

Tanium™ Investigate User Guide

Autonomous IT. Unstoppable Business.

2026H1 Semiannual Release

Version 1.6

May 28, 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/

© 2026 Tanium Inc. All Rights Reserved

© 2026 Tanium Inc. All rights reserved.

Table of contents

Investigate overview **7**

Investigations 7

Performance and activity history 7

Interoperability with other Tanium products 7

Performance 7

Reporting 7

Investigate requirements **8**

Core platform dependencies 8

Computer group dependencies 8

Solution dependencies 8

Tanium recommended installation 9

Import a specific solution 9

Required dependencies 9

Client extensions and endpoint tools 9

Tanium™ Module Server 10

Endpoints 10

Supported operating systems 10

Host and network security requirements 10

Ports 10

Security exclusions 11

User role requirements 14

Installing Investigate **16**

Before you begin 16

Import Investigate with default settings 16

Import Investigate with custom settings 17

Manage solution dependencies 17

Upgrade Investigate 17

© 2026 Tanium Inc. All Rights Reserved

Verify Investigate version ... 17
Configuring Investigate ... **18**
Install and configure Tanium Endpoint Configuration ... 18
Manage solution configurations with Tanium Endpoint Configuration ... 18
Configure Investigate ... 19
Configure the Investigations action group ... 19
(Optional) Configure Investigate for ServiceNow ... 19
Set up Investigate users ... 20
Creating investigations ... **22**
Overview ... 22
Create an investigation ... 22
Work with investigations ... 25
Add annotations to an investigation ... 26
Delete an investigation ... 27
Close an investigation ... 27
Reopen an investigation ... 27
Investigating performance and activity history on an endpoint ... **28**
Performance events ... 28
Activities ... 29
ServiceNow ... 35
Browsing the file system on an endpoint ... **37**
Managing a single endpoint remotely ... **38**
Service control ... 38
Resource summary ... 39
Live process monitor ... 39
Export process data ... 39
Terminate one or multiple processes ... 39
Browse and edit the Windows registry ... 40
Add a new registry value ... 40
Edit a registry value ... 41

© 2026 Tanium Inc. All Rights Reserved

Delete a registry value ... 41
Export registry data ... 41
Viewing Windows events ... **42**
Windows Events ... 42
Windows Event Log Subscriptions ... 43
Create a new subscription ... 43
Troubleshooting the Tanium Client on a single endpoint ... **45**
Logs and actions ... 45
Download client logs ... 45
Download action history ... 45
Gather ... 45
Troubleshooting Investigate ... **47**
Collect logs ... 47
Verify endpoint tools ... 47
Contact Tanium Support ... 47
Reference: Windows events ... **48**
Reference: Event log data ... **61**

© 2026 Tanium Inc. All Rights Reserved

Investigate overview

With Investigate, you can identify the root cause of issues that arise on Tanium-managed endpoints and arrive at resolutions to issues more quickly.

Investigations

Investigations enable you to correlate performance events and activities that came from one or multiple hosts. Add activities that have forensic value to investigations to triage issues more quickly and add notes and comments about these data points and the conditions in which they occur for team collaboration.

For more information, see Creating Investigations.

Performance and activity history

Quickly view and analyze the performance history and review the event history on a single endpoint. Understand the time line of system-impacting events such as patch installations or policy changes, and historical process and performance data.

For more information, see Investigating performance and activity history on an endpoint.

Interoperability with other Tanium products

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

Performance

Tanium™ Investigate uses Performance to display resource consumption data on endpoints, including CPU, memory, network, disk, and IO metrics. For more information, see Tanium Performance.

Reporting

If you have Tanium Reporting 1.28.48 or later, Investigate uses Reporting to create the charts on the Investigate **Overview** page. Reporting is required to see certain tabs and the File Browser on the Endpoint Details page. For more information, see Tanium Reporting.

© 2026 Tanium Inc. All Rights Reserved

Investigate requirements

Review the requirements before you install and use Investigate.

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium license that includes Investigate. For more information about how to get Investigate, see Tanium Solutions & Bundles.
- **Tanium™ Core Platform server**
- **Tanium™ Client**:
  Any supported version of Tanium Client. For more information, see Tanium Client Management User Guide: Client version and host system requirements.
  If you use a Client version that is not listed, certain product features might not be available, or stability issues can occur that can only be resolved by upgrading to one of the listed Client versions.

Computer group dependencies

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

- `All Computers`
- `All Windows`
- `All Linux`
- `All Mac`

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

Solution dependencies

Other Tanium solutions are required for Investigate to function (required dependencies) or for specific Investigate 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 Investigate dependencies have their own dependencies, which you can see by clicking the links in the lists of Required dependencies on page 9. Note that the links open the user guides for the latest version of each solution, not necessarily the minimum version that Investigate requires.

© 2026 Tanium Inc. All Rights Reserved

Tanium recommended installation

If you select **Tanium Recommended Installation** when you import Investigate, 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 a specific solution

If you select only Investigate to import, the Tanium Server automatically imports the latest available versions of any required dependencies that are missing. If some required dependencies are already imported but their versions are not the latest, the Server automatically updates those dependencies to the latest available versions.

Required dependencies

Investigate has the following required dependencies:

- Tanium™ Data Service (TDS)
- Tanium™ Default Content
- Tanium™ Direct Connect
- Tanium™ Endpoint Configuration
- Tanium™ Interact
- Tanium™ Partner Integration Service
    - This service requires the Enhanced Tags FQDN sensor. This sensor is provided by the Core Content - Enhanced Tags solution.
- Tanium™ Patch is required to view patching events.
- Tanium™ RDB Service
- Tanium™ Reporting
- Tanium™ Secrets



PerformanceCX is installed as part of Investigate.

Client extensions and endpoint tools

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

© 2026 Tanium Inc. All Rights Reserved

Tanium™ Module Server

Investigate 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

Supported operating systems

The following endpoint operating systems are supported with Investigate.

Supported operating systems for Tanium Investigate

Operating System	Version
Windows	A minimum of Windows 7 (SP1) or Windows Server 2008 R2 (with SP1) is required.
macOS	Same as Tanium Client support.
Linux	Same as Tanium Client support. For more information, 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 Investigate.

Ports

The following ports are required for Investigate communication.

© 2026 Tanium Inc. All Rights Reserved

Ports for Tanium Investigate communication

Source	Destination	Port	Protocol	Purpose
Module Server	Direct Connect Zone Proxy	17487 (Direct Connect communication port) and 17488 (Direct Connect provision and status monitoring port)	TCP	(Optional) Tanium Direct Connect connection to Direct Connect Zone Proxy
Tanium Server	Module Server	17477	TCP	Tanium Server initiates connections to the Module Server on port 17477
Tanium Client	Direct Connect	17475 (Direct Connect on Module Server) 17486 (Direct Connect Zone Proxy)	TCP	Connections to the Module Serveror the Direct Connect Zone Proxy for live connections



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.



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.

© 2026 Tanium Inc. All Rights Reserved

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

Target Device	Notes	Exclusion Type	Exclusion
Tanium Module Server		Process	<*Module Server*>\services\endpoint-configuration-service\TaniumEndpointConfigService.exe
		Process	<*Module Server*>\services\investigate-service\TaniumInvestigateService.exe
		Process	<*Module Server*>\services\partner-integration-service\TaniumPartnerIntegrationService.exe
Tanium Zone Server		Process	<*Tanium Installation Directory*>\Tanium Direct Connect Zone Proxy\node.exe
		Process	<*Tanium Installation Directory*>\Tanium Direct Connect Zone Proxy\twsm.exe

[1] = TPython requires SHA2 support to allow installation.

Investigate security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows x86 and x64		File	<*Tanium Client*>\extensions\SupportCX.dll
		File	<*Tanium Client*>\extensions\SupportCX.dll.sig
		File	<*Tanium Client*>\extensions\core\TaniumPythonCx.dll
		File	<*Tanium Client*>\extensions\core\TaniumPythonCx.dll.sig
		File	<*Tanium Client*>\TaniumClientExtensions.dll
		File	<*Tanium Client*>\TaniumClientExtensions.dll.sig
		Folder	<*Tanium Client*>\python312
		Process	<*Tanium Client*>\python312\TPython.exe
		File	<*Tanium Client*>\TPython\TPython.bat
		Folder	<*Tanium Client*>\TPython312
		Process	<*Tanium Client*>\TaniumCX.exe
		File	<*Tanium Client*>\extensions\TaniumDEC.dll
		File	<*Tanium Client*>\extensions\TaniumDEC.dll.sig

© 2026 Tanium Inc. All Rights Reserved

Investigate security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
Linux x86 and x64		Process	<*Tanium Client*>/TaniumCX
		Folder	<*Tanium Client*>/python312
		Process	<*Tanium Client*>/python312/bin/pybin
		Process	<*Tanium Client*>/TPython/TPython
		Folder	<*Tanium Client*>/TPython312
		File	<*Tanium Client*>/libTaniumClientExtensions.so
		File	<*Tanium Client*>/libTaniumClientExtensions.so.sig
		File	<*Tanium Client*>/libSupportCX.so
		File	<*Tanium Client*>/libSupportCX.so.sig
		File	<*Tanium Client*>/extensions/core/libTaniumPythonCx.so
		File	<*Tanium Client*>/extensions/core/libTaniumPythonCx.so.sig
		File	<*Tanium Client*>/extensions/libTaniumDEC.so
		File	<*Tanium Client*>/extensions/libTaniumDEC.so.sig
macOS		Process	<*Tanium Client*>/TaniumCX
		Process	<*Tanium Client*>/python312/bin/pybin
		File	<*Tanium Client*>/libTaniumClientExtensions.dylib
		File	<*Tanium Client*>/libTaniumClientExtensions.dylib.sig
		File	<*Tanium Client*>/extensions/core/libTaniumPythonCx.dylib
		File	<*Tanium Client*>/extensions/core/libTaniumPythonCx.dylib.sig
		File	<*Tanium Client*>/extensions/libTaniumDEC.dylib
		File	<*Tanium Client*>/extensions/libTaniumDEC.dylib.sig
		File	<*Tanium Client*>/extensions/libSupportCX.dylib
		File	<*Tanium Client*>/extensions/libSupportCX.dylib.sig

[1] = TPython requires SHA2 support to allow installation.

