

Tanium™ Integrations Gallery User Guide

Autonomous IT. Unstoppable Business.

2025H2 Semiannual Release

Version 1.5

February 05, 2026

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

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

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

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

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

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

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

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

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

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

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

© 2025 Tanium Inc. All Rights Reserved

© 2025 Tanium Inc. All rights reserved.

Table of contents

Integrations Gallery overview **10**

Benefits of Tanium Integrations Gallery 10

Discover integrations across tools 10

Streamlined deployment process 10

Reliability and automation for IT, Risk, and SecOps teams 10

Complete visibility into available solutions 10

Interoperability with other Tanium products 10

Account Management 10

Getting started with Integrations Gallery **11**

Step 1: Configure Integrations Gallery 11

Step 2: Discover integrations 11

Access Integrations Gallery 11

View featured integrations 12

Manage integrations 12

Integrations Gallery 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 14

Host and network security requirements 14

Ports 15

Security exclusions 15

User role requirements 15

© 2025 Tanium Inc. All Rights Reserved

Installing Integrations Gallery **18**
Before you begin 18
Import Integrations Gallery with default settings 18
Import Integrations Gallery with custom settings 18
Manage solution dependencies 18
Verify Integrations Gallery version 18
Troubleshoot issues 19
Configuring Integrations Gallery **20**
Configure Integrations Gallery 20
Link your Account Portal 20
Move your Tanium Account 20
Set up Integrations Gallery users 20
Managing the Microsoft Azure VM Extensions integration **22**
Requirements 22
Operating system support in Microsoft Azure 22
Network connectivity 22
Computer group dependencies 22
User role requirements 22
View the Details page 24
View the Configuration page 25
View the Tanium Content page 25
View the Support page 26
View the About page 26
Enable the integration 26
Create a Tanium Client initialization profile 26
Obtain the tanium-init.dat file for deployment 28
Disable the integration 29
Troubleshoot the Azure VM Extensions integration 29
Collect logs 29
Cannot install the Tanium Client VM extension on Microsoft Azure VMs 29

© 2025 Tanium Inc. All Rights Reserved

Managing the Microsoft Security Copilot integration **31**
Requirements 31
Core platform dependencies 31
Required dependencies 31
Feature-specific dependencies 32
User role and persona requirements 32
View the Details page 34
View the Configuration page 35
View the About page 35
Configure integration between Tanium and Security Copilot 36
Allow secure network connections between Tanium and Microsoft Security Copilot 36
Set up Tanium integration with Security Copilot users 36
Configure Tanium plugin for Security Copilot 36
Use Tanium prompts with Security Copilot 39
Tanium Skills example prompts 41
Get Real-time Data from Endpoints prompt sensor support 47
Troubleshoot issues 52
Allow Security Copilot egress IP addresses 53
Rotate Security Copilot API tokens 53
Review Security Copilot-related API token audit logging 53
Review Security Copilot-related questions in Tanium 54
Improve selection of Tanium Skills 54
Managing the ScreenMeet Screen Sharing integration **56**
Requirements 56
Supported operating systems for ScreenMeet 58
User role requirements 58
View the Details page 62
View the Configuration page 63
View the Tanium Content page 63
View the Support page 63

© 2025 Tanium Inc. All Rights Reserved

View the About page ... 64
Enable the integration ... 64
Configure personas to establish unattended screen sharing sessions ... 64
Open an endpoint screen sharing session ... 65
Open a screen sharing session from an endpoint ... 67
Open a screen sharing session from Direct Connect ... 68
Open a screen sharing session from Reporting ... 69
Open a screen sharing session from Performance ... 71
Open a screen sharing session with an endpoint that does not have a Tanium Client ... 72
View and join screen sharing sessions ... 73
Join active sessions in the list of sessions ... 73
End an endpoint screen sharing session ... 73
End active sessions in the list of sessions ... 73
Configure ScreenMeet settings ... 73
Unlink your Tanium Account ... 74
Troubleshoot the Screen Sharing integration ... 74
Collect logs ... 74
Screen sharing buttons unavailable ... 74
Contact support ... 75
Managing the Tanium Connector for Microsoft Intune ... 76
Before you begin ... 76
Entities and endpoints ... 77
Entity providers ... 78
Architecture ... 78
Requirements ... 79
Core platform dependencies ... 79
Solution dependencies ... 80
Tanium recommended installation ... 80
Import specific solutions ... 80
Required dependencies ... 80

© 2025 Tanium Inc. All Rights Reserved

Feature-specific dependencies ... 80
Endpoints ... 81
Supported Internet protocols ... 81
Supported operating systems ... 81
Device requirements ... 81
Third-party software ... 81
Host and network security requirements ... 81
Ports ... 81
Security exclusions ... 82
User role requirements ... 82
View the Details page ... 84
View the Configuration page ... 84
View the Tanium Content page ... 85
View the Support page ... 85
View the About page ... 85
Configure integration between Tanium and Microsoft Intune ... 86
Tanium Connector for Microsoft Intune ingestion ... 86
Interaction between Asset and Tanium Connector for Microsoft Intune ... 87
Create an Azure client ID and secret ... 89
(Optional) Include Microsoft Intune devices in Asset views ... 89
Create a Tanium Connector for Microsoft Intune instance ... 90
Edit a Tanium Connector for Microsoft Intune instance ... 91
Delete a Tanium Connector for Microsoft Intune instance ... 91
Monitor Tanium Connector for Microsoft Intune ... 91
View Tanium Connector for Microsoft Intune instances ... 91
Filter Tanium Connector for Microsoft Intune instance list ... 91
Use Tanium Connector for Microsoft Intune mobile devices and data ... 92
Issue questions to target Microsoft Intune mobile devices ... 92
Include Microsoft Intune mobile devices in a report ... 93
Export Microsoft Intune mobile device data using Tanium Connect ... 94

© 2025 Tanium Inc. All Rights Reserved

Troubleshooting 94
Collect logs 94
Cannot establish connection between Tanium and Microsoft Intune 94
Cannot authenticate to Microsoft Intune 95
Cannot access a route, or retrieve groups or devices, or Microsoft Intune permissions are missing 95
Troubleshooting Integrations Gallery 96
Collect Tanium Account logs 96
Contact Tanium Support 96

© 2025 Tanium Inc. All Rights Reserved

Integrations Gallery overview

With Integrations Gallery, you can discover, configure, and manage integrations between third parties and Tanium.

Tanium Integrations Gallery simplifies and accelerates the process of connecting the Tanium platform with key technology partners like Microsoft and ServiceNow. It enables customers to discover integrations effortlessly, providing a clear view of the solutions and integrations that are available.

Benefits of Tanium Integrations Gallery

Discover integrations across tools

Get visibility into integrations with Microsoft, ServiceNow, and more to maximize value across the security and IT operation ecosystem. The streamlined integration process removes friction, making Tanium a seamless extension to ecosystem partner solutions.

Streamlined deployment process

Integrations Gallery replaces the manual setup process with a modern, intuitive, and self-sufficient one. Customers no longer need to rely on teams of experts to deploy and maintain integration solutions.

Reliability and automation for IT, Risk, and SecOps teams

Integrations Gallery eliminates complexity concerns that are a barrier to adoption, reduces the risk of limited or broken integrations, and improves overall stability and ease of use.

Complete visibility into available solutions

The Integrations Gallery workbench includes an **Integrations** section that lists all available integrations, with partners such as Microsoft, ServiceNow, and ScreenMeet.

Interoperability with other Tanium products

Account Management

Integrations Gallery provides access to link your Tanium installation to your Tanium Account. For more information, see Tanium Account User Guide: Moving a Tanium instance to a different Tanium Account (Tanium Cloud instances only).

© 2025 Tanium Inc. All Rights Reserved

Getting started with Integrations Gallery

Follow these steps to configure and use Integrations Gallery.

Step 1: Configure Integrations Gallery

For more information, see Configuring Integrations Gallery on page 20.

Step 2: Discover integrations

Access Integrations Gallery

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, filter the list of integrations:
    - Filter by clicking on each category:
        - All
        - AI/ML Platforms
        - IT Asset Management
        - IT Operations Management
        - IT Service Management
        - IT Support
        - Risk Management
        - Security Operations
        - Vulnerability Management
    - Filter by **Enabled**:
        - All
        - Yes
        - No
    - Filter by **Offered By**:
        - All
        - Tanium
        - Partners

© 2025 Tanium Inc. All Rights Reserved

- Filter by selecting a **Solution**
- Filter by selecting a **Partner**
- Filter by text searching

View featured integrations

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Featured Integrations** section, read about each integration and click on the video to learn more.
3. Click on the integration name to manage the integration.

Manage integrations

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click on each integration tile to view more details and configuration options.
    - **Details**: includes the integration service enablement and configuration status and a link to access the integration
    - **Configuration**: includes configuration options and user roles for the integration
    - **Tanium Content**: includes reports or dashboards specific to the integration usage (not available for all integrations)
    - **About**: includes more information about the integration

© 2025 Tanium Inc. All Rights Reserved

Integrations Gallery requirements

Review the requirements before you install and use Integrations Gallery.

Core platform dependencies

Make sure that your environment meets the following requirements:

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

Solution dependencies

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



Some Integrations Gallery dependencies have their own dependencies, which you can see by clicking the links in the lists of Required dependencies on page 14 and Feature-specific dependencies on page 14. Note that the links open the user guides for the latest version of each solution, not necessarily the minimum version that Integrations Gallery requires.

Tanium recommended installation

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

Import specific solutions

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

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

© 2025 Tanium Inc. All Rights Reserved

Required dependencies

Integrations Gallery has the following required dependencies:

- Tanium™ Account Management Broker
- Tanium™ Core Content
- Tanium™ Feature Definitions
- Tanium™ Feature Flag
- Tanium™ Interact
- Tanium™ Reporting
- Tanium™ Secrets

Feature-specific dependencies

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

- Tanium™ Asset for using Tanium Connector for Microsoft Intune
- Tanium™ Endpoint Provider Service for using Tanium Connector for Microsoft Intune
- Tanium™ Gateway for Security Copilot integration
- Tanium™ Screen Sharing for ScreenMeet integration

Tanium™ Module Server

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

Endpoints

Integrations Gallery does not deploy packages to endpoints. For more information about Tanium Client operating system support, see Tanium Client Management User Guide: Client version and host system requirements.

Host and network security requirements

Specific ports and processes are needed to run Integrations Gallery.

© 2025 Tanium Inc. All Rights Reserved

Ports

Integrations Gallery requires no specific open ports to enable communication, but individual integrations might require open ports. For more information, see the page for that integration.



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

Security exclusions

User role requirements

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

- Integrations Gallery solution permissions on page 15
- Integrations Gallery administration and platform content permissions on page 17: The solution permissions automatically provide some of these permissions.

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

Integrations Gallery solution permissions

Permission	Integrations Gallery Administrator[1]	Integrations Gallery Operator[1]	Integrations Gallery Viewer[1]
Partner Integration View the Integrations Gallery workbench	✓ SHOW	✓ SHOW	✓ SHOW
Partner Integration Api Use the Integrations Gallery API	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE

© 2025 Tanium Inc. All Rights Reserved

Integrations Gallery solution permissions (continued)

Permission	Integrations Gallery Administrator[1]	Integrations Gallery Operator[1]	Integrations Gallery Viewer[1]
Partner Integration Credentials View and configure the Integrations Gallery credentials	✓ READ WRITE DELETE	✓ READ WRITE DELETE	✗
Partner Integration Gallery View and configure the Integrations Gallery	✓ READ WRITE	✓ READ	✓ READ
Partner Integration Gallery Account Management View and configure the Account Management settings in Integrations Gallery	✓ READ WRITE	✓ READ	✓ READ
Partner Integration Gallery Azure Vm Extensions View and configure the Azure VM Extensions integration	✓ READ WRITE	✓ READ WRITE	✓ READ
Partner Integration Gallery Copilot View and configure the Microsoft Copilot for Security integration	✓ READ WRITE	✓ READ WRITE	✓ READ
Partner Integration Gallery Screenmeet View and configure the ScreenMeet integration	✓ ADMIN READ WRITE	✓ ADMIN READ WRITE	✓ VIEWER READ
Partner Integration Reporting Metrics View reporting metrics in Integrations Gallery	✓ READ	✓ READ	✓ READ

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

© 2025 Tanium Inc. All Rights Reserved

Integrations Gallery administration and platform content permissions

Permission	Permission Type	Integrations Gallery Administrator	Integrations Gallery Operator	Integrations Gallery Viewer
Action Group	Administration	READ	READ	READ
Public Key	Administration	READ	READ	
Action	Platform	READ WRITE	READ WRITE	READ
Filter Group	Platform	READ	READ	READ
Own Action	Platform	READ	READ	
Package	Platform	READ	READ	READ
Plugin	Platform	READ EXECUTE	READ EXECUTE	READ EXECUTE
Sensor	Platform	READ	READ	READ

To view the content sets to which the platform content permissions apply, see Tanium Console User Guide: View effective role permissions.

© 2025 Tanium Inc. All Rights Reserved

Installing Integrations Gallery

Use Tanium Console **Solutions** page to install Integrations Gallery and choose either automatic or manual configuration:

- **Automatic configuration with default settings**: Integrations Gallery is installed with any required dependencies and other selected products. After installation, the Tanium Server automatically configures the recommended default settings. This option is the best practice for most deployments. For more information about the automatic configuration for Integrations Gallery, see Import Integrations Gallery with default settings on page 18.
- **Manual configuration with custom settings**: After installing Integrations Gallery, you must manually configure required settings. Select this option only if Integrations Gallery requires settings that differ from the recommended default settings. For more information, see Import Integrations Gallery with custom settings on page 18.

Before you begin

- Read the release notes.
- Review the Integrations Gallery requirements on page 13.
- Assign the correct roles to users for Integrations Gallery. For more information, see User role requirements on page 15.
    - To import the Integrations Gallery solution, you must be assigned the Administrator reserved role.

Import Integrations Gallery with default settings

No default settings are configured for Integrations Gallery.

To import Integrations Gallery and configure default settings, see Tanium Console User Guide: Import all modules and services. After the import, verify that the correct version is installed: see Verify Integrations Gallery version on page 18.

Import Integrations Gallery with custom settings

To import Integrations Gallery without automatically configuring default settings, be sure to clear the **Apply All Tanium recommended configurations** option while performing the steps in Tanium Console User Guide: Import or update specific solutions. After the import, verify that the correct version is installed: see Verify Integrations Gallery version on page 18.

Manage solution dependencies

Other Tanium solutions are required for Integrations Gallery to function (required dependencies) or for specific Integrations Gallery features to work (feature-specific dependencies). For more information, see Solution dependencies on page 13.

Verify Integrations Gallery version

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

© 2025 Tanium Inc. All Rights Reserved

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

Troubleshoot issues

If you experience issues with installing Integrations Gallery, you can troubleshoot issues. For more information, see Troubleshooting Integrations Gallery on page 96.

© 2025 Tanium Inc. All Rights Reserved

Configuring Integrations Gallery

Configure Integrations Gallery

Link your Account Portal

Link your Account Portal to view artifacts related to your Tanium instance.

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. Click Settings and then click **Link Account Portal**.

   TIP

   To link a different Tanium Server instance, click **Move** and then enter information to link the different instance. For more information, see Tanium Account User Guide: Moving a Tanium instance to a different Tanium account.
3. Link a Tanium instance. For more information, see Tanium Account User Guide: Moving a Tanium instance to a different Tanium account.

Move your Tanium Account

You can link a different Tanium Server instance, but moving the linkage can cause some integrations to stop working or change behavior.

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. Click Settings and then click **Move**.
3. Enter the **Username** for the new account to which you want to move the instance and click **Move**.
4. Click the link that appears in the dialog, and sign in to your Tanium Account using the new account.
5. When prompted, click **Yes** to grant your Tanium instance the necessary access privileges to communicate with the new account in your Tanium Account.

Set up Integrations Gallery users

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

For more information about specific permissions for each role, see User role requirements on page 15.

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

Integrations Gallery Administrator

Assign the **Integrations Gallery Administrator** role to users who manage the configuration of Integrations Gallery. This role can perform the following tasks:

© 2025 Tanium Inc. All Rights Reserved

- Configure Integrations Gallery service settings.
- View and modify the configuration of all integrations in Integrations Gallery.

Integrations Gallery Operator

Assign the **Integrations Gallery Operator** role to users who manage the configuration of all integrations in Integrations Gallery.

Integrations Gallery Viewer

Assign the **Integrations Gallery Viewer** role to users who need visibility into Integrations Gallery data.
This role can perform the following tasks:

- View Integrations Gallery service settings.
- View configurations of all integrations.

© 2025 Tanium Inc. All Rights Reserved

Managing the Microsoft Azure VM Extensions integration

Tanium provides Azure virtual machine (VM) extensions that can be installed to automatically deploy the Tanium Client on Microsoft Azure VMs and VM Scale Sets. After deploying Tanium Client to the Microsoft Azure VMs, you can manage the VMs from Tanium Console.

For more information about deploying the Tanium Client in Microsoft Azure environments, see Tanium Client Management User Guide: Deploy the Tanium Client in Microsoft Azure environments using the Tanium Client VM extension.

Requirements

Operating system support in Microsoft Azure

The Tanium Client supports both Windows and Linux VMs in Azure. Supported versions and Linux distributions are the same as for any endpoint; for more information, see Tanium Client Management User Guide: Client version and operating system requirements. However, for Linux VMs in Azure, the Tanium Client VM extension is supported only on Linux distributions that are both endorsed by Microsoft and supported by the Tanium Client. For more information about a list of Linux distributions that are endorsed by Microsoft, see Microsoft Azure Documentation: Endorsed Linux distributions on Azure.

