgrade Enforce , verify that the correct version is installed.

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

©2026 Tanium Inc. All Rights Reserved

Configuring Enforce

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.

Endpoint tools are bundled together in a versioned toolset. Each toolset contains a specific version of each tool. The Endpoint Configuration Toolset Solution provides upgrades to the toolset, and it imports upgraded versions of the entire toolset as needed by upgraded or newly installed solutions.

Important:

When you upgrade Enforce, the change management feature enables you to perform a staged rollout of the endpoint tools associated with the new version of Enforce. Enforce remains compatible with earlier versions of the endpoint tools and so continues to function with endpoints in rings that have not yet received the latest tools. However, any functionality added in the upgrade of Enforce might not be available on these endpoints until they receive the upgraded tools.

In some cases, multiple solutions install the same endpoint tool, but upgraded endpoint tools remain compatible with all associated solutions. For example, both Tanium™ Threat Response and Tanium™ Reveal install and use index-cx. When you upgrade Threat Response, it might install version x.6.yyyy of index-cx, superseding version x.5.zzzz that Reveal previously installed. The index-cx upgrade from Threat Response does not affect the Index-related functionality of Reveal on the upgraded endpoints. For more information about the change management feature, see Tanium Endpoint Configuration User Guide: Managing endpoint tool upgrade rollouts.

©2026 Tanium Inc. All Rights Reserved

Note: For information about how to install Endpoint Configuration, see 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 Enforce, see User role requirements. For more information about how to enable and use configuration approvals in Endpoint Configuration, see Managing approvals.

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 Managing action locks.

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

Configure Enforce

Configure Enforce action group

About this task

Importing the Enforce 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 Enforce, the action group targets **No Computers**.

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

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

©2026 Tanium Inc. All Rights Reserved

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

By default, the Enforce action group is set to `All Computers`. You can update the action group if needed.

1. From the Main menu, go to **Administration** > **Actions** > **Action Groups**.
2. Click **Tanium Enforce** to update the action group and then click **Save**.

Set up Enforce users

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

For more information about the specific permissions for each role, see User role requirements on page 44.

Important: During installation, Enforce creates an **Enforce** user to automatically manage the **Enforce service account**. Do not edit or delete the **Enforce** user.

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

Enforce Administrator

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

- Configure all Enforce service settings
- Manage policies, policy templates, policy types, policy priorities, and enforcements
- Manage recovery portal configuration

Enforce Defender Scan User

Assign the **Enforce Defender Scan User** role to users who view and create Defender scans.

©2026 Tanium Inc. All Rights Reserved

Enforce Defender Scan Viewer

Assign the **Enforce Defender Scan Viewer** role to users who view Defender scans.

Enforce Endpoint Configuration Approver

Assign the **Enforce Endpoint Configuration Approver** role to a user who approves or rejects Enforce configuration items in Tanium Endpoint Configuration.

Enforce Operator

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

- Configure most Enforce service settings
- Manage policies, policy templates, policy types, policy priorities, and enforcements

Enforce * Policy Administrator

Assign the **Enforce * Policy Administrator** role to users who manage and prioritize policies. This role can perform the following tasks:

- View, create, and delete policies, policy templates, policy types, and reports
- Prioritize policy priorities
- Enforce policies and edit any policy enforcements

* You can additionally limit access by assigning the Linux, Mac, or Windows roles.

Enforce * Policy User

Assign the **Enforce * Policy User** role to users who manage policies. This role can perform the following tasks:

- View and create policies and policy types
- View, create, and delete reports
- View policy templates

©2026 Tanium Inc. All Rights Reserved

- View and create policy priorities
- Enforce policies

* You can additionally limit access by assigning the Linux, Mac, or Windows roles.

Enforce * Policy Viewer

Assign the **Enforce * Policy Viewer** role to users who view policies, policy templates, policy types, and reports.

* You can additionally limit access by assigning the Linux, Mac, or Windows roles.

Enforce Recovery Key Administrator

Assign the **Enforce Recovery Key Administrator** role to users who manage disk encryption recovery keys.

Enforce Recovery Key User

Assign the **Enforce Recovery Key User** role to users who manage disk encryption recovery keys.

Enforce Recovery Key Viewer

Assign the **Enforce Recovery Key Viewer** role to users who view disk encryption recovery keys.

Enforce Recovery Portal

Assign the **Enforce Recovery Portal** role to users who view disk encryption recovery keys and can be used as the Enforce Recovery Portal.

Enforce Recovery Portal Administrator

Assign the **Enforce Recovery Portal Administrator** role to users who manage recovery portal configuration.

Enforce Recovery Portal Viewer

Assign the **Enforce Recovery Portal Viewer** role to users who view recovery portal configuration and status.

©2026 Tanium Inc. All Rights Reserved

Enforce Write Content Wipe Action

Assign the **Enforce Content Wipe Action** role to users who issue Windows Remediation actions that wipe, freeze, or recover endpoints.

©2026 Tanium Inc. All Rights Reserved

Getting started with policies

Complete these tasks to get started with Enforce policies.

Configure Distribute Over Time settings for policies

About this task

Policy enforcement occurs in the following scenarios:

- The enforcement is first created
- Changes are made to the policy corresponding to the enforcement
- The Tanium Client or Tanium Client process restarts on an endpoint
- At the beginning and end of the enforcement schedule
- Enforce detects a failed or incomplete verification of policies
- (User Administrative Template policies) When a user signs in to an endpoint

These scenarios are typically infrequent, but because endpoints check in with the Active Directory server for policy conflicts, they can temporarily cause a surge in traffic to Active Directory servers if a policy is enforced on many endpoints or many policies are enforced at the same time.

You can configure the intervals when endpoints verify and apply policies and also distribute checks with the Active Directory server over time to diffuse the traffic to the Active Directory server. To configure these settings, you must be assigned the Enforce Administrator or Enforce Operator role.



Note: These settings do not apply to remediation policies.

1. From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. Click Settings .
2. On the **General** tab, update the following settings as needed:

©2026 Tanium Inc. All Rights Reserved

Policy Update: When an enforcement is created or an enforced policy is updated, endpoints immediately update their policies and policy status.

- Specify a value in the **Distribute Over Time** setting to randomize the check in with the Active Directory server for each endpoint by an amount of time up to the value configured.

Policy Verification: By default, endpoints verify policies and update their policy status every 15 minutes.

- Update the **Interval** value to change the frequency of this check. The value must be between 10 minutes and 60 minutes.
- Specify a value in the **Distribute Over Time** setting to randomize the check in with the Active Directory server for each endpoint by an amount of time up to the value configured. The **Distribute Over Time** value must be less than the **Interval** value.

Policy Application: By default, endpoints reapply policies and update policy status every hour.

- Update the **Interval** value to change the frequency of this check. The value must be between 60 minutes and 480 minutes.
- Specify a value in the **Distribute Over Time** setting to randomize the check in with the Active Directory server for each endpoint by an amount of time up to the value configured. The **Distribute Over Time** value must be less than the **Interval** value.

3. Click **Save**.

Manage cluster policies

Install and configure Cloud Workloads

To use cluster policies, you must install and configure Cloud Workloads and deploy the Tanium Client images to the targeted cluster. For more information, see Cloud Workloads User Guide: Overview and Creating policies for Kubernetes clusters on page 142.

Configure settings for cluster policy enforcements

©2026 Tanium Inc. All Rights Reserved

About this task

By default, Enforce checks clusters for violations of enforced policies every hour, and the timeout for HTTP calls between clusters and the Tanium Server is 10 seconds. If needed, you can change these values.

1. From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. Click Settings.
2. On the **General** tab, update the following settings in the **Cluster Policy Enforcement** section as needed:
    - **Audit Schedule**: Specifies how often Enforce checks clusters for violations of enforced policies.
    - **Webhook Timeout**: Specifies the timeout for HTTP calls between clusters and the Tanium Server.
3. Click **Save**.

Manage anti-malware settings

You can use Machine Administrative Template policies to configure anti-malware settings on endpoints. This requires that Windows Defender be installed on those endpoints.

If Enforce has an issue with an anti-malware definition, an Error shows next to the definition in the **Anti-Malware Definitions Status** panel of the **Anti-Malware Health** section on the Enforce **Overview** page.

Important: Due to the way that Microsoft stores and retrieves exclusions, do not use Enforce to manage anti-malware exclusion settings if you are using Microsoft Defender for Endpoint.

Windows Defender platform updates

Microsoft releases monthly updates to the Windows Defender anti-malware platform. To keep the platform up to date and to help ensure compliance with all applicable security standards, enable Defender platform updates in Enforce. When enabled, Enforce automatically downloads and installs new monthly Defender anti-malware platform update packages on managed Windows endpoints. Defender *platform* updates are a separate, environment-wide feature from Defender *definition* (security-intelligence) updates. *Definitions* are configured per anti-malware policy and update more

©2026 Tanium Inc. All Rights Reserved

frequently, often multiple times a day.

> **Important:** Windows Defender platform updates are supported on Defender 4.18.2001.10 or later. Use the **Enforce - Defender Platform Version** sensor in Interact to find endpoints that do not have the required Defender Platform version.

How Defender platform updates are delivered by Tanium

Tanium checks the Microsoft Update Catalog for the current Defender platform version every 15 minutes and publishes an updated content manifest only when the version changes.

Enforce reads the manifest as part of its hourly maintenance cycle, checks again every 3 hours as a backup, and checks immediately when you select **Enable Platform Updates** in the Enforce settings.

If the manifest shows a newer platform version than what is currently deployed, Enforce rebuilds the package, filter group, and scheduled action for each processor architecture (64-bit, ARM64, and 32-bit Windows). The scheduled action starts distributing to all applicable endpoints immediately and reissues every hour after that.

> **Important:** The **Distribute Over Time** and **Reissue Action Interval** settings apply only to Machine Administrative Template policy enforcements that configure managed defintions and have no effect on Defender platform updates. Platform updates always distribute to all applicable endpoints at once and reissue on a fixed hourly schedule.

An endpoint is eligible for a platform update only if it is Windows, matches the processor architecture of the package, reports a readable Defender platform version, already has Defender platform 4.18.2001.10 or later, and is running an older version than the one being deployed. Tanium re-evaluates endpoint eligibility at least every 15 minutes.

Once Microsoft publishes a new platform version, the update typically reaches applicable endpoints within an hour, with a typical upper bound of about 90 minutes end to end.

The Module Server must be able to reach content.tanium.com to retrieve the manifest. The Tanium Server must be able to reach the Microsoft download host to retrieve the platform installer, because the Tanium Server downloads the installer directly at distribution time rather than staging it in advance. If only one of the two servers has the required access, Defender platform updates appear

©2026 Tanium Inc. All Rights Reserved

configured but do not reach endpoints.

Enable Defender platform updates

1. From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. Click Settings.
2. Click the **Anti-Malware** tab.
3. In the **Windows Defender Platform Updates** section, select **Enable Platform Updates** and click **Save**.
   To turn Defender platform updates off, select **Disable Platform Updates** and click **Save**. Enforce removes the packages, filter groups, and scheduled actions it created for all three architectures. Nothing remains after the removal. Re-enabling the setting rebuilds the deployment from scratch.

Windows Defender definition updates

Machine Administrative Template policies that include anti-malware settings can enable **Managed Definitions**, which use Tanium to check for and deliver new Microsoft Defender virus and spyware *definition* (security-intelligence) updates to managed endpoints so that endpoints do not need direct internet access to Microsoft. Definition updates are different from Windows Defender platform updates, described in the preceding section. *Platform* updates keep the Defender engine itself current, typically on a monthly cadence, while *definition* updates keep the virus and spyware signature files current, often multiple times a day.

To enable Managed Definitions:

1. When you configure a Machine Administrative Template policy, expand the **Anti-Malware Specific Settings** section.
2. For **Managed Definitions**, select **Deploy definition updates using Tanium**.
3. Complete the **Definition Grace Period** field to specify how many days the definitions for an endpoint can be outdated before the policy is considered unenforced. The default grace period is 1 day.

For more information, see Machine administrative template on page 117.

©2026 Tanium Inc. All Rights Reserved

Note: By default, anti-malware rules do not use Tanium to deliver definition updates.

Endpoints continue to receive definitions from the source that Microsoft Defender Antivirus is already configured to use, such as Microsoft Update or WSUS, on the existing schedule for that source. Select Managed Definitions to deliver definition updates through Tanium instead. Enabling Managed Definitions also exposes the Definition Grace Period field in the policy and adds two definition checks to the enforcement status for the policy:

- If the endpoint has no anti-malware definitions installed, the policy is considered unenforced.
- If a newer definition is available and the installed definitions for an endpoint are older than the specified **Definition Grace Period**, the policy is considered unenforced. The default grace period is 1 day. Neither check applies to rules that do not use **Managed Definitions**.

How Defender definition updates are delivered by Tanium

Tanium checks the definition locations that Microsoft publishes every 15 minutes and refreshes a signed content manifest only when the definitions have actually changed.

Enforce reads that manifest as part of its regular service checks: at service start and then every 60 minutes. When a newer base or delta definition is available, Enforce downloads the file, validates the file, and stores the file as a Tanium package ready for distribution.

When the definition file changes, the distribution action is rebuilt and starts going out immediately rather than waiting for the next scheduled cycle. From then on, the action reissues on the **Reissue Action Interval** setting, which defaults to every 60 minutes and can be set as low as 10 minutes. The **Distribute Over Time** setting defaults to **Immediate**, so all applicable endpoints are targeted at once; setting **Distribute Over Time** to **Diffused** spreads delivery across the interval to smooth network load.

Important: **Distribute Over Time** and **Reissue Action Interval** govern only Defender *definition* updates. These settings have no effect on Defender platform updates, described in the preceding section: *platform* updates always distribute to all applicable endpoints at once and reissue on a fixed hourly schedule, regardless of how **Distribute Over Time** and **Reissue Action Interval** are configured.

©2026 Tanium Inc. All Rights Reserved

Each endpoint evaluates its own state before downloading anything: Defender or SCEP must be present and not disabled by policy, the Managed Definitions policy must be in effect on the endpoint, and the offered definition version must be newer than what the endpoint already has. Tanium re-evaluates this check at least every 15 minutes. Endpoints that already have the current definition take no action, so no bandwidth is spent on those endpoints.

Applicable endpoints download the definition file and install the update. Tanium re-checks the endpoint within about 10 minutes and marks the action complete once the new definition version is in place.

In most environments a new Microsoft definition reaches targeted endpoints within 90 minutes of Tanium detecting the definition. If you lower the **Reissue Action Interval**, endpoints that have not yet received the update get the update sooner. If you use **Diffused** distribution instead, all endpoints take longer to finish receiving the update, but network load stays lower at any given time.



Note: The Module Server must be able to reach content.tanium.com to retrieve the manifest, and must be able to reach the definition source: Microsoft by default, or your custom URL or UNC path if you configured one to download the definition files.

By default, for compliance reporting, an endpoint whose definitions are more than one day old (the **Definition Grace Period** described in the preceding section) causes the policy to report as unenforced.

Action Lock Override

About this task

You can override action locks on endpoints for anti-malware enforcements. For more information about action locks, see Tanium Console User Guide: Managing action locks.

1. From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. Click Settings and then click the **Anti-Malware** tab.
2. Select the **Anti-Malware Override** option.

Distribute Over Time

About this task

©2026 Tanium Inc. All Rights Reserved

Control whether endpoints apply anti-malware enforcements the moment they receive the action (immediate) or at unique moments within the saved action interval (diffused). Diffusing enforcements over time can help prevent a surge in network traffic in exchange for a slower time to compliance.

1. From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. Click Settings and then click the **Anti-Malware** tab.
2. Select **Immediate** or **Diffused** for the **Distribute Over Time** setting.

   Note: **Distribute Over Time** settings are added when Enforce creates new managed definition packages. New packages are created whenever new definition updates are downloaded from Microsoft. To apply **Distribute Over Time** settings immediately, you can manually delete the managed definition packages and scheduled actions.

Reissue Action Interval

About this task

Control the amount of time the server waits between anti-malware enforcement action attempts.

1. From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. Click Settings and then click the **Anti-Malware** tab.
2. Set the **Reissue Action Interval**.

Configure URLs for platform updates and definitions

About this task

Machine Administrative Template policies containing anti-malware settings can use Tanium to download and distribute Windows anti-malware definitions. If enabled in the Enforce settings, Windows policies can also download and distribute Windows Defender Platform Updates. For more information, see Windows Defender platform updates on page 76. You can select one of the following options for definitions and platform updates:

- **Automatically retrieve definitions/updates from Microsoft**: (Default) Definitions and platform updates are downloaded from Microsoft.
- **Download definitions/updates from custom URLs**: Definitions and platform updates are

©2026 Tanium Inc. All Rights Reserved

downloaded from the specified URLs. Use this option if your network cannot reach Microsoft or you have an air-gapped environment, and you want to host the files on a local server.

> **Note:** These options show for platform updates in the **Managed Windows Defender Platform Updates Download URLs** section only when **Enable Platform Updates** is selected.

(Optional) Complete these steps to specify custom download URLs:

1. From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. Click Settings and then click the **Anti-Malware** tab.
2. In the **Managed Anti-Malware Definitions Download URLs** section, select **Download definitions from custom URLs**.
3. Specify the URLs for each architecture type.

   > **Note:** The URLs listed specify the Microsoft links that Enforce uses to download definitions. Replace these values with the URLs for your local hosting server.

4. If you enabled platform updates, in the **Managed Windows Defender Platform Updates Download URLs** section, select **Download updates from custom URLs**.
5. Specify the URLs for each architecture type and click **Save**.

   > **Note:** The URLs listed specify the Microsoft links that Enforce uses to download platform updates. Replace these values with the URLs for your local hosting server.

Result

> **Important:** Ensure that your security software allows outbound communication from the Tanium Module Server to the specified URLs.

Configure default rules for AppLocker

About this task

From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. Click Settings and then click **AppLocker** to access the AppLocker settings.

©2026 Tanium Inc. All Rights Reserved

In **AppLocker** settings, you can select a **Rule Template** and define default **Allow** and **Deny** rules. A *rule template* contains the default AppLocker rules that are included automatically in any AppLocker policy you create. The rule template includes **Allow** and **Deny** rules to specify which files are allowed to run or are blocked. You must include at least one **Allow** rule.

Note: AppLocker deny rules take precedence over AppLocker allow rules. For more information, see Microsoft: Understanding AppLocker allow and deny actions on rules.

Block List rule template

To access the Block List default template, from the Main menu, go to **Modules** > **Enforce**. Click Settings and then click the **AppLocker** tab. Click **Configure Default Template** > **Block List**.

The **Block List** rule template allows **Everyone** to run all applications through the **(Default Rule) All files** allow rule. This rule is the only rule that is included in this rule template by default. Define the specific applications you want to block by adding **Deny** rules.

You cannot delete or modify the **(Default Rule) All files** allow rule in this rule template because this rule template is intended to allow all files to run except those that you specifically block through a deny rule.

Note: The **Block List** rule template is the default rule template used in Enforce until you change it.

Allow List rule template

To access the Allow List default template, from the Main menu, go to **Modules** > **Enforce**. Click Settings and then click the **AppLocker** tab. Click **Configure Default Template** > **Allow List**.

The **Allow List** rule template, by default, allows only applications that **Administrators** run, or that are run out of these folders:

- **All files located in the Program Files folder**: applies to **Everyone**
- **All files located in the Windows folder**: applies to **Everyone**
- **All files**: applies to **Administrators**

©2026 Tanium Inc. All Rights Reserved

Note: The default rules in the allow list rule template are based on the Windows AppLocker default rules. For more information, see Microsoft: Understanding AppLocker default rules.

Important:

If you enforce the default **Allow List** rule template, you might block applications unintentionally. The **Allow List** rule template blocks applications without explicitly listing the applications. For example, a program run by a user out of that user's profile directory is blocked. For best results, deploy allow list policies initially in **Audit Only** mode until audit reports can be reviewed and the intended results are confirmed. For more information about an example workflow, see AppLocker policies workflow on page 191.

The Tanium Client uses BAT, EXE, and VBS files. Be sure that you do not block files in the Tanium Client directory that might break the client functions.

Best Practice: Add to the existing default rules to allow or deny applications rather than modifying the default rules. Test any modifications in audit mode first to ensure that they are running as intended before you switch to blocking mode.

Custom rule template

Use the **Custom** rule template to create your own template.

To create a custom template, from the Main menu, go to **Modules** > **Enforce**. Click Settings and then click the **AppLocker** tab. Click **Configure Default Template** > **Custom**.

Create Default AppLocker rules

About this task

Use rule exceptions to specify files or folders to exclude from a default AppLocker rule. You can create default executable rules, default Windows Installer rules, and default script rules.

1. From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. Click

©2026 Tanium Inc. All Rights Reserved

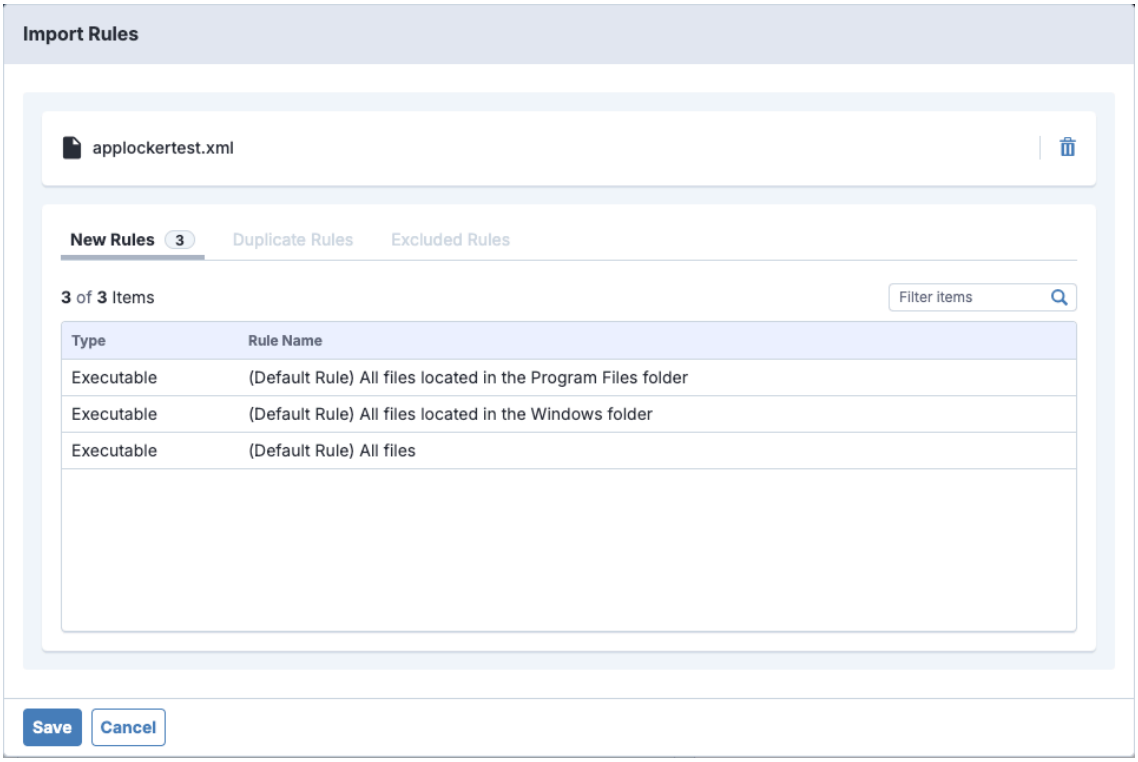
Settings and then click the **AppLocker** tab.

2. Click a tab: **Executable**, **Windows Installer**, or **Script**. Then click **Configure Default Template** and select a template: **Allow List**, **Block List**, or **Custom**.

3. (Optional) To import AppLocker rules to the default rules, click **Import Rules**.

   > **Note:** You can import rules using the XML files generated in the AppLocker section of the Windows **Local Security Policy Tool** or an exported Enforce AppLocker policy to quickly add multiple rules to a policy.

   a. Click **Browse for File** in the **Import Rules From XML** section.
   b. Select the XML file that contains the exported AppLocker rules and click **Open**.
   c. The **Import Rules** window shows up to three tabs, depending on the content in the XML file: the new rules added to the policy from the imported XML file, duplicate rules, and the rules Enforce cannot import.



   d. Click **Save** to import the XML.

4. (Optional) To manually add rules to the default rules, click **Add Rule**.
   a. Specify a **Name** for the rule.
   b. Select an **Action** for the rule.
      - **Deny** rules prevent the specified files from running on endpoints where the policy is enforced.

©2026 Tanium Inc. All Rights Reserved

- **Allow** rules let the specified files run on endpoints where the policy is enforced.

> **Note:**
> AppLocker **Deny** rules take precedence over AppLocker **Allow** rules. You must include at least one **Allow** rule. For more information about best practices and rule precedence, see Configure default rules for AppLocker on page 82.
>
> Be aware of AppLocker allow or deny rules that are set in your Domain Policy. These rules might take precedence over AppLocker rules created in Enforce.

> **Best Practice:** The Tanium Client uses BAT, EXE, and VBS files. Be sure that you do not block scripts in the Tanium Client directory that might break the client functions.

c. Select **Everyone** or **Administrators** for the **Windows User**.
d. In the **Type** section, select **Hash**, **Path**, or **Publisher**.
e. Specify the settings for the file:
   - If you selected **Hash**, click **Add Condition** and provide the **Hash** and optional file size in bytes.

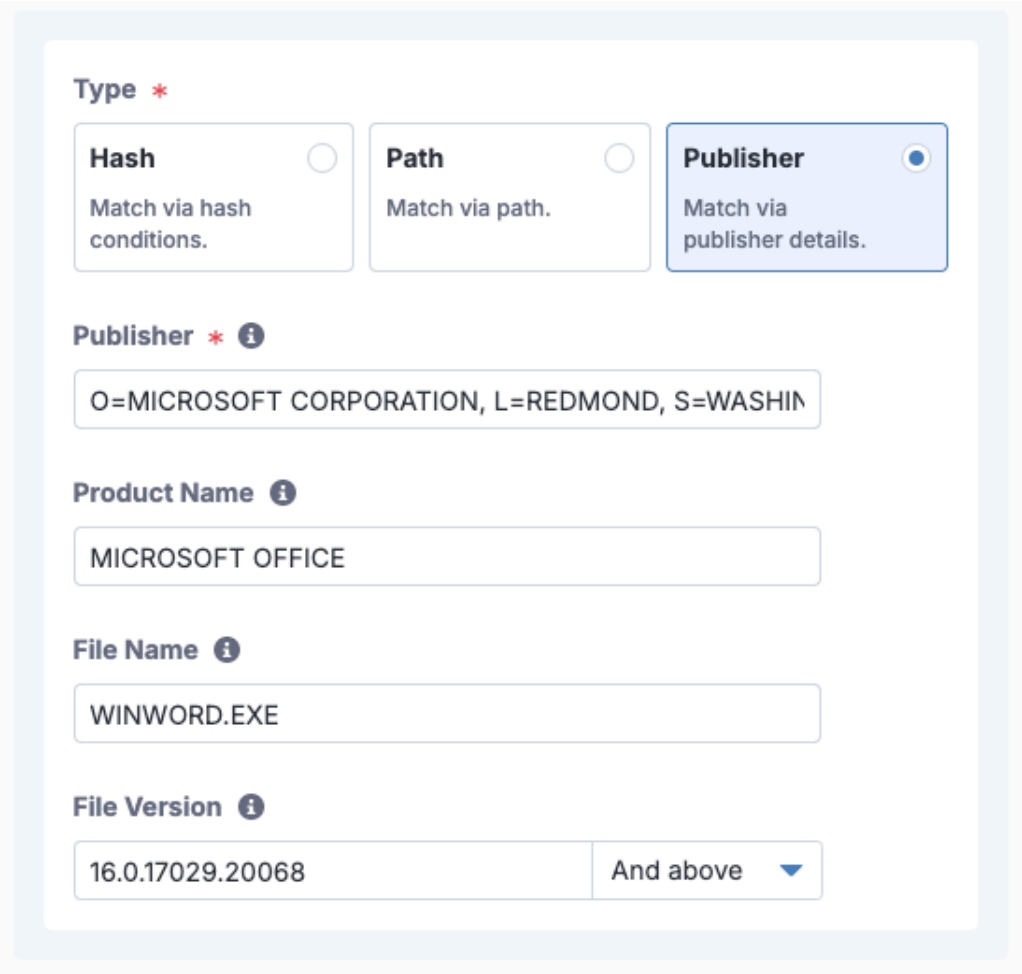
> **Important:** For best results, use a utility other than the Get-AppLockerFileInformation cmdlet to generate the SHA-256 hash. For example, you can use Get-FileHash to generate the hash. Hashes generated with Get-AppLockerFileInformation are different than hashes generated by other utilities and are not supported by Enforce. For more information about Get-FileHash, see Microsoft Documentation: Get-FileHash.

   - If you selected **Path**, provide the file path or file name including the path to the file.

   - If you selected **Publisher**, provide the **Publisher**, **Product Name**, **File Name**, and **File Version**, using the dropdown list to indicate whether you want earlier or later versions included or only the version you specify.

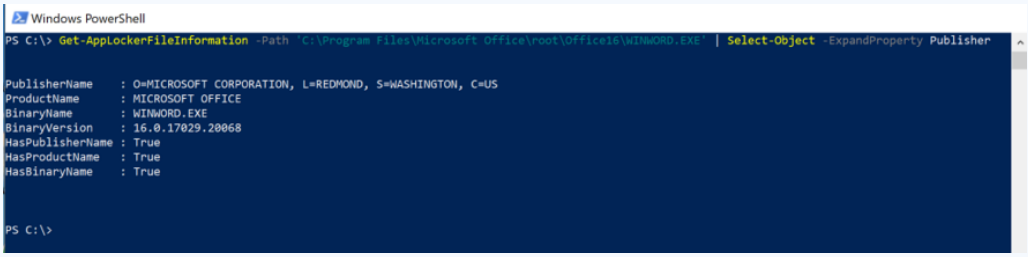
©2026 Tanium Inc. All Rights Reserved

Important: You can use the `*` character as a wildcard character only for the entire value. Partial wildcard values are not valid for any of these values.



©2026 Tanium Inc. All Rights Reserved

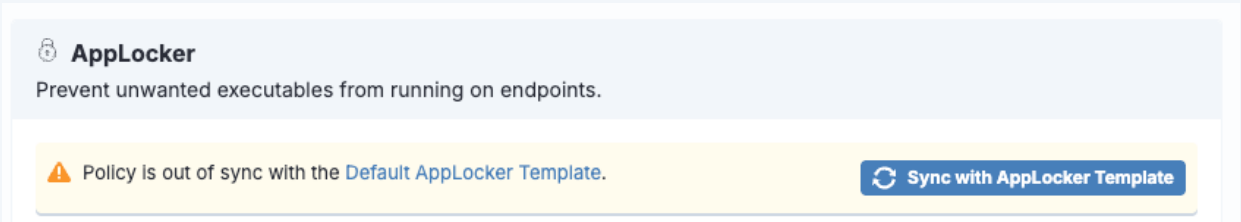
Best Practice: Use the Get-AppLockerFileInformation cmdlet to determine the publisher information. For example: `Get-AppLockerFileInformation -Path 'C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE' | Select-Object -ExpandProperty Publisher`



Ensure that you correctly capture and include any special characters, such as ®. For more information about the Get-AppLockerFileInformation cmdlet, see Microsoft Documentation: Get-AppLockerFileInformation.

5. Configure additional rules as needed.
6. Click **Save**. Select **Apply AppLocker template to existing policies** if you want to apply the changes to existing AppLocker policies, and then click **Save**.

Note: If an existing AppLocker policy is not in sync with the current AppLocker template, a message appears when you open the policy. Click Sync with AppLocker Template to sync the policy with the template.



Configure endpoint encryption

Install Shared Services and endpoint tools

About this task

Tanium BitLocker and FileVault policies require the installation of shared services. The **Endpoint**

©2026 Tanium Inc. All Rights Reserved

Encryption tab of the Enforce settings includes a checklist to show you the status of each of the required services. For more information about shared service version requirements, see Feature-specific dependencies on page 30.

1. The End-User Notifications service must be installed and the End-User Notifications endpoint tool must be pushed out to endpoints where the BitLocker or FileVault policy is enforced.
2. The Direct Connect service must be installed and the Direct Connect endpoint tool must be pushed out to endpoints where the BitLocker or FileVault policy is enforced.
3. Tanium Core Content must be installed and pushed out to endpoints.

Result

For more information, see Client Management User Guide: Client extensions and endpoint tools used for Tanium solutions.

For more information about additional requirements for using BitLocker and FileVault policies, see Reference: Windows encryption management on page 223 and Reference: macOS encryption management on page 234.

Note: You can create BitLocker and FileVault policies even if one or more of these components are not in place, but the policy is not successfully enforced until the entire configuration is on the endpoint.

Manage Windows device classes and devices

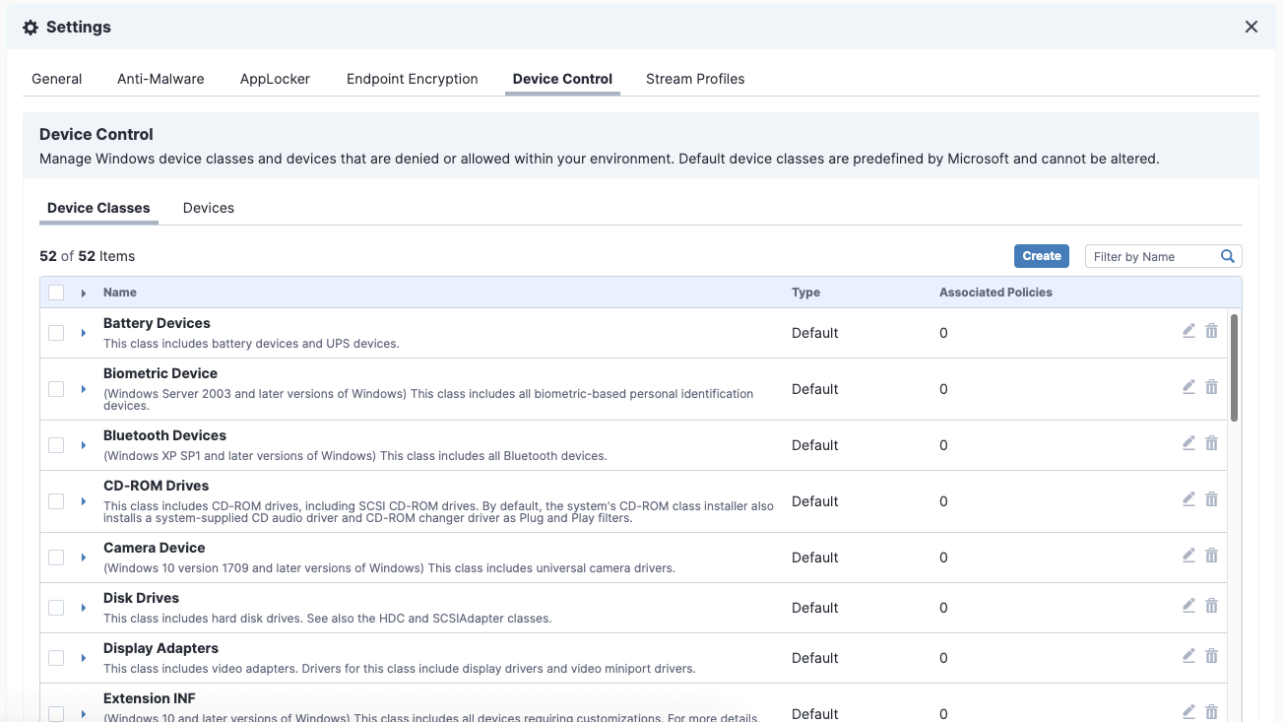
From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. Click Settings and go to **Device Control** to manage the global list of Windows device classes and devices for use with Windows device control policies.

Device Classes

The list includes the predefined device classes that are provided by Microsoft and any additional device classes that were added, either from this page or through a device control policy. Click **Device Classes** to manage the global list of device classes.

Figure 3. List of device classes

©2026 Tanium Inc. All Rights Reserved



- Use the sort menu to sort the list by **Name**, **Type**, or **Associated Policy**.
- Use the **Filter by name** field to filter the list by a specific name.
- Click **Create** to add a custom device class to the global list.
- You can edit or delete custom device classes that are not associated with a policy:
    - Select a custom device class and click **Edit** to update the configuration for that device class.
    - Select a custom device class and click **Delete** to delete that device class.

Note: Only custom device classes that are not associated with a policy can be modified or deleted. You cannot modify or delete default device classes or custom device classes that are associated with a policy.

Devices

This list includes devices that were added from this page or through a device control policy. Click **Devices** to manage the global list of devices.

©2026 Tanium Inc. All Rights Reserved

- Use the sort menu to sort the list by **Name** or **Associated Policy**.
- Use the **Filter by name** field to filter the list by a specific name.
- Click **Create** to add a new device to the global list.
- Select a device that is not associated with a policy and click **Edit** to update the configuration for that device.
- Select a device that is not associated with a policy and click **Delete** to delete that device.

Note: Only devices that are not associated with a policy can be modified or deleted. You cannot modify or delete devices that are associated with a policy.

For more information, see Device Control - All Devices on page 110.

Manage Stream profiles

With Tanium Stream, you can send events generated from Tanium Removable Storage Access Control policies or cluster policies to external Splunk destinations using an HTTP Event Collector (HEC) or TCP connection. With Stream profiles, you can create different Stream configurations to target specific endpoints.

Note:

- Tanium Removable Storage Access Control policies are available only for Windows endpoints.
- Cluster policies are available only when Cloud Workloads is installed.
- You must have the Enforce Endpoint Configuration All permission to create a Stream profile.

Create a Stream profile

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. Click Settings and then click **Stream Profiles** > **Create**.
2. Enter a **Name** and optional **Description** for the profile.
3. Select a **Management Method**:
    - **Automated**: Specify configuration parameters to generate the profile. If you select **Automated**, complete the subsequent steps.
    - **File Upload**: Upload a JSON file of a Stream configuration that you previously exported. If you select **File Upload**, click **Browse for File** and select a JSON file to upload that contains the configuration parameters for the Stream configuration. Skip to Step 6.
4. In the **Events** section, select the event types that you want to stream:
    - (Tanium Removable Storage Access Control policies) **Device Inserted**
    - (Tanium Removable Storage Access Control policies) **Device Removed**
    - (Tanium Removable Storage Access Control policies) **Device Blocked Mount**
    - (Tanium Removable Storage Access Control policies) **Device Blocked File Access**
    - (Cluster policies) **Cluster Violations**: when a cluster policy denies an operation for a cluster

    At least one event type is required. Audit log entries for blocking events are identified with the policy ID and name. Events corresponding to read/write or read only rules in a policy are logged with the policy ID, policy name, and the rule name for the rule that allowed access.
5. In the **Destination** section, select a **Destination Type** and provide the associated configuration settings:

    Splunk HEC
    - **URL**: The URL or IP address to access the Splunk REST API.
    - **Authorization Token**: The authorization token to access your Splunk environment. Do not include the `Splunk` prefix in this token.
    - (Optional) If you want to use a proxy to provide a gateway, provide the host, port, and a username and password for the proxy in the **Proxy** section.
    - (Optional) Select **Allow Unsigned Certificates** in the **Advanced Settings** to disable the validation of the certificate presented by the destination.

©2026 Tanium Inc. All Rights Reserved

Splunk TCP

- **Host**: The fully-qualified Splunk host domain name or IP address.
- **Port**: The port for the stream communication to the host.

Select **Dry Run** if you want to collect statistics about the data that would be streamed to the destination, but not actually send data.



Best Practice: Select **Dry Run** when you first create a stream configuration. Analyze the amount of event data that would be streamed to a destination before you deselect **Dry Run**. While this setting is enabled, no data is streamed to a destination; it must be disabled for data streaming to occur.

You can use the Enforce - Daily Stream Stats sensor to gain an understanding of the amount of data that would be sent.

6. Click **Select Computer Groups** and select the computer groups from which you want to send events generated by Tanium Removable Storage Access Control policies to an external Splunk destination.
7. In the **Additional Filtering Criteria** section, specify additional filtering parameters as needed:
   - **None**: Select **None** to use the selected computer groups with no additional filtering applied.
   - **Specify Individual Endpoints**: Provide a case-insensitive, comma-separated list of computer names. Due to a possible performance impact, this list cannot exceed 50 entries. Duplicate entries are ignored.
   - **Ask a question**: Ask a question to filter the selected computer groups. For example, if the selected computer groups contain non-Windows endpoints, you can filter the endpoints by asking the question: `Operating System contains Windows`.
   - **Define a Rule**: Define a rule to use when filtering the selected computer groups.
8. Click **Create**.

Prioritize Stream profiles

About this task

If an endpoint is targeted by multiple Stream profiles, the profile with the highest priority applies to

©2026 Tanium Inc. All Rights Reserved

that endpoint. The profile with the highest priority has the lowest priority number. For example, a profile with a priority of 1 takes precedence over a profile with a priority of 10.

1. From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. Click Settings and then click **Stream Profiles** > **Prioritize**.
2. Click and drag the profiles to set the priority. Click **Save**.

Take actions on Stream profiles

About this task

You can delete, edit, duplicate, or export Stream profiles.

1. From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. Click Settings and then click **Stream Profiles**.
2. Select a profile.
3. Click **Actions** and select an action to take on the profile:
   - **Delete**: Delete the selected profile.
   - **Edit**: Edit the selected profile.
   - **Duplicate**: Create a new Stream profile using the settings in the selected profile as a starting point.
   - **Export**: Export the selected profile in JSON format, which you can apply in a different Enforce environment. For example, you can export profiles that you have tested from a lab environment and import them into a production environment.

Next steps

Create policies

Create policies for endpoints. For more information, see Creating policies for Windows endpoints on page 96, Creating policies for macOS endpoints on page 136, and Creating policies for Linux endpoints on page 139.

Enforcements

After policies are configured, create enforcements to apply them to endpoints. For more information,

©2026 Tanium Inc. All Rights Reserved

see Enforcing policies on page 163.

©2026 Tanium Inc. All Rights Reserved

Creating policies for Windows endpoints

About this task

Configure policies to manage and secure endpoints across environments by providing control and visibility to all devices. Policies contain *policy settings*, which are specific settings and controls contained within the policy.

1. From the Main menu, go to **Modules** > **Enforce** > **Policy Configurations** > **Create**.
2. Specify a **Name** and optional **Description**.
3. Click **Select Types**.
4. Select **Windows** as the **Platform** for the endpoints that you want to target with the policies.
5. Select the policy types for the policy.
   Use the search field in the **Select Policy Types** modal to filter the list by policy type name and description. Select **Search settings** to also match on setting metadata within each policy type.

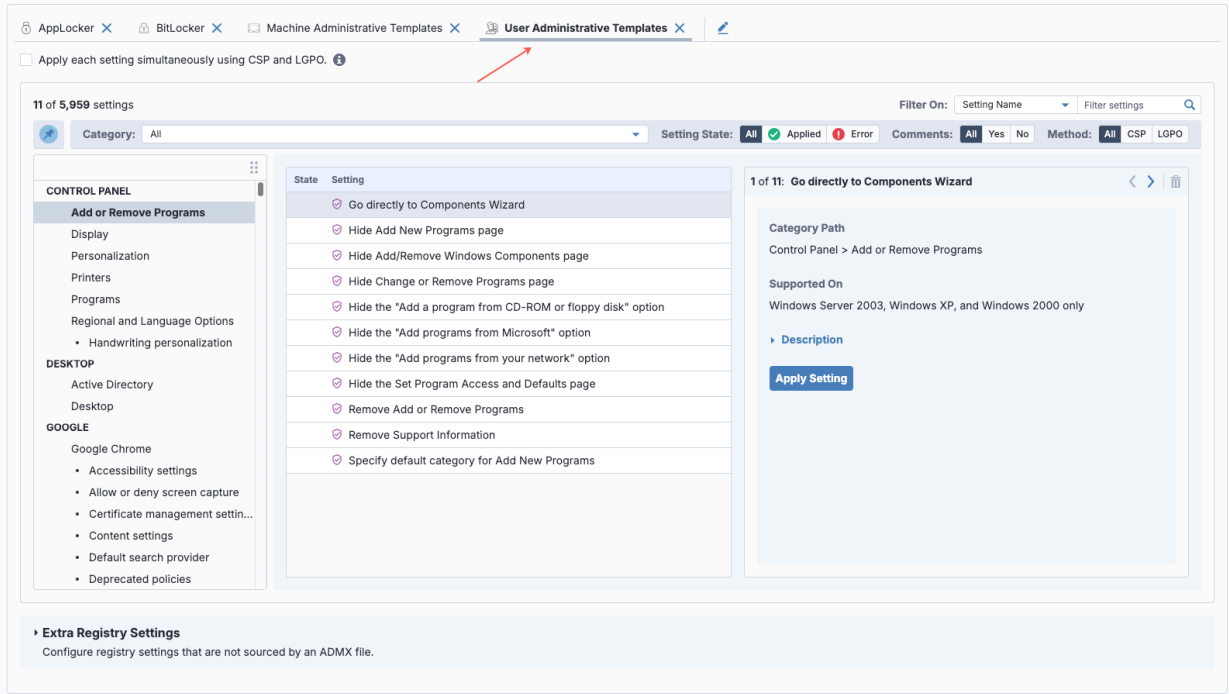
   

   Note:

   - Only Windows policies can include more than one policy type.
   - SRP Management policy types cannot be combined with other policy types.

6. If you do not want to use the default content set for the policy, select a **Content Set**.
   Every policy requires a content set. The content set is configured by default to the platform for the selected policy types, provided that you have the necessary permissions for that content set. If no content set is available, you might need additional permissions. For more information, see Tanium Console User Guide: Role permissions for content sets.
7. Configure the policy settings.
   The available settings vary based on the selected policy types. Click the tab for each policy type to configure the settings for that policy type.

©2026 Tanium Inc. All Rights Reserved



To add or remove policy types, click Edit Type .

For configuration details about the settings for each policy type, see the corresponding topic:

Policy type settings

Policy type	Description
AppLocker on page 98	Prevent unwanted executables from running on endpoints.
BitLocker on page 103	Secure drives on Windows endpoints using Microsoft BitLocker Drive Encryption.
Device Control - All Devices on page 110	Block installation of new devices, allowing only devices specified by device class or hardware ID, using native Windows functionality.
Device Control - Removable Storage on page 113	Deny read or write access to removable storage devices, such as USB, CD/DVD, and floppy drives, using native Windows functionality.
Windows firewall management on page 114	Create rules that block or allow network traffic using the built-in Windows Firewall.
Machine administrative template on page 117	Use ADMX group policy objects to apply consistent rules to Windows endpoints, regardless of the logged-in user.
SRP Management on page 124	Block the execution of applications using the Microsoft Windows Software Restriction Policy (SRP) component.

