Tanium Performance User Guide

2026H2 Semiannual Release

Version 1.31

November 19, 2026



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

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

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

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

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

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

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

Tanium welcomes customer input on making solutions accessible based on your Tanium modules and assistive technology requirements. Accessibility requirements are important to the Tanium customer community and we are

©2026 Tanium Inc. All Rights Reserved

committed to prioritizing these compliance efforts as part of our overall product roadmap. Tanium maintains transparency on our progress and milestones and welcomes any further questions or discussion around this work. Contact your sales representative, Tanium Support atsupport@tanium.com, or email accessibility@tanium.com to make further inquiries.

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

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

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

iOS, iPad, iPadOS, iPhone, Mac, and macOS are trademarks of Apple Inc., and registered in the U.S. and other countries and regions.

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

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

© 2026 Tanium Inc. All rights reserved.

Table of contents

Overview 9
- Profiles and events 9
- Event rules 10
- Performance scores 10
- Alerts 13
- Interoperability with other Tanium products 13

Gaining organizational effectiveness 15

Requirements 22
- Core platform dependencies 22
- Computer group dependencies 22
- Solution dependencies 23
  - Tanium recommended installation 23
  - Import specific solutions 23
  - Required dependencies 23
  - Feature-specific dependencies 24
- Client extensions and endpoint tools 24
- Endpoints 25
  - Supported operating systems 25
  - Disk space requirements 26
  - Processor and memory requirements 26
- Host and network security requirements 26
  - Ports 26
  - Security exclusions 28
    - Performance endpoint exclusions 28
- User role requirements 32

Installing 37
- Before you begin 37

©2026 Tanium Inc. All Rights Reserved

Import Performance with default settings 38
Default settings for Performance 38
Import Performance with custom settings 38
Manage solution dependencies 39
Upgrade Performance 39
Verify Performance version 39

Configuring 40
Install and configure Tanium Endpoint Configuration 40
Manage solution configurations with Tanium Endpoint Configuration 40
Configure Performance 42
Configure the Performance action group 42
Configure Profiles 42
(Optional) Install and configure Direct Connect 43
Set up Performance users 43

Managing profiles 46
Create a profile 46
Set the priority of profiles 50
Modify a profile 51
Delete a profile 52

Analyzing events 53
View the Events page 53
Targeted Endpoint Status 53
View all events 54
View CPU events 55
View memory events 57
View disk capacity events 59
View disk latency events 61
Input/output operations per second (IOPs) 62
View application crashes 63
View system crashes 65
View process network latency events 67
View network outage events 69
View WiFi signal events 70
View Boot Time events 71

©2026 Tanium Inc. All Rights Reserved

View Logon Time events 72
View endpoints with events 72
Customize the results 73
Connect directly to an endpoint 74
View in Tanium Interact 75

Connecting directly to endpoints 76
Create a direct connection 77
Browse and download files from the endpoint 78
Before you begin 78
Browse files 78
Download files 79
View the Live Process Monitor 79
Terminate a process on the endpoint 81
View boot and logon times 82
View endpoint information 83
Set the time frame for the data 84
View the charts 84
Events 85
CPU 86
Memory 87
Network 89
Disk 91
Process Diagnostics 93
Working with charts 94
Scope 94
Resolution 94
Events annotations 95

Monitoring performance scores 97
Before you begin 97
View the Performance Score dashboard 97
View performance scores by event 99
View performance scores by endpoint 100

Monitoring applications 102
Before you begin 102

©2026 Tanium Inc. All Rights Reserved

Configure application monitoring 102
View the monitoring applications dashboard 106
View metrics by application 108
Use report controls 109
Reference 111

Monitoring boot times 113
Boot sensors 113
Prerequisite 114
View the Boot Times dashboard 115

Monitoring logon times 117
Prerequisite 117
View the Logon Times dashboard 117

Monitoring Performance Trends 119

Managing Performance alerts 123
Before you begin 123
Manage alert monitors 124
View alert monitors 124
Silence or disable an alert monitor 126
Manage alerts 127
View alerts 127
Change the status of an alert 129
Export alert data to a Connect destination 129

Managing stream configurations 132
View stream configurations 132
Create a stream configuration 133
Edit a stream configuration 135
Delete a stream configuration 135

Maintaining 137
Perform monthly maintenance 137
Monitor and troubleshoot Performance Coverage 138
Monitor and troubleshoot endpoints with performance events 139

©2026 Tanium Inc. All Rights Reserved

Troubleshooting 141
Collect logs 141
Collect troubleshooting information from endpoints 141
Alerts are not triggering 142
Configuration issue 142
Service issue 143
Information flow overview 143
Sync alert data 143
Unable to configure Retention Settings 144
Error when connecting to endpoints 144
Remove Performance tools from endpoints 145
Verify endpoint tools 146
Uninstall Performance 146
Contact Tanium Support 147
Reference: Advanced Settings 148
Reference: Event Rules 151

©2026 Tanium Inc. All Rights Reserved

Performance overview

With Performance, you can monitor, investigate, and remediate performance issues on endpoints managed using Tanium™ Client.

Configure profiles to define events for specified computer groups. Define event rules to monitor critical metrics related to hardware resource consumption, application health, and system health.

Visualize the issues that have occurred across your environment and the commonalities between them on the **Events** page. Proactively resolving these issues can improve end-user productivity.

To troubleshoot an issue with a single endpoint, use Tanium™ Direct Connect. In Direct Connect, you can view live and historical process-level data from a single endpoint. Use this data to troubleshoot or understand the impact of software and hardware changes on performance.

Profiles and events

Profiles define events for specified computer groups. For each profile, you can select computer groups to monitor and rules that determine when an event occurs.

Events are generated when an endpoint experiences the conditions defined in an event rule in a profile.

When a profile targets an endpoint, tools are distributed to that endpoint to collect and monitor performance data. The tools collect data every 15 seconds. By default, the data is stored for 15 days, and you can change the retention period when you create or edit a profile. Performance queries this local data store when you analyze events.

For example, you might want to know when available memory falls below a certain threshold on specific endpoints. You can create a profile with an **Available Memory is less than 250 MB** event rule and set the target for that profile to a computer group you want to monitor. When you analyze events in Performance, memory events are reported if any endpoints that you are targeting had less than 250 MB of available memory during the time frame (scope) that you selected for analysis.

The **Events** page shows charts that provide a high-level overview of events in the environment. You can also see a list of the specific endpoints that experienced a particular event (such as low memory)

©2026 Tanium Inc. All Rights Reserved

to identify and investigate issues in your environment. For more information, see Analyzing events on page 53.

For each profile, you can add a stream configuration to stream selected event types to an external destination such as Splunk or ELK. For more information about how to create a stream configuration, see Managing stream configurations on page 132.

Event rules

Event rules determine what conditions cause targeted endpoints to report events. Performance includes these event rules:

- **CPU Critical**
- **Available Memory**
- **Disk Capacity**
- **Disk Latency**
- **Application Crashes**
- (Windows) **System Crashes**
- (Windows and macOS) **Process Network Latency**
- **Network Outage**
- (Windows and macOS) **WiFi Signal**
- (Windows) **Boot Time**
- (Windows) **Logon Time**

You can select heuristics for some event rules. For example, if you add the **Disk Latency** event rule, you can monitor **Read Latency** or **Write Latency**. If either heuristic is met, the event rule is triggered.

For more information, see Reference: Event Rules on page 151.

Performance scores

©2026 Tanium Inc. All Rights Reserved

Performance scores represent the health of the endpoints in your environment. Use performance scores to identify endpoints with performance issues and to investigate causes for lower-performing endpoints. You can then connect to individual endpoints through Tanium™ Direct Connect to troubleshoot issues. For each endpoint, Performance calculates a performance score based on the number of events that occur on the endpoint. Performance recalculates scores continuously based on data from the last 24 hours.

Note: Performance scores are driven by the number of performance-related events that occur on an endpoint. If an endpoint is idle and not actively in use, it might not generate new events, and its score remains unaffected.

Performance scores can help you to evaluate the employee experience by providing a comprehensive view of endpoint performance, which is a critical component of the digital employee experience. By monitoring the performance score over time, you can identify trends and patterns in endpoint performance, which enables you to proactively address issues before they become major problems. For example, if a performance score shows that there are frequent application crashes on a particular endpoint, you can investigate the root cause of the issue and take steps toward a resolution. By doing so, you can improve the digital employee experience and reduce the frustration and productivity loss associated with application crashes.

In addition, the performance score can help you evaluate the effectiveness of your technology investments and identify areas for improvement. For instance, if the performance score shows that endpoint performance is consistently low for a specific team or department, you can explore whether the employees in that area have the resources they need to do their jobs effectively.

Performance consolidates the performance scores for all endpoints so you can filter the scores by computer group.

Score calculation

A performance score is a percentage between 1 and 100 that represents the health of the endpoint. The higher the number, the healthier the endpoint. Performance scores are based on events, which are grouped into categories to match the rule types described in Event rules on page 10. Performance scores are weighted by event category.

©2026 Tanium Inc. All Rights Reserved

Default performance score weights by category

Event Category	Weight
CPU Critical	10%
Available Memory	10%
Disk Capacity	20%
Disk Latency	10%
Application Crashes	20%
System Crashes	30%
Process Network Latency	0%
Network Outage	0%
WiFi Signal	0%
Boot Time	0%
Logon Time	0%



Note: Performance score weights for **System Crashes**, **Boot Time**, and **Logon Time** are supported for Windows endpoints only. Performance score weights for **Process Network Latency**, **Network Outage**, and **WiFi Signal** are supported for Windows and macOS endpoints only.

The weighted values add up to 100%.

The score for each event category is calculated based on the number of events in the category.

```
Score = 100 / (1 + Events)
```

Performance calculates the performance score by adding the weighted category scores together:

```
Performance Score = (20% * Application Crashes score) +
                    (10% * Available Memory score) +
                    (10% * CPU Critical score) +
                    (20% * Disk Capacity score) +
                    (10% * Disk Latency score) +
```

©2026 Tanium Inc. All Rights Reserved

```
                    (30% * System Crashes score)
```


Tip: For each profile, you can set the weight of each event category to customize the performance score calculation to your organization's specific needs and priorities. For example, system crashes and application crashes can disrupt employee productivity, so you might consider weighting those two categories higher than the default weights. For more information, see Create a profile on page 46.

Performance score ranges

Icon	Description	Range
	Good	76% to 100%
	Fair	51% to 75%
	Poor	26% to 50%
	Very Poor	1% to 25%

The Performance **Overview** page includes a **Performance Score** section where you can view and manage visualizations of endpoint health.

For more information about viewing performance scores, see Monitoring performance scores on page 97.

Alerts

When you enable alerts for each event rule type in a profile configuration, Performance creates an alert monitor that detects when endpoints meet the alerting thresholds defined in the rule. Targeted endpoints that meet alert monitor thresholds generate alerts. You can view a specific alert on the **Alerts** page or from the alert monitor that triggered it.

For more information about alerts, see Managing Performance alerts on page 123.

Interoperability with other Tanium products

©2026 Tanium Inc. All Rights Reserved

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

Connect

Use Tanium™ Connect to export alert data to Connect destinations. For more information, see Export alert data to a Connect destination on page 129.

Criticality

The **Performance Overview** page contains a chart with **Average Endpoint Performance Score by Criticality**.

Direct Connect

Use Direct Connect to view live and historical data on endpoints to troubleshoot issues. For more information, see Connecting directly to endpoints on page 76.

Engage

Tanium™ Engage uses Performance metrics to monitor, measure, and improve the performance of end-user digital experiences. For more information, see Tanium Engage.

Gateway

Use Tanium™ Gateway to access the Performance API. For more information about what features are available through Gateway, see Tanium Gateway User Guide: Schema reference.

Investigate

Tanium™ Investigate displays Performance event data, including CPU, memory, network, disk, and IO metrics. From any performance event, you can view similar events in the Performance module. For more information, see Tanium Investigate.

Reporting

Performance contains dashboards and charts supplied by Tanium™ Reporting. For more information, see Monitoring performance scores on page 97 and Monitoring Performance Trends on page 119.

©2026 Tanium Inc. All Rights Reserved

Gaining organizational effectiveness with Performance

The four key organizational governance steps to maximizing the value that is delivered by Performance are as follows:

- Develop a dedicated change management process. For more information, see Change management on page 15.
- Define distinct roles and responsibilities. For more information, see RACI chart on page 16.
- Track operational maturity and operating metrics over time. For more information, see Operational metrics on page 17.
- Validate cross-functional alignment. For more information, see Organizational alignment on page 21.

Change management

Develop a tailored, dedicated change management process for endpoint performance monitoring activities, taking into account the new capabilities provided by Tanium.

- Create and integrate a Tanium-specific change management process with updated service-level agreements (SLAs) from identification to resolution of endpoint performance issues.
- Identify key resources in the organization to review and approve changes to endpoint performance requirements that ensure a minimal number of events per endpoint and align with an organizational-specific RACI chart.
- Align activities to key resources for Tanium-managed endpoint performance activities across IT Security, IT Operations, and IT Risk / Compliance.

©2026 Tanium Inc. All Rights Reserved

RACI chart

A RACI chart identifies the team or resource who is Responsible, Accountable, Consulted, and Informed, and serves as a guideline to describe the key activities across the security, risk/ compliance, and operations teams. Every organization has specific business processes and IT organization demands. The following table represents Tanium's point of view for how organizations should align functional resources against endpoint performance. Use the following table as a baseline example.

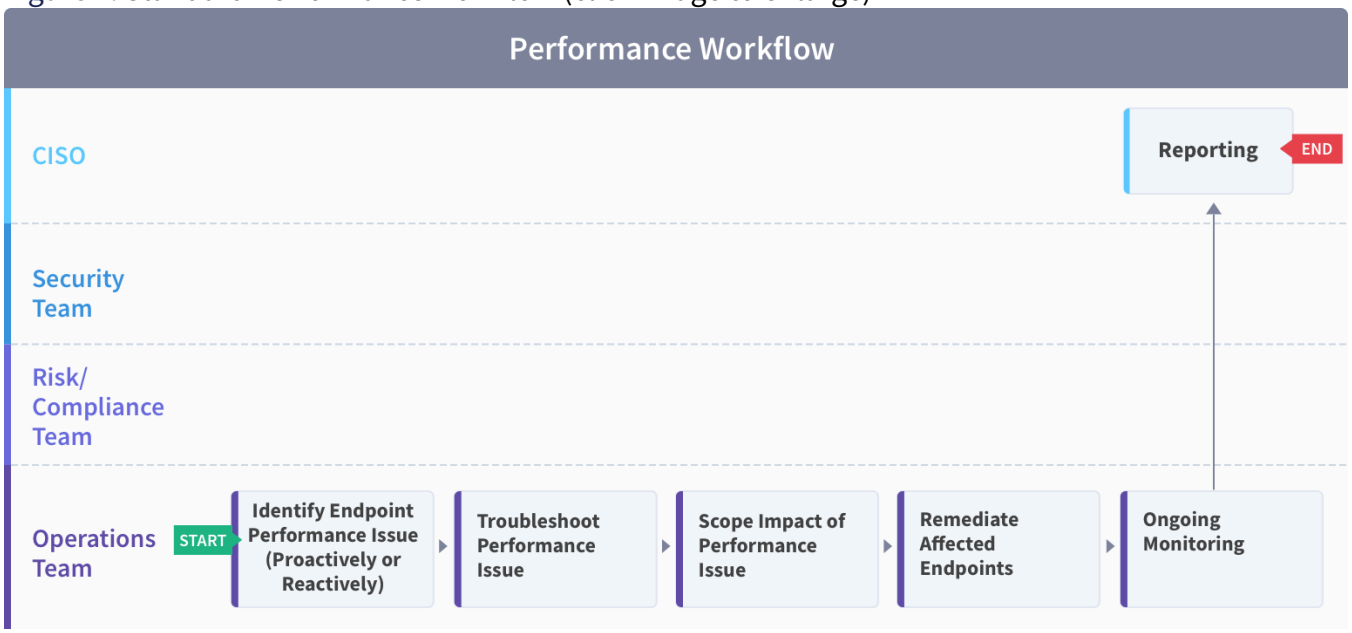
RACI chart for Tanium Performance

Task	IT Security	IT Operations	IT Risk/ Compliance	Executive	Rationale
Identify endpoint performance issue	-	R/A	-	-	The operations team is responsible for identifying endpoint performance issues.
Troubleshoot endpoint performance issue	C	R/A	-	-	The operations team troubleshoots endpoint performance issues and consults with the security team on the troubleshooting process.
Scope the impact of performance issue	C	R/A	-	-	The operations team scopes the impact of performance issues and consults with the IT Security team on the scoping process.
Remediate affected endpoints	C	R/A	-	-	The operations team remediates affected endpoints and consults with the security team on the remediation process.
Ongoing monitoring	I	R/A	-	I	The operations team monitors for endpoint performance issues and informs the executive and security teams of results.
Reporting	I	R	-	A	The operations team is responsible for reporting, and the executive team is accountable for the

©2026 Tanium Inc. All Rights Reserved

Task	IT Security	IT Operations	IT Risk/ Compliance	Executive	Rationale
					task. The security team is informed of all reports.