Tanium provides separate Azure VM extensions for Windows and Linux VMs.

Network connectivity

Each VM must be able to connect to `https://content.tanium.com` for the VM extension to import the files needed to deploy the Tanium Client.

Computer group dependencies

When you first Sign in to Tanium Console after a fresh installation of Tanium Server, the server automatically imports the computer groups that Integrations Gallery requires:

- Integration - All Installed by Azure
- Integration - All Linux Installed by Azure
- Integration - All Windows Installed by Azure

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

User role requirements

Predefined roles grant the following permissions, which are required to use Microsoft Azure VM Extensions functionality:

© 2025 Tanium Inc. All Rights Reserved

- Microsoft Azure VM Extensions solution permissions on page 23
- Microsoft Azure VM Extensions administration and platform content permissions on page 24: The solution permissions automatically provide some of these permissions.

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

Microsoft Azure VM Extensions solution permissions

Permission	Integration Operator - Azure VM Extensions[1]	Integration Viewer - Azure VM Extensions[1]
Partner Integration View the Integrations Gallery workbench	SHOW	SHOW
Partner Integration Api Use the Integrations Gallery API	EXECUTE	EXECUTE
Partner Integration Gallery View and configure the Integrations Gallery	READ	READ
Partner Integration Gallery Account Management View the Account Management settings in Integrations Gallery	READ	READ
Partner Integration Gallery Azure Vm Extensions View and configure the Azure VM Extensions integration	READ WRITE	READ

© 2025 Tanium Inc. All Rights Reserved

Microsoft Azure VM Extensions solution permissions (continued)

Permission	Integration Operator - Azure VM Extensions[1]	Integration Viewer - Azure VM Extensions[1]
Partner Integration Reporting Metrics View reporting metrics in Integrations Gallery	READ	READ

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

Microsoft Azure VM Extensions administration and platform content permissions

Permission	Permission Type	Integration Operator - Azure VM Extensions	Integration Viewer - Azure VM Extensions
Action Group	Administration	READ	READ
Public Key	Administration	READ	
Filter Group	Platform	READ	READ
Package	Platform	READ	READ
Plugin	Platform	READ EXECUTE	READ EXECUTE
Sensor	Platform	READ	READ

To view the content sets to which the platform content permissions apply, see Tanium Console User Guide: View effective role permissions.

View the Details page

The **Details** page for the Microsoft Azure VM Extensions integration shows the following information:

- **Service Enablement** toggle
- **Configuration** status
- **Installations** count
- **Initialization Profile File Downloads** count

© 2025 Tanium Inc. All Rights Reserved

- **Access** link
- **Usage** reports
    - **Client Installations by Azure VM Extensions**
    - **Client Installations by All Methods**

To view the **Details** page:

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Microsoft Azure VM Extensions**.

View the Configuration page

The **Configuration** page for the Microsoft Azure VM Extensions integration shows the following information:

- **Tanium Client Initialization Profiles**: For more information, see Create a Tanium Client initialization profile on page 26.
- **Role Assignment**: For more information, see User role requirements on page 22.
- **Computer Groups**: For more information, see Computer group dependencies on page 22.

To view the **Configuration** page:

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Microsoft Azure VM Extensions**.
3. Click **Configuration**.

View the Tanium Content page

The **Tanium Content** page for the Microsoft Azure VM Extensions integration shows the following information:

- **Dashboards**
    - **Deployments using Azure VM Extensions**
    - **Deployments using Azure VM Extensions - Over Time**
- **Reports**
    - **Azure VM Extension Usage**
    - **Deployments using Azure VM Extensions - Over Time**

To view the **Tanium Content** page:

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Microsoft Azure VM Extensions**.
3. Click **Tanium Content**.

© 2025 Tanium Inc. All Rights Reserved

View the Support page

The **Support** page for the Microsoft Azure VM Extensions integration shows the following information:

- **Create Package** button to create a troubleshooting package for support requests

To view the **Support** page:

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Microsoft Azure VM Extensions**.
3. Click **Support**.

View the About page

The **About** page for the Microsoft Azure VM Extensions integration shows the following information:

- **Tanium Client Deployment Automation** video
- **VM Extension for Linux**
- **VM Extension for Windows**
- **Tanium Initialization Files**

To view the **About** page:

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Microsoft Azure VM Extensions**.
3. Click **About**.

Enable the integration

To get started, you must enable the Microsoft Azure VM Extensions integration.

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Microsoft Azure VM Extensions**.
3. Click **Enable** and then confirm your selection.

You can also access the Microsoft Azure portal by clicking **Open Azure Portal**.

Create a Tanium Client initialization profile

You can create a Client initialization profile in Integrations Gallery to create the `tanium-init.dat` file that can be used to deploy the Tanium Client to Microsoft Azure VMs and VM Scale Sets.

© 2025 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Microsoft Azure VM Extensions**.
3. Click **Configuration** and then click **Create Profile**.
    a. In the **Details** section, enter a **Name** and optionally a **Description**, and select a content set.
    b. In the **Configuration** section, configure any Tanium Server and Client options.
        - Enter a comma-separated list of Tanium **Server Names**, used to manage the Clients. Entering a server name automatically adds the **server_name_list** Client setting. Include host names in any of the following formats:

Tanium Server name format	Format example
host name without port number	`host.example.com`
host name with port number	`host.example.com:8080`
IP address without port number	`192.0.2.10`
IP address with port number	`192.0.2.10:8080`

        - Enter a Tanium **Server Port**, used for establishing a connection with each Tanium Server. Entering a server port automatically adds the **server_port** Client setting. If you specify a host name with port number or IP address with port number in the **Server Names** list, that port number takes priority over this **Server Port** value.
        - If deployed Clients must connect through a proxy server, select one of the following **Proxy** options:
            - **PAC file** (Windows endpoints only): Use a proxy auto-config (PAC) file to configure the proxy on endpoints. Selecting this option automatically adds the **proxy_auto_config_address** Client setting. Configure the URL of the PAC file for the value.
            - **Proxy Server**: Use specific addresses to connect endpoints through a proxy server. Selecting this option automatically adds the **proxy_servers** Client setting. Configure the addresses of proxy servers for the value.

              For more information about using a proxy server, see Tanium Client Management User Guide: Connect through an HTTPS forward proxy server.
        - Enter a **Log Level** for the Tanium Client on targeted endpoints, associated with the **log_verbosity_level** Client setting. The following values are best practices for specific scenarios:
            - `1` (default): Use this value during normal operation.
            - `41`: Use this value during troubleshooting.
            - `91` or higher: Use this value for full logging, for short periods of time only.



A value of `0` disables logging. As a best practice, do not disable logging.

© 2025 Tanium Inc. All Rights Reserved

- To add a custom tag to the Client during deployment, click **Add Custom Tag** and enter a tag name. The `InstalledByAzure` tag is included by default so that you can later easily target Clients that were installed using the Tanium Client VM extension in Integrations Gallery.

4. Click **Create**.

Obtain the `tanium-init.dat` file for deployment

You can copy the base64-encoded version of the `tanium-init.dat` file, or optionally download the file to use when installing the Tanium Client VM extension.

You use the base64-encoded contents during installation of the extension. However, you can download the `tanium-init.dat` file if you use a parameter in template or policy JSON to import the file directly or if you need the file for other deployment purposes.



Be careful not to allow the `tanium-init.dat` file to be distributed or stored outside of your organization, such as in a publicly accessible source code repository or any other location accessible from the public internet. Limit the distribution to specific use in the deployment of Tanium Clients.

Though this file does not contain private keys and cannot be used to provide control over a Tanium environment, a user with malicious intent could use it to connect an unapproved Client and use this unauthorized access to learn how your organization is using Tanium.

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Microsoft Azure VM Extensions**.
3. Click **Configuration**.
4. Copy the base64-encoded contents of a file for a profile, or download the file for one or more profiles:
   - To copy the base64-encoded contents of a `tanium-init.dat` file for a profile, click Copy base64-encoded profile to clipboard in the row for the profile.
   - To download the `tanium-init.dat` files for one or more profiles, click **Configuration**, select one or more profiles, and then click Download.

     If you select multiple profiles, you download a ZIP file that contains the `tanium-init.dat` file for each selected profile.
5. Follow the steps in Tanium Client Management User Guide: Installation methods for the Tanium Client VM extension.

© 2025 Tanium Inc. All Rights Reserved

TIP

You can click **Download All** to download a ZIP file of all profiles.

Disable the integration

Disable the Microsoft Azure VM Extensions integration to stop deploying Tanium Client on Microsoft Azure VMs and VM Scale Sets.

IMPORTANT

If you disable the Microsoft Azure VM Extensions integration, the VM extension is still installed in Azure. Remove the extension if you want to fully remove the integration. For more information, see Microsoft Azure documentation: Rerun a VM extension.

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Microsoft Azure VM Extensions**.
3. On the **Details** page, click the **Service Enablement** toggle.

Troubleshoot the Azure VM Extensions integration

If the Microsoft Azure VM Extensions integration is not performing as expected, you might need to troubleshoot issues or change settings.

Collect logs

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

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Microsoft Azure VM Extensions**.
3. Click **Support**.
4. Click **Create Package**.
   An `integrations-gallery-support-bundle-[timestamp].zip` file downloads to the local download directory.
5. Contact Tanium Support to determine the best option to send the ZIP file. For more information, see View the Support page on page 26.

Cannot install the Tanium Client VM extension on Microsoft Azure VMs

If you encounter an issue with the installation of the Tanium Client VM extension, check the following items:

© 2025 Tanium Inc. All Rights Reserved

1. Make sure the OS on the VM is both supported by the Tanium Client and endorsed by Microsoft. For more information, see Operating system support in Microsoft Azure on page 22.
2. If an ARM template or an Azure Policy fails to evaluate, review the template or policy for errors. For more information, see Microsoft Azure Documentation: Azure virtual machine extensions and features and contact Microsoft Support if necessary. You can try installing the extension on an endpoint manually to make sure the extension itself is working with the VM. For more information, see Tanium Client Management User Guide: Manually install the extension using the Azure Portal, Azure CLO, or Azure PowerShell.
3. If you corrected all issues in a template or policy and continue to experience installation issues, or if you cannot manually install the extension, Contact Tanium Support on page 96 for assistance.

© 2025 Tanium Inc. All Rights Reserved

Managing the Microsoft Security Copilot integration

IMPORTANT

To use the Tanium integration with Microsoft Security Copilot, you must be:

- a Microsoft Security Copilot subscriber
- a Tanium on-premises customer

For more information on Microsoft Security Copilot, see Microsoft Security documentation: What is Microsoft Security Copilot?.

The Tanium plugin for Microsoft Security Copilot enables responses to natural language prompts using Tanium-gathered information and insight. The Security Copilot large language model (LLM) can use these Tanium Skills to query your network, and to respond with the collected information and additional context as needed.

Requirements

Core platform dependencies

Make sure that your environment meets the following requirements:

- **Tanium™ Core Platform servers**
- **Tanium™ Client**: No client requirements.

  NOTE

  For the best results, deploy Tanium Client 7.6 or later to endpoints in your environment. Endpoints running Tanium Client 7.5 and earlier might provide slower responses to questions, which might negatively impact Security Copilot integration performance.

Required dependencies

The Security Copilot integration has the following required dependencies:

- Tanium Interact to view Tanium Console Question Results pages
- Tanium Gateway for Security Copilot integration with Tanium

© 2025 Tanium Inc. All Rights Reserved

Feature-specific dependencies

- Tanium Asset to prompt Security Copilot for information related to Software Bill of Materials (SBOM)
- Tanium Certificate Manager to prompt Security Copilot for information related to encryption certificates
- Tanium Comply to prompt Security Copilot for vulnerability information
- Tanium Direct Connect to view the Threat Response Live Connections page after prompting Security Copilot for a list of running endpoint processes
- Tanium Discover to prompt Security Copilot for information related to Discover content
- Tanium Enforce to prompt Security Copilot for information related to Enforce content
- Tanium Impact to prompt Security Copilot for information related to Impact content
- Tanium Incident Response to prompt Security Copilot for information related to service module, service process, and related information
- Tanium Index to prompt Security Copilot for information related to file metadata
- Tanium SBOM to prompt Security Copilot for information related to SBOM
- Tanium Threat Response to prompt Security Copilot for information related to processes and process details

User role and persona requirements

The following table lists the roles to associate with the persona, required to configure the Security Copilot integration. For more information on personas, see Tanium Console User Guide: Managing personas.

Roles associated with Microsoft Security Copilot Operator persona

Role	Description
Gateway User	system role to generate an API token that has permission to submit Gateway queries
Integration Operator - Security Copilot	system role to use the Security Copilot integration
Interact Power User	system role to view Tanium Console question results

Predefined roles grant the following permissions, which are required to use Microsoft Security Copilot functionality:

- Microsoft Security Copilot integration user role permissions on page 33
- Microsoft Security Copilot integration administration and platform content permissions on page 34: The solution permissions automatically provide some of these permissions.

Some Microsoft Security Copilot integration 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 the Microsoft Security Copilot integration. If you create custom roles for Microsoft Security Copilot integration users, be sure to assign all the solution permissions and content set permissions that are required for Microsoft Security Copilot integration 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:

© 2025 Tanium Inc. All Rights Reserved

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

Microsoft Security Copilot integration user role permissions

Permission	Integration Operator - Security Copilot[1]	Integration Viewer - Security Copilot[1]
Partner Integration View the Integrations Gallery workbench	✅ SHOW	✅ SHOW
Partner Integration Api Use the Integrations Gallery API	✅ EXECUTE	✅ EXECUTE
Partner Integration Credentials View and configure the Integrations Gallery credentials	✅ READ	❌
Partner Integration Gallery View and configure the Integrations Gallery	✅ READ	✅ READ
Partner Integration Gallery Account Management View the Account Management settings in Integrations Gallery	✅ READ	✅ READ
Partner Integration Gallery Copilot View and configure the Security Copilot integration	✅ READ WRITE	✅ READ
Partner Integration Reporting Metrics View reporting metrics in Integrations Gallery	✅ READ	✅ READ

© 2025 Tanium Inc. All Rights Reserved

Microsoft Security Copilot integration user role permissions (continued)

Permission	Integration Operator - Security Copilot[1]	Integration Viewer - Security Copilot[1]
Security Copilot Operate the Security Copilot integration	✓ OPERATOR	✗

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

Microsoft Security Copilot integration administration and platform content permissions

Permission	Permission Type	Integration Operator - Security Copilot	Integration Viewer - Security Copilot
Action Group	Administration	✓ READ	✓ READ
Filter Group	Platform	✓ READ	✓ READ
Package	Platform	✓ READ	✓ READ
Plugin	Platform	✓ READ EXECUTE	✓ READ EXECUTE
Sensor	Platform	✓ READ	✓ READ

To view the content sets to which the platform content permissions apply, see Tanium Console User Guide: View effective role permissions.

View the Details page

The **Details** page for the Microsoft Security Copilot integration shows the following information:

- **Service Enablement** toggle
- **Configuration** status
- **Access** link

© 2025 Tanium Inc. All Rights Reserved

- **Usage** reports
    - **Unique Users for Copilot**
    - **Tanium Requests by Copilot**
    - **Most Used Sensors**

To view the **Details** page:

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Microsoft Security Copilot**.

View the Configuration page

The **Configuration** page for the Microsoft Security Copilot integration shows the following information:

- **Register Tanium with Microsoft Security Copilot** configuration
- **Role Assignment**: For more information, see User role and persona requirements on page 32.

To view the **Configuration** page:

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Microsoft Security Copilot**.
3. Click **Configuration**.

View the About page

The **About** page for the Microsoft Security Copilot integration shows the following information:

- **AI Powered Real-Time Insights** video
- **Enhanced Security**
- **Vulnerability Management**
- **Data-Driven Decision Making**

To view the **About** page:

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Microsoft Security Copilot**.
3. Click **About**.

© 2025 Tanium Inc. All Rights Reserved

Configure integration between Tanium and Security Copilot

Allow secure network connections between Tanium and Microsoft Security Copilot

BEST PRACTICE

For the best results, migrate your deployment to Tanium™ Cloud. Tanium Cloud infrastructure establishes secure network connections between Tanium and Microsoft Security Copilot. For more information, contact Support.

The Security Copilot integration requires bidirectional network communication between the Tanium Server and Security Copilot. Ensure that the Security Copilot egress IP address for your Azure region can establish bidirectional communication with the Tanium Server over port 443/TCP (HTTPS), and decrypt incoming traffic to the Tanium Server to verify that the traffic originates from a trusted source. For more information, see Configure integration between Tanium and Third-party products.

Set up Tanium integration with Security Copilot users

Configure Tanium plugin for Security Copilot

NOTE

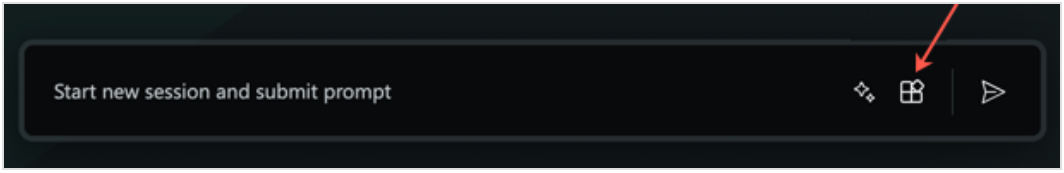
By default, the API token generated from the settings page is valid for 365 days and is not associated with a trusted IP address. You can instead generate an API token from the **API Tokens** page and configure a trusted IP address from the list of Security Copilot egress IP addresses. For more information about how to configure an API token with trusted IP addresses, see Allow Security Copilot egress IP addresses. For more information about how to rotate an API token, see Rotate Security Copilot API tokens.

