Tanium™ Enforce Limited Availability Release User Guide

Version 0.1.0

June 26, 2020

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://docs.tanium.com for the most current Tanium product documentation.

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

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

Tanium is committed to the highest accessibility standards to make interaction with Tanium software more intuitive and to accelerate the time to success. To ensure high accessibility standards, Tanium complies with the U.S. Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. We have conducted third-party accessibility assessments over the course of product development for many years, and most recently a comprehensive audit against the WCAG 2.1 / VPAT 2.3 standards for all major product modules was completed in September 2019. 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 best efforts to address any gaps quickly, as is feasible, given the severity of the issue and scope of the changes. These objectives are factored into the ongoing delivery schedule of features and releases with our existing resources.

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

Table of contents

Enforce overview

Tanium™ Enforce enables unified endpoint management and security by providing centralized policy management across operating system, application, and security for Windows and macOS environments regardless of the device's location - on premises, remote, or cloud.

Policy

To manage and secure endpoints across environments by providing control and visibility to all devices, configure a policy.

Policy setting

Specific settings and controls contained within a policy.

Enforcement

An enforcement occurs when a policy is successfully applied to a computer or user group. Policies can have one of these enforcement states:

Applied

A policy has been successfully enforced. All rules and configurations of the policy are in effect on the targeted endpoint.

Partially Applied

Some of the policy settings are enforced and some are not. This may be because similar policies with one or more duplicate settings are taking precedence. When settings are duplicated across different policies, the settings with the lowest number priority are applied and higher number priority settings are not applied. This results in some settings from a policy being enforced while other settings in the same policy are not enforced.

Note: Five is the maximum number of not applied or partially applied settings that can be displayed in the status column.

Not Applied

The policy is not in effect on the endpoint. This may be due to all settings in the policy being duplicates of lower number priority settings in other policies. It could also be due to a timing issue if the policy has been sent to the endpoint but not yet executed on that endpoint. See the enforcement state reason for more information.

Unsupported

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

Error

All known and unknown errors.

Integration with other Tanium products

Trends

Enforce has built in integration with Tanium™ Trends for additional reporting of related data. The Trends initial gallery features boards that provide data visualization of Enforce concepts.

For more information about how to import the Trends boards that are provided by Performance, see Tanium Trends User Guide: Importing the initial gallery.

Enforce requirements

Review the requirements before you install and use Enforce.

Tanium dependencies

In addition to a license for the Protect module, make sure that your environment meets the following requirements.

Component	Requirement
Tanium™ Client	7.2.314.3211 or later

Tanium™ as a Service

Enforce runs on Tanium as a Service. Module installation and upgrades are handled by the service.

Endpoints

Enforce policies support the following endpoint operating systems:

Windows Machine policy

- Windows 7 and later
- Windows Server 2008 R2 and later

Host and network security requirements

Specific processes are needed to run Enforce.

Security exclusions

If security software is in use in the environment to monitor and block unknown host system processes, your security administrator must create exclusions to allow the Tanium processes to run without interference.

Table 1: Enforce security exclusions

Target Device	Process	Notes
Module Server	*<Tanium Module Server>*\services\enforce-service\7za.exe	
	<Tanium Module Server>\services\enforce-service\node.exe	
Windows x86 endpoints	*<Tanium Client>* \Tools\StdUtils\7za.exe	
	<Tanium Client> \Tools\Enforce\devcon32.exe	
	<Tanium Client >\Python27\TPython.exe	(7.2.*x* clients)
	<Tanium Client >\Python38\TPython.exe	(7.4.*x* clients)
	<Tanium Client>\Python38*.dll	(7.4.*x* clients)
	<Tanium Client>\TaniumCX.exe	