Figure 1. Standard Performance workflow (click image to enlarge)



Operational metrics

Performance maturity

Managing an endpoint performance program successfully includes operationalization of the technology and measuring success through key benchmarking metrics. The four key processes to measure and guide operational maturity of your Tanium Performance program are as follows:

Processes to measure Tanium Performance maturity

Process	Description
Usage	how and when Tanium Performance is used in your organization; for example, is Performance the only tool or is it a supplemental tool for another legacy tool
Automation	how automated Tanium Performance is, and how well is it used in the automation of other systems

©2026 Tanium Inc. All Rights Reserved

Process	Description
Functional Integration	how integrated Tanium Performance is, across security, operations, and risk/compliance teams
Reporting	how data from Tanium Performance is consumed by people and systems within the organization

Benchmark metrics

In addition to the key endpoint performance monitoring processes, the key benchmark metrics that align to the operational maturity of the Tanium Performance program to achieve maximum value and success are as follows:

Benchmark metrics for Tanium Performance maturity

Executive Metrics	Performance Coverage	Endpoints with Critical Performance Events in the Past Day
Description	Returns the number of endpoints in each of these categories: • **Initializing**: Endpoints where Performance tools are installing • **Optimal**: Endpoints where Performance is operational • **Needs attention**: Endpoints that do not have the Performance tools installed, are not targeted by a profile, or do not have a supported version of the Tanium Client installed • **Unsupported**: Endpoints with an operating system version that is not supported by Performance For more information about how to investigate endpoints that are categorized as **Needs Attention** or **Unsupported**, see Monitor and troubleshoot Performance Coverage on page 138.	The percentage of endpoints with a critical performance event in the last 24 hours. Critical performance events include system crashes, low disk capacity, and application crashes.

©2026 Tanium Inc. All Rights Reserved

Executive Metrics	Performance Coverage	Endpoints with Critical Performance Events in the Past Day
	For more information about operating system and Tanium Client versions supported by Performance, see Performance requirements on page 22 .	
Instrumentation	Uses the `Performance - Coverage Status` sensor to determine the endpoints where Performance is optimal, needs attention, and is unsupported.	The number of endpoints that had a critical performance event in the past day divided by the total number of endpoints that are managed by Performance.
Why this metric matters	If Performance is not running on all of your endpoints, you do not have visibility into what problems they are having, which risks more downtime and less productivity for critical systems and end users.	Teams should minimize the number of performance problems that users experience. With this metric, you can get a complete view of end user experience by looking at both the fraction of endpoints experiencing performance problems and how many problems each of these endpoints experience.

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

Maturity levels for Tanium Performance

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
Process	Usage	Performance configured	Performance used by exception to troubleshoot issues with individual endpoints	Performance used to troubleshoot issues with individual endpoints	Performance used to proactively and reactively troubleshoot issues; data from Performance occasionally drives strategic decisions and identifies cost efficiencies	Performance used to proactively and reactively troubleshoot issues; data from Performance often drives strategic decisions and identifies cost efficiencies

©2026 Tanium Inc. All Rights Reserved

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
	Automation	Manual	Manual	Manual	Partial automation to resolve end user problems on an ongoing basis	Partial automation to resolve end user problems on an ongoing basis
	Functional integration	Functionally siloed	Occasionally consult with other teams to troubleshoot tickets	Multiple teams getting value from Performance data	Team uses Performance to troubleshoot and report on end user experience; Performance integrated with ITSM or Business Analytics tools	Multiple teams use Performance to troubleshoot and report on end user experience; Performance integrated with ITSM or Business Analytics tools
	Reporting	Manual; Reporting for Operators only	Manual; Reporting for Operators only and peer group	Automated; Reporting for Operators and peer group only	Automated; Reporting tailored to stakeholders from IT Help Desk, End User Computing, and Operational Leadership teams	Automated; Reporting tailored to stakeholders from IT Help Desk, End User Computing, and Operational Leadership teams
Metrics	Performance Coverage (for Manageable Endpoints)	0-69%	70-79%	80-89%	90-99%	100%
	Percent of Endpoints with Events in the Past	>40%	31-40%	21-30%	10-20%	0-9%

©2026 Tanium Inc. All Rights Reserved

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
	Day					

Organizational alignment

Successful organizations use Tanium across functional silos as a common platform for high-fidelity endpoint data and unified endpoint management. Tanium provides a common data schema that enables security, operations, and risk/compliance teams to assure that they are acting on a common set of facts that are delivered by a unified platform.

In the absence of cross-functional alignment, functional silos often spend time and effort in litigating data quality instead of making decisions to improve endpoint performance monitoring processes.

©2026 Tanium Inc. All Rights Reserved

Performance requirements

Review the requirements before you install and use Performance.

Core platform dependencies

Make sure that your environment meets the following requirements:

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

  Any supported version of Tanium Client. For more information, see 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.

  > **Note:**
  >
  > - Network Outage Events require Tanium Client 7.6.2 or later.
  > - Client registration failures require Tanium Client 7.6.2 or later.

  For more information about supported endpoint operating systems, see Endpoints on page 25.

Computer group dependencies

When you first sign in to Tanium Console after a fresh installation of Tanium Server, the server automatically imports the `All Computers` computers group, which Performance requires.

©2026 Tanium Inc. All Rights Reserved

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

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

Tanium recommended installation

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

Import specific solutions

If you select only Performance to import, the Tanium Server automatically imports the latest available versions of any required dependencies that are missing. If some required dependencies are already imported but their versions are earlier than the minimum required for Performance, the server automatically updates those dependencies to the latest available versions.

Required dependencies

Performance has the following required dependencies:

- Tanium™ Console
- Tanium™ Core Content

©2026 Tanium Inc. All Rights Reserved

        - Core Content requires Tanium™ Client Management. For more information, see Tanium Client Management dependencies.

- Tanium™ Criticality
- Tanium™ Data Service (TDS)
- Tanium™ Direct Connect is required for live endpoint connections
- Tanium™ Endpoint Configuration
- Tanium™ Interact
- Tanium™ RDB Service
- Tanium™ Reporting
- Tanium™ Secrets

Feature-specific dependencies

If you select only Performance to import, you must manually import or update its feature-specific dependencies regardless of Tanium Console or Tanium Core Platform versions.

Performance has the following feature-specific dependencies:

- Tanium™ Findings is required for alert monitors.
- Tanium™ Message Bus is required for alter monitors.
- Tanium™ Connect is required to export alert events.

Client extensions and endpoint tools

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

©2026 Tanium Inc. All Rights Reserved

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

Endpoints

Supported operating systems

The following endpoint operating systems are supported with Performance.

Supported operating systems for Tanium Performance

Operating System	Version	Notes
Windows	• Windows 10 and later • Windows Server 2016 and later	
macOS	macOS 11 Big Sur and later	To collect **Process Network Latency**, **Network Outage: Internet Connection**, and **WiFi Signal** events, the macOS endpoint must meet the following minimum requirements: • Toolset version 2.13
Linux	• Red Hat Enterprise Linux (RHEL) 7.x, 8.x, 9.x • CentOS 7.x, 8.x • Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS • Amazon Linux 2 LTS • AlmaLinux 8.x • Rocky Linux 8.x	• Only POSIX-compliant file systems are supported. • In order for Linux systems to show interrupt time in Performance, IRQ reporting must be enabled in the kernel. Otherwise, interrupt time will always display as 0. For more information, see linux-hiding-interrupt-cpu-usage.

©2026 Tanium Inc. All Rights Reserved

Support for specific metrics varies by operating system. For more information, see Reference: Event Rules on page 151.

Disk space requirements

Performance requires 100 MB plus the amount specified in the Database Maximum Size parameter (1 GB by default).

> **Note:** The Performance database collects approximately 45 MB per day for busy servers and 25-35 MB per day for workstations.

Processor and memory requirements

Same as the Tanium Client. For more information about detailed requirements, 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 Performance.

Ports

The following ports are required for Performance communication.

Ports for Tanium Performance communication

Source	Destination	Port	Protocol	Purpose
Tanium Client (internal)	Module Server	17475	TCP	Used by the Module Server for endpoint connections to internal clients.
Tanium Client (external)	Zone Server [1]	17486	TCP	Used by the Zone Server for endpoint connections to external clients. The default port number is `17486`. If needed, you can specify a different port number when you configure the Zone

©2026 Tanium Inc. All Rights Reserved

Source	Destination	Port	Protocol	Purpose
				Proxy.
	Splunk or ELK (Required for Stream configurations to Splunk or ELK destinations)	Provided by a Splunk or ELK administrator	TCP	Stream event information from clients to an external destination.
Module Server	Zone Server [1]	17487	TCP	Used by the Zone Server for Module Server connections. The default port number is `17487`. If needed, you can specify a different port number when you configure the Zone Proxy.
		17488	TCP	Allows communication between the Zone Server and the Module Server. On TanOS, the Direct Connect Zone Proxy installer automatically opens port `17488` on the Zone Server. This port must be manually opened on Windows.
	Module Server (loopback)	17471	TCP	Internal purposes; not externally accessible
	External destination	80, 443	TCP	Integration of stream destinations

[1] These ports are required only when you use a Zone Server.

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

For more information about Tanium™ Cloud ports, see Tanium Cloud User Guide: Host and network security requirements.

For more information about Direct Connect ports, see Direct Connect User Guide: Host and network security requirements.

©2026 Tanium Inc. All Rights Reserved

Security exclusions

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

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

Note: If the required exclusions are not configured, or if Tanium suspects interference from AV or security software, Tanium might require you to remove or disable the AV or security software temporarily for the purposes of troubleshooting and restore it once troubleshooting is complete.

PERFORMANCE ENDPOINT EXCLUSIONS

Performance security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows (x86 and x64)		File	*<Tanium Client>* \TaniumClientExtensions.dll
		File	*<Tanium Client>* \TaniumClientExtensions.dll.sig
		File	*<Tanium Client>* \extensions\TaniumDEC.dll
		File	*<Tanium Client>* \extensions\TaniumDEC.dll.sig
		File	*<Tanium Client>* \extensions\TaniumPerformance.dll
		File	*<Tanium Client>* \extensions\TaniumPerformance.dll.sig

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	*<Tanium Client>* \Tools\PerformanceTSDB\TaniumTSDB.exe
		File	*<Tanium Client>* \extensions\TaniumTSDB.dll
		File	*<Tanium Client>* \extensions\TaniumTSDB.dll.sig
		File	*<Tanium Client>* \extensions\SupportCX.dll
		File	*<Tanium Client>* \extensions\SupportCX.dll.sig
		File	*<Tanium Client>* \extensions\TaniumConfig.dll
		File	*<Tanium Client>* \extensions\TaniumConfig.dll.sig
		File	*<Tanium Client>* \extensions\performance\data\performance.db
		File	*<Tanium Client>* \extensions\performance\data\performance.db-shm
		File	*<Tanium Client>* \extensions\performance\data\performance.db-wal
		Folder	*<Tanium Client>* \ProgramData\Tanium\PerformanceAutoLogger
		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
		Folder	C:\ProgramData\Tanium\PerformanceAutoLogger
Linux (x86 and x64)		File	*<Tanium Client>* /libTaniumClientExtensions.so
		File	*<Tanium Client>* /libTaniumClientExtensions.so.sig
		File	*<Tanium Client>* /extensions/libTaniumDEC.so

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	<*Tanium Client*> /extensions/libTaniumDEC.so.sig
		File	<*Tanium Client*> /extensions/libTaniumPerformance.so
		File	<*Tanium Client*> /extensions/libTaniumPerformance.so.sig
		Process	<*Tanium Client*> /Tools/PerformanceTSDB/TaniumTSDB
		File	<*Tanium Client*> /extensions/libTaniumTSDB.so
		File	<*Tanium Client*> /extensions/libTaniumTSDB.so.sig
		File	<*Tanium Client*> /extensions/libSupportCX.so
		File	<*Tanium Client*> /extensions/libSupportCX.so.sig
		File	<*Tanium Client*> /extensions/libTaniumConfig.so
		File	<*Tanium Client*> /extensions/libTaniumConfig.so.sig
		File	<*Tanium Client*> /extensions/performance/data/performance.db
		File	<*Tanium Client*> /extensions/performance/data/performance.db-shm
		File	<*Tanium Client*> /extensions/performance/data/performance.db-wal
		Folder	<*Tanium Client*> /python312
		Process	<*Tanium Client*> /python312/bin/pybin
		Process	<*Tanium Client*> /python312/python
		Process	<*Tanium Client*> /TPython/TPython
		Folder	<*Tanium Client*> /TPython312
		Process	<*Tanium Client*> /TaniumCX
macOS		File	<*Tanium Client*> /libTaniumClientExtensions.dylib

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* /libTaniumClientExtensions.dylib.sig
		File	*<Tanium Client>* /extensions/libTaniumDEC.dylib
		File	*<Tanium Client>* /extensions/libTaniumDEC.dylib.so
		File	*<Tanium Client>* /extensions/libTaniumPerformance.dylib
		File	*<Tanium Client>* /extensions/libTaniumPerformance.dylib.sig
		Process	*<Tanium Client>* /Tools/PerformanceTSDB/TaniumTSDB
		File	*<Tanium Client>* /extensions/libTaniumTSDB.dylib
		File	*<Tanium Client>* /extensions/libTaniumTSDB.dylib.sig
		File	*<Tanium Client>* /extensions/libSupportCX.dylib
		File	*<Tanium Client>* /extensions/libSupportCX.dylib.sig
		File	*<Tanium Client>* /extensions/libTaniumConfig.dylib
		File	*<Tanium Client>* /extensions/libTaniumConfig.dylib.sig
		File	*<Tanium Client>* /extensions/performance/data/performance.db
		File	*<Tanium Client>* /extensions/performance/data/performance.db-shm
		File	*<Tanium Client>* /extensions/performance/data/performance.db-wal
		Folder	*<Tanium Client>* /python312
		Process	*<Tanium Client>* /python312/python
		Process	*<Tanium Client>* /python312/bin/pybin
		Process	*<Tanium Client>* /TPython/TPython
		Folder	*<Tanium Client>* /TPython312

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	*<Tanium Client>* /TaniumCX

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

User role requirements

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

- solution permissions on page 33
- administration and platform content permissions on page 35: The solution permissions automatically provide some of these permissions.

For more information about predefined roles, see Set up Performance users on page 43.

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

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



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

©2026 Tanium Inc. All Rights Reserved

Performance solution permissions

Permission	Performance Administrator [1]	Performance Operator [1]	Performance User [1]	Performance Read Only User [1]	Performance Endpoint Configuration Approver [1]
Performance ADMINISTER: View all pages in Performance. Update settings and all profiles; can generate and retrieve a support bundle SHOW: View the Performance workbench	✓ ADMINISTER SHOW	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW
Performance Alerts READ: View alerts WRITE: Modify alerts	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Performance Application Monitoring READ: View application monitoring WRITE: Modify application monitoring	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗
Performance Direct Connect Connect to an endpoint using Direct Connect and read data from that endpoint.	✓ READ	✓ READ	✓ READ	✓ READ	✗
Performance Endpoint Configuration Allows approving endpoint configuration items	✗	✗	✗	✗	✓ APPROVE

©2026 Tanium Inc. All Rights Reserved

Permission	Performance Administrator [1]	Performance Operator [1]	Performance User [1]	Performance Read Only User [1]	Performance Endpoint Configuration Approver [1]
Performance Event View Performance events	✓ READ	✓ READ	✓ READ	✓ READ	✗
Performance File Browse the file system and download a file from an endpoint that you connect to through Performance	✓ DOWNLOAD	✓ DOWNLOAD	✓ DOWNLOAD	✗	✗
Performance Kill Terminate endpoint processes when you connect to an endpoint through Performance	✓ PROCESS	✓ PROCESS	✓ PROCESS	✗	✗
Performance Process Groups READ: View Performance process groups WRITE: Modify Performance process groups	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗
Performance Profile READ: View all Performance profiles WRITE: Modify all Performance profiles	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✓ READ
Performance Settings View Performance settings	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ

©2026 Tanium Inc. All Rights Reserved

Permission	Performance Administrator [1]	Performance Operator [1]	Performance User [1]	Performance Read Only User [1]	Performance Endpoint Configuration Approver [1]
	WRITE	WRITE			
Performance Stream READ: View stream configurations WRITE: Create and modify stream configurations	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✓ READ

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

Performance administration and platform content permissions

Permission	Permission Type	Performance Administrator	Performance Operator	Performance User	Performance Read Only User	Performance Endpoint Configuration Approver
Action Group	Administration	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ
User	Administration	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ
Action	Platform content	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✗
Bypass Action Approval	Platform content	✓ SPECIAL	✓ SPECIAL	✗	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Permission Type	Performance Administrator	Performance Operator	Performance User	Performance Read Only User	Performance Endpoint Configuration Approver
Filter Group	Platform content	READ	READ	READ	READ	READ
Own Action	Platform content	READ	READ	READ	READ	
Package	Platform content	READ WRITE	READ WRITE	READ	READ	
Plugin	Platform content	READ EXECUTE	READ EXECUTE	READ EXECUTE	READ EXECUTE	READ EXECUTE
Saved Question	Platform content	READ	READ	READ	READ	
Sensor	Platform content	READ	READ	READ	READ	READ

To view the content sets to which the platform content permissions apply, see View effective role permissions .