Establish communication between a Tanium instance and Security Copilot using:

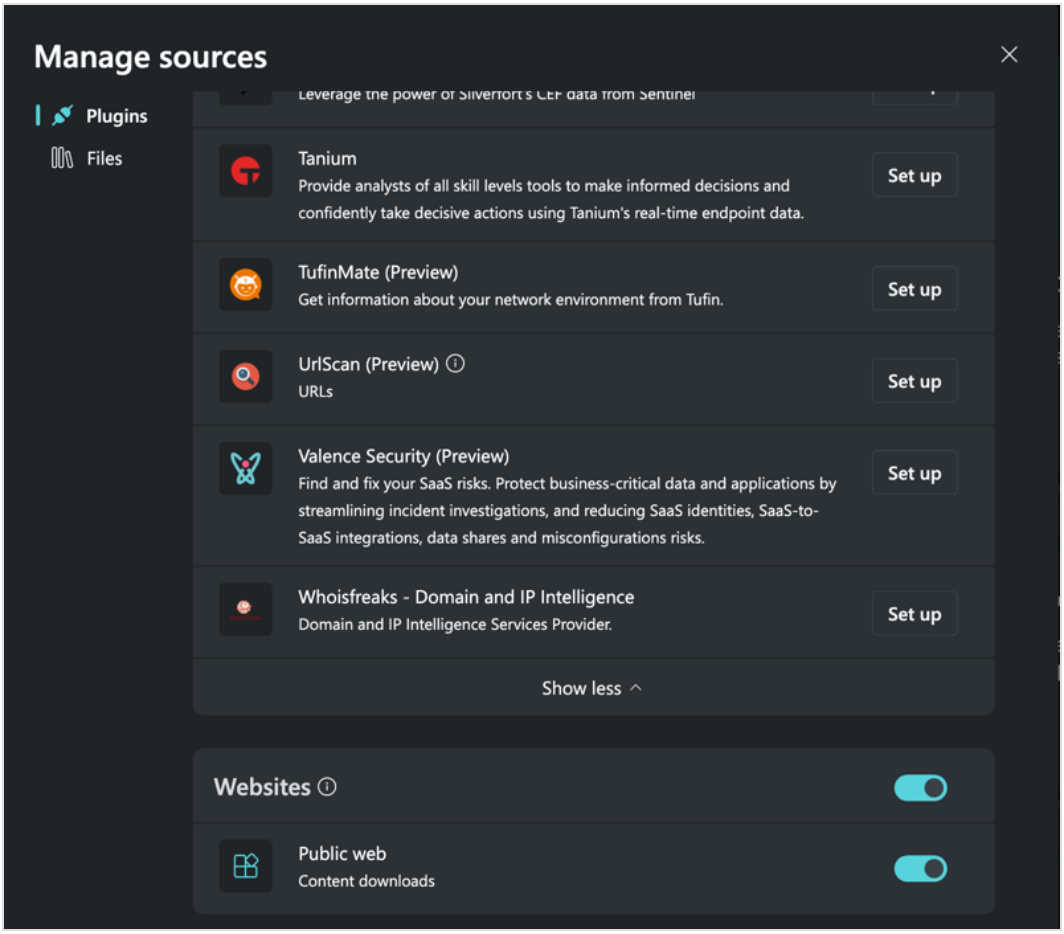
- a URL to a Tanium instance and manifest json file to connect Security Copilot to the Tanium instance and configure skills
- a Tanium API token to grant Security Copilot permission to query your network using Tanium and gather endpoint data

© 2025 Tanium Inc. All Rights Reserved

1. In a browser window, navigate to the Microsoft Security Copilot home page.
2. In the prompt bar at the bottom of the Microsoft Security Copilot home page, click Security Copilot plugin .

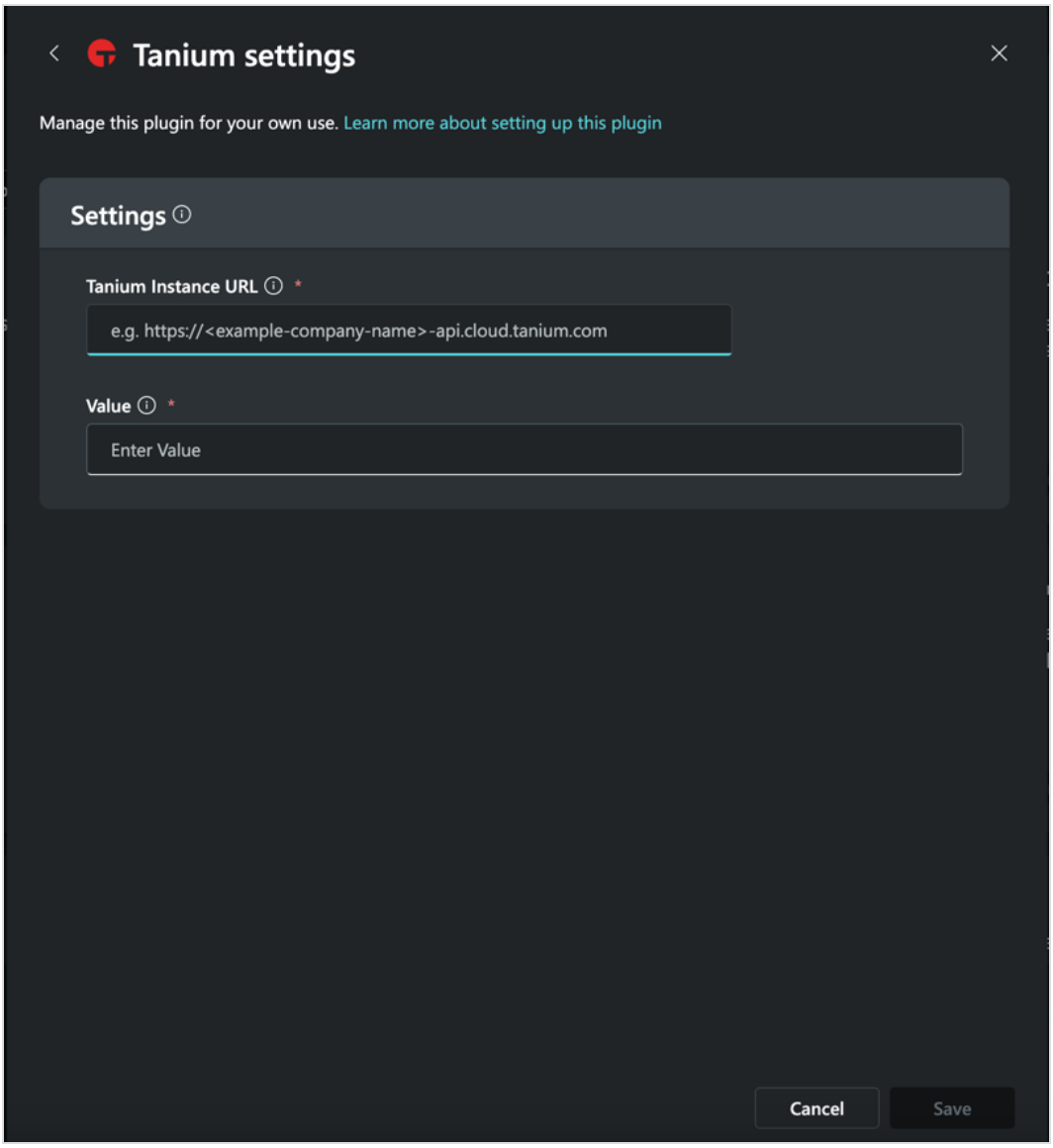


The Manage sources modal appears.



© 2025 Tanium Inc. All Rights Reserved

3. From the list of plugins, click **Set up** next to the **Tanium** plugin. The Tanium settings modal appears.



4. In a separate browser window, navigate to Tanium Console.
5. Click **Tanium Instance URL** Copy to copy the Tanium instance URL to the clipboard.
6. In Security Copilot, paste the **Tanium Instance URL** in the Tanium settings modal.
7. You cannot view the token value in Tanium Console. Paste the value in a plaintext editor and save the file in a secure location if you want to record it for future reference.
8. In Security Copilot, paste the API token value in the **Value** field in the Tanium settings modal.
9. Click **Save**.

© 2025 Tanium Inc. All Rights Reserved

Use Tanium prompts with Security Copilot

Use Tanium prompts with Microsoft Security Copilot to prompt for information about hosts on your network. Security Copilot supports natural language prompts and prompt suggestions:

Types of prompts with Security Copilot

Prompt type	Description	Notes
natural language prompt	a free-form question or request that uses natural language	Natural language prompts offer a more conversational experience when interacting with Security Copilot, and might return more comprehensive responses than prompt suggestions. For more information, see Microsoft Security Copilot documentation: Create your own prompts.
prompt suggestion	an available plugin skill, selected from the list of available system capabilities, and user-provided parameters	Prompt suggestions offer a more structured experience when interacting with Security Copilot, and might return less comprehensive responses than natural language prompts. For more information, see Microsoft Security Copilot documentation: Using the prompts library.

Depending on your situation, submitting a natural language prompt might be more efficient than submitting a prompt suggestion.

A well-composed natural language prompt enables an AI model to better provide a relevant response. AI models might match prompt context and specificity, and might respond to a less-focused prompt with sparse or generic information. Issuing additional prompts to improve response quality increases overall computing resources use and decreases efficiency, compared to a single prompt that retrieves relevant information. Use the following best practices to create a natural language prompt:

Best practices for natural language prompts

Natural language prompt attribute	Considerations
Unambiguous language	• Avoid slang terms and metaphors, which might be interpreted in a different way than intended. • Be consistent with words, phrases, and capitalization within a prompt, as AI models might use additional computing resources to evaluate the same term stated in different ways (such as "endpoint" versus "Endpoint", or "endpoint" versus "workstation"). • Use punctuation, such as commas, colons, and periods, to reduce ambiguity within a prompt.

© 2025 Tanium Inc. All Rights Reserved

Best practices for natural language prompts (continued)

Natural language prompt attribute	Considerations
Specific request	• Start the prompt with a clear, defined task that reflects the information that you want. For example, "Return all endpoints that have risks." does not limit endpoint type or specify the risk type. "Return all Windows endpoints that are running unusual processes and require further investigation." specifies which endpoints to focus on, the risk type (unusual running processes), and the goal of conducting an investigation. • Define a persona so that the AI model can tailor the response to a specific audience. For example, specifying a junior security operations center (SOC) member or a SOC lead helps the AI model to emphasize information relevant for that audience. • Provide relevant and detailed context in the prompt. When providing context, avoid negation and instead request an alternative, as an AI model might misinterpret a negated request. For example, instead of submitting "Do not return Windows 11 endpoints," submit "Instead of Windows 11 endpoints, return endpoints running Windows 10 or earlier versions." • Define information you want in the response and the response output format, such as returning information in a table. For example, instead of "Return the affected endpoints," submit "Return the IP address and host name of affected endpoints in a table, sorted in ascending alphabetical order by host name."
Structured format	• Add additional structure, especially if the prompt contains a complex request. For example, if you want to retrieve multiple types of endpoint information from different endpoint types, add lists of requests to your prompt, such as "For Windows endpoints only, return the IPv4 address, MAC address, and host name. For Linux endpoints only, return the IPv4 address, host name, and Linux distribution and version." • Break down a complex end goal into smaller, defined intermediate steps. Instead of "Provide a summary of remediation steps for all endpoints vulnerable to CVE-2014-123456," submit "Summarize the CVE-2014-123456 vulnerability and the effect on endpoints for a junior SOC member. Identify all endpoints on the network that are vulnerable to CVE-2014-123456. Return these endpoints in a table, and also list the remediation steps necessary to patch these endpoints or otherwise remove the vulnerability from these endpoints, and provide relevant detail for a junior SOC member."

Note the following:

- Microsoft charges Security Copilot users based on the provisioned Security Compute Units (SCU). For more information, see Microsoft Azure documentation: Microsoft Security Copilot pricing.
- Submitting a prompt and receiving a response might take several seconds or more. As you submit additional prompts in a single session, the time to respond might increase. The Security Copilot LLM analyzes all session information, including prior prompts and responses. As a result, creating multiple sessions for different lines of inquiry might save time over a single session containing multiple lines of inquiry.
- Adding specific context to a natural language prompt might improve response accuracy. For example, adding `Using Tanium` to your prompt provides additional context to the Security Copilot LLM to select a relevant Tanium Skill. Alternatively, narrowing the scope of a natural language prompt to a specific host on your network might provide a more relevant response for your situation, rather than prompting for all hosts on the network.

© 2025 Tanium Inc. All Rights Reserved

For more information about how to submit prompts to Security Copilot, see Microsoft Security Copilot documentation: Prompting in Microsoft Security Copilot and Microsoft Security Copilot documentation: Create effective prompts.

Tanium Skills example prompts

The following table provides example natural language prompts related to each Tanium Skill.

> **NOTE** Before submitting an example natural language prompt to Security Copilot, update any variables and adjust the prompt based on your situation or goal.

Natural language prompts related to each Tanium Skill

Required Tanium solutions	Tanium Skill prompt suggestion	Description	Example natural language prompts
Tanium Core Platform	Get Logged In User	Retrieve the user that is currently logged into an endpoint.	`Using Tanium, return the user currently logged into the endpoint with the hostname <hostname> so that I, a junior security operations center member, can investigate possible unauthorized endpoint use. Return a Tanium Console Question Results URL so that I can view more real-time information for this endpoint. Thank you.`
Tanium Core Platform, sensor-dependent	Get Real-time Data from Endpoints	Retrieve real-time data from endpoints based on a Tanium sensor. For more information about supported sensors, see Get Real-time Data from Endpoints prompt sensor support on page 47.	`Using Tanium, return the computer name and IP address of endpoints. Display the results in a table, alphabetically sorted by computer name, and return a Tanium Console Question Results URL so that I, a junior security operations center member, can view the real-time list of endpoints. Thank you.`
Asset, SBOM	Count Endpoints Having Package Version	Retrieve the total number of endpoints that have the given software package at a version.	`Using Tanium, return the total number of endpoints that have a given software package <software-name> at version <software-version>, so that I, a junior security operations center member, can start cataloging which computers have the software installed. Display the results in a table, alphabetically sorted by operating system, and return a Tanium Console Question Results URL so that I can view the real-time list of endpoints. Thank you.`

© 2025 Tanium Inc. All Rights Reserved

Natural language prompts related to each Tanium Skill (continued)

Required Tanium solutions	Tanium Skill prompt suggestion	Description	Example natural language prompts
Asset, SBOM	List Endpoints Having Package	Retrieve up to 10 endpoints that have the given software package.	`Using Tanium, return the endpoints with a software package for <software-name> so that I, a junior security operations center member, can start cataloguing which computers might have an out-of-date version. Display the results in a table, alphabetically sorted by host name, and return a Tanium Console Question Results URL so that I can view the real-time list of endpoints. Thank you.`
Asset, SBOM, Threat Response	List Process SHA-256 Hashes and Versions	Retrieve the SHA-256 file hash and version for a given process	`Using Tanium, return the SHA-256 hash value and process version for the running process <process-name>, so that I, a junior security operations center member, can find other instances of this process based on the hash value. Thank you.`
Comply	Get Vulnerability Test Results	Return whether an endpoint is vulnerable to a given CVE, and the reason why it is vulnerable.	`Using Tanium, examine whether endpoint <hostname> is vulnerable to <cve-id>, and return the reasons that this endpoint is vulnerable, along with a suggested plan of action to remediate the intrusion tailored to a junior security operations center member. Thank you.`
Comply	List Endpoints Vulnerable To CVE	Retrieve up to 10 endpoints vulnerable to a given CVE ID.	`Using Tanium, return the endpoints vulnerable to <cve-id>, so that I, a junior security operations center member, can remediate the vulnerability on these endpoints. Display the results in a table, sorted alphabetically by host name, and return a Tanium Console Question Results URL so that I can view the real-time list of endpoints. Thank you.`
Direct Connect, Threat Response	View Endpoint Processes	Retrieve a URL to the Threat Response Live Connection page for the requested endpoint, which contains a list of running processes. The hostname must match an endpoint hostname exactly.	`Using Tanium, return a Threat Response Live Connection URL for the endpoint with the hostname <hostname>, so that I, a junior security operations center member, can review the running processes and identify potential vulnerabilities. Thank you.`

© 2025 Tanium Inc. All Rights Reserved

Natural language prompts related to each Tanium Skill (continued)

Required Tanium solutions	Tanium Skill prompt suggestion	Description	Example natural language prompts
Incident Response	List Hashes of File	Retrieve the SHA-256 and MD5 file hashes for a given file.	`Using Tanium, retrieve the MD5 and SHA-256 hashes for the file at the file path <full-file-path> so that I, a junior security operations center member, can determine if any malicious file behavior is occurring on the endpoint. Display the results in a table, alphabetically sorted, and return a Tanium Console Question Results URL so that I can view the real-time list. Thank you.` `Using Tanium, retrieve the MD5 and SHA-256 hashes for the file at the file path <full-file-path> on the endpoint named <hostname> so that I, a junior security operations center member, can determine if any malicious file behavior is occurring on the endpoint. Display the results in a table, alphabetically sorted, and return a Tanium Console Question Results URL so that I can view the real-time list. Thank you.`
Incident Response	List Service Module Details	Retrieve running service module information for an endpoint, including name, caption, and image path.	`Using Tanium, return information for the service modules running on the endpoint with the hostname <hostname>, so that I, a junior security operations center member, can review the list for unexpected service modules. Display the results in a table, alphabetically sorted by service module name, and return a Tanium Console Question Results URL so that I can view the real-time list of service modules. Thank you.`
Incident Response	List Service Process Details	Retrieve running service process information for an endpoint, including name, process ID, and file path.	`Using Tanium, return information for the service processes running on the endpoint with the hostname <hostname>, so that I, a junior security operations center member, can review the list for unexpected service processes. Display the results in a table, alphabetically sorted by service process name, and return a Tanium Console Question Results URL so that I can view the real-time list of service processes. Thank you.`