Target Device	Process	Notes
Windows x64 endpoints	<*Tanium Client*>\Tools\StdUtils\7za.exe	
	<*Tanium Client*>\Tools\Enforce\devcon64.exe	
	<*Tanium Client*>\Python27\TPython.exe	(7.2.*x* clients)
	<*Tanium Client*>\Python38\TPython.exe	(7.4.*x* clients)
	<*Tanium Client*>\Python38*.dll	(7.4.*x* clients)
	<*Tanium Client*>\TaniumCX.exe	
macOS endpoints	<*Tanium Client*>/python27/python	(7.2.*x* clients)
	<*Tanium Client*>/python38/python	(7.4.*x* clients)
	<*Tanium Client*>/TaniumCX	
Linux x86 and x64 endpoints	<*Tanium Client*>/python27/python	(7.2.*x* clients)
	<*Tanium Client*>/python38/python	(7.4.*x* clients)
	<*Tanium Client*>/TaniumCX	

User role requirements

Table 2: Enforce Global user role permissions

Permission	Enforce Administrator	Enforce Operator	Enforce Service Account	Enforce Policy Administrator (Global)	Enforce Policy User (Global)	Enforce Policy Viewer (Global)
Enforce Operator Read, edit, and delete most Enforce objects (except edit access to Enforce settings)	✓[2]	✓	✓[2]	✗	✗	✗
Enforce Administrator Unrestricted access to Enforce	✓	✗	✓	✗	✗	✗
Enforce Settings Read Globally all Enforce settings	✓[2]	✓[2]	✓[2]	✗	✗	✗
Enforce Settings Write Globally edit all Enforce settings	✓[2]	✓[2]	✓[2]	✗	✗	✗

Permission	Enforce Administrator	Enforce Operator	Enforce Service Account	Enforce Policy Administrator (Global)	Enforce Policy User (Global)	Enforce Policy Viewer (Global)
Enforce Operator Settings Read Globally read most Enforce settings	✓[2]	✓[2]	✓[2]	✗	✗	✗
Enforce Operator Settings Write Globally edit most Enforce settings	✓[2]	✓[2]	✓[2]	✗	✗	✗
Show Enforce[1] View the Enforce workbench	✓[2]	✓[2]	✓	✓	✓	✓
Enforce Policy Read Read Enforce policies	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓
Enforce Policy Write Edit Enforce policies	✓[2]	✓[2]	✓[2]	✓	✓	✗

Permission	Enforce Administrator	Enforce Operator	Enforce Service Account	Enforce Policy Administrator (Global)	Enforce Policy User (Global)	Enforce Policy Viewer (Global)
Enforce Policy Prioritize Edit Enforce policy priorities	✓[2]	✓[2]	✓[2]	✓	✗	✗
Enforce Create Enforcement Enforce policies	✓[2]	✓[2]	✓[2]	✓	✓	✗
Enforce Edit Any Enforcement Edit available policy enforcements. Users always have access to enforcements that they created.	✓[2]	✓[2]	✓[2]	✓	✗	✗
Enforce Managed Definitions Read Read managed definitions	✓[2]	✓[2]	✗	✗	✗	✗

Permission	Enforce Administrator	Enforce Operator	Enforce Service Account	Enforce Policy Administrator (Global)	Enforce Policy User (Global)	Enforce Policy Viewer (Global)
Enforce Managed Definitions Write Edit managed definitions	✓[2]	✓[2]	✗	✗	✗	✗
Enforce Disk Encryption Recovery Keys - Read Read recovery keys for disk encryption	✓[2]	✓[2]	✗	✗	✗	✗
Enforce Disk Encryption Recovery Keys - Delete Delete recovery keys for disk encryption	✓[2]	✓[2]	✗	✗	✗	✗
Enforce Policy Template Read Read policy templates in given content sets	✓[2]	✓[2]	✓[2]	✓[2]	✓	✓

Permission	Enforce Administrator	Enforce Operator	Enforce Service Account	Enforce Policy Administrator (Global)	Enforce Policy User (Global)	Enforce Policy Viewer (Global)
Enforce Policy Template Write Edit policy templates in given content sets	✓[2]	✓[2]	✓[2]	✓	✗	✗
Enforce Policy Template Delete Delete policy templates in given content sets	✓[2]	✓[2]	✓[2]	✓	✗	✗
Enforce Policy Type Read Read policy types in given content sets	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓
Enforce Policy Type Write Edit policy types in given content sets	✓[2]	✓[2]	✓[2]	✓	✓	✗

