Tanium Zero Trust User Guide

2026H2 Semiannual Release

Version 2.1

November 17, 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 7
- Rules 7
- Events 9
- Supported IAM providers 9
- Interoperability with other Tanium products 10

Getting started with Zero Trust 11

Requirements 13
- Core platform dependencies 13
- Solution dependencies 13
  - Tanium recommended installation 13
  - Import specific solutions 13
  - Required dependencies 14
  - Feature-specific dependencies 14
- Tanium™ Module Server 14
- Endpoints 15
  - Supported internet protocols 15
  - Supported operating systems 15
- Host and network security requirements 16
  - Ports for Zero Trust communication 16
  - Security exclusions 16
    - Zero Trust server exclusions 17
  - Internet URLs 17
- User role requirements 17

Installing 20
- Before you begin 20
- Import Zero Trust 20
- Upgrade Zero Trust 21

©2026 Tanium Inc. All Rights Reserved

Verify Zero Trust version 21

Configuring 22
Configure IAM provider settings 22
Configure Entra ID 22
Configure Zero Trust 26
Set up Zero Trust users 27

Managing rules 29
View rules 29
Create a rule 31
Prioritize rules 34
Take ownership of a rule 35
Edit a rule 36
Clone a rule 37
Delete a rule 37

Auditing events 40
Review data sent to your IAM provider 40
View audit log 41
Microsoft Entra ID 41
Send logs through Connect 42
Create a connection 43

Maintaining 45
Zero Trust monthly maintenance 45

Troubleshooting 46
Collect logs 46
Manually modify endpoint attribute 46
Endpoint does not appear in the audit log 47
Entra ID log shows endpoint does not exist 48
Zero Trust is unable to connect to Microsoft Entra ID 49
Unable to preview rule 50
Not authorized to modify endpoint attribute 50
Cannot apply audit rule 51
Extension attribute is also applied by another rule 51
Audit log export errors 52

©2026 Tanium Inc. All Rights Reserved

Cannot view the audit log 52
Rule and audit log statuses 53
"Failed due to shutdown" error in audit log 53
"Update failed due to tenant change" error in audit log 54
Rule or configuration operation fails 55
Not authorized to view this page 55
Uninstall Zero Trust 56
Contact Tanium Support 56

©2026 Tanium Inc. All Rights Reserved

Zero Trust overview

With Zero Trust, support your zero trust architecture by sending trust data for Tanium Client managed endpoints to your Identity and Access Management (IAM) provider.

Use Zero Trust to:

- Strengthen your security capabilities through a zero trust architecture.
- Identify potentially risky endpoints in your environment.
- Receive alerts when events occur that result in data sent to your IAM provider.
- Audit zero trust events through Tanium Console.

Zero Trust supports Microsoft Entra ID. With Entra ID, you can enable conditional access to Microsoft products through extension attributes.

Best Practice: Zero Trust provides data regarding risky or misconfigured endpoints that can be used to limit access to support other authentication and authorization flows. Zero Trust is intended to be used as a defense-in-depth measure and should not be used as a primary access control.

Rules

In Zero Trust, a rule defines a set of targeted endpoints for which to send trust data from Tanium to your IAM provider.

Zero Trust continuously monitors endpoints that are targeted by rules. A rule triggers when an event occurs that causes an endpoint to match the rule, such as if an endpoint has not restarted within the last 7 days, if an endpoint is missing a critical patch, or if an endpoint has a known vulnerability. When a rule triggers, Tanium applies or removes trust data to send to your IAM provider.

Targeted endpoints

For each rule, you can select one or more sensors that targeted endpoints must match to be subject

©2026 Tanium Inc. All Rights Reserved

to the rule.

After you create a rule, Zero Trust immediately begins to monitor endpoints for the rule conditions. Rules are subject to the computer management group permissions of the user who owns the rule. The initial owner of a rule is the user who creates the rule. A rule can target different endpoints depending on who created the rule. If you want a rule to target different endpoints, you can change the owner of the rule to a user with the necessary computer management group permissions.

- For more information about how to change the owner of a rule, see Take ownership of a rule on page 35.
- For more information about computer management group permissions, see Tanium Console User Guide: Manage computer group assignments for a user.

Sensor data is sourced through Tanium Data Service.

Tanium Data Service stores sensor results for endpoints when you issue a question. After you register sensors for collection, the service queries all managed endpoints to collect the results of those sensors and stores the data. To keep the results current, Tanium Data Service periodically reissues questions that contain the registered sensors.

- For more information about Tanium Data Service, see Tanium Interact User Guide: Managing Tanium Data Service.
- For more information about required permissions to register sensors, see Tanium Interact User Guide: User role requirements.

Modes

Rules run in either *enforcement mode* or *audit mode*.

- **Enforcement mode**: When an event triggers the rule, Zero Trust logs the event and sends data to the IAM provider. Rules in enforcement mode are sometimes referred to as *enforce rules*.
- **Audit mode**: When an event triggers a rule, Zero Trust logs the event but does not send data to the IAM provider. Rules in audit mode are sometimes referred to as *audit rules*. Use this mode to test rules.

©2026 Tanium Inc. All Rights Reserved

Prioritization

An event might cause an endpoint to match more than one rule. An event can match multiple rules, but only one rule can trigger for each extension attribute for each endpoint.

For example, consider an event that matches three rules: **Rule 1**, **Rule 2**, and **Rule 3**. **Rule 1** assigns a string to extension attribute 1, **Rule 2** assigns a string to extension attribute 3, and **Rule 3** removes a string from extension attribute 3. The rules are prioritized in order: **Rule 1** is priority 1, **Rule 2** is priority 2, and **Rule 3** is priority 3. When the event occurs, **Rule 1** always triggers for the endpoint, because that rule has no conflicts with other rules (and it is also the highest priority rule). However, **Rule 2** and **Rule 3** affect the same extension attribute, and thus only **Rule 2** triggers due to the order of priority.

You can prioritize rules to determine which rule triggers when an event occurs. For more information, see Prioritize rules on page 34.

Events

An event occurs when an endpoint matches a rule, or when a user manually updates an extension attribute for an endpoint. Zero Trust triggers the rule and applies or removes the trust data that is specified in the rule. Zero Trust maintains a log of events that you can view in the Zero Trust workbench.

When an event occurs that matches a rule in audit mode, Zero Trust checks for an existing audit log entry that matches the same rule, endpoint, and trust data. If a match is found with a rule that is in audit mode, Zero Trust replaces the older entry with the new event entry. By upserting entries for audit rules, Zero Trust minimizes the size of the logs while maintaining the latest data.



Note: Zero Trust does not upsert entries for rules in enforcement mode.

For more information, see Auditing events on page 40.

Supported IAM providers

Zero Trust supports conditional access for endpoints through Microsoft Entra ID.

©2026 Tanium Inc. All Rights Reserved

Note: Microsoft Entra ID was previously known as Microsoft Azure Active Directory or Microsoft Azure AD.

Microsoft Entra ID

You can configure Zero Trust to send trust data for your endpoints through *extension attributes* to Entra ID. Extension attributes are properties that you can set for each endpoint. An *extension attribute string* is the value that you assign to an extension attribute. Through Entra ID, you can manage 15 extension attributes for each endpoint. When an endpoint matches a configured rule, Zero Trust either applies an extension attribute string to an extension attribute for the endpoint, or Zero Trust removes the extension attribute string from an extension attribute. If the mode for the rule is set to **Enforcement**, Zero Trust sends the updated extension attribute to Entra ID.

To use Zero Trust to monitor endpoints in Entra ID, endpoints must be managed by Tanium and registered in Entra ID with device IDs.

To use the extension attribute as a Conditional Access condition, the endpoint must also meet the additional requirement described in Requirements: Endpoints on page 15.

For more information about extension attributes and device IDs, see:

- Microsoft Azure documentation: Using extension attributes
- Microsoft Entra documentation: What is a device identity?

Interoperability with other Tanium products

Connect

Configure a Tanium™ Connect destination to export audit entries outside of Tanium. For more information, see Send logs through Connect on page 42.

©2026 Tanium Inc. All Rights Reserved

Getting started with Zero Trust

Follow these steps to configure and use Zero Trust.

Step 1: Install and configure Zero Trust and your IAM provider

Install Zero Trust, and then configure Zero Trust and your IAM provider. For more information, see Installing Zero Trust on page 20 and Configuring Zero Trust on page 22.

Step 2: Grant Zero Trust permissions

Grant permissions to users to use Zero Trust. Users with the **Administrator** reserved role have access by default. For more information, see User role requirements on page 17 and Set up Zero Trust users on page 27.

Step 3: (Optional) Register sensors for collection in Tanium Data Service

When you configure targeting for a rule, Zero Trust uses sensor data that Tanium Data Service collects. For more information about which sensors are registered and how to register additional sensors, see Tanium Interact User Guide: Managing Tanium Data Service.

Step 4: Create a test rule

Create a rule in audit mode for testing. For more information, see Create a rule on page 31.

Step 5: Test and monitor the rule

Trigger an event that runs the rule, and then monitor the audit log to verify the entry appears as expected. For more information, see View audit log on page 41.

©2026 Tanium Inc. All Rights Reserved

Step 6: Create rules in enforcement mode

Create one or more rules in enforcement mode, and then monitor the audit log to ensure the rules trigger as expected. For more information, see Create a rule on page 31 and View audit log on page 41.

©2026 Tanium Inc. All Rights Reserved

Zero Trust requirements

Review the requirements before you install and use Zero Trust.

Core platform dependencies

Make sure that your environment meets the following requirements:

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

Solution dependencies

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

Note: Some Zero Trust 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 Zero Trust requires.

Tanium recommended installation

If you select **Tanium Recommended Installation** when you import Zero Trust, 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

©2026 Tanium Inc. All Rights Reserved

If you select only Zero Trust 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 Zero Trust, the server automatically updates those dependencies to the latest available versions.

Required dependencies

Zero Trust has the following required dependencies:

- Tanium™ Core Content
    - Core Content requires Tanium™ Client Management. For more information, see Tanium Client Management dependencies.
- Tanium™ Core AD Query Content
- Tanium™ Data Service (TDS)
- Tanium™ Enforce
- Tanium™ Interact
- Tanium™ RDB Service
- Tanium™ Secrets Service

Feature-specific dependencies

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

- Tanium™ Connect is required to export audit data

Tanium™ Module Server

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

For more information about Module Server sizing in a Windows deployment, see Tanium Core

©2026 Tanium Inc. All Rights Reserved

Platform User Guide for Windows Deployments: Host system sizing guidelines.