© 2025 Tanium Inc. All Rights Reserved

Natural language prompts related to each Tanium Skill (continued)

Required Tanium solutions	Tanium Skill prompt suggestion	Description	Example natural language prompts
Incident Response	List WMI Event Consumers	Retrieve Windows Management Instrumentation (WMI) event consumers running on an endpoint.	`Using Tanium, return the WMI event consumers running on the endpoint with the hostname <hostname> so that I, a junior security operations center member, can ensure only expected event consumers are running, and return a Tanium Console Question Results URL so that I can view the real-time list of event consumers. Thank you.`
Index	List File Details	Retrieve details for a file by name, including the endpoints on which it is installed, the file path, and file size.	`Using Tanium, return information for the file named <file-name> so that I, a junior security operations center member, can determine if it is running on unintended endpoints. Display the results in a table, alphabetically sorted, and return a Tanium Console Question Results URL so that I can view the real-time list. Thank you.`  `Using Tanium, return information for the file named <file-name> installed on the endpoint with the hostname <hostname>, so that I, a junior security operations center member, can determine if it is running on unintended endpoints. Display the results in a table, alphabetically sorted, and return a Tanium Console Question Results URL so that I can view real-time information. Thank you.`
Threat Response	List Child Processes for Process File	Return all child processes running on an endpoint based on a given process file name.	`Using Tanium, list the child processes of <process-name> so that I, a junior security operations center member, can analyze resource usage. Display the results in a table, alphabetically sorted by process name, and return a Tanium Console Question Results URL so that I can view the real-time list of endpoints. Thank you.`  `Using Tanium, list the child processes of <process-name> that are running on the computer with the hostname <hostname>, so that I, a junior security operations center member, can analyze resource usage. Display the results in a table, alphabetically sorted by process name, and return a Tanium Console Question Results URL so that I can view the real-time list of endpoints. Thank you.`

© 2025 Tanium Inc. All Rights Reserved

Natural language prompts related to each Tanium Skill (continued)

Required Tanium solutions	Tanium Skill prompt suggestion	Description	Example natural language prompts
Threat Response	List Endpoints with Process Command	Retrieve up to 10 endpoints running the given command-line command.	`Using Tanium, return the endpoints running the command line command <process-command>, so that I, a junior security operations center member, can ensure this process is not running on unexpected endpoints. Display the results in a table, sorted alphabetically by host name, and return a Tanium Console Question Results URL so that I can view the real-time list of endpoints. Thank you.`
Threat Response	List Endpoints with Process Name	Retrieve up to 10 endpoints running the given process.	`Using Tanium, return the endpoints running a process called <process-name>, so that I, a junior security operations center member, can ensure this process is not running on unexpected endpoints. Display the results in a table, sorted alphabetically by host name, and return a Tanium Console Question Results URL so that I can view the real-time list of endpoints. Thank you.`
Threat Response	List Endpoints with Process MD5 Hash	Retrieve up to 10 endpoints running the given process matching the provided MD5 hash value.	`Using Tanium, return all endpoints that are running a process with the MD5 hash value <md5-hash-value>, so that I, a junior security operations center member, can ensure this process is not running under a different file name. Display the results in a table, sorted alphabetically by host name, and return a Tanium Console Question Results URL so that I can view the real-time list of endpoints. Thank you.`

© 2025 Tanium Inc. All Rights Reserved

Natural language prompts related to each Tanium Skill (continued)

Required Tanium solutions	Tanium Skill prompt suggestion	Description	Example natural language prompts
Threat Response	List File Operations	Retrieve historical file operation information from endpoints, including endpoint name, file path, and the file operation type, such as create or delete.	`Using Tanium, return file operation information for the endpoint named <hostname> running on the file path "<partial-file-path>" over the past <time-frame> so that I, a junior security operations center member, can determine if any malicious file behavior is occuring on the endpoint. Display the results in a table, alphabetically sorted, and return a Tanium Console Question Results URL so that I can view the real-time list. Thank you.`  `Using Tanium, return file operation information for files running on the file path "<partial-file-path>" over the past <time-frame> so that I, a junior security operations center member, can determine if there is any malicious file creation or deletion. Display the results in a table, alphabetically sorted, and return a Tanium Console Question Results URL so that I can view the real-time list. Thank you.`
Threat Response	List Processes Connected To IPv4 Address	Retrieve the processes running on an endpoint with the given IPv4 address.	`Using Tanium, return the processes running on the endpoint with the IPv4 address <ipv4-address>, so that I, a junior security operations center member, can analyze any potential security intrusions and resource usage. Display the results in a table, sorted alphabetically by process name, and return a Tanium Console Question Results URL so that I can view the real-time list of endpoints. Thank you.`

© 2025 Tanium Inc. All Rights Reserved

Natural language prompts related to each Tanium Skill (continued)

Required Tanium solutions	Tanium Skill prompt suggestion	Description	Example natural language prompts
Threat Response	List Process Ran As User	Retrieve the processes running on an endpoint as a given user.	`Using Tanium, return the processes running as the user <user-name>, so that I, a junior security operations center member, can determine whether there are issues with unauthorized access. Display the results in a table, sorted alphabetically by computer name, and return a Tanium Console Question Results URL so that I can view the real-time list of endpoints. Thank you.`  `Using Tanium, return the processes running as the user <user-name> on the endpoint with the hostname <hostname>, so that I, a junior security operations center member, can determine whether there are issues with unauthorized access. Display the results in a table, sorted alphabetically by process name, and return a Tanium Console Question Results URL so that I can view the real-time list of endpoints. Thank you.`

Get Real-time Data from Endpoints prompt sensor support

Use the Get Real-time Data from Endpoints prompt to retrieve real-time data from endpoints based on a Tanium sensor. The following example natural language prompts incorporate language similar to a sensor name, providing additional context to Security Copilot to select a related sensor:

- `Using Tanium, return the computer name and IP address of endpoints, so that I, a junior security operations center member, can inventory endpoints on the network. Display the results in a table, alphabetically sorted by computer name, and return a Tanium Console Question Results URL so that I can view the real-time list of endpoints. Thank you.`
- `Using Tanium, return the last logged in user for endpoints, so that I, a junior security operations center member, can determine if any user accounts have been displaying suspicious behavior. Display the results in a table, alphabetically sorted by the user name, and return a Tanium Console Question Results URL so that I can view the real-time list of endpoints. Thank you.`
- `Using Tanium, return Microsoft Defender path exclusion information for endpoints, so that I, a junior security operations center member, can verify that configured path exclusions are not too broad. Display the results in a table, alphabetically sorted by computer name, and return a Tanium Console Question Results URL so that I can view the real-time list of endpoints. Thank you.`

The Get Real-time Data from Endpoints prompt supports the following sensors.

© 2025 Tanium Inc. All Rights Reserved

NOTE

You must generate an API token with permission to access the content set to which a sensor belongs to prompt Security Copilot using this sensor.

Sensors supported by the Get Real-time Data from Endpoints prompt

Content set	Sensor
AntiVirus	Microsoft Defender AntiMalware Details
AntiVirus	Microsoft Defender AntiSpyware Details
AntiVirus	Microsoft Defender AntiVirus Details
AntiVirus	Microsoft Defender Computer ID
AntiVirus	Microsoft Defender Extension Exclusions
AntiVirus	Microsoft Defender FullScan Details
AntiVirus	Microsoft Defender Health Details
AntiVirus	Microsoft Defender Installed
AntiVirus	Microsoft Defender IP Address Exclusions
AntiVirus	Microsoft Defender Network Inspection Service Details
AntiVirus	Microsoft Defender On Access Protection Status
AntiVirus	Microsoft Defender Org ID
AntiVirus	Microsoft Defender Path Exclusions
AntiVirus	Microsoft Defender Process Exclusions
AntiVirus	Microsoft Defender QuickScan Details
AntiVirus	Microsoft Defender Real-Time Protection Status
AntiVirus	Microsoft Defender Tamper Protection Status
AntiVirus	Microsoft Defender Threat Details
AntiVirus	Microsoft Defender UI Lockdown Status
Base	Endpoint Fingerprint
Base	Last Reboot
Base	Windows OS Release ID

© 2025 Tanium Inc. All Rights Reserved

Sensors supported by the Get Real-time Data from Endpoints prompt (continued)

Content set	Sensor
Certificate Manager	Certificate Manager - SSL Certificate CA Short Name
Certificate Manager	Certificate Manager - SSL Certificate Details
Certificate Manager	Certificate Manager - SSL Certificate Process Details
Certificate Manager	Certificate Manager - SSL Extended Key Usage
Certificate Manager	Certificate Manager - SSL Key Usage
Certificate Manager	Certificate Manager - SSL Server Root Certificate Authority
Certificate Manager	Certificate Manager - Supported SSL/TLS Protocols
Comply Deployment	Comply - Architecture Type
Comply Deployment	Comply - Coverage Status
Comply Reporting	Comply - Compliance Exposure Score
Comply Reporting	Comply - Compliance Findings
Comply Reporting	Comply - Compliance Findings - First Found
Comply Reporting	Comply - Compliance Findings - Last Scan
Comply Reporting	Comply - Compliance Investigation Details
Comply Reporting	Comply - Compliance Percentage
Comply Reporting	Comply - CVE Findings - Last Scan
Comply Reporting	Comply - CVE Investigation Details
Comply Reporting	Comply - Endpoint Scan Status
Comply Reporting	Comply - Has Been Scanned
Comply Reporting	Comply - Is Vulnerable
Comply Reporting	Comply - NMap Scan Results
Comply Reporting	Comply - Open Ports
Comply Reporting	Comply - Oval Findings
Comply Reporting	Comply - Vulnerability Aggregates
Comply Reporting	Comply - Vulnerability Discovery Dates

© 2025 Tanium Inc. All Rights Reserved

Sensors supported by the Get Real-time Data from Endpoints prompt (continued)

Content set	Sensor
Core AD Query Content	AD Query - Local Administrators
Core AD Query Content	AD Query - Local Groups
Core AD Query Content	AD Query - Local Users
Core AD Query Content	AD Query - Primary User
Core Content	Active Devices
Core Content	AD Distinguished Name
Core Content	AD Organizational Unit
Core Content	BIOS Vendor
Core Content	BIOS Version
Core Content	BitLocker Details
Core Content	Boot Device
Core Content	Chrome Extensions
Core Content	Cloud Instance Hostname
Core Content	CPU Details
Core Content	Disk Drive Details
Core Content	Driver Details
Core Content	Firefox Extensions
Core Content	Firewall Status
Core Content	Installed Applications
Core Content	Installed HotFixes
Core Content	Installed Pkgs
Core Content	Installed RPMs
Core Content	Installed Store Apps
Core Content	Kernel Modules
Core Content	Kernel Version

© 2025 Tanium Inc. All Rights Reserved

Sensors supported by the Get Real-time Data from Endpoints prompt (continued)

Content set	Sensor
Core Content	Last Logged In User
Core Content	Listen Ports
Core Content	Local Account Last Password Change Days Ago
Core Content	Local Administrators
Core Content	Local Administrators Without Groups
Core Content	Local User Login Dates
Core Content	Manufacturer
Core Content	Motherboard Manufacturer
Core Content	Motherboard Name
Core Content	Number of Logged In Users
Core Content	Number Of Users
Core Content	Open Share Details
Core Content	Open Shares
Core Content	Run Once Keys
Core Content	Running Applications
Core Content	Running Processes
Core Content	Running Service
Core Content	Startup Programs
Core Content	Unencrypted Wireless Networks
Core Content	Uptime
Core Content	USB Device
Core Content	User Details
Core Content	User Sessions
Core Content	Windows Security Center Registered Antivirus Software
Core Content	Wireless Network Details

© 2025 Tanium Inc. All Rights Reserved

Sensors supported by the Get Real-time Data from Endpoints prompt (continued)

Content set	Sensor
Core Content	Wireless Networks Visible
Discover Content	Open Ports
Enforce Global Objects	Enforce - FileVault Encryption Status
Enforce Global Objects	Enforce - Host Firewall Enabled
Enforce Global Objects	Enforce - Tools Version
Enforce Linux	Enforce - Firewall Rules [Linux]
Enforce Windows	Enforce - BitLocker Encryption Status
Enforce Windows	Enforce - BitLocker Protection Status
Enforce Windows	Enforce - Quarantine Details
Enforce Windows	Enforce - TPM Status
Enforce Windows	Enforce - USB Storage Devices
Impact	Impact - Active User Session SIDs
Impact	Impact - Administrator SIDs
Incident Response	AutoRun Program Details
Incident Response	Elevated Privileges
Incident Response	Loaded Modules Not Matching Whitelist
Incident Response	Running Processes With Filename Mismatch
Incident Response	Running Processes with MD5 Hash
Incident Response	Unsuccessful Elevated Privileges
Reserved	Computer ID
Reserved	Computer Name
Reserved	IP Address
Reserved	Online

Troubleshoot issues

Review troubleshooting tasks for common issues.

© 2025 Tanium Inc. All Rights Reserved

Allow Security Copilot egress IP addresses



Contact Microsoft to confirm the correct egress IP address for your geographical region. These IP addresses are subject to change.

Depending on your geographical region, Security Copilot uses one of several IP addresses for communication with the Tanium instance. Add the appropriate IP address to your network allow list to ensure inbound communication from Security Copilot to your network. For more information about egress IP addresses, see Microsoft Security documentation: Microsoft Security Copilot egress IPs.

You can also generate an API token associated with a trusted IP address that corresponds to an Azure geographical region and configure Security Copilot to use that API token. For more information about how to create an API token, see Tanium Console User Guide: Create an API token.

Rotate Security Copilot API tokens

API tokens generated for the Security Copilot integration are valid for 365 days from generation, associated with the user account creating the API token and the persona, and contain in the **Notes** field. To rotate an API token:

- Administrator users can rotate their existing API token from the **API Tokens** page, using the original token string. For more information about how to rotate an API token, see Tanium Console User Guide: Rotate an API token.
- Non-administrator users can contact an administrator to revoke the existing API token from the **API Tokens** page. The non-administrator users can then generate a new API token. For more information about how to revoke an API token, see Tanium Console User Guide: Revoke an API token.

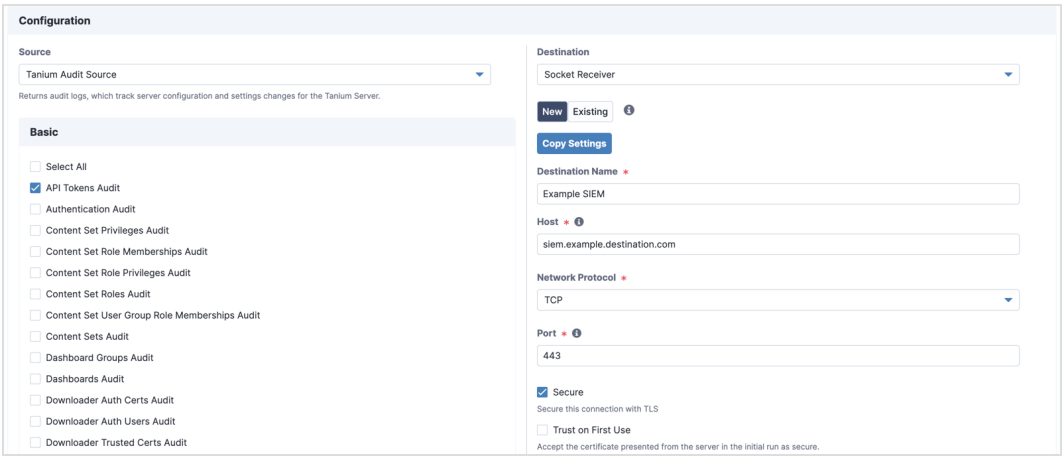
Review Security Copilot-related API token audit logging

Review API token audit logging on a periodic basis to ensure that traffic using Security Copilot-related API tokens is originating from trusted sources, such as a Microsoft egress IP address. You can configure a Connect connection using the **Tanium Audit Source** source, with a SIEM or other logging analysis solution as the destination. After the connection run finishes, filter the log entries for Security Copilot-related API token entries using a regular expression, such as .

1. From the Main menu, go to **Modules > Connect > Connections**.
2. Click **Create Connection**.
3. Enter a destination **Name**.
4. Select the **Tanium Audit Source** source. Then select **API Tokens Audit**.

© 2025 Tanium Inc. All Rights Reserved

5. Select a **Destination** and configure destination settings.



6. Optionally, in the **Schedule** section, select **Enable Schedule** and configure a schedule for connection runs.
7. Click **Save**.

For more information about how to create a Connect connection to a SIEM destination, see Tanium Connect User Guide: Configuring Socket (SIEM) destinations.

Review Security Copilot-related questions in Tanium

If Security Copilot selects the Tanium plugin to evaluate a natural language prompt or prompt suggestion, it uses the configured API token to submit questions in Tanium and generate a response. Responses might include a URL to question results in Tanium Console. You can view the question history and filter results based on the user associated with the API token to review the questions Security Copilot issues, and to confirm communication between Security Copilot and Tanium. For more information about how to view question history, see Tanium Interact User Guide: View question history.

Improve selection of Tanium Skills

To respond to a natural language prompt, Security Copilot analyzes available prompt and session context, and selects a relevant plugin and skill. If you want Security Copilot to select Tanium Skills in response to natural language prompts, and Security Copilot instead repeatedly selects non-Tanium Skills, you have the following options:

- Add specific context to a natural language prompt. For example, adding `Using Tanium` to your prompt provides additional context to the Security Copilot LLM to select a relevant Tanium Skill.
- Submit a prompt suggestion for a specific Tanium Skill.
- Submit additional Tanium Skill-related prompts in a session.
- Provide response feedback to Microsoft to help improve future versions of Security Copilot.