Permission	Enforce Administrator	Enforce Operator	Enforce Service Account	Enforce Policy Administrator (Global)	Enforce Policy User (Global)	Enforce Policy Viewer (Global)
Enforce Policy Type Delete Delete policy types in given content sets	✓[2]	✓[2]	✓[2]	✓	✗	✗
Enforce Reports Read Read reports in given content sets	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓
Enforce Reports Write Edit reports in given content sets	✓[2]	✓[2]	✓[2]	✓	✓	✗
Enforce Reports Delete Delete reports in given content sets	✓[2]	✓[2]	✓[2]	✓	✓	✗

Permission	Enforce Administrator	Enforce Operator	Enforce Service Account	Enforce Policy Administrator (Global)	Enforce Policy User (Global)	Enforce Policy Viewer (Global)
Trends API Board Write Create, edit, delete, and configure boards, sections, and panels for specified content sets	✗	✗	✓[2]	✗	✗	✗
Trends API Board Read View boards, sections, and panels for specified content sets	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]
Trends API Source Write Create, edit, and delete sources for specified content set	✗	✗	✓[2]	✗	✗	✗

Permission	Enforce Administrator	Enforce Operator	Enforce Service Account	Enforce Policy Administrator (Global)	Enforce Policy User (Global)	Enforce Policy Viewer (Global)
Trends API Source Read View and list sources for specified content sets.	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]
Trends Data Read Run data queries against sources	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]
Trends Import Import from file or gallery	✗	✗	✓[2]	✗	✗	✗

Permission	Enforce Administrator	Enforce Operator	Enforce Service Account	Enforce Policy Administrator (Global)	Enforce Policy User (Global)	Enforce Policy Viewer (Global)
Trends Integration Service Account Provides access for module service accounts to read and write data, and to define sources and boards	✗	✗	✓	✗	✗	✗

[1] To install Enforce, you must have the reserved role of Administrator.

[2] Denotes a provided permission.

Table 3: Global Template (Permissions restricted by operating system content sets: Windows, macOS, or Linux) user role permissions

Permission	Enforce Policy Administrator (Template)	Enforce Policy User (Template)	Enforce Policy Viewer (Template)	Enforce Recovery Key Administrator (Template)	Enforce Recovery Key User (Template)	Enforce Recovery Key Viewer (Template)
Enforce Operator Read, edit, and delete most Enforce objects (except edit access to Enforce settings)	✗	✗	✗	✗	✗	✗
Enforce Administrator Unrestricted access to Enforce	✗	✗	✗	✗	✗	✗
Enforce Settings Read Globally read all Enforce settings	✗	✗	✗	✗	✗	✗

Permission	Enforce Policy Administrator (Template)	Enforce Policy User (Template)	Enforce Policy Viewer (Template)	Enforce Recovery Key Administrator (Template)	Enforce Recovery Key User (Template)	Enforce Recovery Key Viewer (Template)
Enforce Settings Write Globally edit all Enforce settings	✗	✗	✗	✗	✗	✗
Enforce Operator Settings Read Globally read most Enforce settings	✗	✗	✗	✗	✗	✗
Enforce Operator Settings Write Globally edit most Enforce settings	✗	✗	✗	✗	✗	✗

Permission	Enforce Policy Administrator (Template)	Enforce Policy User (Template)	Enforce Policy Viewer (Template)	Enforce Recovery Key Administrator (Template)	Enforce Recovery Key User (Template)	Enforce Recovery Key Viewer (Template)
Show Enforce[1] View the Enforce workbench	✓	✓	✓	✓	✓	✓
Enforce Policy Read Read the Enforce policy in given content sets	✓	✓	✓	✗	✗	✗
Enforce Policy Write Edit the Enforce policy in given content sets	✓	✓	✗	✗	✗	✗