©2026 Tanium Inc. All Rights Reserved

Policy type	Description
Security Settings on page 125	Protect endpoints from malicious threats using Windows operating system security settings.
Tanium Removable Storage Access Control on page 129	Block or allow access to USB devices on endpoints using Tanium-managed exception rules.
User Administrative Template on page 130	Use ADMX group policy objects to apply consistent rules to Windows endpoints, based on the logged-in user.

Next steps

After you finish configuring the policy types and settings, click **Create** to save the policy.

Enforce the policy to apply the settings to targeted endpoints. Enforce all policies except remediation policies from the **Enforcements** tab of the **Policy Configurations** page. For more information, see Enforcing policies on page 163.

> **Note:** Enforce remediation policies from the **Enforcements** tab of the **Device Actions** page. For more information, see Managing device actions on page 176.

AppLocker

> **Note:** For successful AppLocker rule enforcement, Enforce starts the Application Identity service on the endpoint.

The Enforce settings include default rule templates for each rule type used in AppLocker policies. The **Block list** rule template is used by default until you change it. For more information about changing the default rule templates, see Configure default rules for AppLocker on page 82.

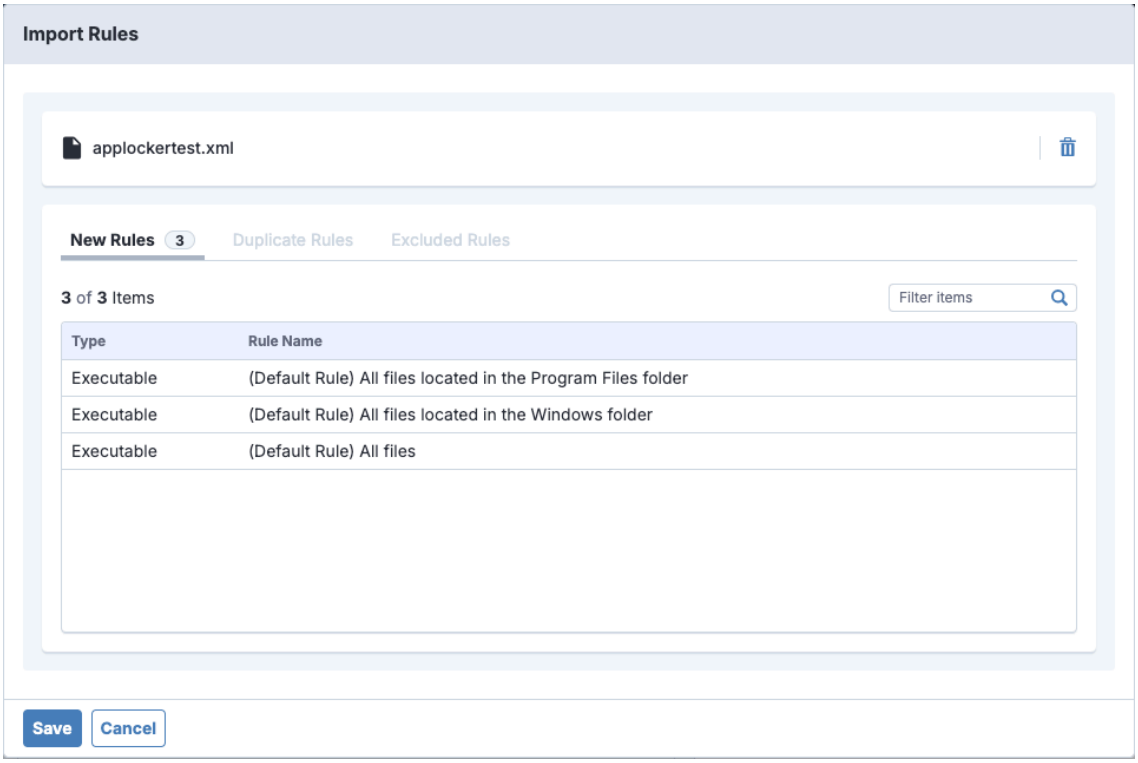
Only one AppLocker policy is in effect on an endpoint at a given time. Therefore, if you want to enforce rules for multiple app types (**Executable**, **Windows Installer**, or **Script**) on a particular endpoint, you must use one policy with AppLocker rules for each app type (and not a separate policy for each one). If there are multiple policies with the same policy type applied to an endpoint, the

©2026 Tanium Inc. All Rights Reserved

priority of the policy is used to resolve the conflict.

Configure the AppLocker policy

1. Select the tab for the app type that you want to configure rules for and click **Enable**.
2. Select whether the rules for the app type are **Audit Only** or **Blocking**. For more information, see AppLocker policies workflow on page 191.
3. (Optional) To import AppLocker rules in addition to the default rules, click **Import Rules**.
    a. Click **Browse for File** in the **Import Rules From XML** section.
    b. Select the XML file that contains the exported AppLocker rules and click **Open**.
    c. The **Import Rules** window shows up to three tabs, depending on the content in the XML file: the new rules added to the policy from the imported XML file, duplicate rules, and the rules Enforce cannot import.



    d. Click **Save** to import the XML.

©2026 Tanium Inc. All Rights Reserved

> **Note:** You can import rules using the XML files generated in the AppLocker section of the Windows **Local Security Policy Tool** or an exported Enforce AppLocker policy to quickly add multiple rules to a policy.

4. (Optional) To manually add rules in addition to the default rules, click **Add Rule**.

    a. Specify a **Name** for the rule.

    b. Select an **Action** for the rule.

    - **Deny** rules prevent the specified files from running on endpoints where the policy is enforced
    - **Allow** rules let the specified files run on endpoints where the policy is enforced

    > **Note:**
    >
    > AppLocker **Deny** rules take precedence over AppLocker **Allow** rules. You must include at least one **Allow** rule. For more information about best practices and rule precedence, see Configure default rules for AppLocker on page 82.
    >
    > Be aware of AppLocker allow or deny rules that are set in your Domain Policy. These rules might take precedence over AppLocker rules created in Enforce.

    > **Best Practice:**
    >
    > Add to the existing default rules to allow or deny files rather than modifying the default rules. Test any modifications in audit mode first to ensure that they are running as intended before you switch to blocking mode.
    >
    > The Tanium Client uses BAT, EXE, and VBS files. Be sure that you do not block scripts in the Tanium Client directory that might break the client functions.

    a. Select **Everyone** or **Administrators** for the **Windows User**.

    b. In the **Type** section, select **Hash**, **Path**, or **Publisher**.

©2026 Tanium Inc. All Rights Reserved

c. Specify the settings for the file:

- If you selected **Hash**, click **Add Condition** and provide the **Hash** and optional file size in bytes.

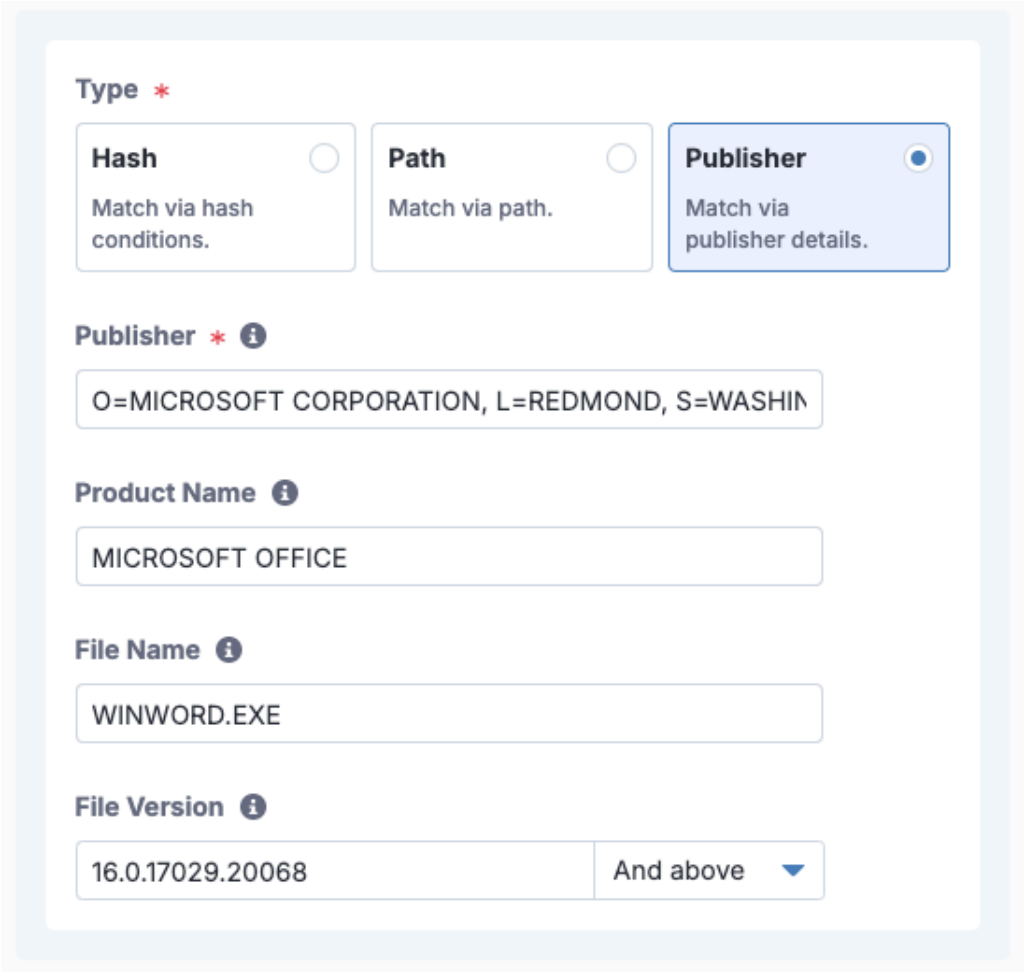
  > **Important:** For best results, use a utility other than the Get-AppLockerFileInformation cmdlet to generate the SHA-256 hash. For example, you can use Get-FileHash to generate the hash. Hashes generated with Get-AppLockerFileInformation are different than hashes generated by other utilities and are not supported by Enforce. For more information about Get-FileHash, see Microsoft Documentation: Get-FileHash.

- If you selected **Path**, provide the file path or file name including the path to the file.

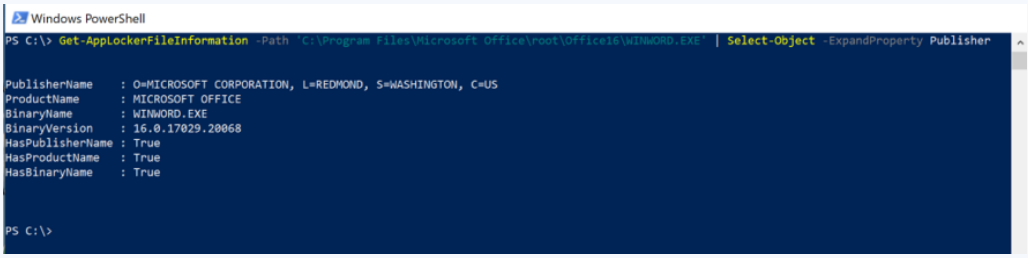
- If you selected **Publisher**, provide the **Publisher**, **Product Name**, **File Name**, and **File Version**, using the dropdown list to indicate whether you want earlier or later versions included or only the version you specify.

  > **Important:** You can use the `*` character as a wildcard character only for the entire value. Partial wildcard values are not valid for any of these values.

©2026 Tanium Inc. All Rights Reserved



Best Practice: Use the Get-AppLockerFileInformation cmdlet to determine the publisher information. For example: `Get-AppLockerFileInformation -Path 'C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE' | Select-Object -ExpandProperty Publisher`



Ensure that you correctly capture and include any special characters, such as ®. For more information about the Get-AppLockerFileInformation cmdlet, see Microsoft Documentation: Get-AppLockerFileInformation.

©2026 Tanium Inc. All Rights Reserved

5. (Optional) Click the **Settings** tab and provide a **Support URL** if you want to display a custom URL when a user tries to run an app that is blocked.

6. Click another policy type tab to configure more settings or click **Create** to create the policy.

For more information about AppLocker event logs, see Review AppLocker event logs on page 208.

Creating policies for Windows endpoints on page 96

BitLocker

Note: Complete the steps detailed in the Configure endpoint encryption on page 88 section before you create BitLocker policies.

Important notes for working with BitLocker and legacy BitLocker policies

Best Practice: Recreate existing legacy BitLocker policies using the new BitLocker policy type so that endpoints use the new functionality for application of the settings (using Client Extensions) which provides better resiliency.

When you enforce a BitLocker policy on an endpoint with settings compatible with an existing enforcement of a legacy BitLocker policy (for example, uses the same encryption type), any existing legacy BitLocker policies are automatically unenforced on that endpoint and report **Not applied** as the **Enforcement Status** in the enforcement. Settings that are available only in BitLocker policies are not considered to be a conflict with existing legacy BitLocker settings. In this scenario, the BitLocker policy is now the enforced encryption policy on the endpoint.

If you enforce a BitLocker policy on an endpoint with settings that are not compatible with an existing enforcement of a legacy BitLocker policy on the endpoint, such as a different encryption type, the legacy BitLocker policy is unenforced and reports **Not applied** as the **Enforcement Status** in the enforcement. The BitLocker policy enforcement status shows the applicable enforcement errors for targeted endpoints and is not enforced on the endpoint. To resolve this scenario, update the BitLocker policy to match the settings in the legacy BitLocker policy. Settings that are available only in BitLocker policies are not considered to be a conflict and can remain. If you want to change the existing settings when you enforce a BitLocker policy on an endpoint where a legacy BitLocker

©2026 Tanium Inc. All Rights Reserved

policy is already enforced, you must decrypt all drives and then enforce the policy so that it can reapply and encrypt the drives using the updated settings.

Important: BitLocker policies always supersede legacy BitLocker policies, even if the legacy BitLocker policy has a higher priority.

Create a BitLocker policy

Tip: Optionally, you can configure a self-service recovery portal that users can access if they forget their PIN or password. For more information, see Reference: Encryption key recovery portal on page 241.

Enforce uses AES 256-bit encryption when storing BitLocker recovery keys, which is FIPS 140-2 compliant. When a BitLocker policy is enforced on an endpoint, Enforce uses the native Windows BitLocker functionality for device encryption, which can be configured to use AES 256-bit encryption in the global policy settings for **Software** and **Hardware and Software** encryption types.

Settings that can be applied using a configuration service provider (CSP) are annotated with this icon . Hover over the icon to see the earliest supported operating system for policy application using a CSP. For more information about Enforce policy application using a CSP, see Configuration service providers (CSPs) on page 163.

Configure the primary encryption settings

In the **BitLocker Encryption** section of the BitLocker policy, configure the primary encryption settings:

1. Configure these settings on the **Global Settings** tab:
    - Select the **Encryption Type**: **Software**, **Hardware and Software**, or **Hardware**.

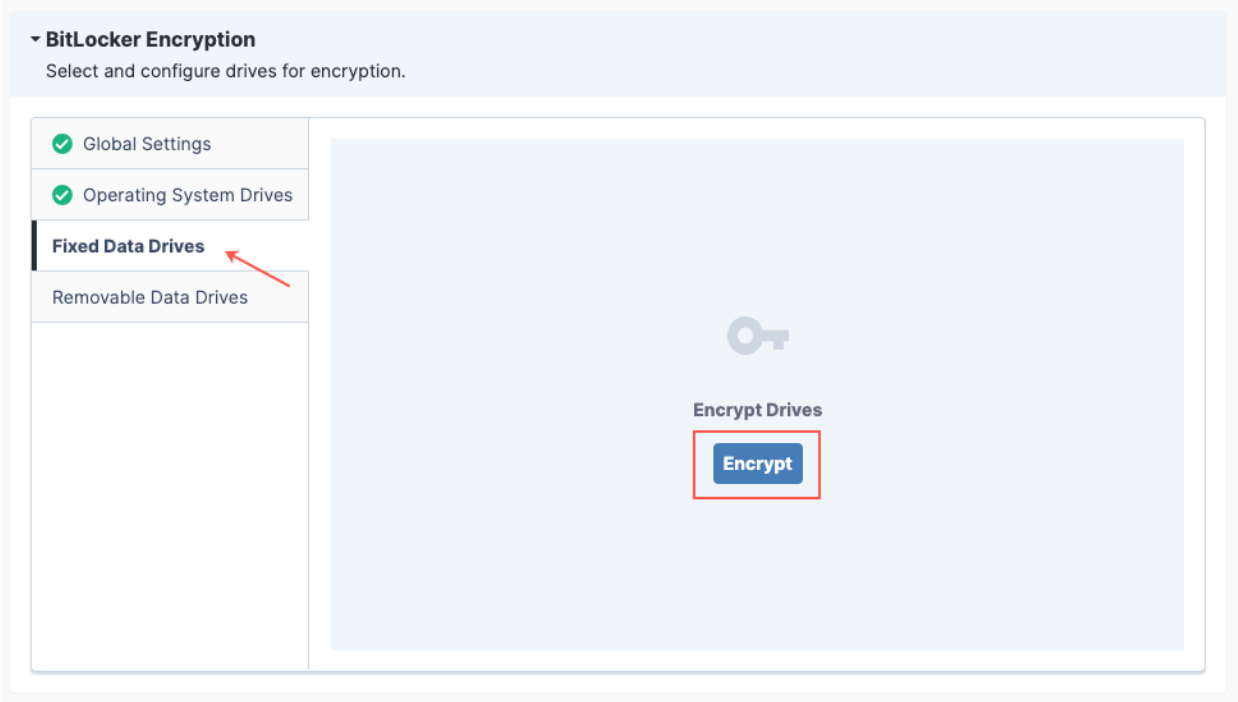
©2026 Tanium Inc. All Rights Reserved

> **Note:**
>
> - If you select **Hardware and Software**, BitLocker software-based encryption is used if the drive does not support hardware-based encryption.
> - If you select **Software** or **Hardware and Software**, set the **Encryption Method** for each operating system.

- Select the time period for the **Recovery Key Rotation**.

> **Important:** Due to Microsoft Windows OS limitations, if you change the protection settings in an existing BitLocker policy, including most of the settings in the **BitLocker Encryption** section, you must decrypt endpoints and re-encrypt them again for the changes to be applied.

2. Configure at least one drive type for encryption. To configure a drive type, click the tab for the drive type and click **Encrypt**.



Then specify the settings for the drive type:

©2026 Tanium Inc. All Rights Reserved

Note:

- **Operating System Drives** are enabled by default.
- You must configure operating system drive encryption if you want to configure fixed data drive encryption.

- **Operating System Drives**:

  a. Select **Full Disk** or **Used Disk Space Only**. For more information about this option, see Microsoft Documentation: Used Disk Space Only encryption.

  b. For computers that have a TPM chip, specify the behavior of the computer at startup or reboot when the drive is encrypted:

  TPM only

  If you choose **TPM only**, the drive is unlocked at startup or reboot using the integrated TPM chip with no user interaction.

  Note: With TPM only, the drive can be encrypted when no end user is signed in to the computer. Keys are backed up to the Tanium database. One or more reboots are required, and you can use a Tanium package to accomplish that. It is recommended that you monitor the system status and push the reboot when needed.

  TPM and PIN

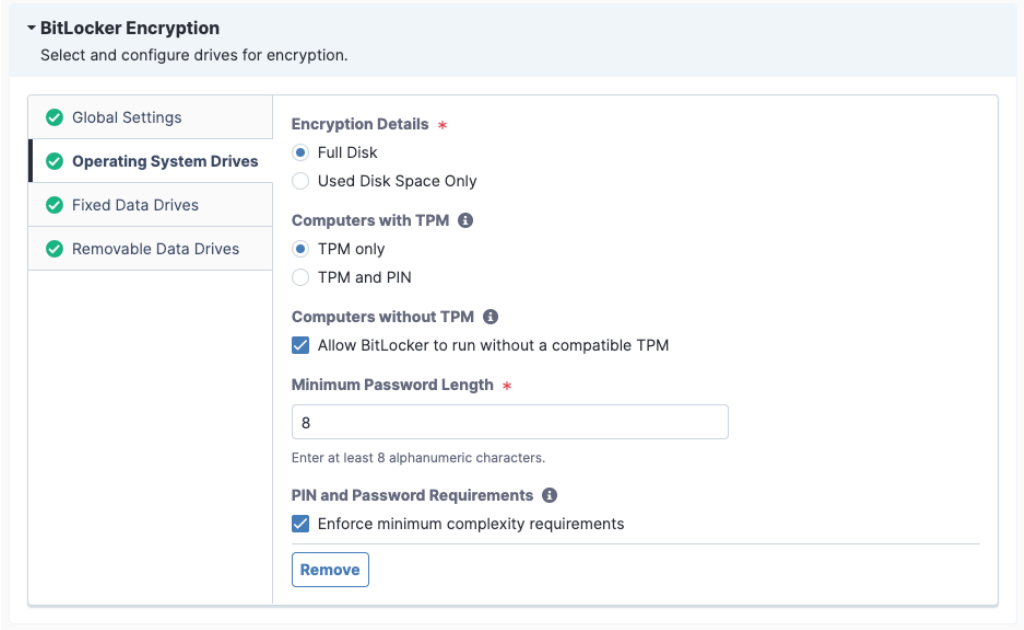
  If you choose **TPM and PIN**, the user configures a PIN during the initial BitLocker setup on the computer. The user must enter that PIN when the computer starts or reboots.

  If you use a PIN, you must set the **Minimum PIN Length**. Set this value to a number between 4 and 20. By default, PINs can include only numbers. If you want to allow PINs to include uppercase and lowercase letters, symbols, numbers, and spaces, select **Enhanced PIN**. If you do not want to allow PINs

©2026 Tanium Inc. All Rights Reserved

or passwords that consist of all the same character (`11111111`) or a sequence of characters (`12345678`), select **Enforce minimum complexity requirements**.

c. (Optional) For computers without a TPM chip, specify whether you want to **Allow BitLocker to run without a compatible TPM** and specify a minimum password length. If you select this option, you can enforce the policy on computers that do not have a compatible TPM chip. Users must enter a password to access the encrypted drive. You can also specify whether you want to **Enforce minimum complexity requirements** for PINs or passwords to prevents PINs from using duplicate or sequential characters.



Tip: If you do not want to configure operating system drive encryption, click **Remove**.

- **Fixed Data Drives**:
  - Select **Full Disk** or **Used Disk Space Only**. For more information about this option, see Microsoft Documentation: Used Disk Space Only encryption.

Tip: If you do not want to configure fixed data drive encryption, click **Remove**.

©2026 Tanium Inc. All Rights Reserved

- **Removable Data Drives**:
    - Select **Full Disk** or **Used Disk Space Only**. For more information about this option, see Microsoft Documentation: Used Disk Space Only encryption.

      Important: To apply removable disk encryption setting updates, reboot the targeted endpoints after you enforce the BitLocker policy.

      Tip: If you do not want to configure removable data drive encryption, click **Remove**.

    For more information about these settings, see Microsoft Documentation: BitLocker Policy settings.

Note: If needed, configure additional settings for drive types using a **Machine Administrative Template** policy type.

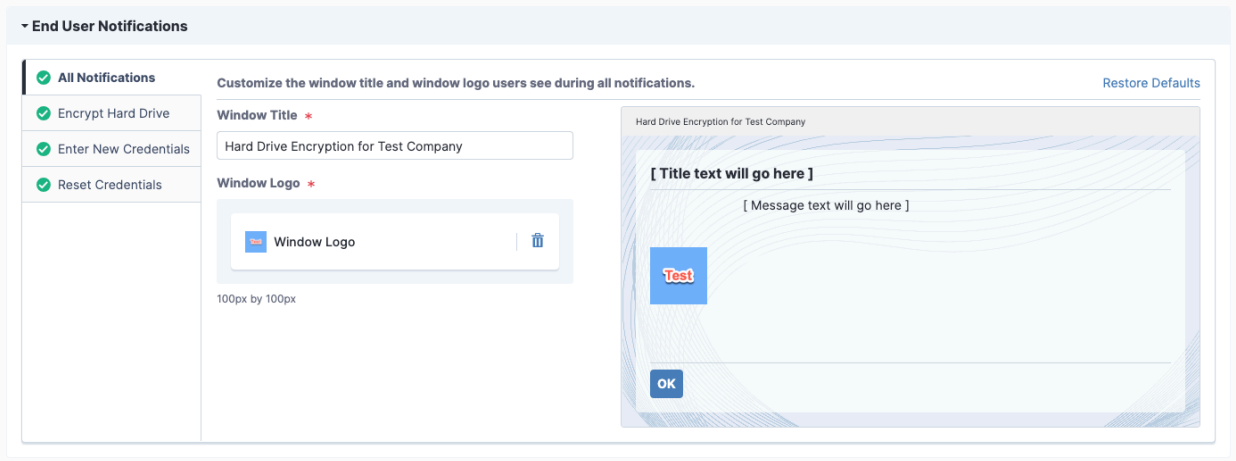
Configure the End User Notifications settings

Configure the notifications that end users receive during the encryption process in the **End User Notifications** section of the BitLocker policy.

Note: The settings that appear in this section are determined by the BitLocker settings that you selected. You might not see all of the settings described in this section.

1. On the **All Notifications** tab, select or drag an image file (GIF, JPG/JPEG, PNG, or SVG) for the **Window Logo** and enter a **Window Title** to use in the notifications window for all BitLocker notifications.

©2026 Tanium Inc. All Rights Reserved



2. On the **Encrypt Hard Drive** tab, provide the notification **Title** and **Message** that you want users to see when their computers are required to be rebooted again to encrypt their hard drives. This message displays when the hard drive is prepared for encryption, which occurs after the first reboot. This message prompts users to reboot their computer when possible to start the encryption.

   Best Practice: Inform users that drive encryption is not a disruptive process and that they can continue to work while encryption is in progress.

3. On the **Enter New Credentials** tab, provide the notification that you want users to see when they must create a new password to unlock their computers. This option appears when you select TPM and PIN for operating system drives.

4. On the **Enter Reset Credentials** tab, provide the notification that you want users to see when they are required to reset their credentials. This option appears when you select TPM and PIN for operating system drives.

5. Click **Create**.

Manage encrypted endpoints

For more information about managing encrypted Windows endpoints, including managing recovery keys, see Reference: Windows encryption management on page 223.

Creating policies for Windows endpoints on page 96

©2026 Tanium Inc. All Rights Reserved

Device Control - All Devices

Windows device control policies provide two modes for administering devices on Windows endpoints: removable storage or all devices. The **Device Control - All Devices** policy type restricts the installation of new devices. This advanced mode provides more granular control by using a list-based approach. With this mode, the installation of any new device is blocked unless the device is explicitly allowed by either the device class or the hardware ID of the device. Optional settings allow administrators to bypass all restrictions and to uninstall existing USB storage devices that are not on the allowed list of devices. On the endpoint, the permissions are managed using local group policy settings located in **Administrative Templates** > **System** > **Device Installation** > **Device Installation Restrictions**.

Note: Complete the steps in the Manage Windows device classes and devices on page 89 section before configuring device control policies.

CAUTION: This mode blocks new installations of all devices by default and includes an optional setting to uninstall existing USB storage devices that are not on the policy allow list. All other existing devices remain installed and unblocked, including devices that are not currently connected but were installed previously. You must add devices to the policy allow list to allow installation to endpoints. Carefully test configurations and their impacts before you deploy them widely.

1. (Optional) In the **General Device Rules** section, configure the following settings:

    a. In the **Administrator Permissions** section, select the **Allow Administrators to bypass all restrictions** option to enable users to bypass the restrictions if they are signed in as an administrator.

    Note: Devices do not install automatically when this option is selected. Administrators must manually install the device through Device Manager.

    b. In the **Existing USB Devices** section, select the **Uninstall existing USB storage devices not on the allowed list of devices** option to uninstall USB storage devices that are not on the allow list.

©2026 Tanium Inc. All Rights Reserved

> **Note:** As a safeguard against uninstalling devices that are required for the system to run, other devices that are currently installed on an endpoint, including devices that are not currently connected but were installed previously, are not uninstalled when this option is selected. If the USB storage device is in use when the policy is enforced on the endpoint, the device is uninstalled at the next reboot of the endpoint. In this scenario, the policy status sensor returns a status indicating that prohibited devices are still installed.

2. On the **Device Classes** tab, define groups of devices that you want to allow in your environment. Many device classes are predefined by Microsoft, and you can define custom device classes. Each device class has a globally unique identifier (GUID). For more information about device classes, see Microsoft Documentation: Windows Hardware Developer: System-Defined Device Setup Classes Available to Vendors. When you add a device class, it is stored in the global device class list, which you can access from the **Settings** page.

   > **Note:** If you add a device by device class, you must allow all of the device nodes in the device tree for that class. For example, if you want to allow the installation of a USB storage device, you must allow the installation of **Disk Drives** and **USB Bus Devices (hubs and host controllers)**. For more information, see Microsoft Documentation: Windows Hardware Developer: Device nodes and device stacks.

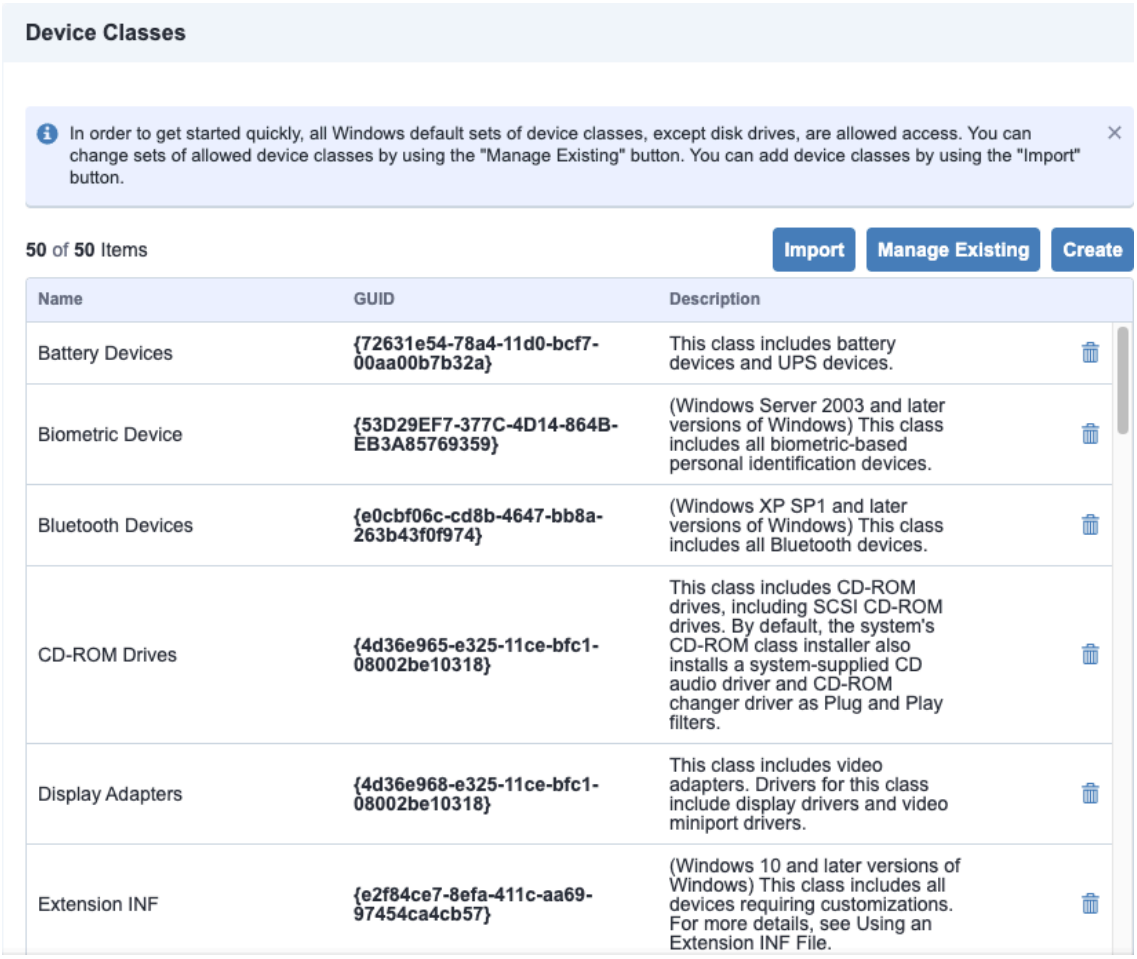
   - Click **Import** to query all Windows endpoints for their installed device classes and import them to the allow list. With this option, you can quickly add any custom device classes that might be used in your environment. Device classes that are already known to Enforce, marked with a warning icon ⚠, are not imported to avoid duplicates. From this page, you can select all device classes that were found on endpoints or you can select individual device classes. Click **Proceed** to add the selected device classes to the allow list.

   - Click **Manage Existing** to add existing device classes to the allow list. This list contains the predefined device classes that are provided by Microsoft and any device classes that were manually added previously. From this page, you can add or remove all available device classes, or add or remove individual device classes.

©2026 Tanium Inc. All Rights Reserved

Note: If you added a device class using the **Create** option, it does not appear in this list until you save the policy.

- Click **Create** to add a new device class. Specify a **Device Class Name**, valid **GUID**, and optional **Description**. Click **Create** to add the device class to the allow list.



3. On the **Devices** tab, define individual devices that you want to allow in your environment. This option is useful if, for example, you want to allow a USB storage device from a specific manufacturer that is supported by your company, but no other USB storage devices. You do not need to allow the associated device classes when you allow a specific device. When you add a device, it is stored in the global device list, which you can access from the Enforce settings page. For more information on the global list, see Manage Windows device classes and devices on page 89.

   - Click **Import** to query all Windows endpoints for their installed USB storage devices and import them to the allow list. With this option, you can quickly add any USB storage devices that might be used in your environment. USB storage devices that are already known to Enforce, marked with a warning icon ⚠, are not imported to

©2026 Tanium Inc. All Rights Reserved

avoid duplicates. From this page, you can select all USB storage devices that were found on endpoints or you can select individual USB storage devices. Click **Proceed** to add the selected USB storage devices to the allow list.

- Click **Manage Existing** to add existing devices to the allow list. This list contains devices that were manually added previously. From this page, you can add or remove all available devices, or add or remove individual devices.
- Click **Create** to add a new device. Specify a device name and an optional ID. Click **Create** again to add the device to the allow list.

> **Note:** Most devices have several hardware IDs. These IDs range from the most specific, which identifies a particular device, to a more general ID, which might identify a device type. Use the hardware ID that is appropriate for your environment.

4. (Optional) On the **Notification** tab, select **Provide a notification message for users when a device is denied access** and specify a message to display when a user attempts to install a restricted device.

Creating policies for Windows endpoints on page 96

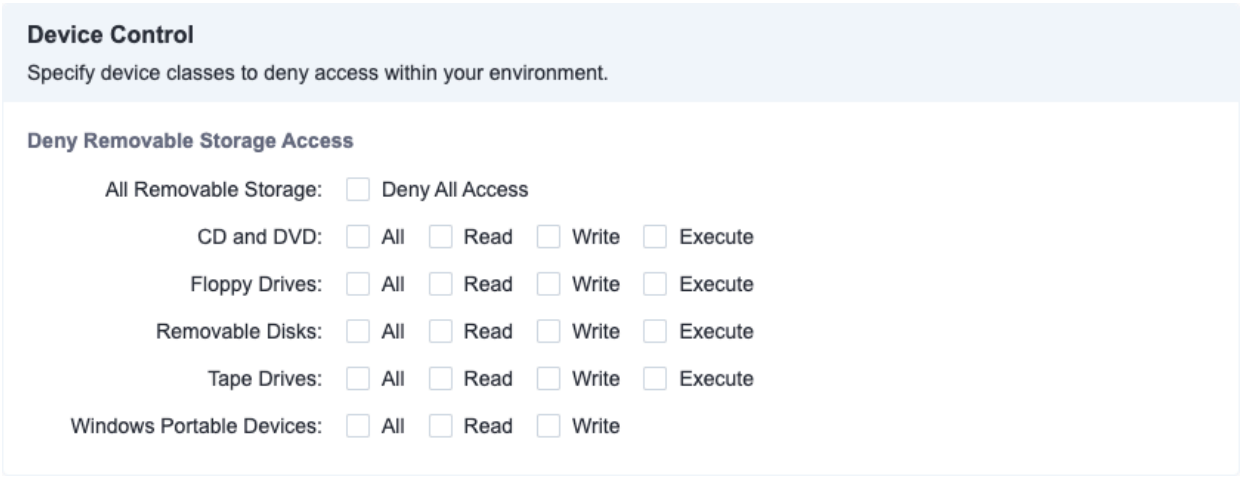
Device Control - Removable Storage

Windows device control policies provide two modes for administering devices on Windows endpoints: removable storage or all devices. The **Device Control - Removable Storage** policy type controls access permissions on removable media. The types of removable media predefined by Microsoft are CD-ROM and DVD drives, floppy disk drives, removable disk drives, tape drives, and Windows Portable Devices (WPD). With this mode, you can deny specific permissions to categories of removable devices. On the endpoint, the permissions are managed using local group policy settings located in **Administrative Templates** > **System** > **Removable Storage Access**.

> **Note:** Complete the steps in the Manage Windows device classes and devices on page 89 section before configuring device control policies.

1. In the **Device Control** section, select the type of removable storage that you want to administer and the access that you want to deny for that storage type.

©2026 Tanium Inc. All Rights Reserved



Creating policies for Windows endpoints on page 96

Windows firewall management

When a Windows firewall management policy is enforced on an endpoint, Enforce starts the MpsSvc (Windows Firewall) service on that endpoint.

Note: Settings in Windows firewall policies are not applied on endpoints where there are existing firewall settings managed by a GPO linked to a domain. In this scenario, the enforcement status is `Not Applied` with the reason `GPO firewall rules found on endpoint`.

1. In the **Firewall Profiles** section, configure the policy profiles for **Domain**, **Private**, and **Public**. For more information about profiles, see Microsoft Documentation: Firewall profiles.
2. For **Network Selection**, choose **Default**, **Enabled**, or **Disabled**
3. In the **Rule Management** section, choose **Replace** or **Merge**.

   The **Replace** option removes all existing firewall rules on the endpoint and replaces them with the rules in this policy. The **Merge** option leaves the existing firewall policies on the endpoint in place and adds the rules in this policy using a new rule with the name of the existing rule preceded with **Tanium Enforce**.
4. (Optional) Create firewall rules:

   Manually create a firewall rule

©2026 Tanium Inc. All Rights Reserved

a. In the **Firewall Rules** section, click **Add Rule**.

b. Complete the following fields for the rule and then click **Create**:

Fields in the Windows Firewall Management policy form

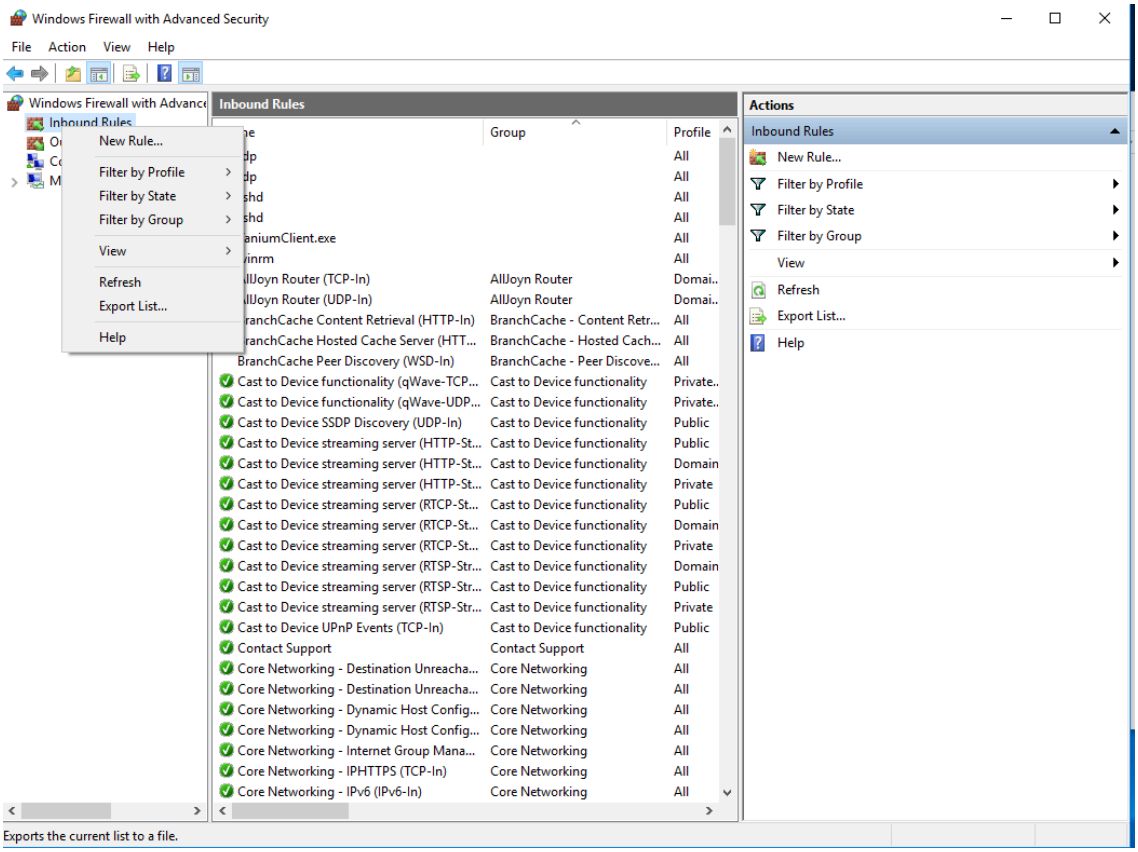
Field	Description
Name	Enter a brief name for the rule.
Direction	Select **Outbound**, **Inbound**, or **Bi-directional** for the direction of the connection.
Action	Select either **Block** or **Allow** as the action to perform for the rule.
Network Protocol	Select a protocol. If you specify **UDP** or **TCP** for the protocol, then you must specify at least one value in the following fields: **Application Path**, **Local Addresses**, **Local Ports**, **Remote Addresses**, **Remote Ports**, or **Service Name**. For more information about protocols, see Microsoft Documentation: Firewall Rule Properties Page: Protocols and Ports Tab.
Group	(Optional) You can specify a group name here or choose one that already exists that can help organize your firewall rules.
Profiles	Select the applicable profiles. If you do not select one or more profiles, the rule is created as if all profiles were selected.
Application Path	(Optional) An example of an application path is C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.
Local Addresses	(Optional) Use this field to target the rule to specific local IP addresses. Separate IP addresses with commas.
Remote Addresses	(Optional) This field can be used to target the rule to a specific remote IP address. Separate IP addresses with commas.
Service Name	(Optional) This field can be used for a Windows Service Display name.

Import firewall rules from a Windows TSV file

a. In Windows, go to **Windows Firewall Advanced Security**.

©2026 Tanium Inc. All Rights Reserved

b. Right-click on **Inbound Rules** and click **Export List...**, and then save the file as a **Text (Tab Delimited) .txt** file.



c. In the **Firewall Rules** section, click **Import** > **Import from Windows TSV file**.

d. Click **Select TSV File** to locate the files that contains the exported firewall rules and click **Open**. The **Import** window shows the file name and how many rules are being imported.

e. Select the **Direction** and then click **Proceed**.

f. Repeat these steps for **Outbound Rules** to export them from Windows and import them into Enforce.

   If the file you are importing does not include a Service column, a warning occurs. If your firewall rules depend on the Service field, add the Service column and re-export the firewall rules from Windows.

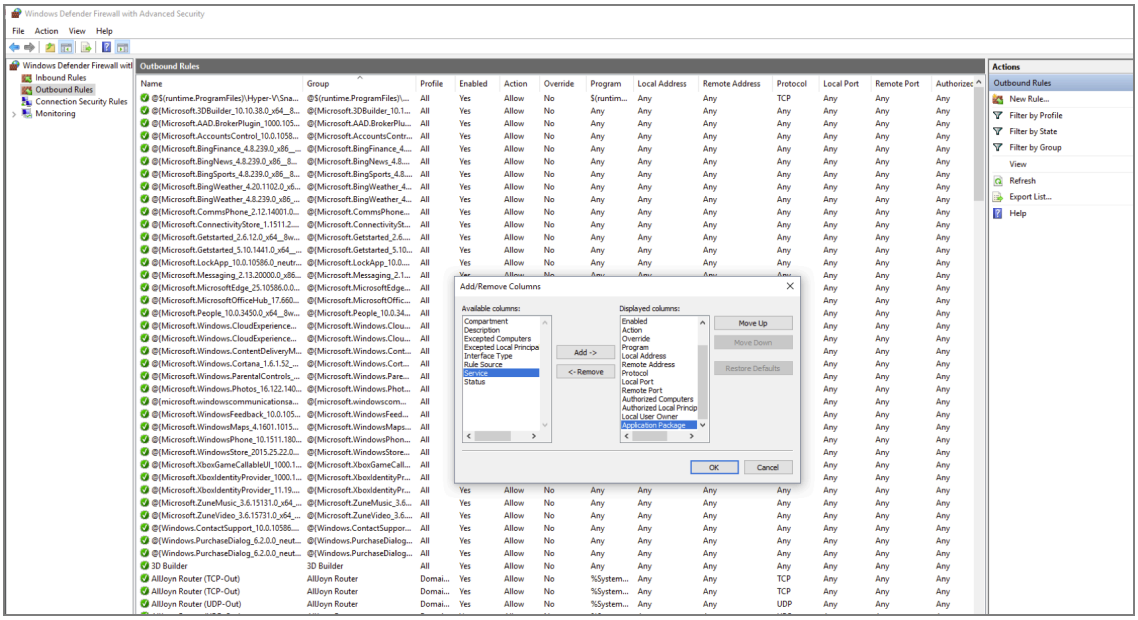
Add a Service column

a. On a Windows endpoint, go to **Windows Firewall with Advanced Security**.

©2026 Tanium Inc. All Rights Reserved

b. Click **View** > **Add/Remove Columns**.

c. Select **Service** from **Available columns**, click **Add** and then click **OK**.



d. Right-click on **Inbound Rules** or Outbound Rules, click **Export List...** and then save the file as a **Text (Tab Delimited) .txt** file.

Import firewall rules from Tanium Client managed endpoints

> **Note:** Before you can import firewall rules into Enforce from a Windows TSV file, you must export them from Windows.

a. In the **Firewall Rules** section, click **Import** > **Import Rules from Tanium Endpoints**.

b. In the **Import Rules from Tanium Endpoints** window, select a **Computer Group** or **Computer Name** and select the existing rules on Tanium Client managed endpoints that you want to import.

c. Click **Import Rules**.

Creating policies for Windows endpoints on page 96

Machine administrative template

©2026 Tanium Inc. All Rights Reserved

Settings that can be applied using a configuration service provider (CSP) are annotated with this icon . Hover over the icon to see the earliest supported operating system for policy application using a CSP. For more information about Enforce policy application using a CSP, see Configuration service providers (CSPs) on page 163.