Endpoints

For an extension attribute to be usable as a Conditional Access condition, each endpoint must also satisfy one of the following:

- Managed by Microsoft Intune
- Marked as compliant in Microsoft Entra ID
- Microsoft Entra hybrid joined

The compliant path for an endpoint that is not managed by Intune is available only through Microsoft Intune Partner Compliance management, which supports Android, iOS/iPadOS, and macOS only. For Windows endpoints, the available paths are Intune enrollment or Microsoft Entra hybrid join.

Intune enrollment alone is sufficient; an endpoint that is managed by Intune does not also need to be marked as compliant for the extension attribute to be evaluated.

For more information, see Microsoft Entra documentation: Filter for devices as a condition in Conditional Access policy.

Supported internet protocols

Zero Trust supports IPv4 and IPv6 addresses.

Supported operating systems

The following endpoint operating systems are supported with Zero Trust.

Supported operating systems for Zero Trust

Operating System	Version	Notes
Windows	Same as Tanium Client support.	For more information, see Tanium Client Management User Guide: Client version and host system requirements .

©2026 Tanium Inc. All Rights Reserved

Operating System	Version	Notes
macOS	Same as Tanium Client support.	For more information, see Tanium Client Management User Guide: Client version and host system requirements .
Linux	Ubuntu Desktop 22.04 and later Ubuntu Desktop 22.04 LTS and later	Endpoints must meet Entra ID requirements. For more information, see Microsoft: Get started with Linux enrollment .

Host and network security requirements

Specific ports and processes are needed to run Zero Trust.

Ports for Zero Trust communication

Required ports for Zero Trust communication

Source	Destination	Port	Protocol	Purpose
Module Server	Module Server (loopback)	17612	TCP	Internal purposes, not externally accessible
	Microsoft Entra ID	443	TCP	Send trust data to Entra ID

Security exclusions

If antivirus (AV) or other security software is in use in the environment to monitor and block unknown host system processes, Tanium requires that a security administrator create exclusions to allow the Tanium processes to run without interference. This software can include security applications that are included with an endpoint operating system, such as fapolicyd on some Linux distributions, or Microsoft Defender on Windows. The configuration of these exclusions varies depending on the security software.

For more information about security exclusions to define across Tanium, see Reference: Endpoint security exclusions. For Windows-based Tanium Core Platform deployments, see Tanium Core Platform Server security exclusions.

©2026 Tanium Inc. All Rights Reserved

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.

ZERO TRUST SERVER EXCLUSIONS

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

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	*<Module Server>* \services\zero-trust-service\TaniumZeroTrustService.exe

Internet URLs

If security software is deployed in the environment to monitor and block unknown URLs, allow the following URLs on the Tanium Module Server:

Zero Trust internet URLs

IAM provider	URL
Microsoft Entra ID	https://graph.microsoft.com/v1.0/devices
	https://login.microsoftonline.com/

User role requirements

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

- Table 5. Zero Trust solution permissions on page 18
- Zero Trust administration, platform content, and global permissions on page 19: The solution permissions automatically provide some of these permissions.

To review a summary of the predefined roles, see Set up Zero Trust users on page 27.

Some Zero Trust 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 Zero Trust. If you create custom roles for Zero Trust users, be sure to assign all the solution permissions and content set permissions

©2026 Tanium Inc. All Rights Reserved

that are required for Zero Trust functionality. If you are not sure which permissions are required for a custom role, view the permissions of the predefined roles. For more information, see the following sections of the Tanium Console User Guide:

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

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

Zero Trust solution permissions

Permission	Zero Trust Operator	Zero Trust User
Zero Trust View the Zero Trust workbench	✓ SHOW OPERATOR USER	✓ SHOW USER
Zero Trust Azure Audit View all Entra ID audit log entries, regardless of computer management group permissions	✓ READ	✗
Zero Trust Azure Config View and edit Entra ID configuration in Zero Trust	✓ READ WRITE	✓ READ
Zero Trust Azure Current Audit View the current Entra ID log	✓ READ	✓ READ
Zero Trust Azure Manual Rules Manually apply Entra ID rules	✓ WRITE	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Zero Trust Operator	Zero Trust User
Zero Trust Azure Rules View and edit Entra ID rules	READ WRITE	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 .		

Zero Trust platform content permissions

Permission	Zero Trust Operator [1]	Zero Trust User [1]
Filter Group	READ	READ
Plugin	READ EXECUTE	READ EXECUTE
Sensor	READ	READ
To view the content sets to which the platform content permissions apply, see View effective role permissions .		

©2026 Tanium Inc. All Rights Reserved

Installing Zero Trust

About this task

Use the Tanium Console **Solutions** page to install Zero Trust.

Before you begin

- Read the release notes.
- Review the Zero Trust requirements on page 13.
- Assign the correct roles to users for Zero Trust. Review the User role requirements on page 17.
    - To import the Zero Trust solution, you must be assigned the Administrator reserved role.
    - To configure the Zero Trust action group, you must be assigned the Administrator reserved role, Content Administrator reserved role, or a role that has the **Action Group** write permission.

Import Zero Trust

About this task

Perform the following steps to install the Zero Trust solution on the Tanium Server.

> **Note:** If you have multiple Tanium Servers in an active-active configuration, you only need to perform these steps on one Tanium Server.

1. Sign in to Tanium Console with an account that has the **Administrator** reserved role.
2. From the Main menu, go to **Administration** > **Configuration** > **Solutions**.

©2026 Tanium Inc. All Rights Reserved

3. In the **Content** section, select the checkbox for **Zero Trust** and click **Import**.

   Tip: If you need to install any prerequisite Tanium solutions, select the corresponding checkboxes for those solutions as well.

4. Review the content to import and click **Begin Install**.

Result

Other Tanium solutions are required for Zero Trust to function (required dependencies) or for specific Zero Trust features to work (feature-specific dependencies).

Upgrade Zero Trust

For the steps to upgrade Zero Trust, see Tanium Console User Guide: Managing Tanium solutions. After the upgrade, verify that the correct version is installed. For more information, see Verify Zero Trust version on page 21.

Verify Zero Trust version

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

1. Refresh your browser.
2. From the Main menu, go to **Shared Services** > **Zero Trust**.
3. To display version information, click Info .

©2026 Tanium Inc. All Rights Reserved

Configuring Zero Trust

No default settings are configured for Zero Trust.

Configure IAM provider settings

Set up Zero Trust to send data to your IAM provider.

Configure Entra ID

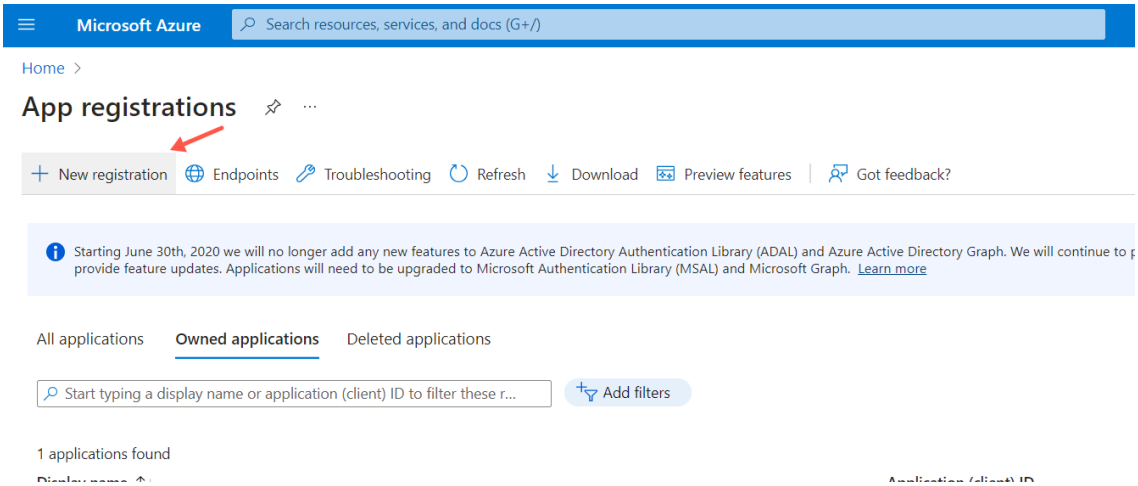
About this task

In the Microsoft Azure portal, create an app registration, configure the application permission, and then create an Azure client ID and secret for Zero Trust to use for authentication.

1. Register Zero Trust with Entra ID.

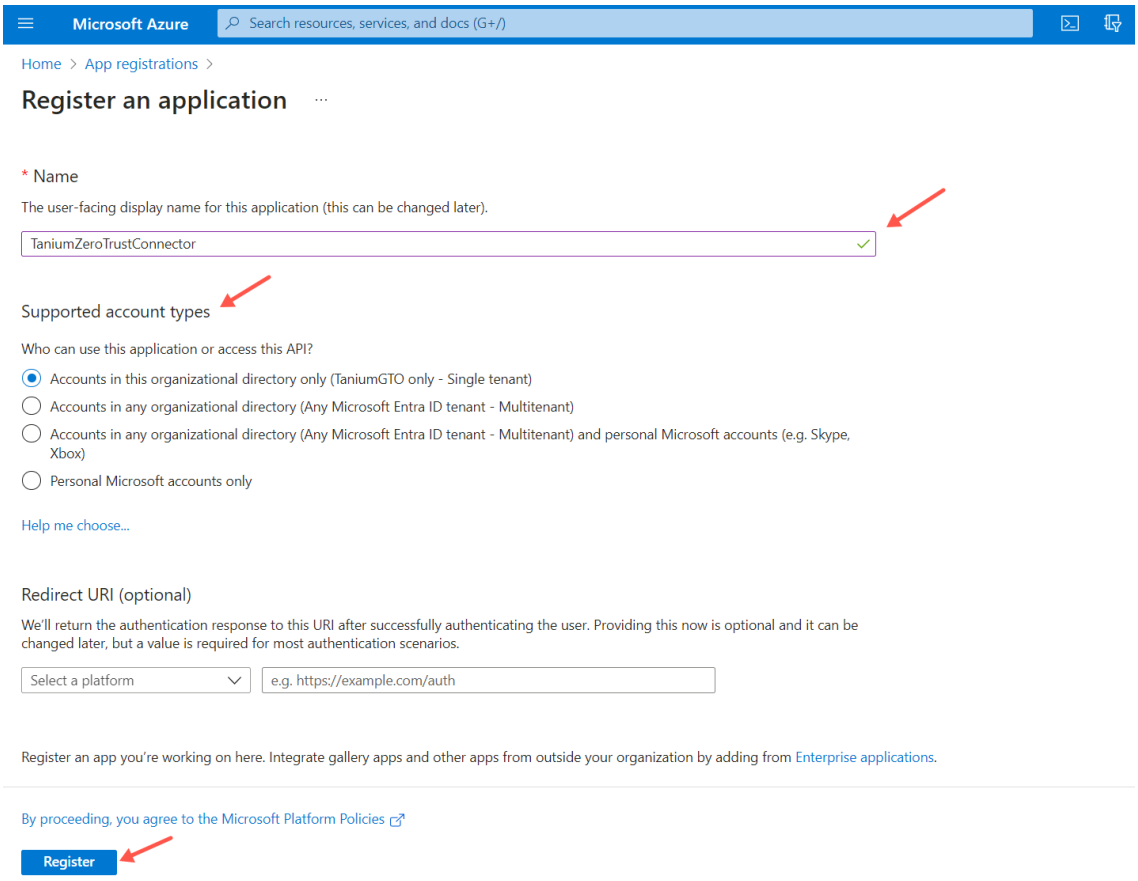
   Note: For more information, see Microsoft Entra documentation: Quickstart: Register an application. You do not need to configure the optional **Redirect URI**.

   a. Go to **App registrations** and click **New Registration**.

   b. Enter a name for the Zero Trust registration, and then select the supported account types. When finished, click **Register**.