© 2026 Tanium Inc. All Rights Reserved

User role requirements

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

- Investigate solution permissions on page 14
- Investigate platform content permissions on page 15: The solution permissions automatically provide some of these permissions.

For more information about how to review a summary of the predefined roles, see Set up Investigate users.

Some Investigate 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 Investigate. If you create custom roles for Investigate users, be sure to assign all the solution permissions and content set permissions that are required for Investigate functionality. If you are not sure which permissions are required for a custom role, view the permissions of the predefined roles. For more information, see the following sections of the Tanium Console User Guide:

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



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

Investigate solution permissions

Permission	Investigate Administrator[1]	Investigate Operator[1]	Investigate User[1]	Investigate Read Only User
Investigate Allows viewing the Investigate workbench	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW
Investigate API Allows using the Investigate API	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE
Investigate Artifacts Allows deleting Investigate artifacts	✓ DELETE	✓ DELETE	✓ DELETE	✗

© 2026 Tanium Inc. All Rights Reserved

Investigate solution permissions (continued)

Permission	Investigate Administrator[1]	Investigate Operator[1]	Investigate User[1]	Investigate Read Only User
Investigate Comments Allows deleting Investigate comments	DELETE	DELETE	DELETE	
Investigate Direct Connect Allows issuing Direct Connect queries on an endpoint for an investigation	READ	READ	READ	
Investigate Investigations Allows reading, authoring, updating, and deleting investigations	READ WRITE DELETE	READ WRITE DELETE	READ WRITE	READ
Investigate Remote Management Allows remote management in Single Endpoint View.	SHOW	SHOW		
Investigate Partner Integration Allows issuing queries to partner integrations for an investigation	READ	READ	READ	

[1] This role provides module permissions for Tanium Direct Connect. You can view which Direct Connect permissions are granted to this role in the Tanium Console. For more information, see Tanium Direct Connect User Guide: User role requirements.

Investigate platform content permissions

Permission	Investigate Administrator[1]	InvestigateOperator[1]	InvestigateUser[1]	Investigate Read Only User
Plugin	READ EXECUTE	READ EXECUTE	READ EXECUTE	READ EXECUTE

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

[1] This role provides module permissions for Tanium Direct Connect. You can view which Direct Connect permissions are granted to this role in the Tanium Console. For more information, see Tanium Direct Connect User Guide: User role requirements.

© 2026 Tanium Inc. All Rights Reserved

Installing Investigate

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

- **Automatic configuration with default settings**: Investigate 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 Investigate, see Import Investigate with default settings on page 16.
- **Manual configuration with custom settings**: After installing Investigate, you must manually configure required settings. Select this option only if Investigate requires settings that differ from the recommended default settings. For more information, see Import Investigate with custom settings on page 17.

Before you begin

- Read the release notes.
- Review the Investigate requirements on page 8.

Import Investigate with default settings

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

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

Default settings for Tanium Investigate

Setting	Default value
Action group	• Restricted targeting disabled (default): `All Computers` computer group • Restricted targeting enabled: `No Computers` computer group

For more information about how to import Investigate and configure default settings, see Tanium Console User Guide: Import all modules and services. After the import, verify that the correct version is installed. For more information, see Verify Investigate version on page 17.

© 2026 Tanium Inc. All Rights Reserved

Import Investigate with custom settings

To import Investigate without automatically configuring default settings, be sure to clear the **Apply All Tanium recommended configurations** checkbox while performing the steps in Tanium Console User Guide: Import or update specific solutions. After the import, verify that the correct version is installed. For more information, see Verify Investigate version on page 17.

Manage solution dependencies

Other Tanium solutions are required for Investigate to function (required dependencies) or for specific Investigate features to work (feature-specific dependencies). For more information, see Solution dependencies on page 8.

Upgrade Investigate

For more information about how to upgrade Investigate, see Tanium Console User Guide: Managing Tanium solutions. After the upgrade, verify that the correct version is installed. For more information, see Verify Investigate version on page 17.

Verify Investigate version

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

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

© 2026 Tanium Inc. All Rights Reserved

Configuring Investigate

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

Install and configure Tanium Endpoint Configuration

Manage solution configurations with Tanium Endpoint Configuration

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

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

IMPORTANT

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

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

NOTE

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

Optionally, you can use Endpoint Configuration to require approval of configuration changes. When configuration approvals are enabled, Endpoint Configuration does not deploy a configuration change to endpoints until a user with approval permission approves the change. For information about the roles and permissions that are required to approve configuration changes for Investigate, see User role requirements on page 14. For more information about how to enable and use configuration approvals in Endpoint Configuration, see Tanium Endpoint Configuration User Guide: Managing approvals.

© 2026 Tanium Inc. All Rights Reserved

IMPORTANT

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

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

Configure Investigate

Configure the Investigations action group

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

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

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

BEST PRACTICE

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

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

(Optional) Configure Investigate for ServiceNow

Investigate provides the ability to integrate activities from ServiceNow.

1. From the Investigate Overview page, click Settings.
2. In the **ServiceNow Configuration** section provide the **Host URL**, **Username**, and **Password** for the ServiceNow environment from which you want to add activities.
3. Click **Submit**.

NOTE

The ITIL role in ServiceNow is required to integrate activities from ServiceNow.

© 2026 Tanium Inc. All Rights Reserved

Set up Investigate users

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

For more information about how to review specific permissions for each role, see User role requirements on page 14.



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

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

Investigate Administrator

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

- View and modify Investigate investigations.
- Dismiss or reject approvals for Investigate tasks in Tanium Endpoint Configuration.

Investigate Operator

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

- View and modify Investigate investigations.
- Dismiss or reject approvals for Investigate tasks in Tanium Endpoint Configuration.

InvestigateUser

Assign the **InvestigateUser** role to users who manage the configuration and deployment of Investigate functionality to endpoints but do not need to administer or configure settings for Investigate. This role can perform the following tasks:

- View connections to remote endpoints.
- View and modify Investigate investigations.

Investigate Read Only User

Assign the **Investigate Read Only User** role to users who need visibility into Investigate data.
This role can perform the following tasks:

- View connections to remote endpoints.
- View investigations.

© 2026 Tanium Inc. All Rights Reserved

NOTE

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

© 2026 Tanium Inc. All Rights Reserved

Creating investigations

Overview

Investigations provide visibility into activity and performance history across endpoints and leverage Tanium knowledge for activities of interest across endpoints. Investigations enable intelligent workflows for learning more about activities of interest and their potential impacts across all the endpoints in an environment. Investigations provide a better way to view and organize data from Tanium Clients. Investigations enable you to correlate data points that came from one or multiple endpoints. Add activities that have forensic value to investigations to triage issues quickly, and add comments about these data points and the conditions in which they occur for team collaboration.

Analyze the context of activities in an investigation such as performance and system events, software installations, and installations of browser plugins. Investigations provide summaries of all known details for activities of interest and intelligently present detailed visualizations to provide deeper understanding of what is occurring in an environment. With summary context, you can view endpoints that are of interest to investigators, understand which activities on those endpoints are likely relevant, and what actors participated in those events.

You can assign an owner to each investigation, analyze the impacts of each investigation, and use Tanium solutions to take actions such as remediation measures or complete quarantine on specific endpoints or groups of endpoints. You can view each investigation as a unique entity where comments regarding the investigation are preserved.



You can add comments to closed investigations, but you cannot edit the investigation in any other way without reopening the investigation. From the **Investigations** page, select a closed investigation and click **Actions > Reopen** to reopen a closed investigation.

Create an investigation

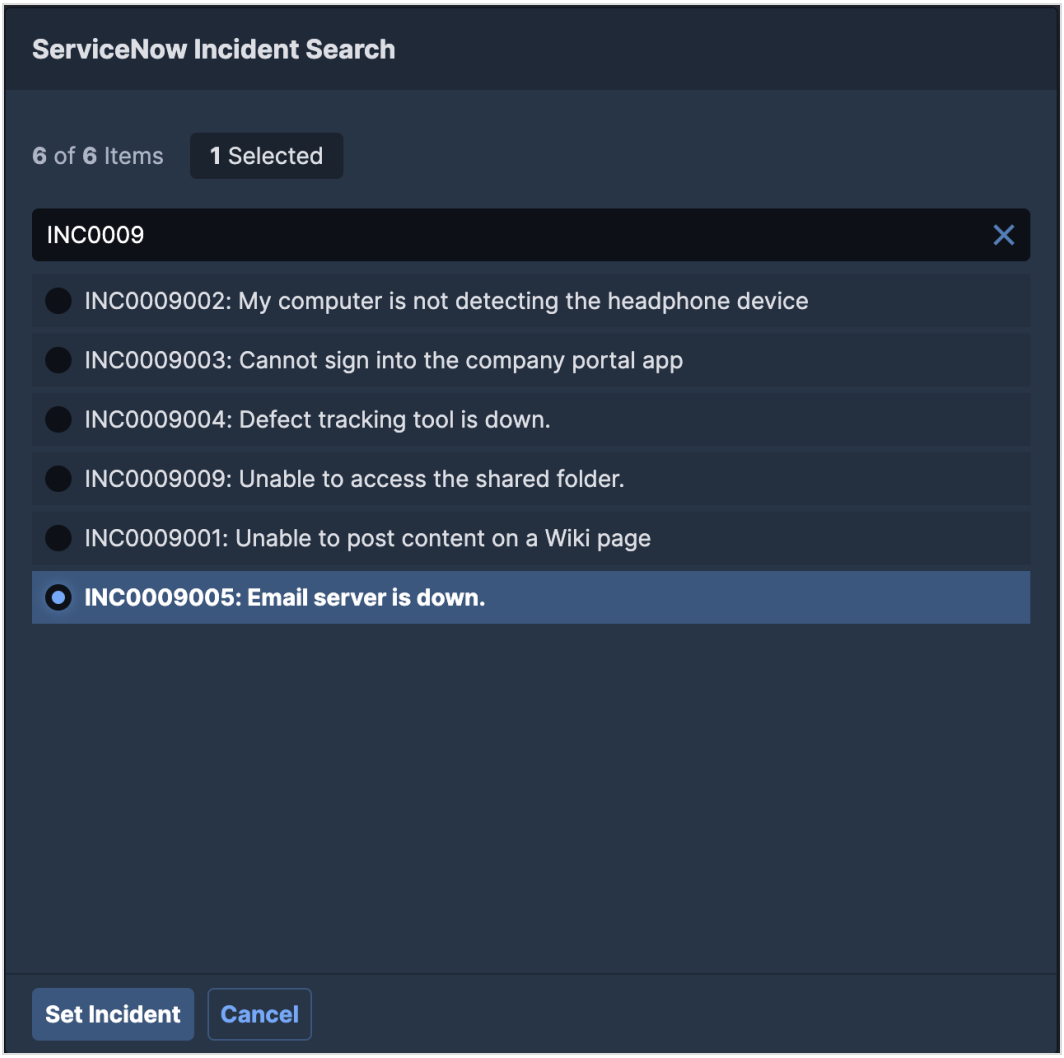
1. From the Main menu, go to **Modules > Investigate > Overview**. You can view summary charts for all current open investigations.
   The **Overview** page shows the number of open investigations based on different distributions:
   - **Investigations by priority** - shows the number of open investigations distributed by the priority of each investigation.
   - **Investigations by assignee** - shows the number of open investigations distributed by the owners of each investigation.
   - **Investigations by status** - shows the number of open investigations distributed by the current status of each investigation.
2. Select activities to add from the **Investigate** tab on the Endpoint Details page. For more information on accessing the Endpoint Details page, see Tanium Reporting User Guide: View endpoint details.