©2026 Tanium Inc. All Rights Reserved

Installing Performance

About this task

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

- Automatic configuration with default settings: Performance 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 Performance, see Import Performance with default settings on page 38.
- Manual configuration with custom settings: After installing Performance, you must manually configure required settings. Select this option only if Performance requires settings that differ from the recommended default settings. For more information, see Import Performance with custom settings on page 38.



Best Practice: Use the **Automatic configuration with default settings** option.

Before you begin

- Read the release notes.
- Review the Performance requirements on page 22.
- For more information about upgrading from a previous version, see Upgrade Performance on page 39.
- Assign the correct roles to users for Performance. Review the User role requirements on page 32.
    - To import the Performance solution, you must be assigned the Administrator reserved role.

©2026 Tanium Inc. All Rights Reserved

- To configure the Performance action group, you must be assigned the Administrator reserved role, Content Administrator reserved role, or a role that has the **Action Group write** permission.

Import Performance with default settings

About this task

You can set the Performance action group to target the **No Computers** filter group by enabling restricted targeting before importing Performance. This option enables you to control Performance tools deployment through scheduled actions that are created during the import and that target the Performance action group. For example, you might want to test Performance tools on a subset of endpoints before deploying the Performance tools to all endpoints. In this case, you can manually deploy the Performance 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.

For more information about how to import Performance 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 Performance version.

Default settings for Performance

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

Default settings for Tanium Performance

Setting	Default value
Action group	• Restricted targeting disabled (default): `All Computers` • Restricted targeting enabled: `No Computers` computer group.
Profiles	A profile is created with the default event rule configuration that targets `All Computers`.

Import Performance with custom settings

About this task

©2026 Tanium Inc. All Rights Reserved

To import Performance 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 Performance version.

For more information about how to configure the Performance action group, see Configure the Performance action group on page 42.

For more information about how to configure a profile, see Configure Profiles on page 42.

(Optional) For more information about how to install and configure Direct Connect, see (Optional) Install and configure Direct Connect on page 43.

Manage solution dependencies

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

Upgrade Performance

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



Note: You can configure **Retention Settings** to specify the **Database maximum size** and **Database maximum days** in profiles. If you do not see these settings in an existing profile, edit the profile to specify the **Retention Settings** and then save the profile.

Verify Performance version

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

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

©2026 Tanium Inc. All Rights Reserved

Configuring Performance

About this task

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

Install and configure Tanium Endpoint Configuration

About this task

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.

©2026 Tanium Inc. All Rights Reserved

Important:

When you upgrade Performance, the change management feature enables you to perform a staged rollout of the endpoint tools associated with the new version of Performance. Performance 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 Performance 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 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 Performance, see User role requirements. For more information about how to enable and use configuration approvals in Endpoint Configuration, see Managing approvals.

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

©2026 Tanium Inc. All Rights Reserved

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

Configure Performance

Configure the Performance action group

About this task

Importing the Performance 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 Performance, the action group targets `No Computers`.

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

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

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

Important: Only endpoints that are members of the Performance action group can be targets of profiles because the necessary tools are distributed exclusively to endpoints in this action group. Metric collection begins when these tools and profiles are installed on an endpoint.

1. From the Main menu, go to **Administration** > **Actions** > **Action Groups**.
2. Click **Tanium Performance**.
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.

Configure Profiles

About this task

©2026 Tanium Inc. All Rights Reserved

Profiles define performance events for specified computer groups.

1. From the Main menu, go to **Modules** > **Performance > Management** > **Profiles**.
2. Create and prioritize profiles. For more information, see Managing profiles on page 46.

(Optional) Install and configure Direct Connect

About this task

If you want to connect directly to endpoints to see live and historical performance data, install and configure Direct Connect.

1. From the Main menu, go to **Administration** > **Configuration** > **Solutions**.
2. In the **Content** section, select **Direct Connect**, and click **Import Selected**.
3. Enter your password and click **OK**.
4. Configure Direct Connect. You must configure Direct Connect before you can connect to endpoints from Performance. For more information, see Direct Connect User Guide: Configuring Direct Connect.

Result

For more information about using Direct Connect with Performance, see Connecting directly to endpoints on page 76.

Set up Performance users

About this task

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

For more information about specific permissions for each role, see User role requirements on page 32.

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

©2026 Tanium Inc. All Rights Reserved

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

Performance Administrator

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

- Configure Performance service settings, including creating and editing profiles
- View Performance events
- Connect to an endpoint using Direct Connect and read data, kill processes, and download files from that endpoint
- Generate and view the Performance support bundle

Performance Operator

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

- Configure Performance service settings, including creating and editing profiles
- View Performance events
- Connect to an endpoint using Direct Connect and read data, kill processes, and download files from that endpoint

Performance User

Assign the **Performance User** role to users who analyze and remediate performance events on endpoints. This role can perform the following tasks:

- View Performance profiles and events
- Connect to an endpoint using Direct Connect and read data, kill processes, and download files from that endpoint

©2026 Tanium Inc. All Rights Reserved

Performance Read Only User

Assign the **Performance Read Only User** role to users who perform analysis of performance events on endpoints. This role has the same privileges as the **Performance User** role, except that users with this role cannot download files or kill processes on endpoints. This role can perform the following tasks:

- View Performance profiles and events
- Connect to an endpoint using Direct Connect and read data from that endpoint

Performance Endpoint Configuration Approver

Assign the **Performance Endpoint Configuration Approver** role to a user who approves or rejects Performance configuration items in Tanium Endpoint Configuration. This role can approve, reject, or dismiss changes that target endpoints where Performance is installed.



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

©2026 Tanium Inc. All Rights Reserved

Managing profiles

About this task

Profiles define events for targeted computer groups. For each profile, configure event rules and select the target computer groups to which the event rules apply.

Profiles and the event rules that they contain do not determine what data is collected on endpoints. The same data is monitored on all endpoints that a profile targets. Profiles determine which conditions on the endpoint generate a negative performance event.

For each profile, you can add a stream configuration to stream selected event types to an external destination such as Splunk or ELK. For more information about how to create a stream configuration, see Managing stream configurations on page 132.

Performance stores data locally on the endpoint in a time series database named TaniumTSDB. The **Database maximum size** parameter determines the maximum amount of space that the Performance database can use on the endpoint. To analyze the average disk space that this database uses on endpoints, review the **Performance Database Size** panel in the **Performance Trends** dashboard. For more information, see Monitoring Performance Trends on page 119.



Best Practice: Minimize the total number of profiles in your environment. For example, you might want to have two profiles: one for standard workstations and one for high-profile workstations because you want to set stricter thresholds for the heuristics on high-profile workstations. As a best practice, do not create multiple profiles with the same event rules and thresholds as a way to organize the endpoints that you are monitoring. Instead, on the **Events** page, you can filter results by computer groups to analyze the data.

Create a profile

1. From the Main menu, go to **Modules** > **Performance** > **Management** > **Profiles** and then click **Create Profile**.
2. In the **Details** section, specify the **Profile Name** and optional **Description**.

©2026 Tanium Inc. All Rights Reserved

3. In the **Target** section, select the computer groups to which the event rules in the profile apply.

   Best Practice: Ensure that the computer groups in your profiles cover all of your endpoints.

   Note: Manual computer groups are not supported. For more information, see Tanium Core Platform User Guide: Managing computer groups.

4. In the **Retention Settings** section, specify the **Database Maximum Size** and **Database Maximum Days**.
   These settings determine the maximum amount of space that the Performance database can use on the endpoint and the maximum number of days of historical data that can be stored on an endpoint.

   Note:

   - The data storage on the endpoint is limited by size or by time, whichever is reached first.
   - The database maximum size setting limits only the size of the metrics time-series database. Due to the overhead of tools and other supporting files, the total storage used will be slightly higher than this value.
   - The minimum allowed value for the **Database maximum size** is `100 MB` and the minimum allowed value for the **Database maximum days** is `1 day`. The default values are **1000 MB** and **15 days**.

   CAUTION: If you reduce the **Database Maximum Size** in an active profile, the database is wiped on endpoints where the amount of storage space used is already greater than the reduced retention size.

5. In the **Data Collection** section, select the datasets to collect:
   - The **Boot Time and Logon Time** option collects boot times and logon times on Windows endpoints. Endpoints must be restarted to begin reporting data. When this option is selected, the boot times and logon times are enabled and contain metrics. For more information, see Monitoring boot times on page 113 and Monitoring logon

©2026 Tanium Inc. All Rights Reserved

times on page 117.

- The **Application Crashes** and **System Crashes** options are selected by default. Clear an option to disable crash event collection for that crash type.

  Important: Targeted endpoints must run performance-cx 2.9.1153.0 or later to disable crash event collection.

6. In the **Event Rules** section, configure event rules and alerts. Each rule is evaluated separately.
   a. Configure the heuristics for each event rule. For more information, see Reference: Event Rules on page 151.

      Note:

      - All event rules are selected by default. Clear the selection for any event rules that you do not want to monitor.
      - If a rule or heuristic applies to a specific operating systems only, then the operating system icon (, ,) appears beside the setting.

   b. To enable alerts for an event rule, select **Enable Alerts** and update options as needed. View alerts from the **Alert Monitors** page. For more information, see Managing Performance alerts on page 123.
      You can create a grouped alert or individual alert. A grouped alert sends a single alert for all endpoints that meet the alert conditions. Create a grouped alert when you need to know when a percentage or a number of your endpoints meet an alert threshold. To remediate a grouped alert, you must log into the Tanium Console to view details about endpoints that are currently online and alerting.

      An individual alert sends information about each endpoint that meets the alert conditions. Create an individual alert when you need a detailed view of an endpoint to pinpoint its performance issues. Because the alert contains information about the endpoint, you can triage an individual alert with external tools, even if the endpoint is offline.

      The default threshold settings for alerts are a grouped alert with 5 triggered events on any one endpoint over a period of 1 hour.

©2026 Tanium Inc. All Rights Reserved

- If you want details about each endpoint that meets the alert criteria, select **Create an individual alert for each endpoint that has a finding**.

- If you want a minimum number of endpoints to meet the alert criteria, select **Create a grouped alert for all endpoints that have finding** > **Create grouped alert when a number of endpoints meets the criteria**, and update the options. Default threshold settings are 10 endpoints meeting the alert criteria within 2 hours.

- If you want a minimum percentage of endpoints to meet the alert criteria, select **Create a grouped alert for all endpoints that have finding** > **Create grouped alert when percentage of endpoints meets the criteria**, and update the options. Default threshold settings are 80% of endpoints meeting the alert criteria within 2 hours.

  The number of endpoints that contribute to a percentage threshold is calculated using the number of endpoints reporting into TDS with the associated profile. For more information, see Tanium Interact User Guide: Managing Tanium Data Service.

  Best Practice: For a small set of targeted endpoints, do not use the percentage option because you might end up meeting the alert threshold prematurely if some of the endpoints go offline. Instead, use the static number option.



Best Practice: When you first enable alerts, target high-value endpoints that you have critical concerns about rather than targeting all endpoints. For example, you might want to enable alerts to monitor disk space on web servers. If you target a substantial number of endpoints with low triggering thresholds, you might receive a high volume of alerts.

7. In the **Performance Score** section, you can set the weight of each event category to customize the performance score calculation to your organization's specific needs and priorities. For example, system crashes and applications crashes can disrupt employee productivity, so you might consider weighing those two categories higher than the default weights.
   - To use the default weights, select **Default Configuration.**
   - To customize the weights, select **Custom Configuration** and then update the

©2026 Tanium Inc. All Rights Reserved

weights as desired. The weights must add up to 100%.

When you set a **Custom Configuration**, the configuration determines the performance score for the endpoints that the profile targets.

> **Tip:** By default, the **Process Network Latency**, **Network Outage**, **WiFi Signal**, **Boot Time**, and **Logon Time** event categories are set to 0% because those categories do not apply to all operating systems. When you customize performance score weights, consider how you weigh each event category in your score based on the available operating systems in the target computer groups. For example, weighing a score heavily on events that are only produced on Windows machines, such as Boot Time and Logon Time, could skew a score comparison between Linux and macOS endpoints.

> **Note:** For information about performance scores, see Performance scores on page 10 and Monitoring performance scores on page 97.

8. In the **Stream** section, enable the **Stream Event Findings** option, select a stream configuration, and then select events to stream. For more information, see Managing stream configurations on page 132.

   > **Note:** Ongoing events are resent through stream every five minutes until the event duration is over.

9. When finished, click **Save**.

Result

When you save a profile, the changes are sent to Endpoint Configuration to distribute the profile to endpoints. The profiles should be distributed within an hour, and metric monitoring and collection begins after the profile is placed on an endpoint. Any events that occur on the targeted endpoints based on the configured profile appear on the **Events** page. For more information, see Analyzing events on page 53.

> **Note:** If you enabled configuration approvals in Endpoint Configuration, profile changes must be approved in Endpoint Configuration before they deploy to endpoints.

Set the priority of profiles

©2026 Tanium Inc. All Rights Reserved

About this task

All profiles are exclusive, meaning that only one profile can be in effect on an endpoint at a given time. If you target multiple profiles with the same event rules to a particular endpoint, Performance must resolve the conflict to decide which profile to apply.

If two or more profiles target an endpoint with the same event rules, only the highest priority profile is applied.

Set the prioritization of profiles to determine which profile is applied if a conflict exists. The **Profiles** page shows the current priority for each profile.

1. From the Main menu, go to **Modules** > **Performance > Management** > **Profiles** and then click **Prioritize Profiles**.

   Note: **Prioritize Profiles** is disabled until you have two or more profiles configured.

2. Drag and drop the profiles into the order that you want and then click **Prioritize**. The profile with the highest priority is at the top of the list.

Modify a profile

About this task

To modify profiles, you must either have the **Administrator** reserved role, or have a role with the **Performance Profile write** permission. Roles with this permission include **Performance Administrator** and **Performance Operator**.

1. From the Main menu, go to **Modules** > **Performance > Management** > **Profiles**.
2. Click the name of the profile that you want to edit and then click Edit Profile .
3. Modify the profile details, targeting, and retention settings.
4. Modify the event rules.
   a. Edit existing event rules and alerts as needed.
   b. To delete an event rule from the profile, clear the selection for the event rule.
   c. To add a previously deleted event rule to the profile, select the event rule.
5. Modify the Performance Score configuration options and then click **Save**.

©2026 Tanium Inc. All Rights Reserved

Result

Note: If you enabled configuration approvals in Endpoint Configuration, profile changes must be approved in Endpoint Configuration before they deploy to endpoints.

Delete a profile

About this task

To delete profiles, you must either have the **Administrator** reserved role, or have a role with the **Performance Profile write** permission. Roles with permission include **Performance Administrator** and **Performance Operator**.

1. From the Main menu, go to **Modules** > **Performance** > **Management** > **Profiles**.
2. Select one or more profiles that you want to delete and then click **Delete**.

Result

Endpoint Configuration is notified and removes the profile from the endpoint. For more information about Endpoint Configuration, see Manage solution configurations with Tanium Endpoint Configuration on page 40.

©2026 Tanium Inc. All Rights Reserved

Analyzing events

About this task

A targeted endpoint reports an event after experiencing the conditions that you defined in an event rule in a profile. The **Events** page provides charts that provide more information about events in your environment.

View the Events page

1. From the Main menu, go to **Modules** > **Performance > Events**.
2. Specify the computer group for which you want to see events in the **Define Computer Groups** field.
3. Select a time period for the events from the **Scope** menu. The default option is **Past Day**.
4. If you change the default values, click **Get Results**.

Result

The **Events** page shows only events that occurred on endpoints targeted by a profile during the specified **Scope**. If no events occurred during the specified scope, or no profile is configured to monitor for events of that type, the chart for that event type shows **No data to display**.

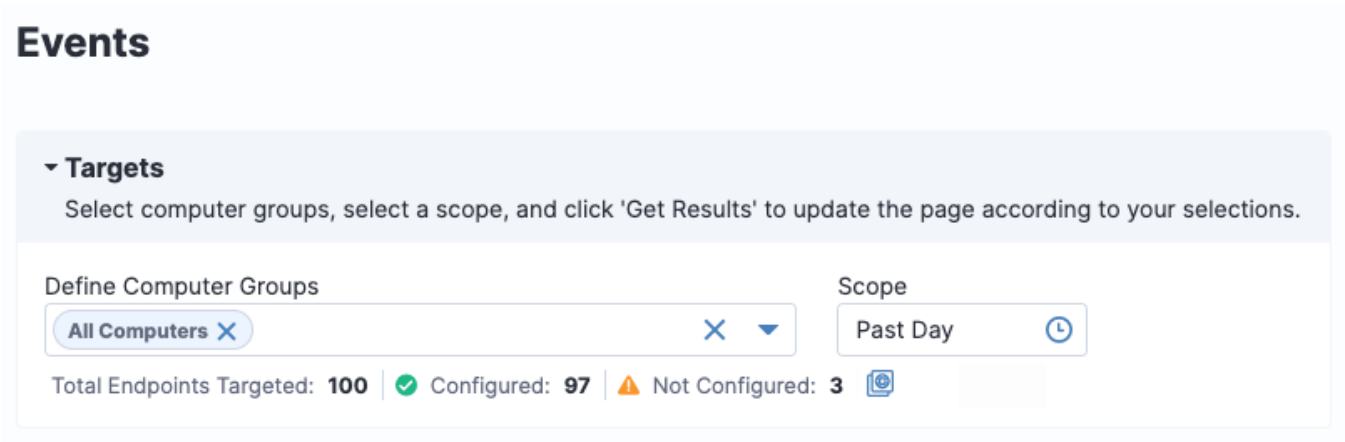
Targeted Endpoint Status

About this task

The **Targets** section shows a high-level overview of the current configuration status of targeted endpoints:

Figure 2. Targeted endpoint status

©2026 Tanium Inc. All Rights Reserved



Total Endpoints Targeted

The total number of endpoints that are currently targeted by a profile.