If Security Copilot continues to select non-Tanium Skills, you can disable other Microsoft and non-Microsoft plugins, improving the possibility that Security Copilot selects a Tanium Skill. For more information, see Microsoft Security Copilot documentation: Manage plugins in Microsoft Security Copilot.

© 2025 Tanium Inc. All Rights Reserved

NOTE

Disabling the Public web plugin, which retrieves internet content, might decrease overall response quality.

1. From the Security Copilot home page, click Security Copilot plugin . The Manage plugins modal appears.
2. Select the toggle for each enabled non-Tanium plugin to turn off the plugin.
3. Close the modal.

© 2025 Tanium Inc. All Rights Reserved

Managing the ScreenMeet Screen Sharing integration

With the ScreenMeet Screen Sharing integration, you can easily manage and have complete control of your end-user devices. Secure remote takeover gives you quick access to your endpoints. Agents and employees work together over video, voice, screen share, and mobile camera share.



To enable this functionality, you must purchase the ScreenMeet offering. With the ScreenMeet offering provided through Tanium, you must initiate all interactions with ScreenMeet through Tanium Console. Contact Tanium for details.

Requirements

- Tanium Screen Sharing is required.
- Obtain Screen Sharing per-operator licenses based on the number of Tanium Console operators you expect to establish screen sharing sessions.
    - A per-operator license is allocated to each Tanium Console operator establishing a screen sharing session or accessing the ScreenMeet console from Tanium Console. Each Tanium Console operator can create unlimited concurrent screen sharing sessions.
    - The license allocation lasts for 30 days and counts as an active operator license. The 30-day license allocation restarts each time that a Tanium Console operator establishes a screen sharing session or opens the ScreenMeet console.
    - If the active operator license count exceeds your total per-seat license count, additional Tanium console operators cannot establish a screen sharing session.
- Set up screen sharing users in Tanium. For more information about permissions provided by these roles, see User role requirements on page 58. For more information about configuring permissions to establish unattended screen sharing sessions, see Configure personas to establish unattended screen sharing sessions on page 64.
    - **Integration Admin - ScreenMeet**: With this role, a user can change settings, features and policies; access data; and join active sessions created by active users. A user assigned this role in Tanium is automatically assigned the **ScreenMeet Admin** role in ScreenMeet and can access the ScreenMeet console to configure ScreenMeet settings for the organization using a magic link accessed from the **Details** page of the **ScreenMeet Screen Sharing** integration in Integrations Gallery. For more information, see Configure ScreenMeet settings.
    - **Integration Viewer - ScreenMeet**: With this role, a user can view the ScreenMeet integration in Integrations Gallery

© 2025 Tanium Inc. All Rights Reserved

- **Screen Sharing Agent**: With this role, a user can start sharing sessions and use standard ScreenMeet features. A user assigned this role in Tanium is automatically assigned the **ScreenMeet Agent** role in ScreenMeet. This role includes the **Screen Sharing Console** permission, which allows access to the ScreenMeet console without the ability to modify organizational settings using a magic link accessed from the Direct Connect settings.
- **Screen Sharing Support Session Unattended Execute** permission: Establish unattended sessions with Windows endpoints that do not require endpoint user permission. After the user ends the unattended session, the endpoint locks by default. This permission is not assigned to any default role.
- **Screen Sharing Support Session Disable Autolock Execute** permission: Disable automatic endpoint locking after ending an unattended session that the user established. This permission requires the **Screen Sharing Support Session Unattended Execute** permission to establish unattended sessions. This permission is not assigned to any default role.



Use a least-privilege model for your screen sharing users.

- Verify endpoint operating systems. For more information, see Supported operating systems for ScreenMeet on page 58.
- Verify network requirements.
  - Configure the host and network security requirements.
  - Allow ScreenMeet application traffic through port 443/TCP and 443/UDP. ScreenMeet application traffic goes through TLS-encrypted connections.
  - The endpoints in your environment require access to certain URLs to establish screen sharing sessions. If security software is deployed in the environment to monitor and block unknown URLs, your security administrator might need to allow the hosts and IP addresses listed at ScreenMeet Documentation: Firewall configuration / whitelisting and ScreenMeet Documentation: Egress IP Addresses, and allow the following URL.

Third-party URL required for Screen Sharing

URL	Source	Port	Protocol	Description
`*.screenmeet.com`	ScreenMeet client	443	TCP / UDP	Required for endpoints to establish screen sharing connections



For the best results, allow traffic from the preceding URL to bypass proxy servers if you deployed such servers in your network. Screen sharing traffic that passes through proxy servers negatively impacts performance. For more information, see ScreenMeet Documentation: ScreenMeet Enterprise Deployment Guide.

  - Ensure that the ScreenMeet security requirements are configured. For more information, see ScreenMeet Documentation: Security.

© 2025 Tanium Inc. All Rights Reserved

- Create and sign in to a Tanium Account to link the Tanium instance where you will use Screen Sharing. If your Tanium license includes Screen Sharing, it is automatically configured for your Tanium instance when your account is linked.

  For more information, see Tanium Account User Guide: Creating and managing your Tanium Account.

Supported operating systems for ScreenMeet

The following endpoint operating systems are supported for screen sharing through Tanium. For more information about the operating systems that ScreenMeet supports, see ScreenMeet Documentation: Requirements.

> **NOTE** The first time a Tanium Console operator establishes a screen sharing session with a macOS endpoint, the endpoint user must select **ScreenMeetSupport** in the **Screen Recording** and **Accessibility** permissions in **System Settings**, then click **Later** when prompted. For more information, see ScreenMeet Documentation: Connecting to Mac devices.

Supported operating systems for Screen Sharing

Operating System	Version	Notes
Windows	• Windows 11 • Windows 10S • Windows 10	Windows operating systems also require .NET Framework 4.6.2 or later. Windows operating systems support attended and unattended screen sharing sessions.
Windows Server	• Windows Server 2022 • Windows Server 2019 • Windows Server 2016	
macOS	• 10.14 or later	macOS operating systems support only attended screen sharing sessions.

Screen Sharing requires the following port.

Ports for Screen Sharing communication

Source	Destination	Port	Protocol	Purpose
Tanium Module Server	`*.cloud.tanium.com`	443	TCP	Required for the Tanium Module Server to connect to Tanium™ Account for provisioning an on-premises configuration

User role requirements

Predefined roles grant the following permissions, which are required to use ScreenMeet Screen Sharing integration functionality:

© 2025 Tanium Inc. All Rights Reserved

- ScreenMeet Screen Sharing solution permissions on page 59
- ScreenMeet Screen Sharing administration and platform content permissions on page 62: The solution permissions automatically provide some of these permissions.

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

ScreenMeet Screen Sharing solution permissions

Permission	Integration Admin - ScreenMeet[1]	Integration Viewer - ScreenMeet[1]	Screen Sharing Agent[1]
Partner Integration View the Integrations Gallery workbench	✓ SHOW	✓ SHOW	✓ SHOW
Partner Integration Api Use the Integrations Gallery API	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE
Partner Integration Credentials View and configure the Integrations Gallery credentials	✓ READ WRITE DELETE	✗	✗
Partner Integration Gallery View and configure the Integrations Gallery	✓ READ	✓ READ	✓ READ
Partner Integration Gallery Screenmeet View and configure the ScreenMeet integration	✓ READ WRITE	✓ READ	✓ READ
Partner Integration Reporting Metrics View reporting metrics in Integrations Gallery	✓ READ	✓ READ	✓ READ

© 2025 Tanium Inc. All Rights Reserved

ScreenMeet Screen Sharing solution permissions (continued)

Permission	Integration Admin - ScreenMeet[1]	Integration Viewer - ScreenMeet[1]	Screen Sharing Agent[1]
Screen Sharing Api Connect to Screen Sharing API	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE
Screen Sharing Audit Event Log View or create event log for auditing purposes	✓ READ WRITE	✗	✗
Screen Sharing Config For internal purposes only	✓ READ WRITE	✓ READ	✓ READ
Screen Sharing Console Get magic URL for accessing ScreenMeet console	✓ EXECUTE	✗	✓ EXECUTE
Screen Sharing Console Admin Get magic URL for accessing ScreenMeet console and organizational settings	✓ EXECUTE	✗	✗
Screen Sharing Feed Integration User Interact with notifications from Tanium Feed	✓ ACCOUNT	✗	✗
Screen Sharing Gallery View the ScreenMeet content in Integrations Gallery	✓ READ	✓ READ	✗
Screen Sharing Integration Configure ScreenMeet in Integrations Gallery	✓ ADMIN	✓ VIEWER	✗
Screen Sharing Platform Integration User Interact with the platform	✓ ACCOUNT	✗	✓ ACCOUNT
Screen Sharing Product Options Retrieve ScreenMeet product options values: Show recording option (provided by **Screen Sharing Support Session** Write)	✓ READ	✗	✓ READ

© 2025 Tanium Inc. All Rights Reserved

ScreenMeet Screen Sharing solution permissions (continued)

Permission	Integration Admin - ScreenMeet[1]	Integration Viewer - ScreenMeet[1]	Screen Sharing Agent[1]
Screen Sharing Provisioning Otp Set provisioning information in one-time passcode	✓ WRITE	✗	✗
Screen Sharing Reporting Metrics Get reporting metrics	✓ READ	✓ READ	✓ READ
Screen Sharing Settings Configure screen sharing settings	✓ READ WRITE	✓ READ	✓ READ
Screen Sharing Support Session Start a screen sharing session on a remote endpoint, requiring endpoint user permission	✓ READ WRITE EXECUTE DELETE	✓ READ	✓ READ WRITE EXECUTE DELETE
Screen Sharing Support Session All Join any screen sharing session, even if another user started the session	✓ READ EXECUTE DELETE	✗	✗
Screen Sharing Support Session Options[2] Set screen sharing options that do not have corresponding settings available in the ScreenMeet console	✓ READ WRITE	✓ READ	✓ READ
Screen Sharing Tds Integration User Interact with data from Tanium Data Service	✓ ACCOUNT	✓ ACCOUNT	✓ ACCOUNT

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

[2]This permission does not currently have any effect on the available settings in the Screen Sharing workbench. It is provided in support of internal APIs used by the Screen Sharing service.

© 2025 Tanium Inc. All Rights Reserved

ScreenMeet Screen Sharing administration and platform content permissions

Permission	Permission Type	Integration Admin - ScreenMeet	Integration Viewer - ScreenMeet	Screen Sharing Agent
Action Group	Administration	✓ READ	✓ READ	✓ READ
Action	Platform	✓ READ WRITE	✗	✓ WRITE
Filter Group	Platform	✓ READ	✓ READ	✓ READ
Own Action	Platform	✓ READ	✗	✓ READ
Package	Platform	✓ READ	✓ READ	✓ READ
Plugin	Platform	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE
Sensor	Platform	✓ READ	✓ READ	✓ READ

To view the content sets to which the platform content permissions apply, see Tanium Console User Guide: View effective role permissions.

View the Details page

The **Details** page for the ScreenMeet Screen Sharing integration shows the following information:

- **Service Enablement** toggle
- **Account Status**
- **Licenses** count
- **Licenses in Use** count
- **License Alert Threshold** percentage
- **Access** link
- **Usage** reports
    - **Sessions**
    - **License Usage**

© 2025 Tanium Inc. All Rights Reserved

- **Screen Sharing Sessions** list
- **License Usage** list

To view the **Details** page:

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Screen Sharing Service Powered by ScreenMeet**.

View the Configuration page

The **Configuration** page for the ScreenMeet Screen Sharing integration shows the following information:

- **Role Assignment**: For more information, see Managing the ScreenMeet Screen Sharing integration on page 56.
- **License Usage** with **Users** list and **Alert Threshold** setting

To view the **Configuration** page:

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Screen Sharing Service Powered by ScreenMeet**.
3. Click **Configuration**.

View the Tanium Content page

The **Tanium Content** page for the ScreenMeet Screen Sharing integration shows the following information:

- **Reports**
    - **Endpoints Ready for Screen Sharing**

To view the **Tanium Content** page:

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Screen Sharing Service Powered by ScreenMeet**.
3. Click **Tanium Content**.

View the Support page

The **Support** page for the ScreenMeet Screen Sharing integration shows the following information:

- **Create Package** button to create a troubleshooting package for support requests

To view the **Support** page:

© 2025 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Screen Sharing Service Powered by ScreenMeet**.
3. Click **Support**.

View the About page

The **About** page for the ScreenMeet Screen Sharing integration shows the following information:

- **Real-Time Support** video
- **Collaborate**

To view the **About** page:

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Screen Sharing Service Powered by ScreenMeet**.
3. Click **About**.

Enable the integration

To get started, you must enable the Screen Sharing integration.

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Screen Sharing Service Powered by ScreenMeet**.
3. Click **Enable** and then confirm your selection.

Configure personas to establish unattended screen sharing sessions

The ability to establish unprompted (unattended) screen sharing sessions is intentionally limited by default to only Tanium administrators to prevent misuse. The default **Integration Admin - ScreenMeet**, **Screen Sharing Agent**, and **Integration Viewer - ScreenMeet** user roles do not have this permission. In addition, Tanium Console operators that establish an unattended screen sharing session with an endpoint and then close the session lock the endpoint by default.

You can configure a custom role and persona with permissions to establish unattended screen sharing sessions with an endpoint, and leave the endpoint unlocked after the unattended screen sharing session is closed. You can restrict the persona to a given computer group, and assign the persona to only certain Tanium Console operators.

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

1. From the Main menu, go to **Administration > Permissions > Roles** and click **New Role**.
2. Specify a **Role Name**, such as `Screen Sharing Unattended Role`.
3. Set the **Permission Type** to **Allow**.

© 2025 Tanium Inc. All Rights Reserved

4. Select the **Screen Sharing Support Session Unattended Execute** permission to allow users to establish unattended screen sharing sessions.
5. If you want a Tanium Console operator to have the option to leave an endpoint unlocked after closing an unattended screen sharing session, select **Screen Sharing Support Session Disable Autolock Execute**.
6. Click **Save**.
7. From the Main menu, go to **Administration > Permissions > Personas** and click **New Persona**.
8. Specify a persona **Name**, such as `Screen Sharing Unattended Persona`.
9. Click **Manage Roles**.
10. Select the following roles:
    - **Interact Basic User** for Interact access
    - **Screen Sharing Agent** for screen sharing access
    - **Screen Sharing Unattended Role** (or the name of the role you created) for unattended screen sharing session options
11. Click **Apply**.
    The Permissions table displays the union of permissions from these roles, including **Screen Sharing Support Session Unattended Execute** and, if you configured it, **Screen Sharing Support Session Disable Autolock Execute**.
12. Expand the **Computer Groups** section and click **Manage Computer Groups**.
13. Select the computer groups that contain the endpoints to which you want to establish unattended screen sharing sessions, then click **Select**.
14. If you configured a user group to contain your Tanium Console operators that will establish screen sharing sessions with endpoints, such as a help desk-related user group, expand the **User Groups** section and click **Manage User Groups**.
15. Select the user group, then click **Select**.
16. If you want to configure individual users to establish screen sharing sessions with endpoints, expand the **Users** section and click **Manage Users**.
17. Select the users, then click **Select**.
18. Click **Save**.
    Tanium Console operators assigned this persona can establish unattended screen sharing sessions when this persona is active.

Open an endpoint screen sharing session

To open a screen sharing session, you must have access to the endpoint in Tanium, and the endpoint must have Screen Sharing tools installed using Tanium Endpoint Configuration unless you are connecting to an endpoint without a Tanium Client. After you initiate a connection, the connection screen for the endpoint shows the status. Establishing connections can take between one and three minutes.

© 2025 Tanium Inc. All Rights Reserved

NOTE

After installing or upgrading Screen Sharing or Endpoint Configuration, or adding new endpoints to your environment, it might take several minutes for Endpoint Configuration to install Screen Sharing tools on an endpoint. If an endpoint does not have Screen Sharing tools installed, attempts to establish a screen sharing session with that endpoint fail. Wait several minutes for installation of Screen Sharing tools and then try again. For more information on Endpoint Configuration and endpoint tools, see Tanium Endpoint Configuration User Guide: Managing endpoint tools.

You can establish an attended connection, which requires the endpoint user to accept the screen sharing connection, or an unattended connection, which allows you to establish the connection without endpoint user permission.

IMPORTANT

Screen Sharing sessions are only established on endpoints that are included in the Screen Share action group. Therefore, the **Open Screen Sharing** button is only available for endpoints that are included in the Screen Share action group. By default, the action group is set to All Computers.

NOTE

The first time a Tanium Console operator establishes a screen sharing session with a macOS endpoint, the endpoint user must select **ScreenMeetSupport** in the **Screen Recording** and **Accessibility** permissions in **System Settings**, then click **Later** when prompted. For more information, see ScreenMeet Documentation: Connecting to Mac devices.

During the connection process, a ScreenMeet executable file is deployed to the endpoint with a Tanium Action. This executable file connects to the ScreenMeet services and establishes a connection with Tanium. The connection behavior depends on the endpoint operating system and whether you establish an attended or unattended connection:

- For attended connections to Windows endpoints, the endpoint user must accept the screen sharing session to continue. This establishes an active session and the Tanium Console operator takes control.
- For attended connections to macOS endpoints, if the endpoint user has allowed the proper screen sharing permissions on the endpoint, a view-only session is initially established. The Tanium Console operator must request control, and the endpoint user must accept, which then allows the operator to take control.
- For unattended connections to Windows endpoints, a new session is created without endpoint user permission and the Tanium Console operator takes control.
- Unattended connections to macOS endpoints are not supported.