© 2026 Tanium Inc. All Rights Reserved

3. Click **Select Activities** to display a list activities across many categories that you can add. The ⚠ icon next to an activity indicates that there are a large number of activities and it might take a while to load the activities grid. As a best practice, limit the number of activities that you select to less than 1,000 before selecting them. Click **Save** to view the activities in the activities grid. For any activity, you can click **Add to Investigation** to add the activity to an investigation. You can select multiple activities and click **Add to Investigation** to add multiple activities.
4. Select the content set to which the investigation is saved. When you create a new investigation, the investigation content set is default. You can save a new investigation without selecting a content set, but if you edit an existing investigation that is inside a deleted content set, the content set field displays as blank and you cannot save the investigation until you have provided a new content set option.
5. (Optional) If you have configured Investigate for ServiceNow, click **Link ServiceNow Incident** under the External Record heading to associate a ServiceNow incident with the investigation. Associating a ServiceNow incident with an investigation enables you to view data associated with a ServiceNow incident in Investigate. For example, you can view when a ServiceNow incident was opened on the timeline view in the Investigate tab. For more information on configuring Investigate for ServiceNow, see Configure Investigate for ServiceNow.

© 2026 Tanium Inc. All Rights Reserved

a. From the ServiceNow Incident Search panel, enter search terms to locate the ServiceNow incident that you want to associate with the investigation. You can only associate one ServiceNow incident with each investigation.



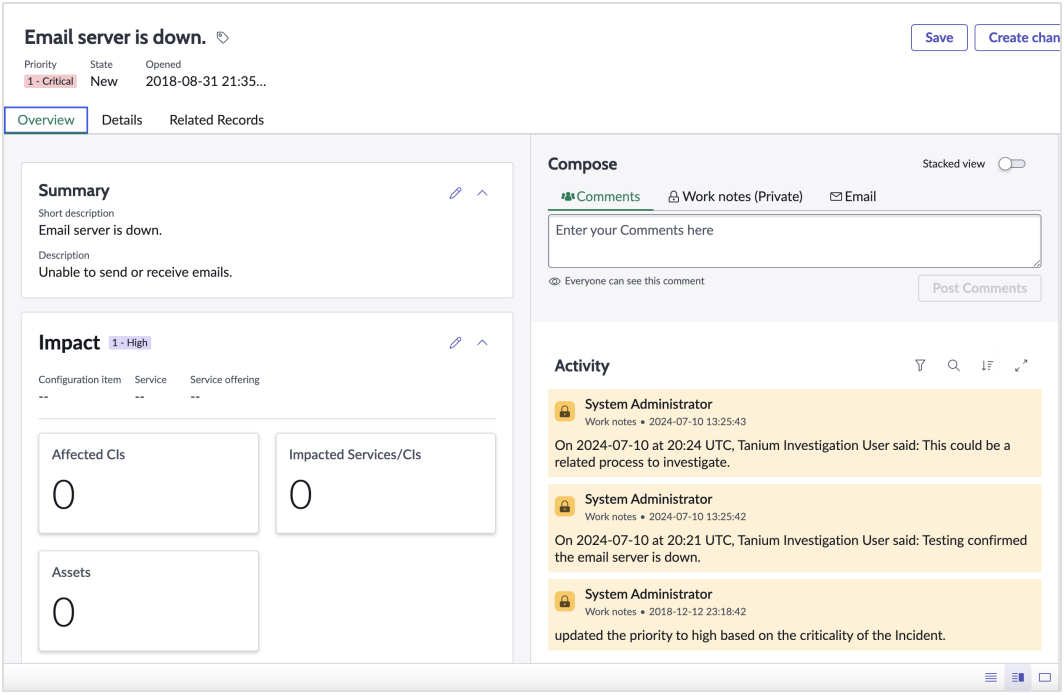
b. Select an incident and click **Set Incident**. At any time you can select an investigation and remove the ServiceNow incident from the investigation. Data that is associated with a ServiceNow incident appears as part of an investigation for linked ServiceNow incidents, and originates from the `Incident` and `CI` objects in ServiceNow. ServiceNow activities can contain the following data, where data from the ServiceNow Incident and CI objects display as follows:

ServiceNow data	Investigate data
`id`	The incident name
`description`	The short description of the incident
`caller`	The incident caller
`incidentCategory`	The incident category
`incidentSubcategory`	The incident subcategory

© 2026 Tanium Inc. All Rights Reserved

ServiceNow data	Investigate data
`state`	The incident state
`assignee`	The incident assignee
`assignmentGroup`	The incident assignment group
`priority`	The incident priority
`businessService`	The incident business service

c. Content from Investigate, such as comments that you add, appears as a worknote that is associated with the linked incident in ServiceNow.



6. Click **New** or **Existing**. If you select **Existing**, select the name of the investigation that you want to add the activity to and click **Save**. If you click **New**, provide a name and description for the new investigation. Assign the investigation to a user and assign a priority. The user that you assign the investigation to is typically tasked with further analysis of the implications of the investigation and is responsible for performing any required tasks on the endpoints.
7. Click **Save**.

Alternatively, you can create an investigation from the **Investigate** tab on the Endpoint Details page. For more information, see Investigating performance and activity history on an endpoint.

Work with investigations

1. From the Main menu, go to **Modules > Investigate > Overview**.

© 2026 Tanium Inc. All Rights Reserved

2. Select the name of an investigation to drill down into the details of the investigation and the activities that the investigation contains. Click **Actions > Edit** to change the name, content set, assignee, or priority. Click **Actions > Export** to download data for all activities and comments that are included in an investigation in JSON format. The JSON file is downloaded to the local downloads directory on the local system.
3. The **Investigations** page provides status, priority, assignee, creator, and dates when the investigation was created and last updated.
4. The **Activities Timeline** provides a view of the activities across time for endpoints. You can zoom into the **Activities Timeline** to understand the relationships between activities in an investigation and double-click an activity to make it the center point in the timeline. Time filters can be very useful in the combined view; however, you might need a very short window due to the quantity of events. Click **Revert** to revert the **Activities Timeline** to the default display for the investigation.
5. (Optional) For each activity in an investigation you can view and add comments. Click the number in the comments column for any activity to view or add comments. In the comments drawer, click **Add** to add a new comment. You can edit or delete existing comments that you have added. You can add comments to closed investigations, but you cannot add additional activities to a closed investigation without reopening the investigation. On the **Overview** page, click the name of a closed investigation and select **Actions > Reopen**.
6. (Optional) For some types of activities, you can select one or more pivot actions to view similar events or data in other Tanium solutions. Click the vertical ellipsis and select a pivot action to perform from the context menu.

When any of the following fields in an investigation change, a description and time of change along with the name of the user who made the change is displayed on the **Audit Log** tab:

- Name
- Description
- Content Set
- Assignee
- Priority

Add annotations to an investigation

You can add annotations to investigations to communicate observations or notations that do not fit any other activity type. Annotations appear in both the **Activities Timeline** and the Activities grid for any investigation. Annotations provide the ability to add comments directly to the **Activities Timeline** that shows endpoint and user activity. Annotations are valuable to help explain the visualization in the **Activities Timeline**, or for noting relevant information when reviewing the data at a later time.

1. In the **Activities Timeline**, click a time that corresponds with the annotation that you want to create and Shift + Click to add an annotation, or click **Add Annotation** in the activities grid.
2. Type the IP address or computer name of the **Endpoint** that you want to associate with the annotation. An endpoint does not need to be online to associate with an annotation. If you do not associate an endpoint, the annotation does not appear on the endpoint tab of the **Activities Timeline**.

© 2026 Tanium Inc. All Rights Reserved

3. Specify a **User** that is associated with the annotation. If you do not associate a user, the annotation does not appear on the users tab of the **Activities Timeline**.
4. Provide **Details** for the annotation. Details that you provide appear in the **Details** column of the activities grid in the investigation.
5. Provide any **Comments** for the annotation. Comments that you provide appear in the comments list for an investigation. You can add comments to closed investigations.
6. Select a **Start Time (UTC)** that corresponds with the time on the **Activities Timeline**. If you create an annotation from the **Activities Timeline**, the **Start Time (UTC)** is populated with the time that corresponds to the area of the **Activities Timeline** you select. Optionally, you can select an **End Time (UTC)**.
7. Click **Add**.