Note: Windows 11 ADMX policies are used in Enforce 2.1.273 and later. Microsoft deprecated some settings in Windows 11 ADMX policies that were previously available in Windows 10 ADMX policies, such as **Scan Packed Executables**. Enforce includes this deprecated policy setting in the machine administrative template policy settings for backwards compatibility. However, if you apply the policy to a Windows 11 endpoint where this setting is not supported, the overall policy might return a **Partially Applied** status for the endpoint.

Important: Due to the way that Microsoft stores and retrieves exclusions, do not use Enforce to manage anti-malware exclusion settings if you are using Microsoft Defender for Endpoint.

1. (Optional) Configure anti-malware settings:

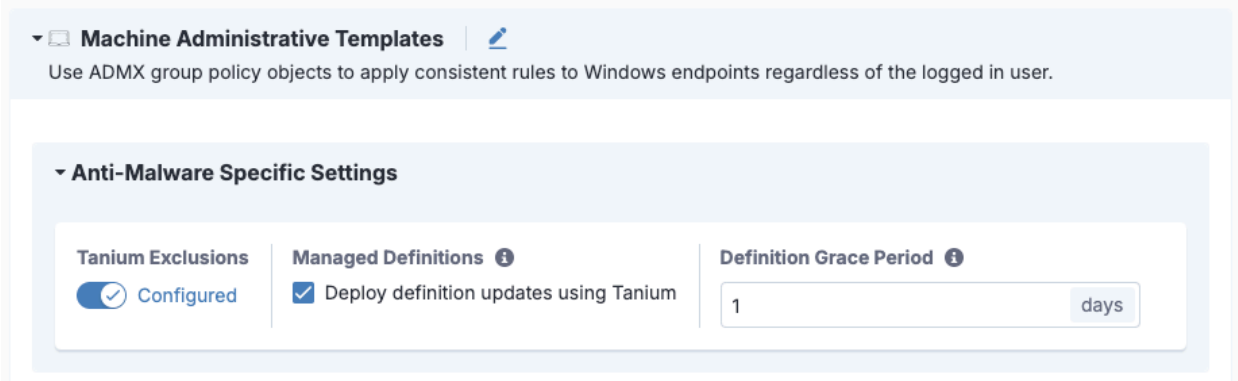
    a. Expand the **Anti-Malware Specific Settings** section.

    b. To automatically add the required Tanium exclusions to the policy, select **Configured** for the **Tanium Exclusions** toggle.

    c. If needed, select **Deploy definition update using Tanium** for **Managed Definitions** and then complete the fields for **Definition Grace Period** to specify how often endpoints use Tanium to check for anti-malware definition updates. This value represents how old an anti-malware definition can be before the policy is considered unenforced. The default grace period is 1 day.

    Note: By default, anti-malware rules are configured to retrieve definitions directly from Microsoft. If an endpoint does not receive an update within the specified grace period, it is considered unenforced. When this option is selected, anti-malware rules are configured to use Tanium to deploy anti-malware definition updates.

©2026 Tanium Inc. All Rights Reserved

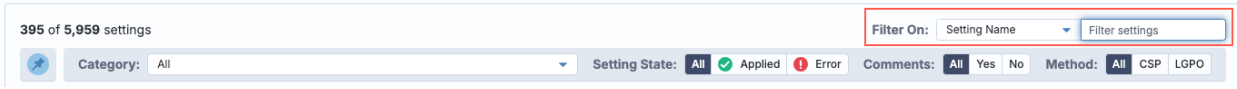


2. (Optional) To apply policy settings using both CSP and LGPO, select **Apply each setting simulaneously using CSP and LGPO**.

> **Note:** Some compliance reports check only one application method to determine whether a CIS benchmark is set properly. Select this option to apply settings using both methods to improve reporting results for compliance tools.

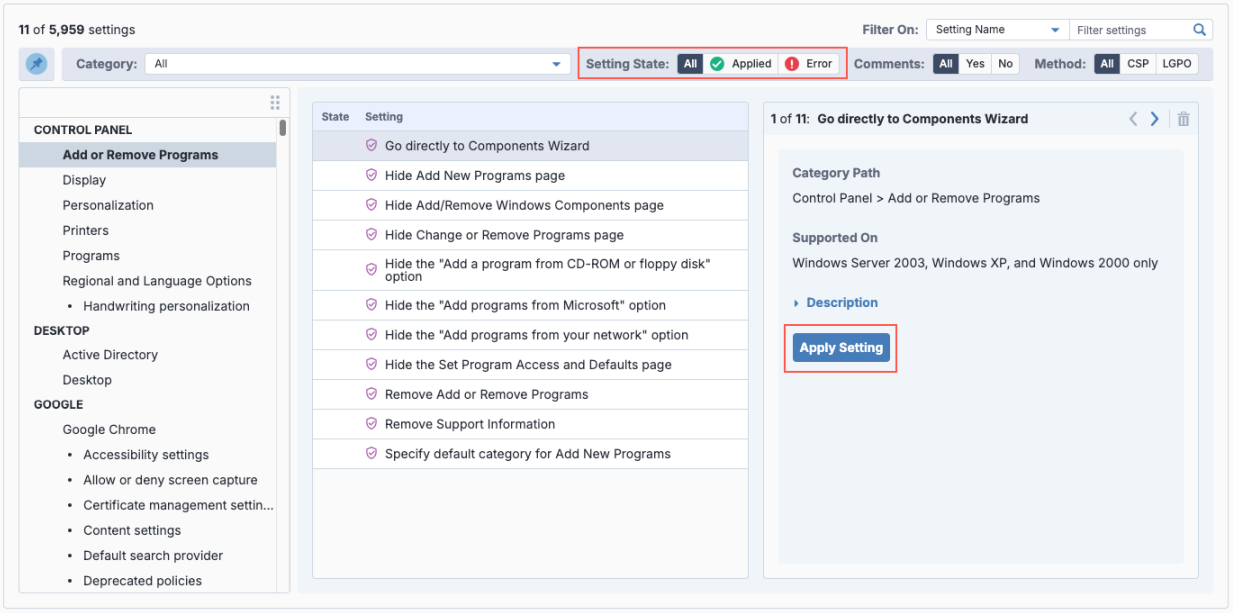
3. From the list of policy setting categories, select a category and view the available policy settings.

   Use the filter field to filter the available settings by the setting name or the setting metadata.

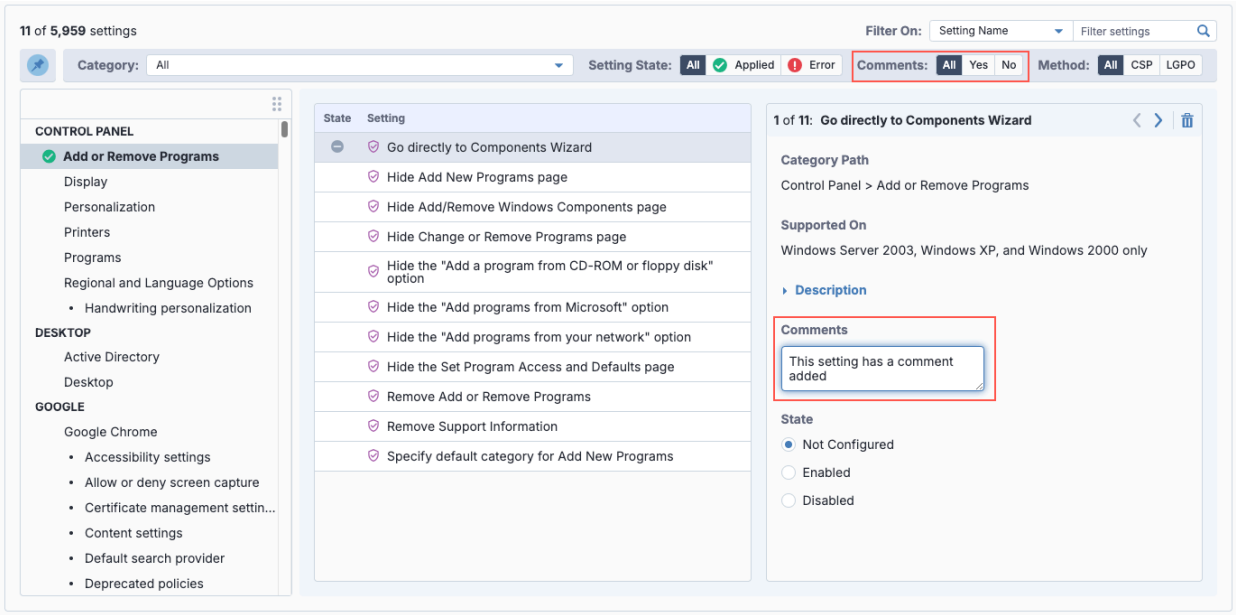


   Use the **Category** dropdown list to show only the settings for the selected category. You can further filter the settings by using the **Setting** options to show only settings that are Applied or contain an Error.

©2026 Tanium Inc. All Rights Reserved

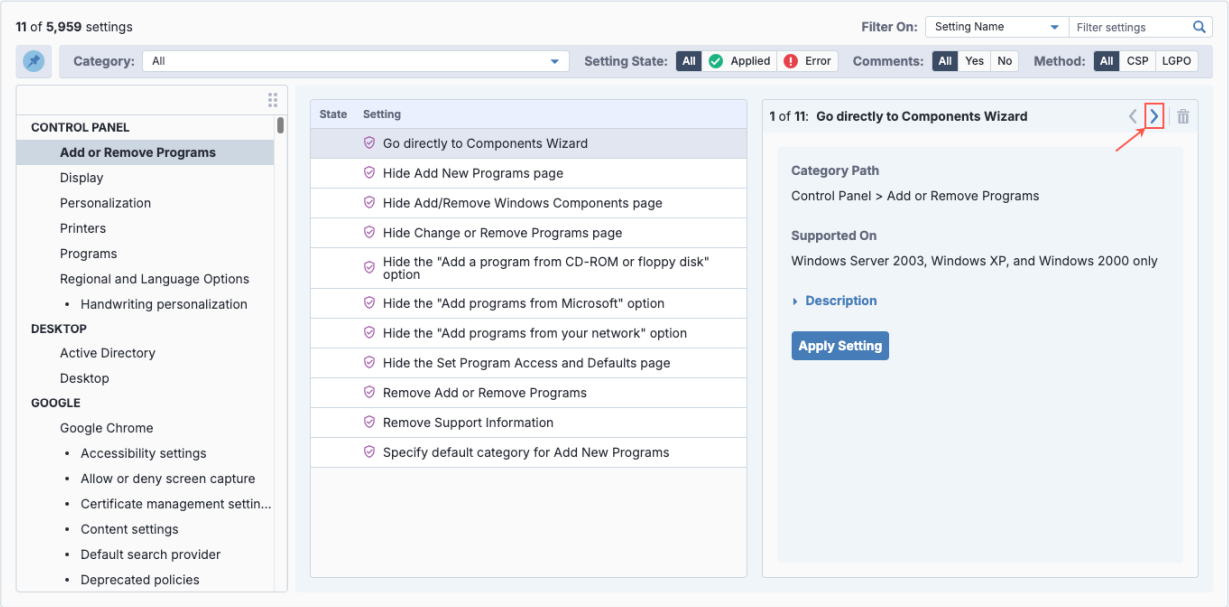


You can also filter the settings by the method of application: configuration service providers (**CSP**) or Local Group Policy Object (**LGPO**). For more information about these application methods, see Applying policy settings on endpoints on page 163. Use the **Comments** filter to filter settings based on whether a comment was added.



The available settings, based on any filters that you applied, appear when you select a category. Click Next Setting › to proceed to the next setting.

©2026 Tanium Inc. All Rights Reserved



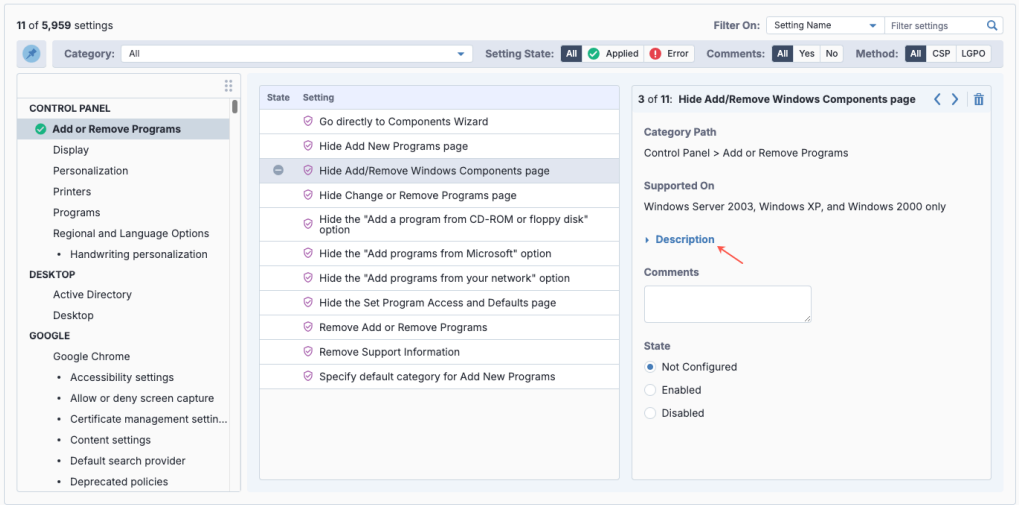
Tip:

Click Pin Categories to pin the list of available settings for a category.

a. To apply a setting to the policy, click **Apply Setting**.

b. Configure the parameters for the setting.

- Expand the **Description** for a brief explanation of the setting.



For more information about high-level Machine administrative template policy categories, see Policy setting category examples on page 123.

©2026 Tanium Inc. All Rights Reserved

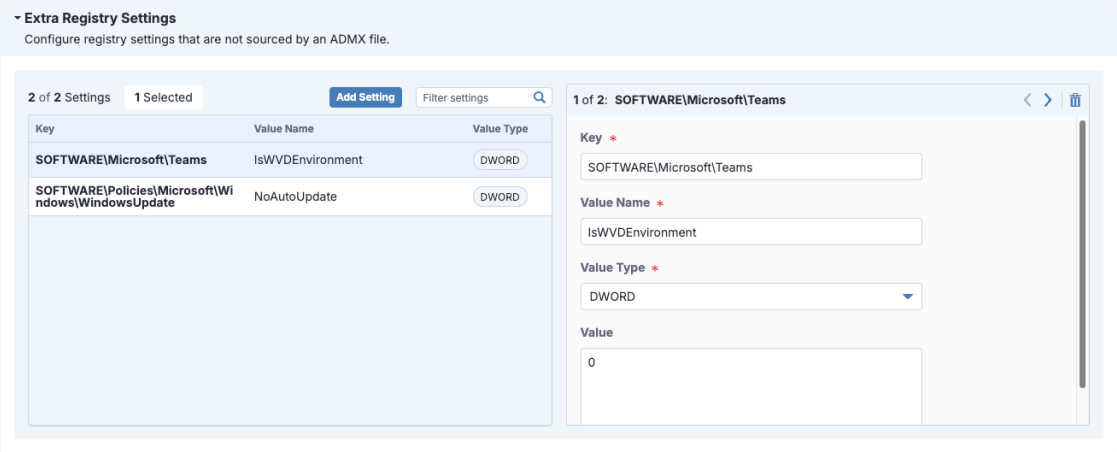
Note:

- For more information about the policy settings included in Windows administrative template files, see Microsoft Documentation: Group Policy Settings Reference for Windows and Windows Server and Microsoft Security Compliance Toolkit 1.0.
- The **Set a default associations configuration file** setting in the **Windows Components** category provides two options:
  - **Default Associations Configuration File**: Use this option for endpoints where the policy is applied using group policy object (GPO). Specify the path to an associations configuration XML file on the endpoint or a network drive.
  - **Default Associations Configuration File (CSP)**: Use this option for endpoints that support policy application using a configuration service provider (CSP). Copy and paste the contents of the associations configuration XML file into the field. When the policy is enforced on an endpoint, the contents of this field is encoded into base64 and sent to the endpoint to apply the settings.

4. When you apply a policy setting, select one of the following states:
   - **Not Configured:** The setting might be determined by another group policy setting. Otherwise, default Microsoft settings are used.
   - **Enabled** Enable the setting using the specified parameters, if applicable.
   - **Disabled** Default Microsoft settings are used.
5. (Optional) To remove a configured setting, click Remove Setting .
6. (Optional) To configure registry settings that are not sourced by an ADMX file, expand the **Extra Registry Settings** section.
   a. Click **Add Setting**.
   b. Specify the **Key**, **Value Name**, **Value Type**, and optional **Value**.

©2026 Tanium Inc. All Rights Reserved

For more information, see Microsoft Documentation: Structure of the Registry and Microsoft Documentation: Registry value types.



Note: Do not include `HKLM` or `HKEY_LOCAL_MACHINE` in the **Key** path; otherwise the policy fails to enforce.

c. Click **Add Setting** to add additional registry settings.

Policy setting category examples

You can configure Machine administrative template policies with a variety of policy settings. Policy settings are organized into the same categories used by Microsoft to manage group policies. The following table includes many of the high-level categories and the types of policy settings that each category contains.

Machine Administrative Template Policy Category Examples

Category (top level)	Policy Setting Overview
Control Panel	Includes display, personalization, regional and language options, and printers.
Google Chrome	Includes cookies, Javascript, and image settings.
MS Security Guide	Includes UAC restrictions and SMB server and client.
MSS (Legacy)	Includes legacy Windows registry values that predate group policy.

©2026 Tanium Inc. All Rights Reserved

Category (top level)	Policy Setting Overview
Microsoft Edge	Includes download restrictions and autofill.
Microsoft Office	Includes Window security restrictions and storage of user passwords.
Mozilla	Includes authentication, certificates, cookies, location, notifications, extensions, bookmarks, and other preferences.
Network	Includes network connections.
OneDrive	Includes OneDrive sync app, accounts, permissions, bandwidth management, and disk space options.
Printers	Includes prevention of security issues with print driver installation.
Start Menu and Taskbar	Includes notifications.
System	Includes driver installation, display, locale services, group policy, mitigation options, logon, power management, removable storage access, and user profiles.
Windows Components	Includes app runtime, attachment manager, autoplay policies, cloud content, credential user interface, edge UI, and Windows Defender antivirus.

Creating policies for Windows endpoints on page 96

SRP Management

Note:

- SRP policy types cannot be combined with other policy types.
- When you enable Windows SRP for the first time, targeted endpoints must be rebooted for SRP Management policies to be enforced.

©2026 Tanium Inc. All Rights Reserved

Best Practice: Enforce an SRP Management policy that does not block anything or allows a path that is always trusted, such as the Tanium Client. With this practice, the required reboot does not have to take place when you need to push out an urgent policy, such as a policy to block a malicious application.

1. Click **Add Rule**.
2. Enter a **Name** for the rule.
3. Select the rule **Type**: **Hash** or **Path**.
4. For hash rules, Enter the **MD5 Hash File Size** in bytes
5. For path rules, enter the path or filename in the **Path** field. Full paths, environment variables, and filenames are supported.
6. Click **Add Rule** to add additional rules as necessary.

Note: Be aware of AppLocker Allow or Deny rules set in your Domain Policy – these rules might prevent SRP process rules created in Enforce from being enforced.

Creating policies for Windows endpoints on page 96

Security Settings

Settings that can be applied using a configuration service provider (CSP) are annotated with this icon . Hover over the icon to see the earliest supported operating system for policy application using a CSP. For more information about Enforce policy application using a CSP, see Configuration service providers (CSPs) on page 163.

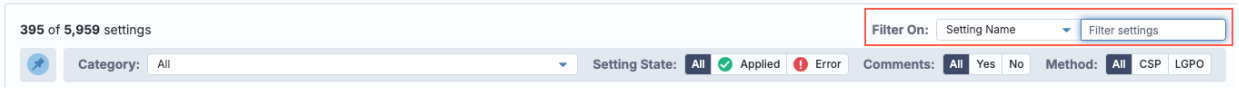
1. (Optional) To apply policy settings using both CSP and LGPO, select **Apply each setting simultaneously using CSP and LGPO**.

   Note: Some compliance reports check only one application method to determine whether a CIS benchmark is set properly. Select this option to apply settings using both methods to improve reporting results for compliance tools.

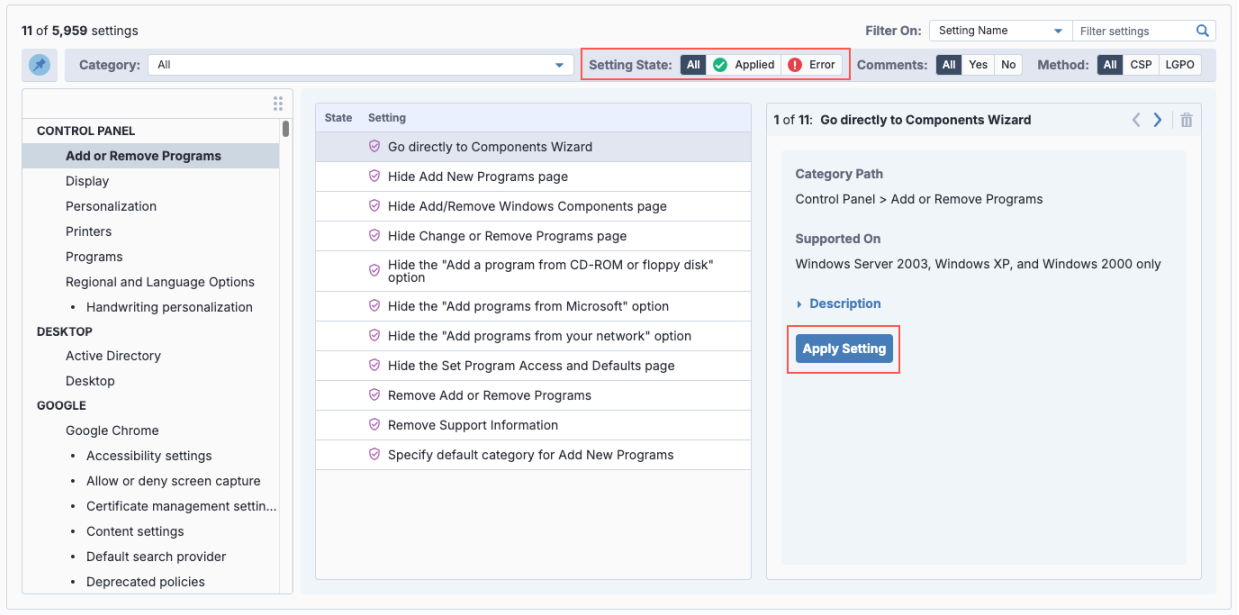
©2026 Tanium Inc. All Rights Reserved

2. From the list of policy setting categories, select a category and view the available policy settings.

   Use the filter field to filter the available settings by the setting name or the setting metadata.

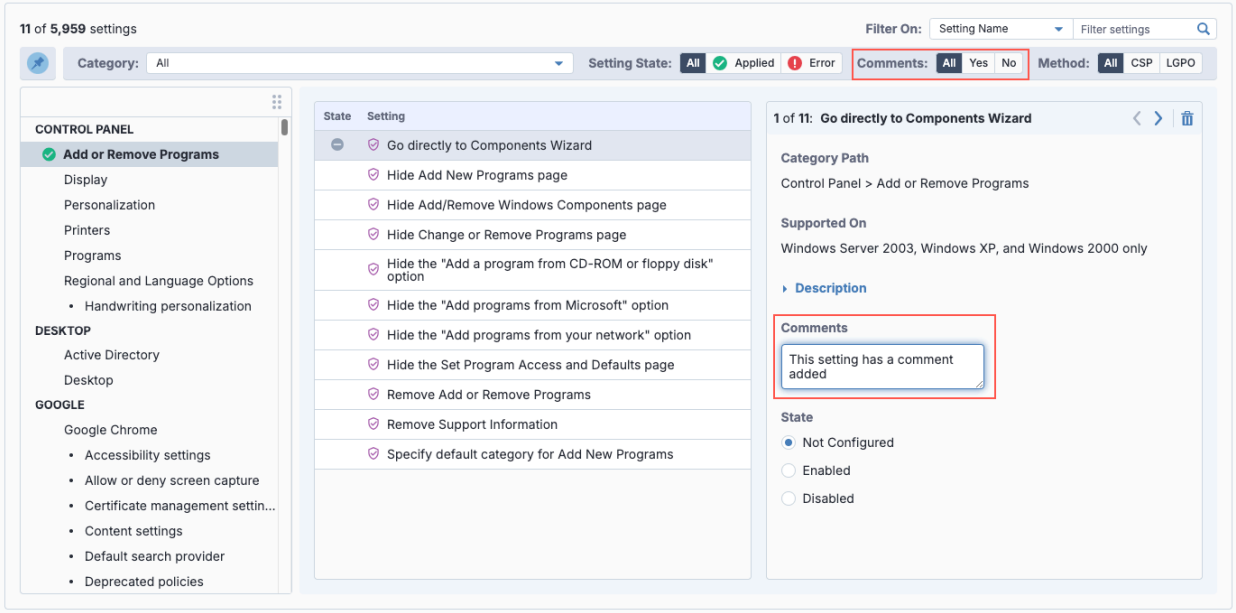


   Use the **Category** dropdown list to show only the settings for the selected category. You can further filter the settings by using the **Setting** options to show only settings that are Applied or contain an Error.

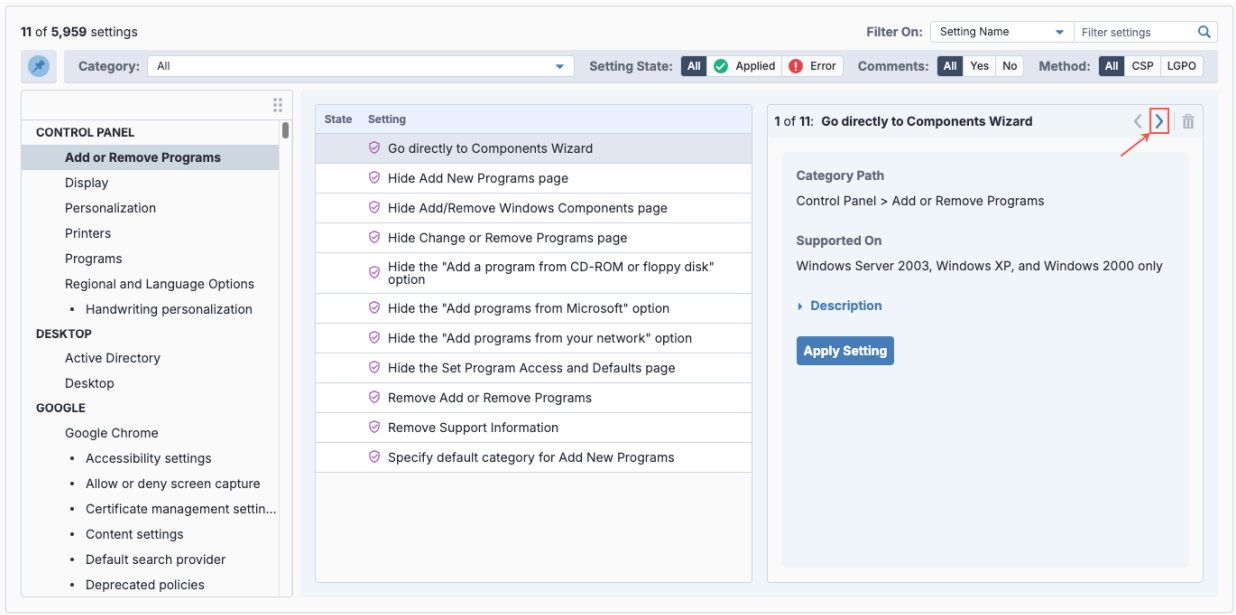


   You can also filter the settings by the method of application: configuration service providers (**CSP**) or Local Group Policy Object (**LGPO**). For more information about these application methods, see Applying policy settings on endpoints on page 163. Use the **Comments** filter to filter settings based on whether a comment was added.

©2026 Tanium Inc. All Rights Reserved



The available settings, based on any filters that you applied, appear when you select a category. Click Next Setting ❯ to proceed to the next setting.



Tip:

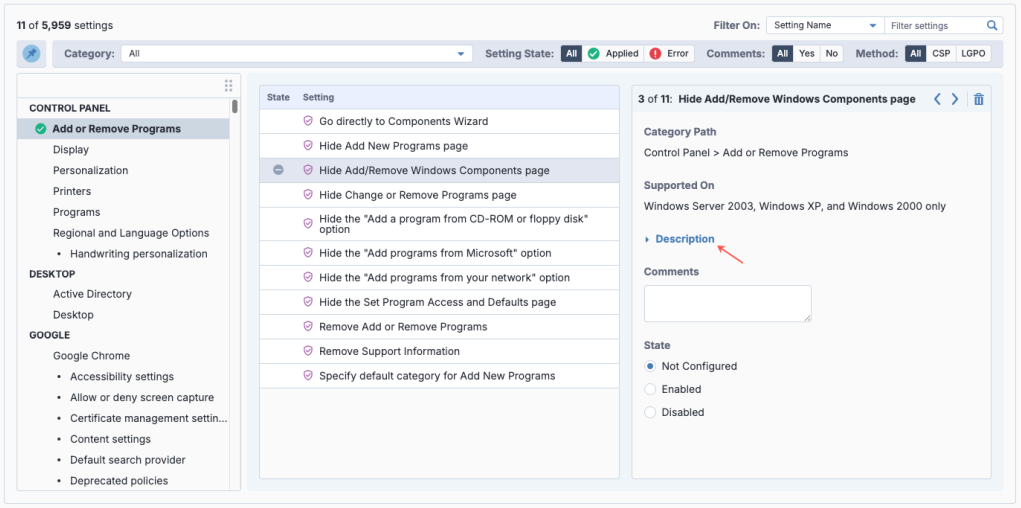
Click Pin Categories 📌 to pin the list of available settings for a category.

a. To apply a setting to the policy, click **Apply Setting**.

©2026 Tanium Inc. All Rights Reserved

b. Configure the parameters for the setting.

- Expand the **Description** for a brief explanation of the setting.



Note: For more information about the policy settings included in Security Settings policies, see Microsoft Documentation: Security policy settings reference, Microsoft Documentation: Group Policy Settings Reference for Windows and Windows Server (Security tab) and Microsoft Security Compliance Toolkit 1.0.

3. To configure settings for services, expand the **Service Settings** section.

Tip: You can use these settings to disable system services to comply with Center for Internet Security (CIS) benchmarks. For example, if the benchmark states `Ensure Windows Mobile Hotspot Service (icssvc)' is set to 'Disabled'`, you can use this section to disable to icssvc service on endpoints. Consult the Microsoft documentation for details about disabling system services. For example, for Windows Server 2016, see Microsoft documentation: Guidance on disabling system services on Windows Server 2016 with Desktop Experience.

a. Click **Add Setting**.

b. Specify the **Service Name**.

c. Specify the **Start Type**.

d. To add more settings, click **Add Setting**.

©2026 Tanium Inc. All Rights Reserved

Note: When you remove an enforcement for a Security Settings policy, the settings from the policy remain on the endpoint. When this scenario occurs, the following warning-level message (0) is logged in the endpoint's extensions log: `Unenforced Security Policy - settings remain on endpoint`.

For more information about this behavior, see the section "Persistence in security settings" in Microsoft documentation: Applying security settings.

Creating policies for Windows endpoints on page 96

Tanium Removable Storage Access Control

By default, Tanium Removable Storage Access Settings policies block access to USB devices on endpoints where the policy is enforced. In the policy configuration, you can create exception rules to allow access to devices that meet specific criteria. Each exception rule has an associated name, which is logged when an action occurs due to that rule. If you want to send events generated from Tanium Removable Storage Access Control policies to external Splunk destinations using an HTTP Event Collector (HEC) or TCP connection, create a Stream profile. For more information, see Manage Stream profiles on page 91.

Note:

If you enforce more than one Tanium Removable Storage Access Settings policy on an endpoint, the most permissible rules take precedence over the least permissible rules; **Read/Write** exception rules override **Read** and **Block** rules, and **Read** exception rules override **Block** rules.

For example, you can create a Tanium Removable Storage Access Settings policy to block all access to USB devices and enforce it on all endpoints in your environment. If you want to allow read/write permissions for USB devices with Vendor ID 456 on only a subset of those endpoints, create a second Tanium Removable Storage Access Settings policy with a **Read/Write** exception rule for USB devices with Vendor ID 456 and enforce it on only the subset of endpoints.

1. Click **Add Rule**.
2. Specify a **Name** to associate with the actions for this rule when logging events.

©2026 Tanium Inc. All Rights Reserved

3. Select the **Access** for the rule:
    - To allow read access to specific devices, select **Read**.
    - To allow read and write access to specific devices, select **Read/Write**.
4. Specify a name to associate with the actions for this rule when logging events.
5. Select an attribute, operator and value for the rule.

    Acceptable wildcard characters for values are `*` (many characters) and `?` (one character).
6. Click Apply ✓.
7. (Optional) To group additional conditions using AND or OR operators, click Add Row + in the section for the rule.

Creating policies for Windows endpoints on page 96

User Administrative Template

Settings that can be applied using a configuration service provider (CSP) are annotated with this icon. Hover over the icon to see the earliest supported operating system for policy application using a CSP. For more information about Enforce policy application using a CSP, see Configuration service providers (CSPs) on page 163.

> **Note:** Some policy settings are not supported for application on Windows 11 endpoints. For more information, see Microsoft Documentation: Supported configuration service provider (CSP) policies for Windows 11 taskbar.

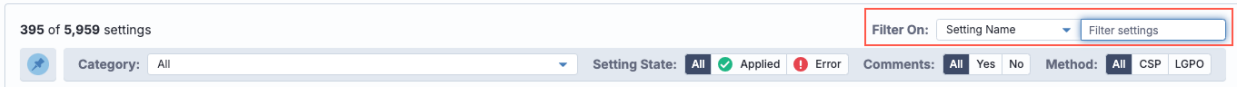
1. (Optional) To apply policy settings using both CSP and LGPO, select **Apply each setting simulaneously using CSP and LGPO**.

    > **Note:** Some compliance reports check only one application method to determine whether a CIS benchmark is set properly. Select this option to apply settings using both methods to improve reporting results for compliance tools.

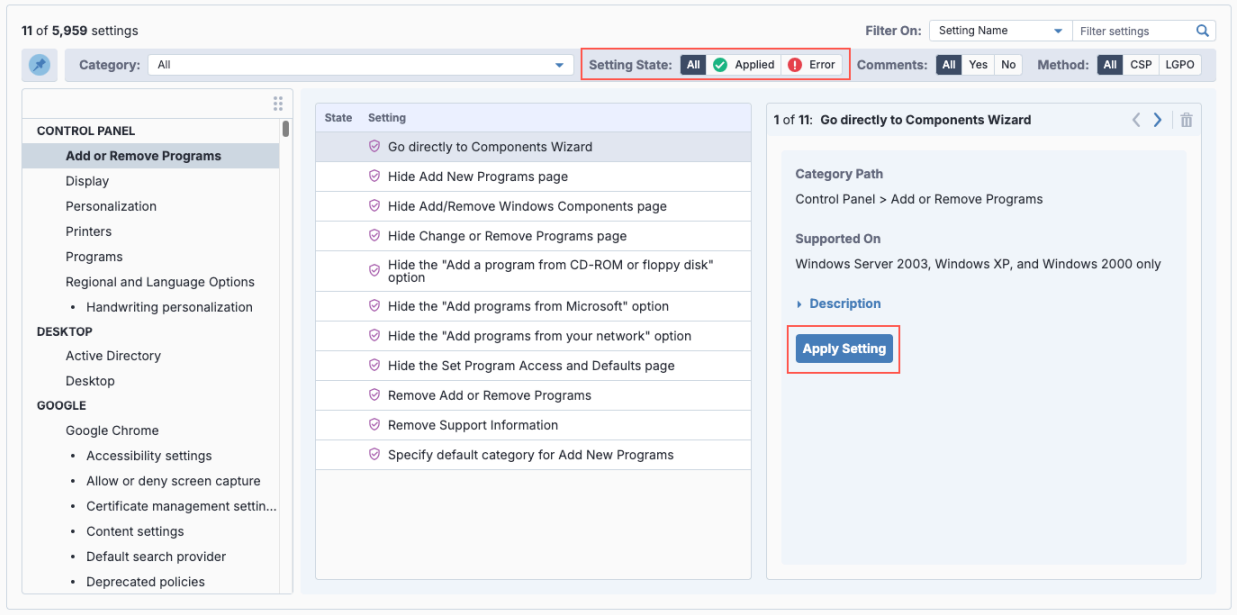
©2026 Tanium Inc. All Rights Reserved

2. From the list of policy setting categories, select a category and view the available policy settings.

   Use the filter field to filter the available settings by the setting name or the setting metadata.

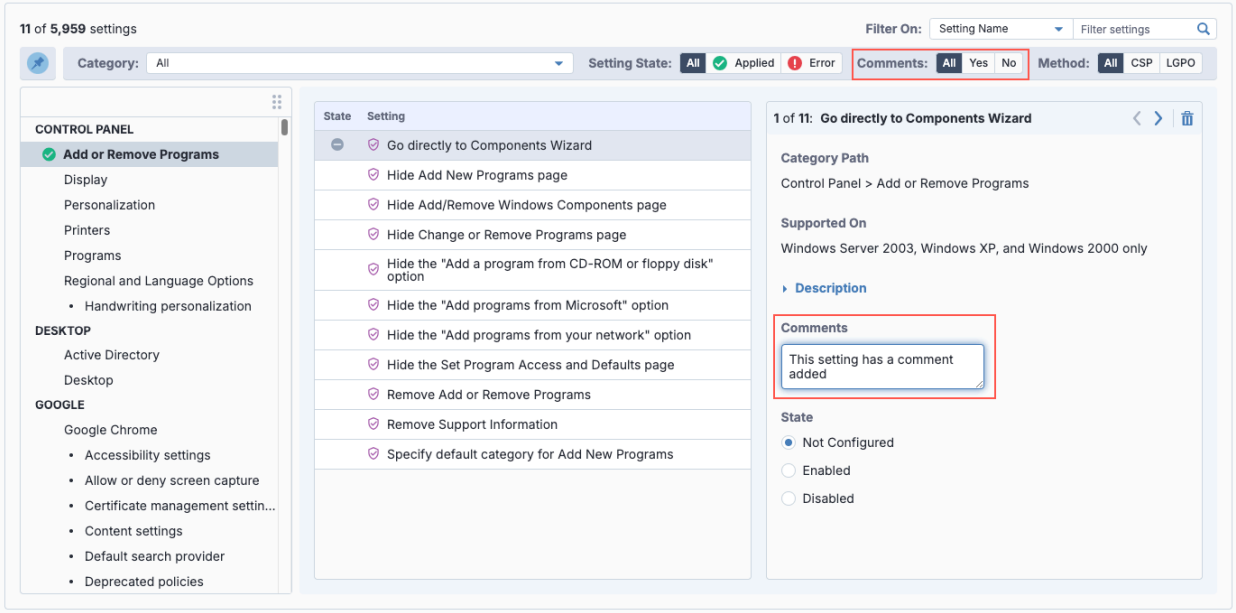


   Use the **Category** dropdown list to show only the settings for the selected category. You can further filter the settings by using the **Setting** options to show only settings that are Applied or contain an Error.

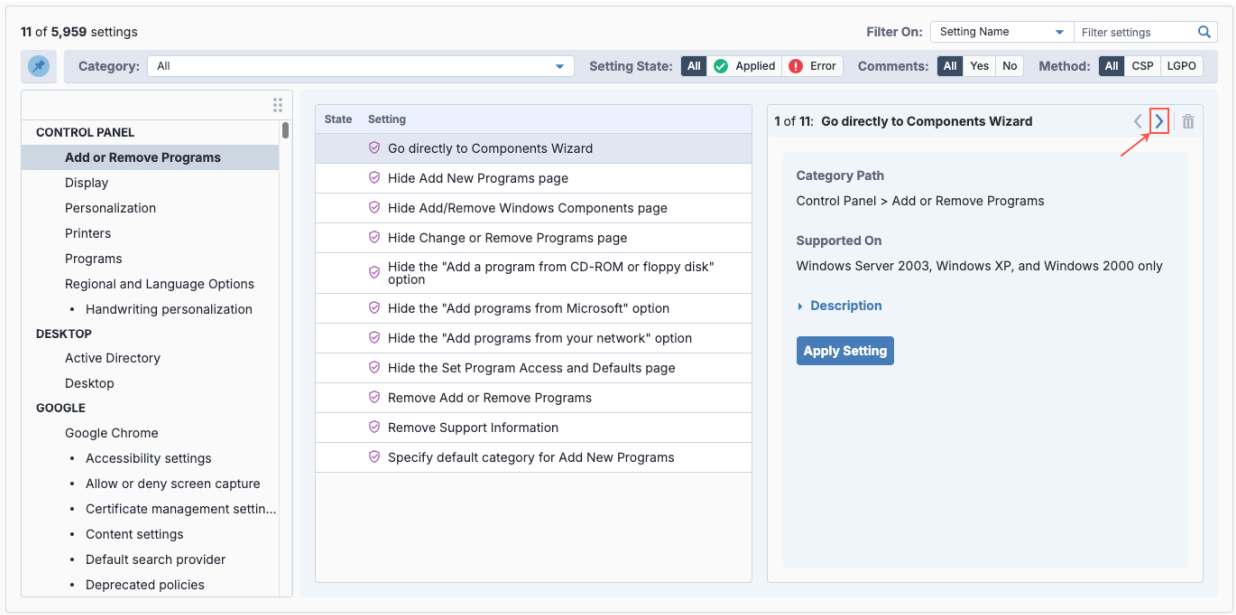


   You can also filter the settings by the method of application: configuration service providers (**CSP**) or Local Group Policy Object (**LGPO**). For more information about these application methods, see Applying policy settings on endpoints on page 163. Use the **Comments** filter to filter settings based on whether a comment was added.

©2026 Tanium Inc. All Rights Reserved



The available settings, based on any filters that you applied, appear when you select a category. Click Next Setting ❯ to proceed to the next setting.



Tip:

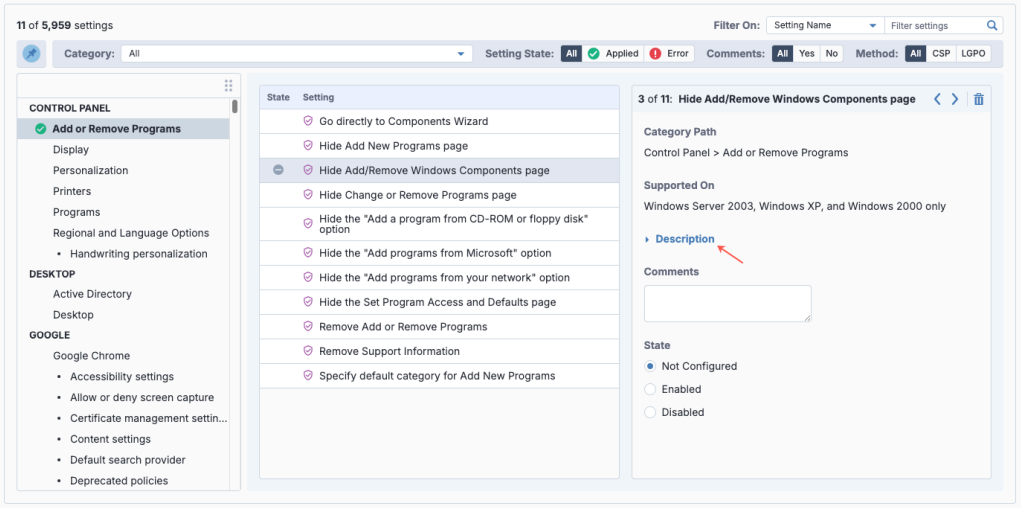
Click Pin Categories 📌 to pin the list of available settings for a category.

a. To apply a setting to the policy, click **Apply Setting**.

©2026 Tanium Inc. All Rights Reserved

b. Configure the parameters for the setting.

- Expand the **Description** for a brief explanation of the setting.



3. When you apply a policy setting, select one of the following states:

   - **Not Configured:** The setting might be determined by another group policy setting. Otherwise, default Microsoft settings are used.
   - **Enabled** Enable the setting using the specified parameters, if applicable.
   - **Disabled** Default Microsoft settings are used.

   For more information, see Microsoft Documentation: Use the Settings app Group Policy in Windows 10.

   For more information about user administrative template policy categories, see Policy setting category examples on page 134.

   > **Note:** For more information about the policy settings included in Windows administrative template files, see Microsoft Documentation: Group Policy Settings Reference for Windows and Windows Server and Microsoft Security Compliance Toolkit 1.0.

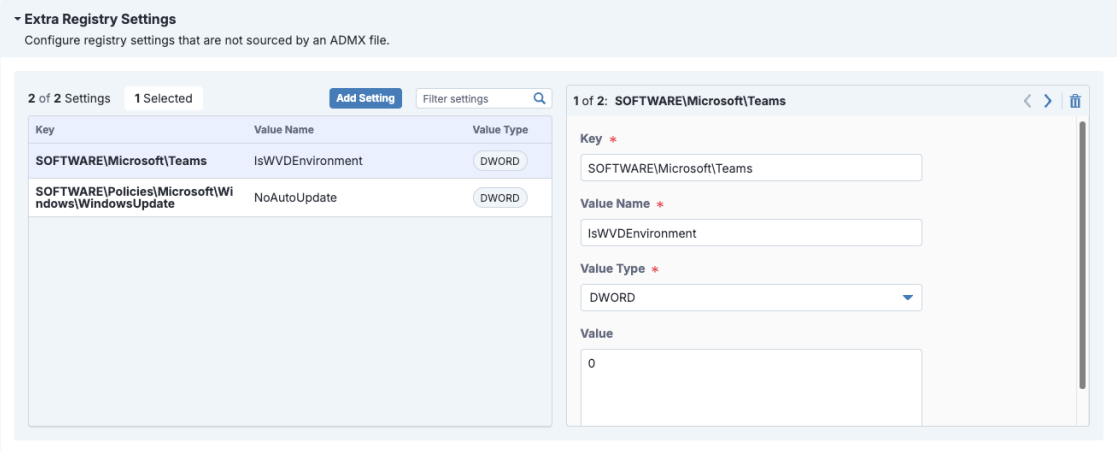
4. (Optional) To configure registry settings that are not sourced by an ADMX file, expand the **Extra Registry Settings** section.

   a. Click **Add Setting**

©2026 Tanium Inc. All Rights Reserved

b. Specify the **Key**, **Value Name**, **Value Type**, and optional **Value**.

For more information, see Microsoft Documentation: Structure of the Registry and Microsoft Documentation: Registry value types.



Note: Do not include `HKCU` or `HKEY_CURRENT_USER` in the **Key** path; otherwise the policy fails to enforce.

c. Click **Add Setting** to add additional registry settings.

Policy setting category examples

You can configure user administrative template policies with a variety of policy settings. Policy settings are organized into the same categories used by Microsoft to manage group policies. The following table includes many of the high-level categories and the types of policy settings that each category contains.