IMPORTANT

If PowerShell is in the `ConstrainedLanguage` language mode on Windows endpoints, the Screen Sharing script to open a user session (`<Tanium Client installation directory>\Tools\ScreenSharing\start-session.ps1`), which is signed, must be allowed to run in `FullLanguage` mode through Windows Defender application control (WDAC) or other system policies.

© 2025 Tanium Inc. All Rights Reserved

NOTE

If no endpoint users are logged in to an endpoint and you establish an unattended connection, after you enter operating system login information, the session displays a disconnection message. Wait several seconds for the login process to complete and reestablish the connection.

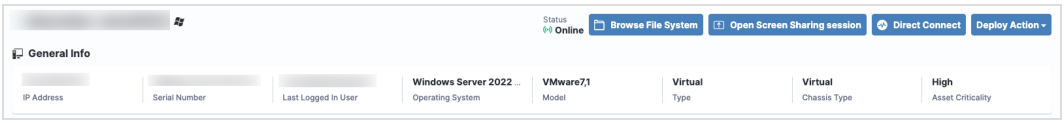
When you configure session recording in the ScreenMeet console (**Organization > Settings and Policies > Remote Support Features > Session Recording**), if you select:

- **Always**, the Tanium screen sharing session is always recorded.
- **Let the Agent Decide**, and the Tanium Console operator has the **Screen Sharing Product Options Read** permission, the Tanium Console operator has the option to record a screen sharing session. If the session is recorded, users have the option to disable recording before joining the session.
- **Never**, the Tanium screen sharing session is never recorded.

  For more information about configuring session recording, see ScreenMeet Docs: Remote Support Settings.

Open a screen sharing session from an endpoint

1. From the Tanium **Home** page, go to **Search for endpoints** and type the IP address or computer name of the computer, then click the computer name.
2. Click **Open Screen Sharing session**.



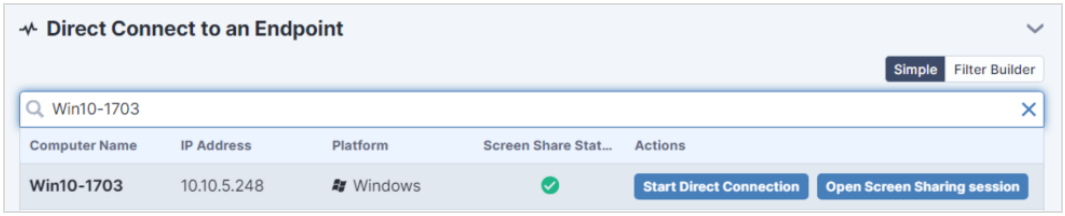
3. (Windows endpoints) If you have the **Screen Sharing Support Session Unattended Execute** permission, you have the following options:
   - Select **Ask the endpoint user for permission** to start an attended session.
   - Clear **Ask the endpoint user for permission** to start an unattended session. After you end the session, by default, the endpoint locks.
4. (Windows endpoints) If you have the **Screen Sharing Support Session Unattended Execute** and **Screen Sharing Support Session Disable Autolock Execute** permissions, then start an unattended session, you have the following options:
   - Select **Automatically lock after session ends** to lock the endpoint after you end the unattended session.
   - Clear **Automatically lock after session ends** to leave the endpoint unlocked after you end the unattended session.

© 2025 Tanium Inc. All Rights Reserved

5. (Windows and macOS endpoints) If you have the **Screen Sharing Product Options Read** permission, and **Let the Agent Decide** is selected in the ScreenMeet console **Session Recording** settings, you have the following options:
    - Select **Record session** to record the screen sharing session. Users have the option to disable recording before joining the session.
    - Clear **Record session** to establish the screen sharing session without recording.
6. Click **Open**.
7. A Tanium action deploys to the endpoint that includes an executable file that connects to ScreenMeet services. Establishing connections can take between one and three minutes. If the attended session is on an end user's computer, the user must accept the session on the endpoint to continue.
8. When the screen sharing session is connected, your screen switches to ScreenMeet in Tanium. You can use Support Tools in ScreenMeet to run Windows commands, tasks, and tools.

Open a screen sharing session from Direct Connect

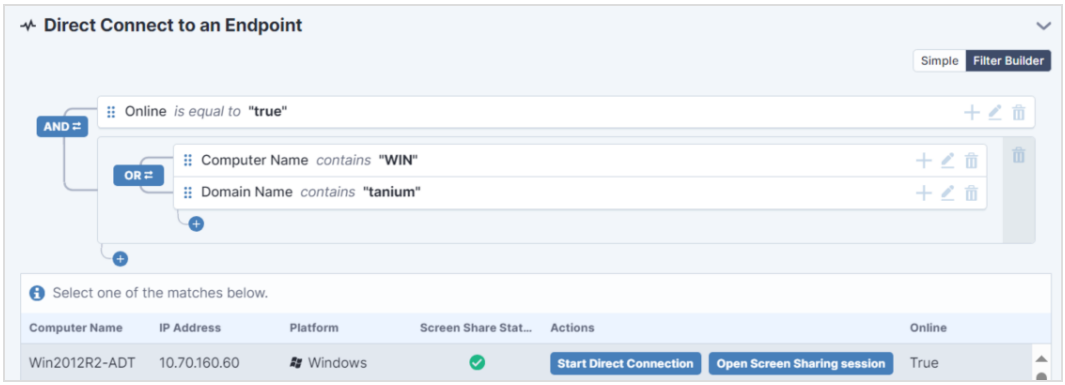
1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. Go to the **Direct Connect to an Endpoint** section and select a search option to find the endpoint for which you want to start a connection:
    - **Simple**: Enter the IP address or computer name of the endpoint.



    - **Filter Builder**: Configure one or more sensor-based filters to find the endpoint. Select a sensor (such as **Last Logged In User**), select an operator (such as **contains**), enter the value to match, and click Apply. For each additional filter, hover over Add, select **Add Row** or **Add Group**, and repeat the configuration steps. Integrations Gallery processes group (nested) filters and applies Boolean AND/OR logic in the same way that Tanium Interact does for question results filters, and the configuration steps are similar. For more information, see Tanium Interact User Guide: Filter by

© 2025 Tanium Inc. All Rights Reserved

advanced conditions.



3. In the result list, click **Open Screen Sharing session** for the endpoint.
4. (Windows endpoints) If you have the **Screen Sharing Support Session Unattended Execute** permission, you have the following options:
    - Select **Ask the endpoint user for permission** to start an attended session.
    - Clear **Ask the endpoint user for permission** to start an unattended session. After you end the session, by default, the endpoint locks.
5. (Windows endpoints) If you have the **Screen Sharing Support Session Unattended Execute** and **Screen Sharing Support Session Disable Autolock Execute** permissions, then start an unattended session, you have the following options:
    - Select **Automatically lock after session ends** to lock the endpoint after you end the unattended session.
    - Clear **Automatically lock after session ends** to leave the endpoint unlocked after you end the unattended session.
6. (Windows and macOS endpoints) If you have the **Screen Sharing Product Options Read** permission, and **Let the Agent Decide** is selected in the ScreenMeet console **Session Recording** settings, you have the following options:
    - Select **Record session** to record the screen sharing session. Users have the option to disable recording before joining the session.
    - Clear **Record session** to establish the screen sharing session without recording.
7. Click **Open**.
8. A Tanium action deploys to the endpoint that includes an executable file that connects to ScreenMeet services. Establishing connections can take between one and three minutes. If the attended session is on an end user's computer, the user must accept the session on the endpoint to continue.
9. When the screen sharing session is connected, your screen switches to ScreenMeet in Tanium. You can use Support Tools in ScreenMeet to run Windows commands, tasks, and tools.

Open a screen sharing session from Reporting



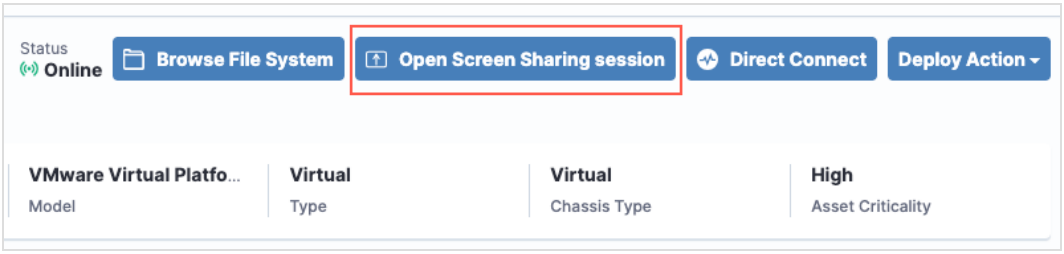
Tanium Reporting 1.43.40 or later is required to open screen sharing sessions in Reporting.

© 2025 Tanium Inc. All Rights Reserved

When you view, create, or edit a report that contains the **Computer Name** column, you can click an endpoint in the column to view details for the endpoint and to deploy an action to it. For information about Reporting, see Tanium Reporting User Guide: Working with a single endpoint.

1. Open a report that contains the **Computer Name** column.
2. Click Endpoint Details next to the name of an endpoint in the **Computer Name** column.

   An **Endpoint Details** dialog opens with basic details for the endpoint. If multiple endpoints have the same **Computer Name**, click Previous or Next in the **Multiple Results Found** banner to find the details for a specific endpoint.
3. Click **View Details** to open a page that shows a single endpoint view with detailed information.
4. Click **Open Screen Sharing session** to connect to the endpoint.



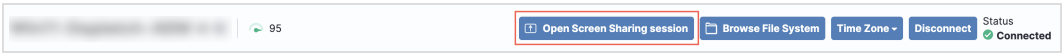
5. (Windows endpoints) If you have the **Screen Sharing Support Session Unattended Execute** permission, you have the following options:
   - Select **Ask the endpoint user for permission** to start an attended session.
   - Clear **Ask the endpoint user for permission** to start an unattended session. After you end the session, by default, the endpoint locks.
6. (Windows endpoints) If you have the **Screen Sharing Support Session Unattended Execute** and **Screen Sharing Support Session Disable Autolock Execute** permissions, then start an unattended session, you have the following options:
   - Select **Automatically lock after session ends** to lock the endpoint after you end the unattended session.
   - Clear **Automatically lock after session ends** to leave the endpoint unlocked after you end the unattended session.
7. (Windows and macOS endpoints) If you have the **Screen Sharing Product Options Read** permission, and **Let the Agent Decide** is selected in the ScreenMeet console **Session Recording** settings, you have the following options:
   - Select **Record session** to record the screen sharing session. Users have the option to disable recording before joining the session.
   - Clear **Record session** to establish the screen sharing session without recording.
8. Click **Open**.

© 2025 Tanium Inc. All Rights Reserved

9. A Tanium action deploys to the endpoint that includes an executable file that connects to ScreenMeet services. Establishing connections can take between one and three minutes. If the attended session is on an end user's computer, the user must accept the session on the endpoint to continue.
10. When the screen sharing session is connected, your screen switches to ScreenMeet in Tanium. You can use Support Tools in ScreenMeet to run Windows commands, tasks, and tools.

Open a screen sharing session from Performance

1. From the Main menu, go to **Modules > Performance > Direct Connect**. Search for the endpoint by IP address, computer name, or by using the Filter Builder.
2. From the results list, click the name of the endpoint in the **Computer Name** column.
3. After a connection is established, click **Open Screen Sharing session**.



4. (Windows endpoints) If you have the **Screen Sharing Support Session Unattended Execute** permission, you have the following options:
    - Select **Ask the endpoint user for permission** to start an attended session.
    - Clear **Ask the endpoint user for permission** to start an unattended session. After you end the session, by default, the endpoint locks.
5. (Windows endpoints) If you have the **Screen Sharing Support Session Unattended Execute** and **Screen Sharing Support Session Disable Autolock Execute** permissions, then start an unattended session, you have the following options:
    - Select **Automatically lock after session ends** to lock the endpoint after you end the unattended session.
    - Clear **Automatically lock after session ends** to leave the endpoint unlocked after you end the unattended session.
6. (Windows and macOS endpoints) If you have the **Screen Sharing Product Options Read** permission, and **Let the Agent Decide** is selected in the ScreenMeet console **Session Recording** settings, you have the following options:
    - Select **Record session** to record the screen sharing session. Users have the option to disable recording before joining the session.
    - Clear **Record session** to establish the screen sharing session without recording.
7. Click **Open**.
8. A Tanium action deploys to the endpoint that includes an executable file that connects to ScreenMeet services. Establishing connections can take between one and three minutes. If the attended session is on an end user's computer, the user must accept the session on the endpoint to continue.
9. When the screen sharing session is connected, your screen switches to ScreenMeet in Tanium. You can use Support Tools in ScreenMeet to run Windows commands, tasks, and tools.

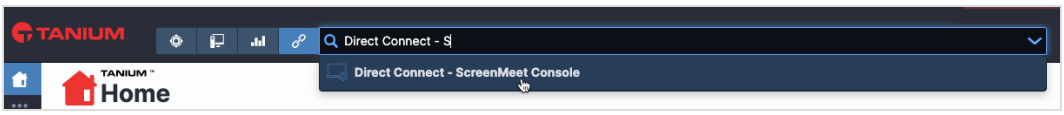
© 2025 Tanium Inc. All Rights Reserved

Open a screen sharing session with an endpoint that does not have a Tanium Client

You can open screen sharing sessions initiated from Tanium with unmanaged endpoints. This option can be helpful if you need to connect to the endpoint to troubleshoot issues with the Tanium Client. In this scenario, the user at the endpoint must manually download and install the ScreenMeet files since they cannot be distributed using Tanium. To use this method, you must be assigned a role that includes either the **Screen Sharing Console** or **Screen Sharing Console Admin** permission.

> NOTE
>
> Use this method to open a screen sharing session with a mobile device.

1. From the Tanium **Home** page, go to Navigate with quick links and enter **Direct Connect - ScreenMeet Console**. Click the **Direct Connect - ScreenMeet Console** quick link.



2. If you have more than one ScreenMeet product configured in your environment, click **Remote Support**.
3. Enter a **Description** for the session and configure the session options.

> NOTE
>
> Only the default ScreenMeet session options are available when you use this method to start the session.

4. Click **Create Session**.
5. Provide the user at the endpoint with the session URL and PIN code.
6. Ask the user at the endpoint to access the URL using a web browser and download and install the ScreenMeet client.
   For more information, see ScreenMeet documentation: Instructions to Person at End Point Device and ScreenMeet documentation: Providing Remote Support assistance to mobile devices.
7. After the user at the endpoint installs the ScreenMeet client and allows the session (if applicable), click **Enter Session** in the ScreenMeet console.

> NOTE
>
> The **Enter Session** button appears only when the user at the endpoint has installed the ScreenMeet client and allowed the session on the endpoint.

8. When the screen sharing session is connected, your screen switches to ScreenMeet in Tanium. You can use Support Tools in ScreenMeet to run Windows commands, tasks, and tools.

© 2025 Tanium Inc. All Rights Reserved

View and join screen sharing sessions

If you have **Integration Admin - ScreenMeet** role, you can see all sessions, and you can join sessions that were started by other Tanium Console operators.

If you have **Screen Sharing Agent** role, you can see and rejoin sessions that you started.



Multiple Tanium Console operators can join an endpoint screen sharing session, but only one operator at a time can take control of the session.

Join active sessions in the list of sessions

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Screen Sharing Service Powered by ScreenMeet**. The **Screen Sharing Sessions** section lists the active sessions.
3. Select one or more active sessions to an endpoint, then click **Join Screen Sharing** to join the sessions.

End an endpoint screen sharing session

When you stop a session, screen sharing processes are removed from the endpoint.



For attended connections to macOS endpoints, after the Tanium Console operator ends the session, a message is displayed to the endpoint user that the session is closed. The endpoint user must close the ScreenMeet application before a Tanium Console operator can establish another connection to that endpoint.

End active sessions in the list of sessions

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Screen Sharing Service Powered by ScreenMeet**. The **Screen Sharing Sessions** section lists the active sessions.
3. Select one or more endpoints and click **End Screen Sharing**.

Configure ScreenMeet settings

To configure settings in ScreenMeet, you must have a **Integration Admin - ScreenMeet** role. Users with the **Screen Sharing Agent** role can access the ScreenMeet console using a magic link but cannot configure organizational settings.

© 2025 Tanium Inc. All Rights Reserved

1. The following options are available:

   - Click the **Open ScreenMeet Configuration** link to use a magic link to open an authenticated session in the ScreenMeet console. In the ScreenMeet console, you can view session history, detailed logging of actions taken during a session, and so on. For more information, see ScreenMeet Docs: Remote Support Settings.

     Opening the ScreenMeet console from Tanium Console allocates a per-operator license to your user account, regardless of whether you establish a screen sharing session with this account.

   - In the **License Usage** section, view a list of users allocated a per-user license, and the time that each user most recently signed in to Tanium Console.
   - Click **Export > Export to CSV** to export a comma-separated value (CSV) file containing the list of users.

Unlink your Tanium Account

If you unlink your Tanium instance in Tanium Account, you lose access to the ScreenMeet account associated with your Tanium instance and you cannot use Screen Sharing. You can restore Screen Sharing functionality by linking the Tanium instance again, but your organization settings are reset and session history is lost. For more information about unlinking a Tanium instance, see Unlink a Tanium instance.

Troubleshoot the Screen Sharing integration

If the ScreenMeet Screen Sharing integration is not performing as expected, you might need to troubleshoot issues or change settings.

Collect logs

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

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Screen Sharing Service Powered by ScreenMeet**.
3. Click **Support**.
4. Click **Create Package**.
   An `integrations-gallery-support-bundle-[timestamp].zip` file downloads to the local download directory.
5. Contact Tanium Support to determine the best option to send the ZIP file. For more information, see View the Support page on page 63.