Delete an investigation

1. From the Main menu, go to **Modules > Investigate > Overview**.
2. The **Overview** page provides a list view of all current investigations. Select the name of an investigation.
3. Select Delete investigation. Click **Delete** when prompted.

Close an investigation

1. From the Main menu, go to **Modules > Investigate > Overview**.
2. Select the name of an investigation.
3. Click **Actions > Close** to close the investigation.
4. Provide a comment to explain the reason for closing the investigation. The comment you provide is the final comment in the thread for the investigation unless you reopen the investigation.
5. Click **Close Investigation**.

Reopen an investigation

1. From the Main menu, go to **Modules > Investigate > Overview**.
2. (Optional) You can filter for closed investigations to locate potential investigations to reopen.
3. Select the name of a closed investigation.
4. Click **Actions > Reopen** to reopen the investigation.
5. Provide a comment to explain the reason for reopening the investigation.
6. Click **Reopen Investigation**.

© 2026 Tanium Inc. All Rights Reserved

Investigating performance and activity history on an endpoint

If you are viewing an endpoint in Reporting or Interact, you can quickly view and analyze performance history and activity history on a single endpoint.

View performance and activity history from the **Investigate** tab. You access the **Investigate** tab on the Endpoint Details page of the Reporting workbench. For more information about accessing the Endpoint Details page, see Tanium Reporting User Guide: View endpoint details.

Performance events

Investigate provides a visualization of resource consumption over a specific period of time. Performance events include data for CPU, memory, network, disk, and IO. For each type of performance event you can select specific metrics and view the average, minimum, and maximum values of usage over a time frame. For example, for CPU events, you can view the average, minimum, and maximum percentage of CPU usage over a period of time that you select or provide. The selected or provided time frame displays as a line graph that you can zoom in and out of to analyze with deeper focus. Select multiple metrics to visualize how they correlate with one another.

CPU and memory events display a visualization of the processes that were running at any single point in time during the time frame you select or provide, enabling you to understand which processes were consuming CPU or memory resources at that precise time. You can filter for specific processes to display in the visualization. Wildcards and regular expressions are not supported.

1. At the top of the performance timelines, select the scope to use as a time frame, or select **Custom**. If you select **Custom**, provide values for the date and time that correspond with the start and end of the time frame and click **Apply Scope**.
2. Click the provided icons to zoom in and out of the time frame to analyze a specific time or understand a bigger picture visualization. Panning back and forward in the time frame moves the time frameback or forward by half the current time frame until you reach the minimum (2 weeks ago) or maximum (current time) supported values. For example: Panning out of a "Last 4 Hours" range moves backward in time by two hours, showing six hours ago to two hours ago. Hover over the line chart to show metrics at that specific point in time. Click a highlight to filter the grid to those activities.
3. (Optional) You can filter for specific processes to display in the visualization. Select a sub-tab (CPU, Memory, Network, Disk, or IO) and select or clear the checkboxes of Metrics and Processes to show or hide them in the charts.

For any performance event, the following actions are available to the current user to view the performance event in the context of other Tanium software:

Tanium Interact: Retrieve all computers that have had a similar event happen in the past 14 days.

Tanium Performance: View similar events in the Performance module if the current user has access to Performance.

© 2026 Tanium Inc. All Rights Reserved

Activities

On the Endpoint Details page, select the Investigate tab and go to the activities grid. Events display system-impacting events such as patch installations or policy changes.



Enterprise-Wide Pivots from the Investigate Tab in Single Endpoint View will become available with the release of Reporting 1.36.

The following events are available:

Event types

Event Type	OS	Time Type	Description	Dependency	Available Actions in Tanium Software
Patch installation by Tanium Patch	Linux macOS Windows	Point in time	An operating system patch was installed on the endpoint.	Tanium Patch	Tanium Interact: Gets all computers with the matching patch ID installed. Tanium Patch: Navigate to the specific patch in the Patch module (if the current user has access to Patch).

© 2026 Tanium Inc. All Rights Reserved

Event types (continued)

Event Type	OS	Time Type	Description	Dependency	Available Actions in Tanium Software
Application installation or upgrade by Tanium Deploy	Linux macOS Windows	Point in time	An application was installed or upgraded on the endpoint.	Tanium Deploy	Tanium Interact: Retrieve all computers that have the matching Software Package Id installed on them.
Browser plugins	macOS Windows	Point in time	Browser plugins have been installed, updated or uninstalled.		Tanium Interact: Retrieve all computers that have the same version of the upgraded extension installed.
System reboot	Linux macOS Windows	Point in time	An endpoint has been rebooted.	Tanium Threat Response	Tanium Interact: Queries for all computers where the last reboot time is less than the reboot time referenced in the activity.

© 2026 Tanium Inc. All Rights Reserved

Event types (continued)

Event Type	OS	Time Type	Description	Dependency	Available Actions in Tanium Software
External storage connected	Windows	Point in time	An external storage device has been connected.		Tanium Interact: Query for computers that have had the same device (based on device id) inserted or removed.
GPO policy changes performed by Tanium Enforce	Windows	Point in time	A new Windows group policy setting has been applied or a currently applied policy has been changed.	Tanium Enforce	Tanium Enforce: View the related policy in the Enforce module if the current user has access to Enforce.

© 2026 Tanium Inc. All Rights Reserved

Event types (continued)

Event Type	OS	Time Type	Description	Dependency	Available Actions in Tanium Software
User logon/logoff	Windows	Point in time	A user has logged into or off of an endpoint.		Tanium Interact: Get all computers where this user has logged in. Tanium Interact: Get all computers that have the same explicit subject login. Tanium Interact: Get all computers that have the same explicit target login.
Local account lockout	Windows	Point in time	A local account has been locked out.		Tanium Interact: Get all computers where a particular user has been locked out of.
ServiceNow ticket creation	Linux macOS Windows	Point in time	A ServiceNow ticket has been created.	ServiceNow integration	

© 2026 Tanium Inc. All Rights Reserved

Event types (continued)

Event Type	OS	Time Type	Description	Dependency	Available Actions in Tanium Software
DNS	Windows 8.1 or later and Linux endpoints where eBPF is enabled	Point in time	Request information, including the process path, user, query, response, and the type of operation. On Windows and Linux endpoints where eBPF is enabled, DNS events are only recorded when you use the system DNS client. DNS events for applications that use their own DNS client are not recorded. For example, nslookup and Google Chrome.	Tanium Threat Response	
Driver	Linux macOS Windows	Point in time	Historical data from each endpoint regarding driver loads; for example, the full path and hash of a driver. By default, Driver Load events are not selected. Selecting Driver Loads on Windows filters for image and process.path is 'system'. Selecting Driver Loads on Linux or macOS filters for image.	Tanium Threat Response	
File	Linux macOS Windows	Point in time	File system events, such as files written to directory locations on the endpoint. The associated process and user context are included. Examples: A malware file copied to a location that Windows Update uses, or content changes made to a file.	Tanium Threat Response	
Image	Windows	Point in time	Historical data from each endpoint regarding image loads; for example, the full path and hash, the entity that signed an image, or a designation of "Unsigned" if the image is not signed. A possible example is the loading of an unsigned DLL. If you do not select Image Loads, any Signal that uses the image event type results in an Unmatched Events warning in the Alert Details. Selecting Image Loads filters for image and process.path is not 'system'. Selecting Image Loads does not apply filters for Linux or Mac endpoints.	Tanium Threat Response	

© 2026 Tanium Inc. All Rights Reserved

Event types (continued)

Event Type	OS	Time Type	Description	Dependency	Available Actions in Tanium Software
Network	Linux macOS Windows	Point in time	Network connection events, such as an HTTP request to an internet location, including the associated process and user context. Events are recorded for all inbound and outbound TCP connections.	Tanium Threat Response	
Process	Linux macOS Windows	Point in time	Process events, such as path, hash, command line, user information, ancestry, and the signed status of a process.	Tanium Threat Response	
Registry	Windows	Point in time	Changes to the registry, such as the creation or alteration of registry keys and values. Includes the associated process and user context.	Tanium Threat Response	
Security	Linux macOS Windows	Point in time	Security events such as authentication, privilege escalation, and more. This event type includes logon events, even if operating system logs have rolled. For more information about specific event IDs and Linux security events, see https://github.com/linux-audit/audit-userspace/blob/master/lib/libaudit.h. For more information about specific event IDs and Windows security events, see https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-auditing-faq.	Tanium Threat Response	

© 2026 Tanium Inc. All Rights Reserved

Event types (continued)

Event Type	OS	Time Type	Description	Dependency	Available Actions in Tanium Software
Windows Events	Windows	Point In Time	Log data from the following Windows Event logs: • Applications • Security • Setup • System • Forwarded Events For more information, see Windows Logs.		

For each activity in the grid, you can click to view advanced details for the activity. Advanced details provide the start and stop times of the activity and information about the specific event. For example, if the activity is a Windows event, you can view information from the Windows event log and view the Windows event message.

In the activities grid, click **Scope Charts to Timeframe**in the Actions column to view the activities timeline that is focused on the selected activity. Focusing on the selected activity enables you to understand how the selected activity occurs with regards to other activities occurring around the same time.

You can select an activity in the grid and click **Show Recorder Data** to display events from the Client Recorder Extension that occurred within a 10 minute timeframe of the selected activity. Selecting this option displays recorder events that occurred five minutes before and five minutes after the activity start time. For more information about the types of events that the Client Recorder Extension captures, see Tanium Client Recorder Extension User Guide.

In the activities grid, select one or more events and click **Add to Investigation** to add the activity to a new or existing investigation.

ServiceNow

Investigate provides the ability to integrate activities from ServiceNow. You can add ticket creation in ServiceNow as an activity in an investigation.



Using ServiceNow integration requires the **Investigate Partner Integration** permission.

1. From ServiceNow, select a ticket for which you want to add activities to an investigation.
2. Click **Launch Tanium Live UI**.