Permission	Enforce Policy Administrator (Template)	Enforce Policy User (Template)	Enforce Policy Viewer (Template)	Enforce Recovery Key Administrator (Template)	Enforce Recovery Key User (Template)	Enforce Recovery Key Viewer (Template)
Enforce Create Enforcement Enforce policies in given content sets	✓	✓	✗	✗	✗	✗
Enforce Edit Any Enforcement Edit available policy enforcements. Users always have access to enforcements that they created	✓	✗	✗	✗	✗	✗

Permission	Enforce Policy Administrator (Template)	Enforce Policy User (Template)	Enforce Policy Viewer (Template)	Enforce Recovery Key Administrator (Template)	Enforce Recovery Key User (Template)	Enforce Recovery Key Viewer (Template)
Enforce Managed Definitions Read Read managed definitions in given content sets	✗	✗	✗	✗	✗	✗
Enforce Managed Definitions Write Edit managed definitions in given content sets	✗	✗	✗	✗	✗	✗

Permission	Enforce Policy Administrator (Template)	Enforce Policy User (Template)	Enforce Policy Viewer (Template)	Enforce Recovery Key Administrator (Template)	Enforce Recovery Key User (Template)	Enforce Recovery Key Viewer (Template)
Enforce Disk Encryption Recovery Keys - Read Read recovery keys for disk encryption in given content sets	✗	✗	✗	✓	✓	✓
Enforce Disk Encryption Recovery Keys - Delete Delete recovery keys for disk encryption in given content sets	✗	✗	✗	✓	✓	✗

Permission	Enforce Policy Administrator (Template)	Enforce Policy User (Template)	Enforce Policy Viewer (Template)	Enforce Recovery Key Administrator (Template)	Enforce Recovery Key User (Template)	Enforce Recovery Key Viewer (Template)
Enforce Policy Template Read Read policy templates in given content sets	✓	✓	✓	✗	✗	✗
Enforce Policy Template Write Edit policy templates in given content sets	✓	✗	✗	✗	✗	✗
Enforce Policy Template Delete Delete policy templates in given content sets	✓	✗	✗	✗	✗	✗

Permission	Enforce Policy Administrator (Template)	Enforce Policy User (Template)	Enforce Policy Viewer (Template)	Enforce Recovery Key Administrator (Template)	Enforce Recovery Key User (Template)	Enforce Recovery Key Viewer (Template)
Enforce Policy Type Read Read policy types in given content sets	✓	✓	✓	✗	✗	✗
Enforce Policy Type Write Edit policy types in given content sets	✓	✗	✗	✗	✗	✗
Enforce Policy Type Delete Delete policy types in given content sets	✓	✗	✗	✗	✗	✗

Permission	Enforce Policy Administrator (Template)	Enforce Policy User (Template)	Enforce Policy Viewer (Template)	Enforce Recovery Key Administrator (Template)	Enforce Recovery Key User (Template)	Enforce Recovery Key Viewer (Template)
Enforce Reports Read Read reports in given content sets	✓	✓[2]	✓	✗	✗	✗
Enforce Reports Write Edit reports in given content sets	✓	✓[2]	✓	✗	✗	✗
Enforce Reports Delete Delete reports in given content sets	✓	✓[2]	✓	✗	✗	✗

Permission	Enforce Policy Administrator (Template)	Enforce Policy User (Template)	Enforce Policy Viewer (Template)	Enforce Recovery Key Administrator (Template)	Enforce Recovery Key User (Template)	Enforce Recovery Key Viewer (Template)
Trends API Board Write Create, edit, delete, and configure boards, sections, and panels for specified content sets	✗	✗	✗	✗	✗	✗
Trends API Board Read View boards, sections, and panels for specified content sets	✓[2]	✓[2]	✓[2]	✗	✗	✗

Permission	Enforce Policy Administrator (Template)	Enforce Policy User (Template)	Enforce Policy Viewer (Template)	Enforce Recovery Key Administrator (Template)	Enforce Recovery Key User (Template)	Enforce Recovery Key Viewer (Template)
Trends API Source Write Create, edit, and delete sources for specified content sets	✗	✗	✗	✗	✗	✗
Trends API Source Read View and list sources for specified content sets	✓[2]	✓[2]	✓[2]	✗	✗	✗
Trends Data Read Run data queries against sources	✓[2]	✓[2]	✓[2]	✗	✗	✗