©2026 Tanium Inc. All Rights Reserved

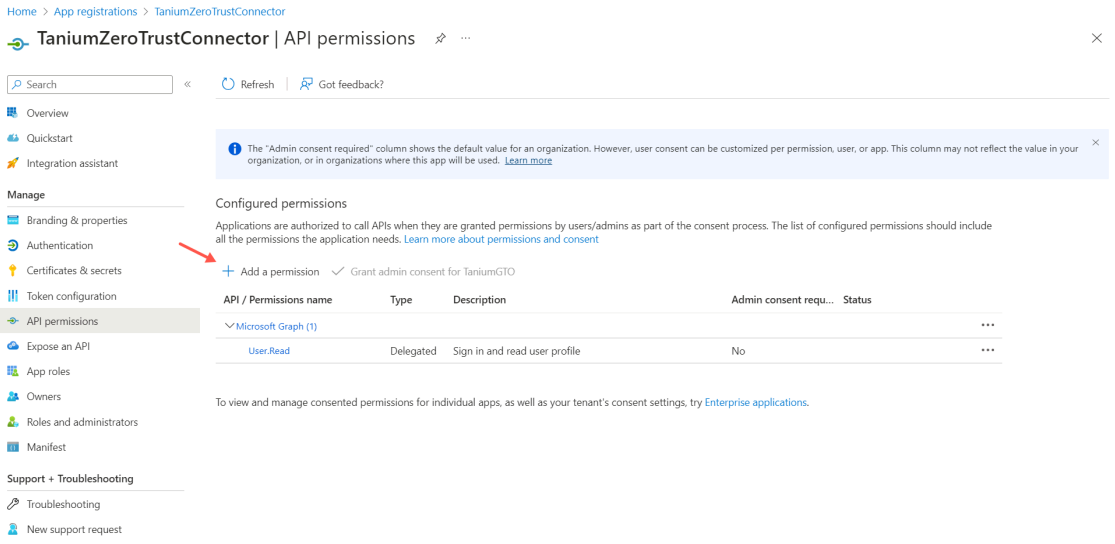


c. Record the **Application (client) ID** for the new registration.

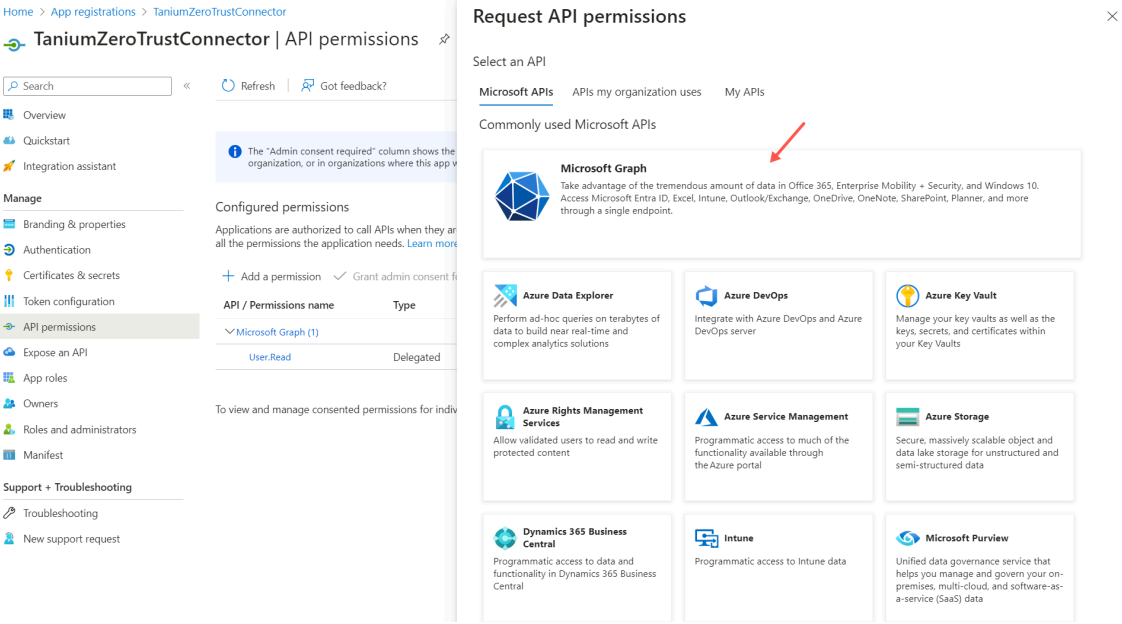


2. Grant the necessary API permission.
    a. From the **App registration**, go to **API permissions** and select **Add a permission**.

©2026 Tanium Inc. All Rights Reserved

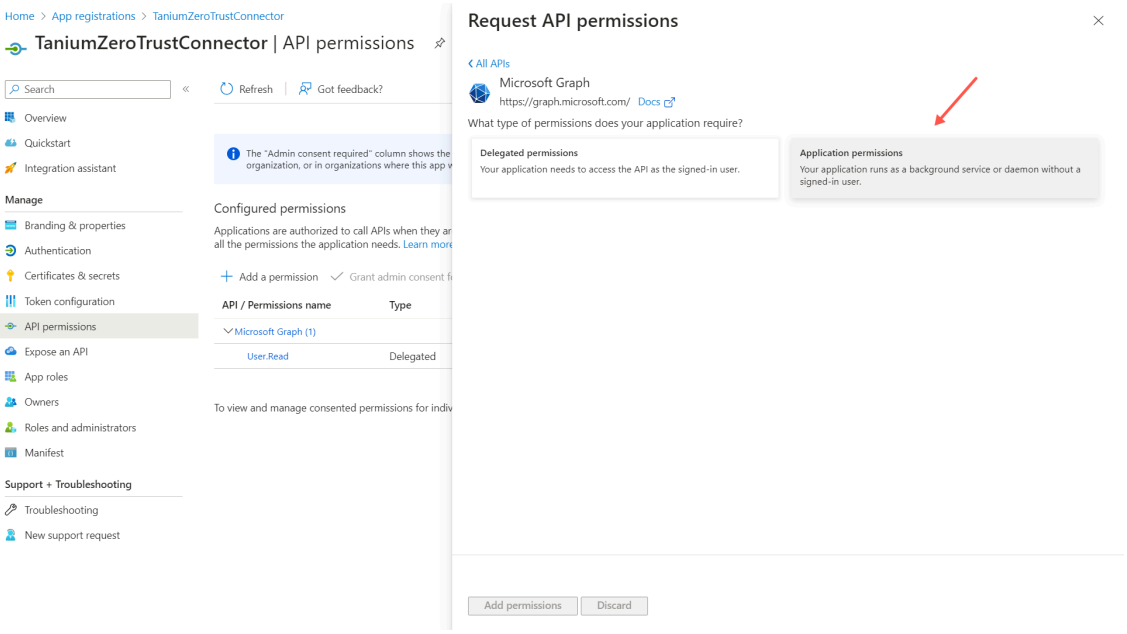


b. From the **Request API permissions** panel, select **Microsoft Graph**.

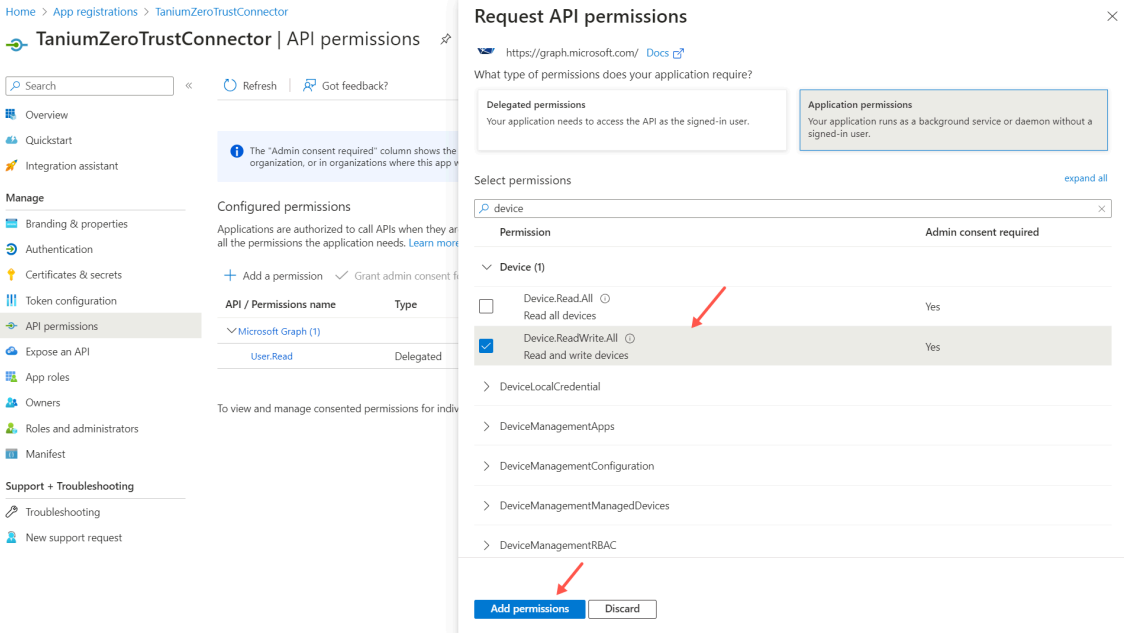


c. Select **Application permissions**.