Configured

The total number of endpoints that have the necessary configuration in place for metric collection. They are targeted by a profile and the Performance tools are installed.

Not Configured

The total number of endpoints that do not have the necessary configuration in place for metric collection. They might not be targeted by a profile, or they might be missing the Performance tools.

Click View question results in Interact in this section to open the question results in Tanium™ Interact. From there, you can drill down into the results to determine which specific endpoints are missing the required configuration or profile.

View all events

About this task

Click the **All** tab in the charts section to show a chart with all reported events for the defined computer groups during the time frame that you selected in the **Scope** parameter. One chart shows a summary of the reported events:

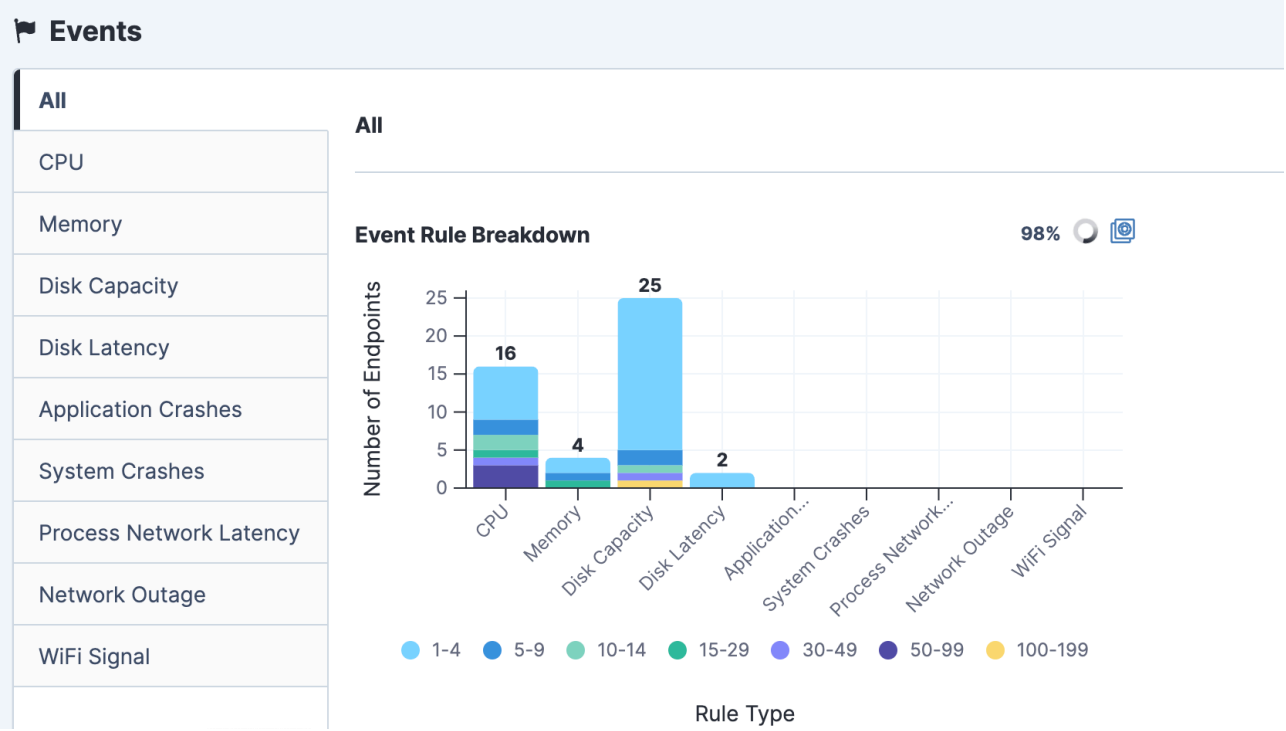
Event Rule Breakdown

The number of endpoints that reported each type of event: **CPU**, **Memory**, **Disk Capacity**, **Disk Latency**, **Application Crashes**, **System Crashes**, **Process Network Latency**, **Network Outage**,

©2026 Tanium Inc. All Rights Reserved

WiFi Signal. Each bar in the bar chart is color coded to indicate how many events of that type were reported by each endpoint. For example, the light blue portion of the bar indicates the number of endpoints that reported 1-4 events. Hover your mouse over the bar to see a breakdown of the number of events per endpoint. Click a bar in the chart to load the endpoints represented by that piece of the chart.

Figure 3. Event Rule Breakdown



View CPU events

About this task

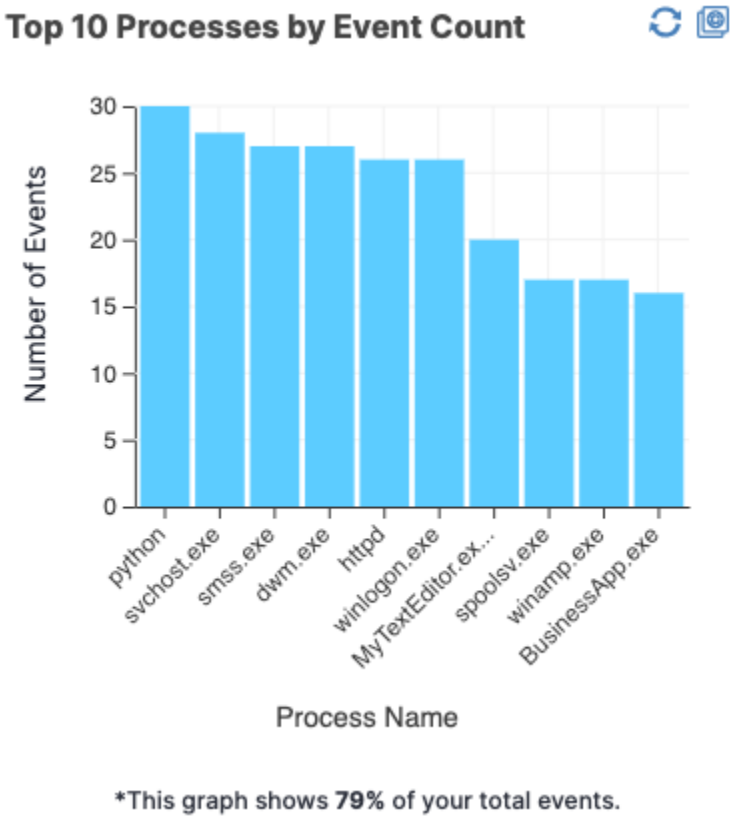
Click the **CPU** tab in the charts section to show charts that provide more information about endpoints in the defined computer groups that reported CPU events during the selected time frame. These charts are designed to help you find patterns and commonalities among the endpoints that are having issues in your environment. Two charts show a summary of the reported events:

Top 10 Processes by Event Count

This chart shows the top ten processes with the highest number of CPU events and the number of CPU events that are associated with each of those processes. The process that consumes the highest amount of CPU for the duration of the event is reported as the process associated with the event.

©2026 Tanium Inc. All Rights Reserved

Figure 4. Top 10 Processes by Event Count



Consider an example where you create an event rule in a profile to trigger an event if the CPU use is above 90% for longer than 10 minutes. The CPU on an endpoint that is targeted by that profile has CPU usage at 95% for an hour, which generates a performance event. The highest process consumer during that hour was badprocess.exe. Because badprocess.exe was the highest CPU consumer during that event, it is reported as the process that is associated with the event in the chart. If several endpoints are reporting events that are associated with badprocess.exe, you can investigate this process further. For example, perhaps a recent upgrade touched this process and the associated program needs to be tuned, or perhaps anti-virus software settings are not configured correctly.

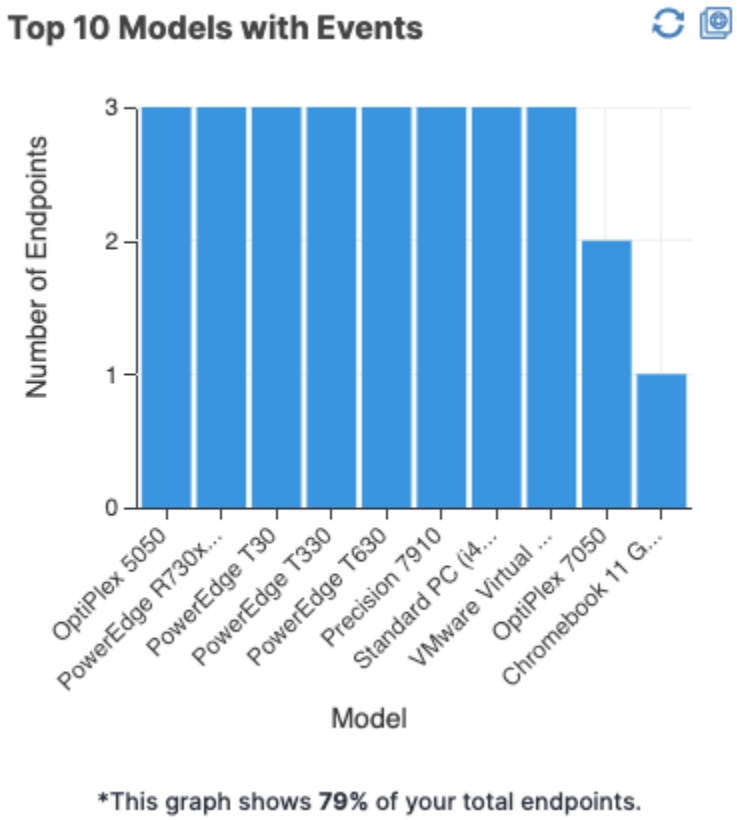
Top 10 Models with Events

This chart shows the top ten models with the highest number of reported CPU events and the number of endpoints with that model that reported a CPU event. An endpoint is counted only once in the charts, even if that endpoint reported more than one CPU event.

©2026 Tanium Inc. All Rights Reserved

Note: To see the full list of models that reported a CPU event, click View question results in Interact . From there, you see a list of all endpoints that reported a CPU event and filter by model.

Figure 5. Top 10 Models with Events



View memory events

About this task

Click the **Memory** tab in the charts section to show charts that provide more information about endpoints in the defined computer groups that reported memory events during the selected time frame. Two charts show a summary of the reported events:

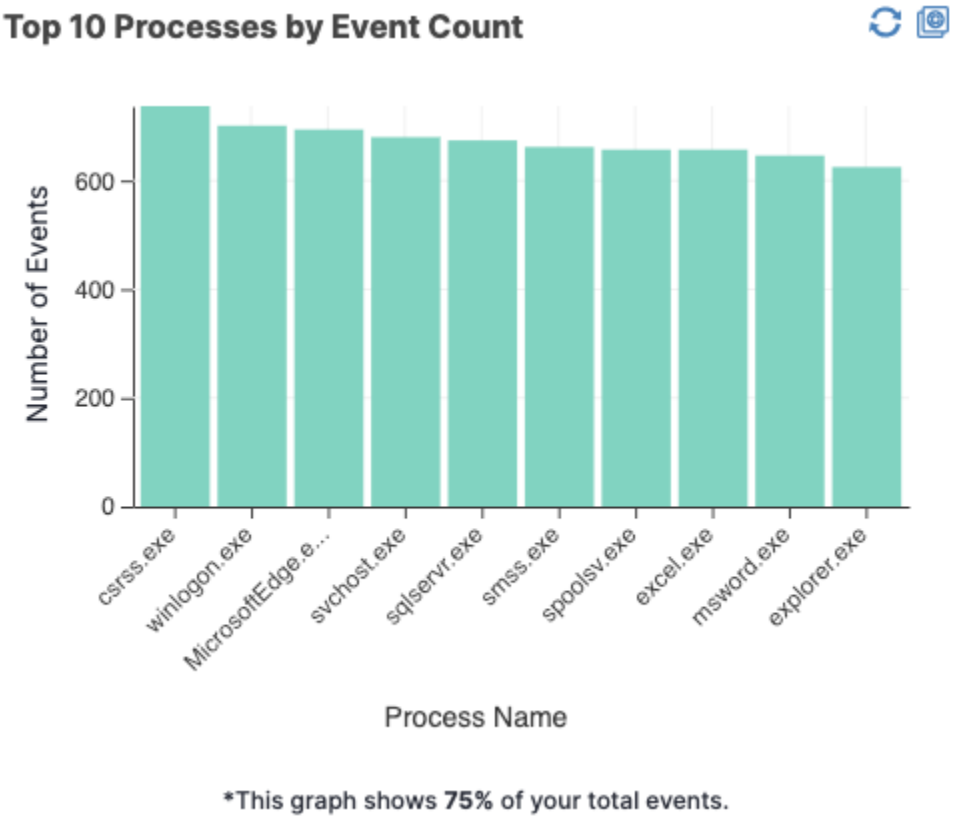
Top 10 Processes by Event Count

This chart shows the top ten processes with the highest number of memory events and the number of memory events that are associated with each of those processes. The process that consumes the highest amount of memory for the duration of the event is reported as the process

©2026 Tanium Inc. All Rights Reserved

associated with the event.

Figure 6. Top 10 Processes by Event Count



Consider an example where you create an event rule in a profile to trigger an event if the available memory is less than 50 MB for longer than 10 minutes. The memory on an endpoint that is targeted by that profile has only 40 MB of free memory for an hour, which generates a performance event. The highest memory consumer during that hour was badprocess2.exe. Because badprocess2.exe was the highest consumer of memory during that event, it is reported as the process that is associated with the event in the chart.

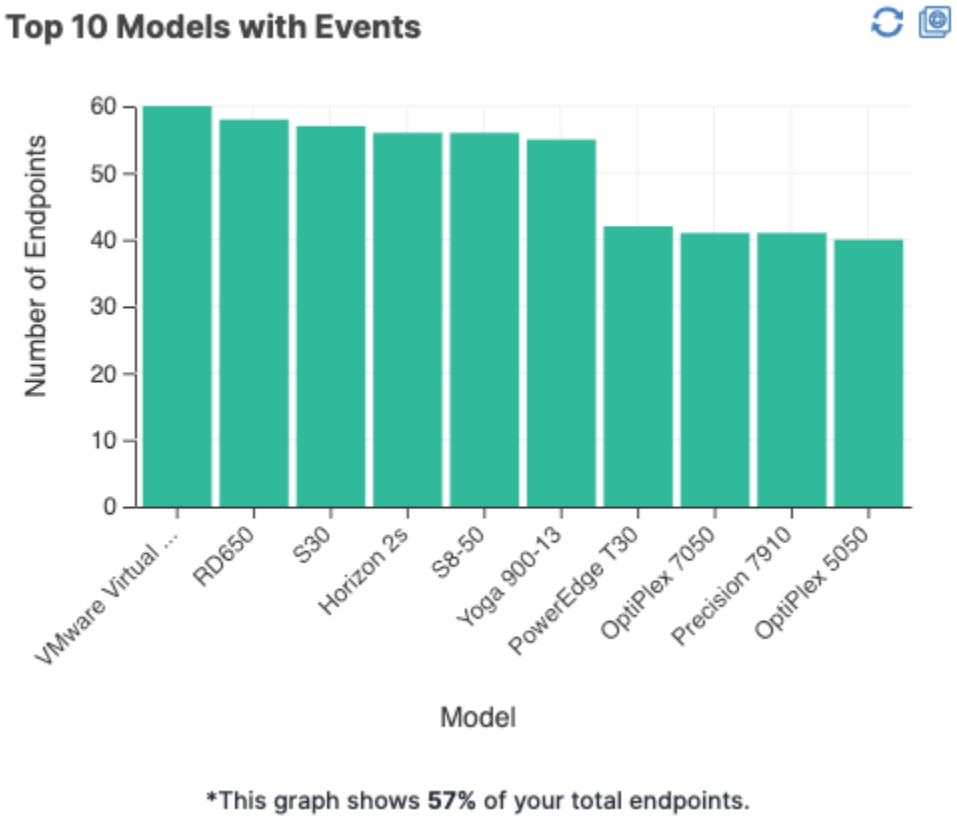
Top 10 Models with Events

This chart shows the top ten models with the highest number of reported memory events and the number of endpoints with that model that reported a memory event. An endpoint is counted only once in the charts, even if that endpoint reported more than one memory event.

©2026 Tanium Inc. All Rights Reserved

Note: To see the full list of models that reported a memory event, click View question results in Interact . From there, you see a list of all endpoints that reported a memory event and filter by model.

Figure 7. Top 10 Models with Events



Hover over a bar in the chart to see the exact number of endpoints with that model that reported an event. Click a bar in the chart to populate the results grid with the endpoints represented by that bar.