User Administrative Template Policy Category Examples

Category (top level)	Policy Setting Overview
Control Panel	Includes add or remove programs, display, personalization, printers, programs, and regional and language options.
Desktop	Includes active directory and desktop settings.

©2026 Tanium Inc. All Rights Reserved

Category (top level)	Policy Setting Overview
Google	Includes Google Chrome and password alert settings.
Microsoft Edge	Includes Microsoft Edge and WebView2 settings.
Microsoft Office	Includes settings for Microsoft Access 2016, Microsoft Excel 2016, Microsoft Office 2016, Microsoft OneNote 2016, Microsoft Outlook 2016, Microsoft PowerPoint 2016, Microsoft Project 2016, Microsoft Publisher 2016, Microsoft Teams, Microsoft Visio 2016, Microsoft Word 2016, and Skype for Business 2016.
Mozilla	Includes settings for Mozilla Firefox.
Network	Includes network connections, offline files, and Windows Connect Now.
OneDrive	Includes OneDrive settings.
Shared Folders	Includes settings for Allow DFS roots to be published and Allow shared folders to be published.
Start Menu and Taskbar	Includes notifications.
System	Includes ctrl+alt+del options, display settings, driver installation, folder redirection, group policy, internet communication management, locale services, logon, mitigation options, power management, removable storage access, scripts, and user profiles.
Windows Components	Includes add features to Windows 10, app runtime, application compatibility, attachment manager, AutoPlay policies, calculator, cloud content, credential user interface, data collection and preview builds, desktop gadgets, desktop window manager, digital locker, Edge UI, file explorer, file revocation, IME, instant search, Internet Explorer, location and sensors, Microsoft Edge, Microsoft Management Console, Microsoft User Experience Virtualization, multitasking, NetMeeting, network sharing, OOBE, presentation settings, RSS feeds, remote desktop services, search, sound recorder, store, tablet PC, task scheduler, Windows calendar, Windows color system, Windows Defender SmartScreen, Windows error reporting, Windows Hello for Business, Windows installer, Windows logon options, Windows Media Player, Windows Messenger, Windows Mobility Center, Windows PowerShell, Windows Update, and work folders settings.

Creating policies for Windows endpoints on page 96

©2026 Tanium Inc. All Rights Reserved

Creating policies for macOS endpoints

About this task

Create a FileVault policy to manage endpoint encryption settings for macOS endpoints.

Before you begin

Complete the requirements in the Configure endpoint encryption on page 88 section before you create FileVault policies. Optionally, you can configure a self-service recovery portal that users can access if they forget their PIN or password. For more information, see Reference: Encryption key recovery portal on page 241.

If requirements for this policy are missing, that information appears. For more information about FileVault requirements, see Configure endpoint encryption on page 88.

Important: If endpoints already have FileVault enabled without using the Tanium Enforce FileVault policy, you must run the **Enforce - Decrypt FileVault** package on those endpoints first. Then you can deploy the **Enforce FileVault** policy. If you fail to do this, the **Enforce FileVault** policy appears to be successfully enforced, but the recovery key is not backed up. Therefore recovery keys do not work.

For more information about managing encrypted macOS endpoints, including managing recovery keys, see Reference: macOS encryption management on page 234.

1. From the Main menu, go to **Modules** > **Enforce** > **Policy Configurations** > **Create**.
2. Specify a **Name** and optional **Description**.
3. Click **Select Types**.
4. Select **Apple** as the **Platform** for the endpoints that you want to target with the policies.
5. Select the **FileVault** policy type.

   Note: Only Windows policies can include more than one policy type.

©2026 Tanium Inc. All Rights Reserved

6. Click **Confirm**.

7. If you do not want to use the default content set for the policy, select a **Content Set**. Every policy requires a content set. The content set is configured by default to the platform for the selected policy types, provided that you have the necessary permissions for that content set. If no content set is available, you might need additional permissions. For more information, see Tanium Console User Guide: Role permissions for content sets.

8. On the **Recovery Key** tab, select the recovery key type:
   - Select **Institutional Recovery Key** if you are using a private key. For more information about generating institutional recovery keys, see Apple Documentation: How to use institutional recovery keys with Intel-based Macs. After the keychain is generated, remove the private key from the master keychain. Then in the Enforce policy, click **Upload Public Key** to locate the public key and upload it to Tanium Console. This key is sent to endpoints along with the FileVault policy. The public key, in combination with the private key you securely store elsewhere, is used to recover encrypted data if a user forgets their password.
   - Select **Personal Recovery Key** if you are using a unique, machine-generated public key that is accessible to end users. If you are using the recovery portal (Postgres DB), select this key type. For more information about recovery portal configuration details, see Reference: Encryption key recovery portal on page 241.

   Important: For Institutional Recovery Key, you must remove the private key from the master keychain before sending the FileVault policy to endpoints. If you fail to do this, the private key is placed on each endpoint along with the public key.

   After you upload a key, a **Download Public Key** link appears that allows you to retrieve the key to verify it, if necessary. After the disk is encrypted after a reboot, it can take up to an hour for recovery keys to be backed up.

9. On the **Prompt Options** tab, configure additional options as needed:
   a. Select **Prompt** to prompt the user for the enable FileVault password at the next attempt to sign in. If you do not select this option, the user is prompted for the enable FileVault password at the next attempt to sign out.
   b. Select **Cancel** to allow the user to cancel the prompt to enable FileVault. If you select this option, select the **Conditions**:
      - Select **Always allow user to cancel prompt** to give the user unlimited access to the cancel the enable FileVault password prompt.

©2026 Tanium Inc. All Rights Reserved

- Select **Only allow user to cancel prompt** to put a limit on the number of times the user can cancel the prompt before being forced to enter a password to enable FileVault.

10. Configure the settings on the **End User Notification** tab:
    a. Provide a concise **Window Title** for the window prompt, such as FileVault Encryption.
    b. Provide a brief **Message Title** that describes the policy for the user.
    c. Select or drag an image file (PNG, GIF, or JPG/JPEG) to use in the notifications window for all FileVault notifications.
    d. Provide the **Message** that you want to display to users. This message is the first message that appears to the user after the policy is enforced.
11. Click **Create**.

Next steps

Enforce the policy from the **Enforcements** tab of the **Policy Configurations** page. For more information, see Enforcing policies on page 163.

For more information about managing encrypted macOS endpoints, including managing recovery keys, see Reference: macOS encryption management on page 234.

©2026 Tanium Inc. All Rights Reserved

Creating policies for Linux endpoints

About this task

Create Linux firewall management policies to manage firewall settings on Linux endpoints.

1. From the Main menu, go to **Modules** > **Enforce** > **Policy Configurations** > **Create**.
2. Specify a **Name** and optional **Description**.
3. Click **Select Types**.
4. Select **Linux** as the **Platform** for the endpoints that you want to target with the policies.
5. Select **Firewall Management - Linux** as the policy type.

   > **Note:** Only Windows policies can include more than one policy type.

6. Click **Confirm**.
7. If you do not want to use the default content set for the policy, select a **Content Set**.
   Every policy requires a content set. The content set is configured by default to the platform for the selected policy types, provided that you have the necessary permissions for that content set. If no content set is available, you might need additional permissions. For more information, see Tanium Console User Guide: Role permissions for content sets.
8. In the **Default Chain Policies** section, select **Accept** or **Drop** for the **Input**, **Output**, and **Forward** fields.
9. In the **Default Rules** section, view the default input, output, and forward rules. You cannot edit these defaults.
10. (Optional) To create a new Linux firewall rule, click **Add Rule** in the **Firewall Rules** section. Complete the following fields for the firewall rule:

Field	Description
Name	Enter a brief name for the rule.

©2026 Tanium Inc. All Rights Reserved

Field	Description
Table	Filter is the only supported table at this time.
Chain	Select **Input** , **Output** , or **Forward** to specify where in the delivery path of a packet a rule is evaluated.
Target	Select one of the following options: **Accept** : Allows the packet. **Drop** : Drops the packet. **Log** : Logs the packet to the kernel log without allowing or denying it. Evaluation continues with subsequent rules. **Queue** : Pass the packet to userspace. **Reject** : Send a response back and drop the packet.  **Important:** Ensure that rule configurations are supported by the Linux distributions and versions on endpoints where the policy is enforced. For example, the **Queue** target is not supported by default on RHEL and CentOS 7 and later. Refer to the documentation for a specific distribution and firewall for information about supported configurations.
Network Protocol	(Optional) Select the protocol of the rule or of the packet to check. The specified protocol can be one of the predefined options or it can be a numeric value, representing one of these protocols or a different one. Protocol **all** is the default when this option is omitted. Select the **Inverse** option to include everything except for the selected protocol.
State	(Optional) Select one of the following options: • **New**: The packet has started a new connection. • **Established**: The packet is associated with a connection which has seen packets in both directions. • **Related**: The packet is starting a new connection, but is associated with an existing connection. • **Invalid**: The packet could not be identified for some reason.
Source Address	(Optional) A comma separated list of network names, IP addresses with masks, plain IP addresses, or IP address ranges. Select the **Inverse** option to include everything except for addresses you entered.
Destination Address	(Optional) A comma separated list of network names, IP addresses with masks, plain IP addresses, or IP address ranges.

©2026 Tanium Inc. All Rights Reserved

Field	Description
	Select the **Inverse** option to include everything except for addresses you entered.
Optional fields that might appear depending on choices you make for some of the fields above:	
Source Port(s)	A comma separated list of ports or port ranges (0–65535). If you are specifying port ranges, use a colon as a delimiter.
Destination Port(s)	A comma separated list of ports or port ranges (0–65535). If you are specifying port ranges, use a colon as a delimiter.
In Interface	Name of an interface by which a packet was received.
Out Interface	Name of an interface by which a packet is going to be sent.

Note: Depending on the choices you make for the **Chain**, **Target**, and **Network Protocol** fields, additional optional fields might appear that you can complete.

11. Click **Add Rule** to add additional rules as necessary.
12. (Optional) To Import Linux firewall rules from Tanium endpoints, click **Import** > **Import Rules from Tanium endpoints** in the **Firewall Rules** section.
    a. In the **Import Rules from Tanium Endpoints** window, select a **Computer Group** or **Computer Name** and select the existing rules on Tanium Client managed endpoints that you want to import.
    b. Click **Import Rules**.

Note: Some rules might specify **rule not supported.** in the **Table** column, which means that Enforce does not support this rule. In this scenario, the rule configuration shows in the **Table** field so that you can configure it manually if needed.

Next steps

Enforce the policy from the **Enforcements** tab of the **Policy Configurations** page. For more information, see Enforcing policies on page 163.

©2026 Tanium Inc. All Rights Reserved

Creating policies for Kubernetes clusters

Use cluster policies to manage images and resources for Kubernetes clusters. Cluster policies are available only when Cloud Workloads is configured and the Tanium Client images are deployed to the targeted cluster.

Create an Allow External Services by IP policy

About this task

Use **Allow External Services by IP** policies to allow external services that have any of the specified IP addresses.

1. From the Main menu, go to **Modules** > **Enforce** > **Policy Configurations** > **Create**.
2. Click **Select Types**.
3. Select **Kubernetes** as the **Platform** for the endpoints that you want to target with the policies.
4. Select **Allow External Services by IP** as the policy type.

   > **Note:** Only Windows policies can include more than one policy type.

5. Click **Confirm**.
6. In the **Summary** section, provide the identifying details for the policy.
   a. Enter a **Name** and optional **Description** for the policy.
   b. If you do not want to use the default content set for the policy, select a **Content Set**. Every policy requires a content set. The content set is configured by default to the platform for the selected policy types, provided that you have the necessary permissions for that content set. If no content set is available, you might need additional permissions. For more information, see Tanium Console User Guide: Role permissions for content sets.

©2026 Tanium Inc. All Rights Reserved

7. On the **Rules** tab, review the default rule, which specifies the resources to evaluate with the policy, and update it if needed.
    - (Optional) Click **Add Rule** to add rules to specify additional resources to evaluate with the policy.

      > **Note:** The **Resource Types**, **API Groups**, and **API Versions** rules can be modified only for **Block Resources by Version** and **Custom OPA** policy types.

8. On the **Object Labels** tab, review the default rules, which specify the labels to evaluate with the policy. Only objects that match the specified label selectors are evaluated by this policy. The default **Object Labels** rules cannot be modified.
    - (Optional) Click **Add Label** to add additional labels to evaluate with the policy. Specify the **Key**, **Operator**, and **Value** for the label.

      For more information about object labels in Kubernetes, see Kubernetes Documentation: Labels and Selectors.

9. On the **Namespace Labels** tab, review the default rules, which specify the namespace labels to evaluate with the policy. Only objects in namespaces that match the specified label selectors are evaluated by this policy. The default **Namespace Labels** rules cannot be modified.
    - (Optional) Click **Add Label** to add additional namespace labels to evaluate with the policy. Specify the **Key**, **Operator**, and **Value** for the label.

      For more information about namespaces in Kubernetes, see Kubernetes Documentation: Namespaces.

10. On the **Configuration** tab, provide the configuration details for the policy:
    a. Select a **Mode**:
        - **Dry Run**: Logs the results that the policy would have in the **Event History** of the enforcement details page, but does not enforce the policy.
        - **Enforce**. Enforces the policy on targets in a given enforcement.

    b. Select a **Failure Policy**:
        - **Fail Closed**: If the Tanium Admission Controller fails to evaluate a request for this policy, deny the request.
        - **Fail Open**: If the Tanium Admission Controller fails to evaluate a request for

©2026 Tanium Inc. All Rights Reserved

this policy, allow the request.

c. In the **Allowed External IP Addresses** section, select the IP addresses to allow when creating service resources in Kubernetes.

11. Click **Create**.

Next steps

Enforce the policy from the **Enforcements** tab of the **Policy Configurations** page. For more information, see Enforcing policies on page 163.

Create an Allow Images by Registry policy

About this task

Use **Allow Images by Registry** policies to select specific registries that should be allowed for use in the cluster.

1. From the Main menu, go to **Modules** > **Enforce** > **Policy Configurations** > **Create**.
2. Click **Select Types**.
3. Select **Kubernetes** as the **Platform** for the endpoints that you want to target with the policies.
4. Select **Allow Images by Registry** as the policy type.

   Note: Only Windows policies can include more than one policy type.

5. Click **Confirm**.
6. In the **Summary** section, provide the identifying details for the policy.
   a. Enter a **Name** and optional **Description** for the policy.
   b. If you do not want to use the default content set for the policy, select a **Content Set**. Every policy requires a content set. The content set is configured by default to the platform for the selected policy types, provided that you have the necessary permissions for that content set. If no content set is available, you might need additional permissions. For more information, see Tanium Console User Guide: Role permissions for content sets.
7. On the **Rules** tab, review the default rule, which specifies the resources to evaluate with the

©2026 Tanium Inc. All Rights Reserved

policy, and update it if needed.

- (Optional) Click **Add Rule** to add rules to specify additional resources to evaluate with the policy.

> **Note:** The **Resource Types**, **API Groups**, and **API Versions** rules can be modified only for **Block Resources by Version** and **Custom OPA** policy types.

8. On the **Object Labels** tab, review the default rules, which specify the labels to evaluate with the policy. Only objects that match the specified label selectors are evaluated by this policy. The default **Object Labels** rules cannot be modified.
   - (Optional) Click **Add Label** to add additional labels to evaluate with the policy. Specify the **Key**, **Operator**, and **Value** for the label.

     For more information about object labels in Kubernetes, see Kubernetes Documentation: Labels and Selectors.

9. On the **Namespace Labels** tab, review the default rules, which specify the namespace labels to evaluate with the policy. Only objects in namespaces that match the specified label selectors are evaluated by this policy. The default **Namespace Labels** rules cannot be modified.
   - (Optional) Click **Add Label** to add additional namespace labels to evaluate with the policy. Specify the **Key**, **Operator**, and **Value** for the label.

     For more information about namespaces in Kubernetes, see Kubernetes Documentation: Namespaces.

10. On the **Configuration** tab, provide the configuration details for the policy:
    a. Select a **Mode**:
       - **Dry Run**: Logs the results that the policy would have in the **Event History** of the enforcement details page, but does not enforce the policy.
       - **Enforce**. Enforces the policy on targets in a given enforcement.

    b. Select a **Failure Policy**:
       - **Fail Closed**: If the Tanium Admission Controller fails to evaluate a request for this policy, deny the request.
       - **Fail Open**: If the Tanium Admission Controller fails to evaluate a request for this policy, allow the request.

©2026 Tanium Inc. All Rights Reserved

c. In the **Image Registries** section, select an existing image registry or add a new image registry to allow.
d. (Optional) Select **Always Pull Image** to set `imagePullPolicy=Always`. This setting forces Kubernetes to compare the manifest of a local image to its remote counterpart to ensure a possibly manipulated local image does not imitate the trusted remote image. This option is enabled by default.

11. Click **Create**.

Next steps

Enforce the policy from the **Enforcements** tab of the **Policy Configurations** page. For more information, see Enforcing policies on page 163.

Create an Allow Ingress Actions by Hostname policy

About this task

Use **Allow ingress actions by Hostname** policies to specify the hostnames that are allowed when creating ingress resources in the cluster.

1. From the Main menu, go to **Modules** > **Enforce** > **Policy Configurations** > **Create**.
2. Click **Select Types**.
3. Select **Kubernetes** as the **Platform** for the endpoints that you want to target with the policies.
4. Select **Allow Ingress Actions by Hostname** as the policy type.

   > **Note:** Only Windows policies can include more than one policy type.

5. In the **Summary** section, provide the identifying details for the policy.
   a. Enter a **Name** and optional **Description** for the policy.
   b. If you do not want to use the default content set for the policy, select a **Content Set**. Every policy requires a content set. The content set is configured by default to the platform for the selected policy types, provided that you have the necessary permissions for that content set. If no content set is available, you might need additional permissions. For more information, see Tanium Console User Guide: Role permissions for content sets.

©2026 Tanium Inc. All Rights Reserved

6. On the **Rules** tab, review the default rule, which specifies the resources to evaluate with the policy, and update it if needed.
    - (Optional) Click **Add Rule** to add rules to specify additional resources to evaluate with the policy.

    > **Note:** The **Resource Types**, **API Groups**, and **API Versions** rules can be modified only for **Block Resources by Version** and **Custom OPA** policy types.

7. On the **Object Labels** tab, review the default rules, which specify the labels to evaluate with the policy. Only objects that match the specified label selectors are evaluated by this policy. The default **Object Labels** rules cannot be modified.
    - (Optional) Click **Add Label** to add additional labels to evaluate with the policy. Specify the **Key**, **Operator**, and **Value** for the label.

      For more information about object labels in Kubernetes, see Kubernetes Documentation: Labels and Selectors.

8. On the **Namespace Labels** tab, review the default rules, which specify the namespace labels to evaluate with the policy. Only objects in namespaces that match the specified label selectors are evaluated by this policy. The default **Namespace Labels** rules cannot be modified.
    - (Optional) Click **Add Label** to add additional namespace labels to evaluate with the policy. Specify the **Key**, **Operator**, and **Value** for the label.

      For more information about namespaces in Kubernetes, see Kubernetes Documentation: Namespaces.

9. On the **Configuration** tab, provide the configuration details for the policy:
    a. Select a **Mode**:
        - **Dry Run**: Logs the results that the policy would have in the **Event History** of the enforcement details page, but does not enforce the policy.
        - **Enforce**. Enforces the policy on targets in a given enforcement.

    b. Select a **Failure Policy**:
        - **Fail Closed**: If the Tanium Admission Controller fails to evaluate a request for this policy, deny the request.
        - **Fail Open**: If the Tanium Admission Controller fails to evaluate a request for

©2026 Tanium Inc. All Rights Reserved

this policy, allow the request.

c. In the **Allowed Ingress Hostnames** section, specify the hostnames allowed when creating ingress resources in Kubernetes.

10. Click **Create**.

Next steps

Enforce the policy from the **Enforcements** tab of the **Policy Configurations** page. For more information, see Enforcing policies on page 163.

Create a Block Images by Registry policy

About this task

Use **Block Images by Registry** policies to block images that are included in the set of selected registries.

1. From the Main menu, go to **Modules** > **Enforce** > **Policy Configurations** > **Create**.
2. Click **Select Types**.
3. Select **Kubernetes** as the **Platform** for the endpoints that you want to target with the policies.
4. Select **Block Images by Registry policy** as the policy type.

   Note: Only Windows policies can include more than one policy type.

5. Click **Create**.
6. In the **Summary** section, provide the identifying details for the policy.
   a. Enter a **Name** and optional **Description** for the policy.
   b. If you do not want to use the default content set for the policy, select a **Content Set**. Every policy requires a content set. The content set is configured by default to the platform for the selected policy types, provided that you have the necessary permissions for that content set. If no content set is available, you might need additional permissions. For more information, see Tanium Console User Guide: Role permissions for content sets.
7. On the **Rules** tab, review the default rule, which specifies the resources to evaluate with the

©2026 Tanium Inc. All Rights Reserved

policy, and update it if needed.

- (Optional) Click **Add Rule** to add rules to specify additional resources to evaluate with the policy.

> **Note:** The **Resource Types**, **API Groups**, and **API Versions** rules can be modified only for **Block Resources by Version** and **Custom OPA** policy types.

8. On the **Object Labels** tab, review the default rules, which specify the labels to evaluate with the policy. Only objects that match the specified label selectors are evaluated by this policy. The default **Object Labels** rules cannot be modified.
   - (Optional) Click **Add Label** to add additional labels to evaluate with the policy. Specify the **Key**, **Operator**, and **Value** for the label.

     For more information about object labels in Kubernetes, see Kubernetes Documentation: Labels and Selectors.

9. On the **Namespace Labels** tab, review the default rules, which specify the namespace labels to evaluate with the policy. Only objects in namespaces that match the specified label selectors are evaluated by this policy. The default **Namespace Labels** rules cannot be modified.
   - (Optional) Click **Add Label** to add additional namespace labels to evaluate with the policy. Specify the **Key**, **Operator**, and **Value** for the label.

     For more information about namespaces in Kubernetes, see Kubernetes Documentation: Namespaces.

10. On the **Configuration** tab, provide the configuration details for the policy:
    a. Select a **Mode**:
       - **Dry Run**: Logs the results that the policy would have in the **Event History** of the enforcement details page, but does not enforce the policy.
       - **Enforce**. Enforces the policy on targets in a given enforcement.

    b. Select a **Failure Policy**:
       - **Fail Closed**: If the Tanium Admission Controller fails to evaluate a request for this policy, deny the request.
       - **Fail Open**: If the Tanium Admission Controller fails to evaluate a request for this policy, allow the request.

©2026 Tanium Inc. All Rights Reserved

c. In the **Image Registries** section, select an existing image registry or add a new image registry to block.
d. (Optional) Select **Always Pull Image** to set `imagePullPolicy=Always`. This setting forces Kubernetes to compare the manifest of a local image to its remote counterpart to ensure a possibly manipulated local image does not imitate the trusted remote image. This option is enabled by default.

11. Click **Create**.

Next steps

Enforce the policy from the **Enforcements** tab of the **Policy Configurations** page. For more information, see Enforcing policies on page 163.

Create a Block Images by Tag policy

About this task

Use **Block Images by Tag** policies to block any images that have any of the specified image tags.

1. From the Main menu, go to **Modules** > **Enforce** > **Policy Configurations** > **Create**.
2. Click **Select Types**.
3. Select **Kubernetes** as the **Platform** for the endpoints that you want to target with the policies.
4. Select **Block Images by Tag** as the policy type.

   Note: Only Windows policies can include more than one policy type.

5. Click **Confirm**.
6. In the **Summary** section, provide the identifying details for the policy.
   a. Enter a **Name** and optional **Description** for the policy.
   b. If you do not want to use the default content set for the policy, select a **Content Set**. Every policy requires a content set. The content set is configured by default to the platform for the selected policy types, provided that you have the necessary permissions for that content set. If no content set is available, you might need additional permissions. For more information, see Tanium Console User Guide: Role permissions for content sets.

©2026 Tanium Inc. All Rights Reserved

7. On the **Rules** tab, review the default rule, which specifies the resources to evaluate with the policy, and update it if needed.
    - (Optional) Click **Add Rule** to add rules to specify additional resources to evaluate with the policy.

      > **Note:** The **Resource Types**, **API Groups**, and **API Versions** rules can be modified only for **Block Resources by Version** and **Custom OPA** policy types.

8. On the **Object Labels** tab, review the default rules, which specify the labels to evaluate with the policy. Only objects that match the specified label selectors are evaluated by this policy. The default **Object Labels** rules cannot be modified.
    - (Optional) Click **Add Label** to add additional labels to evaluate with the policy. Specify the **Key**, **Operator**, and **Value** for the label.

      For more information about object labels in Kubernetes, see Kubernetes Documentation: Labels and Selectors.

9. On the **Namespace Labels** tab, review the default rules, which specify the namespace labels to evaluate with the policy. Only objects in namespaces that match the specified label selectors are evaluated by this policy. The default **Namespace Labels** rules cannot be modified.
    - (Optional) Click **Add Label** to add additional namespace labels to evaluate with the policy. Specify the **Key**, **Operator**, and **Value** for the label.

      For more information about namespaces in Kubernetes, see Kubernetes Documentation: Namespaces.

10. On the **Configuration** tab, provide the configuration details for the policy:
    a. Select a **Mode**:
        - **Dry Run**: Logs the results that the policy would have in the **Event History** of the enforcement details page, but does not enforce the policy.
        - **Enforce**. Enforces the policy on targets in a given enforcement.

    b. Select a **Failure Policy**:
        - **Fail Closed**: If the Tanium Admission Controller fails to evaluate a request for this policy, deny the request.
        - **Fail Open**: If the Tanium Admission Controller fails to evaluate a request for

©2026 Tanium Inc. All Rights Reserved

this policy, allow the request.

c. In the **Image Tags** section, select an existing tag or add a new tag to block.
d. (Optional) Select **Always Pull Image** to set `imagePullPolicy=Always`. This setting forces Kubernetes to compare the manifest of a local image to its remote counterpart to ensure a possibly manipulated local image does not imitate the trusted remote image. This option is enabled by default.

11. Click **Create**.

Next steps

Enforce the policy from the **Enforcements** tab of the **Policy Configurations** page. For more information, see Enforcing policies on page 163.

Create a Block Resources by Version policy

About this task

Use **Block Resources by Version** policies to block the creation of out of date APIs.

1. From the Main menu, go to **Modules** > **Enforce** > **Policy Configurations** > **Create**.
2. Click **Select Types**.
3. Select **Kubernetes** as the **Platform** for the endpoints that you want to target with the policies.
4. Select **Block Resources by Version** as the policy type.

   > **Note:** Only Windows policies can include more than one policy type.

5. In the **Summary** section, provide the identifying details for the policy.
   a. Enter a **Name** and optional **Description** for the policy.
   b. If you do not want to use the default content set for the policy, select a **Content Set**. Every policy requires a content set. The content set is configured by default to the platform for the selected policy types, provided that you have the necessary permissions for that content set. If no content set is available, you might need additional permissions. For more information, see Tanium Console User Guide: Role permissions for content sets.

©2026 Tanium Inc. All Rights Reserved

6. On the **Rules** tab, review the default rule, which specifies the resources to evaluate with the policy, and update it if needed.
    - (Optional) Click **Add Rule** to add rules to specify additional parameters to evaluate with the policy. Specify the details for the rule:
        - **Operations**: Select Kubernetes operations to evaluate the policy against.
        - **Resources Types**: Select the Kubernetes resource types to evaluate the policy against.
        - **API Groups**: Specify the API groups to evaluate with this policy.
        - **API Versions**: Specify the Kubernetes API versions to block.
7. On the **Object Labels** tab, review the default rules, which specify the labels to evaluate with the policy. Only objects that match the specified label selectors are evaluated by this policy. The default **Object Labels** rules cannot be modified.
    - (Optional) Click **Add Label** to add additional labels to evaluate with the policy. Specify the **Key**, **Operator**, and **Value** for the label.

      For more information about object labels in Kubernetes, see Kubernetes Documentation: Labels and Selectors.
8. On the **Namespace Labels** tab, review the default rules, which specify the namespace labels to evaluate with the policy. Only objects in namespaces that match the specified label selectors are evaluated by this policy. The default **Namespace Labels** rules cannot be modified.
    - (Optional) Click **Add Label** to add additional namespace labels to evaluate with the policy. Specify the **Key**, **Operator**, and **Value** for the label.

      For more information about namespaces in Kubernetes, see Kubernetes Documentation: Namespaces.
9. On the **Configuration** tab, provide the configuration details for the policy:
    a. Select a **Mode**:
        - **Dry Run**: Logs the results that the policy would have in the **Event History** of the enforcement details page, but does not enforce the policy.
        - **Enforce**. Enforces the policy on targets in a given enforcement.

©2026 Tanium Inc. All Rights Reserved

b. Select a **Failure Policy**:
   - **Fail Closed**: If the Tanium Admission Controller fails to evaluate a request for this policy, deny the request.
   - **Fail Open**: If the Tanium Admission Controller fails to evaluate a request for this policy, allow the request.

10. Click **Create**.

Next steps

Enforce the policy from the **Enforcements** tab of the **Policy Configurations** page. For more information, see Enforcing policies on page 163.

Create a Block Rogue Containers policy

About this task

Use **Block Rogue Containers** policies to block any images that are not from the list of trusted registries configured in Cloud Workloads.

1. From the Main menu, go to **Modules** > **Enforce** > **Policy Configurations** > **Create**.
2. Click **Select Types**.
3. Select **Kubernetes** as the **Platform** for the endpoints that you want to target with the policies.
4. Select **Block Rogue Containers** as the policy type.

   Note: Only Windows policies can include more than one policy type.

5. Click **Confirm**.
6. In the **Summary** section, provide the identifying details for the policy.
   a. Enter a **Name** and optional **Description** for the policy.
   b. If you do not want to use the default content set for the policy, select a **Content Set**. Every policy requires a content set. The content set is configured by default to the platform for the selected policy types, provided that you have the necessary permissions for that content set. If no content set is available, you might need additional permissions. For more information, see Tanium Console User Guide: Role

©2026 Tanium Inc. All Rights Reserved

permissions for content sets.

7. On the **Rules** tab, review the default rule, which specifies the resources to evaluate with the policy, and update it if needed.
    - (Optional) Click **Add Rule** to add rules to specify additional resources to evaluate with the policy.

      > **Note:** The **Resource Types**, **API Groups**, and **API Versions** rules can be modified only for **Block Resources by Version** and **Custom OPA** policy types.

8. On the **Object Labels** tab, review the default rules, which specify the labels to evaluate with the policy. Only objects that match the specified label selectors are evaluated by this policy. The default **Object Labels** rules cannot be modified.
    - (Optional) Click **Add Label** to add additional labels to evaluate with the policy. Specify the **Key**, **Operator**, and **Value** for the label.

      For more information about object labels in Kubernetes, see Kubernetes Documentation: Labels and Selectors.

9. On the **Namespace Labels** tab, review the default rules, which specify the namespace labels to evaluate with the policy. Only objects in namespaces that match the specified label selectors are evaluated by this policy. The default **Namespace Labels** rules cannot be modified.
    - (Optional) Click **Add Label** to add additional namespace labels to evaluate with the policy. Specify the **Key**, **Operator**, and **Value** for the label.

      For more information about namespaces in Kubernetes, see Kubernetes Documentation: Namespaces.

10. On the **Configuration** tab, provide the configuration details for the policy:
    a. Select a **Mode**:
        - **Dry Run**: Logs the results that the policy would have in the **Event History** of the enforcement details page, but does not enforce the policy.
        - **Enforce**. Enforces the policy on targets in a given enforcement.

    b. Select a **Failure Policy**:
        - **Fail Closed**: If the Tanium Admission Controller fails to evaluate a request for this policy, deny the request.

©2026 Tanium Inc. All Rights Reserved

- **Fail Open**: If the Tanium Admission Controller fails to evaluate a request for this policy, allow the request.

c. (Optional) Select **Always Pull Image** to set `imagePullPolicy=Always`. This setting forces Kubernetes to compare the manifest of a local image to its remote counterpart to ensure a possibly manipulated local image does not imitate the trusted remote image. This option is enabled by default.

11. Click **Create**.

Next steps

Enforce the policy from the **Enforcements** tab of the **Policy Configurations** page. For more information, see Enforcing policies on page 163.

Create a Custom OPA policy

About this task

Use **Custom OPA** policies to provide a block of Rego code to configure custom Open Policy Agent (OPA) policies.

1. From the Main menu, go to **Modules** > **Enforce** > **Policy Configurations** > **Create**.
2. Click **Select Types**.
3. Select **Kubernetes** as the **Platform** for the endpoints that you want to target with the policies.
4. Select **Custom OPA policy** as the policy type.

   Note: Only Windows policies can include more than one policy type.

5. In the **Summary** section, provide the identifying details for the policy.
   a. Enter a **Name** and optional **Description** for the policy.
   b. If you do not want to use the default content set for the policy, select a **Content Set**. Every policy requires a content set. The content set is configured by default to the platform for the selected policy types, provided that you have the necessary permissions for that content set. If no content set is available, you might need additional permissions. For more information, see Tanium Console User Guide: Role permissions for content sets.

©2026 Tanium Inc. All Rights Reserved

6. On the **Rules** tab, review the default rule, which specifies the resources to evaluate with the policy, and update it if needed.
    - (Optional) Click **Add Rule** to add rules to specify additional parameters to evaluate with the policy. Specify the details for the rule:
        - **Resources Types**: Select the Kubernetes resource types to evaluate the policy against.
        - **API Groups**: Specify the API groups to evaluate with this policy.
        - **API Versions**: Specify the Kubernetes API versions to block.

        > **Note:** The **Operations** rules cannot be modified for **Custom OPA** policy types.

7. On the **Object Labels** tab, review the default rules, which specify the labels to evaluate with the policy. Only objects that match the specified label selectors are evaluated by this policy. The default **Object Labels** rules cannot be modified.
    - (Optional) Click **Add Label** to add additional labels to evaluate with the policy. Specify the **Key**, **Operator**, and **Value** for the label.

      For more information about object labels in Kubernetes, see Kubernetes Documentation: Labels and Selectors.

8. On the **Namespace Labels** tab, review the default rules, which specify the namespace labels to evaluate with the policy. Only objects in namespaces that match the specified label selectors are evaluated by this policy. The default **Namespace Labels** rules cannot be modified.
    - (Optional) Click **Add Label** to add additional namespace labels to evaluate with the policy. Specify the **Key**, **Operator**, and **Value** for the label.

      For more information about namespaces in Kubernetes, see Kubernetes Documentation: Namespaces.

9. On the **Configuration** tab, provide the configuration details for the policy:
    a. Select a **Mode**:
        - **Dry Run**: Logs the results that the policy would have in the **Event History** of the enforcement details page, but does not enforce the policy.
        - **Enforce**. Enforces the policy on targets in a given enforcement.

©2026 Tanium Inc. All Rights Reserved

b. Select a **Failure Policy**:
   - **Fail Closed**: If the Tanium Admission Controller fails to evaluate a request for this policy, deny the request.
   - **Fail Open**: If the Tanium Admission Controller fails to evaluate a request for this policy, allow the request.

c. In the **Rego Policy** section, provide the Rego code for the policy.



Note: Click **Copy Template** to copy an example policy and modify the policy for your environment:

- Package: The policy package must be named `tanium`.
- Expressions: The policy must include a single expression, named `deny`, that consists of a list of strings that represent the reasons for which the request is denied. To allow a request, set `deny` to an empty list.
- Input: Use `input.request` to reference the input to the policy, where `request` is the admission request received by the Kubernetes admissions controller.

10. Click **Create**.

Next steps

Enforce the policy from the **Enforcements** tab of the **Policy Configurations** page. For more information, see Enforcing policies on page 163.

Kubernetes®, K8s®, and the Kubernetes logo are registered trademarks of The Linux Foundation®.

Managing policies

(Windows) Importing policies from a Group Policy backup

About this task

You can import a Windows Group Policy backup and automatically create a policy with the configuration required for endpoint compliance.

1. Download a build kit from the CIS website or export Group Policy settings to create a Group Policy backup. Compress the files into a ZIP file.
2. From the Main menu, go to **Modules** > **Enforce** > **Policy Configurations** > **Import**.
3. Browse to the build kit file or Group Policy backup. Click **Open**.
4. If the file contains more than one backup, select one or more of the backups in the file to include with the import.
   If the file contains many backups, use the search field to filter the list by backup name.

   If selected backups contain conflicting settings, the conflicting backups are highlighted with . Deselect one of the conflicting backups and try the import again.
5. Click **Import**.
6. A page shows the high-level details and the settings configured by the imported file. Click **Create Policy**.
7. The Create Policy page opens. Specify the details for the policy in the Summary section:
   a. **Name**
   b. (Optional) **Description**
   c. **Content Set**

   > **Note:** The content set is selected automatically based on the policy type. Change it only if the default is not the content set you want to use.
8. Check for any settings that require attention (noted with ) and resolve the issue.

©2026 Tanium Inc. All Rights Reserved

9. Click **Create**.

Next steps
Enforce the policy on endpoints. For more information, see Enforcing policies on page 163

Import policies

About this task

You can import one or more policies from a JSON file.

> **Note:** Legacy BitLocker policies cannot be imported.

1. From the Main menu, go to **Modules** > **Enforce** > **Policy Configurations** > **Import**.
2. Click **Browse for file**, select the JSON file, and click **Import**.
3. Make any necessary changes and then click **Save**.

   > **Note:** The content set is selected automatically based on the policy type. Change it only if the default is not the content set you want to use.

   > **Note:** You might have to change an imported policy name if the name conflicts with the name of an existing policy.

Result

Imported policies appear on the **Policies** page.

Export policies

1. From the Main menu, go to **Modules** > **Enforce** > **Policy Configurations**.
2. Select the policies that you want to export. Then click Options ⋮ and **Export**.

Result

Each policy is downloaded as a separate JSON file. You can use each downloaded JSON file to import

©2026 Tanium Inc. All Rights Reserved

each policy.

Prioritize policies

About this task

All cluster policies are enforced on targeted endpoints, so these policy types are not prioritized.

A single policy can contain multiple settings. When several policies are enforced on an endpoint, unique settings across all policies are applied. If duplicate settings exist for an endpoint, the setting with the lowest priority number takes precedence. See Applying policy settings on endpoints on page 163 for more information about how policy settings are applied to endpoints.

Note: The **Prioritize** button appears only if you have the **Enforce Policy Prioritize** permission and read access to the **All Computers** computer group.

Note:

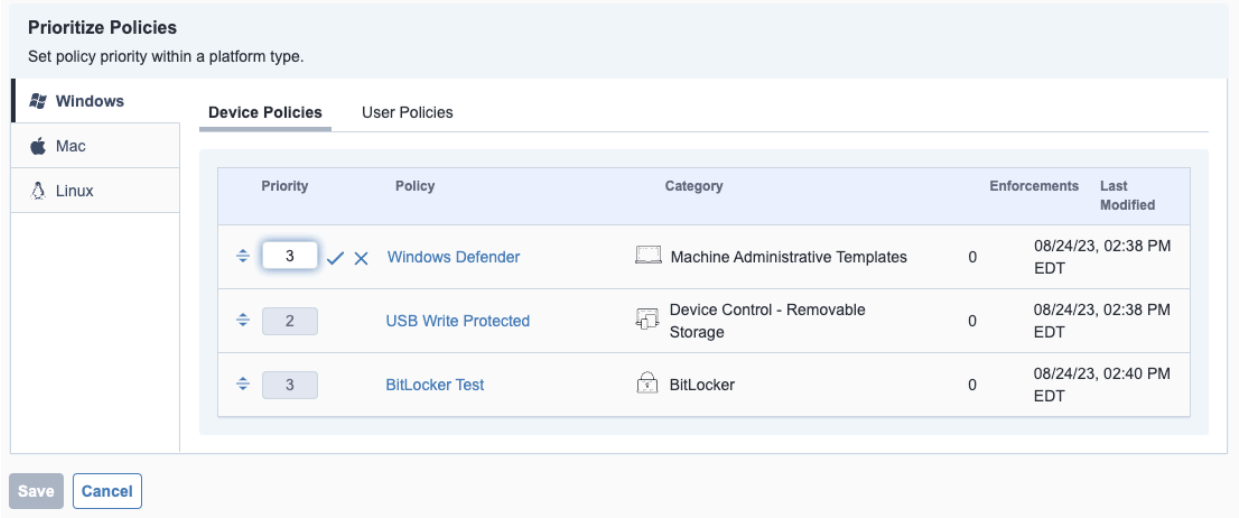
- The policy with the highest priority has the lowest priority number. For example, a policy with a priority of **1** takes precedence over a policy with a priority of **10**.
- Tanium Removable Storage Access Control policies are additive; therefore, these policies are not included on the **Prioritize Policies** page.
- BitLocker policies always supersede legacy BitLocker policies, even if the legacy BitLocker policy has a higher priority.
- All cluster policies are enforced on targeted endpoints, so these policy types are not prioritized.

Set the prioritization of policies to determine which policy setting is applied if a conflict exists.

1. From the Main menu, go to **Modules** > **Enforce** > **Policy Configurations** > **Prioritize** to make the priority fields editable.
2. Click the priority field for the policy you want to change and enter a new priority number.

©2026 Tanium Inc. All Rights Reserved

Click Preview updated priorities ✓ to accept the change or Cancel ✕ to undo the change. When you click Preview updated priorities ✓, the priority number for all policies update based on your change.



3. (Optional) To revert your changes back to the original priorities, click **Cancel**.
4. To keep the new priorities, click **Save**.

©2026 Tanium Inc. All Rights Reserved

Enforcing policies

How you enforce a policy depends on the type of policy you want to enforce:

- You enforce remediation policies from the **Enforcements** tab of the **Device Actions** page.
- You enforce all other policy types from the **Enforcements** tab of the **Policy Configurations** page.

You can also click a policy name and create an enforcement from the policy page.

After you create a policy, it is enforced in the following scenarios:

- The enforcement is first created
- Changes are made to the policy corresponding to the enforcement
- The Tanium Client or Tanium Client process restarts on an endpoint
- At the beginning and end of the enforcement schedule
- Enforce detects a failed or incomplete verification of policies
- (User Administrative Template policies) When a user signs in to an endpoint

Enforce verifies policies approximately every 15 minutes.

Applying policy settings on endpoints

The policy type and endpoint setup determine how policy settings are applied.

Configuration service providers (CSPs)

When you enforce a Bitlocker policy, Machine Administrative Template policy, Security Settings policy, or User Administrative Template policy, settings on supported Windows 10 and later endpoints are applied using configuration service providers (CSPs) when possible. Settings that can be applied using a CSP are annotated with this icon in the Enforce policy. When you apply policies

©2026 Tanium Inc. All Rights Reserved

using a CSP, domain-joined endpoints do not need to be connected to a Domain Controller to configure settings, unlike policy application using Group Policy Object (GPO). If an Enforce policy setting is applied using a CSP that is also applied by a group policy, local policy, or already configured manually in the registry, the setting that is applied by the CSP takes precedence. This means that you do not need to first configure settings as **Not Configured** before you can configure a setting using a CSP. For more information about CSPs, see Microsoft Documentation: What is a CSP?.

Enforce uses the WMI-to-CSP Bridge to apply policies on endpoints, so a mobile device management (MDM) service is not required to use this feature. For more information about the WMI-to-CSP Bridge, see Microsoft Documentation: The WMI-to-CSP Bridge.

Microsoft Policy DDF files determine which policy settings can be applied using a CSP. For more information about Policy DDF files, see Microsoft documentation: Policy DDF file. To determine the earliest supported Windows 10 operating system versions for a specific setting, hover over next to the setting. For more information about the supported operating system versions for each policy setting, see Microsoft Documentation: Policy Areas.

Enforce policies that were created before Enforce 2.1.273 are not applied using a CSP by default. To apply existing policies using a CSP, edit and re-save the policy.

Note: On Windows 10 version 1709 and earlier endpoints, policies enforced using GPO might override policies enforced using a CSP because the **ControlPolicyConflict** setting is not available. In this scenario, a message is logged to the endpoint client extension log: `Group Policy will override CSP policies in Windows 10 Version 1709 and earlier`. For more information about this limitation, see Microsoft Blog: Windows 10 Group Policy vs. Intune MDM Policy who wins?.

ADMX-backed CSP

Some settings in Machine Administrative Template and User Administrative Template policies are applied using ADMX-backed CSP. For more information, see Microsoft Documentation: ADMX-backed policies in Policy CSP.

Local Group Policy (LGPO)

When you enforce an AppLocker, Device Control - All Devices, or Device Control - Removable Storage policy, settings are applied using Local Group Policy (LGPO)

©2026 Tanium Inc. All Rights Reserved

For policy settings that are applied using LGPO, domain-joined endpoints must be able to connect to a domain controller so that Enforce can resolve conflicts and apply some settings. For more information, see Resolve Active Directory policy conflicts on page 211.

This requirement does not apply to Windows endpoints that are not joined to a domain or are EntraID-joined, Security Policy settings, or configuration service providers (CSPs).

Scheduled actions

When you enforce an Anti-Malware, Remediation, Remediation Purge, or Software Restriction policy, settings are applied using Tanium scheduled actions. These policies are not reported on by the **Enforce - Diagnostic - Applied Policy Settings** sensor. Instead, you can check the action history and action logs for status. For more information about scheduled actions, see Tanium Console User Guide: View action status.

API or CLI

When you enforce a FileVault, Firewall - Windows, or Firewall - Linux policy, settings are applied using the API or CLI on the endpoint.

> **Note:** Settings in Windows firewall policies are not applied on endpoints where there are existing firewall settings managed by a GPO linked to a domain. In this scenario, the enforcement status is `Not Applied` with the reason `GPO firewall rules found on endpoint`.

Create enforcements

Create an enforcement for a remediation policy

1. From the Main menu, go to **Modules** > **Enforce** > **Device Actions** > **Enforcements** > **Create**.
2. Enter a name for the enforcement and select a policy.
3. Go to Complete the enforcement creation on page 167 to continue creating the enforcement.

Create an enforcement for a cluster policy

About this task

©2026 Tanium Inc. All Rights Reserved

Note: Cluster policies are available only when Cloud Workloads is installed.