Screen sharing buttons unavailable

Screen sharing buttons and related functionality might not be available in Tanium Console while the system rotates ScreenMeet key information. By default, this action occurs once every 30 days. Wait up to 30 minutes for this action to complete and then try accessing screen sharing functionality. For more information about next steps if you still cannot access screen sharing functionality,

© 2025 Tanium Inc. All Rights Reserved

see Contact Tanium Support.

Contact support

If you require assistance with ScreenMeet tools, contact ScreenMeet. For more information, see ScreenMeet support.

© 2025 Tanium Inc. All Rights Reserved

Managing the Tanium Connector for Microsoft Intune

IMPORTANT

To use the Tanium Connector for Microsoft Intune, you must be:

- a Microsoft Intune subscriber
- a Tanium on-premises customer

For more information about Microsoft Intune, see Microsoft Intune documentation: Microsoft Intune securely manages identities, manages apps, and manages devices.

The Tanium Connector for Microsoft Intune entity provider integrates a Microsoft Intune instance with Tanium to ingest mobile device data. Ingesting Intune mobile device data alongside other endpoints in your network allows you to better manage all endpoints in Tanium Console, instead of using multiple endpoint management methods. You can view mobile devices managed using Tanium Connector for Microsoft Intune in Tanium Console alongside devices managed using Tanium Client.

IMPORTANT

In the context of the Tanium Connector for Microsoft Intune, devices that run Android, ChromeOS, iOS, and iPadOS are considered mobile devices. Conversely, laptops and other devices that support running Tanium Client are not considered mobile devices.

Before you begin

- You must have a Microsoft Intune subscription. There should be at least one mobile device enrolled.
  - Microsft Intune requires a license. For more information, see Microsoft Intune documentation: Microsoft Intune licensing.
  - Microsoft Intune supports mobile devices running Android, ChromeOS, iOS, or iPadOS. For more information, see Microsoft Intune documentation: Configure Chrome Enterprise connector, Microsoft Intune documentation: Enrollment guide: Enroll Android devices in Microsoft Intune, and Microsoft Intune documentation: Enrollment guide: Enroll iOS and iPadOS devices in Microsoft Intune.
- You must create an app registration for your Microsoft Intune instance. For more information, see Microsoft Entra documentation: Register an application in Microsoft Entra ID. As you complete the steps, make sure you do the following:
  - Copy the **Application (client) ID** and **Directory (tenant) ID** values to a plain text editor.
  - Assign permission scopes to the app registration. For more information, see Microsoft Intune documentation: How to use Microsoft Entra ID to access the Intune APIs in Microsoft Graph and Microsoft Intune documentation: Intune permission scopes.

© 2025 Tanium Inc. All Rights Reserved

Microsoft Intune app registration permission scope	Description
DeviceManagementManagedDevices.Read.All	Read Microsoft Intune device data and ingest device data into Tanium Core Platform

- Grant admin consent to the app registration to allow the Tanium Connector for Microsoft Intune permission to access the Microsoft Intune instance. For more information, see Microsoft Intune documentation: Grant admin consent (external tenants only).

  > NOTE
  >
  > The **Global Administrator** role has permission to grant admin consent.

- Add a client secret or public key certificate application credential to the app registration. For more information, see Microsoft Entra documentation: Add and manage application credentials in Microsoft Entra ID.

  > NOTE
  >
  > Public key certificates must be in PEM format.

- Configure network allow list rules to allow bidirectional traffic between the Tanium Server and a Microsoft Graph endpoint over port 443/TCP.

Microsoft Cloud Environment	Allowed endpoint[1]	Description
global environment	`https://graph.microsoft.com/<api_version>/deviceManagement/<api_version>/<api_version>`	Retrieve Microsoft Intune managed mobile device information
	`https://login.microsoftonline.com`	Authenticate the connection between Tanium Connector for Microsoft Intune and Microsoft Intune instance

[1]Endpoint URLs might include the API version, such as `v1.0`.

Entities and endpoints

An *entity* is any discrete computing-related unit or node on a computer network that can be tracked, such as an endpoint, compute instance, cloud service, or user data.

An *endpoint* is a computing device or node that connects to a computer network, through which data can enter or exit the network. Endpoints are a subset of entities; all endpoints are entities, but not all entities are endpoints. Endpoints include physical or virtual workstations that run Windows, macOS, or Linux, mobile devices that run Android or iOS, and other similar devices. In contrast, routers and switches are entities, but not endpoints, because routers and switches direct network traffic through the network, but do not provide a direct entry or exit point for data.

© 2025 Tanium Inc. All Rights Reserved

Entity providers

You can ingest data from endpoints managed using Tanium Client or an entity provider into the same Tanium instance to gain broader visibility into your entire network.

An *entity provider* is an adapter that ingests entity data into Tanium Core Platform. Tanium Core Platform uses this data to manage the entity. Entity providers collect entity data without installing Tanium Client on the endpoint. For example, you cannot install Tanium Client on mobile devices that run Android or iOS. You can configure the Tanium Connector for Microsoft Intune to integrate with a Microsoft Intune instance to ingest mobile device data or enroll Apple devices with Device Management.

- Management using Tanium Client: Tanium Client runs on endpoints that run a compatible operating system (OS), such as computers or virtual machines that run Linux, macOS, or Windows. These endpoints are generally part of the linear chain. Tanium Client reports information back to Tanium Core Platform through the linear chain.
- Management using entity providers, which collect device information in different ways:
    - Through integrations, such as the Tanium Connector for Microsoft Intune that ingests Microsoft Intune mobile device data

  Management of these devices does not rely on Tanium Client being installed directly on an entity. The entity provider might report endpoint information that is different from the information that a Tanium Client reports, due to the difference in entity type. For example, mobile devices are assigned an International Mobile Equipment Identity (IMEI) serial number, which are not assigned to other types of devices, such as an endpoint that runs Windows Server.

Each entity is associated with a **Provider Type**, **Provider Name**, and **Entity Type**, which identify how Tanium Core Platform manages the entity.

Entity providers and related sensor values

Entity Provider	Provider Type value	Provider Name value	Entity Type value
Tanium Client	Tanium Client	Tanium	Computer
Tanium Connector for Microsoft Intune	Microsoft Intune	*<configured-entity-provider-name>*	Mobile Device
Device Management	Device Management	• Device Management Computer (for macOS) • Device Management Mobile Device (for iOS and iPadOS)	• Computer (for macOS) • Mobile Device (for iOS and iPadOS)

Architecture

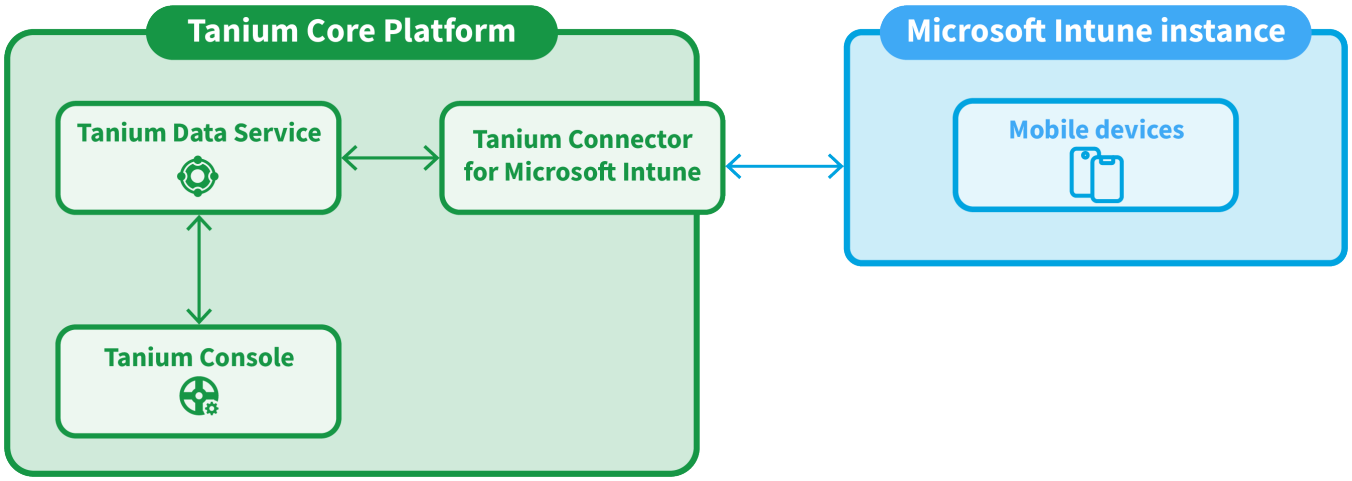
The Tanium Connector for Microsoft Intune establishes a secure connection with a Microsoft Intune instance and retrieves mobile device data from Microsoft Intune. This data is cached in Tanium Core Platform. Once every eight hours, the Tanium Connector for Microsoft Intune fully synchronizes with the Microsoft Intune instance, retrieves all mobile device data, and updates Tanium Core Platform with this information. Once every two minutes, the Tanium Connector for Microsoft Intune incrementally synchronizes with

© 2025 Tanium Inc. All Rights Reserved

the Microsoft Intune instance, retrieving only changes to managed devices, and updates Tanium Core Platform with this information. Depending on the number of mobile devices that the Microsoft Intune instance manages, this synchronization might take several minutes to complete.

Tanium operators that issue questions in Tanium Console can target all types of managed entities, including endpoints managed using Tanium Connector for Microsoft Intune and endpoints managed using Tanium Client. Tanium operators can also include endpoints managed using Tanium Connector for Microsoft Intune in Tanium Reporting reports and dashboards, or export the data using Tanium Connect.

Example Tanium Connector for Microsoft Intune architecture



Requirements

Review the requirements before you install and use the Tanium Connector for Microsoft Intune.

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium license that includes an Endpoint Management Standard or Endpoint Management Plus bundle, which includes the Tanium Connector for Microsoft Intune. For more information about how to get an Endpoint Management bundle and Tanium Connector for Microsoft Intune, see Tanium Solutions & Bundles .

  IMPORTANT

  If you obtained your Tanium license prior to May 2025, you must update your license prior to configuring the Tanium Connector for Microsoft Intune. For more information, contact Tanium support.

  NOTE

  Mobile devices ingested using the Tanium Connector for Microsoft Intune do not count against endpoint licensing totals.

© 2025 Tanium Inc. All Rights Reserved

- Tanium™ Core Platform servers
- Tanium™ Client: No client requirements.
- Tanium™ Console

Solution dependencies

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



Some Tanium Connector for Microsoft Intune dependencies have their own dependencies, which you can see by clicking the links in the lists of Required dependencies on page 80 and Feature-specific dependencies on page 80. Note that the links open the user guides for the latest version of each solution, not necessarily the minimum version that the Tanium Connector for Microsoft Intune requires.

Tanium recommended installation

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

Import specific solutions

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

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

REQUIRED DEPENDENCIES

The Tanium Connector for Microsoft Intune has the following required dependencies:

- Tanium™ Asset
- Tanium™ Endpoint Provider

FEATURE-SPECIFIC DEPENDENCIES

If you select only Endpoint Provider to import, you must manually import or update its feature-specific dependencies regardless of Tanium Console or Tanium Core Platform versions. The Tanium Connector for Microsoft Intune has the following feature-specific dependencies:

© 2025 Tanium Inc. All Rights Reserved

- Tanium™ Interact to ask questions and retrieve Microsoft Intune mobile device data
- Tanium™ Connect to export Microsoft Intune mobile device data to a destination
  Tanium™ Reporting to include Microsoft Intune mobile device data in reports and dashboards

Endpoints

Supported Internet protocols

The Tanium Connector for Microsoft Intune supports IPv4 and IPv6 addresses.

Supported operating systems

The following endpoint operating systems are supported with the Tanium Connector for Microsoft Intune.

- Android
- ChromeOS
- iPadOS
- iOS

For more information about supported operating systems, see Microsoft Intune documentation: Supported operating systems and browsers in Intune.

The Tanium Connector for Microsoft Intune does not install the Tanium Client or deploy packages to endpoints. For more information about Tanium Client operating system support, see Tanium Client Management User Guide: Client version and host system requirements.

Device requirements

For more information about mobile device minimum requirements, see Microsoft Intune: Configure Chrome Enterprise connector, Microsoft Intune: Enrollment guide: Enroll Android devices in Microsoft Intune, and Microsoft Intune: Enrollment guide: Enroll iOS and iPadOS devices in Microsoft Intune.

Third-party software

You must have a Microsoft Intune subscription to use the Tanium Connector for Microsoft Intune. Formore information about Microsoft Intune licensing, see Microsoft Intune: Microsoft Intune licensing.

Host and network security requirements

Specific ports and processes are needed to run the Tanium Connector for Microsoft Intune.

Ports

The following ports are required for Tanium Connector for Microsoft Intune communication.

© 2025 Tanium Inc. All Rights Reserved

Source	Destination	Port	Protocol	Purpose
Module Server	Microsoft Intune instance	443	TCP	Establish a connection between the Module Server and Microsoft Intune

BEST PRACTICE

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

SECURITY EXCLUSIONS

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

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.

No additional security exclusions are required.

User role requirements

Predefined roles grant the following permissions, which are required to use Tanium Connector for Microsoft Intune functionality:

- Tanium Connector for Microsoft Intune solution permissions on page 83
- Tanium Connector for Microsoft Intune administration and platform content permissions on page 84: The solution permissions automatically provide some of these permissions.

Some Tanium Connector for Microsoft Intune 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 Tanium Connector for Microsoft Intune. If you create custom roles for Tanium Connector for Microsoft Intune users, be sure to assign all the solution permissions and content set permissions that are required for Tanium Connector for Microsoft Intune 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:

© 2025 Tanium Inc. All Rights Reserved

- 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 **Endpoint Provider Service Account** and **Endpoint Provider Service Account - All Content Sets** roles to users. These roles are for internal purposes only.

Tanium Connector for Microsoft Intune solution permissions

Permission	Integration Operator - Intune[1]	Integration Viewer - Intune[1]
Partner Integration Access Integrations Gallery	SHOW	SHOW
Partner Integration API Use the Partner Integration API	EXECUTE	EXECUTE
Partner Integration Connection Verify a Partner Integration connection with a third party	VERIFY	VERIFY
Partner Integration Credentials Access Partner Integration credentials	READ WRITE	READ WRITE
Partner Integration Gallery View the Integrations Gallery	READ	READ
Partner Integration Gallery Intune View Microsoft Intune information in Integrations Gallery	READ WRITE	READ
Partner Integration Reporting Metrics View metrics information in Integrations Gallery	READ	READ

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

© 2025 Tanium Inc. All Rights Reserved

Tanium Connector for Microsoft Intune administration and platform content permissions

Permission	Permission Type	Integration Operator - Intune	Integration Viewer - Intune
Action Group	Administration	READ	READ
Filter Group	Platform Content	READ	READ
Package	Platform Content	READ	READ
Plugin	Platform Content	READ EXECUTE	READ EXECUTE
Sensor	Platform Content	READ	READ

To view the content sets to which the platform content permissions apply, see Tanium Console User Guide: View effective role permissions.

View the Details page

The **Details** page for the Tanium Connector for Microsoft Intune shows the following information:

- **Service Enablement** toggle
- **Microsoft Intune Instances** count and link
- **Synced Devices** count
- **Access** link
- **Usage** graph
- **Sync History** table

To view the **Details** page:

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Microsoft Intune**.

View the Configuration page

The **Configuration** page for the Tanium Connector for Microsoft Intune shows the following information:

© 2025 Tanium Inc. All Rights Reserved

- **Instances** table
- **Role Assignment**: For more information, see User role requirements on page 82.

To view the **Configuration** page:

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Microsoft Intune**.
3. Click **Configuration**.

View the Tanium Content page

The **Tanium Content** page for the Tanium Connector for Microsoft Intune shows the following information:

- **Dashboard** summary panes
- **Reports** table

To view the **Tanium Content** page:

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Microsoft Intune**.
3. Click **Tanium Content**.

View the Support page

The **Support** page for the Tanium Connector for Microsoft Intune shows the following information:

- **Create Package** button to create a troubleshooting package for support requests

To view the **Support** page:

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Microsoft Intune**.
3. Click **Support**.

View the About page

The **About** page for the Tanium Connector for Microsoft Intune shows the following information:

- **Extend Visibility**
- **Streamline Reporting**
- **Asset Management**

To view the **About** page:

© 2025 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Microsoft Intune**.
3. Click **About**.

Configure integration between Tanium and Microsoft Intune

Perform the following to ingest mobile device data from Microsoft Intune to Tanium:

1. Understand how Tanium Connector for Microsoft Intune ingests data and functions with Asset. For more information, see Tanium Connector for Microsoft Intune ingestion on page 86.
2. Understand how Tanium Connector for Microsoft Intune functions with Asset. For more information, see Interaction between Asset and Tanium Connector for Microsoft Intune on page 87.
3. In Microsoft Azure, create an application registration, configure the application permissions, and then create an Azure client ID and secret for Tanium Connector for Microsoft Intune to use for authentication. For more information, see Create an Azure client ID and secret on page 89.
4. By default, Tanium Asset views do not include devices managed using Tanium Connector for Microsoft Intune. If you want to include these devices, configure Asset to include devices managed using Tanium Connector for Microsoft Intune. For more information, see (Optional) Include Microsoft Intune devices in Asset views on page 89.
5. Configure a Tanium Connector for Microsoft Intune instance. For more information, see Create a Tanium Connector for Microsoft Intune instance on page 90.

Tanium Connector for Microsoft Intune ingestion

Configure a Tanium Connector for Microsoft Intune instance to connect to a Microsoft Intune instance and ingest mobile device data. Optionally, configure Asset to exclude mobile device data from Asset views.