© 2026 Tanium Inc. All Rights Reserved

3. A direct connection is opened to the endpoint that is the subject of the ticket.
4. On the Endpoint Details page, select the **Investigate** tab and go to the activities grid.
5. In the activities grid, select one or more activities and click **Add to Investigation** to add the activity to an investigation.

© 2026 Tanium Inc. All Rights Reserved

Browsing the file system on an endpoint

If you are viewing an endpoint in Reporting, you can browse the file system on connected endpoints and download files. You can delete files on an endpoint if you have the **direct connect file write** permission.

1. Click an online endpoint in an investigation.
2. Click **File Browser** to open a file browser at the root directory. On Windows endpoints the default location is `c:\`. On macOS and Linux endpoints the default location is `/`. File Browser requires an active direct connection. When you click **File Browser** on an online endpoint, a direct connection is initiated.
3. Navigate the file system by typing a path, or by clicking directories in the file browser of the breadcrumbs of the path. For each file in a directory you can view the size, creation date, modification date, and the permissions for the file. Symbolic links are visible while file browsing in a live connection.
4. Click one or more files to download or delete. To delete a file, ensure that you have the **direct connect file write** permission and click the delete icon at the end of the row. Click **Delete**.

© 2026 Tanium Inc. All Rights Reserved

Managing a single endpoint remotely

In Reporting or Interact, you can take action on Windows services and quickly view a resource summary and live process monitor on a single endpoint. Use the live process monitor to view, copy, export, and terminate live processes on an endpoint.

View a resource summary and live process monitor from the **Remote Management** tab. You access the **Remote Management** tab on the Endpoint Details page. For more information on accessing the Endpoint Details page, see Tanium Reporting User Guide: View endpoint details.

Service control

The Service Control section of the **Remote Management** tab enables you to manage Windows services. You can start, stop, or restart Windows device drivers and startup programs. From the Service Control section, you can view a list of all services on a Windows endpoint along with a description of the service that is useful for troubleshooting. You can filter the list by the name of the service, status of the service, the startup type of the service, and the log in of the service. You can take action on any service that includes stopping or restarting a running service or starting a stopped service.

You can filter by the following startup types:

Automatic

The Automatic startup type includes services that are started by the operating system at system start-up.

Boot

The Boot startup type includes device drivers that are started by the system loader. This type is only for device drivers.

Disabled

The Disabled startup type includes disabled services. A disabled service cannot be started by a user or application.

Manual

The Manual startup type includes services that are started manually by a user (using the Service Control Manager) or by an application.

System Start

The System Start startup type includes device drivers that are started by the IOInitSystem function. This type is only for device drivers.

To take action on a service in the Service Control section, go to the row that corresponds to the service you want to act on. From the **Actions** column, click the ellipsis and click an available action.

© 2026 Tanium Inc. All Rights Reserved

Resource summary

The resource summary offers a visualization of CPU, memory, network, and disk usage on an endpoint. You can view network and disk data for all network controllers and drives on an endpoint.

CPU

View the total number of processors on an endpoint, the total percentage of CPU resources presently in use, and the current speed of CPU resources.

Memory

View the available amount and total current percentage of memory use on an endpoint.

Network

Select a connected network controller and view the send and receive throughput for the network controller. The throughput represents the amount of data moved successfully from one place to another per second.

Disk

Selected a connected drive and view the read and write throughput for the drive. The throughput represents the amount of data read or written per second.

Live process monitor

Use the live process monitor to view, copy, export, and terminate processes on an endpoint. All of the live processes on an endpoint display in a grid that provides the process ID, process name, percentage of CPU resources that the process is using, the working set size (the amount of memory the process needs to continue running), and I/O read and write bytes for the process (the amount of data read or written per second). You can filter the grid by process ID and process, and you can sort the grid by any heading.

Export process data

1. Select checkboxes that correspond with one or more processes.
2. Click **Export > Export to CSV** to export the process data to a CSV file that is saved to the download location of the web browser, or click **Export > Copy to clipboard** to copy the process data to the clipboard of the local system.

Terminate one or multiple processes



The **Direct Connect Terminate process** permission is required to terminate processes.

© 2026 Tanium Inc. All Rights Reserved

1. Select one or more checkboxes that correspond with processes in the live process grid.
2. Click Terminate Process(es).
3. Confirm that you want to terminate the processes that are listed in the confirmation panel. Terminating system processes can result in system instability or data loss.
4. Click **Terminate Process(es)** or **Force Terminate Process(es)**.

Browse and edit the Windows registry

The registry browser enables you to view and remediate issues with the Windows registry on endpoints. You can view a hierarchical view of registry hives, keys, values, and data and edit and delete keys, values, and data. Expand a hive in the registry browser to view the keys that it contains, and the values and data that are associated with each key.



The **Direct Connect Registry** permission is required to browse and edit the Windows registry.



Consider creating a registry backup if you decide to edit the registry. You can revert back to the previous state of the Windows registry from a backup.

Add a new registry value

1. In the **Browse and Edit the Windows Registry** section, expand a hive in the registry browser and select the key that a new registry value should exist under.
2. Click **New Value**.
3. Provide a **Value Name**.
4. Provide a **Value Type**. The available types are:

   String Value (REG_SZ)

   A Unicode or an ANSI string.

   Binary Value (REG_BINARY)

   Data in binary form.

   DWORD Value (REG_DWORD)

   A 32-bit number.

   QWORD Value (REG_QWORD)

   A 64-bit number.

   Multi-String Value (REG_MULTI_SZ)

   A sequence of null-terminated strings, terminated by an empty string.

© 2026 Tanium Inc. All Rights Reserved

Expandable String Value (REG_EXPAND_SZ)

A null-terminated string that contains unexpanded references to environment variables.

5. Provide **Value Data**.
6. Click **Save**.

When you create a registry value in `HKEY_CLASSES_ROOT` it is created in `HKEY_LOCAL_MACHINE\Software\Classes` since Investigate is running as `SYSTEM`. If you use RegEdit to view the value, you can view it in this location.

If you create a registry value using RegEdit in `HKEY_CLASSES_ROOT`, it is created in `HKEY_USERS\<SID>\Software\Classes` where `<SID>` is the security identifier for the user logged onto the endpoint running RegEdit. If you use the registry browser to view the value, you can view it in this location.

Any values you create in `HKEY_CURRENT_USER` using the registry browser is created in `HKEY_USERS\<SID>`. If you use RegEdit to view the value, you can view it in this location.

Edit a registry value

1. In the **Browse and Edit the Windows Registry** section, expand a hive in the registry browser and select the key that a you want to edit.
2. From the actions column for the key, select **Edit**.
3. You can edit the **Value Name**, **Value Type**, and **Value Data**.
4. Click **Save**.

Delete a registry value

1. In the **Browse and Edit the Windows Registry** section, expand a hive in the registry browser and select the key that a you want to delete.
2. From the actions column for the key, select **Delete**.

Export registry data

1. In the **Browse and Edit the Windows Registry** section, expand a hive in the registry browser and select the key that a you want to export.
2. Click **Export**.
3. Select one of the following options:

   Export to CSV

   Export the registry key data to a CSV file that is saved to the download location of the web browser.

   Copy to clipboard

   Copy the registry key data to the clipboard of the local system.

© 2026 Tanium Inc. All Rights Reserved

Viewing Windows events

In Reporting or Interact, you can quickly view details of Windows Event Logs on a single endpoint.

View Windows Logs from the **Windows Events** tab. You access the **Windows Events** tab on the Endpoint Details page. For more information about accessing the Endpoint Details page, see Tanium Reporting User Guide: View endpoint details.

Windows Events

The Windows Event Browser replicates the event viewer experience on Windows devices to support administrators and analysts with remotely addressing endpoint challenges. For example, use the Windows Event Browser to detect and troubleshoot issues such as errors, unauthorized activity, external threats, or system failures on an endpoint by analyzing event logs. Futhermore, the Windows Event Browser provides the ability to focus on events that follow specific parameter matches within a specific log to enable you to filter out the events displayed that are not specific to your needs.

If you are experiencing unstable performance on a Windows device and experiencing frequent crashes, you might suspects a problem with the RAM on the device and run the Windows Memory Diagnostic Tool to check for memory problems. The detailed results of the RAM testing are logged and stored in the Windows Event Log Viewer. You can view the results of the Memory Diagnostic, however there is a large number of events in the System Logs. Rather than searching through the 100s of events in the System Log to find the relevant one, you can use the Search functionality for a keyword search of “Memory Diagnostic”, which returns the event that is associated with the output of the diagnostic tool.

Use the Windows Event Browser to view log data from the following Windows Event logs:

- Applications
- Security
- Setup
- System
- Forwarded Events

Additionally, Applications and Services Logs are provided if available.

1. Select a log and filter with the following options:

   Level

   Select one of All, Critical, Error, Warning, Information, or Verbose.

   Event Source

   The event source is the name of the software that logs the event. For more information about event sources, see https://learn.microsoft.com/en-us/windows/win32/eventlog/event-sources.

© 2026 Tanium Inc. All Rights Reserved

Event ID

Event identifiers uniquely identify a particular event. Each event source can define its own numbered events and the description strings to which they are mapped in its message file. For more information about Event IDs, see https://learn.microsoft.com/en-us/windows/win32/eventlog/event-identifiers.

2. For any item in the list of returned log matches, select Advanced Details to view information about the match. For example, you can view a message that describes the logged event, the Log Name, Source, Event ID, Level, User, OpCode Logged Time, Task Category, or Keywords that are associated with the match.
3. (Optional) Click **Add to Investigation** from the Advanced Details panel or **Add Event to Investigation** from the actions column of the grid to add the log entry to a new or existing investigation.

Windows Event Log Subscriptions

Windows Event Log Subscriptions displays default subscriptions to Windows Events you can use to troubleshoot common problems and perform root cause analysis across a broad range of scenarios. You can enable or disable subscriptions to accommodate a variety of scenarios. You can select to display all Event Log Subscriptions, or subscriptions that are either enabled or disabled. To enable or disable a subscription, locate the row of the subscription that you want to enable or disable and move the toggle appropriately. You can view the results of subscriptions that you enable in the activities drop down in the Investigate tab.