©2026 Tanium Inc. All Rights Reserved



d. Select the **Device.ReadWrite.All** permission and then click **Add permissions**.



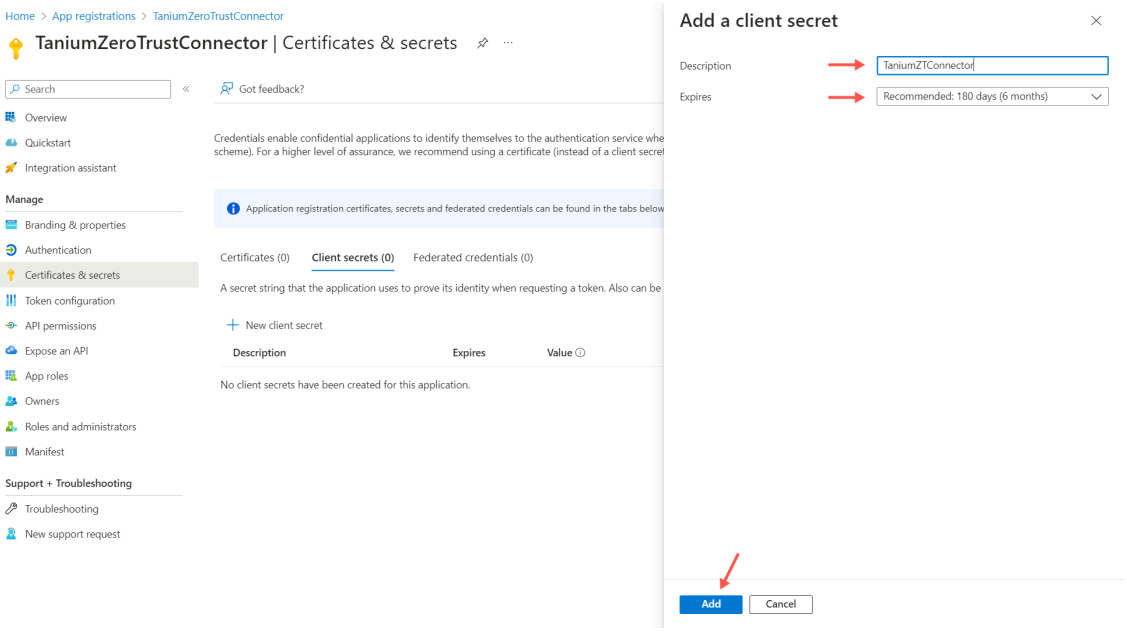
3. If administrator consent is required, make sure your Entra ID admin provides consent before you proceed to the next step.

4. Add a client secret.
   For more information, see Microsoft Entra documentation: Quickstart: Add a client secret

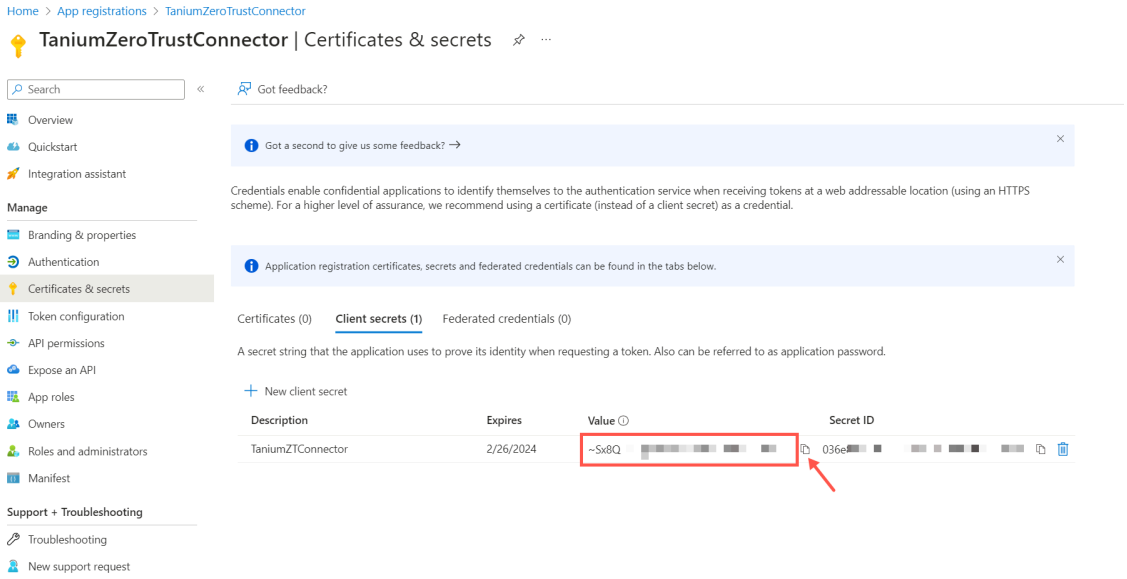
> **Note:** Zero Trust also supports the use of certificates.

   a. From the **App registration**, go to **Certificates & secrets**.
   b. Enter a description for the client secret, select an expiration date, and then click **Add**.

©2026 Tanium Inc. All Rights Reserved



c. After you add the client secret, record the **Value** for the client secret and save it to a secure location. You cannot see this value again after you leave this page.



Configure Zero Trust

1. From the Main menu, go to **Shared Services** > **Zero Trust**. Click Settings ⚙.
2. Enter the following information:

©2026 Tanium Inc. All Rights Reserved

Zero Trust configuration settings

Option	Description
Microsoft Entra ID Tenant ID	The tenant ID for your Entra ID.
Microsoft Entra ID App ID	The application (client) ID of the application that interacts with Entra ID through the Microsoft Graph API.
Authentication	Select the authentication type for your Entra ID. • If you select **Secret**, enter the value of the client secret in the **Client Secret** field. • If you select **Certificate**, upload the client certificate and enter the certificate password. **Note:** If you change any settings for your IAM provider, you must re-enter the certificate password.

3. Click **Save**.

Note: You can edit or delete the configuration at any time. If you delete the configuration or enter credentials that are not valid, any rules that send data to the provider continue to run but will fail when sending data.

Set up Zero Trust users

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

About this task

For more information about the specific permissions for each role, see User role requirements on page 17.

Important: On installation, Zero Trust creates a Zero Trust user to automatically manage the Zero Trust service account. Do not edit or delete the Zero Trust user.

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

©2026 Tanium Inc. All Rights Reserved

Zero Trust Operator

Assign the **Zero Trust Operator** role to users who manage the configuration and deployment of zero trust rules. Users with the **Zero Trust Operator** role can view all audit log entries, regardless of their assigned computer management group permissions.

Zero Trust User

Assign the **Zero Trust User** role to users who need to view rules.



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

©2026 Tanium Inc. All Rights Reserved

Managing rules

Use rules to determine which endpoints to target and what information to send to your IAM provider.

View rules

About this task

Users with the **Zero Trust Microsoft Entra ID Rules** Read permission can view all rules in Zero Trust.

1. From the Main menu, go to **Shared Services** > **Zero Trust** > **Rules**.
2. (Optional) Use the following filter options to find specific rules if the list is long. The list shows only the rules that match all the filters that you specify.

   #### Rule filter options

Option	Description
Select mode	Use the **Mode** buttons to toggle between showing **All** rules, **Audit** rules, and **Enforce** rules.
Select action	Use the **Action** buttons to toggle between **All** rules, rules that **Apply** an extension attribute, and rules that **Remove** an extension attribute.
Select extension attribute number	Select a value for **Extension Attribute #** to only show rules that remove or apply a value to the extension attribute.
Select extension attribute	Select a value for **Extension Attribute** to only show rules that remove or apply the extension attribute.
Filter items	Enter an alphanumeric string to match text in any column.
Filter by field	Expand **Filters** and specify any additional filters. You can filter by **Name**, **Creator**, and **Owner**.
Sort by column	Click any column header to sort the list of rules by that column.

3. (Optional) Take action on a rule. The following actions are available:

©2026 Tanium Inc. All Rights Reserved

Available actions for the rule list

Option	Description
Create rule	Click **Create Rule** .
Edit rule	Select the checkbox next to the rule that you want to edit and then click Edit .
Prioritize rules	An event can trigger more than one rule for an endpoint, but only one rule for each extension attribute. When an endpoint matches multiple rules that affect the same extension attribute, the rule with the highest priority determines which result is sent to the zero trust service. Rule priority is in descending order, with 1 the highest priority. To prioritize rules, click **Prioritize** , drag the rules to change the order of evaluation, and then click **Save** . For more information, see Prioritize rules on page 34 .
Refresh list	Click **Refresh** .
Export rules	To retrieve a list of the rules, apply any filters and then click **Export** . You have the following options: • Select **Export to CSV** to download the list of rules as a CSV file. • Select **Copy to clipboard** to copy the list of rules in CSV format to your clipboard. The exported list contains the rules that match the filters you set.
Take ownership	Rules run against the endpoints allowed by the computer management group permissions for the owner of the rule. To change ownership of a rule to yourself, select the checkbox next to the rule, click **Actions** > **Take Ownership** , and then click **Save** .
Clone rule	Select the checkbox next to the rule and then click **Actions** > **Clone** . The **Create Microsoft Entra ID Rule** page opens with fields populated from the original rule. Edit the fields as needed and click **Save** . For more information about available fields, see Create a rule on page 31 .
Delete rule	Select the checkbox next to the rule. Click Delete and then click **Delete** to confirm.

4. Click a rule to view details for the rule. The following actions are available when you view an individual rule:

Available actions for individual rules

Option	Description
Preview	In the **Summary** section, click the number that appears in the **Matching Endpoints** column and then

©2026 Tanium Inc. All Rights Reserved

Option	Description
targeted endpoints	choose one of the following options: • Click **View Online Data** to ask a live question to see online endpoints that the rule targets. • Click **View Cached Data** to view targeted endpoints from results collected by Tanium Data Service in the last 30 days. **Note:** When you view cached data, any value set for the **Endpoint Last Seen** option in the rule is ignored, and all matching endpoints from Tanium Data Service appear. If you do not change the **Endpoint Last Seen** value when you create the rule, then viewing cached data shows you exact matches. If you changed the **Endpoint Last Seen** value, the actual matching endpoints are a subset of the results that appear. By default, Tanium Data Service retains results for 30 days, but users can configure settings for all endpoints, or endpoints by computer group, to reduce the retention period. For more information, see Tanium Interact User Guide: Configure removal of expired results .
Edit rule	Click **Actions** > **Edit** .
Clone rule	Click **Actions** > **Clone** . The **Create Microsoft Entra ID Rule** page opens with fields populated from the original rule. Edit any fields and click **Save** . For more information about available fields, see Create a rule on page 31 .
Take ownership	Rules run against the endpoints allowed by the computer management group permissions for the owner of the rule. To change ownership of a rule to yourself, click **Actions** > **Take Ownership** , and then click **Save** .
Delete rule	Click **Actions** > **Delete** and then click **Delete** to confirm.