View disk capacity events

About this task

Click the **Disk Capacity** tab in the charts section to show a chart that provides more information about endpoints in the defined computer groups that reported disk capacity events during the selected time frame. An event is created when the free disk space on a logical drive is less than the specified threshold. One chart shows a summary of the reported events:

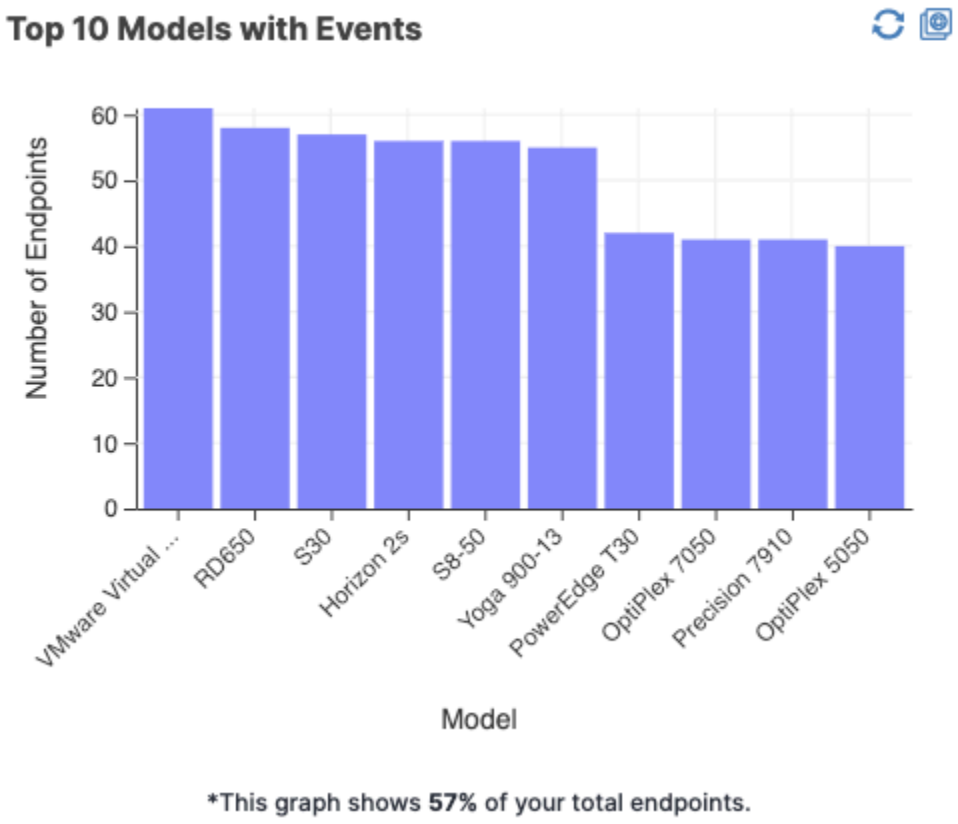
©2026 Tanium Inc. All Rights Reserved

Top 10 Models with Events

This chart shows the top ten models with the highest number of reported disk capacity events and the number of endpoints with that model that reported a disk capacity event. An endpoint is counted only once in the charts, even if that endpoint reported more than one disk capacity event.

Note: To see the full list of models that reported a disk capacity event, click View question results in Interact . From there, you see a list of all endpoints that reported a disk capacity event and filter by model.

Figure 8. Top 10 Models with Events



Hover over a bar in the chart to see the exact number of endpoints with that model that reported a disk capacity event. Click a bar in the chart to load the endpoints represented by that bar in the chart.

©2026 Tanium Inc. All Rights Reserved

View disk latency events

About this task

Click the **Disk Latency** tab in the charts section to show a chart that provides more information about endpoints in the defined computer groups that reported disk latency events during the selected time frame. An event is created when the average amount of time that an operation (read or write) takes to complete on a physical drive is greater than the specified threshold. One chart shows a summary of the reported events:

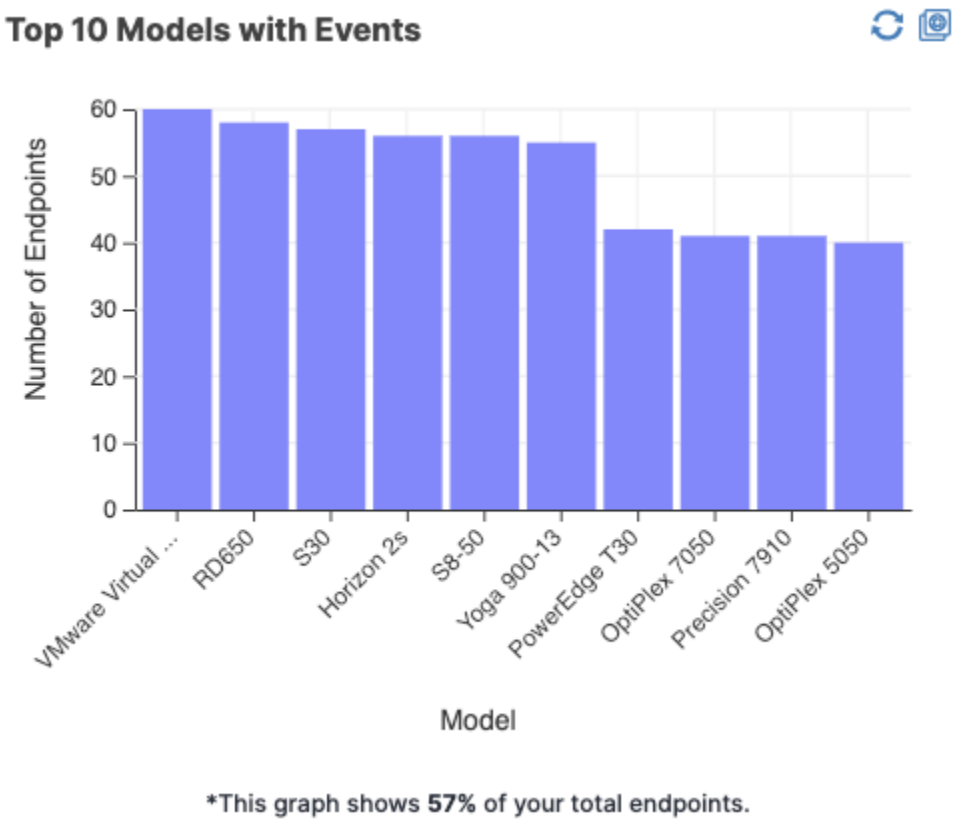
Top 10 Models with Events

This chart shows the top ten models with the highest number of reported disk latency events and the number of endpoints with that model that reported a disk latency event. An endpoint is counted only once in the charts, even if that endpoint reported more than one disk latency event.

Note: To see the full list of models that reported a disk latency event, click View question results in Interact . From there, you see a list of all endpoints that reported a disk latency event and filter by model.

Figure 9. Top 10 Models with Events

©2026 Tanium Inc. All Rights Reserved



Hover over a bar in the chart to see the exact number of endpoints with that model that reported a disk latency event. Click a bar in the chart to populate the results grid with the endpoints represented by that bar.

Input/output operations per second (IOPs)

IOPs is an industry measurement of the hardware throughput of a disk or a collection of disks. For example, a typical laptop with a 5400 RPM disk drive can deliver 80 IOPs. Assuming moderate levels of fragmentation, 80 IOPs equals about 50 MB of sustained disk performance.

An average response time longer than 15 ms is considered slow, and the response time becomes logarithmically slower as latency increases.

Typical IOPs by disk type

Storage	Max IOPs/MBps	Access Time
USB floppy drive	10 IOPs/0.25 MBps	500 ms

©2026 Tanium Inc. All Rights Reserved

Storage	Max IOPs/MBps	Access Time
5400 RPM hard disk	80 IOPs/50 MBps	15 ms
7200 RPM hard disk	100 IOPS/80 MBps	10 ms
15K RPM hard disk	200 IOPs/125 MBps	2.5 ms
SATA 6 based SSD	1000-5000 IOPs/500 MBps	.02 ms or 200 us
NMVe M.2	>= 80,000 IOPs/2-4 GBps	<= .0020 ms or 20 us

View application crashes

About this task

Click the **Application Crashes** tab in the charts section to show charts that provide more information about endpoints in the defined computer groups that reported application crashes during the selected time frame. Two charts show a summary of the reported events. Click a bar in either chart to populate the results grid with the endpoints represented by that bar.

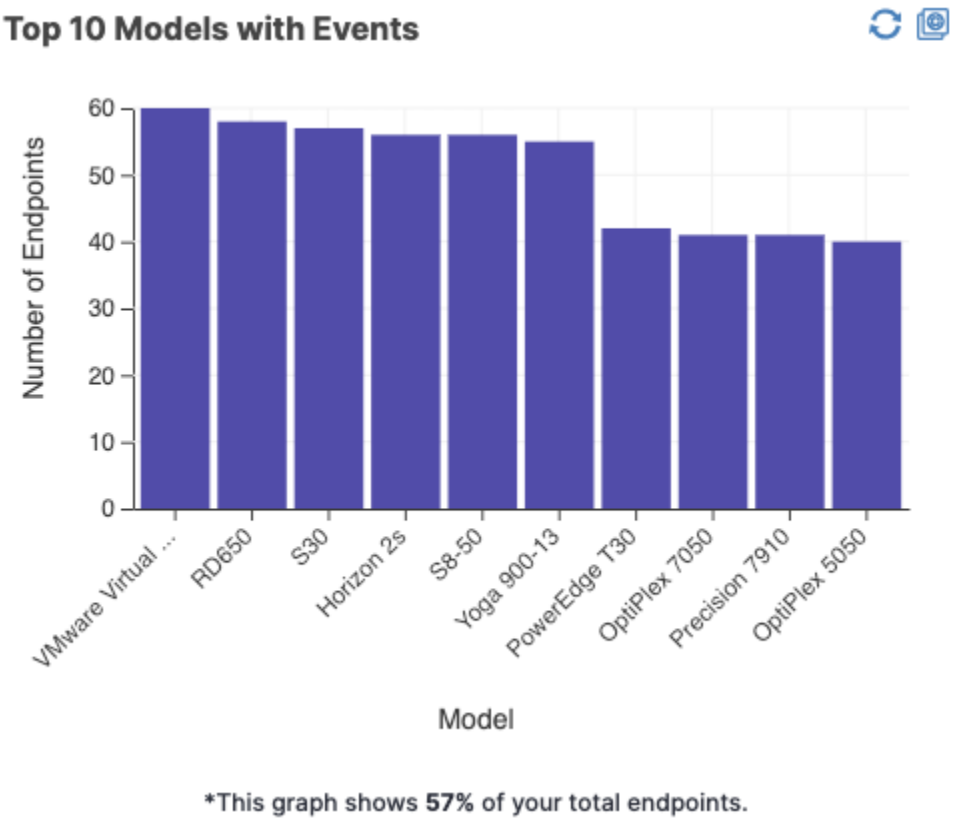
Top 10 Models with Events

This chart shows the top ten models with the highest number of reported application crashes and the number of endpoints with that model that reported an application crash.

Note: To see the full list of models that reported an application crash, click View question results in Interact . From there, you see a list of all endpoints that reported an application crash and filter by model.

Figure 10. Top 10 Models with Events

©2026 Tanium Inc. All Rights Reserved



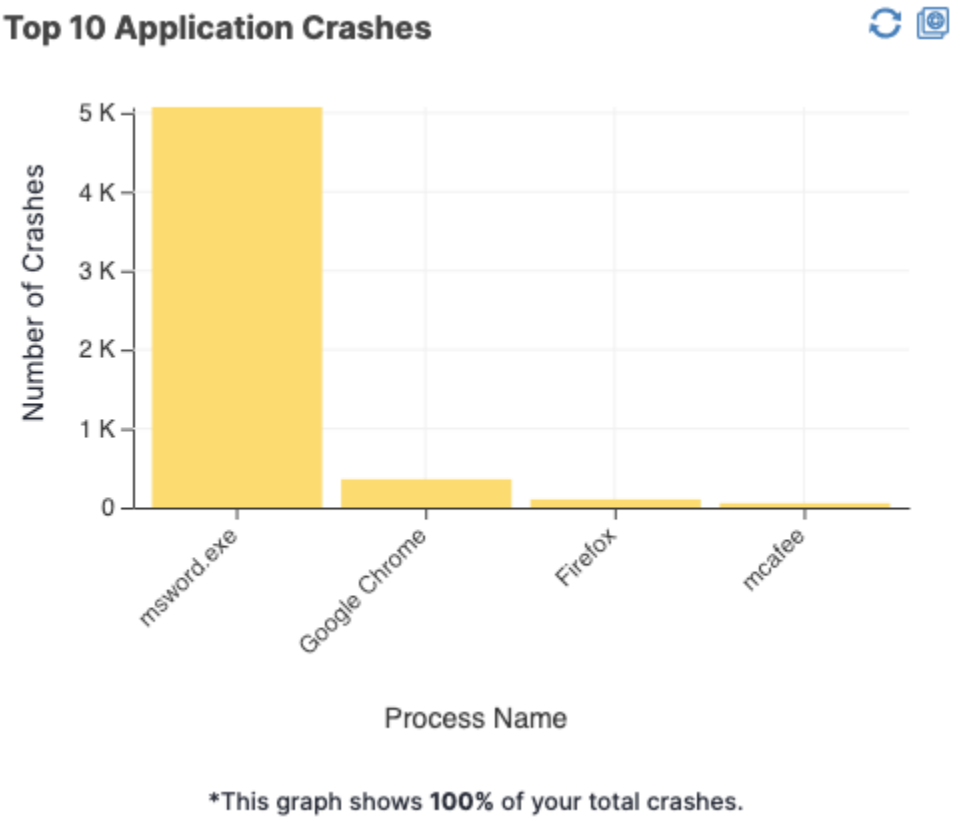
Hover over a bar in the chart to see the exact number of endpoints with that model that reported an application crash. Click a bar in the chart to populate the results grid with the endpoints represented by that bar.

Top 10 Application Crashes

This chart shows the top ten processes that caused a crash and the number of crashes that occurred due to each of those processes. Click a bar in the chart to populate the results grid with the endpoints represented by that bar.

Figure 11. Top 10 Application crashes

©2026 Tanium Inc. All Rights Reserved



View system crashes

About this task

Click the **System Crashes** tab in the charts section to show charts that provide more information about endpoints in the defined computer groups that reported system crashes during the selected time frame. Two charts show a summary of the reported events.

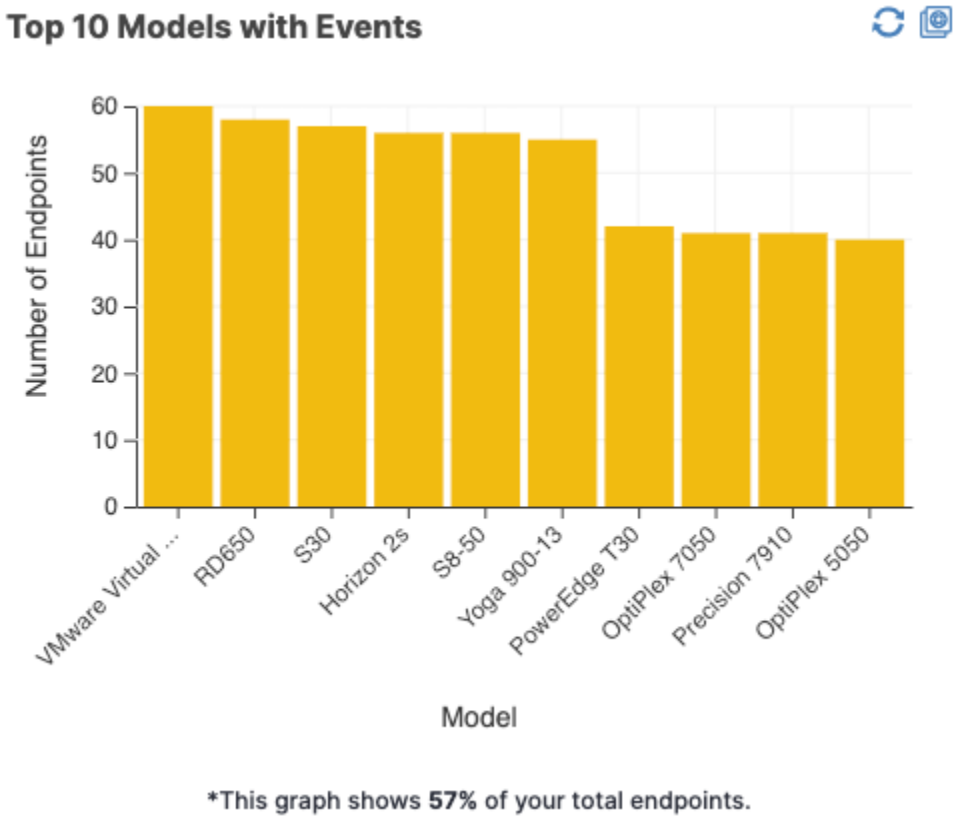
Top 10 Models with Events

This chart shows the top ten models with the highest number of reported system crashes and the number of endpoints with that model that reported a system crash.

Note: To see the full list of models that reported a system crash, click View question results in Interact . From there, you see a list of all endpoints that reported a system crash and filter by model.