You can filter the list by the category, source, or author of the subscription. After you filter the list of subscriptions, you can export the list as a CSV file, or copy the data to the Windows clipboard. Click **Export > Export to CSV** or **Export > Copy to Clipboard**.

For more information about any of the provided subscriptions, see Reference: Windows events.

Create a new subscription

You can manually create subscriptions without having to Direct Connect to an endpoint.

1. Click **Create Subscription**.
2. Provide the following information:

Event ID

Event identifiers uniquely identify a particular event. Each event source can define its own numbered events and the description strings to which they are mapped in its message file. For more information about Event IDs, see https://learn.microsoft.com/en-us/windows/win32/eventlog/event-identifiers.

Event Source

The event source is the name of the software that logs the event. For more information about event sources, see https://learn.microsoft.com/en-us/windows/win32/eventlog/event-sources.

Log Path

The path to the event log file in the local file system.

Name

A name for the subscription that you can use to quickly find it in a list of subscriptions.

© 2026 Tanium Inc. All Rights Reserved

Category

Select one of Application, System & OS Event, System Configuration, or User Logon / Logoff Events

3. Click **Save** or **Save and Create Another Subscription**.



Subscriptions that do not have a name or category assigned display at the bottom of the Windows Event Log Subscriptions list with the Event ID used as the name.

For more information about locating values such as Event Source and Log Path for subscriptions, see Reference: Event log data.

© 2026 Tanium Inc. All Rights Reserved

Troubleshooting the Tanium Client on a single endpoint

In Reporting or Interact, you can quickly download log files, action history, and other useful troubleshooting data from a single endpoint.

Download log files, action history, and access logically grouped bundles of logs and other artifacts, sometimes referred to as an Endpoint Must Gather (EMG) from the **Client Health** tab. You access the **Client Health** tab on the Endpoint Details page. For more information on accessing the Endpoint Details page, see Tanium Reporting User Guide: View endpoint details.

Logs and actions

Use the **Client Health** tab to download log files and action history from an endpoint. the Review Tanium Client logs to help you troubleshoot client issues. For example, a client might not answer questions or appear in the Tanium Console (**Administration > Configuration > Client Status**) because that client cannot connect to the Tanium Server or Zone Server. In this case, you can review the client logs to determine whether the connection failed due to an invalid server IP address, DNS resolution failure, missing Tanium public key file, or firewall rule. For more information on Tanium Client logs, see Tanium Client Management User Guide: Access individual endpoint logs in Client Management.

When a package does not seem to work after you deploy it through an action, review action logs and the files associated with the action to help troubleshoot. Each time the Tanium Client receives an action message with an instruction set to execute, the client creates an action log file named Action_<ID>.log, where <ID> is the action identifier. The action log contains the CLI output associated with the action command. The Tanium Client stores any files that are required to deploy an action package in Action_ID directories. For more information on action history, see Tanium Client Management User Guide: Review action logs and associated files to troubleshoot actions and packages .

Download client logs

From the **Logs** panel on the **Client Health**tab, select a log file to view or download the contents. Click **Download** to download the contents to the download location of the web browser.

Download action history

From the **Actions** panel on the **Client Health** tab, select a log file to view or download the contents. Click **Download** to download the contents to the download location of the web browser.

Gather

Use the **Client Health** tab to collect a bundle of logs and other artifacts, sometimes referred to as an Endpoint Must Gather (EMG).

© 2026 Tanium Inc. All Rights Reserved

1. From the **Available Steps** panel in the **Client Health** tab, select one or more available steps for which you want to gather troubleshooting information. Available steps are grouped by domain, which corresponds to a Tanium solution area to which the troubleshooting information is relevant.
2. Click **Gather from Endpoint**. The available steps that you selected display in the **Must Gathers** panel. When the value of the result column for each available step you select displays as Complete, you can download the troubleshooting information for that available step.
3. From the **Must Gathers** panel, select one or more completed available steps, and click **Download** to download the contents to the download location of the web browser.

For more information on collecting troubleshooting information from endpoints, see Tanium Client Management User Guide: Collect troubleshooting information from endpoints .

© 2026 Tanium Inc. All Rights Reserved

Troubleshooting Investigate

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

Collect logs

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

To download logs:

1. From the Investigate **Overview** page, click Help .
2. From the **Troubleshooting** tab, select the solutions for which to gather troubleshooting packages and click **Create Packages**. By default, all solutions are selected.
3. When the packages are ready, click **Download Support Bundle**.
   ZIP files of all the selected packages download to the local download directory.

   Some browsers might block multiple downloads by default. Make sure to configure your browser to permit multiple downloads from the Tanium Console.
4. Contact Tanium Support to determine the best option to send the ZIP files. For more information, see Contact Tanium Support on page 47.

Verify endpoint tools

If you are experiencing issues such as a feature not working on an endpoint or seeing incorrect data in the workbench, confirm that your endpoints have the latest toolset version. For more information, see Tanium Endpoint Configuration User Guide: Identify and resolve issues with endpoint tools or Client Extensions.

Contact Tanium Support

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

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

© 2026 Tanium Inc. All Rights Reserved

Reference: Windows events

The following reference provides details about the various Windows events that Investigate provides subscriptions for.

Windows event types available for subscription in Investigate

Event Type	Category	Event ID	Log Path	Source	Reference
Application Install	Application	1033	Application	MsiInstaller	https://learn.microsoft.com/en-us/windows/win32/msi/event-logging
Application Uninstall	Application	1034	Application	MsiInstaller	https://learn.microsoft.com/en-us/windows/win32/msi/event-logging
Reboot Required	System & OS Event	1038	Application	MsiInstaller	https://learn.microsoft.com/en-us/windows/win32/msi/event-logging
OS/App Update Removal	System & OS Event	1037	Application	MsiInstaller	https://learn.microsoft.com/en-us/windows/win32/msi/event-logging
OS/App Update Complete	System & OS Event	1036	Application	MsiInstaller	https://learn.microsoft.com/en-us/windows/win32/msi/event-logging
Group Policy Processing Failed due to Network	System Configuration	1129	System	Microsoft-Windows-GroupPolicy	Applying Group Policy troubleshooting guidance - Windows Server | Microsoft Learn
Group Policy Processing Failed due to DNS	System Configuration	1054	System	Microsoft-Windows-GroupPolicy	Applying Group Policy troubleshooting guidance - Windows Server | Microsoft Learn

© 2026 Tanium Inc. All Rights Reserved

Windows event types available for subscription in Investigate (continued)

Group Policy Processing Failed due to Authentication	System Configuration	1006	System	Microsoft-Windows-GroupPolicy	Applying Group Policy troubleshooting guidance - Windows Server | Microsoft Learn
Group Policy Processing Failed due to System Allocation	System Configuration	1002	System	Microsoft-Windows-GroupPolicy	Applying Group Policy troubleshooting guidance - Windows Server | Microsoft Learn
Group Policy Processing Failed	System Configuration	1030	System	Microsoft-Windows-GroupPolicy	Applying Group Policy troubleshooting guidance - Windows Server | Microsoft Learn
Group Policy Processing Failed to read file	System Configuration	1058	System	Microsoft-Windows-GroupPolicy	Applying Group Policy troubleshooting guidance - Windows Server | Microsoft Learn
Group Policy Processing Failed to resolve user name	System Configuration	1053	System	Microsoft-Windows-GroupPolicy	Applying Group Policy troubleshooting guidance - Windows Server | Microsoft Learn
Group Policy Processing Failed to determine computer account	System Configuration	1097	System	Microsoft-Windows-GroupPolicy	Applying Group Policy troubleshooting guidance - Windows Server | Microsoft Learn
Group Policy Processing Started	System Configuration	4016	System	Microsoft-Windows-GroupPolicy	Applying Group Policy troubleshooting guidance - Windows Server | Microsoft Learn
Group Policy Processing Completed Successfully	System Configuration	5016	System	Microsoft-Windows-GroupPolicy	Applying Group Policy troubleshooting guidance - Windows Server | Microsoft Learn
Windows Firewall Setting Changed	System Configuration	4950	Security	Microsoft-Windows-Security-Auditing	4950(S) A Windows Firewall setting has changed. - Windows Security | Microsoft Learn

© 2026 Tanium Inc. All Rights Reserved

Windows event types available for subscription in Investigate (continued)

Windows Firewall Settings Restored to Default	System Configuration	4949	Security	Microsoft-Windows-Security-Auditing	4949(S) Windows Firewall settings were restored to the default values. - Windows Security | Microsoft Learn
Windows Firewall Rule Ignored due to Unrecognized Version	System Configuration	4951	Security	Microsoft-Windows-Security-Auditing	4951(F) A rule has been ignored because its major version number wasn't recognized by Windows Firewall. - Windows Security | Microsoft Learn
Windows Firewall Rule Partially Ignored due to Unrecognized Version	System Configuration	4952	Security	Microsoft-Windows-Security-Auditing	4952(F) Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall. The other parts of the rule will be enforced. - Windows Security | Microsoft Learn
Windows Firewall Rule Ignored because it couldn't be parsed	System Configuration	4953	Security	Microsoft-Windows-Security-Auditing	4953(F) Windows Firewall ignored a rule because it couldn't be parsed. - Windows Security | Microsoft Learn
Windows Firewall Group Policy Settings Changed	System Configuration	4954	Security	Microsoft-Windows-Security-Auditing	4954(S) Windows Firewall Group Policy settings have changed. The new settings have been applied. - Windows Security | Microsoft Learn
Windows Firewall Rule Not Applied	System Configuration	4957	Security	Microsoft-Windows-Security-Auditing	4957(F) Windows Firewall did not apply the following rule. - Windows Security | Microsoft Learn
Windows Firewall Active Profile Changed	System Configuration	4956	Security	Microsoft-Windows-Security-Auditing	4956(S) Windows Firewall has changed the active profile. - Windows Security | Microsoft Learn