Permission	Enforce Policy Administrator (Template)	Enforce Policy User (Template)	Enforce Policy Viewer (Template)	Enforce Recovery Key Administrator (Template)	Enforce Recovery Key User (Template)	Enforce Recovery Key Viewer (Template)
Trends Import Import from file or gallery	⊗	⊗	⊗	⊗	⊗	⊗
Trends Integration Service Account Provides access for module service accounts to read and write data, and to define sources and boards	⊗	⊗	⊗	⊗	⊗	⊗

[1] To install Enforce, you must have the reserved role of Administrator.

[2] Denotes a provided permission.

Table 4: 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	✗	✗	✗	✓	✓	✗	✓
Content Set	✓	✓	✓	✗	✗	✓	✗

Table 5: Provided Enforce Advanced user role permissions

Permission	Enforce Administrator	Enforce Operator	Enforce Service Account	Enforce Policy Administrator	Enforce Policy User	Enforce Policy Viewer
Read Sensor	✓	✓	✓	✓	✓	✓
Read Plugin	✓[1]	✓[1]	✓[1]	✓[1]	✓[1]	✓[1]
Execute Plugin	✓	✓	✓	✓	✓	✓

[1] Denotes a provided permission.

For more information and descriptions of content sets and permissions, see the Tanium Core Platform User Guide: Users and user groups.

Getting started

> **IMPORTANT:** For Tanium as a Service, module installation and upgrades are handled by the service.

Perform the following tasks to get started with Enforce.

Configure action group

By default, the action group is set to `All Computers`. You can update the action group if needed in the Administration section of Tanium Console. See Tanium Platform User Guide: Managing Computer Groups.

Enforce tools

All policies and sensors require Enforce tools to be deployed to the endpoint. Enforce tools are automatically deployed to all endpoints in the action group.

Next steps

Create Policies

Configure Windows administrative policies for computer groups. See Creating policies on page 34.

Enforcements

After policies are configured, create enforcements to apply them to endpoints. See Enforcing policies on page 36.

Creating policies

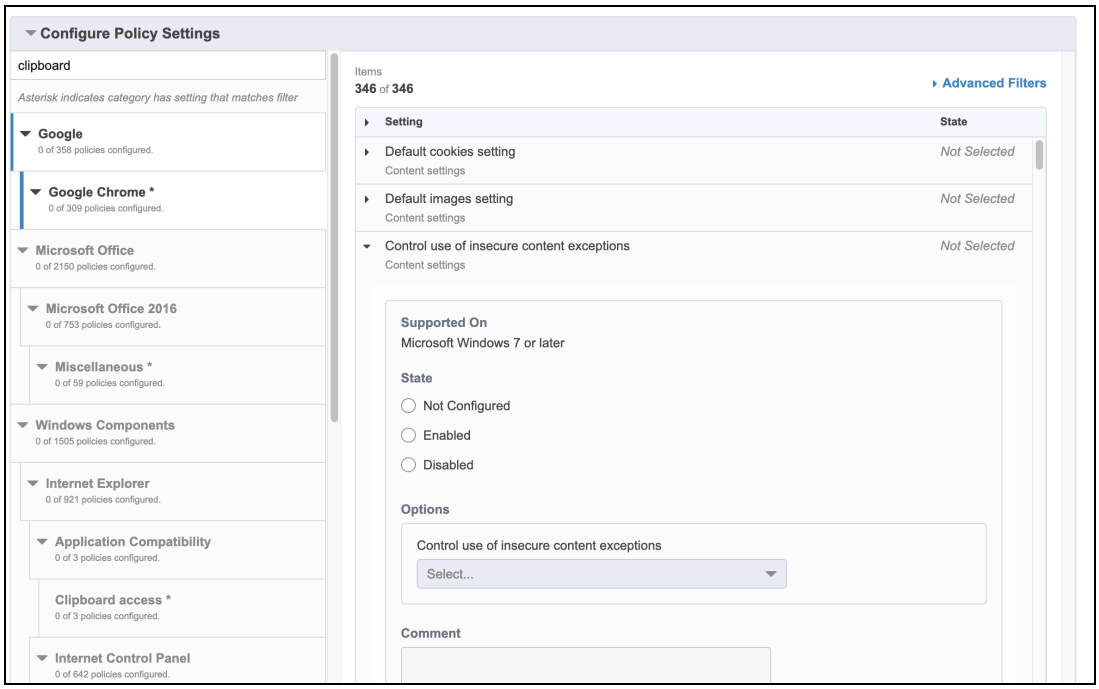
You can create the following policies in Enforce.