Figure 12. Top 10 Models with Events

©2026 Tanium Inc. All Rights Reserved



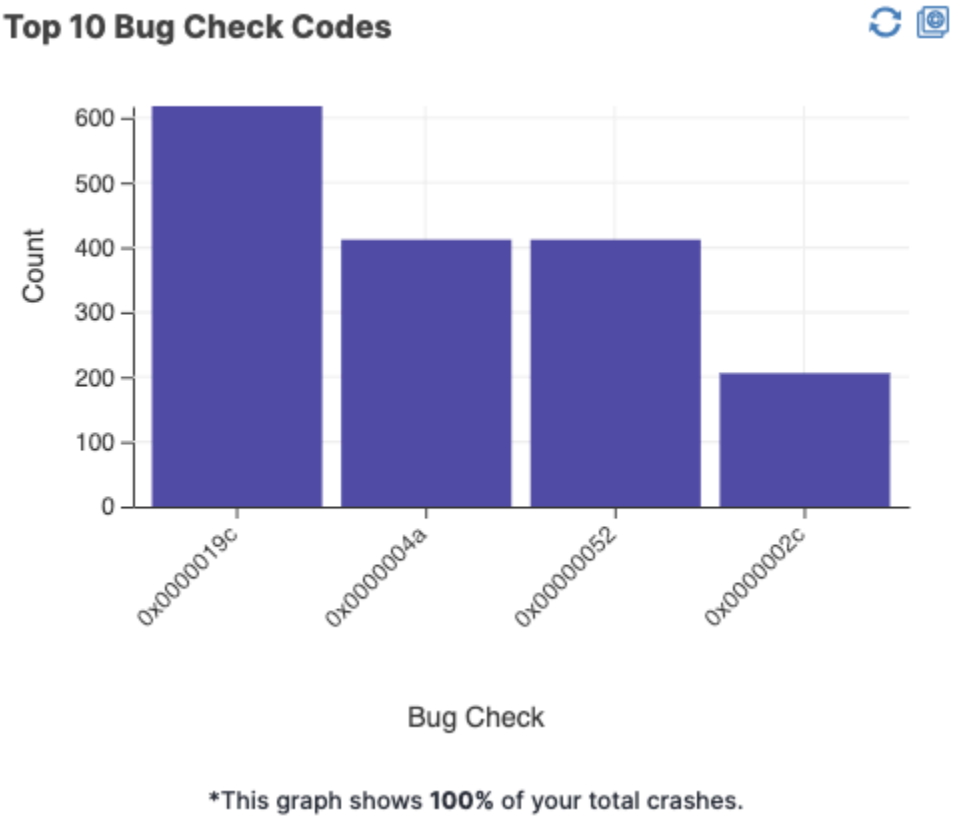
Hover over a bar in the chart to see the exact number of endpoints with that model that reported a system crash. Click a bar in the chart to load the endpoints represented by that bar in the chart.

Top 10 Bug Check Codes

This chart shows the top ten bug check error codes that caused a system crash and the number of crashes that are due to each of those error codes. For more information about these bug check codes, see Microsoft: Bug Check Code Reference.

Figure 13. Top 10 Bug Check Codes

©2026 Tanium Inc. All Rights Reserved



View process network latency events

About this task

Click the **Process Network Latency** tab in the charts section to show charts that provide more information about endpoints in the defined computer groups that reported process network latency events during the selected time frame. Two charts show a summary of the reported events.

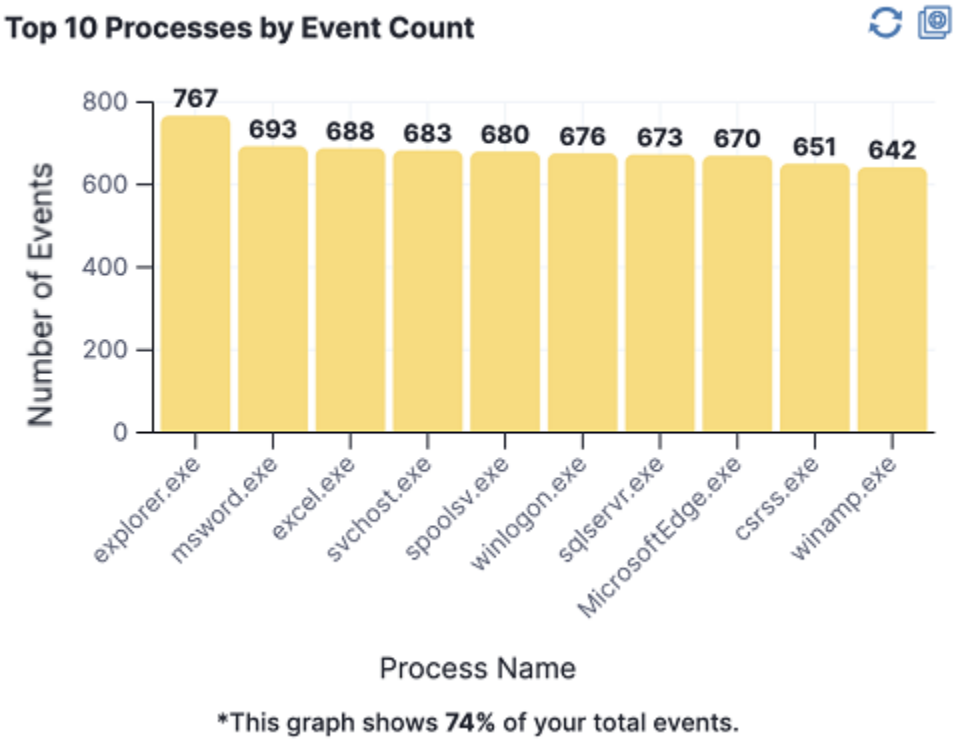
Tip: Performance records network latency events for Windows and macOS endpoints only.

Note: To see the full list of models that reported a process network latency event, click View question results in Interact . From there, you see a list of all endpoints that reported this event type and filter by model.

©2026 Tanium Inc. All Rights Reserved

Top 10 Processes by Event Count

Figure 14. Top 10 Processes by Event Count

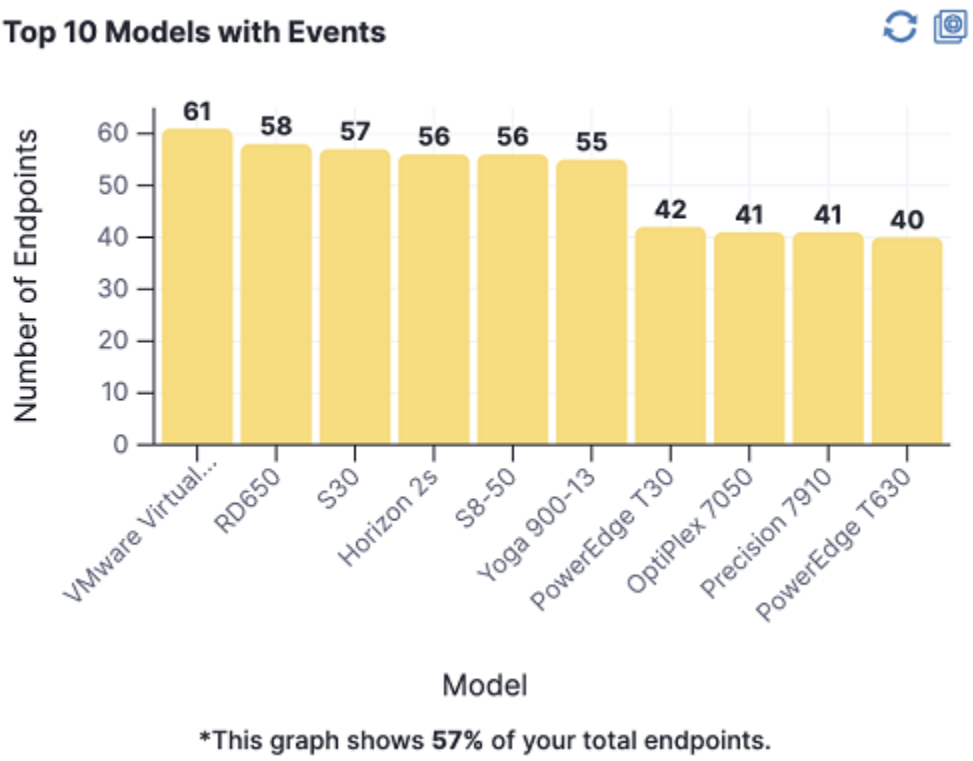


Top 10 Models with Events

Hover over a bar in the chart to see the exact number of endpoints with that model that reported a network latency event. Click a bar in the chart to populate the results grid with the endpoints represented by that bar.

Figure 15. Top 10 Models with Events

©2026 Tanium Inc. All Rights Reserved



View network outage events

About this task

Click the **Network Outage** tab in the charts section to show charts that provide more information about endpoints in the defined computer groups that reported network outage events during the selected time frame. The chart shows a summary of the reported events:

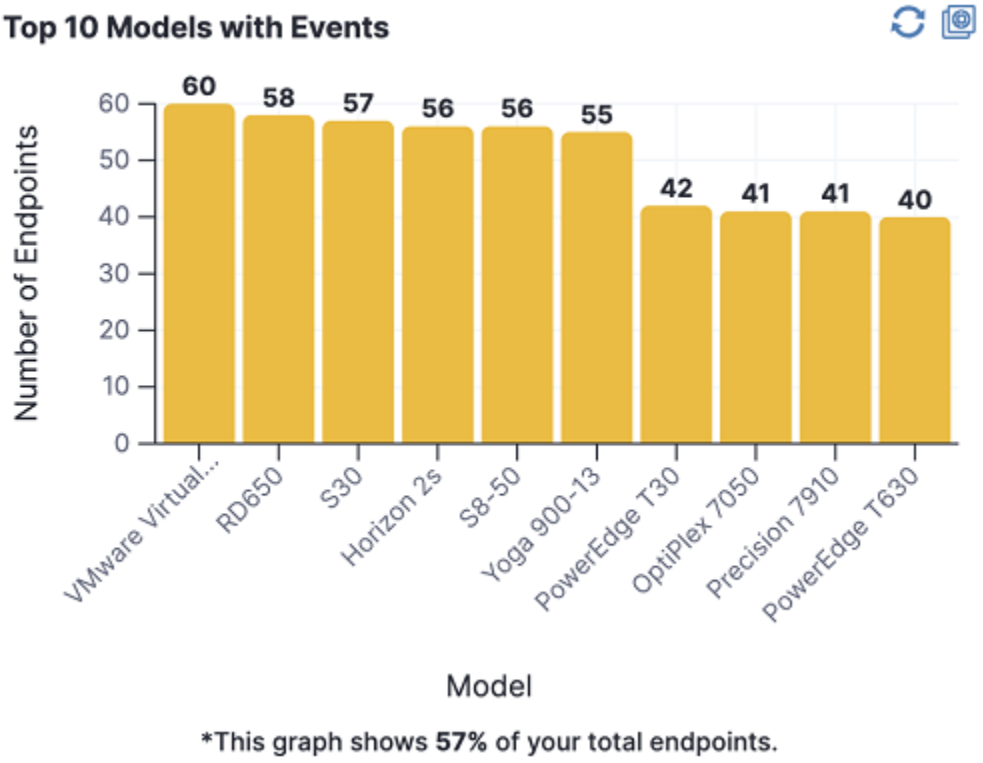
Note: To see the full list of models that reported a network outage event, click View question results in Interact . From there, you see a list of all endpoints that reported this event type and filter by model.

Top 10 Models with Events

Hover over a bar in the chart to see the exact number of endpoints with that model that reported a network outage. Click a bar in the chart to populate the results grid with the endpoints represented by that bar.

©2026 Tanium Inc. All Rights Reserved

Figure 16. Top 10 Models with Events



View WiFi signal events

About this task

Click the **WiFi Signal** tab in the charts section to show charts that provide more information about endpoints in the defined computer groups that reported WiFi signal quality events during the selected time frame. The chart shows a summary of the reported events:

Tip: Performance records WiFi signal events for Windows and macOS endpoints only.

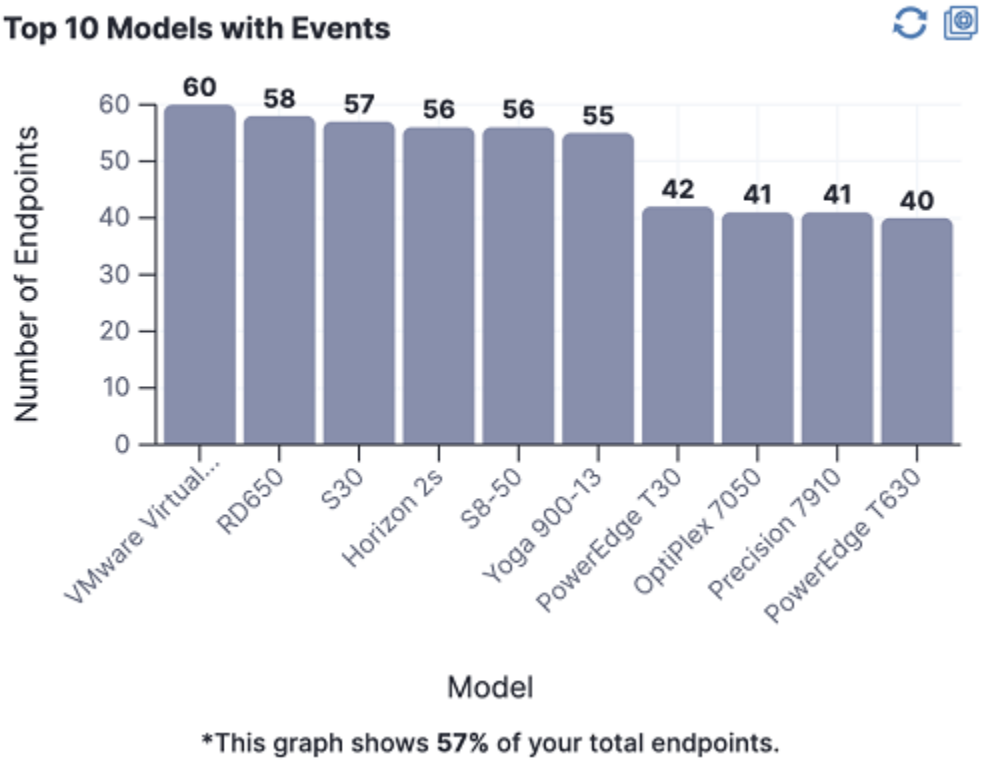
Note: To see the full list of models that reported a WiFi signal quality event, click View question results in Interact . From there, you see a list of all endpoints that reported this event type and filter by model.

©2026 Tanium Inc. All Rights Reserved

Top 10 Models with Events

Hover over a bar in the chart to see the exact number of endpoints with that model that reported a WiFi signal event. Click a bar in the chart to populate the results grid with the endpoints represented by that bar.

Figure 17. Top 10 Models with Events



View Boot Time events

About this task

In the Events section, click the **Boot Time** tab to view events where boot durations were longer than the defined threshold.

Tip: Performance records Boot Time events for Windows endpoints only.

Top 10 Models with Events

The chart shows the top ten models with the most boot time events. The x-axis represents the model

©2026 Tanium Inc. All Rights Reserved

names. The y-axis represents the number of endpoints for each model that reported a boot time event.

Note: To see the full list of models that reported a boot time event, click View question results in Interact . From there, you see a list of all endpoints that reported a boot time event, and you can filter by model.

View Logon Time events

About this task

In the Events section, click the **Logon Time** tab to view events where logon durations were longer than the defined threshold.

Top 10 Models with Events

The chart shows the top ten models with the most logon time events. The x-axis represents the model names. The y-axis represents the number of endpoints for each model that reported a logon time event. An endpoint is counted only once in the charts, even if that endpoint reported more than one logon time event.

Note: To see the full list of models that reported a logon time event, click View question results in Interact . From there, you see a list of all endpoints that reported a logon time event, and you can filter by model.

View endpoints with events

About this task

The results grid below the charts shows a list of the endpoints that reported that event type.

Expand the **Filters** section and select a column name in **Select Attribute** to filter the results. The available filters vary based on the selected chart. You can also click a bar in a chart to filter the results to list all endpoints that are represented by that bar.

©2026 Tanium Inc. All Rights Reserved

To save the data that is displayed in the results grid as a CSV file, click Export . to open the **Export All** window. Enter a file name and select a formatting option, then click **Export** to download the CSV file.

Customize the results

About this task

Click Customize Columns to add or remove the following columns from the results table.

- **Computer Name**
- **IP Address**
- **Events**

  The number of events for the selected chart (**All**, **CPU**, **Memory**, **Disk Capacity**, **Disk Latency**, **Application Crashes**, or **System Crashes**) that occurred during the selected **Scope**.
- **Bitness** (available only for **All** and **CPU**)
- **Is Virtual** (available only for **All** and **CPU**)
- **Total Memory** (available only for **Memory**)
- **Free Disk Space** (available only for **Disk Capacity**)
- **Total Disk Space** (available only for **Disk Capacity**)
- **Disk ID** (available only for **Disk Latency**)
- **Disk Model** (available only for **Disk Latency**)
- **Device Interface** (available only for **Disk Latency**)
- **Platform**
- **Model**
- **Performance Score**
- **Top Process** (available only for **CPU** and **Memory**)

©2026 Tanium Inc. All Rights Reserved

The processes that consume the highest amount of CPU or memory, depending on the chart that is selected, for the duration of the event are reported as the top processes associated with the event.