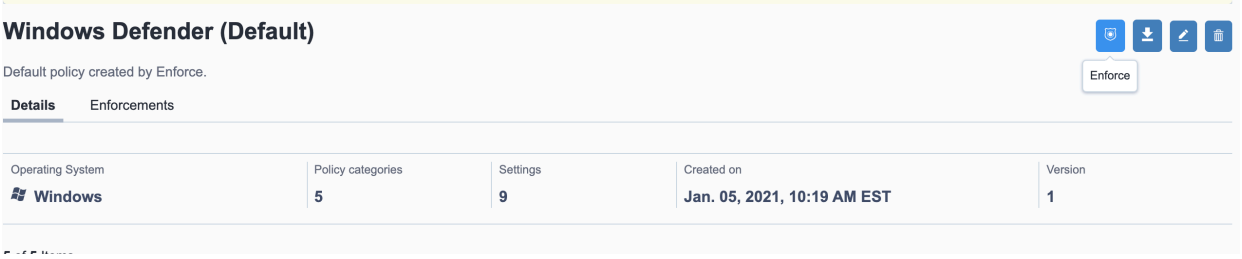
1. From the Main menu, go to **Modules** > **Enforce** > **Policy Configurations** > **Enforcements** > **Create**.
2. Enter a name for the enforcement and select a policy.
3. Go to Complete the enforcement creation for a cluster policy on page 169 to continue creating the enforcement.

Create an enforcement for all other types of policies

1. From the Main menu, go to **Modules** > **Enforce** > **Policy Configurations** > **Enforcements** > **Create**.
2. Enter a name for the enforcement and select a policy.
3. Go to Complete the enforcement creation on page 167 to continue creating the enforcement.

Create an enforcement from an individual policy

1. From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. From the Enforce menu, complete one of the following tasks:
   - For a remediation policy, click **Device Actions** > **Remediations**.
   - For all other policy types, click **Policy Configurations** > **Policies**.
2. Click the policy to be enforced and then click Enforce .
3. Enter a name for the enforcement.



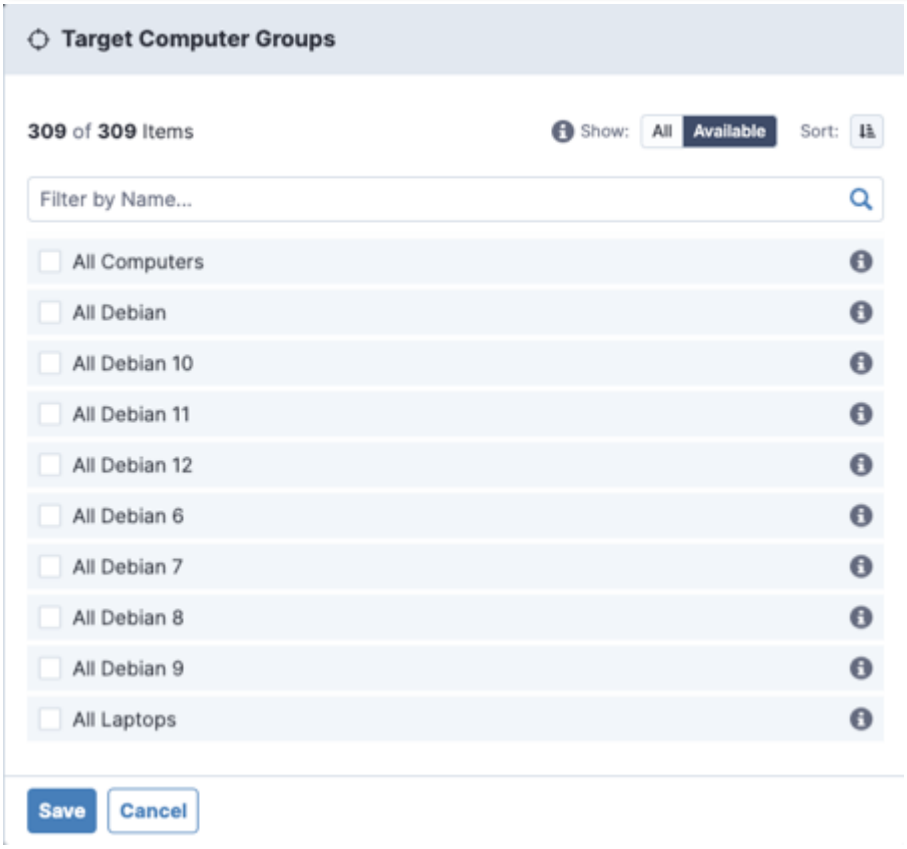
   The policy that you selected is automatically populated in the **Policy** field.
4. Go to Complete the enforcement creation on page 167 to continue creating the enforcement.

©2026 Tanium Inc. All Rights Reserved

Complete the enforcement creation

1. In the **Targeting** section, click **Select Computer Groups**, select one or more computer groups and then click **Save**. To search for a group, type the first few letters of the group into the search field.

   > **Note:** You might not have access to all computer groups that appear in the target list. Click **All** and **Available** in the target window to see every computer group or only the ones that you have permissions to view. Additionally, rules might limit your access to computers within the groups you select. For more information, see Role-based access control and configuration visibility on page 193.



2. (Optional) Select **Additional Filtering Criteria**:
   - Specify Endpoints: Enter a comma-separated list of computer names into the **Computer Names** field. This list cannot exceed 50 computer names.
   - Question Criteria: Enter a filter question or use the **Filter Builder** to build a filter.

©2026 Tanium Inc. All Rights Reserved

> **Note:**
>
> - If specified, the **Additional Filtering Criteria** is joined with the targeted computer groups using a logical AND.
> - You can use **Additional Filtering Criteria** to exclude endpoints from the targeted computer groups. If you use a question or rule, exclude computers by using a **does not contain**, **does not match**, or similar condition.

3. In the **Preview** section, review the computers that you want to target.
4. (Optional) In the **Scheduling** section, select the **Include Start Time** and **Include End Time** options for the enforcement.
   - Schedule a start time.
   - Schedule an end time if you want the policy enforcement to expire after a certain time frame. For example, allow writing to removable drives for only a finite period of time.

> **Note:**
>
> - When you select **Include Start Time** or **Include End Time**, Coordinated Universal Time (UTC) is selected and displayed by default. If you change the time to Endpoint Local Time (ELT), the selected time does not automatically update to reflect ELT. You must select a valid ELT before you can create the enforcement.
> - When you schedule an enforcement, allow enough time for the endpoint to receive the scheduling information. If the endpoint receives the scheduling information after the scheduled end time, then the enforcement does not run.

5. (Optional) For remediation policies, you can also set the following options:
   - **Repeat**: Select this option to repeat the action. The minimum allowed value for this field is 60 minutes.
   - **Distribute Over Time**: Control whether endpoints apply enforcements the moment they receive the action (immediate) or randomly within the saved action interval (diffused). Diffusing enforcements over time can help prevent a surge in network traffic in exchange for a slower time to compliance.
6. Click **Create** to create the enforcement.

©2026 Tanium Inc. All Rights Reserved

Result

> **Note:** To un-enforce or remove a policy from an endpoint, delete the enforcement. For more information, see Remove an enforcement on page 175.

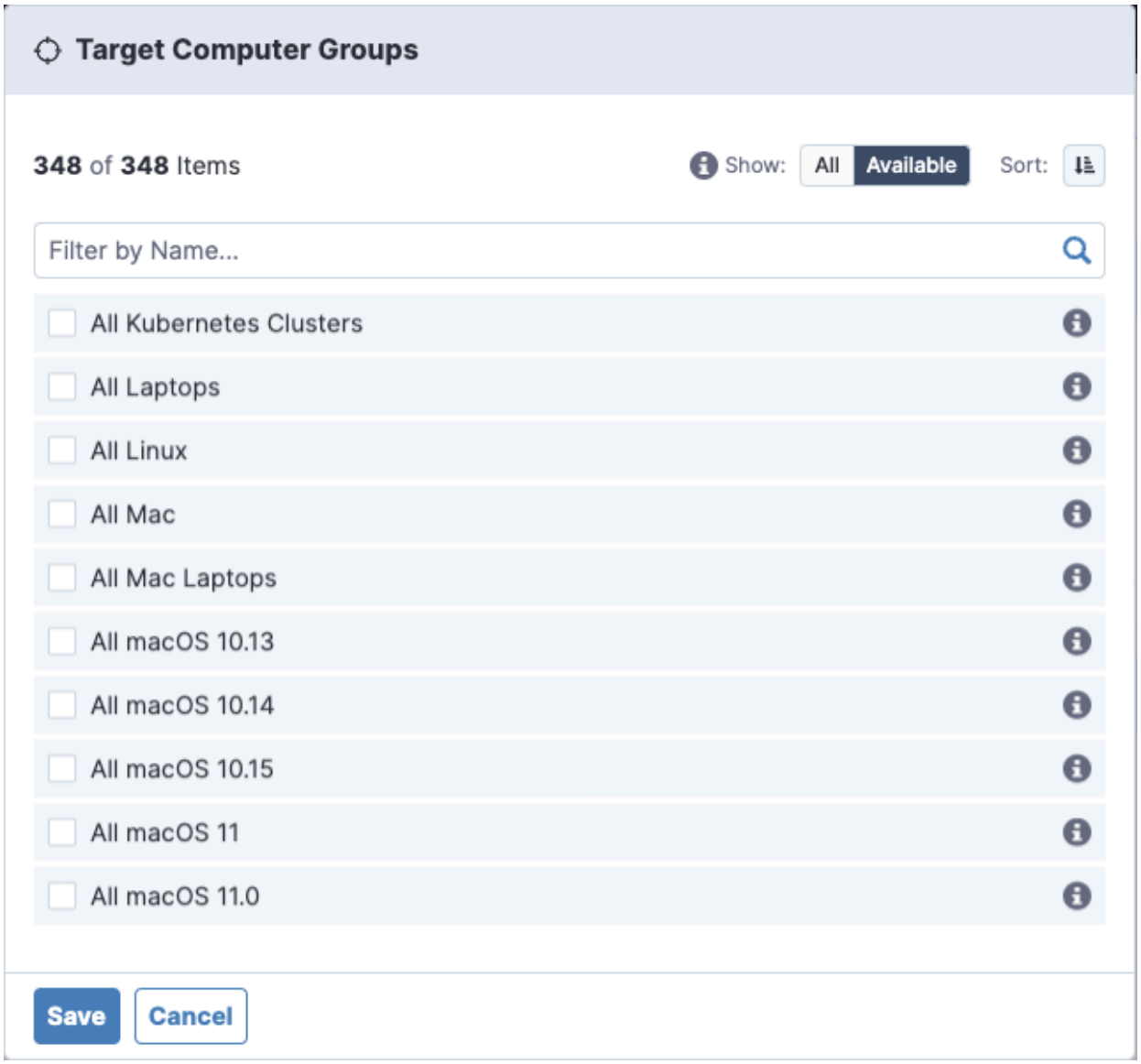
To view the status of an enforcement on the **Enforcements** tab of the **Policy Configurations** page, click the arrow next to an enforcement to expand the status information. You can also view the status information in the **Summary** section of the enforcement details page. For more information about each enforcement state, see Enforcements on page 17.

Complete the enforcement creation for a cluster policy

1. In the **Targeting** section, click **Select Computer Groups**, select one or more computer groups and then click **Save**. To search for a group, type the first few letters of the group into the search field.

   > **Note:** You might not have access to all computer groups that appear in the target list. Click **All** and **Available** in the target window to see every computer group or only the ones that you have permissions to view. Additionally, rules might limit your access to computers within the groups you select. For more information, see Role-based access control and configuration visibility on page 193.

©2026 Tanium Inc. All Rights Reserved



2. Specify the **Cluster Labels** to identify the targeted cluster. This label is assigned when you deploy the Tanium client to a cluster. For more information, see Cloud Workloads User Guide: Deploying clients. If you do not provide a **Cluster Label**, the policy is enforced on all clusters in the environment.
3. Click **Create** to create the enforcement.

Result

Note: To un-enforce or remove a policy from an endpoint, delete the enforcement. For more information, see Remove an enforcement on page 175.

To view the status of an enforcement on the **Enforcements** tab of the **Policy Configurations** page, click the arrow next to an enforcement to expand the status information. You can also view the status

©2026 Tanium Inc. All Rights Reserved

information in the **Summary** section of the enforcement details page. For more information about each enforcement state, see Enforcements on page 17.

View enforcements

Required access rights

To view enforcements, you must have one of the following access rights:

- The **Unrestricted Management Rights** permission.
- Access to the computer groups targeted by the enforcement.

> **Note:** You must have access to the exact computer group targeted by the enforcement to view the enforcement. Access to another computer group that includes the endpoints from the targeted computer group does not provide viewing access. For example, if you have access to the **All Windows** computer group, but not the **All Windows 10** computer group, you cannot view enforcements that target only the **All Windows 10** computer group.

For more information, see Tanium Console User Guide: Assign computer groups.

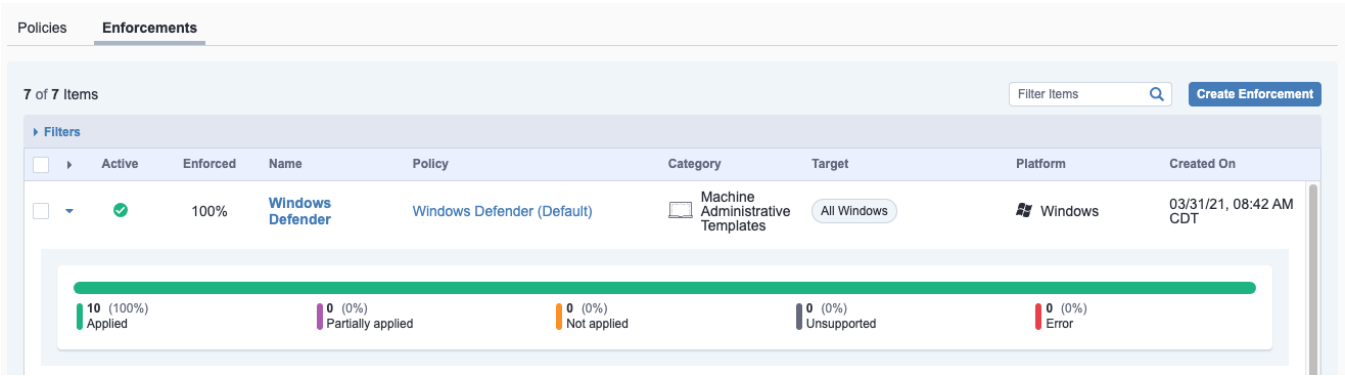
View the enforcement

- For a remediation policy: From the Main menu, go to **Modules** > **Enforce** > **Device Actions** > **Enforcements**.
- For all other policy types: From the Main menu, go to **Modules** > **Enforce** > **Policy Configurations** > **Enforcements**.

Expand the details for the enforcement to view the application status.

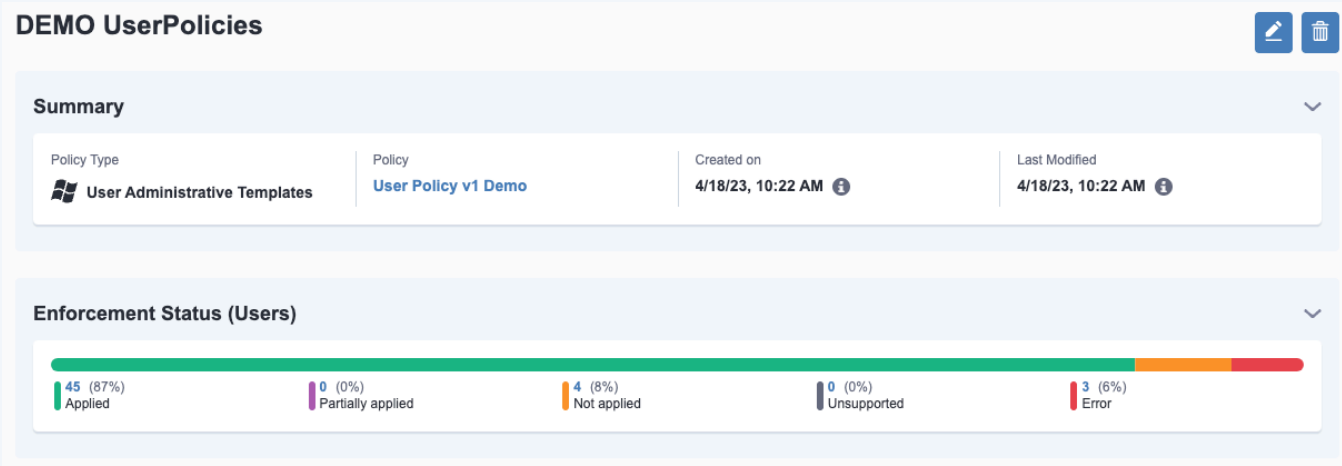
Figure 4. Enforcement status for a policy

©2026 Tanium Inc. All Rights Reserved



Click the name of the enforcement to open the enforcement details page.

Note: Enforcements for User Administrative Template policies show the enforcement status per user, not per endpoint.

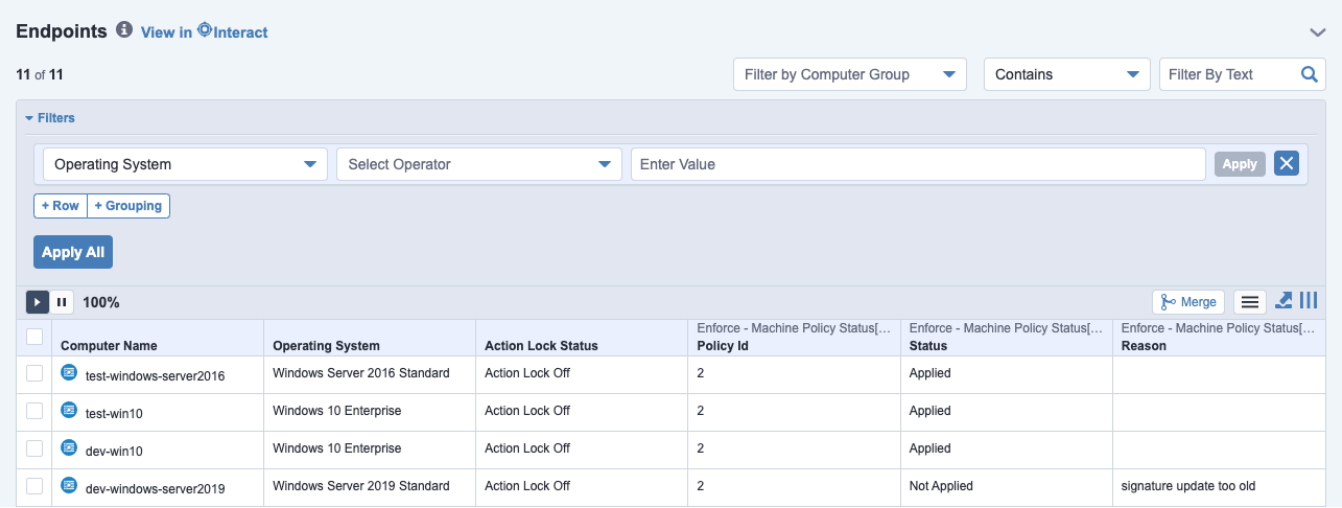


Filter results

In the **Endpoints** section on the enforcement details page, you can filter results by items such as computer name, operating system, operators (**contains** or **does not contain**), and plain text. You can also add additional rows and groupings to the filter.

Figure 5. Endpoints section of the Enforcement Details page

©2026 Tanium Inc. All Rights Reserved



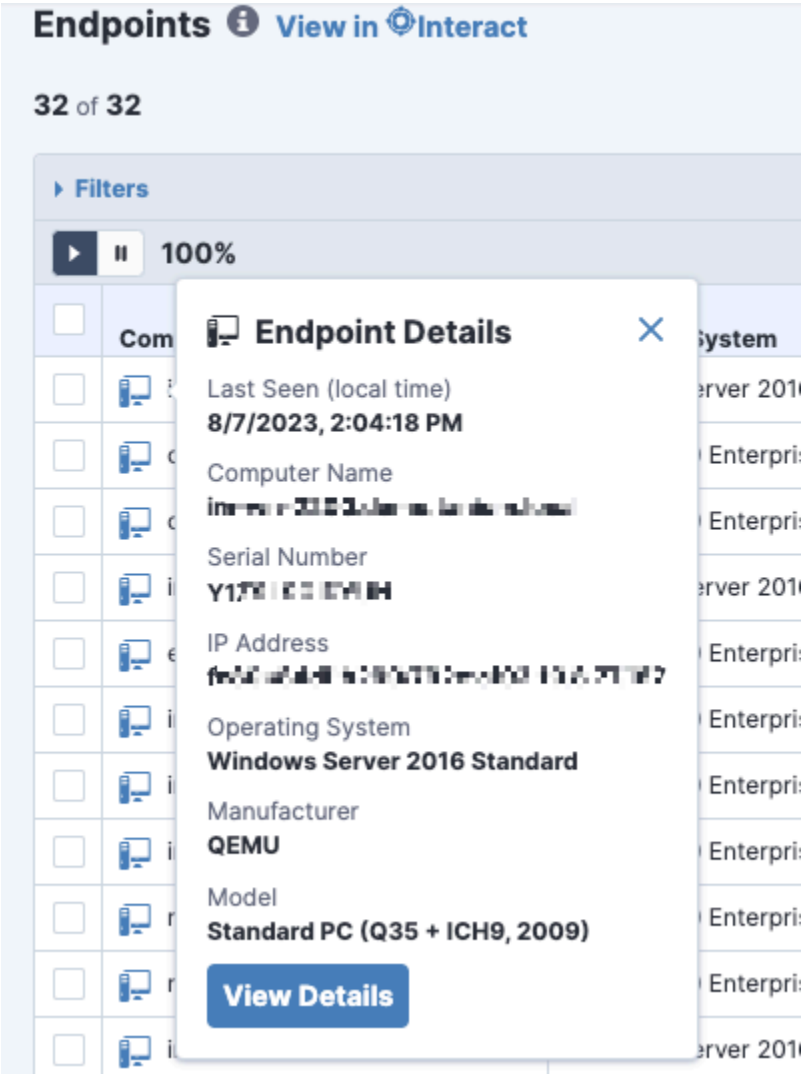
For more information about filtering and merging question results, see the Tanium Interact User Guide: Managing question results.

View endpoint details

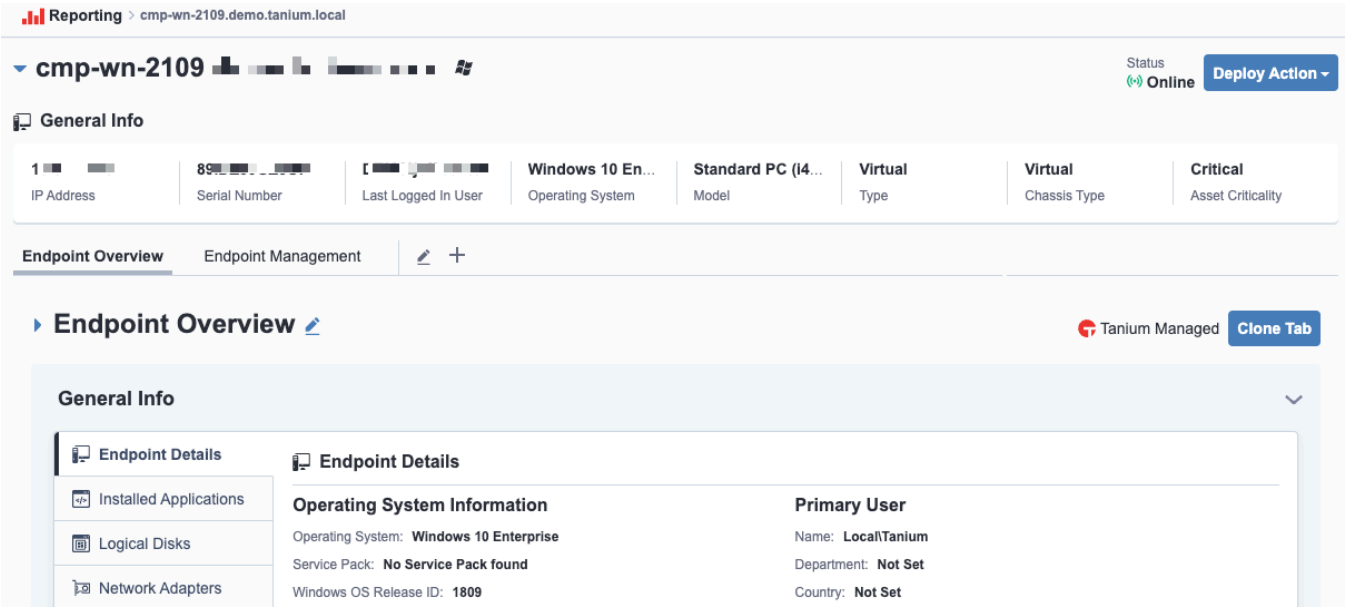
You can use Enforce with Reporting to view enhanced endpoint details in enforcements. In the **Endpoints** section on the enforcement details page, click Endpoint Details .

Figure 6. Endpoint Details slideout

©2026 Tanium Inc. All Rights Reserved



Click **View Details** to open the endpoint details in Reporting. For more information, see Reporting User Guide: View endpoint details.



©2026 Tanium Inc. All Rights Reserved

Remove an enforcement

From the list of enforcements, select one or more enforcements and click Delete. You can also click an individual enforcement and then click Delete.

Note: When you remove an enforcement for a Security Settings policy, the settings from the policy remain on the endpoint. When this scenario occurs, the following warning-level message (0) is logged in the endpoint's extensions log: `Unenforced Security Policy - settings remain on endpoint`.

For more information about this behavior, see the section "Persistence in security settings" in Microsoft documentation: Applying security settings.

©2026 Tanium Inc. All Rights Reserved

Managing device actions

About this task

Use the **Device Actions** page to manage remediation policies and enforcements.

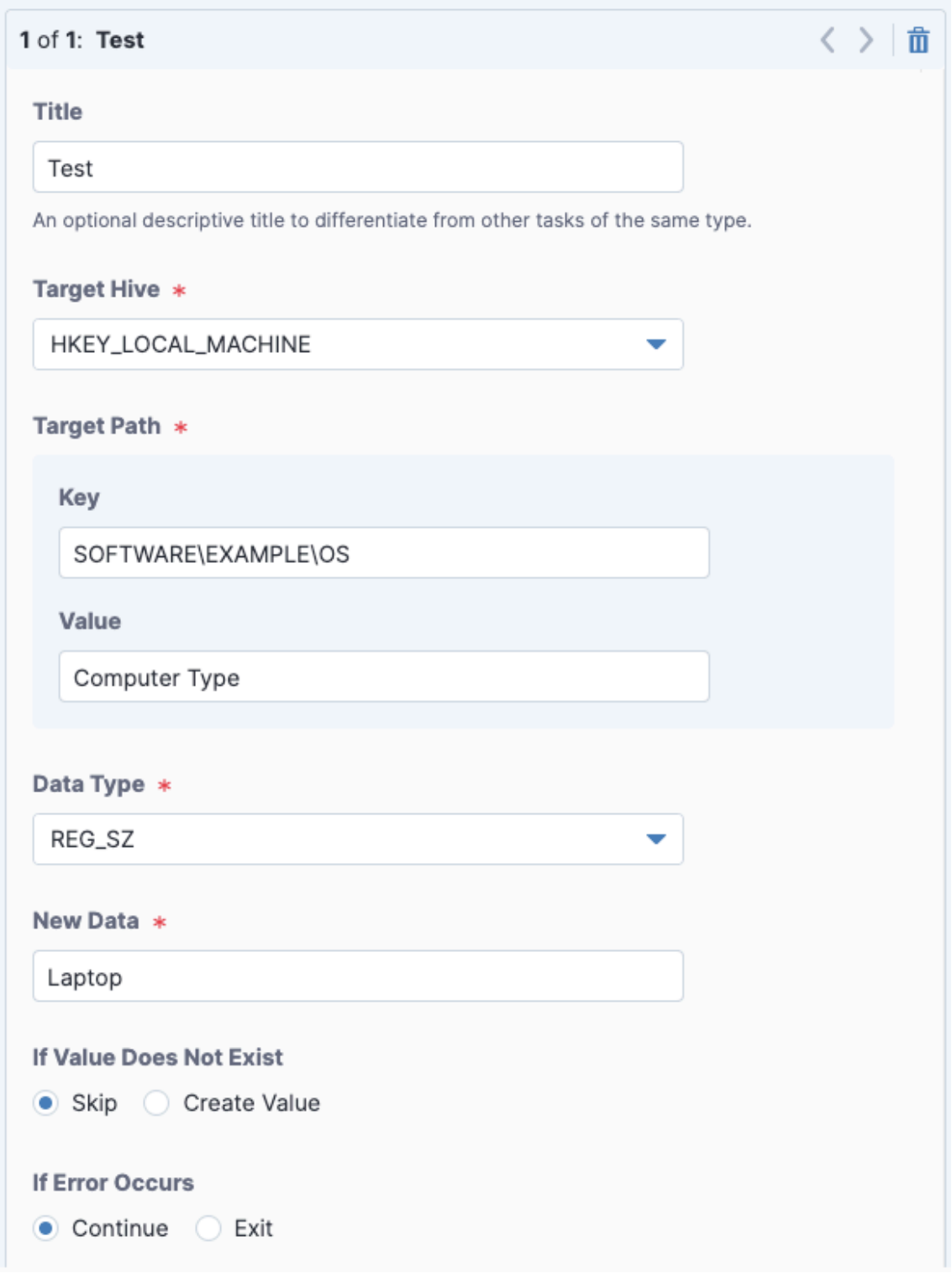
Create a remediation policy

1. From the Main menu, go to **Modules** > **Enforce** > **Device Actions** > **Create**.
2. Click **Select Types**.
3. Select the **Platform** of the endpoints on which you want to perform the tasks and click **Confirm**.
4. In the **Summary** section, provide the identifying details for the policy.
    a. Enter a **Name** and optional **Description** for the policy.
    b. If you do not want to use the default content set for the policy, select a **Content Set**. Every policy requires a content set. The content set is configured by default to the platform for the selected policy types, provided that you have the necessary permissions for that content set. If no content set is available, you might need additional permissions. For more information, see Tanium Console User Guide: Role permissions for content sets.
5. In the **Remediation** section, select the tasks that you want to run on the targeted endpoints from the **Add Task** dropdown list. Optionally, specify the **Title** for the task to identify it in the list of tasks in the policy.
   You can add the following tasks to a Windows remediation:

    - **Delete File**: deletes a single file or multiple files matching a pattern. For more information, see Remediation policy file pattern matching examples on page 178.
    - **Delete Registry Key**: deletes a registry key if it exists.
    - **Edit Registry Data**: modifies an existing registry value if it exists; optionally, the value can be created if it does not exist.

©2026 Tanium Inc. All Rights Reserved

For the **Target Path**, do not include the hive and do not use a leading slash (\).



- **Kill Process**: kills all processes that match the specified **Process Type** options: name, path, or hash. You can also optionally enter **Command Line Args** to use a regular expression to match against process command line arguments for any of the **Process Type** options.

©2026 Tanium Inc. All Rights Reserved

- **Run Service Action**: changes the running state of the specified service.

  > **Important:** For the **Service Name** field, enter the Service Name, not the Service Display Name.

- **Run Service Configuration**: changes the `startup config` of the specified service.

  > **Important:** For the **Service Name** field, enter the Service Name, not the Service Display Name.

- **Update Registry Value**: changes the name of a registry value if it exists or deletes the value if the `delete` option is selected.

  > **Note:** For tasks that modify the registry and target the `HKEY_USERS` hive, if you use the wildcard character (`*`) to target all users, users that are signed out when the policy is enforced are skipped.

You can add the following tasks to a Mac or Linux remediation:

- **Delete File**: deletes a single file or multiple files matching a pattern.
- **Kill Process**: kills all processes that match the specified Process Type options: name, path, or hash. You can also optionally enter Command Line Args to use a regular expression to match against process command line arguments for any of the Process Type options.
- **Run Service Action**: changes the running state of the specified service.

  > **Important:** For the Service Name field, enter the Service Name, not the Service Display Name.

6. Complete the required fields for the task.
7. Add other tasks as needed for the policy. When you are finished adding all tasks, click **Create**.

Remediation policy file pattern matching examples

©2026 Tanium Inc. All Rights Reserved

Note: Recursive matching is not supported. Each directory level must be specified.

Definition	Example
Match a file by name in an unknown directory path.	Actual Path: c:\a\b\c\file.exe Wildcard: c:***\file.exe
Match any file in a known directory path.	Actual Path: c:\a\b\c\file.exe Wildcard: c:\a\b\c*
Match a specific file type in a partially known directory path.	Actual Path: c:\a\b\c\file.exe Wildcard: c:\a*\c*.exe
Disable case sensitivity for the first character in a file name.	Actual Path: c:\a\b\c\File.exe Wildcard: c:\a\b\c\[Ff]ile.exe
Match a single character in a file name.	Actual Path: c:\a\b\c\cat.exe Actual Path: c:\a\b\c\bat.exe Wildcard: c:\a\b\c\?at.exe
Do not match a character in a file name.	Actual Path: c:\a\b\c\cat.exe Wildcard: c:\a\b\c\[!c]at.exe

Managing remediation policies

View remediation policies

About this task

The **Remediations** tab on the **Device Actions** page shows all remediation policies in your environment, both enforced and unenforced.

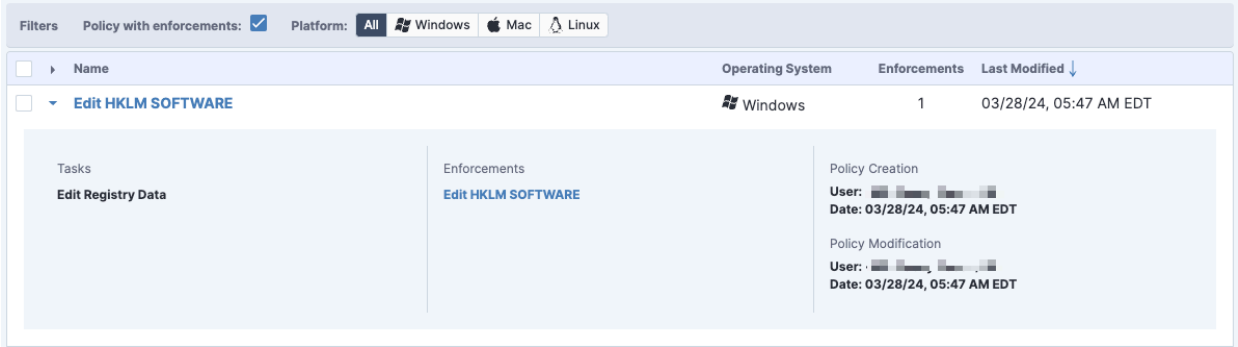
1. From the Main menu, go to **Modules** > **Enforce** > **Device Actions** > **Remediations**.
2. (Optional) Enter a string in the **Filter Items** field to filter the results using the specified string.
3. (Optional) To show only enforced remediation policies, select **Policy with enforcements**.

©2026 Tanium Inc. All Rights Reserved

4. (Optional) To filter the results by operating system, select an operating system in the **Platform** section.



5. (Optional) Click Expand to see the high-level details for the policy.



Edit remediation policies

About this task

If needed, you can edit remediation policies.

Note: Tasks in remediation policies with an enforcement are read-only and cannot be edited.

1. From the Main menu, go to **Modules** > **Enforce** > **Device Actions** > **Remediations**.
2. Select a policy and click Edit.
3. Make the necessary changes and click **Save**.

Delete remediation policies

About this task

If needed, you can delete remediation policies.

Note: You cannot delete remediation policies with an enforcement.

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Enforce** > **Device Actions** > **Remediations**.
2. Select a policy and click Delete .

Duplicate remediation policies

About this task

You can duplicate remediation policies to use as a starting point for a new policy.

1. From the Main menu, go to **Modules** > **Enforce** > **Device Actions** > **Remediations**.
2. Select a policy and click More Actions and then click **Duplicate**.
3. Edit the duplicate policy, if needed, and click **Create**.

Export remediation policies

About this task

You can export remediation policies for use in another Enforce environment.

Note: You can export remediation policies with an enforcement, but the enforcement is not exported with the policy.

1. From the Main menu, go to **Modules** > **Enforce** > **Device Actions** > **Remediations**.
2. Select a policy and click More Actions and then click **Export**.

Result

A JSON file for the policy downloads to your local downloads folder.

Import remediation policies

About this task

You can import remediation policies that were exported from another Enforce environment.

1. From the Main menu, go to **Modules** > **Enforce** > **Device Actions** > **Remediations**.

©2026 Tanium Inc. All Rights Reserved

2. Click **Import**.
3. Browse to the JSON file for the policy that you want to import. Click **Open**.
4. Click **Import**.
5. Edit the imported policy, if needed, and click **Save**.

Viewing remediation policy details, results, and enforcements

About this task

Select a remediation policy to view detailed information, such as policy details, results, and enforcements.

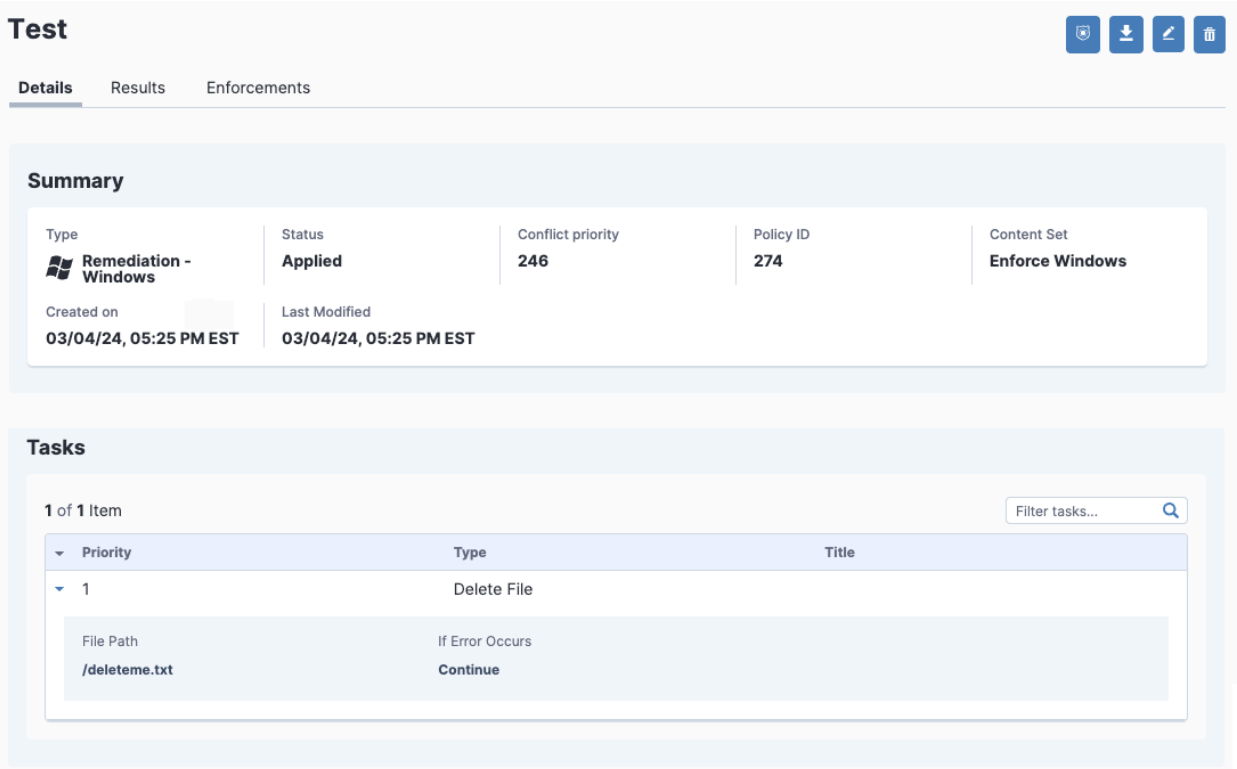
From the Main menu, go to **Modules** > **Enforce** > **Device Actions** > **Remediations**. Click the name of a policy and review the information for the policy:

Details

The **Details** tab includes two sections:

- **Summary:** Shows the details for the policy.
- **Tasks:** Shows the tasks for the policy, including the priority, type, and title (if specified during policy creation). Click Expand next to a task to see additional details about that task.

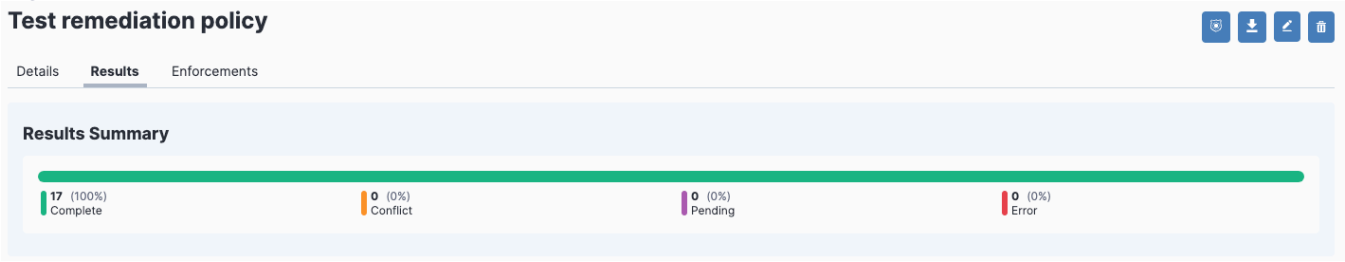
©2026 Tanium Inc. All Rights Reserved



Results

The **Results** tab includes a **Results Summary** graph that shows a summary of the status of the tasks for endpoints targeted by an enforcement of the policy, if applicable.

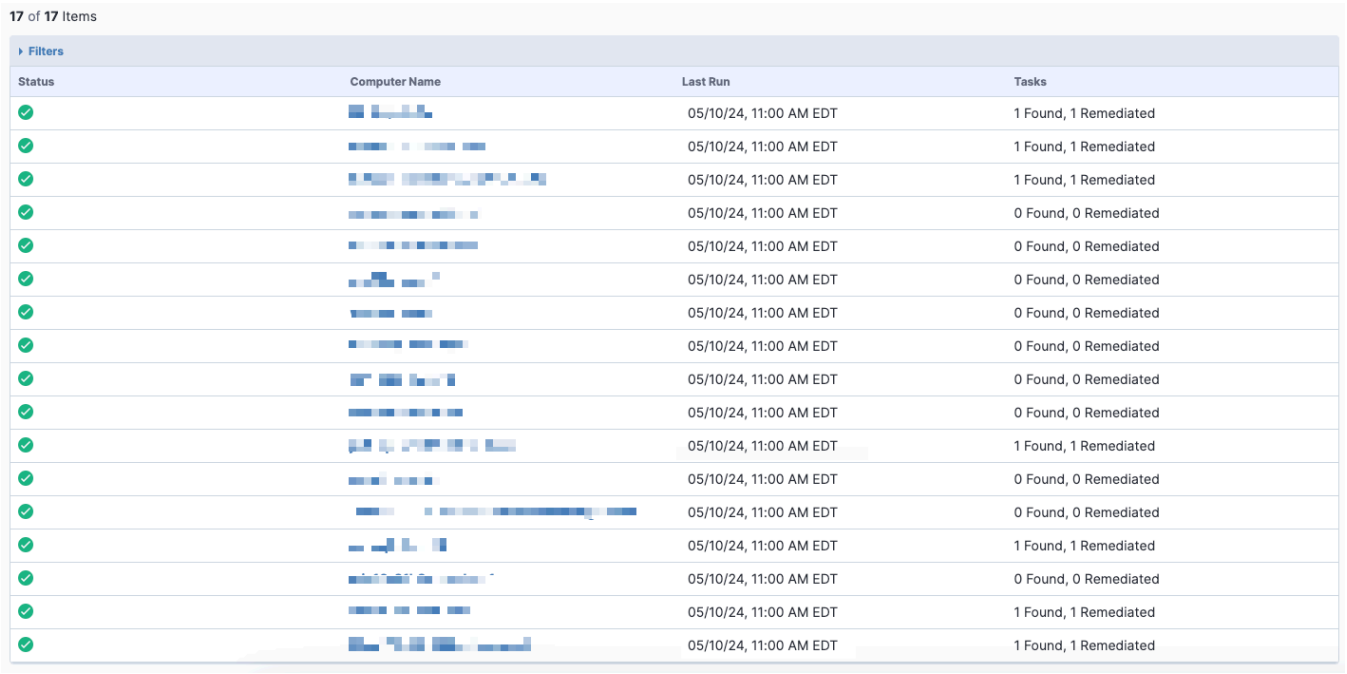
Figure 7. Results Summary



The results grid shows the status of the tasks for each endpoint targeted by an enforcement for the policy.

Figure 8. Results Grid

©2026 Tanium Inc. All Rights Reserved



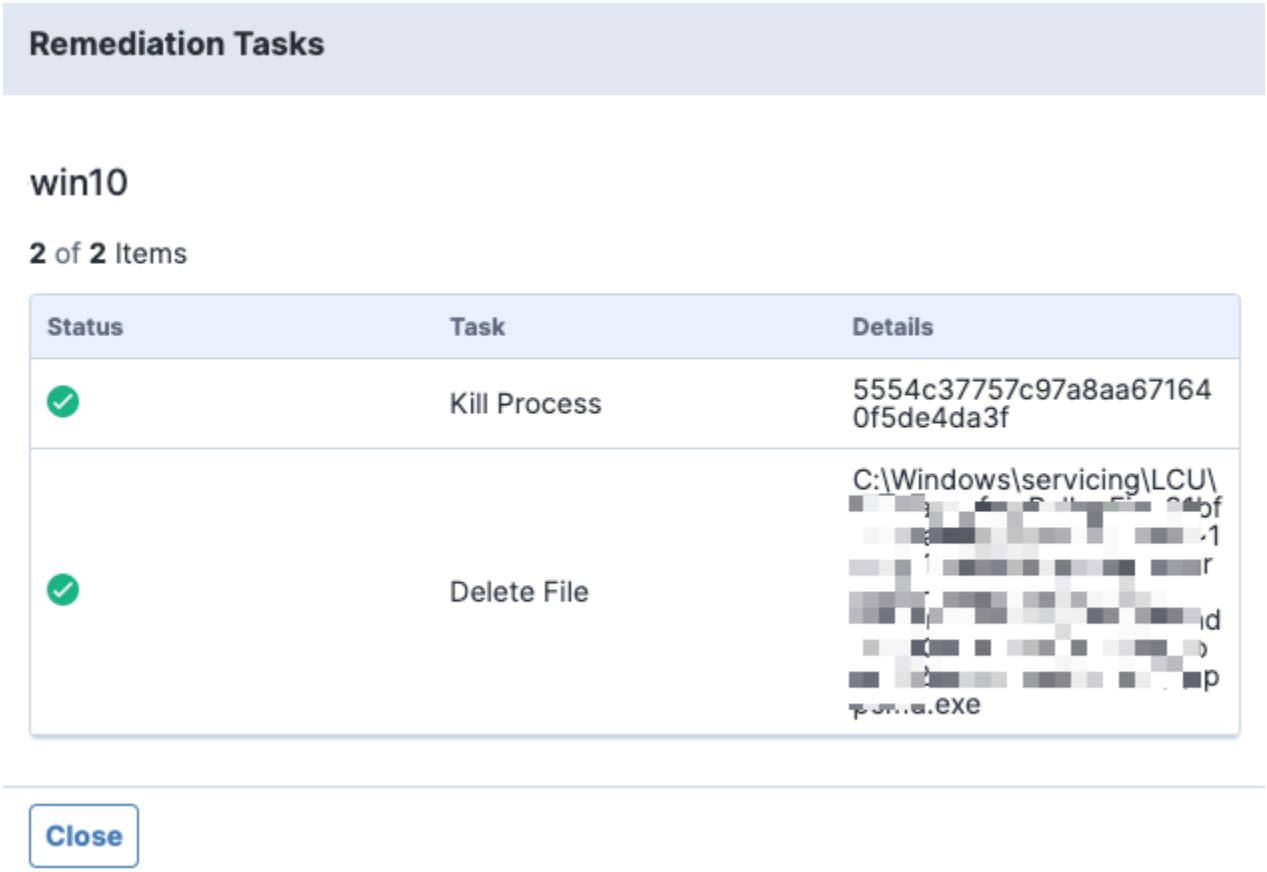
Status of the tasks on the endpoint

Status	Description
Complete	Action to run the tasks on the endpoint is complete.
Conflict	Not applicable for remediation policies.
Pending	Action to run the tasks is deployed on the endpoint, but work is not started.
Error	Action to run the tasks on the endpoint failed to complete.