© 2026 Tanium Inc. All Rights Reserved

Windows event types available for subscription in Investigate (continued)

Windows Firewall Rule Not Applied due to Configuration	System Configuration	4958	Security	Microsoft-Windows-Security-Auditing	4958(F) Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer. - Windows Security | Microsoft Learn
Windows Firewall Policy Activated on Startup	System Configuration	4944	Security	Microsoft-Windows-Security-Auditing	4944(S) The following policy was active when the Windows Firewall started. - Windows Security | Microsoft Learn
Windows Firewall Rule listed on Startup	System Configuration	4945	Security	Microsoft-Windows-Security-Auditing	4945(S) A rule was listed when the Windows Firewall started. - Windows Security | Microsoft Learn
Windows Firewall Exception List Rule Added	System Configuration	4946	Security	Microsoft-Windows-Security-Auditing	4946(S) A change has been made to Windows Firewall exception list. A rule was added. - Windows Security | Microsoft Learn
Windows Firewall Exception List Rule Modified	System Configuration	4947	Security	Microsoft-Windows-Security-Auditing	4947(S) A change has been made to Windows Firewall exception list. A rule was modified. - Windows Security | Microsoft Learn
Windows Firewall Exception List Rule Deleted	System Configuration	4948	Security	Microsoft-Windows-Security-Auditing	4948(S) A change has been made to Windows Firewall exception list. A rule was deleted. - Windows Security | Microsoft Learn
Bitlocker TPM Not Found	System & OS Event	853	Microsoft-Windows-Bitlocker/Management	Microsoft-Windows-BitLocker-API	Enforcing BitLocker policies by using Intune: known issues - Windows Client | Microsoft Learn
Bitlocker Encryption Started	System & OS Event	768	Microsoft-Windows-Bitlocker/Management	Microsoft-Windows-BitLocker-API	BitLocker encryption was started for volume %3 using %4 algorithm.

© 2026 Tanium Inc. All Rights Reserved

Windows event types available for subscription in Investigate (continued)

Bitlocker Decryption Started	System & OS Event	770	Microsoft-Windows-Bitlocker/Management	Microsoft-Windows-BitLocker-API	BitLocker decryption was started for volume %3.
Bitlocker Decryption Stopped	System & OS Event	771	Microsoft-Windows-Bitlocker/Management	Microsoft-Windows-BitLocker-API	BitLocker encryption was stopped for volume %3.
Computer joined a domain	System & OS Event	1	System	Microsoft-Windows-DomainJoinManagerTriggerProvider	
Computer left a domain	System & OS Event	2	System	Microsoft-Windows-DomainJoinManagerTriggerProvider	
DHCP Lease Lost	System & OS Event	1000	Microsoft-Windows-Dhcp-Client/Admin	Microsoft-Windows-Dhcp-Client	Your computer has lost the lease to its IP address %1 on the Network Card with network address %3.
DHCP Lease Could Not Be Obtained	System & OS Event	1001	Microsoft-Windows-Dhcp-Client/Admin	Microsoft-Windows-Dhcp-Client	Your computer was not assigned an address from the network (by the DHCP Server) for the Network Card with network address %2. The following error occurred: %3. Your computer will continue to try and obtain an address on its own from the network address (DHCP) server.
DHCP Lease Denied	System & OS Event	1002	Microsoft-Windows-Dhcp-Client/Admin	Microsoft-Windows-Dhcp-Client	The IP address lease %1 for the Network Card with network address %3 has been denied by the DHCP server %4 (The DHCP Server sent a DHCPNACK message).

© 2026 Tanium Inc. All Rights Reserved

Windows event types available for subscription in Investigate (continued)

DHCP Lease Could Not Be Renewed	System & OS Event	1003	Microsoft-Windows-Dhcp-Client/Admin	Microsoft-Windows-Dhcp-Client	Your computer was not able to renew its address from the network (from the DHCP Server) for the Network Card with network address %2. The following error occurred: %3. Your computer will continue to try and obtain an address on its own from the network address (DHCP) server.
DHCP Lease Obtained	System & OS Event	1007	Microsoft-Windows-Dhcp-Client/Admin	Microsoft-Windows-Dhcp-Client	Your computer has automatically configured the IP address for the Network Card with network address %2. The IP address being used is %3.
Document Printed	System & OS Event	307	Microsoft-Windows-PrintService/Operational	Microsoft-Windows-PrintService	Document %1, %2 owned by %3 on %4 was printed on %5 through port %6. Size in bytes: %7. Pages printed: %8. No user action is required.
Printer Added	System & OS Event	300	Microsoft-Windows-PrintService/Operational	Microsoft-Windows-PrintService	Printer %1 was created. No user action is required.
Printer Deleted	System & OS Event	301	Microsoft-Windows-PrintService/Operational	Microsoft-Windows-PrintService	Printer %1 was deleted, and users will no longer be able to print to this printer. No user action is required.
Printer Configuration Changed	System & OS Event	306	Microsoft-Windows-PrintService/Operational	Microsoft-Windows-PrintService	Settings for printer %1 were changed. No user action is required.
Network Connected	System & OS Event	10000	Microsoft-Windows-NetworkProfile/Operational	Microsoft-Windows-NetworkProfile	Network Connected
Network Disconnected	System & OS Event	10001	Microsoft-Windows-NetworkProfile/Operational	Microsoft-Windows-NetworkProfile	Network Disconnected

© 2026 Tanium Inc. All Rights Reserved

Windows event types available for subscription in Investigate (continued)

WiFi Disconnected	System & OS Event	8003	Microsoft-Windows-WLAN-AutoConfig/Operational	Microsoft-Windows-WLAN-AutoConfig	WLAN AutoConfig service has successfully disconnected from a wireless network.
WiFi Failed to Connect	System & OS Event	8002	Microsoft-Windows-WLAN-AutoConfig/Operational	Microsoft-Windows-WLAN-AutoConfig	WLAN AutoConfig service failed to connect to a wireless network.
WiFi Connected	System & OS Event	8001	Microsoft-Windows-WLAN-AutoConfig/Operational	Microsoft-Windows-WLAN-AutoConfig	WLAN AutoConfig service has successfully connected to a wireless network.
Windows Update Installed	System & OS Event	19	Microsoft-Windows-WindowsUpdateClient/Operational	Microsoft-Windows-WindowsUpdateClient	Installation Successful: Windows successfully installed the following update: %1
Windows Update Install Failed	System & OS Event	20	Microsoft-Windows-WindowsUpdateClient/Operational	Microsoft-Windows-WindowsUpdateClient	Installation Failure: Windows failed to install the following update with error %1: %2.
Windows Update Restart Required	System & OS Event	21	Microsoft-Windows-WindowsUpdateClient/Operational	Microsoft-Windows-WindowsUpdateClient	Restart Required: To complete the installation of the following updates, the computer must be restarted. Until this computer has been restarted, Windows cannot search for or download new updates: %1
Windows Update Restart Initiated	System & OS Event	22	Microsoft-Windows-WindowsUpdateClient/Operational	Microsoft-Windows-WindowsUpdateClient	Restart Required: To complete the installation of the following updates, the computer will be restarted within %1 minutes: %2
Windows Update failed to check for updates	System & OS Event	25	Microsoft-Windows-WindowsUpdateClient/Operational	Microsoft-Windows-WindowsUpdateClient	Windows Update failed to check for updates with error %1.
Windows Update Downloaded	System & OS Event	41	Microsoft-Windows-WindowsUpdateClient/Operational	Microsoft-Windows-WindowsUpdateClient	An update was downloaded.

© 2026 Tanium Inc. All Rights Reserved

Windows event types available for subscription in Investigate (continued)

SMB Client Disconnected from server	System & OS Event	30805	Microsoft-Windows-SMBClient/Connectivity	Microsoft-Windows-SMBClient	The client lost its session to the server.
SMB Client Reconnected to server	System & OS Event	30806	Microsoft-Windows-SMBClient/Connectivity	Microsoft-Windows-SMBClient	The client re-established its session to the server. You should expect this event if there was a previous event 30805, but the client successfully resumed the cached connection before the timeout expired.
SMB Client Disconnected from share	System & OS Event	30807	Microsoft-Windows-SMBClient/Connectivity	Microsoft-Windows-SMBClient	The connection to the share was lost. If the server is a Windows Failover Cluster file server, then this message occurs when the file share moves between cluster nodes. There should also be an anti-event 30808 indicating the session to the server was re-established. If the server is not a failover cluster, it is likely that the server was previously online, but it is now inaccessible over the network.

© 2026 Tanium Inc. All Rights Reserved

Windows event types available for subscription in Investigate (continued)

SMB Client Reconnected to share	System & OS Event	30808	Microsoft-Windows-SMBClient/Connectivity	Microsoft-Windows-SMBClient	The connection to the share was re-established. If the server is a Windows Failover Cluster file server, then this message occurs when the file share moves between cluster nodes. There should also be an anti-event 30808 indicating the session to the server was re-established. If the server is not a failover cluster, it is likely that the server was previously online, but it is now inaccessible over the network.
SMB Client Network Disconnected	System & OS Event	30804	Microsoft-Windows-SMBClient/Connectivity	Microsoft-Windows-SMBClient	A network connection was disconnected. This indicates that the client's connection to the server was disconnected. Frequent, unexpected disconnects when using an RDMA over Converged Ethernet (RoCE) adapter may indicate a network misconfiguration. RoCE requires Priority Flow Control (PFC) to be configured for every host, switch and router on the RoCE network. Failure to properly configure PFC will cause packet loss, frequent disconnects and poor performance.