- **Top Process Events** (available only for **CPU** and **Memory**)
- **Process** (available only for **Application Crashes**)

  The process associated with the crash.
- **Version** (available only for **Application Crashes**)
- **Bug Check** (available only for **System Crashes**)
- **Crashes** (available only for **Application Crashes** and **System Crashes**)
- **Affected Disks** (available only for **Disk Capacity** and **Disk Latency**)
- **Last Boot Duration (sec)** (available only for **Boot Time**)
- **Last Logon Duration (sec)** (available only for **Logon Time**)
- **Direct Connect**

  If you installed Direct Connect, provides a link to connect to the endpoint.

Drag and drop the items in the **Customize Columns** list to change the order of the columns in the results table. Click a column header to sort the results by that column.

Connect directly to an endpoint

About this task

Click Direct Connect to Endpoint in the **Action** column to connect directly to the endpoint for further troubleshooting.

> **Note:** You must have the Direct Connect solution installed and configured to use this action. For more information, see Connecting directly to endpoints on page 76.

©2026 Tanium Inc. All Rights Reserved

View in Tanium Interact

About this task

Click View question results in Interact  to open the question results in Interact. From there, you can modify the question or drill down in the results to find more details about the endpoints that reported an event.

You might want to use this feature to refine the data that is returned or to schedule an action on the endpoints. For more information about working with the **Question Builder**, see Tanium Console User Guide: Using the Question Builder. This button is available in the event charts and lists of endpoints on the **Events** page.

©2026 Tanium Inc. All Rights Reserved

Connecting directly to endpoints

About this task

Use Direct Connect to connect directly to an endpoint to troubleshoot an issue with live and historical data. You can use this data to:

- Understand performance events that occurred on that endpoint.
- Visualize process-level resource consumption data from the time of an incident.
- See what processes are currently running and the resources they are consuming. If needed, you can terminate one or more processes on the endpoint.
- Access important attributes about the endpoint (such as model, CPU speed, memory capacity, and disk space).
- Download files from the endpoint to use for troubleshooting, such as log files.
- Open a screen sharing session. For more information, see Tanium Direct Connect User Guide: Opening screen sharing sessions..

Note:

Direct Connect has the following restrictions:

- You can directly connect only to an endpoint that has an IPv4 address.
- To connect to endpoints with action lock turned on, you must enable the **Bypass Action Lock** setting in Direct Connect. To access this setting, from the Direct Connect **Overview** page, click Settings and select **Endpoint Connection**. For more information, see Configure Direct Connect and Managing action locks.

For more information, see Tanium Direct Connect User Guide.

©2026 Tanium Inc. All Rights Reserved

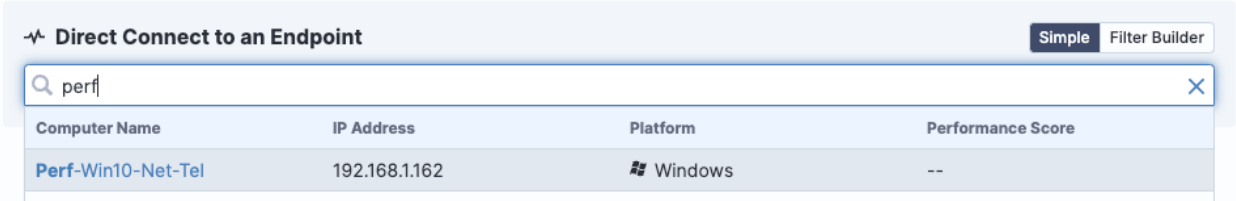
Create a direct connection

About this task

Connect directly to an endpoint from the Performance **Overview** page. The **Direct Connect** page provides detailed process and event information from the endpoint.

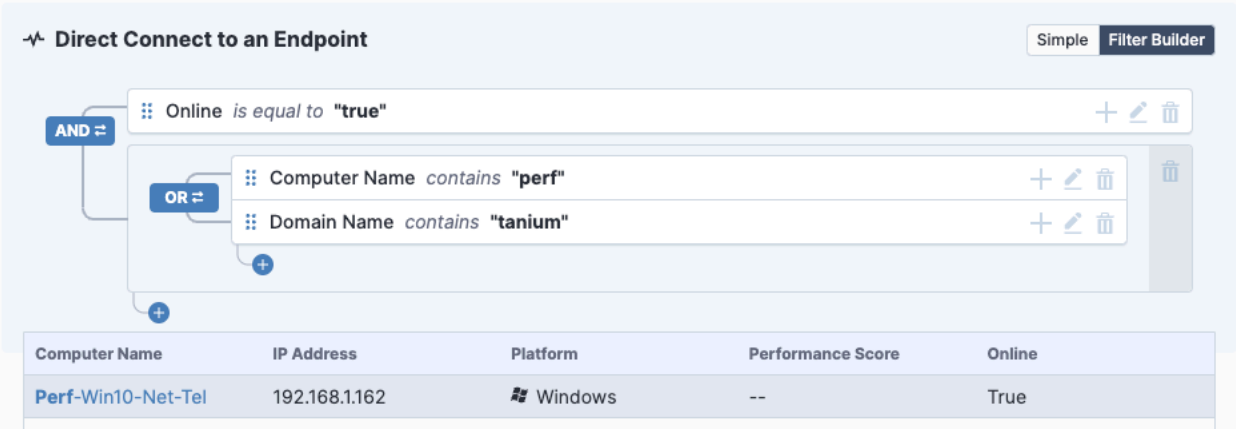
- To use the simple search, enter the IP address or Computer Name (exactly as it appears in the Computer Name sensor) for the endpoint to which you want to test a connection. Select the endpoint from the results.

  Figure 18. Simple search for an endpoint

- To use a filter, click **Filter Builder**. Build a query to search for the endpoint using advanced filters to filter question results based on match conditions.

  Figure 19. Filter Builder query

  Click **+** and use the controls to add filter conditions:

  - **Add Row**: Add one or more conditions.
  - **Add Group**: Select this option to nest a Boolean operator and then use **Add Row** to build the nested expression.

You can also connect to an endpoint from Performance by clicking Direct Connect to Endpoint in

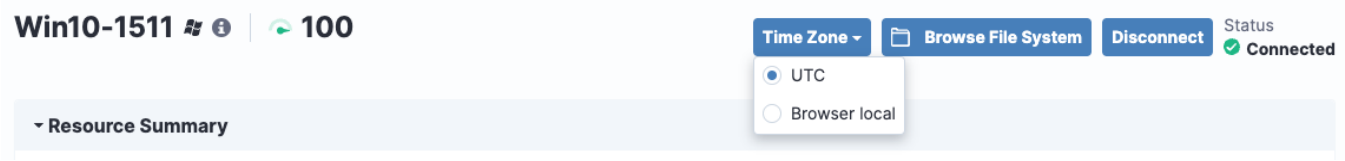
©2026 Tanium Inc. All Rights Reserved

the **Action** column of a table. For more information, see Connect directly to an endpoint on page 74.

The status of the connection is shown at the top of the page. To end the current connection, click **Disconnect**. If the connection ends due to a time-out, click **Cancel**, and then reconnect to the endpoint.

Click **Time Zone** to set the time zone for the data on the page: **UTC** or **Browser local**.

Figure 20. Time Zone options



Browse and download files from the endpoint

About this task

Use the file browser to download files that might be helpful for troubleshooting, such as log files.

Before you begin

You must be assigned the **Performance Administrator** role, the **Performance Operator** role, or the **Performance File Download** permission to use this feature.

Browse files

About this task

Click **Browse File System** to open the file browser.

Figure 21. File browser

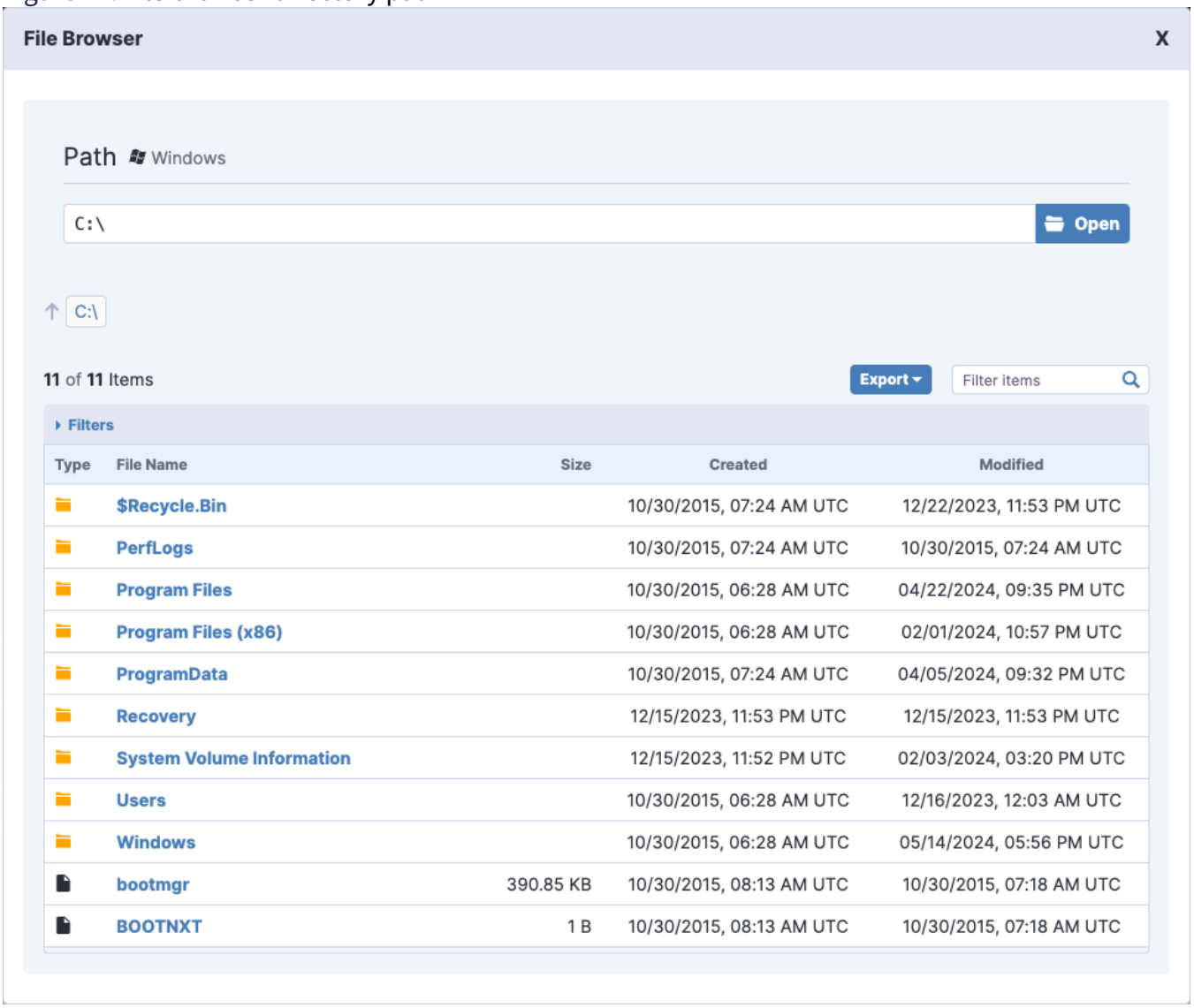


From the **File Browser** page, you can manually enter the path to a directory and click **Open** or select the directory from the list.

©2026 Tanium Inc. All Rights Reserved

Best Practice: Include the trailing slash when you manually enter a directory path.

Figure 22. File browser directory path



Download files

About this task

Manually enter the full path to a file and click **Open** or select a file from the list to download it. The file streams directly to your browser's download manager, which shows download progress and lets you pause or cancel the download.

View the Live Process Monitor

©2026 Tanium Inc. All Rights Reserved

About this task

The **Live Process Monitor** section displays details about the processes currently running on the endpoint. By default, it includes columns in the following table:

Default Live Process Monitor columns

Column	Description
CPU (Normalized)	Average CPU utilization for the process across all cores on the endpoint, normalized to a percentage of 0-100. On Windows endpoints, this normalized value usually matches what Task Manager reports.
CPU (Raw)	CPU utilization calculated as the 0-100 value multiplied by the number of cores on the endpoint. This value provides insight into whether one core on the endpoint might be over utilized by a process.
WSS	Working set size, the amount of physical memory that the process currently uses. Windows endpoints only.
RES	Resident set size, the amount of physical memory that the process currently uses, excluding memory swapped to disk. Linux endpoints only.
RSIZE	Resident memory size, the amount of physical memory that the process currently uses. macOS endpoints only.
Command Line	Command that started the process.

Click Customize Columns to add any of the columns described in the following table.

Additional Live Process Monitor columns

Column	Description
Process Group	Shows how Tanium Client Performance CX groups processes for the Tanium Server database. This is useful when you need to diagnose why a specific process is not listed individually in the charts on the **Direct Connect** page. You can modify this configuration by editing your process groups. For more information, see Configure process groups on page 148.
Commit	Windows endpoints only.
VIRT	Linux endpoints only.
FDs	Linux endpoints only.
I/O Reads	Windows and Linux endpoints only.

©2026 Tanium Inc. All Rights Reserved

Column	Description
I/O Writes	Windows and Linux endpoints only.
Handles	Windows and macOS endpoints only.
VSIZE	macOS and Linux endpoints only.
Threads	macOS and Linux endpoints only.
Efficiency Mode	Windows endpoints only. Indicates whether power throttling is enabled for the process.

Note: For Windows, **I/O** is generic and refers to file, network, and device I/O. For Linux, I/O is specific to storage and includes subprocesses.

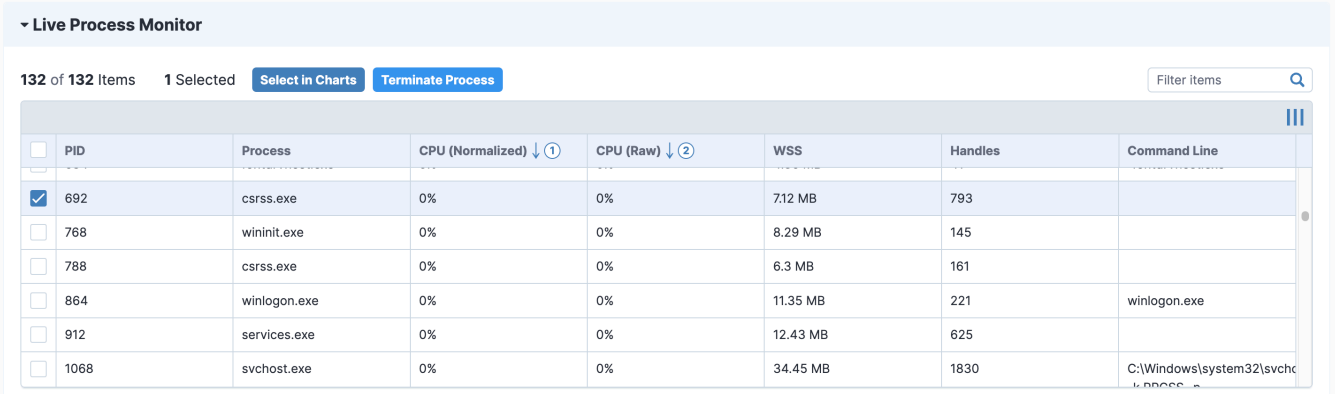
Terminate a process on the endpoint

About this task

You can terminate one or more processes on the endpoint, which might resolve performance issues if a process hangs or uses too many resources. You must be assigned the **Performance Administrator** role, the **Performance Operator** role, or the **Performance Kill Process** permission to use this feature.

Select one or more processes in the **Live Process Monitor** table and click **Terminate Process** (or **Terminate Processes** for multiple processes).

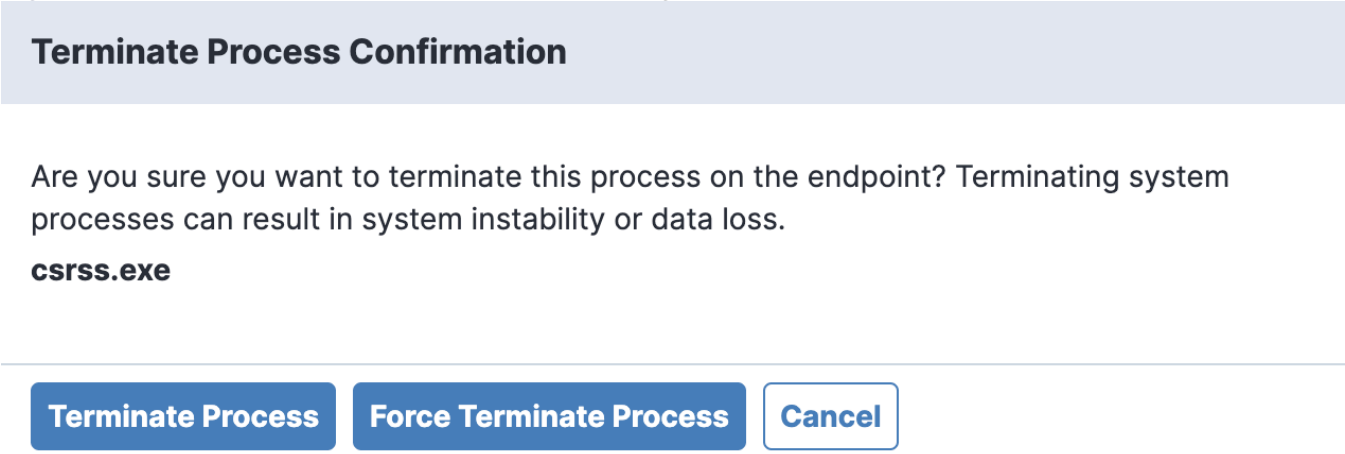
Figure 23. Live Process Monitor table



©2026 Tanium Inc. All Rights Reserved

Click **Terminate Process**, **Force Terminate Process**, or **Cancel** (**Terminate Processes**, **Force Terminate Processes**, or **Cancel** for multiple processes). Enter your user name and password, and click **Submit**.