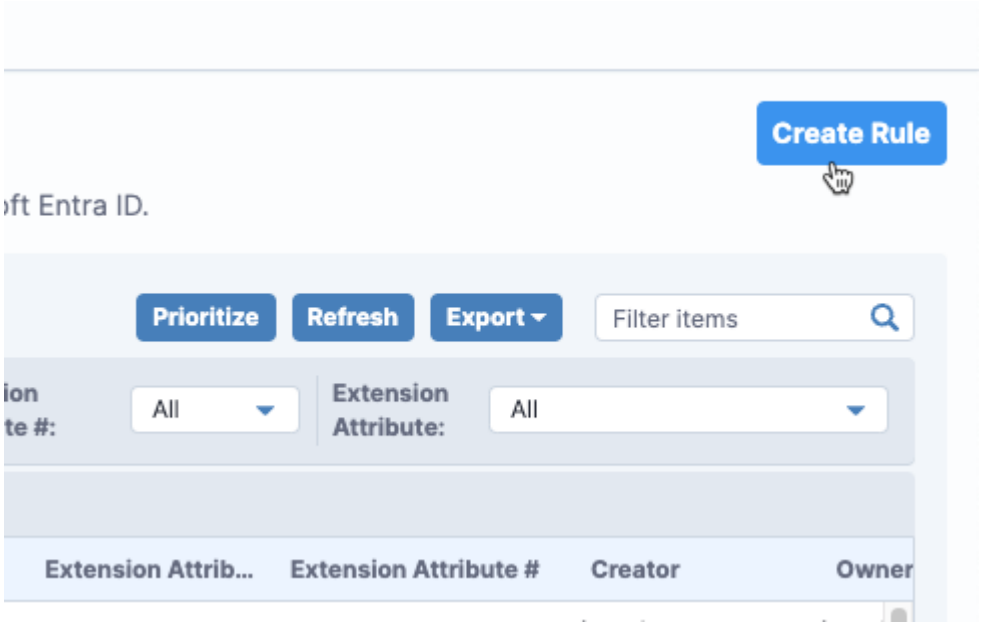
Create a rule

About this task

To create a rule, you must have a role with the **Zero Trust Microsoft Entra ID Config** Write permission.

1. From the Main menu, go to **Shared Services** > **Zero Trust** > **Rules > Create Rule**.

©2026 Tanium Inc. All Rights Reserved



2. Enter a name for the rule and optionally add a description.
3. Select a **Mode**:
    - Select **Enforcement** if you want Zero Trust to send data to your IAM provider when events occur.
    - Select **Audit** if you want Zero Trust to log events but not send data to your IAM provider.
4. Click **Add Targeting** to define a filter using the same **from computers with** fields as in the Interact **Question Builder**. You can base the matching on a **Sensor** or **Computer Group** (management group or filter group). For each rule, you can configure multiple filters, including nested filters. For more information about using the builder, see Tanium Console User Guide: Issue a question through the Question Builder.

    Tip: The sensors that appear in the builder are sourced by Tanium Data Service. For more information about viewing registered sensors and registering sensors for collection with Tanium Data Service, see Tanium Interact User Guide: Managing Tanium Data Service.

    Note: Disregard the **Force Computer Id** option in the **Advanced Question Options** section. That option is not used by Zero Trust.

©2026 Tanium Inc. All Rights Reserved

Note:

For Entra ID rules, Zero Trust adds a filter to target only the following endpoints:

- Endpoints that do not have a tenant ID
- Endpoints whose tenant ID matches a configured tenant ID in Entra ID

The filter appears when you view the targeting for the rule and cannot be removed. For more information about finding your tenant ID in Entra ID, see Microsoft Azure documentation: How to find your Azure Active Directory tenant ID.

5. (Optional) Click **Preview Targeted Endpoints** to view the endpoints that the rule targets, and then adjust your targeting criteria if necessary.

   Note: Be aware that rules are subject to the computer management group permissions of the default persona of the user who owns the rule. If you change ownership of the rule, the rule might target different endpoints.

6. (Optional) To limit targeting to endpoints seen online recently, update the value for **Endpoint Last Seen**. The default value is 720 hours (30 days), which is the default amount of time that Tanium Data Service stores results.

   Tip: For best results, do not set the value lower than 96 hours. Rules run on data that Tanium Data Service provides; setting this value to 96 hours or more prevents stale data if endpoints are powered down over a long weekend.

7. Specify the **Microsoft Entra ID Device Attribute**.
   - **Action**: To apply an extension attribute when an event occurs, select **Apply**. To remove an extension attribute when an event occurs, select **Remove**.
   - **Extension Attribute**: Select the attribute to apply or remove a string when an event occurs. Each extension attribute can only contain one extension attribute string.
   - **Extension Attribute String**: Enter the string to assign to, or remove from, the extension attribute. If you set **Action** to **Apply**, this string is applied to the selected **Extension Attribute**. If you set **Action** to **Remove**, the rule only removes the string if it matches the value that you set in this field.
   - If you select **Apply** as the **Action** type, you can select **Automatically remove**

©2026 Tanium Inc. All Rights Reserved

attribute if target conditions are no longer met to remove the attribute when an endpoint no longer meets the target conditions. If you do not select **Automatically remove attribute if target conditions are no longer met**, the extension attribute string remains until another rule applies or removes the string.

8. Click **Save**.
   Zero Trust creates and activates the rule.

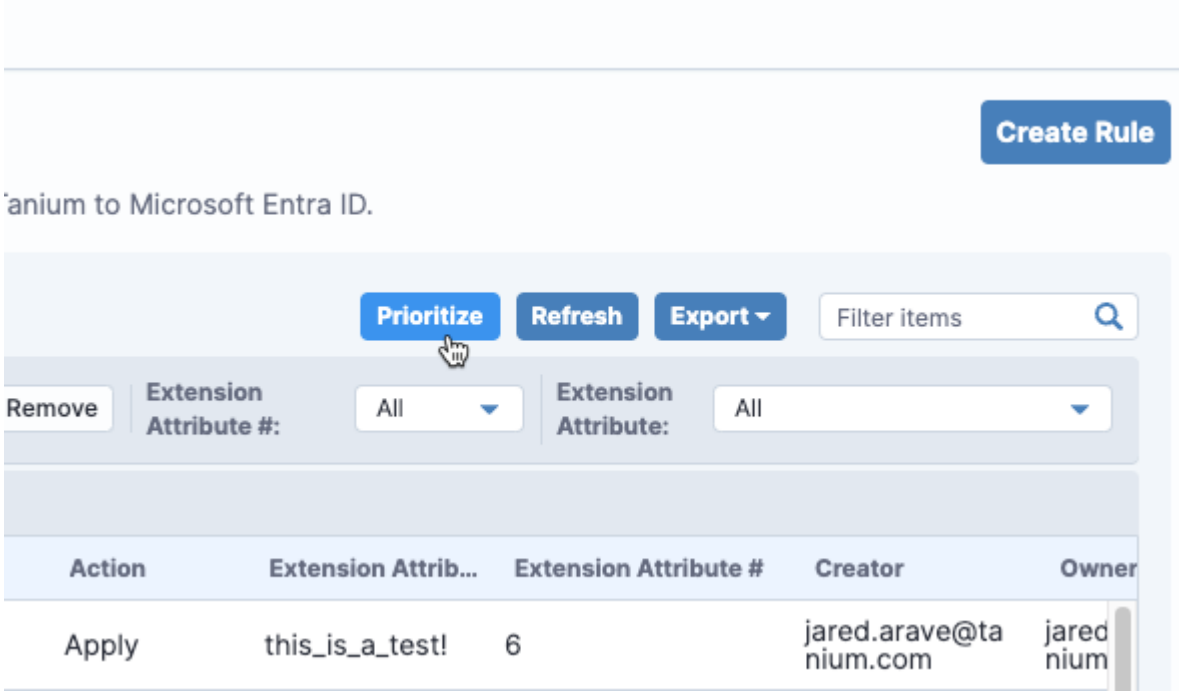
Prioritize rules

About this task

An event might cause an endpoint to match more than one rule. An event can match multiple rules, but only one rule can trigger for each extension attribute for each endpoint.

For example, consider an event that matches three rules: **Rule 1**, **Rule 2**, and **Rule 3**. **Rule 1** assigns a string to extension attribute 1, **Rule 2** assigns a string to extension attribute 3, and **Rule 3** removes a string from extension attribute 3. The rules are prioritized in order: **Rule 1** is priority 1, **Rule 2** is priority 2, and **Rule 3** is priority 3. When the event occurs, **Rule 1** always triggers for the endpoint, because that rule has no conflicts with other rules (and it is also the highest priority rule). However, **Rule 2** and **Rule 3** affect the same extension attribute, and thus only **Rule 2** triggers due to the order of priority.

1. From the Main menu, go to **Shared Services** > **Zero Trust** > **Rules > Prioritize**.



©2026 Tanium Inc. All Rights Reserved

2. Drag the rules in the order that you prefer. Rule priority is in descending order (1 is the highest priority). Click **Save**.

Take ownership of a rule

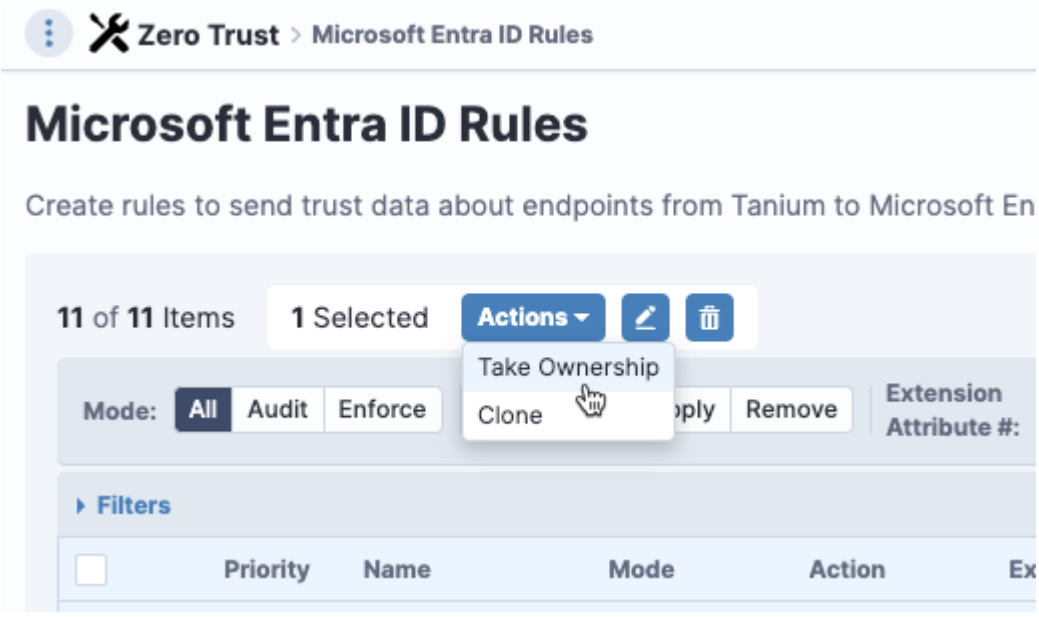
About this task

A rule is subject to the computer management group permissions of the user who creates the rule. If a rule does not trigger for an endpoint, you can expand the computer management group permissions for the user, or you can transfer ownership of the rule to a user with the necessary permissions.