© 2026 Tanium Inc. All Rights Reserved

Windows event types available for subscription in Investigate (continued)

SMB Client Failed to establish network connection	System & OS Event	30803	Microsoft-Windows-SMBClient/Connectivity	Microsoft-Windows-SMBClient	Failed to establish a network connection. This indicates a problem with the underlying network or transport, such as with TCP/IP or QUIC/UDP, and not with SMB. A firewall that blocks TCP port 445 or UDP port 443 or TCP port 5445 when using an iWARP RDMA adapter can also cause this issue.
SMB Client Failed to resolve name	System & OS Event	30800	Microsoft-Windows-SMBClient/Connectivity	Microsoft-Windows-SMBClient	The server name cannot be resolved. The client cannot resolve the server address in DNS or WINS. This issue often manifests immediately after joining a computer to the domain, when the client's DNS registration may not yet have propagated to all DNS servers. You should also expect this event at system startup on a DNS server (such as a domain controller) that points to itself for the primary DNS. You should validate the DNS client settings on this computer using IPCONFIG /ALL and NSLOOKUP.
System Certificate Expired	System & OS Event	1002	Microsoft-Windows-CertificateServicesClient-Lifecycle-System/Operational	Microsoft-Windows-CertificateServicesClient-Lifecycle-System	A certificate has expired. For more information, see the "Details" section.
User Certificate Expired	System & OS Event	1002	Microsoft-Windows-CertificateServicesClient-Lifecycle-User/Operational	Microsoft-Windows-CertificateServicesClient-Lifecycle-User	A certificate has expired. For more information, see the "Details".
Service State Change	System & OS Event	7036	System	Service Control Manager	The %1 service entered the %2 state.

© 2026 Tanium Inc. All Rights Reserved

Windows event types available for subscription in Investigate (continued)

Service Hung	System & OS Event	7022	System	Service Control Manager	The %1 service hung on starting.
Service Installed	System & OS Event	7045	System	Service Control Manager	A service was installed in the system.
Service Start Type Changed	System & OS Event	7040	System	Service Control Manager	The start type of the %1 service was changed from %2 to %3.
Service Terminated Unexpectedly	System & OS Event	7034	System	Service Control Manager	The %1 service terminated unexpectedly. It has done this %2 time(s).
DNS Timeout	System & OS Event	1014	System	Microsoft-Windows-DNS-Client	Name resolution for the name %1 timed out after none of the configured DNS servers responded. Client PID %4.
DNS IPv4 Not Configured	System & OS Event	1000	System	Microsoft-Windows-DNS-Client	There are currently no IPv4 DNS servers configured for any interface on this host. Please configure DNS server settings, or renew your dynamic IP settings.
DNS IPv6 Not Configured	System & OS Event	1019	System	Microsoft-Windows-DNS-Client	There are currently no IPv6 DNS servers configured for any interface on this host. Please configure DNS server settings, or renew your dynamic IP settings.
Application Hang	System & OS Event	1002	Application	Application Hang	The program %1 version %2 stopped interacting with Windows and was closed. To see if more information about the problem is available, check the problem history in the Security and Maintenance control panel.
Application Error	System & OS Event	1000	Application	Application Error	

© 2026 Tanium Inc. All Rights Reserved

Windows event types available for subscription in Investigate (continued)

Successful Logon	User Logon/Logoff Events	4624	Security	Microsoft-Windows-Security-Auditing	https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4624
Failed Logon	User Logon/Logoff Events	4625	Security	Microsoft-Windows-Security-Auditing	https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4625
Explicit Logon	User Logon/Logoff Events	4648	Security	Microsoft-Windows-Security-Auditing	https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4648
SIDs Filtered	User Logon/Logoff Events	4675	Security	Microsoft-Windows-Security-Auditing	https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4675
Successful Logoff	User Logon/Logoff Events	4634	Security	Microsoft-Windows-Security-Auditing	https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4634

© 2026 Tanium Inc. All Rights Reserved

Windows event types available for subscription in Investigate (continued)

User Initiated Logoff	User Logon/Logoff Events	4647	Security	Microsoft-Windows-Security-Auditing	https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4647
User Account Lockout	User Logon/Logoff Events	4740	Security	Microsoft-Windows-Security-Auditing	https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4740
System Shutdown/Reboot	System & OS Event	1074	System	User32	

© 2026 Tanium Inc. All Rights Reserved

Reference: Event log data

The following commands are useful for retrieving XML schemas for events you might be interested in subscribing to. You can use the data in the content that is returned from each command to locate information such as the Event Source and Log Path to use when creating a new subscription. Run each line in a PowerShell terminal and substitute the Event IDs and providers you want to investigate.



Some of these commands require an elevated shell (Run As Administrator) to run.

```
# List all event providers
Get-WinEvent -ListProvider * | Format-Table

# List all policy-related event providers.
Get-WinEvent -ListProvider *policy* | Format-Table

# List the logs on the machine where the name is like 'policy'
Get-WinEvent -ListLog *policy*

# List all possible event IDs and descriptions for the provider
(Get-WinEvent -ListProvider Microsoft-Windows-GroupPolicy).Events |
   Format-Table id, description -AutoSize

# List all of the event log entries for the provider
Get-WinEvent -LogName Microsoft-Windows-GroupPolicy/Operational

# Each event in each provider has its own message data schema.
# Use this line to find the schema of each event ID.
# For a specific event
(Get-WinEvent -ListProvider Microsoft-Windows-GroupPolicy).Events |
   Where-Object {$_.Id -eq 5314}

# For a keyword in the event data
(Get-WinEvent -ListProvider Microsoft-Windows-GroupPolicy).Events |
   Where-Object {$_.Template -like "*reason*"}
```

© 2026 Tanium Inc. All Rights Reserved

```
# Find an event ID across all ETW providers:
Get-WinEvent -ListProvider * |
   ForEach-Object { $_.Events | Where-Object {$_.ID -eq 4168} }
```

An example of the data that is returned as a result of running a command:

```
PS C:\> (Get-WinEvent -ListProvider Microsoft-Windows-GroupPolicy).Events |
 Where-Object {$_.Id -eq 5314}


Id          : 5314
Version     : 0
LogLink     : System.Diagnostics.Eventing.Reader.EventLogLink
Level       : System.Diagnostics.Eventing.Reader.EventLevel
Opcode      : System.Diagnostics.Eventing.Reader.EventOpcode
Task        : System.Diagnostics.Eventing.Reader.EventTask
Keywords    : {}
Template    : <template
              xmlns="http://schemas.microsoft.com/win/2004/08/events">
              <data name="BandwidthInkbps" inType="win:UInt32"
                  outType="xs:unsignedInt"/>
              <data name="IsSlowLink" inType="win:Boolean"
                  outType="xs:boolean"/>
              <data name="ThresholdInkbps" inType="win:UInt32"
                  outType="xs:unsignedInt"/>
              <data name="PolicyApplicationMode" inType="win:UInt32"
                  outType="xs:unsignedInt"/>
              <data name="ErrorCode" inType="win:UInt32"
                  outType="win:HexInt32"/>
              <data name="LinkDescription" inType="win:UnicodeString"
                  outType="xs:string"/>
              </template>
```

© 2026 Tanium Inc. All Rights Reserved

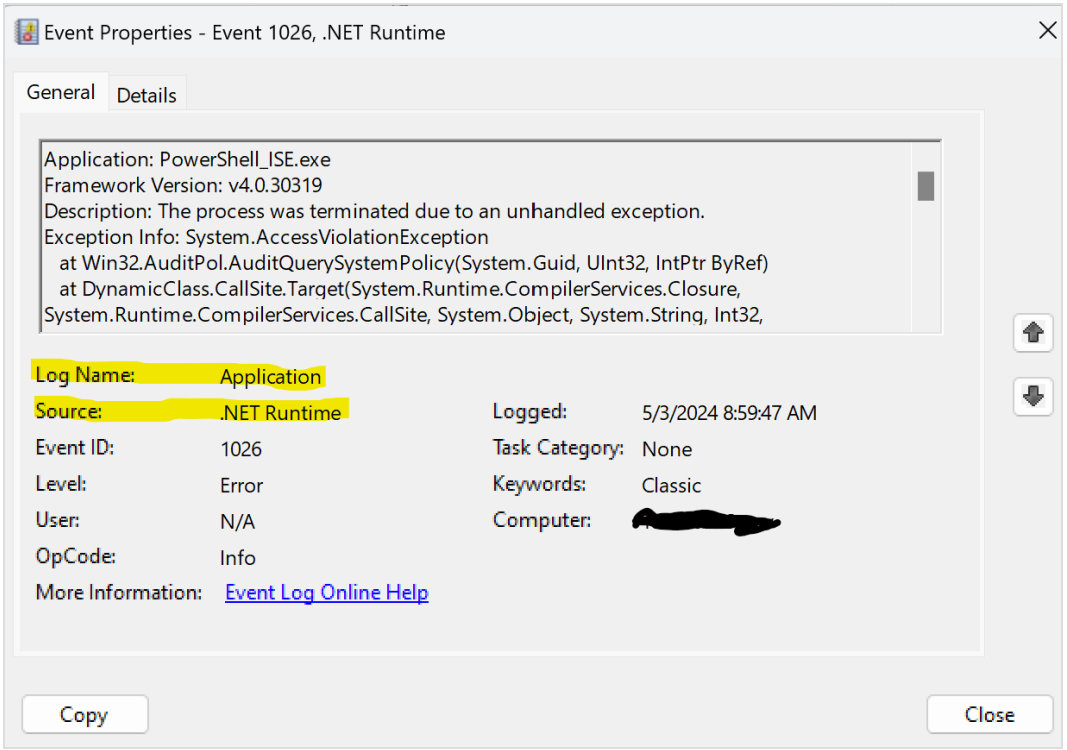
```
Description : A %6 link was detected. The Estimated bandwidth is %1 kbps. The
              slow link threshold is %3 kbps.
```

In the following example, "Name" in the output corresponds to the "Event Source" and the "LogLinks" corresponds to "Log Path" when creating a subscription.

```
PS C:\>Get-WinEvent -ListProvider *policy*


Name     : Microsoft-Windows-GroupPolicy
LogLinks : {System, Microsoft-Windows-GroupPolicy/Operational}
Opcodes  : {win:Start, win:Stop}
Tasks    : {}
```

Another way of identifying values you can use to create a new subscription is through the Windows Event Viewer. Locate an event and select it to view details.



© 2026 Tanium Inc. All Rights Reserved