Windows Machine

Windows machine policies target machine-based ADMX (Active Directory administrative templates) group policy objects on Windows systems. Use Windows machine policies to apply consistent rules to Windows devices regardless of the logged in user.

Create a Windows machine policy

1. From the **Enforce** menu, go to **Policies** and click the **Create Policy** button.
2. In the **Summary** section,
   - Enter a **Name** and **Description** for the policy.
   - From the **Policy Type** drop-down, select **Windows Machine**. Windows machine policies target machine-based ADMX (Active Directory administrative templates) group policy objects.
3. In the **Configure Policy Settings** section, select a category on the left side, and the available settings for that category appear on the right side.
   - **Search Categories and Settings**— There is a search field at the top of the categories column on the left side. Type the name of the category or setting you are looking for and an asterisk appears to the right of all items that contain the search criteria.



- Some high-level categories for Windows Machine policies are listed in the Windows Machine Policy Categories Example on page 35 table below.

Table 6: Windows Machine Policy Categories Example

Category (top level)	Overview
Control Panel	Includes display, personalization, regional and language options, and printers.
Google Chrome	Includes cookies, Javascript, and image settings.
Microsoft Office	Included Window security restrictions and storage of user passwords.
Network	Includes network connections.
Printers	Includes prevention of security issues with print driver installation.
Start Menu and Task Bar	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, and edge UI.

> **Note:** For the full list of policy settings included in Windows administrative template files, see Microsoft: Group Policy Settings Reference for Windows and Windows Server.

4. When you configure a policy, the following settings are available: **Not Configured**, **Enabled**, and **Disabled**. Both **Not Configured** and **Disabled** use default Microsoft settings. When you change the state to **Enabled**, you can enter your own settings. Refer to Microsoft for a detailed explanation of each state.

   > **Note:** There is help text from Microsoft for each Policy Setting in the Enforce UI page for that setting.

5. Click the **Save** button after you configure a policy setting.
6. Click the **Create** button at the bottom of the page once all settings for the policy are complete. The policy now appears in the **Policies** list in the **Machines** tab.

You can enforce a policy from three different places in the UI.

- The Enforcements page
- The Policy list page
- The Policy details page

See Enforcing policies on page 36 for details.

Enforcing policies

Create enforcements

You can create an enforcement from the policy list page, the policy details page, or the enforcements page.

1. From the **Enforce** menu, click **Policies**.
2. To display a policy, click the **Machine** tab.
3. Click the Enforce icon for the policy.
4. Enter a **Name** for the enforcement.

5. Select one or more groups or users:
    - For a **Machine Policy**, you can use computer groups that you define in the Administration section of Tanium Console. See Tanium Platform User Guide: Managing Computer Groups.
        - Click **Computer Group** and type the first few letters of the group. **Individual Computers**, paste a comma-separated list of computer names into the available field. This list must be no longer than 50 computers.
6. Click **Create**. Click **Yes** to confirm.

Note: To un-enforce or remove a policy from an endpoint, delete the enforcement.

Create enforcements from policy details

1. From the **Enforce** menu, click **Policies**.
2. To display a policy, click the **Machine** tab.
3. Click the policy to be enforced. This takes you to the details page for that policy.
4. Click the **Enforce** button. Refer to Create enforcements on page 36 for the remaining instructions.