Click the computer name for an endpoint to see the status for each task on that endpoint.

Figure 9. Remediation task status

©2026 Tanium Inc. All Rights Reserved



Tip:

If a task fails on an endpoint, check the action history status for additional details. From the Main menu, go to **Administration** > **Actions** > **Action History**. The action name associated with a remediation policy is typically **Enforce - Enforcement: <policy name> on <enforcement name>**. Select the row for the action associated with the policy/enforcement and click **Show Status**. Click **Show Client Status Details** to see the action status for each targeted endpoint. For more information about working with action statuses, see Tanium Console User Guide: View action status.

You can also get additional details about the status by asking a question using the `Enforce - Remediation Results` sensor.

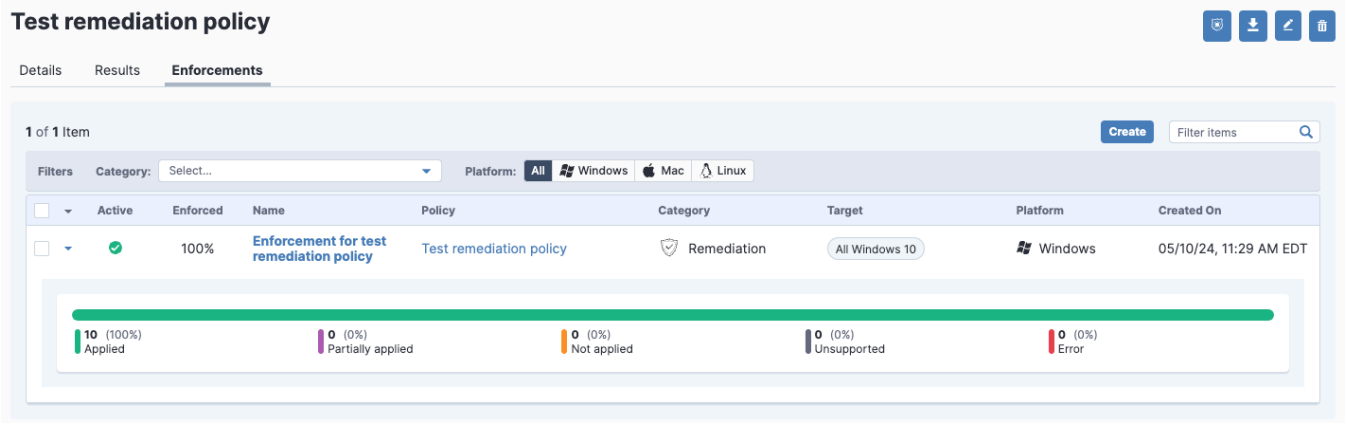
Enforcements

The **Enforcements** tab shows the status for enforcements for the selected policy. Click Expand ▶ to

©2026 Tanium Inc. All Rights Reserved

see a summary of the status for an enforcement.

Figure 10. Enforcements



For more information about enforcement statuses, see Enforcements on page 17.

Click **Create** or Enforce to create a new enforcement for the policy. To create an enforcement from the **Remediations** tab, select a policy and click More Actions and then click **Enforce**. For more information about creating enforcements, see Enforcing policies on page 163.

©2026 Tanium Inc. All Rights Reserved

Restricting policy visibility

Create policies for specific content sets so that you can segment policy visibility between functional roles or groups.

Note: You can also use a custom role to limit users to a specific policy type. For more information, see Create custom roles to only allow access to policies associated with a specific content set on page 63.

Overview

To restrict policy visibility by groups, you can create a content set and an RBAC role for your functional group. This example uses a content set named **West** and an RBAC role named **West Policy Users**.

Create a content set for a functional group

1. From the Main menu, go to **Administration** > **Permissions** > **Content Sets** and then click **New Content Set**.
2. For this example, enter `West` for the content set name, an optional description and then click **Save**.
   For more information about content sets, see Tanium Console User Guide: Managing content sets.

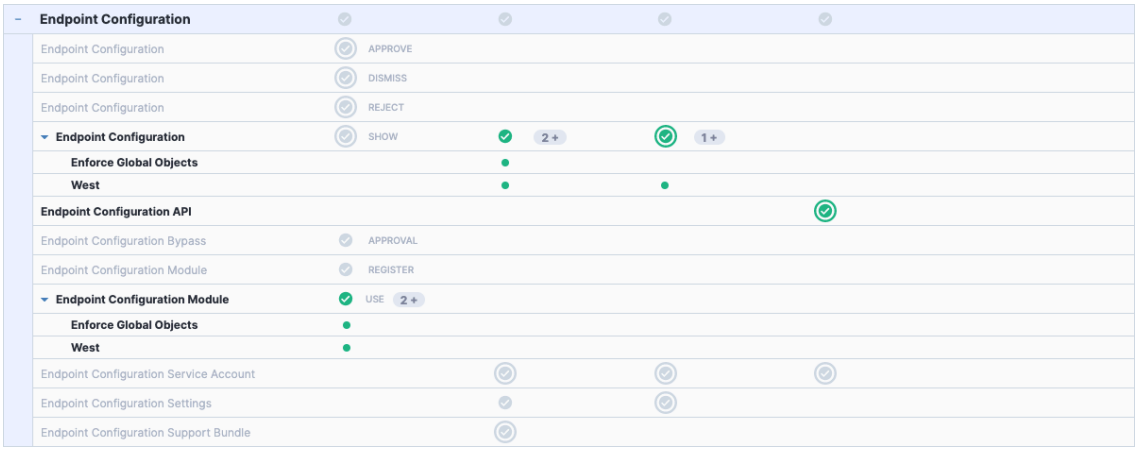
Create a role to assign to a user or user group

1. From the Main menu, go to **Administration** > **Permissions** > **Roles** > **New Role**.
2. In the **Role Details** section, enter `West Policy Users` for the role name for this example and an optional description.
3. In the **Permissions** section, grant the following permissions and add required content sets

©2026 Tanium Inc. All Rights Reserved

for this example.

a. Expand **Endpoint Configuration** to grant the following permissions:

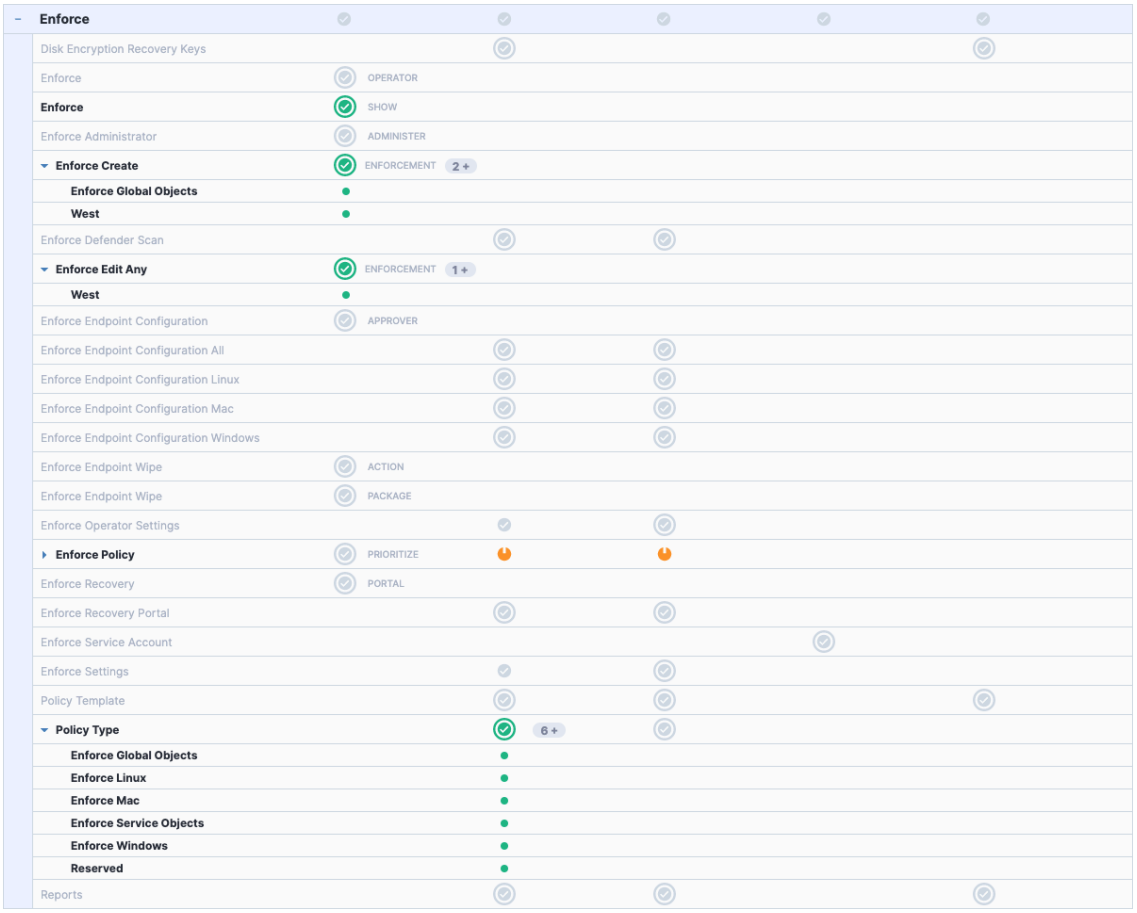


Tanium Endpoint Configuration permissions and content sets for this example

Permission	Access	Content Sets
Endpoint Configuration	READ	Enforce Global Objects West
	WRITE	West
Endpoint Configuration API	EXECUTE	
Endpoint Configuration Module	USE	Enforce Global Objects West

b. Expand **Enforce** to grant the following permissions:

©2026 Tanium Inc. All Rights Reserved



Enforce permissions and content sets for this example

Permission	Access	Content Sets
Enforce	SHOW	
Enforce Create	ENFORCEMENT	Enforce Global Objects West
Enforce Edit Any	ENFORCEMENT	West
Policy Type	READ	Enforce Global Objects Enforce Linux Enforce Mac Enforce Service Objects Enforce Windows Reserved

4. Click **Save**.

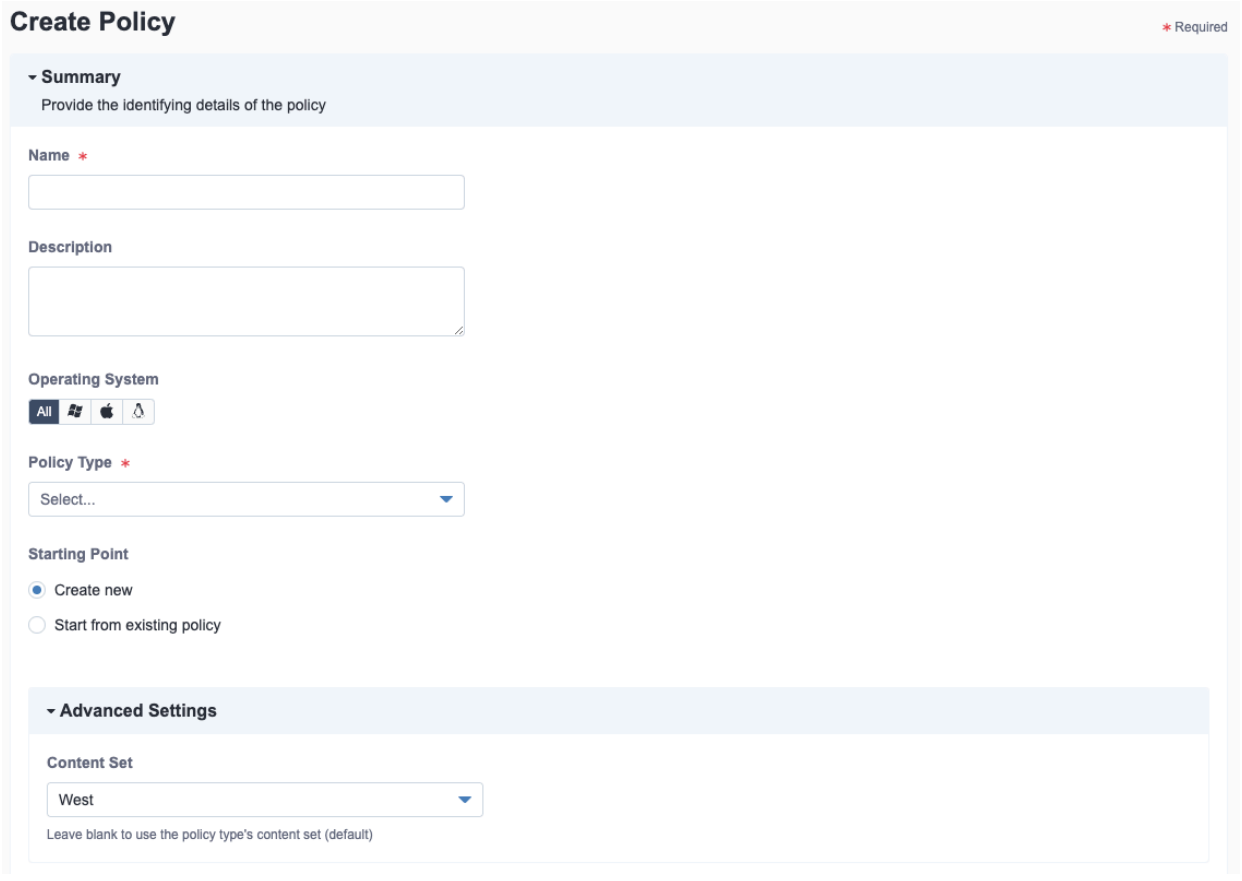
©2026 Tanium Inc. All Rights Reserved

5. To test this example, assign the **West Policy Users** RBAC role to the user or user group of your choice.
    a. From the Main menu, go to **Administration** > **Permissions** > **Users** or **Administration** > **Permissions** > **User Groups** and then click on the name of the user or user group.
    b. Click **Edit Mode**.
    c. In the **Roles** section, click **Manage Roles**, select **West Policy Users** and then click **Apply**.
    d. Click **Save**.

    For more information about RBAC roles, see Tanium Console User Guide: Managing roles.

Create a policy

1. To create a policy using this example, sign in to Tanium Console as the user with the **West Policy Users** RBAC role.
2. From the Main menu, go to **Modules** > **Enforce**.
3. Follow the steps in Creating policies for Windows endpoints on page 96 to create a policy and select the **West** content set in the **Content Set** section.



©2026 Tanium Inc. All Rights Reserved

Using best practices with policies

Content sets

Important: For content that is provided through Tanium solutions, keep the content objects in their original Tanium-provided content sets. To sustain this practice when moving content between content sets, create copies of Tanium-provided content and move the copies instead of the original versions. Contact Tanium Support before proceeding if you need to move original Tanium-provided content. For more information, see Contact Tanium Support on page 222.

For more information, see Console User Guide: Content Sets.

Anti-malware policies

For anti-malware policies to be enforced correctly, you must enable Managed Definitions to deploy Microsoft anti-malware definitions through Tanium.

AppLocker policies workflow

For more information about creating AppLocker rules, see Microsoft Technet: AppLocker.

By default, block list rules allow all executables to run. Allow list rules allow only administrators to run applications unless otherwise specified.

Deploy a policy in audit mode with reporting enabled in your test environment before deploying the policy in your production environment. Review any warning events in the reports and modify the policy as needed.

Follow this example workflow to better understand how the default Enforce **Allow List Rule Template** works.

Example workflow using default Allow List Rule Template

©2026 Tanium Inc. All Rights Reserved

This workflow can help you confirm you are achieving the results you want with your allow list policy.

1. Enforce the default **Allow List Rules Template** in **Audit Only** mode on a representative computer group.

2. Create the **AppLocker Warnings** report to run for the appropriate number of days. You must enforce the policy for approximately 7 to 30 days to collect an accurate representation of user activity on the endpoint.

3. Based on the aggregated data of blocked applications in the **AppLocker Warnings** report, click the Interact icon next to the application to go to Interact to view detailed event information about that specific application.

4. Select the **AUDIT** rows in the resulting **Question Results** and click **Drill Down**.

5. On the **Create Question** tab of the **Select Drilldown Question** window, begin typing `applocker threat details` and click on the resulting query **Get AppLocker Threat Details Last X Days** from all machines.

6. In the **Number of days to display** results for field, enter the same number of days for which you created the report (in this example, `7`) and click **Go**.

7. The **Question Results** page shows the paths for the application. To allow the application to run, edit the policy and add the path in the **Allow** section of the policy.

8. Click **Enforce Changes** and **Confirm Save of Enforced Policy**.

Firewall rules

With Enforce, do not manage Windows Firewall with Group Policy Management Editor. For firewall policies created in Enforce to take effect, the Group Policy Firewall setting must be set to **Not configured**.

SRP management rules

Windows SRP is capable of blocking applications started by the user. Windows SRP does not prevent Windows services from starting. SRP does not prevent SYSTEM privileges from starting applications. For more information, see Microsoft TechNet Software Restriction Policies.

©2026 Tanium Inc. All Rights Reserved

Role-based access control and configuration visibility

When policies are put in content sets by different users with different permissions, a user might have partial visibility into configuration items or lose visibility into items which that user originally had access. For example, if you create a policy and apply it to a group of endpoints, then another user applies that same policy to a different group of endpoints for which you do not have permissions, you lose the permission to edit that policy. For more information about role definitions, see User role requirements on page 44.

Note: If you move a policy from one content set to another content set, it can take up to an hour for all configuration changes to take place. The policy is updated immediately, but packages and saved content can take up to an hour to align because they require a sync activity to take place.

©2026 Tanium Inc. All Rights Reserved

Scanning for anti-malware on-demand

Configure scans

About this task

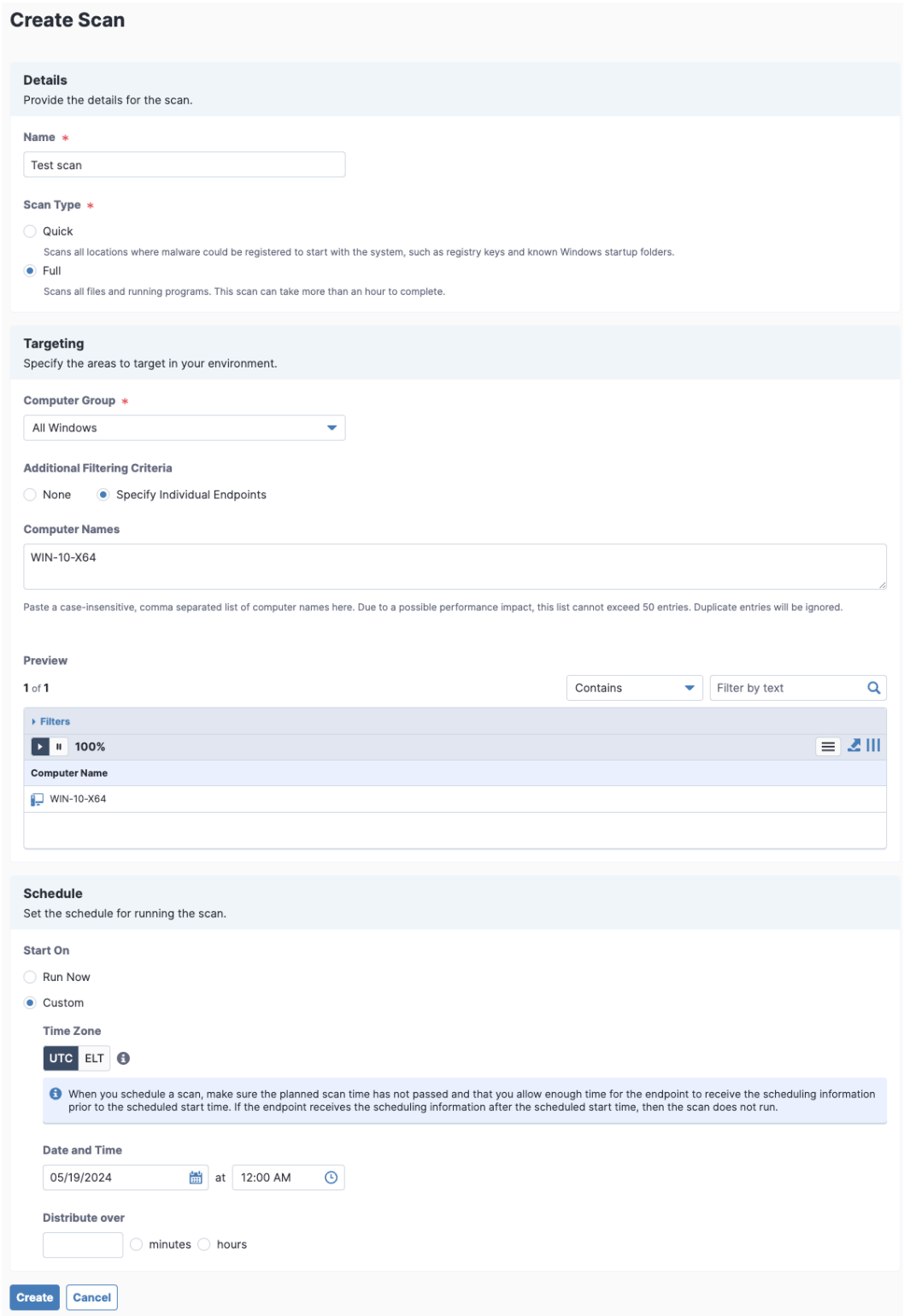
Configure anti-malware scans to run by Defender on targeted computer groups immediately or on a set schedule that you define.

For information about different scan types, see Microsoft: Defender Scans.

1. From the Main menu, go to **Modules** > **Enforce** > **Anti-Malware** > **Scans** > **Create Scan**.
2. In the **Details** section, enter a name for the scan and select one of the following scan types:
   - Select **Quick** scan to search for malware in Windows system startup locations such as registry keys and certain file folders.
   - Select **Full** scan for a more thorough scanning of systems that might be compromised. This scan type can take over an hour to complete.
3. In the **Targeting** section, select the endpoints to scan:
   - Select a **Computer Group**.
   - (Optional) If you want to specify individual endpoints within the selected computer group, select **Specify Individual Endpoints** and provide the list of endpoints in the **Computer Names** field.

   A preview appears with the targeted endpoints.
4. In the **Schedule** section, select when to run the scan:
   - To run the scan immediately, select **Run Now**.
   - To configure when you want the scan to start, select **Custom** and specify the date and time to run the scan. Optionally, select to distribute the scan over a set number of minutes or hours.

©2026 Tanium Inc. All Rights Reserved



Note: When you schedule a scan, make sure the scheduled start time has not passed and that you allow enough time for the endpoint to receive the scheduling information. If the endpoint receives the scheduling information after the scheduled start time, then the scan does not run.

©2026 Tanium Inc. All Rights Reserved

5. Click **Create**.

View scan details

Required access rights

To view scans, you must have one of the following access rights:

- The **Unrestricted Management Rights** permission.
- Access to the computer groups targeted by the scan.

> **Note:** You must have access to the exact computer group targeted by the scan to view the scan. Access to another computer group that includes the endpoints from the targeted computer group does not provide viewing access. For example, if you have access to the **All Windows** computer group, but not the **All Windows 10** computer group, you cannot view scans that target only the **All Windows 10** computer group.

View the scan details

From the Main menu, go to **Modules** > **Enforce** > **Anti-Malware** > **Scans**. Click the scan name. Scans have one of the following statuses:

- **Pending:** The scan action has not begun yet. Scans scheduled for a future date and time remain in **Pending** until the scheduled start time.
- **Running:** The scan action is in progress and has not expired.
- **Completed:** The scan action has completed or expired. Note that the status can be **Completed** even if the scan is still running on endpoints. The **Completed** status indicates the action is no longer being issued to new endpoints.
- **Errors:** Errors occurred during the scan action.
- **Deleted:** The saved scan configuration has expired and been automatically deleted or ended by the administrator.

You can also view the status of a scan from the **Actions** page in Tanium Console. Scans work similar

©2026 Tanium Inc. All Rights Reserved

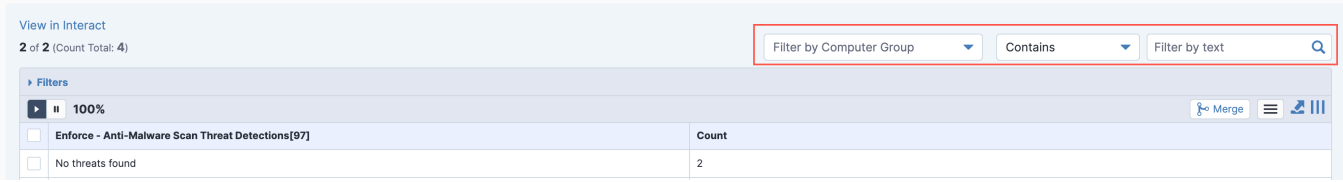
to other Tanium scheduled actions. For more information, see Tanium Console User Guide: Actions Overview.

Note: The **Scan Results** section is not updated immediately and might have a delay of up to 20 minutes before it shows that a scan completed on an endpoint.

Filtering

Filter scan results using the dropdown categories.

Figure 11. Filter options for scan results



The Tanium Server combines the filters with Booleans AND/OR. For example, if you select a computer group filter and also configure a results filter, the server combines the logic of both filters.

View scan results

Required access rights

To view scans, you must have one of the following access rights:

- The **Unrestricted Management Rights** permission.
- Access to the computer groups targeted by the scan.

  Note: You must have access to the exact computer group targeted by the scan to view the scan. Access to another computer group that includes the endpoints from the targeted computer group does not provide viewing access. For example, if you have access to the **All Windows** computer group, but not the **All Windows 10** computer group, you cannot view scans that target only the **All Windows 10** computer group.

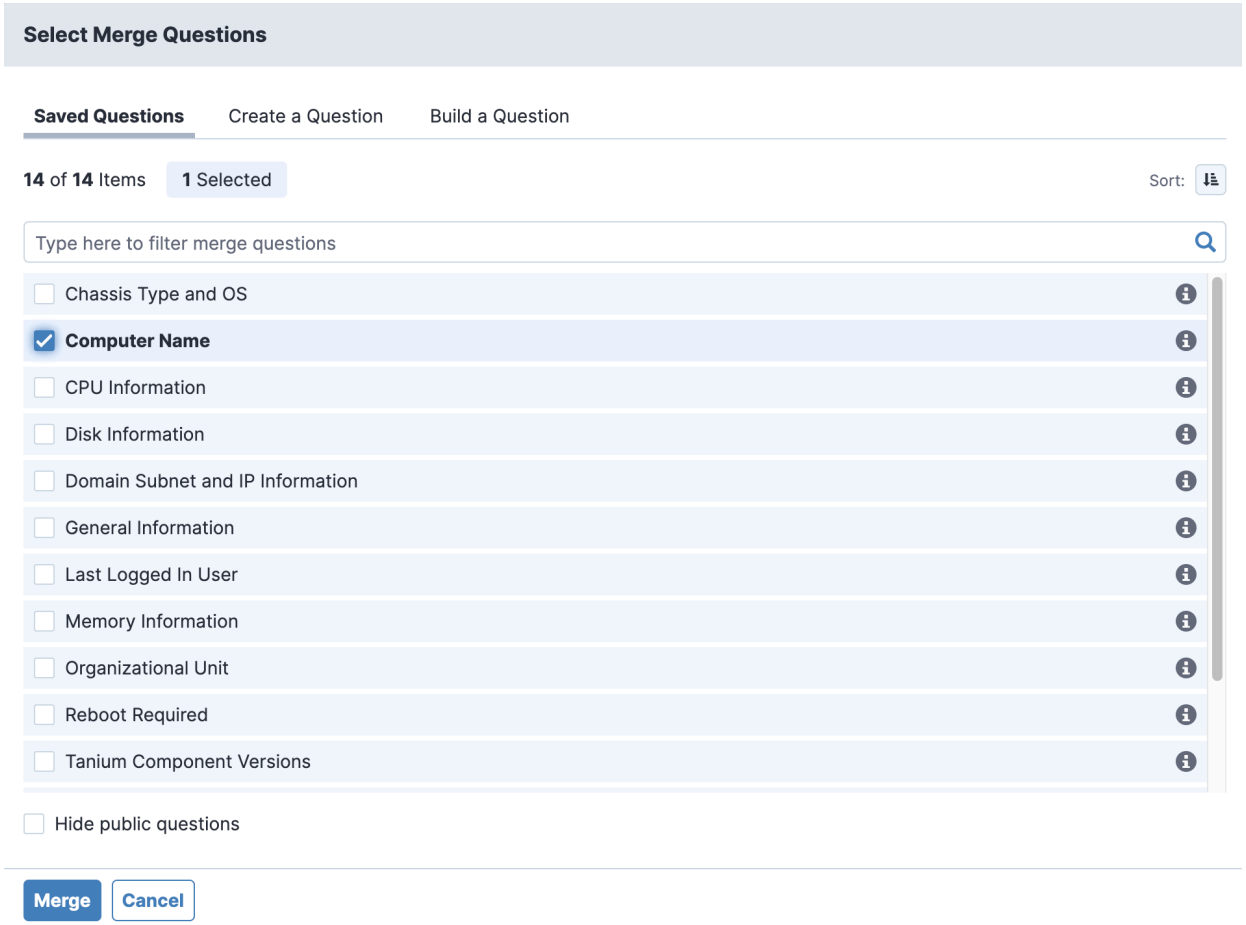
©2026 Tanium Inc. All Rights Reserved

Merge

About this task

You can use the merge function to combine questions to further investigate scan results. View the scan details to review all threats found on endpoints.

1. From the Main menu, go to **Modules** > **Enforce** > **Anti-Malware** > **Scans**.
2. Click the scan name.
3. Click **Merge**.
4. In the **Select Merge Questions** window, combine multiple questions, create new questions, or build advanced questions and apply them to scan results.
   For more information about filtering and merging question results, see Tanium Interact User Guide: Merge questions.



Drill down

©2026 Tanium Inc. All Rights Reserved

About this task

Click the scan name to view all threats detected on endpoints. If threats were found, they are listed in the results section. You can use the drill down feature to investigate further.

1. From the Main menu, go to **Modules** > **Enforce** > **Anti-Malware** > **Scans**.
2. Click the scan name.
3. In the **Details** section, select the result that you want to explore and click **Drill Down**.
4. In the **Select Drill-down Question** window, apply a question to the scan results. For example, if you select **Computer Name**, this drill-down question shows a list of computer names where the threat was detected. For more information about drill-down questions, see Tanium Interact User Guide: Drill down.

TAKE ACTION ON A THREAT

About this task

From the drill-down question results, you can click **Deploy Action** to take an action on a threat. For more information about deploying actions, see Tanium Interact User Guide: Deploying actions in Interact.

You can also use a remediation policy to configure a set of tasks that run sequentially on endpoints to remediate a threat. For more information, see Create a remediation policy on page 176.

Copy results

About this task

You can copy results to the clipboard in text format.

1. From the Main menu, go to **Modules** > **Enforce** > **Anti-Malware** > **Scans**.
2. Click the scan name.
3. In the results grid in the **Details** section, select one or more results and click **Copy**.

Export results

About this task

©2026 Tanium Inc. All Rights Reserved

You can export results to a CSV file.

1. From the Main menu, go to **Modules** > **Enforce** > **Anti-Malware** > **Scans**.
2. Click the scan name.
3. In the results grid in the **Details** section, select one or more results and click **Export**.
4. Specify a file name.
5. (Optional) Select **Include headers in export** to include the column headings in the exported content.
6. Click **Export**.

Manage quarantined files

About this task

You can view a list of threats that are detected on endpoints and then view and manage the endpoints and files that are affected by each threat. Each item in the list has one of the following statuses:

- **Quarantined:** The file was quarantined by Defender.
- **Error:** There was a problem restoring the file from quarantine.

Important: In some cases, when an error occurs, Tanium might not be able to restore a file from quarantine. When this scenario occurs, you must manually correct the issue on the endpoint.

You can schedule Defender to automatically remove files from quarantine. Create a Machine Administrative policy and configure this setting: **Windows Components** > **Microsoft Defender Antivirus** > **Configure removal of items from Quarantine folder**. For more information, see Machine administrative template on page 117.

View threats detected on endpoints

About this task

View a list of threats detected on endpoints to see the severity of each threat and the number of

©2026 Tanium Inc. All Rights Reserved

endpoints affected by the threat.

Note: Because different endpoint scan methods can sometimes classify threats with different severity levels, some threats can be displayed multiple times.

1. From the Main menu, go to **Modules** > **Enforce** > **Anti-Malware** > **Management**.
2. (Optional) To filter the list by severity, select a severity from the **Filters** list.
3. From the list of threats, click a threat to view the affected endpoints and their statuses.

Restore all files quarantined at the same time for the same threat

About this task

When you select a file to restore, that file and all other files that were quarantined at the same time for the same threat are restored from quarantine. The version of Windows Defender on the endpoint must support selecting specific files to restore. Otherwise, you can select to restore all quarantined files on the endpoint, or just the most recent file or group of files to be quarantined.

Note:

- Restoring a file from quarantine might take a few minutes. If multiple copies of the same file are quarantined, only the latest version of the file is restored.
- You cannot individually restore files from quarantine that have Unicode characters in the file name. To restore files that have Unicode characters in the file name, you must select **Restore All Items from Quarantine**.

1. From the Main menu, go to **Modules** > **Enforce** > **Anti-Malware** > **Management**.
2. (Optional) To filter the list by severity, select a severity from the **Filters** list.
3. From the list of threats, click a threat to view the affected endpoints.
4. From the list of endpoints with quarantined files, click Additional data in the row for the endpoint that contains the files you want to restore from quarantine.

©2026 Tanium Inc. All Rights Reserved

5. Select the files you want to restore from quarantine.
    - If the version of Defender on the endpoint supports selecting specific files to restore, select the file you want to restore and click **Restore from Quarantine**. Remember that this operation restores all files quarantined at the same time as the file you selected.

    - If the version of Defender on the endpoint does not support selecting specific files, checkboxes do not appear next to individual files on the Additional data page. To restore all quarantined files on the endpoint, click **Restore from this Endpoint** and select **All Quarantined Items** . To restore only the last file or group of files to be quarantined on that endpoint, select **Most Recent Quarantined Items**.

    Important: **Most Recent Quarantined Items** restores the last group of files quarantined for a specific threat on an endpoint. Before restoring files, the endpoint checks if additional files have been quarantined more recently for the same threat. If additional affected files are found, then no files are restored. Review the list of affected files before you attempt the restore operation again.

Restore all quarantined files on a single endpoint

About this task

Select an endpoint and then quickly restore all files from quarantine. You might do this, for example, when all files on an endpoint are quarantined in error because of a false positive result during a scan.

CAUTION: Before proceeding, be certain you want to restore ALL files from quarantine on the selected endpoints. This operation cannot be undone.

1. From the Main menu, go to **Modules** > **Enforce** > **Anti-Malware** > **Management**.
2. From the list of threats, click a threat to view the affected endpoints.
3. From the list of endpoints with quarantined files, select the row for the endpoint on which you want to restore files and click **Restore All Items from Quarantine**.

    Note: Restoring a file from quarantine can take a few minutes.

©2026 Tanium Inc. All Rights Reserved

Restore all quarantined files on all endpoints

About this task

> **CAUTION:** Before proceeding, be certain you want to restore all files from quarantine on ALL endpoints. This operation cannot be undone.

1. From the Main menu, go to **Modules** > **Enforce** > **Anti-Malware** > **Management**.
2. From the list of threats, click a threat to view the affected endpoints.
3. Click **Restore All Quarantined Items from All Endpoints**. Restoring a file from quarantine can take a few minutes.

Check health

From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. In the **Anti-Malware Health** section of the Enforce **Overview** page, you can view the current status of anti-malware definition files, including the time the last update was downloaded.

©2026 Tanium Inc. All Rights Reserved

Maintaining Enforce

Perform monthly maintenance tasks to ensure that Enforce successfully performs scheduled activities on all the targeted endpoints and does not overuse endpoint or network resources. If Enforce is not performing as expected, you might need to troubleshoot issues or change settings. For more information about related procedures, see Troubleshooting Enforce on page 207.

Enforce monthly maintenance

1. From the Main menu, go to **Modules** > **Enforce** > **Overview**.
2. Go to the **Health** dashboard and verify whether Tanium™ Enforce tools are installed and active on all endpoints.
3. To investigate endpoints that do not have Enforce tools installed, click the number above **Not Installed**. The Tanium Server issues the following question:
   `Get?forceComputerIdFlag=1 Endpoint Configuration - Tools Status?ignoreCase=0&maxAge=600 contains Enforce from all machines`
4. For more information about troubleshooting installation issues for Enforce tools, see Tanium Enforce User Guide: Monitor and troubleshoot Enforce coverage status (% of total).

Monitor and troubleshoot Enforce coverage status (% of total)

The following table lists contributing factors into why the Enforce coverage might be lower than expected, and corrective actions you can take.

Factors that contribute to a lower-than-expected Enforce coverage status metric

Contributing Factor	Corrective Actions
Incorrect targeting criteria used in computer groups	Ensure computers that should be managed by Enforce are included in computer group creation.
Enforce action group is too narrow	Ensure computer groups that should be managed by Enforce are included in the

©2026 Tanium Inc. All Rights Reserved

Contributing Factor	Corrective Actions
	Enforce action group.

Monitor and troubleshoot policy enforcement status (% of total)

The following table lists contributing factors into why the Enforce policy enforcement coverage might be lower than expected, and corrective actions you can take.

Factors that contribute to a lower-than-expected policy enforcement status metric

Contributing Factor	Corrective Actions
Enforce tools are not deployed	Ensure computer groups that should be managed by Enforce are included in the Enforce action group.
Domain Group Policy is currently applied	Reference the output from enforcement policy status and work with Active Directory team to set conflicting policy items to “Not Defined” in the domain policy.

Monitor and troubleshoot host firewall status on endpoints

The following table lists contributing factors into why the Enforce host firewall metric might be lower than expected, and corrective actions you can take.

Factors that contribute to a lower-than-expected host firewall status metric

Contributing Factor	Corrective Actions
Host based firewall is not installed	Deploy Windows firewall policy.
Host based firewall is not enabled	Deploy the Windows firewall policy that enables the Windows firewall for all profiles (Domain, Public, and Private).

Monitor and troubleshoot disk encryption status on endpoints

©2026 Tanium Inc. All Rights Reserved

The following table lists contributing factors into why the Enforce disk encryption metric might be lower than expected, and corrective actions you can take.

Factors that contribute to a lower-than-expected disk encryption status metric

Contributing Factor	Corrective Actions
No corporate policy mandating full disk encryption is enabled	Reference Trends board shown in Enforce that highlights lack of FDE. Work with security stakeholders to deploy disk encryption policies.
Segments of enterprise do not have full disk encryption enabled	Use drill down questions to explore commonalities between machines that are lacking FDE that should have it in place.
Operating systems do not support native disk encryption (BitLocker, Filevault)	Use Enforce policy status report to determine endpoints that have operating systems but do not support BitLocker (such as Windows 10 Home). Work on endpoint “recap” plan with asset team.
Weak or unapproved encryption is being used	Use Enforce policy status report to determine endpoints that have weak encryption enabled. Deploy decryption package and enforce a FDE policy with the correct encryption type.

Monitor and troubleshoot antivirus status on endpoints

The following table lists contributing factors into why the Enforce antivirus metric might be lower than expected, and corrective actions you can take.

Factors that contribute to a lower-than-expected antivirus status metric

Contributing Factor	Corrective Actions
Third-party antivirus product is not installed	Deploy anti-malware policy.
Real-time scanning is not enabled	Deploy anti-malware policy that enables real-time scanning.
Definition files are not up-to-date	Ensure Tanium is downloading Defender definition files from Microsoft.

©2026 Tanium Inc. All Rights Reserved

Troubleshooting Enforce

If Enforce is not performing as expected, you might need to troubleshoot issues or change settings.

Collect logs

Enforce Logs

About this task

Log information is saved as a ZIP file that you can download with your browser.

1. From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. Click Help ? and then click **Troubleshooting**.
2. In the **Collect Information for Support Requests** section, select the additional solutions for which to gather troubleshooting packages. All available solutions are selected by default.
3. Click **Download Support Bundle**. tanium-solution name-support-[timestamp].zip files download to the local download directory.
4. Contact Tanium Support on page 222 to determine the best option to send the ZIP files.

Endpoint Logs

Use the following information to collect logs from your endpoints.

Enforce endpoint logs

Log Source	Description
Policy database	The Enforce configuration database. Go to <tanium client directory>\extensions\enforce\policy.db .
Group policy export	A record of domain and local policies that are applied to the endpoint. To generate this export, from the command line on the endpoint, enter: `gpresult /h gpo-report.html` .

©2026 Tanium Inc. All Rights Reserved

Log Source	Description
Extensions log	A log of Active Directory administrative template (ADMX) group polices. Go to <tanium client directory>\Logs\extensions0.txt . During the troubleshooting process, for best results, increase the log verbosity level. 1. From the command line on the endpoint, enter, `TaniumClient.exe config set Logs.extensions.enforce.LogVerbosityLevel 99`. 2. Restart the Tanium Client. When you finish troubleshooting, remove the setting. 1. From a command line on the endpoint, enter `TaniumClient.exe config remove Logs.extensions.enforce.LogVerbosityLevel`. 2. Restart the Tanium Client.
Enforce log	A log of Enforce actions. Go to <tanium client directory>\Logs\enforce.txt

You can also use Client Management to directly connect to an endpoint and collect the artifacts above. For more information, see Tanium Client Management User Guide: Collect troubleshooting information from endpoints.

Update default log level

1. From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. Click Help ? and then click **Troubleshooting**.
2. In the **Log Level** section, select the log level.

Review AppLocker event logs

About this task

To see more details about AppLocker blocks on Windows endpoints, review the AppLocker event logs in Event Viewer.

1. Open the Control Panel on the Windows endpoint and then click **System and Security** >

©2026 Tanium Inc. All Rights Reserved

Administrative Tools.

2. To open the Event Viewer, double-click **Event Viewer**.
3. Expand **Applications and Services Logs** and click either **Tanium Enforce - AppLocker** or **Tanium Enforce - AppLocker - MSI and Script**.
4. Double-click any of the events to review more details about AppLocker blocks.

Result

All AppLocker logs are gathered into the **Tanium Enforce - AppLocker** event log when aggregate results is run. Each of the two log file sizes is 10 MB.

Use Enforce sensors

About this task

The following list is a sample of available Enforce sensors. To view all sensors, go to **Administration** > **Content** > **Sensors**.

> **Note:** Not all Enforce sensors report back the most recent data. Most sensors provide information that is gathered during the latest validation check on the endpoint. Validation checks are performed at intervals of approximately 15 minutes.

Enforce - Anti-Malware Definition Outdated

Reports the current Windows anti-malware definition version installed on the computer is out of date.

Enforce - Anti-Malware Definition Version

Reports the current Windows anti-malware definition version installed on the computer.

Enforce - Anti-Malware Engine Version

Reports the current Windows anti-malware engine version installed on the computer.

Enforce - Anti-Malware Threat Details

Reports all anti-malware threats along with detection date, process name, and file paths.

©2026 Tanium Inc. All Rights Reserved

Enforce - Anti-Malware Threats Last X Days

Given a number of days in the past, this sensor reports all anti-malware threats since that date.

Enforce - Anti-Malware Threat Counts Last X Days

Given a number of days in the past, this sensor reports all anti-malware threats counts since that date.

Enforce - Total Anti-Malware Threats Last X Days

Given a number of days in the past, this sensor reports to the total number of anti-malware threats detected since that date.

Enforce - Coverage Status

Returns "Optimal" if Enforce is installed and running, "Needs Attention" if Enforce is not installed or is not healthy, "Unsupported" if the operating system is not supported.

Enforce - Device Setup Classes

Lists all device setup classes.

Enforce - Diagnostic - Applied Machine Policies

Specifically for small scale diagnostics. Returns the status of machine policy settings that are applied or partially applied on endpoints

Enforce - Diagnostic - Applied Policy Settings

Specifically for small scale diagnostics. Returns a list of all policy items to be applied on endpoints, including those that do not apply because they are superseded by a duplicate setting.

Enforce - Firewall Rules [Linux]

Reports all configured firewall rules on Linux endpoints.

Enforce - Firewall Rules [Windows]

Reports all configured firewall rules.

©2026 Tanium Inc. All Rights Reserved

Enforce - Host Firewall Enabled

Returns Yes if firewall is enabled. Otherwise, it returns No.

Enforce - Machine Policy Status

Given a list of Policy Id numbers, reports the enforcement status of each.

Enforce - Machine Policy Status [VBS]

Given a list of Policy Id numbers, reports the enforcement status of each. Unlike other sensors, VBS sensors provide up-to-the-minute results.

Enforce Managed Definitions Targeting

Used for targeting Tanium Enforce Managed Definitions packages. This sensor determines if a host should require download and execution of the definitions package.

Enforce Prerequisites

Reports the installed prerequisites needed by some Enforce policies.

Enforce - USB Storage Devices

Lists hardware IDs for all USB storage devices.

Enforce - Tools Version

Reports support and installation details. Checks if the endpoint supports the tools and has enough disk space. If a package has been deployed, reports the install location, version of tools, and if all the required tools are present.

Resolve Active Directory policy conflicts

Enforce uses Local Group Policy Objects (LGPO) to apply policy settings that cannot be applied using a configuration service provider (CSP). When a setting is applied using LGPO, if an endpoint is joined to a domain and is receiving a domain policy that contains the same policy setting Enforce is trying to apply, the Domain Group Policy (DGPO) takes precedence. To resolve this, the DGPO policy setting must be set to **Not configured** for Enforce to manage it.