Note: For more information about changing computer management group permissions for a user, see Tanium Console User Guide: Manage computer group assignments for a user.

Important: Rules use the computer management group permissions for the default persona of the user.

1. From the Main menu, go to **Shared Services** > **Zero Trust** > **Rules**.
2. Select the checkbox next to the rule and then click **Actions** > **Take Ownership**.



3. Click **Save**.

©2026 Tanium Inc. All Rights Reserved

Result

The rule immediately uses the management rights of the new owner.

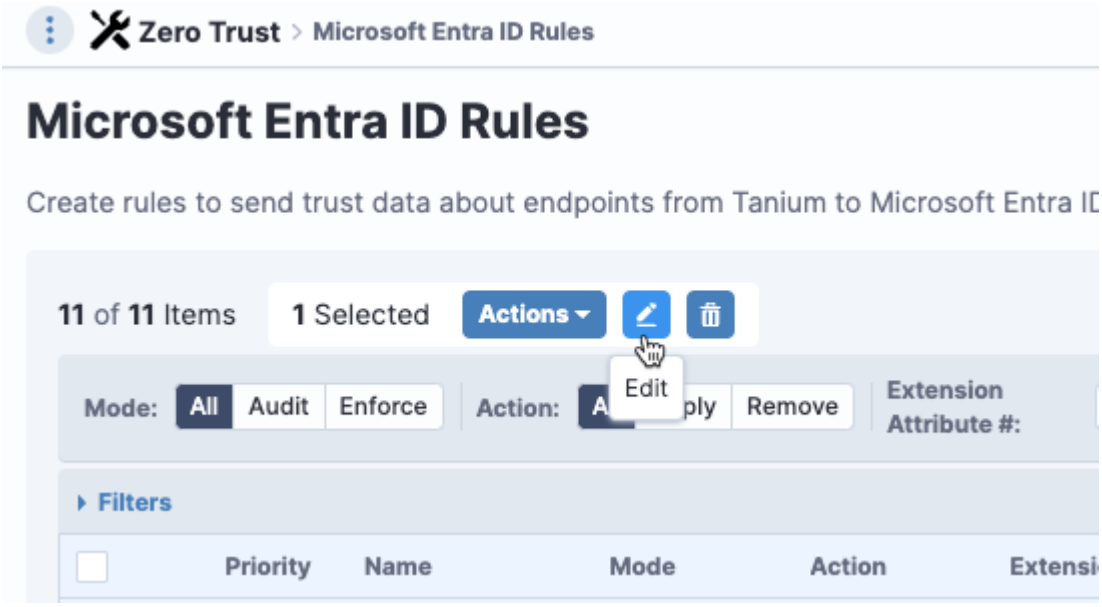
Edit a rule

About this task

You can edit the name and description of an existing rule.

Tip: After you create a rule, you can only edit the name and description of the rule. If you want to edit any other fields, you can clone the rule, modify the fields as needed, and then save the new rule. For example, if you create a rule in audit mode and want to change the rule to enforcement mode, clone the rule, edit the mode, and then save the new rule. For more information, see Clone a rule on page 37.

1. From the Main menu, go to **Shared Services** > **Zero Trust** > **Rules**.
2. Select the checkbox next to the rule and click Edit .



Tip: Alternatively, you can click the name of the rule to view the rule. From the page that opens, select **Actions** > **Edit**.

3. Edit the name or description of the rule.

©2026 Tanium Inc. All Rights Reserved

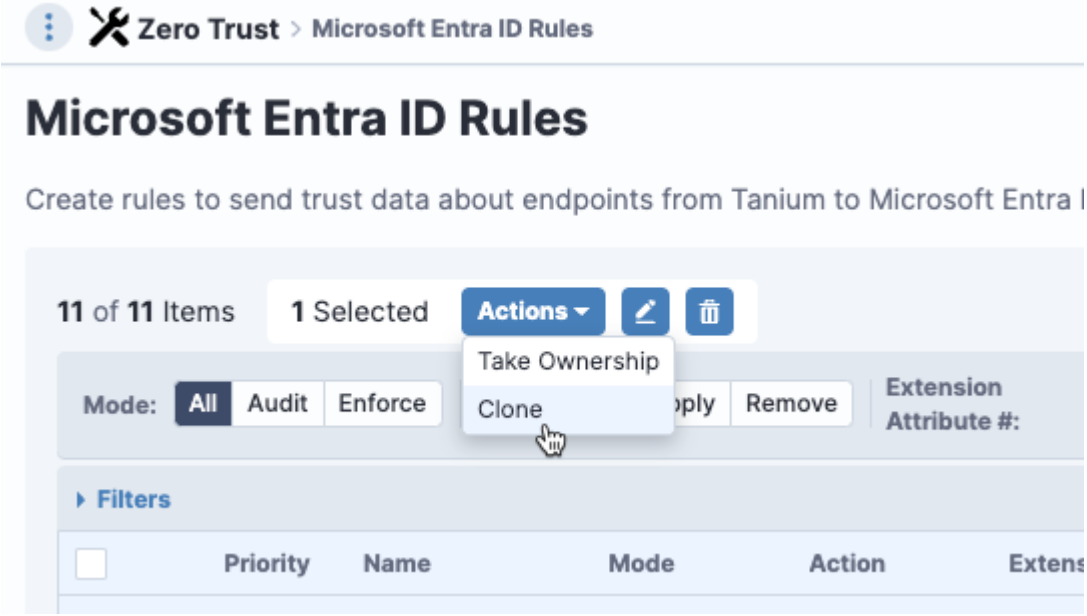
4. Click **Save**.

Clone a rule

About this task

To quickly create a rule that is similar to an existing rule, you can clone the rule.

1. From the Main menu, go to **Shared Services** > **Zero Trust** > **Rules**.
2. Select the checkbox next to the rule that you want to clone and select **Actions** > **Clone**.



Step result: The **Create Microsoft Entra ID Rule** page opens with fields populated from the original rule.

3. Edit any fields and click **Save**.
   For more information about available fields, see Create a rule on page 31.
4. (Optional) Change the priority of the rule.
   For more information, see Prioritize rules on page 34.