Enforce policies from enforcements

1. From the **Enforce** menu, click **Enforcements**.
2. To display a policy, click the **Machine** tab.
3. Click the **Create Enforcement** button. Refer to Create enforcements on page 36 for the remaining instructions.

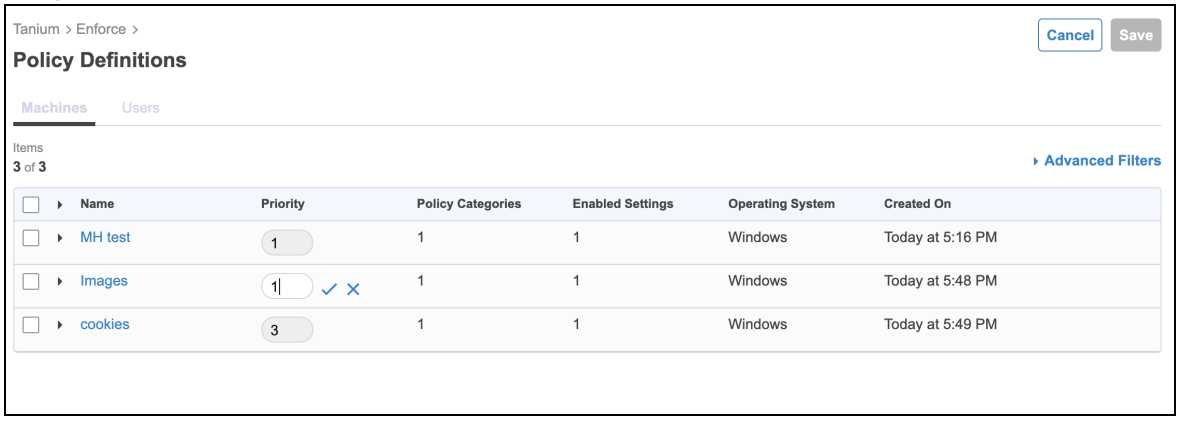
Prioritize policies

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. Duplicate settings of a higher priority number are not applied.

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**.

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

1. Navigate to **Policies** and click the **Prioritize** button to make the priority fields editable.
2. Click the priority field for the policy you want to change and enter a new priority number. Click the ✓ to accept the change or the ✕ to undo the change. When you click the check mark, the priority number for all policies update based on your change.



3. Click **Save** to keep the new priorities or cancel to undo them and revert back to the original priorities.

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 to 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 on which you do not have permissions, you lose the permissions to edit that policy.

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.

Troubleshooting Enforce

To collect and send information to Tanium for troubleshooting, collect logs and other relevant information.

Collect logs

The information is saved as a ZIP file that you can download with your browser.

1. From the Enforce home page, click Help ❓, then the **Troubleshooting** tab.
2. Click **Collect**.
   A `Enforce-support.[timestamp].zip` file downloads to the local download directory.
3. Attach the ZIP file to your Tanium Support case form or send it to your TAM.

Tanium Enforce maintains logging information in the `Enforce.log` file in the `\Program Files\Tanium\Tanium Module Server\services\Enforce` directory.

Change endpoint status report settings

Click **Settings** and go to **General** to change the following settings that govern how you can use Enforce to interact with endpoints:

Question Completion Percentage

This setting specifies what percentage of endpoints must respond to the question before the question is considered complete. If questions take a long time to complete in your Tanium environment, you might want to lower the percentage in this setting. By default, **Question Completion Percentage** is set to 85%.

Reissue Action Interval

This setting specifies how often Enforce enforcement actions are reissued. By default, enforcement actions are reissued every hour. The minimum allowed value for this field is 10 minutes.

Distribute Over Time

This setting controls whether endpoints apply 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. The default setting for **Distribute Over Time** is **0** where all enforcements are deployed at once.

Enforce sensors

The following Enforce sensors are available:

Enforce - Machine Policy Status

Given a list of Policy Id numbers, reports the enforcement status of each.

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.

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 Items

Specifically for small scale diagnostics. Returns a list of all policy items to be applied on endpoints, including those that will not apply because they are superseded by a duplicate setting.