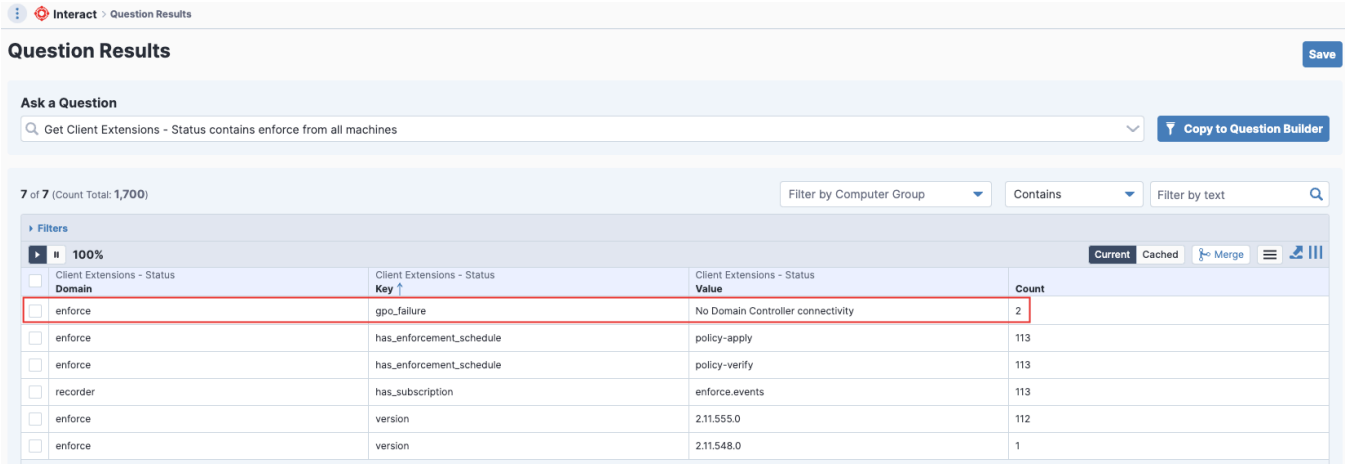
Domain-joined endpoints attempt to reach out to a domain controller to resolve conflicts between DGPO and LGPO settings when Enforce applies policies on the endpoint (at the initial enforcement

©2026 Tanium Inc. All Rights Reserved

time and then every 60 minutes thereafter). If a domain-joined endpoint cannot reach a domain controller, the endpoint cannot determine if LGPO settings are in conflict with DGPO settings. In this case, LGPO settings are not applied and consequently Enforce cannot apply policies of this type.

To determine whether an endpoint has policy settings that cannot be applied due to a lack of connectivity with the domain controller, ask this question in Interact: Get `Client Extensions - Status contains Enforce from all machines` and look for a `gpo_failure` key with the value `No Domain Controller connectivity`. You can drill down into that row in the results to identify the specific endpoints.

Figure 12. Question results



Note:

- Conflicting DGPO and LGPO settings are reported as either **Not Applied** (only one policy setting exists in the policy and it conflicts with DGPO) or **Partially Applied** (more than one policy setting exists in the policy and at least one is in conflict with DGPO). Enforce does not apply policy items that are in conflict with DGPO. The group policy engine on the endpoint resolves that internally. The enforcement status drill down reports in the **Reason** column that the setting was verified with no items applied.

- An LGPO setting that does not use a GPO client-side extension (CSE) is applied directly to the registry. These settings show as **Applied** even if the endpoint cannot connect to the domain controller. For more information about CSE, see Microsoft: Client-side Extensions.

©2026 Tanium Inc. All Rights Reserved

Review policy settings when Windows Defender tamper protection is enabled

When you enable tamper protection in Windows Defender, the following policy settings are locked with their default values and cannot be edited through group policy. These settings might cause log errors if configured as part of an anti-virus policy or machine administrative template policy. For more information about settings that are disabled by Windows Defender tamper protection, see Microsoft Documentation: Protect security settings with tamper protection.

Settings related to Windows Defender tamper protection

Setting Name	Value
Join Microsoft MAPS	HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet\SpynetReporting
Configure the 'Block at First Sight' feature	HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet\DisableBlockAtFirstSeen
Scan all downloaded files and attachments	HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableIOAVProtection
Turn off Microsoft Defender Antivirus	HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware
Turn off real-time protection	HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring
Monitor file and program activity on your computer	HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time\Protection\DisableOnAccessProtection
Turn on behavior monitoring	HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time\Protection\DisableBehaviorMonitoring
Turn on process scanning whenever real-time protection is enabled	HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableScanOnRealtimeEnable
Suppress all notifications	HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\UX Configuration\Notification_Suppress

©2026 Tanium Inc. All Rights Reserved

Review the status for policy settings on Windows endpoints

When you enforce a BitLocker policy, Machine Administrative Template policy, Security Settings policy, or User Administrative Template policy, settings on supported Windows 10 and later endpoints are applied using configuration service providers (CSPs) when possible. For more information, see Configuration service providers (CSPs) on page 163. Policy settings that cannot be applied using a CSP are applied using Local Group Policy (LGPO), the Group Policy Security Settings extension, or the Group Policy Audit Configuration Extension.

To check the status of a policy setting on Windows endpoints, you can ask this question: `Get Enforce - Diagnostic - Applied Policy Settings from <targeted endpoints>` in Interact. In the results, the **Status** column shows the status and how the setting was applied. For example:

Policy setting statuses

Status	Meaning
`CSP:VERIFIED_FULL SECURITY:VERIFIED_NOT_APPLIED`	`CSP:VERIFIED_FULL` indicates that the setting was successfully applied on the endpoint using a CSP. The `SECURITY:VERIFIED_NOT_APPLIED` status can be ignored; the setting application was not attempted using the Group Policy Security Settings extension because the setting was already successfully applied using a CSP.
`CSP:VERIFIED_NOT_APPLIED LGPO:VERIFIED_FULL`	`CSP:VERIFIED_NOT_APPLIED` indicates that the setting was not successfully applied on the endpoint using a CSP. The setting was then successfully applied using Local Group Policy (LGPO).
`LGPO:VERIFIED_SUPERSEDED`	The setting was superseded by another policy with a higher priority. Check the **Errors** column for the policy ID of the policy that superseded the setting. For more information about prioritizing policies, see Prioritize policies on page 161.
`LGPO:VERIFIED_FULL`	The setting was successfully applied using LGPO. Either the setting or the endpoint operating system is not supported by CSP, so that method was not attempted.
`AUDIT:VERIFIED_FULL`	The setting was successfully applied using the Group Policy Audit Configuration Extension. Audit settings are not supported for application using a CSP, so that method was not attempted.
`CSP:VERIFIED_ERROR LGPO:VERIFIED_FULL`	An error occurred when attempting to apply the setting using a CSP, but the setting

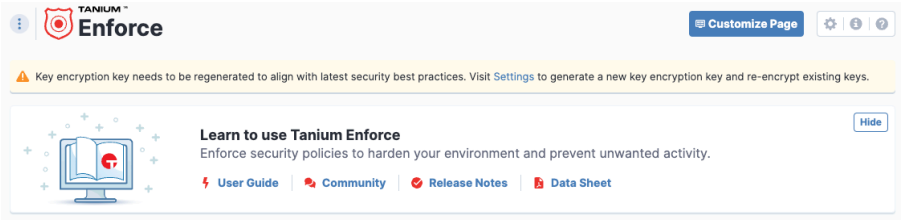
©2026 Tanium Inc. All Rights Reserved

Status	Meaning
	was successfully applied using LGPO. Check the **Errors** column for more information on the CSP error. If both methods fail with an error, the setting application retries later. For more information, see Enforcing policies on page 163 .

Regenerate the Key Encryption Key to align with security best practices

About this task

When you upgrade to Enforce 2.4.230 or later from an earlier version, you might receive this message in the workbench: `Key encryption key needs to be regenerated to align with latest security best practices. Visit Settings to generate a new key encryption key and re-encrypt existing keys.`



For more information about regenerating the Key Encryption Key, see Generate the Key Encryption Key on page 224.

"Access is Denied" error when attempting to manually encrypt a removable drive

If you attempt to manually encrypt a removable drive using BitLocker in a remote desktop session (RDP), you might receive this error: `Access is denied`. This error can occur in this scenario if the **All Removable Storage: Allow direct access in remote sessions** policy setting is not enabled. To resolve this error, either enable BitLocker using the local console (not over RDP) or enable the policy setting using a Machine Administrative Template policy. This setting is in the **System** > **Removable Storage Access** section of the policy.

©2026 Tanium Inc. All Rights Reserved

Translate encryption method values in an exported BitLocker policy

When you export a BitLocker policy, the encryption method settings appear in the JSON as unsigned integer values rather than algorithm names. To translate these integers to the corresponding algorithm, see BitLocker encryption method values in exported policies on page 232.

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 and Reference: Client extensions and endpoint tools used for Tanium solutions.

Identify and resolve issues with Client Extensions

About this task

Use the following steps to troubleshoot issues with the Client Extensions that Enforce installs and uses. During troubleshooting, consider environmental factors such as security exclusions, file locks, CPU usage, RAM usage, and disk failures.

Tip: For more information about the Client Extensions that Enforce installs and uses, see Client Extensions on page 31.

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 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

©2026 Tanium Inc. All Rights Reserved

point to deploy actions that might help correct the issue. Filter the results and drill down as necessary to investigate results that indicate errors.

Tip: 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 Enforce tools from endpoints on page 219 and Endpoint Configuration User Guide: Uninstall a tool installed by Endpoint Configuration.



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.

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 <Tool_Name> from all machines with Endpoint Configuration - Tools Status:Tool Name contains <Tool_Name>`

Review the columns in the results for specific information about errors. The following table provides guidance for some common error conditions:

Potential errors returned by the Endpoint 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:

©2026 Tanium Inc. All Rights Reserved

Error Condition	Possible Resolution
	• 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. • Enforce is no longer installed, or it is no longer targeting the endpoint. In some cases, Enforce might stop targeting an endpoint because it no longer needs the endpoint for a particular workload. Consider whether Enforce should still target the endpoint: • If it is expected or intentional that Enforce no longer targets the endpoint, you can optionally uninstall Enforce tools and dependencies. For more information, see Remove Enforce tools from endpoints on page 219. • If Enforce should still target the endpoint, make sure that the Enforce action group includes the endpoint, and make sure Enforce 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 Review tool installations that are scheduled for a retry .

©2026 Tanium Inc. All Rights Reserved

Error Condition	Possible Resolution
Manually Blocked: `blocked`	The tool was previously blocked, either manually or during a previous uninstallation. Unblock the tool. For more information, see 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 0.

Next steps

For additional help, collect all logs for Enforce on page 207, and contact Tanium Support on page 222.

Review the Extensions log for an endpoint

About this task

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**.

Next steps

For additional help, collect all logs for Enforce on page 207, and contact Tanium Support on page 222.

Remove Enforce tools from endpoints

About this task

You can deploy an action to remove Enforce tools from an endpoint or computer group. Separate actions are available for Windows and non-Windows endpoints.

©2026 Tanium Inc. All Rights Reserved

1. 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`
2. In the results, select the row for Enforce, drill down as necessary, and select the targets from which you want to remove Enforce tools. For more information, see Tanium Interact User Guide: Drill Down.
3. Click **Deploy Action**.
4. For the **Deployment Package**, select **Endpoint Configuration - Uninstall Tool [Windows]** or **Endpoint Configuration - Uninstall Tool [Non-Windows]**, depending on the endpoints you are targeting.
5. For **Tool Name**, select Enforce.
6. (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 Enforce 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.
7. (Optional) To remove all Enforce 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.
8. (Optional) To also remove any tools that were dependencies of the Enforce tools that are not

©2026 Tanium Inc. All Rights Reserved

dependencies for tools from other solutions, select **Remove unreferenced dependencies**.

9. (Optional) In the **Deployment Schedule** section, configure a schedule for the action.

   Tip: If some target endpoints might be offline when you initially deploy the action, select **Recurring Deployment** and set a reissue interval.

10. Click **Show preview to continue**.

11. 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 Enforce

1. From the Main menu, go to **Administration** > **Configuration** > **Solutions**.

2. Select Enforce and click **Uninstall**. Click **Yes** to complete the process.

Note:

- After you uninstall Enforce you might need to disable the associated firewall policies to ensure they are cleanly removed from endpoints in some instances, such as if some endpoints are offline when you uninstall Enforce. In this case, deploy actions including the **Remove Enforce Firewall Rules** package that was created when Enforce was installed. For more information, see Disable and remove Enforce firewall policies on page 221.

- To complete a clean uninstallation and removal of Enforce policies, you must uninstall Enforce before you disable the associated firewall policies.

Disable and remove Enforce firewall policies

©2026 Tanium Inc. All Rights Reserved

About this task

You might need to disable Enforce firewall policies after you uninstall Enforce, which might occur if some endpoints are offline when you uninstall Enforce. In this case, deploy actions including the **Remove Enforce Firewall Rules** package that was created when Enforce was installed. For more information about packages and deploying actions, see Tanium Console User Guide: Managing scheduled actions and action history and Tanium Console User Guide: Managing packages.

To disable and remove Enforce firewall policies, first find all of the endpoints that are online and then deploy the removal package.

1. From the Main menu, click **Interact**.
2. Ask a question to target the endpoints from which you want to remove the policies. For example, `Get Enforce - Tools Version from all machines`.
3. Select the row for the endpoints from which you want to remove the policies.
4. Click **Deploy Action**.
5. Select the **Remove Enforce Firewall Rules** Package.
6. Click **Show preview to continue** in the **Targeting Criteria** section.
7. Review the targeted endpoints.
8. Click **Deploy Action** and enter your credentials. The **Action Summary** page appears.

Result

Important: The **Remove Enforce Firewall Rules** package removes all firewall rules created by Enforce. It does not disable the firewall on the endpoint.

Contact Tanium Support

To contact Tanium Support for help, sign in to the Tanium Customer Community.

For more information about submitting a support case, see Case Submission Form.

©2026 Tanium Inc. All Rights Reserved

Reference: Windows encryption management

Encryption management policies encrypt drives on endpoints using Windows BitLocker Drive Encryption. For more information, see Microsoft Documentation: BitLocker.

Endpoint requirements

- Windows 10 Education, Pro Education, Enterprise, or Pro
- Windows 11 Enterprise or Pro[1]
- Windows Server 2019 and later

For more information about Windows endpoint requirements and TPM compatibility, see Microsoft Documentation: BitLocker.

[1] Windows 11 endpoints with Arm processors are supported with Enforce 2.4.213 or later. For versions of the Tanium Client that support this architecture, see Tanium Client Management User Guide: Client version and host system requirements.

Configuration requirements

Complete the following steps to configure your environment to use encryption management policies:

- Generate the Key Encryption Key on page 224
- Create a database to store the recovery keys on page 224
- Install the End-User Notifications service and initialize endpoints on page 225
- Install and configure Direct Connect on page 225.
- (Optional) Install and configure the encryption key recovery portal on page 225

©2026 Tanium Inc. All Rights Reserved

- Create and enforce the encryption management policy on page 225

Generate the Key Encryption Key

About this task

Before you create a BitLocker policy, you must generate the Key Encryption Key (KEK). Recovery keys are encrypted using this KEK for additional security.

If needed, you can generate a new KEK to replace an existing KEK. If you generate a new KEK, existing keys are re-encrypted using the new KEK.

1. From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. Click Settings and then click **Endpoint Encryption** > **General Settings**.
2. Click **Generate Key** > **Generate**.
3. Click Copy to Clipboard and save the key in a secure location.

   Important: Save this key in a secure location, outside of Tanium Console, for future use. In a disaster recovery scenario, you must use this key to retrieve recovery keys.
4. Click **Save**.

Create a database to store the recovery keys

About this task

Recovery keys are used to unlock the drive if a user forgets the PIN or password. Before you create and enforce encryption management policies, you must create a database to store the recovery keys. That database can be hosted on the Tanium Module Server (TMS hosted) or you can host it on your own server (self hosted). Hosting the database on the TMS requires no additional configuration beyond selecting the **TMS hosted** option during configuration. For more information about creating a self-hosted database, see Reference: Creating a self-hosted database to store recovery keys on page 262.

For more information about managing recovery keys, see Managing recovery keys on page 229

©2026 Tanium Inc. All Rights Reserved

Note: If you configure the optional encryption key recovery portal, a user can retrieve their recovery key by signing in to the encryption key recovery portal to retrieve their recovery key using the recovery key ID or their computer name. Users can only retrieve their own recovery keys.

Install the End-User Notifications service and initialize endpoints

About this task

Encryption management policies use the End-User Notifications service to display notifications throughout the encryption process. This service must be installed and initialized on endpoints before you can enforce encryption management policies. For more information, see Tanium End-User Notifications User Guide: Installing End-User Notifications.

If this service is not installed and pushed out to endpoints, the policy fails to enforce. In this scenario, the End-User Notifications service is listed as the enforcement failure reason.

Install and configure Direct Connect

About this task

Encryption management policies use Direct Connect to transfer encryption keys securely from the client to the recovery key database during the encryption process. This service must be installed and initialized on endpoints before you enforce encryption management policies. For more information, see Tanium Direct Connect User Guide: Installing Direct Connect.

If this service is not installed and pushed out to endpoints, the policy fails to enforce. In this scenario, the Direct Connect service is listed as the enforcement failure reason.

(Optional) Install and configure the encryption key recovery portal

The encryption key recovery portal is an optional self-service website that users can access if they forget their PIN or password. This website is typically internet-facing in a DMZ so that users who forget their PIN or password can access it from another device. For more information, see Reference: Encryption key recovery portal on page 241.

Create and enforce the encryption management policy

Create the policy and enforce it on endpoints. For more information, see Create a BitLocker policy on

©2026 Tanium Inc. All Rights Reserved

page 103.

Endpoint workflow

After the policy is enforced and pushed out to endpoints, the encryption process takes place in several stages.

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.

Prepare the drive for encryption

After the policy is enforced on an endpoint, a notification appears to instruct the user to reboot the computer to prepare the drive for encryption. The user can dismiss this message. It appears every hour until the user reboots the computer.

Configure the text for this notification in the **Reboot Computer** section of the BitLocker policy.

Note: This action is the only BitLocker action that does not automatically repeat if it fails because manual intervention is usually required to recover from a failure during drive preparation. If this action fails on an endpoint, a failure message appears to the user and the policy is reported as unenforced with `Failed to prepare volume for encryption` as the enforcement error.

Configure the PIN or password

Note: This stage occurs only if you configured the policy for **TPM + PIN** or **Allow BitLocker to run without a compatible TPM**.

After the computer reboots, the user is prompted within five minutes to set a PIN or password. Configure the text for this message in the **Enter New Credentials** section of the BitLocker policy.

©2026 Tanium Inc. All Rights Reserved

After the user enters a PIN or password and clicks **Create PIN**, a notification appears to alert the user that encryption begins after the next reboot. Configure the text for this message in the **Encrypt Hard Drive** section of the BitLocker policy. Depending on the operating system configuration, the user might also see a Windows notification that encryption begins after the computer is rebooted.

Encryption occurs

The next time that the user reboots the computer, they are prompted to enter the PIN or password if one was set. Encryption begins. The encryption process is not disruptive. The user sees an icon in the system tray that indicates that the drive is being encrypted, but the user can continue to work. If needed, the user can right click the system tray icon and select to pause the encryption process.

Behavior at subsequent starts or restarts

After encryption completes, users are prompted for the PIN or password each time they start or reboot the computer, if one was set. In the boot screen, users see the instructions for unlocking the drive using the recovery the key if they forget their PIN or password. Configure the text for this pre-boot message in the **Key Recovery** section of the BitLocker policy.

User forgets the PIN or password

If a user forgets their password, they can use a recovery key to access the operating system. For more information about the self-service workflow with the encryption key recovery portal, see End user self-service workflow on page 259. For more information about managing recovery keys from the Enforce workbench, see Managing recovery keys on page 229

When a user is prompted to enter the PIN or password, there is an instruction to **Press Esc for BitLocker recovery**. When the user presses the Esc key, the **BitLocker recovery** page opens where the user can enter the recovery key for the drive.

After the drive is unlocked, the user is prompted to change the PIN or password within five minutes. On subsequent starts or restarts, the user uses this new PIN or password to unlock the drive.

Prompt the user to reset their PIN or password

About this task

Enforce 2.10 and later includes the **Enforce - Rotate Bitlocker Password** package. You can use this

©2026 Tanium Inc. All Rights Reserved

package to prompt a user to change their PIN or password with an End User Notifications prompt. Only **TPM and PIN** and password (configured using the **Allow BitLocker to run without a compatible TPM** option for endpoints without a TPM) protectors are supported by this package. For more information about using actions to deploy packages to endpoints, see Deploying actions and playbooks in Console and Interact.



Note: This package is not supported for use on endpoints where a legacy BitLocker policy is enforced.

Suspend and resume BitLocker

During system maintenance or troubleshooting, you might need to temporarily suspend BitLocker. The key protectors are disabled when you suspend BitLocker, which allows you to bypass BitLocker without unencrypting the drive. You can resume BitLocker after you complete the maintenance or troubleshooting without having to encrypt the drive again.

Enforce includes these packages to suspend and resume BitLocker: **Enforce - Suspend BitLocker** and **Enforce - Resume BitLocker**.

Enforce - Suspend BitLocker

Use this package to suspend BitLocker on an endpoint. This package has one parameter, `rebootcount`. Use this parameter to specify the number of reboots before BitLocker automatically resumes. If you set this parameter to `0`, BitLocker never automatically resumes and must be manually resumed by running the **Enforce - Resume BitLocker** package.

Enforce - Resume BitLocker

Use this package to resume BitLocker on an endpoint where it was previously suspended.

When you suspend BitLocker on an enforced endpoint, the BitLocker policy enforcement status is **Unenforced** with `BitLocker has been suspended` as the reason.

For more information about using actions to deploy packages to endpoints, see Deploying actions and playbooks in Console and Interact.

Remove BitLocker encryption from an endpoint

©2026 Tanium Inc. All Rights Reserved

1. Remove the BitLocker policy enforcement on the endpoint. For more information, see Remove an enforcement on page 175.
2. Deploy an action to run one of these packages on the endpoint, depending on the type of drive:

    - **Enforce - Decrypt BitLocker**: Use this package to decrypt the drive on which the operating system is installed.
    - **Enforce - Decrypt BitLocker Fixed Drives**: Use this package to decrypt **fixed** drives other than the operating system drive.

    For more information, see Deploying actions and playbooks in Console and Interact.

    Note:

    - Use the operating system to manually decrypt removable drives.
    - This multi-step design is intentional so that encryption is not removed from a drive if an administrator inadvertently removes enforcement of the policy from an endpoint.

Managing recovery keys

Note:

- For more information about the roles that can view the recovery keys for users on the **Endpoint Encryption** page in the Enforce workbench, see User role requirements on page 44.
- You can only view and download keys for endpoints for which you have management rights.
- Enforce does not automatically delete recovery keys. To view deleted recovery keys, select **Show Deleted Keys**. If needed, you can manually delete a recovery key by clicking Delete Key in the row for that key.

©2026 Tanium Inc. All Rights Reserved

View BitLocker recovery keys

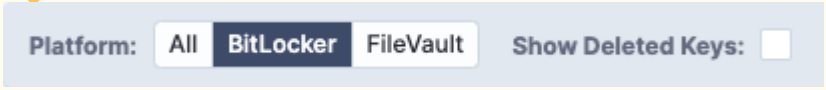
View recovery key information, such as computer name, user name, recovery key ID, and last rotation.

From the Main menu, go to **Modules** > **Enforce** > **Endpoint Encryption** > **Overview** to view health data. Click **Recovery Keys** to view recovery keys.

Retrieve a single recovery key

1. From the Enforce menu, click **Endpoint Encryption** > **Recovery Keys**.
2. In the row for the endpoint for which you want to save the recovery key, click Copy Key .

   Tip: Use the **Platform** filter to show only BitLocker keys.

3. Save the key to a local file.

Export all recovery keys and the recovery keys access log

About this task

You can generate a recovery key access log to audit access to the recovery keys. You can also export endpoint encryption recovery keys to a CSV file to use for disaster recovery purposes. To export recovery keys, you must have the **Disk Encryption Recovery Keys - Export** permission. This permission is granted only to the Enforce Administrator and Enforce Operator roles by default.

©2026 Tanium Inc. All Rights Reserved

Note:

- You can download keys only from endpoints for which you have management rights.
- Generated files are available to download for 10 minutes. After that time, the file must be generated again.
- You can filter the recovery keys shown on the Recovery Keys page using the **Category** filter, but this filter is not applied to generated files.

CAUTION: The generated files include sensitive data. Ensure that you store the files in a secure location.

1. From the Main menu, go to **Modules** > **Enforce** > **Endpoint Encryption** > **Recovery Keys**.
2. (Optional) Complete these steps to export the recovery keys access log:
   a. Click **Export** > **Recovery Key Access Log**.
   b. Read the warning about the contents of the file and click **Generate**.
   c. When the file is ready, click **Download**.
3. (Optional) Complete these steps to export the recovery keys:
   a. Click **Export** > **Recovery Keys**.
   b. Read the warning about the contents of the file and click **Generate**.
   c. When the file is ready, click **Download**.

Rotate a recovery key

1. From the Enforce menu, click **Endpoint Encryption** > **Recovery Keys**.
2. In the row for the endpoint for which you want to rotate the recovery key, click Rotate Key. You can also use the **Enforce - Rotate Bitlocker Recovery Keys** package to rotate recovery keys for endpoints. For more information about using actions to deploy packages to endpoints, see Deploying actions and playbooks in Console and Interact.

   Note: On endpoints where a legacy BitLocker policy is enforced, this action is supported only for use with operating system drives.

©2026 Tanium Inc. All Rights Reserved

BitLocker encryption method values in exported policies

When you export a BitLocker policy, the encryption method settings appear in the JSON as unsigned integer values rather than algorithm names. Use the following tables to translate these integers to the corresponding algorithm. The mapping depends on which field contains the value, so the same integer can represent different algorithms in different fields.

For more information about these values, see Microsoft Documentation: GetEncryptionMethod method of the Win32_EncryptableVolume class.

`encryptionMethod`

Values for the encryptionMethod field

Algorithm	Integer value
AES_128_WITH_DIFFUSER	1
AES_256_WITH_DIFFUSER	2
AES_128	3
AES_256	4

`encryptionMethodNoDiffuser`

Values for the encryptionMethodNoDiffuser field

Algorithm	Integer value
AES_128	3
AES_256	4

`encryptionMethodWithXtsOs`

©2026 Tanium Inc. All Rights Reserved

Values for the encryptionMethodWithXtsOs field

Algorithm	Integer value
AES_CBC_128	3
AES_CBC_256	4
XTS_AES_128	6
XTS_AES_256	7

©2026 Tanium Inc. All Rights Reserved

Reference: macOS encryption management

Encryption management policies encrypt drives on endpoints using macOS FileVault. For more information, see Apple Documentation: Use FileVault to encrypt the startup disk on your Mac.

Endpoint requirements

- macOS 10.13.6 High Sierra or later

Configuration requirements

Complete the following steps to configure your environment to use encryption management policies:

- Generate the Key Encryption Key on page 234
- Create a database to store the recovery keys on page 235
- Install the End-User Notifications service and initialize endpoints on page 235
- Install and configure Direct Connect on page 236
- (Optional) Install and configure the recovery portal on page 236
- Creating policies for macOS endpoints on page 136

Generate the Key Encryption Key

About this task

Before you create a FileVault policy, you must generate the Key Encryption Key (KEK). Recovery keys are encrypted using this KEK for additional security.

If needed, you can generate a new KEK to replace an existing KEK. If you generate a new KEK, existing keys are re-encrypted using the new KEK.

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. Click Settings and then click **Endpoint Encryption** > **General Settings**.
2. Click **Generate Key** > **Generate**.
3. Click Copy to Clipboard and save the key in a secure location.

   Important: Save this key in a secure location, outside of Tanium Console, for future use. In a disaster recovery scenario, you must use this key to retrieve recovery keys.
4. Click **Save**.

Create a database to store the recovery keys

About this task

Recovery keys are used to unlock the drive if a user forgets the PIN or password. Before you create and enforce encryption management policies, you must create a database to store the recovery keys. That database can be hosted on the Tanium Module Server (TMS) or you can host it on your own server (Self hosted). Hosting the database on the TMS requires no additional configuration beyond selecting the **TMS hosted** option during configuration. For more information about creating a self-hosted database, see Reference: Creating a self-hosted database to store recovery keys on page 262.

For more information about managing recovery keys, see Managing recovery keys on page 237

Note: If you configure the optional encryption key recovery portal, a user can retrieve their recovery key by signing in to the encryption key recovery portal to retrieve their recovery key using the recovery key ID or their computer name. Users can only retrieve their own recovery keys.

Install the End-User Notifications service and initialize endpoints

About this task

Encryption management policies use the End-User Notifications service to display notifications throughout the encryption process. This service must be installed and initialized on endpoints before you enforce encryption management policies. For more information, see Tanium End-User Notifications User Guide: Installing End-User Notifications.

If this service is not installed and pushed out to endpoints, the policy fails to enforce. In this scenario,

©2026 Tanium Inc. All Rights Reserved

the End-User Notifications service is listed as the enforcement failure reason.

Install and configure Direct Connect

About this task

Encryption management policies use Direct Connect to transfer encryption keys securely from the client to the recovery key database during the encryption process. This service must be installed and initialized on endpoints before you enforce encryption management policies. For more information, see Tanium Direct Connect User Guide: Installing Direct Connect.

If this service is not installed and pushed out to endpoints, the policy fails to enforce. In this scenario, the Direct Connect service is listed as the enforcement failure reason.

(Optional) Install and configure the recovery portal

The recovery portal is an optional self-service website that users can access if they forget their PIN or password. This website is typically internet-facing in a DMZ so that users who forget their PIN or password can access it from another device.

Create and enforce the encryption management policy

Create the policy and enforce it on endpoints. For more information, see Creating policies for macOS endpoints on page 136.

Endpoint workflow

After the policy is enforced and pushed out to endpoints, the encryption process takes place in several stages.

Prepare the drive for encryption

After the policy is enforced on an endpoint, a notification displays either at sign out or during the next sign in to instruct the user to enable FileVault encryption. The user can dismiss this message multiple times if your FileVault policy allows it.

Configure the text for this notification in the **End User Notification** section of the FileVault policy.

©2026 Tanium Inc. All Rights Reserved

Encryption occurs

After the user enables FileVault, encryption begins.

User forgets the password

If a user forgets their password, they can use a recovery key to access the operating system. For more information about the self-service workflow with the encryption key recovery portal, see End user self-service workflow on page 259. For more information about managing recovery keys from the Enforce workbench, see Managing recovery keys on page 237.

To enter the recovery key into the computer, the user clicks the **?** in the password field when prompted for the password. Then the user clicks the arrow beside the text that reads "If you forgot your password, you can reset it using your recovery key." and enters the recovery key.

After the drive is unlocked, the user is prompted to create a new password the next time the user signs in.

Note: If the FileVault policy uses an Institutional Recovery Key, users must start from the macOS Recovery OS (hold Command-R while booting) to enter the recovery key. For more information, see Apple Documentation: How to use institutional recovery keys with Intel-based Macs.

Remove FileVault encryption from an endpoint

1. Remove the FileVault policy enforcement on the endpoint. For more information, see Remove an enforcement on page 175.
2. Deploy an action to run the Enforce - Decrypt FileVault package on the endpoint. For more information, see Tanium Console User Guide: Deploying actions.

   Note: This multi-step design is intentional so that encryption is not removed from a drive if an administrator inadvertently removes enforcement of the policy from an endpoint.

Managing recovery keys

©2026 Tanium Inc. All Rights Reserved

Note:

- For more information about the roles that can view the recovery keys for users on the **Endpoint Encryption** page in the Enforce workbench, see User role requirements on page 44.
- You can only view and download keys for endpoints for which you have management rights.
- Enforce does not automatically delete recovery keys. To view deleted recovery keys, select **Show Deleted Keys**. If needed, you can manually delete a recovery key by clicking Delete Key in the row for that key.
- FileVault keys escrowed from Tanium™ Device Management appear in the **Recovery Keys** list alongside keys collected by Enforce. You can rotate these keys from the Enforce workbench. For more information, see Rotate a recovery key on page 239.

View FileVault recovery keys

View recovery key information, such as computer name, user name, recovery key ID, and last rotation.

From the Main menu, go to **Modules** > **Enforce** > **Endpoint Encryption** > **Overview** to view health data. Click **Recovery Keys** to view recovery keys.

Retrieve a single recovery key

1. From the Main menu, go to **Modules** > **Enforce** > **Endpoint Encryption** > **Recovery Keys**.
2. In the row for the endpoint for which you want to save the recovery key, click Copy Key.

   Tip: Use the **Platform** filter to show only FileVault keys.

3. Save the key to a local file.

©2026 Tanium Inc. All Rights Reserved

Export all recovery keys and the recovery keys access log

About this task

You can generate a recovery key access log to audit access to the recovery keys. You can also export endpoint encryption recovery keys to a CSV file to use for disaster recovery purposes. To export recovery keys, you must have the **Disk Encryption Recovery Keys - Export** permission. This permission is granted only to the Enforce Administrator and Enforce Operator roles by default.

Note:

- You can download keys only from endpoints for which you have management rights.
- Generated files are available to download for 10 minutes. After that time, the file must be generated again.
- You can filter the recovery keys shown on the Recovery Keys page using the **Category** filter, but this filter is not applied to generated files.

CAUTION: The generated files include sensitive data. Ensure that you store the files in a secure location.

1. From the Main menu, go to **Modules** > **Enforce** > **Endpoint Encryption** > **Recovery Keys**.
2. (Optional) Complete these steps to export the recovery keys access log:
   a. Click **Export** > **Recovery Key Access Log**.
   b. Read the warning about the contents of the file and click **Generate**.
   c. When the file is ready, click **Download**.
3. (Optional) Complete these steps to export the recovery keys:
   a. Click **Export** > **Recovery Keys**.
   b. Read the warning about the contents of the file and click **Generate**.
   c. When the file is ready, click **Download**.

Rotate a recovery key

©2026 Tanium Inc. All Rights Reserved

1. From the Enforce menu, click **Endpoint Encryption** > **Recovery Keys**.
2. In the row for the endpoint for which you want to rotate the recovery key, click Rotate Key .

Result

> **Note:**
>
> For FileVault keys escrowed from Tanium Device Management, the Rotate Key

©2026 Tanium Inc. All Rights Reserved

Reference: Encryption key recovery portal

The recovery portal is an optional self-service website that users can access if they forget their PIN or password. This website is typically internet-facing in a DMZ so that users who forget their PIN or password can access it from another device.

Best Practice: Do not host this website on the same machine as the database that is used to store the recovery keys.

Requirements

Supported operating systems for the server hosting the recovery portal

- Amazon Linux 2023
- Amazon Linux 2 LTS
- CentOS 8 and later
- Oracle Linux (OEL) 8 and later
- Red Hat Enterprise Linux (RHEL) 8 and later
- Rocky Linux 8.10 and later
- Ubuntu 22.04 LTS and later
- Windows Server 2016 or later

©2026 Tanium Inc. All Rights Reserved

Important:

- The recovery portal installation fails if Security-Enhanced Linux (SELinux) is enabled.
- If you attempt to install or upgrade the recovery portal on a computer that is not running a supported version of one of these operating systems, the installation fails.

Port requirements

The recovery portal requires the following ports. For more information about Enforce port requirements, see Ports for Enforce communication on page 38.

Ports required for Enforce recovery portal communication

Inbound	443	TCP	Allows users to access the recovery portal.
Outbound	443	TCP	Allows the recovery portal to access the Tanium Server.

Hardware requirements

- CPU: 4 Cores
- RAM: 8 GB
- Hard Drive: 80 GB

Supported identity providers for authentication

These Identity Providers (IdPs) are supported for use with the recovery portal for both OpenID Connect (OIDC) and security assertion markup language (SAML):

- Okta
- Microsoft Entra ID
- Oracle
- Active Directory Federation Services (AD FS)

©2026 Tanium Inc. All Rights Reserved

- Google

Before you begin

Complete the following prerequisites before you configure the recovery portal.

Solution configuration

- Install and configure Enforce. For more information, see Installing Enforce on page 65 and Configuring Enforce on page 68.
- Complete the endpoint encryption configuration. For more information, see Configure endpoint encryption on page 88.

DNS configuration

Verify that DNS resolution is configured correctly for the server where you will host the recovery portal.

Server names must resolve correctly. If necessary, use the local hosts file or create appropriate DNS records to ensure proper name resolution.

Obtain or create SSL certificates

Create a certificate and private key pair, named server.key and server.crt, to use to secure HTTPS traffic from the recovery portal to the user. As a best practice, create a certificate signed by a certificate authority (CA) with the common name (CN) set to the DNS name for the server that is hosting the recovery portal.

©2026 Tanium Inc. All Rights Reserved

Tip:

You can use a self-signed certificate for testing. Use the following OpenSSL command to generate a self-signed certificate:

```
.\openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout server.key -out server.crt
```

When prompted, set the Common Name (CN) to match the DNS name of the server hosting the recovery portal.

Create a Tanium persona or user and API token

Create a dedicated Tanium persona or user that has the **Enforce Recovery Portal** role granted, an API token to enable secure access to the recovery portal, and the appropriate computer management groups assignments.

TANIUM PERSONA OR USER

If you use a persona for this purpose, assign the persona to a user account. This user can be a service account or your own user account, depending on your setup.

If you assign the persona to your own user account, refresh the page or sign out of and back in to Tanium Console to ensure that the changes appear when you generate the API token.

Best Practice: Ensure that this user has computer management group assignments for all endpoints with BitLocker policy enforcements.

API TOKEN

Create an API token for the recover portal to use when authenticating with the Tanium Server. For more information, see Console User Guide: API tokens overview.

©2026 Tanium Inc. All Rights Reserved

Important:

- Include the IPv4 and IPv6 formats in the Trusted IP addresses: x.x.x.x/x,::/x (and not just x.x.x.x/x) or the configuration will fail.
- Record the API token in a secure location to use when you install the recovery portal.

Note details about your configuration

Note the following identifiers for your environment to use during the configuration of the recovery portal:

- Tanium Server API URL
- Recovery Portal FQDN
- User Domain Name (for sign-in)
- SSO Redirect URL

(Microsoft Entra) Create a Microsoft Entra enterprise application and configure an identity provider

About this task

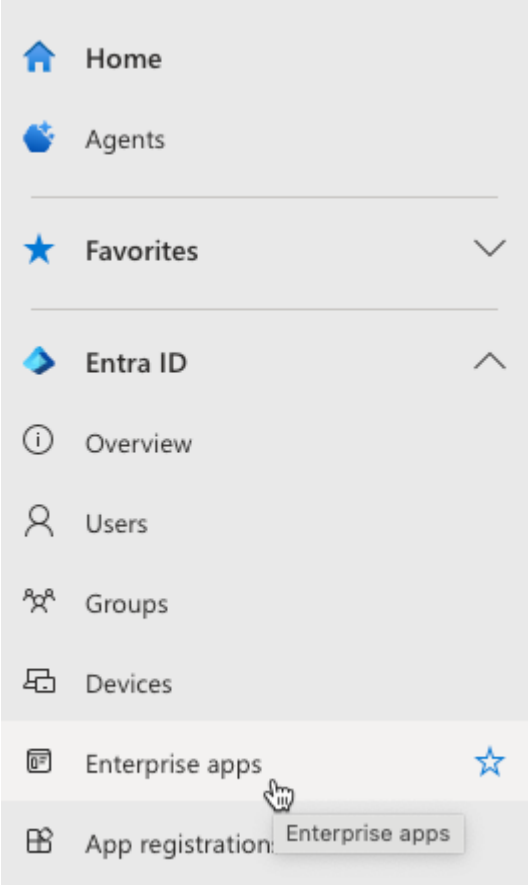
If you are using Microsoft Entra, complete these steps to create and register a custom enterprise application in Microsoft Entra to enable single sign-on (SSO) integration for the recovery portal.

Note: This section describes one way to configure this integration. You might need to modify these steps and the suggested selections and values depending on your environment. Ensure that you test this configuration in a lab or test environment before you use it in a production environment. Consult the Microsoft documentation for detailed steps. For more information, see Microsoft Entra Documentation: Register an application in Microsoft Entra ID

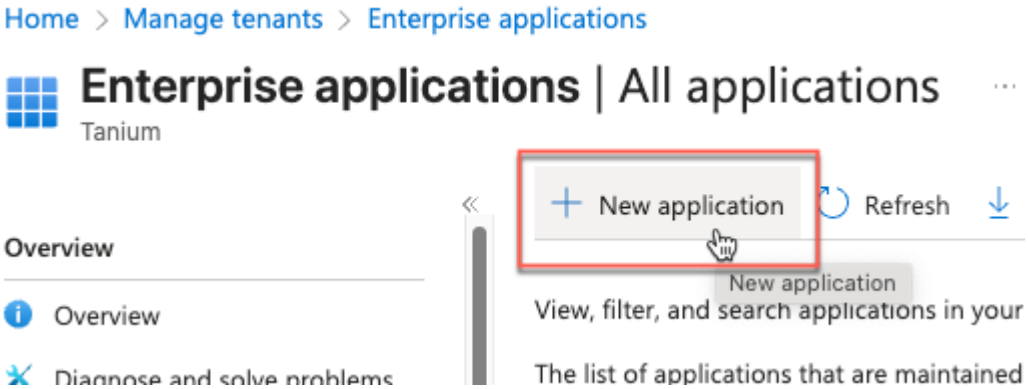
Create an enterprise application

©2026 Tanium Inc. All Rights Reserved

1. In Microsoft Entra, go to **Applications** > **Enterprise applications**.

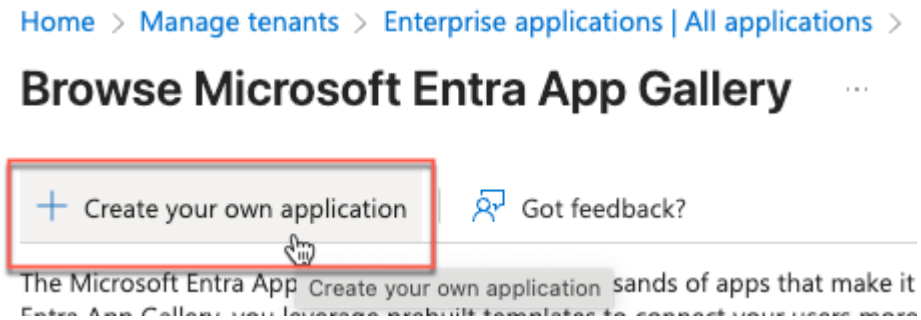


2. Click **New application**.

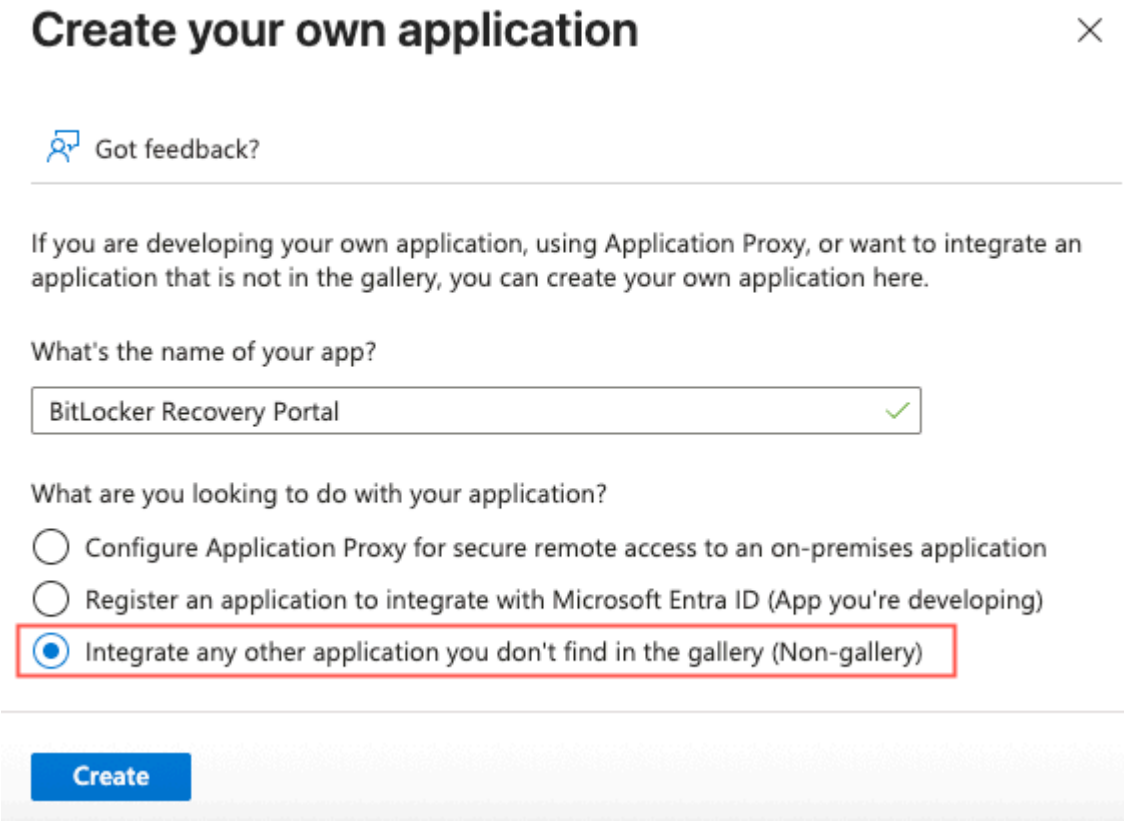


3. Click **Create your own application**.

©2026 Tanium Inc. All Rights Reserved



4. Specify a name for the application. For example, `BitLocker Recovery Portal`.
5. Select this option: **Integrate any other application you don't find in the gallery**.