Each Tanium Connector for Microsoft Intune instance connects to one Microsoft Intune instance in a one-to-one relationship, using the following components:

- The Microsoft Entra tenant ID, used to locate the Microsoft Intune instance
- The Microsoft Intune application (client) ID, used to connect to the Microsoft Intune instance
- Either a client secret or certificate, used to authenticate the connection between Microsoft Intune and the Tanium Connector for Microsoft Intune instance

The Tanium Connector for Microsoft Intune instance fully synchronizes with the Microsoft Intune instance once every eight hours, ingesting all mobile device data into Tanium Core Platform, and incrementally synchronizes changes to devices once every two minutes. This mobile device data is associated with the following attributes:

- A **Provider Type** of **Microsoft Intune**
- A **Provider Name** of the Tanium Connector for Microsoft Intune instance that ingested the data
- An **Entity Type** of **Mobile Device**

© 2025 Tanium Inc. All Rights Reserved

Depending on the number of managed mobile devices in the Microsoft Intune instance, this synchronization might take several minutes. If you retrieve data associated with mobile devices in Tanium Core Platform, such as by issuing a question, the information is accurate as of the synchronization time. Any updates since the synchronization with Microsoft Intune are not reflected in Tanium Core Platform until the next synchronization.

Note the following:

- Tanium Client is not installed on mobile devices when you use the Tanium Connector for Microsoft Intune to ingest mobile device data. Tanium functionality that requires a Tanium Client, such as deploying a package or retrieving certain sensor data, cannot be performed on this mobile device data. For example, you cannot apply custom tagging to mobile device data, as custom tagging requires a package.
- Because data associated with mobile devices is cached during synchronization, Interact questions that return mobile device data might return the data for mobile devices much faster than for devices managed using Tanium Client, as the Tanium Clients might need time to respond to the question. For example, if you issue a question that targets all entities, the live updates percentage might significantly increase almost immediately as the mobile device data is available, and then increase at a slower rate as Tanium Clients respond.
- If a mobile device is removed from Microsoft Intune, the data is not removed from Tanium Core Platform until the next full synchronization, once every eight hours. The incremental synchronization once every two minutes retrieves mobile device changes, but does not collect mobile device removal. You can view the **Sync History** table on the **Details** page. For more information, see View the Details page on page 84.
- If you delete a Tanium Connector for Microsoft Intune instance, this action also removes all mobile devices that the deleted instance ingested into Tanium Core Platform. For more information, see Delete a Tanium Connector for Microsoft Intune instance on page 91.

Interaction between Asset and Tanium Connector for Microsoft Intune

The Asset custom source for Microsoft Intune ingests data for both mobile devices and other device types from a configured Microsoft Intune instance on a configured schedule. The Tanium Connector for Microsoft Intune ingests data for only mobile devices from a configured Microsoft Intune instance.



Do not configure the Tanium Connector for Microsoft Intune and the Asset custom source for Microsoft Intune at the same time. Configuring both might result in unexpected behavior.

If you configure both the Tanium Connector for Microsoft Intune and the Asset custom source for Microsoft Intune:

© 2025 Tanium Inc. All Rights Reserved

- The Tanium Connector for Microsoft Intune synchronizes only mobile device data from Microsoft Intune into Tanium Core Platform.
- The Asset custom source for Microsoft Intune synchronizes data for both mobile devices and other device types from Microsoft Intune into Asset.
    - If you configure the source to perform asset reconciliation, devices must match on both reconciliation keys (`computer_name` and `serial_number`) to be reconciled.
    - Asset reconciliation first checks against the Tanium source in Asset, and then checks against endpoints ingested by the Tanium Connector for Microsoft Intune.

      
      NOTE

      In this scenario, you cannot configure asset reconciliation to check against only the Tanium source in Asset.
    - If a device managed using Tanium Client or Tanium Connector for Microsoft Intune matches the Tanium source in Asset, the data is merged, and then the data ingested from the Asset custom source for Microsoft Intune is removed.
- The Tanium source in Asset synchronizes all Microsoft Intune mobile device data from Tanium Core Platform into Asset.
- Because the synchronization schedules might not overlap, you might see different update times for devices managed using Tanium Connector for Microsoft Intune versus devices managed using Tanium Client.

If you configure only the Asset custom source for Microsoft Intune:

- The Asset custom source synchronizes data for both mobile devices and other device types from Microsoft Intune into Asset.
    - If you configure the source to perform asset reconciliation, devices must match on both reconciliation keys (`computer_name` and `serial_number`) to be reconciled.
    - Asset reconciliation checks against the Tanium source in Asset.
    - If a device managed using Tanium Client matches a Microsoft Intune device, the data is merged, and then the data ingested from the Asset custom source for Microsoft Intune is removed.
- Tanium Core Platform does not ingest Microsoft Intune device data.

If you configure only the Tanium Connector for Microsoft Intune:

- The Tanium Connector for Microsoft Intune synchronizes only mobile device data from Microsoft Intune into Tanium Core Platform.
- The Microsoft Intune-Mobile Device source in Asset ingests Microsoft Intune device data.
- Tanium Core Platform does not ingest Microsoft Intune data for other device types.

If you configure neither the Asset custom source for Microsoft Intune nor the Tanium Connector for Microsoft Intune, neither Tanium Core Platform nor Asset ingests Microsoft Intune device data.

© 2025 Tanium Inc. All Rights Reserved

Create an Azure client ID and secret

In the Microsoft Azure portal, create an application registration, configure the application permissions, and then create an Azure client ID and secret for Tanium Connector for Microsoft Intune to use for authentication.

For more information, see Microsoft Entra documentation: Quickstart: Register an application with the Microsoft identity platform.

1. In the Microsoft Azure portal, go to **App registrations** and click **New registration**.
2. Enter a name for the app registration and then select the supported account types. When finished, click **Register**.

   For more information about registering an application, see Microsoft Entra documentation: Quickstart: Register an application.
3. Record the **Application (client) ID** and **Directory (tenant) ID**.
4. Add a client secret. Go to **Certificates & secrets**, open the **Client secrets** tab, and click **New client secret**. Enter a description and expiration for the secret and then click **Add**.

   For more information about creating a client secret, see Microsoft Entra documentation: Quickstart: Add a client secret
5. After you add the client secret, record the **Value** for the client secret and save it to a secure location.

   You cannot see the client secret value again after you leave this page.
6. Add the **DeviceManagementManagedDevices** permission to the application registration.
   a. From the left-hand navigation menu, go to **API permissions**.
   b. Click **Add a permission**.
   c. Select **Microsoft Graph > Application Permissions**.
   d. Search for **DeviceManagementManagedDevices**.
   e. Select the **DeviceManagementManagedDevices.Read.All** permission and then click **Add Permissions**.
   f. The configured API permissions appear with the added **DeviceManagementManagedDevices** permission.
   g. Click **Grant admin consent for <your_tenant>**. A message appears to confirm that admin consent is granted to the permissions.

(Optional) Include Microsoft Intune devices in Asset views

By default, Tanium Asset views do not include devices managed using Tanium Connector for Microsoft Intune. If you want to include these devices, configure Asset to include devices managed using Tanium Connector for Microsoft Intune.

© 2025 Tanium Inc. All Rights Reserved

IMPORTANT

Do not enable this without understanding potential third-party provider and integration costs and limitations. Enabling this includes additional data in an Asset view, which might result in additional bandwidth and storage use, monetary charges, and other related costs.

1. From the Main menu, go to **Modules > Asset > Overview**, and then click Settings.
2. From the **Advanced** tab, in the **Tanium Entity Providers** section, click to enable **Microsoft Intune-Mobile Device** in addition to any other third-party providers that you want to enable.
3. Click **Save**.

Create a Tanium Connector for Microsoft Intune instance

Use the Application (client) ID, Directory (tenant) ID, and client secret or certificate PEM file from Microsoft Azure to configure a connection to the Microsoft Intune instance.

NOTE

Use the **Integration Operator - Microsoft Intune** system role to configure the Tanium Connector for Microsoft Intune instance.

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Microsoft Intune** and then click **Configuration**.
3. Click **Add Instance**.
4. Enter a Tanium Connector for Microsoft Intune instance **Name**.
5. Select a **Microsoft Cloud Environment** endpoint to allow communication between the Tanium Connector for Microsoft Intune instance and your Microsoft Intune instance.

   NOTE

   Configure a network allow list rule to allow bidirectional traffic between the Tanium Server and the Microsoft Cloud Environment endpoint over port 443/TCP.
6. Enter a **Tenant Name**, used to identify this configuration.
7. Copy your Microsoft Entra tenant GUID and paste it in **Tenant ID**.
8. Enter your Microsoft Intune **Application (Client) ID**.
9. Configure one of the following authentication options:
   a. Select **Secret** authentication, and then enter the **Client Secret**.
   b. Select **Certificate** authentication. Click **Upload Certificate** to upload a certificate PEM file. If the certificate PEM file is password-protected, enter the **Certificate Password**.
10. Assign the Tanium Connector for Microsoft Intune instance configuration to a **Content Set**.

© 2025 Tanium Inc. All Rights Reserved

11. Click **Verify Connection** to test the connection settings. If the connection cannot be established, check the Microsoft Intune configuration and the Tanium Connector for Microsoft Intune instance configuration settings, and then try again.
12. Click **Create**.

Edit a Tanium Connector for Microsoft Intune instance

Edit a Tanium Connector for Microsoft Intune instance to update the display **Name**, **Content Set**, and the **Authentication** method, including the **Client Secret** or **Certificate**. Update the instance if you need to update the authentication, such as for rotating a certificate, or if you want to update the content set to change or restrict Tanium operator access to the instance.

After you create a Tanium Connector for Microsoft Intune instance, you cannot update the **Microsoft Cloud Environment** endpoint, **Tenant Name**, **Tenant ID**, or **Application (Client) ID**. If you want to change these values, delete the existing Tanium Connector for Microsoft Intune instance and then create a new one.

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Microsoft Intune** and then click **Configuration**
3. Click Edit Instance .
4. Configure the settings for the Tanium Connector for Microsoft Intune instance.
5. Click **Save**.

Delete a Tanium Connector for Microsoft Intune instance

Deleting a Tanium Connector for Microsoft Intune instance also removes all Microsoft Intune mobile device data that this entity provider ingested. Delete the instance if you want to stop managing Microsoft Intune mobile device data in Tanium Console.

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Microsoft Intune** and then click **Configuration**
3. Click Delete Instance  for the Tanium Connector for Microsoft Intune instance that you want to delete.

Monitor Tanium Connector for Microsoft Intune

View Tanium Connector for Microsoft Intune instances

To view the Tanium Connector for Microsoft Intune instances:

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Microsoft Intune**.
3. Click **Configuration**.

Filter Tanium Connector for Microsoft Intune instance list

You can filter or order the list of Tanium Connector for Microsoft Intune instances.

© 2025 Tanium Inc. All Rights Reserved

- To filter for a specific instance, enter a string value in the **Filter items** field. The list updates with any instances that contain the value you entered. To clear the filter, click **X** in the **Filter items** field.
- To filter for a specific field value, enter a string value in the **Tenant ID Name**, **Tenant ID Value**, **Application (Client) ID**, or **Content Set** filter fields.
- Click a column header to sort the instances by the data in the column in descending order. Click the column header again to sort the list in ascending order. To clear the sort, click the column header a third time.

Use Tanium Connector for Microsoft Intune mobile devices and data

Issue questions to target Microsoft Intune mobile devices

You can use the **Provider Type**, **Provider Name**, and **Entity Type** sensors to return results from certain types of managed endpoints, such as endpoints managed using Tanium Client or endpoints managed using Tanium Connector for Microsoft Intune.

Entity providers and related sensor values

Entity Provider	Provider Type value	Provider Name value	Entity Type value
Tanium Client	Tanium Client	Tanium	Computer
Tanium Connector for Microsoft Intune	Microsoft Intune	*<configured-entity-provider-name>*	Mobile Device
Device Management	Device Management	• Device Management Computer (for macOS) • Device Management Mobile Device (for iOS and iPadOS)	• Computer (for macOS) • Mobile Device (for iOS and iPadOS)

The following question returns all mobile devices, such as those ingested by the Tanium Connector for Microsoft Intune entity provider:

```
Get Computer Name and Provider Name and Provider Type and Entity Type from all
entities where Entity Type equals Mobile Device
```

The following question returns all computers or workstations, such as those managed by Tanium Client:

```
Get Computer Name and Provider Name and Provider Type and Entity Type from all
entities where Entity Type equals Computer
```

The following question returns all mobile devices ingested by Tanium Connector for Microsoft Intune:

```
Get Computer Name and Provider Name and Provider Type and Entity Type from all
entities where Provider Type equals Microsoft Intune
```

© 2025 Tanium Inc. All Rights Reserved

The following questions returns all devices managed using Tanium Client:

```
Get Computer Name and Provider Name and Provider Type and Entity Type from all
entities where Provider Type equals Tanium Client
```

```
Get Computer Name and Provider Name and Provider Type and Entity Type from all
entities where Provider Name equals Tanium
```

The following question returns all mobile devices ingested by the Tanium Connector for Microsoft Intune instance named `Example Connector for Microsoft Intune`:

```
Get Computer Name and Provider Name and Provider Type and Entity Type from all
entities where Provider Name equals Example Connector for Microsoft Intune
```

Include Microsoft Intune mobile devices in a report

When you work in the **Explore Data** page or edit a report, the **Source Data** panel lists all registered sensors, along with certain sources of data that are not present on endpoints (for more information, see Tanium Reporting User Guide: Registered sensors). You use the panel to add data sources as columns to the grid in the page or report. Each column lists the results that endpoints returned for the corresponding sensor or lists the values that Tanium solutions calculated for other data sources. If a single source produces multiple columns of results, the column headings show the source name above the column names.

1. Perform one of the following steps based on whether you plan to edit an existing report or create a new view of endpoint data that you might or might not save as a report.
   - **Existing report**: Open the report and click **Edit Data**.
   - **New view or report**: From the Main menu, go to **Data > Explore Data**.

     You can also access the **Explore Data** page from the following locations:
     - An existing report: Click **New Report** or, in a non-editable report, click **Explore Data**.
     - The **Data > Reports** page: Click **Create Report**.
2. Select a **Data Source** to limit the results to endpoints managed using Tanium Client or an entity provider, or select **All Entities** to return results from all endpoints.

   Select **Save as default** to save your current **Data Source** selection for future reports.

© 2025 Tanium Inc. All Rights Reserved

3. Configure the report. For more information, see Tanium Reporting User Guide: Explore data and create reports.

> NOTE
>
> If you select **Microsoft Intune** or **All Endpoints** as the **Data Source**, you can filter results to show only endpoints running the iOS or Android operating system.

Export Microsoft Intune mobile device data using Tanium Connect

If the connection source supports Microsoft Intune mobile device data, such as the **Tanium Reporting (Source Data)** source, you can export this data using Tanium Connect. For more information, see Tanium Connect User Guide: Overview.

Troubleshooting

If the Tanium Connector for Microsoft Intune is not performing as expected, you might need to troubleshoot issues or change settings.

Collect logs

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

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. In the **Integrations** section, click **Microsoft Intune**.
3. Click **Support**.
4. Click **Create Package**.
   An `integrations-gallery-support-bundle.[timestamp].zip` file downloads to the local download directory.
5. Contact Tanium Support to determine the best option to send the ZIP file. For more information, see View the Support page on page 85.

Cannot establish connection between Tanium and Microsoft Intune

If the Tanium Connector for Microsoft Intune cannot establish a connection with Microsoft Intune, verify that all IDs match the Microsoft Intune settings, and that the network traffic is allowed.

- Verify that the **Tenant ID** and **Application (Client) ID** values match the Intune app registration values.
- Verify that you selected the intended Microsoft Cloud Environment endpoint.
- Configure a network allow list rule to allow bidirectional traffic between the Tanium Server and the Microsoft Cloud Environment endpoint over port 443/TCP.
- Ensure that no network block list rules block traffic to the Microsoft Cloud Environment endpoint. If a network block list rule identifies a CIDR range or uses wildcards to identify URLs, and includes the Microsoft Cloud Environment endpoint, either create an exception or adjust the evaluation priority to allow this traffic.

© 2025 Tanium Inc. All Rights Reserved

Cannot authenticate to Microsoft Intune

If the provided Microsoft Intune credentials do not allow authentication to the Microsoft Intune instance, verify that the credentials are in the correct format:

- If you entered a **Client Secret**, verify that the value matches the value in the Microsoft Intune app registration.
- If you uploaded a public key **Certificate**, verify that the certificate is in PEM format and well-formed, and if required, that the certificate **Password** value matches the password needed to access the certificate.

Cannot access a route, or retrieve groups or devices, or Microsoft Intune permissions are missing

If Microsoft Intune content cannot be accessed or retrieved, verify that the correct Microsoft Intune permissions are assigned to the Microsoft Intune app registration.

Microsoft Intune app registration permission scope	Description
DeviceManagementManagedDevices.Read.All	Read Microsoft Intune device data and ingest device data into Tanium Core Platform

© 2025 Tanium Inc. All Rights Reserved

Troubleshooting Integrations Gallery

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

Collect Tanium Account logs

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

1. From the Main menu, go to **Shared Services > Integrations Gallery**.
2. Click Help .
3. Click **Download Support Bundle**.
   A `tanium-Account Management-support-[timestamp].zip` file downloads to the local download directory.
4. Contact Tanium Support to determine the best option to send the ZIP file. For more information, see Contact Tanium Support on page 96.

Contact Tanium Support

To contact Tanium Support for help, sign in to the Tanium Customer Community.

For more information about how to submit a support case, see Case Submission Form.

© 2025 Tanium Inc. All Rights Reserved