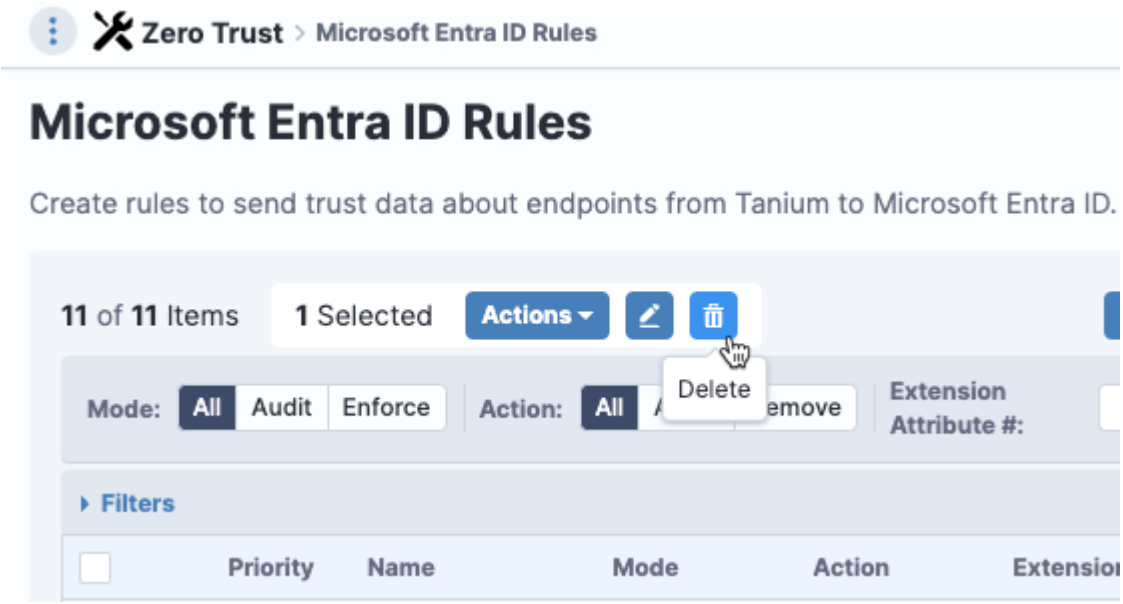
Delete a rule

About this task

©2026 Tanium Inc. All Rights Reserved

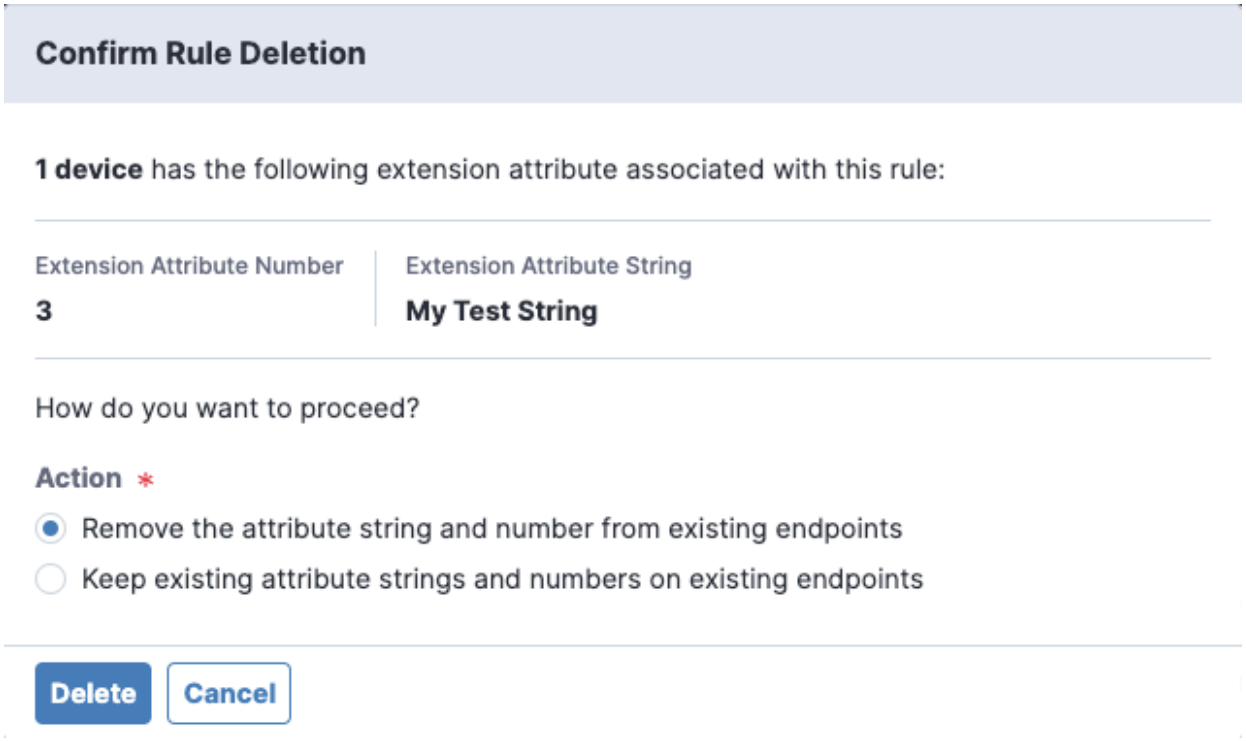
Best Practice: When you delete a rule, you have the option to remove the extension attribute string from endpoints that were targeted by the rule. To ensure you remove the extension attribute string from all possible endpoints that might have been affected by the rule, change the ownership of the rule to a user who has computer management group permissions to all endpoints that have been targeted by the rule, and then have that user delete the rule. You can also have a user with unrestricted management rights create a temporary rule to remove an extension attribute string from all managed endpoints.

1. From the Main menu, go to **Shared Services** > **Zero Trust** > **Rules**.
2. Select the checkbox next to the rule that you want to delete and click Delete .



3. If the rule sets an extension attribute on any endpoints, a prompt appears to determine how to handle those endpoints.
   You can choose to remove the extension attribute and string for the endpoints or keep the existing extension attribute and string for the endpoints.

©2026 Tanium Inc. All Rights Reserved



4. Click **Delete**.

©2026 Tanium Inc. All Rights Reserved

Auditing events

Zero Trust provides an audit log that you can use to monitor zero trust events.

Review data sent to your IAM provider

1. From the Main menu, go to **Shared Services** > **Zero Trust**.
2. Review the data in the **Sent to Microsoft Entra ID** section.

   Note:

   To view the **Sent to Microsoft Entra ID** section, you must have unrestricted management rights. If you have **Zero Trust Microsoft Entra ID Audit** read permission, you can use filters to view the audit entries on the **Microsoft Entra ID Audit Log** page.

   - For more information about the steps to view the **Microsoft Entra ID Audit Log** page, see View audit log on page 41.
   - For more information about how to set computer group permissions, see Tanium Console User Guide: Manage computer group assignments for a user.

3. (Optional) Use the following filter options to find specific entries if the list is long. The list shows only the entries that match all the filters that you specify.

   ### Event filter options

Option	Description
Select action	Use the **Action** buttons to toggle between **All** entries, entries for rules that **Apply** an extension attribute, and rules that **Remove** an extension attribute.
Select extension attribute number	Select a value for **Extension Attribute #** to only show entries that removed or applied a value to the extension attribute.
Select extension attribute	Select a value for **Extension Attribute** to only show entries that removed or applied the extension attribute.

©2026 Tanium Inc. All Rights Reserved

Option	Description
Filters	Expand **Filters** and specify any additional filters.
Filter items	Enter an alphanumeric string to match text in the **Computer Name**, **IP Address**, **MAC Address**, **Rule** columns. Select a **Rule** or specify the **Execution Start** and **Execution End** dates.
Manage columns	In the header, click Customize Columns. To remove a column, clear the checkbox for the column. To adjust the column order, click and drag the column names.
Refresh entries	Click Refresh. Any filters that you added apply to the updated results.

View audit log

Perform the following steps to review all audit entries, including entries generated from rules in audit mode.

Microsoft Entra ID

About this task

Note: You require **Zero Trust Microsoft Entra ID Audit** read permission to access the **Microsoft Entra ID Audit Log** page.

1. From the Main menu, go to **Shared Services** > **Zero Trust** > **Audit Log**.
   The **Microsoft Entra ID Audit Log** page shows a log of events captured by Tanium.
2. (Optional) Use the following filter options to find specific entries if the list is long. The list shows only the events that match all the filters that you specify.

   ### Event filter options

Option	Description
Select mode	Use the **Enforcement Mode** buttons to toggle between entries for **All** rules, **Audit** rules, and **Enforce** rules.
Select	Use the **Action** buttons to toggle between **All** entries, entries for rules that **Apply** an extension

©2026 Tanium Inc. All Rights Reserved

Option	Description
action	attribute, and rules that **Remove** an extension attribute.
Select trigger mechanism	Use the **Triggered by** buttons to toggle between **All** rules, events triggered by a **Rule**, and entries recorded by users who **Manually** added an endpoint. For more information, see Manually modify endpoint attribute on page 46.
Filters	Expand **Filters** and specify any additional filters.
Filter items	Specify the **Execution Start** and **Execution End** dates or select a **Rule**. Enter an alphanumeric string to match text in the **Computer Name** and **Device ID** columns. You can also filter by selecting an **Extension Attribute #**, and **Extension Attribute**.
Manage columns	In the log header, click Customize Columns. To remove a column, clear the checkbox for the column. To adjust the column order, click and drag the column names.

3. (Optional) Take action on a rule. The following actions are available:

Available actions

Option	Description
View audit entry	Click Open Side Panel in the row of the entry to view additional details for the entry.
Export audit entries	Click **Export**, and then click **Download** when the audit log is ready. The ZIP file contains all visible log entries in a CSV format.
Refresh entries	Click Refresh. Any filters that you added apply to the updated results.
Manage columns	In the header, click Customize Columns. To remove a column, clear the checkbox for the column. To adjust the column order, click and drag the column names.

Send logs through Connect

About this task

Use Connect to send Zero Trust log entries to Connect destinations. You can configure Connect to

©2026 Tanium Inc. All Rights Reserved

send log entries as they occur through the event source in Connect. For more information about event sources, see Tanium Connect User Guide: Connection Sources.

Before you begin

- Tanium™ Connect 5.0 or later is required
- You must have access to Connect with the Connect Operator or Connect Administrator role.

Create a connection

About this task

The following steps describe the basic settings that you configure for a connection. Additional settings vary by connection destination. For more information, see Tanium Connect User Guide: Managing connections.

1. From the Main menu, go to **Modules** > **Connect**.
2. From the Connect **Overview** page, go to the **Connections** section and click **Create Connection**.
3. In the **General Information** section, enter a **Name** and optional **Description** for the connection.
4. In the **Configuration** section, select **Event** for the **Source**.
5. Select **Tanium Zero Trust** for the **Event Group**.
6. Select **Microsoft Entra ID Device Rule**.
7. Select the **Destination** where you want Connect to send the data. Provide any additional configuration for the type of destination you select.
8. Go to the **Configure Output** section and select a **Format** for the exported data.
9. Go to the **Enablement** section and select **Listen for this Event**.

   Tip: Connections that use the event source run automatically when an event occurs.

   To disable the connection, deselect **Listen for this Event**.
10. Click **Save**.

©2026 Tanium Inc. All Rights Reserved

Result

When an event occurs, Connect sends the log entry to the destination that you set.

©2026 Tanium Inc. All Rights Reserved

Maintaining Zero Trust

About this task

Perform monthly maintenance tasks to ensure that Zero Trust successfully monitors events on all the targeted endpoints and does not overuse endpoint or network resources. If Zero Trust is not performing as expected, you might need to troubleshoot issues or change settings. For more information about related procedures, see Troubleshooting Zero Trust on page 46.

Zero Trust monthly maintenance

1. Verify that the credentials for your Identity and Access Management (IAM) provider are valid. For more information about changing credentials with Tanium™ Zero Trust, see Tanium Zero Trust User Guide: Configure IAM provider settings.
2. Review the audit logs to verify that Zero Trust is sending data to your provider. For more information, see Tanium Zero Trust User Guide: Review data sent to your IAM provider.
3. Review existing rules for outdated, unused, or overlapping rules. Delete obsolete rules as necessary. For more information, see Tanium Zero Trust User Guide: Managing rules.
4. Verify that any Connect jobs that send audit data are running and sending data. For more information, see Tanium Connect User Guide: Managing connections.

©2026 Tanium Inc. All Rights Reserved

Troubleshooting Zero Trust

About this task

If Zero Trust is not performing as expected, you might need to troubleshoot issues or change settings.

Collect logs

About this task

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

1. From the Main menu, go to **Shared Services** > **Zero Trust**. Click Help ?.
2. From the **Troubleshooting** tab, click **Download Support Bundle**.
   A ZIP file downloads to the local download directory.
3. Contact Tanium Support to determine the best option to send the ZIP file. For more information, see Contact Tanium Support on page 56.

Manually modify endpoint attribute

About this task

You can manually apply or remove an extension attribute from an existing rule for one or more endpoints. The option to manually modify an endpoint attribute uses enforcement rules only. Manually editing an extension attribute is useful to test a rule.

> **Note:** For each endpoint, any attribute that you modify is subject to change the next time a rule runs and targets the endpoint.

1. From the Main menu, go to **Shared Services** > **Zero Trust** > **Modify Endpoint Attribute**.
2. Select the endpoints to target:
   a. In **Target Endpoints**, enter a string to search for endpoints by computer name, IP

©2026 Tanium Inc. All Rights Reserved

address, or device ID.

b. Click Add Endpoint + next to the endpoint in the results that appear.

> **Important:**
> The Add Endpoint + option only appears for endpoints that have a device ID. The device ID is provided by your IAM provider. For more information about device IDs, see Microsoft Entra documentation: Manage device identities using the Microsoft Entra admin center.

c. Repeat to add additional endpoints.