6. Click **Create**.

Assign users or groups to the enterprise application

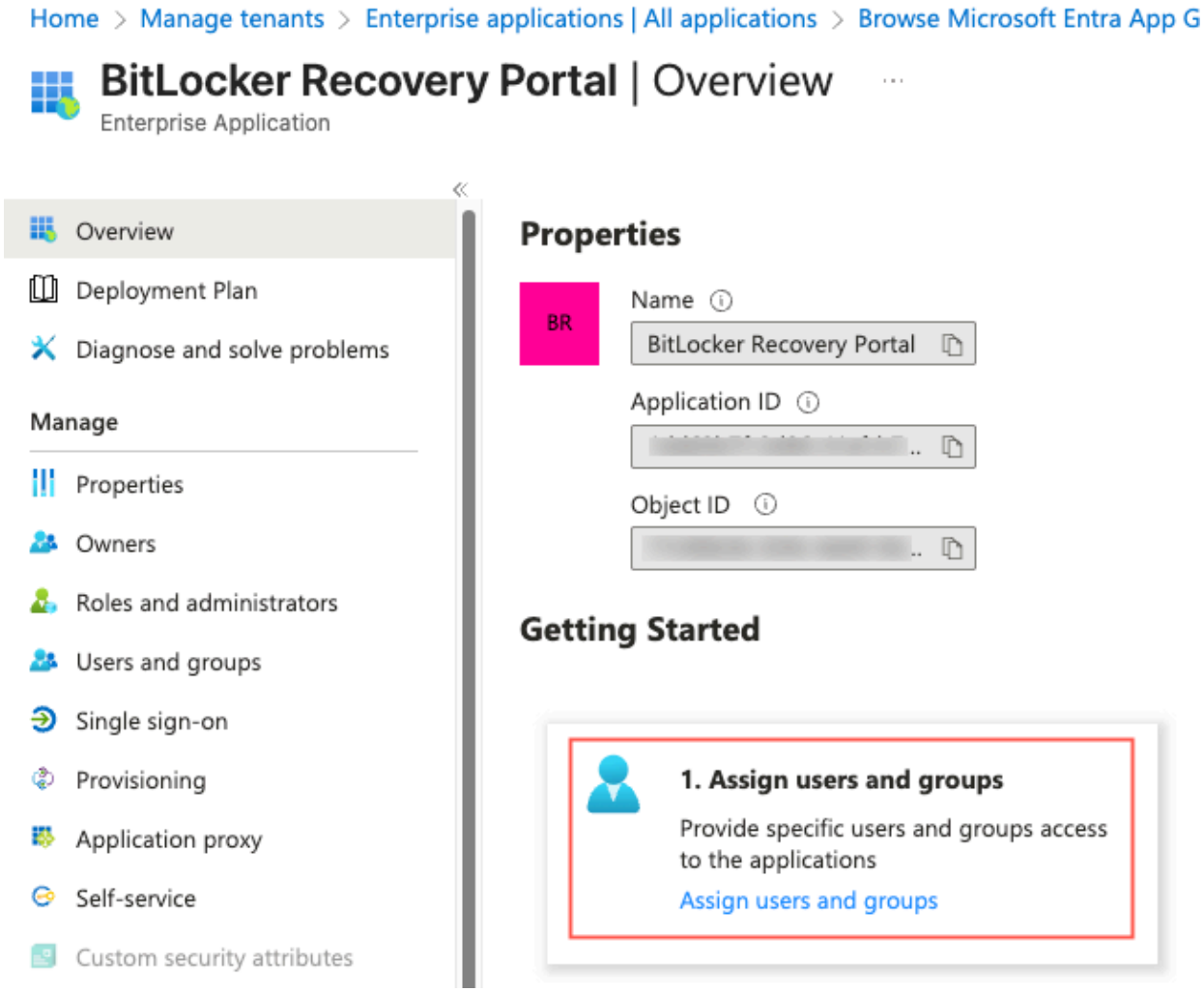
About this task

To enable SSO access to the BitLocker Recovery Portal, users must be granted access to the Entra enterprise application. You can assign individual users or groups.

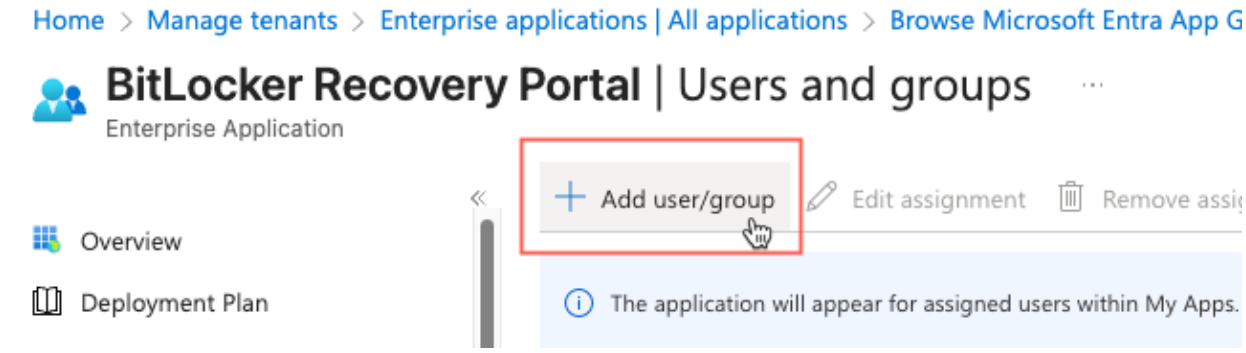
1. In Microsoft Entra, open the application, and on the **Overview** page, select **Assign users and**

©2026 Tanium Inc. All Rights Reserved

groups.

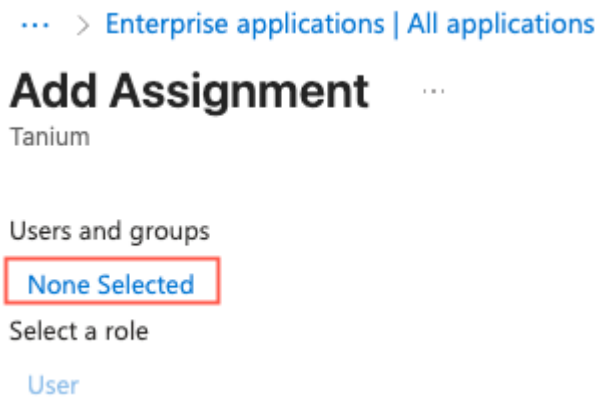


2. Click **Add user/group**.

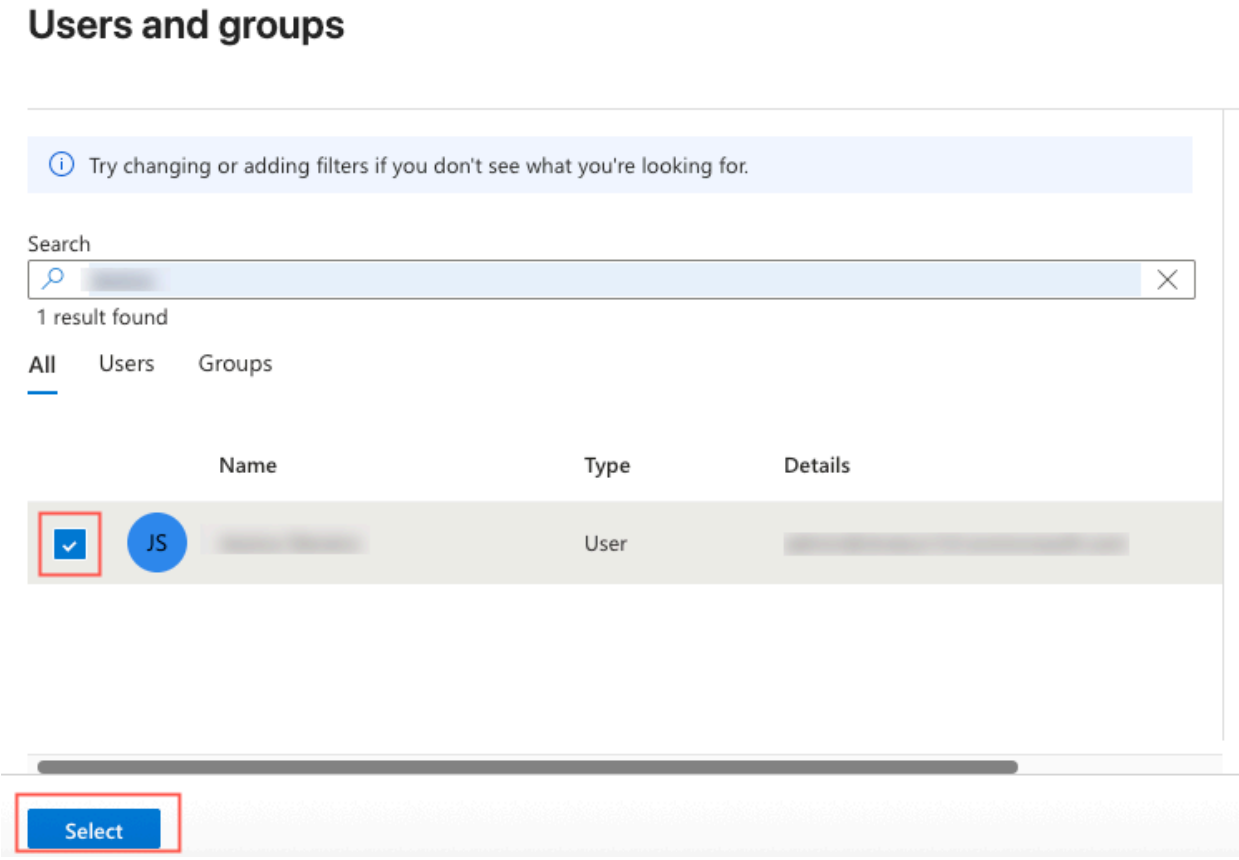


3. In the resulting panel, click **None Selected**.

©2026 Tanium Inc. All Rights Reserved



4. Search for and select the appropriate users and groups.
5. Click **Select** to confirm your choices.



6. Click **Assign** to complete the application assignment.

Set up the Identity Provider and SSO

PART 1: CONFIGURE THE INITIAL IDP SETTINGS IN ENFORCE

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page.
2. Click Settings and then click **Endpoint Encryption** > **Add Identity Provider**.
3. Configure the identity provider settings:
   - **Domain**: Used by the recovery portal to identify the correct identity provider. Format: `<second-level domain>.<top-level domain>`. For example, if you specify `mydomain.com`, users sign in with `username@mydomain.com`.
   - **Type**: Select **SAML**.
   - **Content Set**: Select **Enforce** (default value).
   - **Recovery Application Domain**: Provide the fully qualified domain name (FQDN) of the recovery portal server.
4. In the **SSO Redirect URL** section, click Copy to clipboard. Save this value to use in Microsoft Entra.

   Note: This field appears when you specify the **Recovery Application Domain**.
5. Leave this page open and return to Microsoft Entra to configure the identity provider.

PART 2: CONFIGURE THE IDP SETTINGS IN MICROSOFT ENTRA

1. In Microsoft Entra, go to **Applications** > **Enterprise applications**. Open the application that you created in the previous section.
2. In the Manage section, click **Single sign-on** > **SAML**.
3. In the **Basic SAML Configuration** section, click Edit and specify the following parameters:
   a. **Identifier (Entity ID)**: `https://<portal server FQDN>:443/<domain.name>/saml/acs`

      Important: You copied this value when you configured the initial settings in Enforce. Ensure that you add the port number to this URL when you specify it in Microsoft Entra. The port number is not included in the value that you copied.

   b. **Reply URL**: `https://<portal server FQDN>`. Leave the **Index** value blank.
   c. **Sign-on URL**: `https://<portal server FQDN>/<domain.name>/saml/acs`

   Click **Save** and close that page, if needed, to return to the **SAML-based Sign-on** page.

©2026 Tanium Inc. All Rights Reserved

4. In the **Attributes & Claims** section, click Edit.
5. Click Add new claim and specify the details:
    a. **Name**: Enter `email`.
    b. **Source**: Select **Attribute**.
    c. **Source Attribute**: Select **user.userprincipalname**

    > **Note:** This value might vary depending on your Tanium and Entra environments. If the user names do not align to this value, adjust the SAML attributes and claims to align to the user names in your environment.

    Click **Save** and close that page, if needed, to return to the **SAML-based Sign-on** page.
6. In the **SAML Certificates** section, in the **Token Signing Certificate** subsection, either copy the **App Federation Metadata URL** or download the **Federation Metadata XML**. Return to Enforce to complete the configuration.

PART 3: COMPLETE THE IDP SETTINGS IN ENFORCE

1. On the same Add Identity Provider page that you left open in part 1, in the **Required Identity Provider Entries** section, select **I have updated my SAML provider with the required information**.
2. In the SAML Settings section, select **File** or **URL**, depending on whether you copied the **App Federation Metadata URL** or downloaded the **Federation Metadata XML** in the previous part and provide the URL or drag and drop the file.
3. In the **Attribute Mapping** section, specify `email` in the **Email** field.

    > **Note:** This value must match the name associated with the claim that you added in the **Attributes & Claims** section in Entra in Part 2.
4. (Optional) In the **Branding** section, drag and drop the image files that you want to use for the **Site Logo**, **Site Icon**, **Site Background**.
5. Click **Add**.
6. (Optional) If needed, click **Add Identity Provider** to add more IdP configurations.
7. In the **Recovery Portal Servers** section, click **Download** to download the recovery portal installer for this configuration.

©2026 Tanium Inc. All Rights Reserved

(Other Identity Providers) Set up an identity provider and SSO

The recovery portal requires OIDC or SAML authentication with Service Provider (SP) initiated SSO. You can configure a recovery portal to use more than one IdP or authentication protocol and then use content sets to associate an IdP with a user group.

Prerequisites

Complete these prerequisites before you install the recovery portal server.

Configure the recovery portal

About this task

Note: You must have the Enforce Recovery Portal write permission to configure and edit these settings. For more information, see User role requirements on page 44.

1. From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. Click Settings and then click **Endpoint Encryption** > **Encryption Key Recovery Portal** > **Configure Identity Providers**.
2. Enter the following information for the recovery portal server:
    a. Enter the **Domain**. This value is the domain associated with this identity provider.
    b. Select the identity provider protocol: **SAML** or **OIDC**.
    c. If you do not want to use the default content set, Enforce, assign a **Content Set** for this IdP.

    Tip: You can use this content set to associate an IdP with a user group.

    d. Specify the **Recovery Application Domain**. This value is the domain for the recovery portal server web server.

    Note: This value is not stored, and therefore cannot later be edited in the IdP configuration. If this domain changes after the initial configuration, update the entry in your IdP.

©2026 Tanium Inc. All Rights Reserved

e. Configure the IdP settings:
SAML:

i. Update your IdP with the **SSO Redirect URL** that is in the **Required Identity Provider Entries** section.

You must update this entry before you provide your IdP metadata to Tanium. After you update your IdP with the SSO Redirect URL, select **I have updated my SAML provider with the required information**.

ii. In the **SAML Settings** section, select how you want to provide metadata (**File** or **URL**) and complete one of the following steps.

- For **File**: Upload the XML metadata file from your IdP.
- For **URL**: In the **URL** field, enter the URL for your IdP metadata.

iii. In the **Email** field, enter the name of the attribute from your IdP that contains the email address that you want users to use to sign in to the recovery portal. For example, enter `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`.

OIDC:

i. Update your IdP with the **Redirect URI** that is in the **Required Identity Provider Entries** section.

You must update this entry before you provide your IdP metadata to Tanium. After you update your IdP with the Redirect URI, select **I have updated my OIDC provider with the required information**.

ii. In the **OIDC Settings** section, enter the following information from your IdP.

OIDC settings

Client ID	A unique, public identifier from your identity provider.
Client Secret	A secret that is known only by the identity provider and the authorization server. It is often encrypted or hashed.
Issuer	The URL of the IdP that allows the API server to find the public signing keys for the IdP. Must begin with https://.

©2026 Tanium Inc. All Rights Reserved

iii. In the **Email** field, enter the name of the attribute from your IdP that contains the email address that you want users to use to sign in to the recovery portal. For example, enter `email`.

f. (Optional) In the **Branding** section, drag and drop the image files that you want to use for the **Site Logo**, **Site Icon**, **Site Background**.
g. Click **Add**.
h. (Optional) If needed, click **Add Identity Provider** to add more IdP configurations.

3. In the **Recovery Portal Servers** section, click **Download** to download the recovery portal installer for this configuration.

(Windows) Install and configure the recovery portal

1. Upload the recovery portal installation file that you downloaded in a previous section to a location on the server that hosts the recovery portal.
2. Change to the location where you uploaded tanium-key-recovery-portal.zip and extract the files.
3. Change to the directory where you extracted the files.
4. Copy the TLS certificates that you created for the server to the \<directory where you extracted the files>\configs directory on the recovery portal server. Create the configs folder in this location if it does not exist. If you have a trusted.crt certificate, put the trusted.crt certificate in the parent directory. The installation process copies this certificate to the \<directory where you extracted the files>\configs directory.
5. Run the Windows installation script, install.ps1, using a PowerShell prompt with administrator privileges: `./install.ps1`.
   As the script runs, you are prompted for the following details:

   a. Specify whether you are upgrading an existing installation.

   b. Specify the Tanium Server URL.

   c. Specify whether the Tanium Server is Cloud-based.

   d. Provide the API token that you created for use with the recovery portal server.

   e. Enter the DNS name or IP address of the recovery portal server.

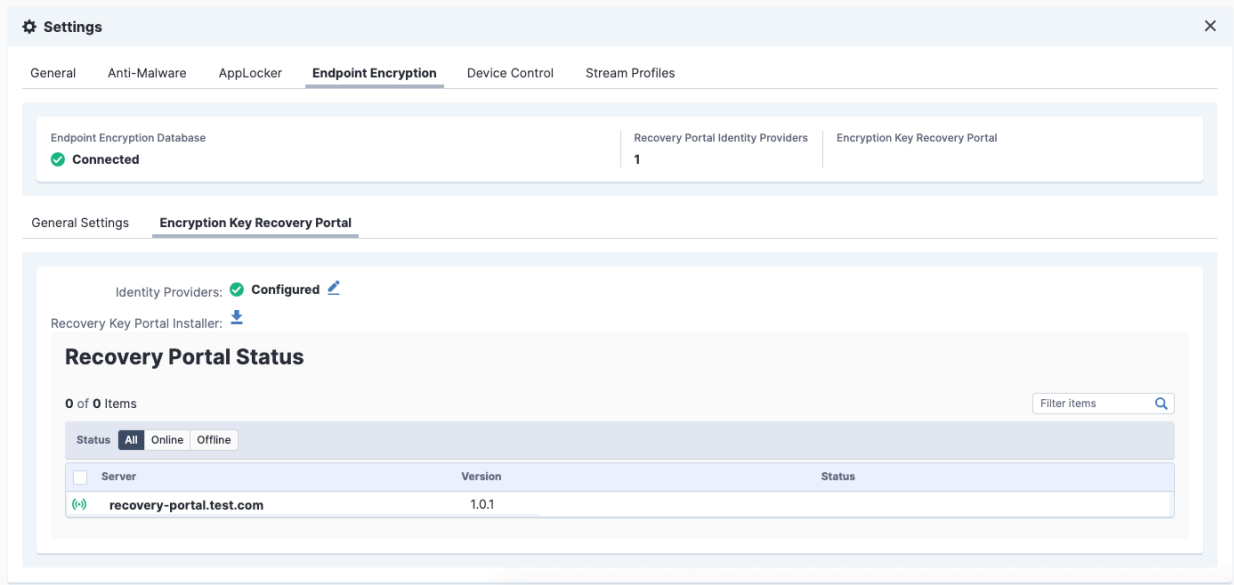
©2026 Tanium Inc. All Rights Reserved

f. Specify the service port. By default, this port is 443. If you are using a custom port, ensure that your IdP configuration uses the same port.

6. After the installation script runs, check the status of the recovery portal by opening the recovery portal from a web browser using the recovery portal hostname.

Note:

You can also check the status of the recovery portal in the Enforce settings: From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. Click Settings and then click **Endpoint Encryption** > **Recovery Portal**.



Important: The nameID format from the IdP application user name and the format for the recovery key viewer (**Enforce** > **Endpoint Encryption** > **Recovery Keys**) must match. For example, if user names in the recovery key viewer are formatted as firstname.lastname, then the IdP format must also be firstname.lastname. If the IdP application uses the format username@domain.com, then the recovery key viewer must use username@domain.com. If these formats do not match, users cannot view their keys.

(Linux) Install and configure the recovery portal

1. Upload the recovery portal installation file that you downloaded in a previous section to a location on the server that hosts the recovery portal.

©2026 Tanium Inc. All Rights Reserved

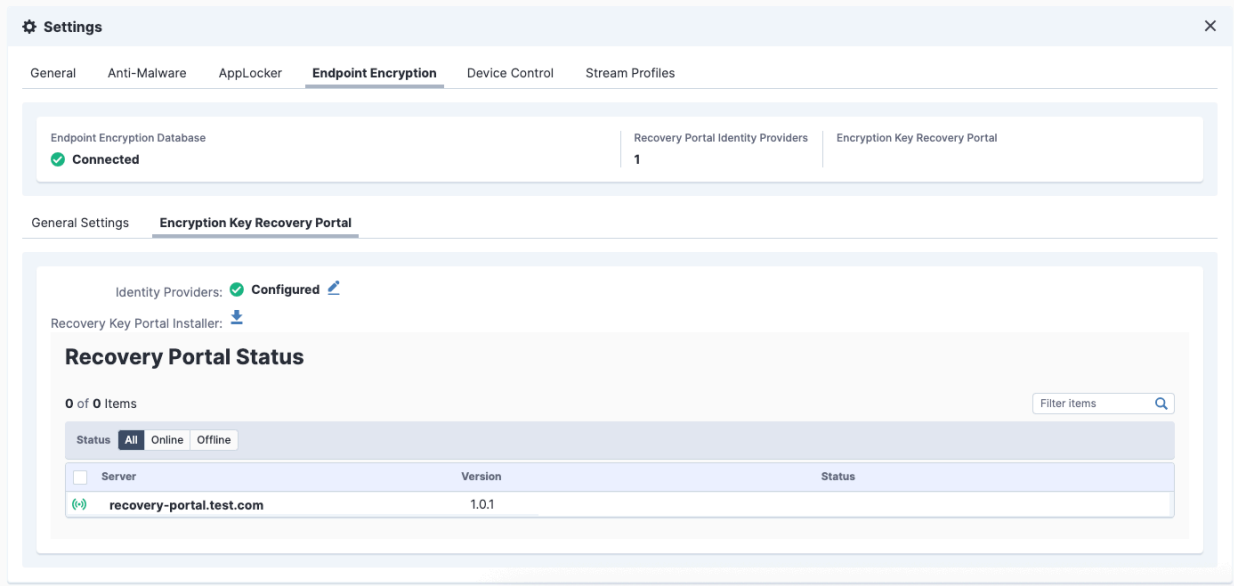
Best Practice: Use the /var/www/tanium-enforce-recovery-portal directory on the server.

2. Change to the location where you uploaded tanium-recovery-key-portal.zip and extract the files.
3. Change to the directory where you extracted the files.
4. Copy the TLS certificates that you created for the server to the /<directory where you extracted the files>/configs directory on the recovery portal server. Create the configs folder in this location if it does not exist. If you have a trusted.crt certificate, put the trusted.crt certificate in the parent directory. The installation process copies this certificate to the \<directory where you extracted the files>\configs directory.
5. Make the installation script executable: `chmod +x install.sh`.
6. Run the installation script using `sudo`: `sudo ./install.sh`.
   As the script runs, you are prompted for the following details:
   a. Specify whether you are upgrading an existing installation.
   b. Specify the Tanium Server URL.
   c. Specify whether the Tanium Server is Cloud-based.
   d. Provide the API token that you created for use with the recovery portal server.
   e. Enter the DNS name or IP address of the recovery portal server.
   f. Specify the service port. By default, this port is 443. If you are using a custom port, ensure that your IdP configuration uses the same port.
   g. Specify a user on the server running the recovery portal to use for running the service. For example, `root`.
   h. Specify a group on the server running the recovery portal to use for running the service. For example, `root`.
7. After the installation script runs, check the status of the recovery portal using the following command: `systemctl status tanium-key-recovery-portal.service`

©2026 Tanium Inc. All Rights Reserved

Note:

You can also check the status of the recovery portal in the Enforce settings: From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. Click Settings and then click **Endpoint Encryption** > **Recovery Portal**.



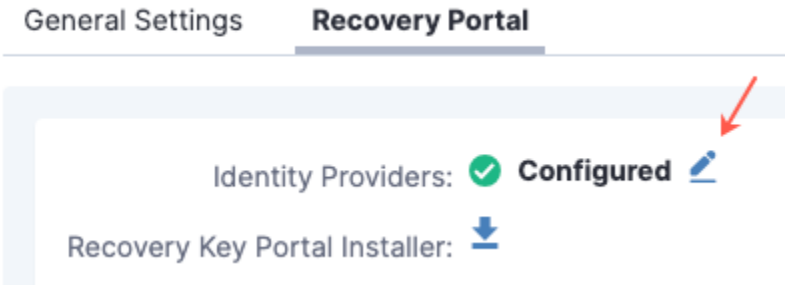
Important: The nameID format from the IdP application user name and the format for the recovery key viewer (**Enforce** > **Endpoint Encryption** > **Recovery Keys**) must match. For example, if user names in the recovery key viewer are formatted as firstname.lastname, then the IdP format must also be firstname.lastname. If the IdP application uses the format username@domain.com, then the recovery key viewer must use username@domain.com. If these formats do not match, users cannot view their keys.

Add or update IdP providers

From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. Click Settings and then click **Endpoint Encryption** > **Recovery Portal** > Edit Identity Providers. To edit an existing IdP, select an IdP and click Edit. To add a new Identity Provider, click **Add Identity Provider** and complete the steps in the Configure the recovery portal on page 252 section. After you are finished, download and install the recovery portal again. For more information, see (Windows) Install and configure the recovery portal on page 254 or (Linux) Install and configure the recovery portal on page 255.

Figure 13. Add an Identity Provider

©2026 Tanium Inc. All Rights Reserved



Replace the SSL certificates

Windows

About this task

Complete these steps on the machine hosting the recovery portal to replace expiring SSL certificates.

1. Stop the `tanium-key-recovery-portal` service.
2. Rename the existing certificates, which should be server.crt and server.key in the \<directory where you extracted the recovery portal installation files>\configs directory on the recovery portal server.
3. Copy the new certificates to the \<directory where you extracted the recovery portal installation files>\configs directory on the recovery portal server.
4. Start the `tanium-key-recovery-portal` service.

Linux

About this task

Complete these steps on the machine hosting the recovery portal to replace expiring SSL certificates.

1. Run this command to stop the recovery portal service: `sudo systemctl stop tanium-key-recovery-portal.service`.
2. Rename the existing certificates, which should be server.crt and server.key in the /<directory where you extracted the recovery portal installation files>/configs directory on the recovery portal server.
3. Copy the new certificates to the /<directory where you extracted the recovery portal

©2026 Tanium Inc. All Rights Reserved

installation files>/configs directory on the recovery portal server.

4. Run these commands to start the recovery portal service:
    a. `systemctl start tanium-key-recovery-portal.service`
    b. `systemctl status tanium-key-recovery-portal.service`

Update the recovery portal

Recovery portal functionality matches the associated Enforce version. When an Enforce release includes an update to the recovery portal, you must uninstall and reinstall the recovery portal using a configuration file generated from that version of Enforce. To determine whether a release requires an update to the recovery portal, check the Enforce release notes.

Uninstall the recovery portal

To uninstall the recovery portal, run the uninstall script that is located in the directory where you extracted the installation files:

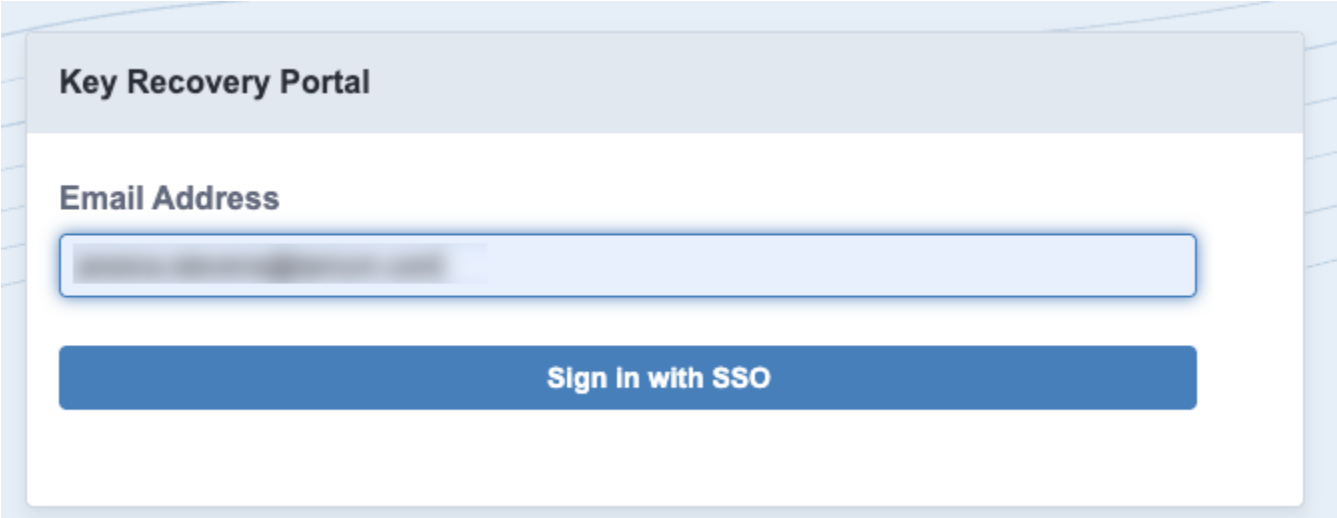
- (Linux) uninstall.sh
- (Windows) uninstall.ps1

Note: The portal certificates located in the configs directory are deleted when you uninstall the recovery portal. If you want to preserve these certificates, copy them to another location before uninstalling.

End user self-service workflow

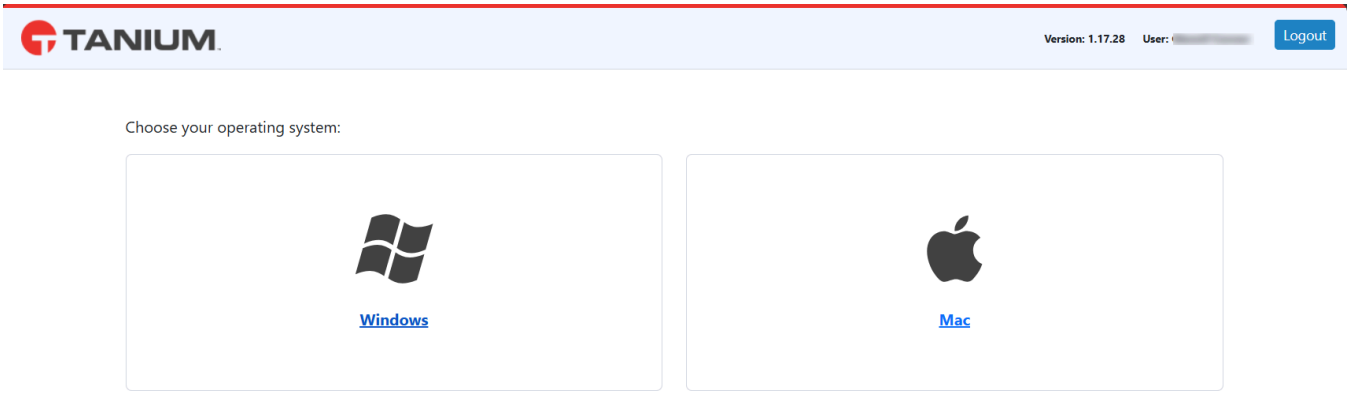
To retrieve their recovery key, end users access the recovery portal from a web browser. They enter an email address associated with an identity provider configured for the portal and click the **Sign in with SSO** link.
Figure 14. Recovery portal sign in

©2026 Tanium Inc. All Rights Reserved



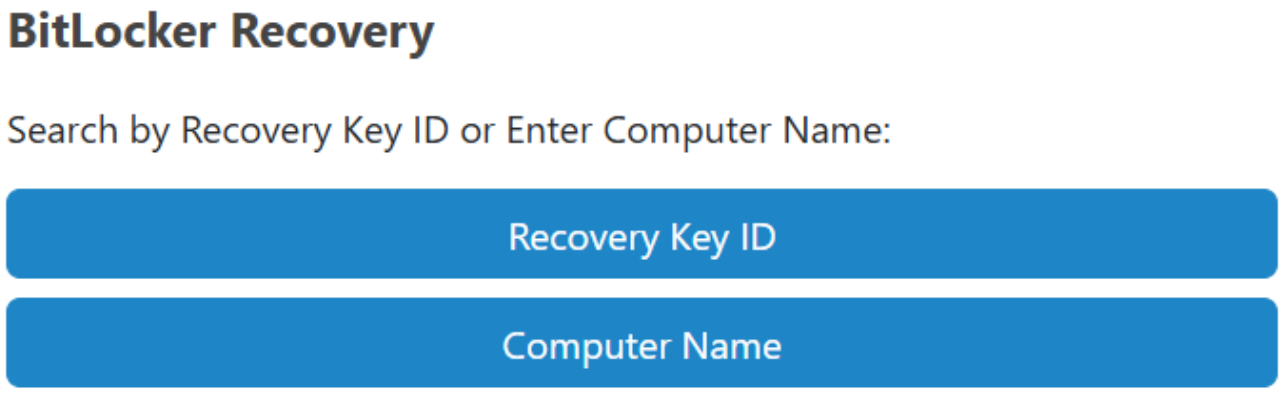
This action redirects them to the identity provider, where they enter their SSO credentials. After authentication, users are redirected back to the recovery portal and prompted to select their operating system.

Figure 15. Operating system selection



After they select their operating system, they can search for their recovery key using either the recovery key ID (which is typically provided on the operating system recovery page) or the computer name for the endpoint.

Figure 16. Recovery key search options



©2026 Tanium Inc. All Rights Reserved

After they retrieve their recovery key, they can provide the recovery key on the operating system recovery page to access the operating system.

Note: Users can only access their own recovery keys. Ownership is determined by the user who was signed in to the operating system when the key was generated.

©2026 Tanium Inc. All Rights Reserved

Reference: Creating a self-hosted database to store recovery keys

To use a self-hosted database to store recovery keys for endpoints with encryption management policy enforcements, you must create a database and service account in your database management system that meets the following requirements:

- An empty PostgreSQL or Microsoft SQL database with the required collation and encoding
- A service account with sufficient permissions
- The Tanium Server where Enforce is installed must be able to communicate with the database server
- (PostgreSQL) PEM (Privacy Enhanced Mail) or SSL certificates (CRT) to encrypt the connection to the database

Complete the setup in this order:

1. Create an empty database (this task is typically handled by a database administrator)
2. Create and configure the service account with the appropriate permissions
3. Configure the database connection in the encryption settings in the Enforce workbench

   After this connection is configured, the Enforce service runs migrations on the database to automatically create all necessary tables and schema objects.

©2026 Tanium Inc. All Rights Reserved

Best Practice: As a best practice, adhere to these security guidelines:

- Encrypt stored passwords (Enforce handles this automatically)
- Use Windows Authentication for Microsoft SQL when possible
- Use domain group membership for SQL server level login
- Restrict network access to the database server
- Regularly rotate credentials

Important: This section describes one way to set up this configuration. You might need to modify these steps and the suggested commands depending on your environment. Ensure that you test this configuration in a lab or test environment before you use it in a production environment. Consult the documentation for your database management system for detailed steps.

Step 1: Create the database

Important: You must create and configure this database before you configure the encryption settings in Enforce. Creation of the tables, indexes, and schema objects are operations that are handled by Enforce. Because database creation requires elevated permissions that must not be granted to a service account, Enforce does not create this database.

PostgreSQL

Run the following commands as a user with database administrator privileges:

```
-- Create the database
                CREATE DATABASE <database_name>
                  OWNER  <service_account>
 ENCODING 'UTF8'
                  LC_COLLATE = 'en_US.UTF-8'
                  LC_CTYPE = 'en_US.UTF-8'
                  TEMPLATE template0;

                -- Connect to the new database
                \c <database_name>
```

©2026 Tanium Inc. All Rights Reserved

Alternately, you can run this command from a command line: `createdb -O <service_account> -E UTF8 <database_name>`.

Microsoft SQL

Run the following commands as a user with database administrator privileges (typically `sa` or a member of the `sysadmin` role):

```
-- Create the database
                                CREATE DATABASE <database_name>
                                COLLATE SQL_Latin1_General_CP1_CI_AS;
                                -- Switch to the new database
                                USE <database_name>;
                                GO
```

Step 2: Configure the required permissions for the database service account

This service account is used to connect from Enforce to the database. The service account must have permissions to perform the following operations:

- Create and modify tables (for schema migrations)
- Insert, update, delete, and select data (for storing/retrieving keys)
- Manage sequences/identity columns
- Execute stored procedures/functions

PostgreSQL

For a self-hosted PostgreSQL database, the service account needs permissions configured in one of the following ways:

OPTION 1: SIMPLIFIED PERMISSIONS

This option provides more permissions to the service account than might be needed to use it with Enforce, but this method is simpler to set up and maintain.

©2026 Tanium Inc. All Rights Reserved

Database-Level Permissions

```
-- Connect to the database
                                GRANT CONNECT ON DATABASE <database_name> TO
<service_account>;
                                -- Grant all privileges on the database (recommended for
simplicity)GRANT ALL PRIVILEGES ON DATABASE <database_name> TO <service_account>;
```

Schema-Level Permissions

```
-- Full access to the public schema
                                GRANT ALL ON SCHEMA public TO <service_account>;
                                -- Allow creating new objects
                                GRANT CREATE ON SCHEMA public TO <service_account>;
```

Object-Level Permissions

```
-- Full access to all tables (for both migrations and operations)
                GRANT ALL ON ALL TABLES IN SCHEMA public TO <service_account>;

                -- Full access to all sequences (for auto-increment columns)
                        GRANT ALL ON ALL SEQUENCES IN SCHEMA public TO <service_account>;

                -- Execute access to all functions
                GRANT ALL ON ALL FUNCTIONS IN SCHEMA public TO <service_account>;

                -- Set default privileges for future objects
                ALTER DEFAULT PRIVILEGES IN SCHEMA public
                GRANT ALL ON TABLES TO <service_account>;

                ALTER DEFAULT PRIVILEGES IN SCHEMA public
                GRANT ALL ON SEQUENCES TO <service_account>;

                ALTER DEFAULT PRIVILEGES IN SCHEMA public
                GRANT ALL ON FUNCTIONS TO <service_account>;
```

OPTION 2: MORE RESTRICTIVE PERMISSIONS

This option provides only the specific permissions to the service account that are needed to use it with Enforce, but this method is more complex to set up and maintain.

```
-- Database
                GRANT CONNECT ON DATABASE <database_name> TO <service_account>;

                -- Schema
                GRANT USAGE, CREATE ON SCHEMA public TO <service_account>;
                -- Tables (DDL + DML)
                GRANT SELECT, INSERT, UPDATE, DELETE ON ALL TABLES IN SCHEMA public TO
<service_account>;
                ALTER DEFAULT PRIVILEGES IN SCHEMA public
                GRANT SELECT, INSERT, UPDATE, DELETE ON TABLES TO <service_account>;

                -- Sequences
                GRANT USAGE, SELECT, UPDATE ON ALL SEQUENCES IN SCHEMA public TO
<service_account>;
                ALTER DEFAULT PRIVILEGES IN SCHEMA public
                                                                GRANT USAGE, SELECT,
UPDATE ON SEQUENCES TO <service_account>;
```

©2026 Tanium Inc. All Rights Reserved

```
                                                                                -- Functions
                                                                                GRANT EXECUTE
ON ALL FUNCTIONS IN SCHEMA public TO <service_account>;
                                                                                        ALTER
DEFAULT PRIVILEGES IN SCHEMA public
                                                                                        GRANT
EXECUTE ON FUNCTIONS TO <service_account>;


-- DDL permissions (for migrations)

-- The account needs to be able to create/alter/drop tables

-- This typically requires ownership or superuser, so using a role:

CREATE ROLE enforce_admin;

GRANT ALL ON SCHEMA public TO enforce_admin;

GRANT enforce_admin TO <service_account>;
```

Microsoft SQL

For a self-hosted Microsoft SQL database, the service account needs permissions configured in one of the following ways:

OPTION 1: SIMPLIFIED PERMISSIONS (DATABASE OWNER SA AUTH)

```
USE <database_name>;
                                GO

                                -- Create login (if not using Windows Authentication)
                                CREATE LOGIN <service_account> WITH PASSWORD = '<password>';
                                                GO

                                                -- Create user in database
                                                CREATE USER <service_account> FOR LOGIN
<service_account>;
                                                                        GO


                                                                        -- Grant db_owner role
(allows everything)
                                                                        ALTER ROLE db_owner ADD
MEMBER <service_account>;
                                                                                GO
```

OPTION 2: BEST PRACTICE - WINDOWS AUTHENTICATION (DOMAIN ACCOUNT)

This method is typically the easiest to manage after it is configured. If necessary, you can use the more restrictive specific settings with Windows Authentication, which is described in the preceding section.

©2026 Tanium Inc. All Rights Reserved

```
-- Create the SQL Server Login for user or group (if using Windows Authentication)
 -- Domain security group membership is recommended best practice
 -- be sure to add the service account user to security group if leveraging an AD group
 CREATE LOGIN <service_account or group> FROM WINDOWS;
 GO

 USE <database_name>;
 GO

 -- Create user for domain account
 CREATE USER [DOMAIN\service_account] FOR LOGIN [DOMAIN\service_account];
 GO

 -- Grant db_owner or specific permissions
 ALTER ROLE db_owner ADD MEMBER [DOMAIN\service_account];
 GO
```

OPTION 3: MORE RESTRICTIVE SPECIFIC PERMISSIONS (SA AUTH)

```
-- First, create the login at server level
 CREATE LOGIN <service_account> WITH PASSWORD = '<password>';
 GO

 -- Switch to the database
 USE <database_name>;
 GO

 -- Create database user
 CREATE USER <service_account> FOR LOGIN <service_account>;
 GO

 -- CHOOSE ONE APPROACH BELOW (ROLES or EXPLICIT GRANTS, not both):
 _____________________________________
 -- APPROACH 1: Use built-in roles for simpler management (RECOMMENDED)
 ALTER ROLE db_ddladmin ADD MEMBER <service_account>;  -- DDL operations (create/alter
tables)
 ALTER ROLE db_datareader ADD MEMBER <service_account>; -- SELECT
 ALTER ROLE db_datawriter ADD MEMBER <service_account>; -- INSERT, UPDATE, DELETE
 GO


 _____________________________________
 -- APPROACH 2: Grant specific permissions individually (more granular control)
 -- If using this approach, COMMENT OUT the ALTER ROLE statements above
 -- Uncomment the following lines:

 -- DDL Permissions (for migrations - allows creating and modifying database objects)
 -- GRANT CREATE TABLE TO <service_account>;
 -- GRANT CREATE VIEW TO <service_account>;
 -- GRANT CREATE FUNCTION TO <service_account>;
 -- GRANT CREATE PROCEDURE TO <service_account>;
 -- GRANT ALTER ON SCHEMA::dbo TO <service_account>;
 -- GO

 -- DML Permissions (for operations - allows reading and writing data)
 -- GRANT SELECT ON SCHEMA::dbo TO <service_account>;
 -- GRANT INSERT ON SCHEMA::dbo TO <service_account>;
 -- GRANT UPDATE ON SCHEMA::dbo TO <service_account>;
 -- GRANT DELETE ON SCHEMA::dbo TO <service_account>;
 -- GRANT EXECUTE ON SCHEMA::dbo TO <service_account>;
 -- GO
```

©2026 Tanium Inc. All Rights Reserved

```
-- Additional permissions needed for full functionality
-- GRANT REFERENCES ON SCHEMA::dbo TO <service_account>;  -- For foreign keys
-- GRANT VIEW DEFINITION ON SCHEMA::dbo TO <service_account>;  -- View object definitions
-- GO

-- Set default permissions for objects created in the future
-- GRANT CONTROL ON SCHEMA::dbo TO <service_account>;  -- Allows altering tables after
creation
-- GO
```

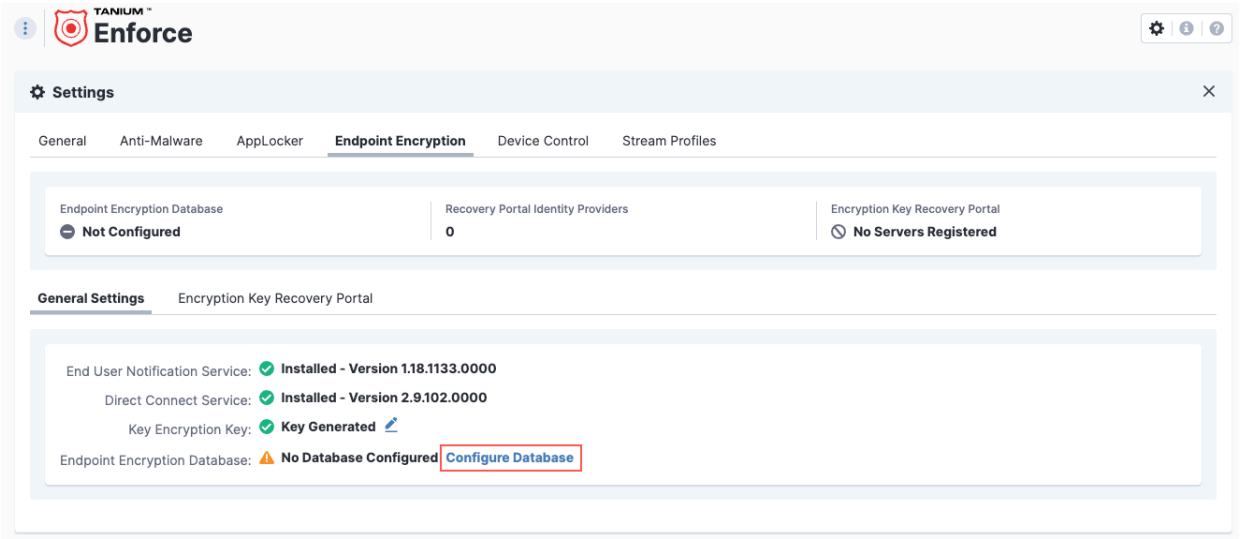
Step 3: Configure the database connection in Enforce

Configure Enforce to connect to the database that you configured in the preceding sections.

Note: Before you configure this connection, ensure that the other Endpoint Encryption requirements are complete. For more information, see Configure endpoint encryption on page 88.

1. From the Main menu, go to **Modules** > **Enforce** to open the **Enforce Overview** page. Click Settings.

2. On the **Endpoint Encryption** tab, click **Configure Database**.



3. Select **Self-Hosted**, select the appropriate **Database Server Type** (**PostgreSQL** or **Microsoft SQL**), and provide the details for the database and service account:

   PostgreSQL

   - **Host name**: Specify the name of your PostgreSQL server where you created the

©2026 Tanium Inc. All Rights Reserved

database and service account.

- **Port**: Specify the port for your database management server (default is 5432)
- **User name**: Specify the user name for the service_account that you configured.
- **Password**: Specify the password for the service account that you configured.
- **Database Name**: Specify the name of the empty database that you created.
- **Postgres Server CRT File**: Provide the SSL certificate required for encrypted connections (PEM or CRT format).

Microsoft SQL

- **Host name**: Specify the name of your Microsoft SQL server where you created the database and service account.
- **Port**: Specify the port for your database management server (default is 1433)
- **User name**: Specify the user name for the service_account that you configured.
- **Password**: Specify the password for the service account that you configured.
- **Domain**: If you are using Windows/NTLM Authentication (Domain Account), specify the domain for the account.
- **Database Name**: Specify the name of the empty database that you created.

©2026 Tanium Inc. All Rights Reserved