3. Select an **Action**.
   - To apply the extension attribute, select **Apply**.
   - To remove the extension attribute, select **Remove**.
4. For **Rule Attributes**, select the enforcement rule with the extension attribute and extension attribute string that you want to apply.
5. Click **Save**.

Result
Zero Trust attempts to apply the attribute to the selected endpoints. To verify the attribute was successfully applied, review the Entra ID audit log. For more information, see Review data sent to your IAM provider on page 40.

Endpoint does not appear in the audit log

Symptom

The audit log does not contain expected entries for an endpoint.

Cause

Possible causes include:

- The endpoint might not be registered in Entra ID. Tanium Zero Trust does not monitor endpoints that are not registered with Entra ID.
- There are no rules that target the endpoint.

©2026 Tanium Inc. All Rights Reserved

- The endpoint is registered in a different Microsoft Entra ID tenant than the one configured in Zero Trust settings. Endpoints from other tenants, such as a subsidiary tenant, are not processed.

Solution

- Re-register the endpoint in Entra ID. For more information, see Microsoft Entra documentation: Manage device identities using the Microsoft Entra admin center.
- Verify that there are one or more rules that target the endpoint.
- Verify that the endpoint is registered in the same Entra ID tenant configured in Zero Trust settings. To check the configured tenant, go to **Shared Services** > **Zero Trust** and click Settings.

Entra ID log shows endpoint does not exist

Symptom

The audit log contains error messages that an endpoint does not exist, such as the following:

```
making patch request: Call to https://graph.microsoft.com/v1.0/
devices(deviceId='285a3512-728f-4ac1-9295-485f9e3312ee'): Bad Status Code Received: 404 Not
Found {"error":{"code":"Request_ResourceNotFound","message":"Resource
'285a3522-728f-4ae1-9295-485f5e3812ee' does not exist or one of its queried reference-
property objects are not present.","innerError":{"date":"2023-06-23T20:31:25","request-
id":"132288da-b683-4d24-b6ec-ff2a539f9752","client-request-id":"132288da-b683-4d24-b6ec-
ff2a539f9752"}}}
```

Cause

These messages commonly occur when an endpoint de-registers from Entra ID. Although the endpoint is no longer registered in Entra ID, the endpoint still qualifies for one or more enforcement rules in Tanium Zero Trust.

Solution

- To continue monitoring the endpoint:

  Re-register the endpoint in Entra ID. For more information, see Microsoft Entra documentation: Manage device identities using the Microsoft Entra admin center.

©2026 Tanium Inc. All Rights Reserved

- To discontinue monitoring for the endpoint:
    - Remove the following registry entry key on the endpoint:

      ```
      HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\WorkplaceJoin\JoinInfo
      ```

    - Replace any rules that target the endpoint. After you create a rule, you can only edit the name and description of the rule. To update the targets for a rule, clone the rule, modify the targeting, and then save the new rule. For more information, see Clone a rule on page 37.

Zero Trust is unable to connect to Microsoft Entra ID

Symptom

A banner appears with the following message: **Zero Trust is unable to connect to Microsoft Entra ID. Make sure your credentials are valid and Zero Trust is configured correctly for your Microsoft Entra ID instance. Go to Settings.**

Cause

Possible causes include:

- The credentials saved in the Zero Trust settings are invalid or have expired.
- The Entra ID application registration is missing the **Device.ReadWrite.All** permission.
- The selected cloud location does not match your Entra ID tenant. For example, a commercial tenant configured with a US Government endpoint.

Solution

1. From the Main menu, go to **Shared Services** > **Zero Trust**. Click Settings ⚙.
2. Verify that the **Microsoft Entra ID Tenant ID**, **Microsoft Entra ID App ID** are correct.
3. Re-enter your client secret or upload a new certificate and save the configuration.

©2026 Tanium Inc. All Rights Reserved

4. In the Entra ID portal, confirm that the app registration has the **Device.ReadWrite.All** API permission granted.

Unable to preview rule

Symptom

When previewing a rule, the following message appears: **Unable to preview rule. Make sure all sensors are registered with Tanium Data Service. The missing sensor is: [sensor name]**

Cause

One or more sensors required to evaluate the targeting criteria for the rule have not been registered with Tanium Data Service and cannot be queried.

Solution

Register the missing sensors with Tanium Data Service and then retry the preview. For more information about registering sensors, see the Tanium Interact User Guide: Register or unregister sensors for collection.

Not authorized to modify endpoint attribute

Symptom

When manually modifying an endpoint attribute, the action fails with the following error: **User does not have the device management rights to perform this action.**

Cause

The signed-in user does not have device management rights for one or more of the selected endpoints. The user must have management rights for all selected endpoints for the action to proceed.

©2026 Tanium Inc. All Rights Reserved

Solution

Remove endpoints that you do not have management rights for and retry the action, or contact your administrator to request the appropriate rights.

Cannot apply audit rule

Symptom

When manually modifying an endpoint attribute, the action fails with the following error: **Cannot apply audit rule.**

Cause

The selected rule is in audit mode. Manual endpoint attribute modifications can only use rules that are in enforcement mode.

Solution

Select an enforcement rule, or clone the audit rule and set the mode to enforcement on the new rule. For more information, see Clone a rule on page 37.

Extension attribute is also applied by another rule

Symptom

When removing an extension attribute from one or more endpoints, a warning indicates that the same extension attribute is also applied by other rules.

Cause

The extension attribute is targeted by more than one rule. Removing the attribute through one rule does not prevent another rule from reapplying the same attribute to the same endpoints.

©2026 Tanium Inc. All Rights Reserved

Solution

To completely remove the attribute from the affected endpoints, delete or modify the other rules that apply the same extension attribute. After you create a rule, you can only edit the name and description of the rule. To change the targeting, attribute, or action, clone the rule, modify the new rule, and then delete the original. For more information, see Clone a rule on page 37.

Audit log export errors

Symptom

The audit log export does not download, or an error occurs when initiating an export.

Cause

Possible causes include:

- An export is already in progress. Only one export can run at a time.
- No export has been initiated yet.
- A previous export failed before it completed.

Solution

- If an export is in progress, wait for the **Audit log export is in progress** status to change to **Audit log export is available. Download.** before initiating a new export.
- If no export has been initiated, click **Export** in the Audit Log view to start one.
- If a previous export failed, click **Export** to start a new export.

Cannot view the audit log

Symptom

The audit log fails to load, or an error indicates that unrestricted management rights are required.

©2026 Tanium Inc. All Rights Reserved

Cause

Viewing the Zero Trust audit log requires unrestricted management rights. Users assigned to a restricted computer group cannot view audit log entries.

Solution

Sign in as a user that has unrestricted management rights, or contact your administrator to update your computer group assignment. For more information about user role requirements, see User role requirements on page 17.

Rule and audit log statuses

The following statuses appear in the Zero Trust audit log and rule views.

Rule and audit log statuses

Status	Description
Pending	Tanium data has been sent to Microsoft Entra ID and is awaiting confirmation.
Success	Microsoft Entra ID successfully received and applied the Tanium data.
Error	The operation failed. Review the error detail in the audit log row for more information. For help with specific error messages, see "Failed due to shutdown" error in audit log on page 53 and "Update failed due to tenant change" error in audit log on page 54 .
Audit	The rule is running in audit mode. No changes are made to Entra ID. If the rule were enforced, the configured action would be applied.
Enforce	The rule is running in enforcement mode. Extension attributes are applied to or removed from endpoints in Entra ID.

"Failed due to shutdown" error in audit log

Symptom

One or more entries in the audit log show **Failed due to shutdown** in the **Error** column.

©2026 Tanium Inc. All Rights Reserved

Cause

When the Zero Trust service restarts, it marks any enforcement audit events that were pending execution at the time of shutdown with this error. These events were not sent to Microsoft Entra ID before the service stopped.

> **Note:** Audit-only rule events are not affected by this error. Only enforcement rule events that were pending at shutdown are marked.

Solution

No action is required. This error is expected after a service restart and does not indicate data loss, a misconfiguration, or erroneous policy enforcement. After the service starts, the engine creates new actions on the next processing interval, which automatically retries any work that was pending at shutdown. To confirm that enforcement is working correctly, verify that recent audit log entries show a **Success** status.

"Update failed due to tenant change" error in audit log

Symptom

One or more entries in the audit log show **Update failed due to tenant change** in the **Error** column.

Cause

The Microsoft Entra ID tenant was reconfigured after an audit event was created but before the event was sent to Entra ID. The pending event was abandoned because the tenant ID no longer matched the updated configuration.

Solution

No action is required for audit events that already have this error. After the tenant is reconfigured, new audit events are created and processed using the updated tenant configuration.

©2026 Tanium Inc. All Rights Reserved

Rule or configuration operation fails

Symptom

A Zero Trust operation fails, and a notification appears with a message such as the following:

- **Failed to create rule.**
- **Failed to update rule.**
- **Failed to delete rule.**
- **Failed to prioritize rules.**
- **Failed to update rule owner.**
- **Failed to modify endpoint attribute.**
- **Configuration update failed.**
- **Failed to delete configuration.**

Cause

The Zero Trust service could not complete the requested operation. Common causes include a temporary service issue, insufficient privileges, or a problem connecting to Microsoft Entra ID.

Solution

1. Retry the operation.
2. If the operation continues to fail, verify that you have the required Zero Trust role and that the connection to Microsoft Entra ID is working. For more information, see Zero Trust is unable to connect to Microsoft Entra ID on page 49.
3. If the operation still fails, contact Tanium Support. For more information, see Contact Tanium Support on page 56.

Not authorized to view this page

©2026 Tanium Inc. All Rights Reserved

Symptom

When opening a Zero Trust page, the following message appears: **Not authorized to view this page.**

Cause

The signed-in user does not have the role required to view the requested page.

Solution

Contact your administrator to request the required role. For more information about user role requirements, see User role requirements on page 17.

Uninstall Zero Trust

If you need to uninstall Zero Trust, perform the following steps.

Important: Consult with Tanium Support before you uninstall or reinstall Zero Trust.

1. Sign in to Tanium Console as a user with the Administrator role.
2. From the Main menu, go to **Administration** > **Configuration** > **Solutions**.
3. In the **Content** section, select the Zero Trust row and click **Uninstall**.
4. Review the summary and click **Yes** to proceed with the uninstallation.
5. When prompted to confirm, enter your password.

Note: The uninstall does not remove the Zero Trust log from the Tanium Module Server. To remove the log after the uninstall completes, manually delete the \Program Files\Tanium\Tanium Module Server\services\zero-trust-files\services\zero-trust-files\ directory.

Contact Tanium Support

©2026 Tanium Inc. All Rights Reserved

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