Figure 24. Terminate Process Confirmation message



View boot and logon times

Note: Available for Microsoft Windows endpoints only.

The **Boot and Logon Times** section includes the following details that occurred within the last 30 days:

- **Last Logon**: The time stamp of the last sign in.
- **Last Boot**: The time stamp of the last start up.
- **Last Logged on User**: The last user to sign in.
- **Average Boot Duration**: The average boot duration over the last 30 days.
- **Average Logon Duration**: The average logon duration over the last 30 days.
- **Logon Event Threshold**: The threshold as configured in the profile settings. For more information, see Managing profiles on page 46.
- **Boot Event Threshold**: The threshold as configured in the profile settings. For more information, see Managing profiles on page 46.

©2026 Tanium Inc. All Rights Reserved

The bar chart shows the average boot times and logon times across all users for each day. Hover over the bars to view additional information.

After the bar chart, a grid shows all boot and logon activities within the last 30 days.

- In the **Actions** column, click Scope charts to time frame to scope the charts on the page to the time frame in which the boot or logon action occurred.
- In the **Duration** column, a flag indicates that the activity created a Performance event because the duration was longer than the configured threshold.

> **Note:**
>
> The `Start time` of the Log event in this **Boot & Logon Times grid** might not match the `Start time` of the Performance event in the **Events grid**. The Start time in the **Events** grid shows the time when the Performance event was triggered. For example, a computer was turned on at 12:00 PM and the boot threshold is set at one minute.
>
> - The Start time in the Events grid shows the time that the Performance boot event was triggered, which is 12:01 PM.
> - The Start time in the Boot & Logon Times grid shows the time when the boot or logon was initiated, which is 12:00 PM.

View endpoint information

About this task

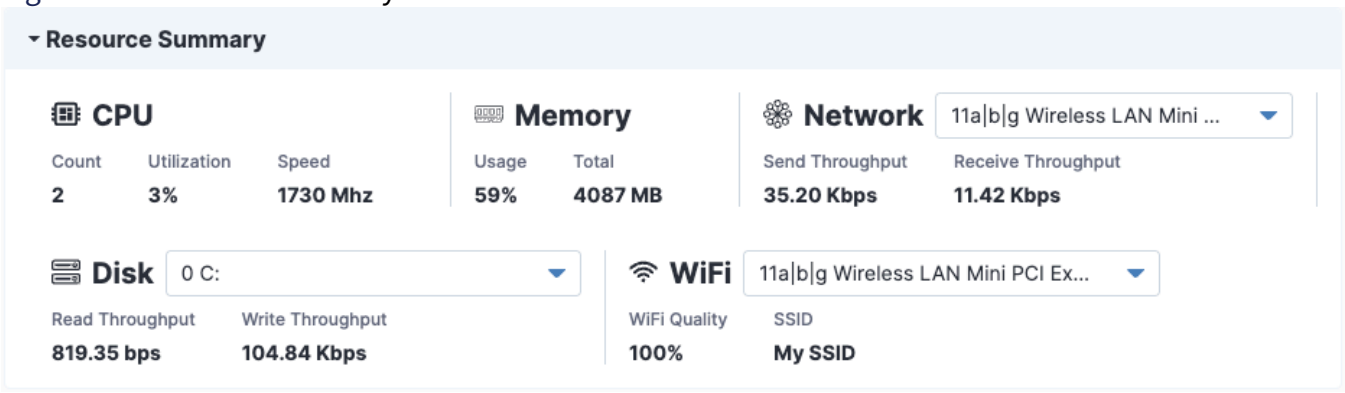
Hover over Info to view the details about the endpoint: **Platform**, **Model**, **Serial Number**, **IP Address**, **Logged In Users**, **Profile**, **Profile Revision**, **Operating System Generation**.

The **Resource Summary** section shows the **CPU**, **Memory**, **Network**, **Disk**, and **WiFi** information.

Note: If the endpoint has multiple WiFi adapters, you can view each one from the dropdown list. The adapter with highest signal quality is shown by default. If the endpoint has no WiFi adapters, the **WiFi** section does not appear.

©2026 Tanium Inc. All Rights Reserved

Figure 25. Resource Summary section



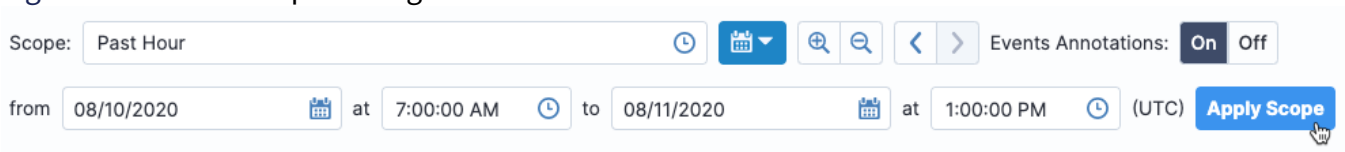
Set the time frame for the data

About this task

Click to select a time frame for the data: **Past hour**, **Past 4 hours**, **Past 8 hours**, **Past day**, **Past 2 days**, **Past week**, **Custom**.

Select **Custom** or click Set custom scope to define a custom date and time (in UTC) frame. After you set the custom date and time frame, click **Apply Scope**.

Figure 26. Custom scope settings



Note: Each time you update the time frame and apply the new scope, performance metrics are retrieved from the Tanium Time Series Database (TSDB) to populate charts in the **Events** section. Frequently changing the scope and resolution might increase the CPU usage on the endpoint.

View the charts

About this task

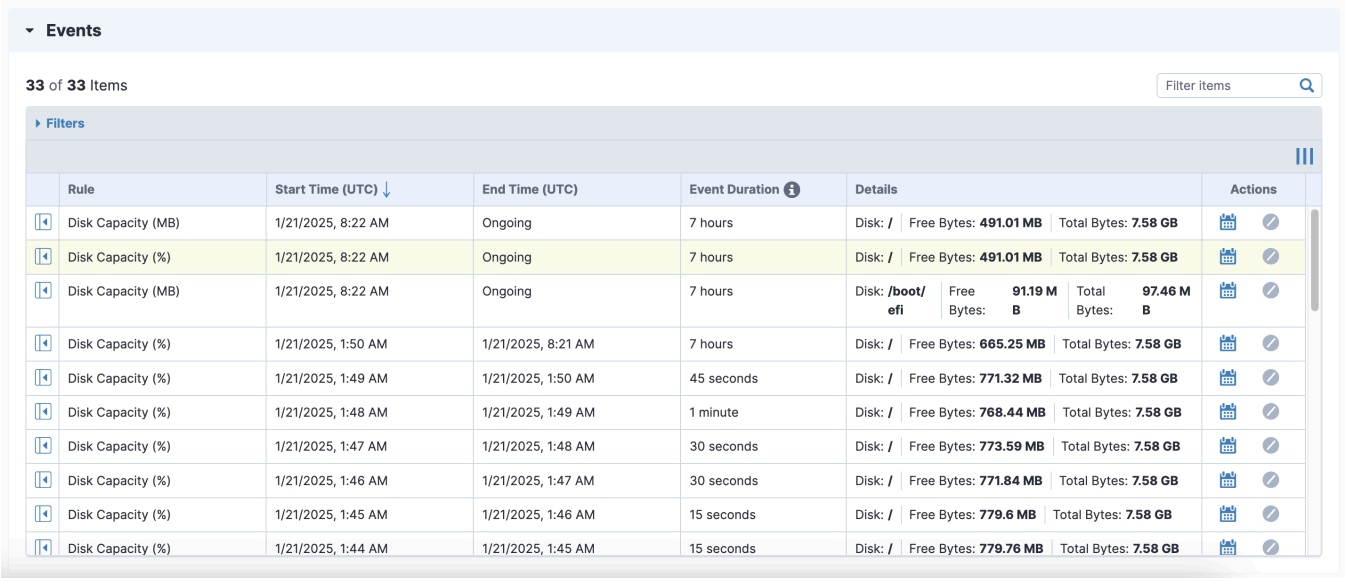
Charts show performance information for the endpoint for the selected time frame. You can expand and collapse the section for each chart.

©2026 Tanium Inc. All Rights Reserved

Events

The **Events** section includes a grid with events that occurred on the endpoint during the selected time frame and the associated **Rule Type**, **Start Time**, **End Time**, **Duration**, and **Details**. Use the **Filter items** field to quickly filter the grid results.

Figure 27. Events section



In the **Actions** column, click Scope charts to time frame to scope the charts on the page to the time frame in which the event occurred. If the event was associated with specific processes, you can click Select top processes for this event in charts to select only those processes in the subsequent process-related charts.

Click Expand Details to open a side panel with a summary of an individual Performance Event. The panel shows relevant information of the event, scoped to the timeframe of when the event occurred.

In the panel, click the arrows to view other events. Click **Actions** to view additional options similar to the Actions column in the Events grid. Select an action to close the details panel and apply the settings to the Events page.

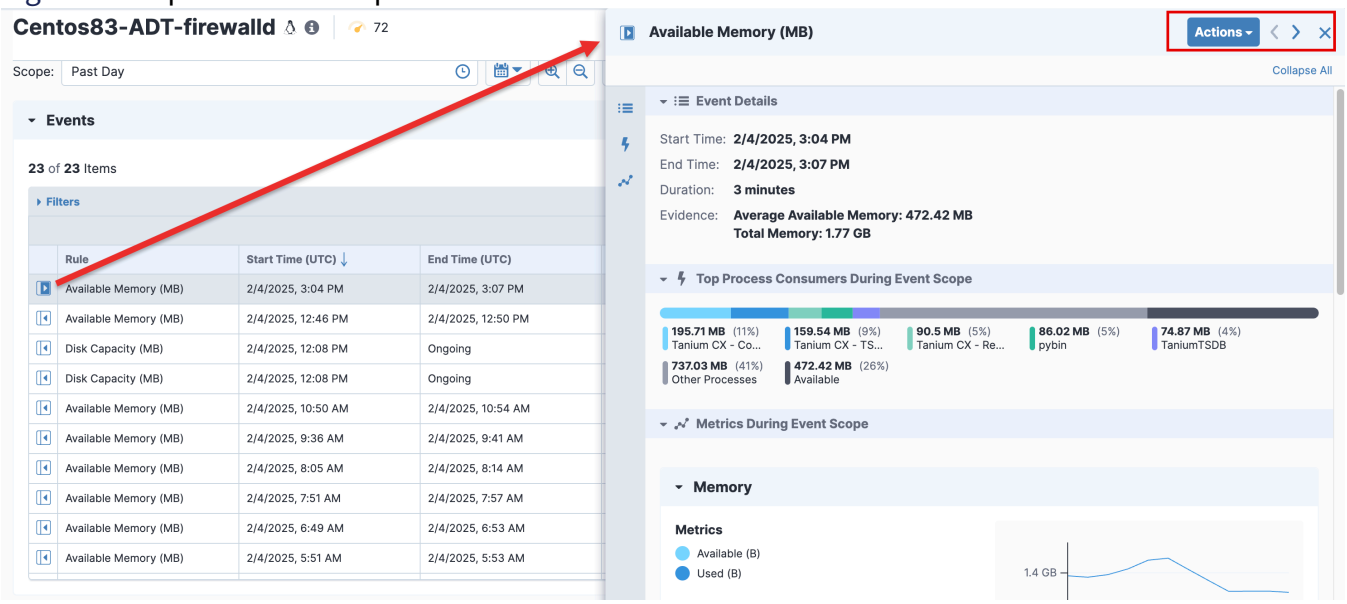
- **Scope to event timeframe**: Closes the details panel and scopes all charts on the Direct Connect page to the time of the event.
- **Select top processes**: Closes the details panel and selects the top five processes for process-related charts.
- **Scope and select top processes**: Closes the details panel, scopes to the event timeframe,

©2026 Tanium Inc. All Rights Reserved

and selects top processes.

- **Add to Investigation**: Opens the **Add to Investigation** window where you can add the event to a new or existing investigation in Tanium Investigations. This option is available only if you have Tanium Investigate installed and permissions to create an investigation. For more information, see Tanium Investigate User Guide: User role requirements.

Figure 28. Expanded Details panel



CPU

The **CPU** section contains two charts:

- **Metrics**: Shows several CPU-related metrics to show more detail about the CPU use: **CPU (%)**, **User (%)**, **Kernel (%)**, and **Interrupt (%)**. Windows endpoints also include **DPC (%)**. For Linux and macOS endpoints, you can select **Load [1m]**, **Load [5m]**, and **Load [15m]** to add those metrics to the chart.

  > **Note:** In order for Linux systems to show interrupt time in Performance, IRQ reporting must be enabled in the kernel. For more information, refer to linux-hiding-interrupt-cpu-usage.

- **Processes**: Shows the processes that were running on the endpoint during the selected time frame. Select the specific processes that you want to see in the chart.

©2026 Tanium Inc. All Rights Reserved

If the selected time frame is one day or less, you can click **Top processes** to select only the top processes for the selected time frame.

The top processes are the processes that consumed the highest amount of CPU for the duration of the selected time frame.

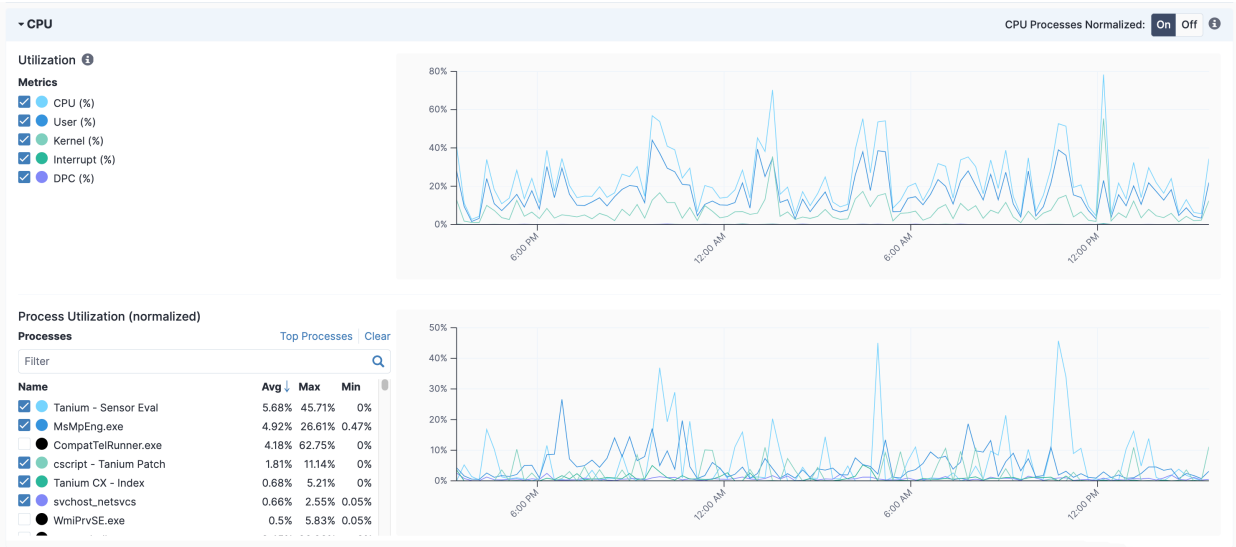
Tip:

By default, the process percentages show normalized utilization values instead of raw utilization values.

- Raw CPU utilization is the combined utilization across all cores. In a multi-core system, the raw utilization values can surpass 100%.
- Normalized CPU utilization is derived by dividing the raw utilization values by the number of cores.

To show raw CPU utilization, click **CPU Processes Normalized: Off**

Figure 29. CPU Metrics and Process sections



Memory

The **Memory** section contains the following charts:

- **Metrics**: Shows two memory-related metrics to show more detail about the memory use:

©2026 Tanium Inc. All Rights Reserved

Available and **Used**. For Windows endpoints, you can select **Non-Paged Pool**, **Paged Pool**, **Pagefile Size**, **Pagefile Used**, **Commit Limit**, and **Committed** to add those metrics to the chart.

- **Processes**: Shows the processes that were running on the endpoint during the selected time frame. The charts that appear depend on the operating system:

  Linux and macOS endpoints

  - **Process Resident Memory**: Shows the processes that were consuming physical memory on the endpoint during the selected time frame.
  - **Process Virtual Memory**: Shows the processes that were consuming virtual memory on the endpoint during the selected time frame.

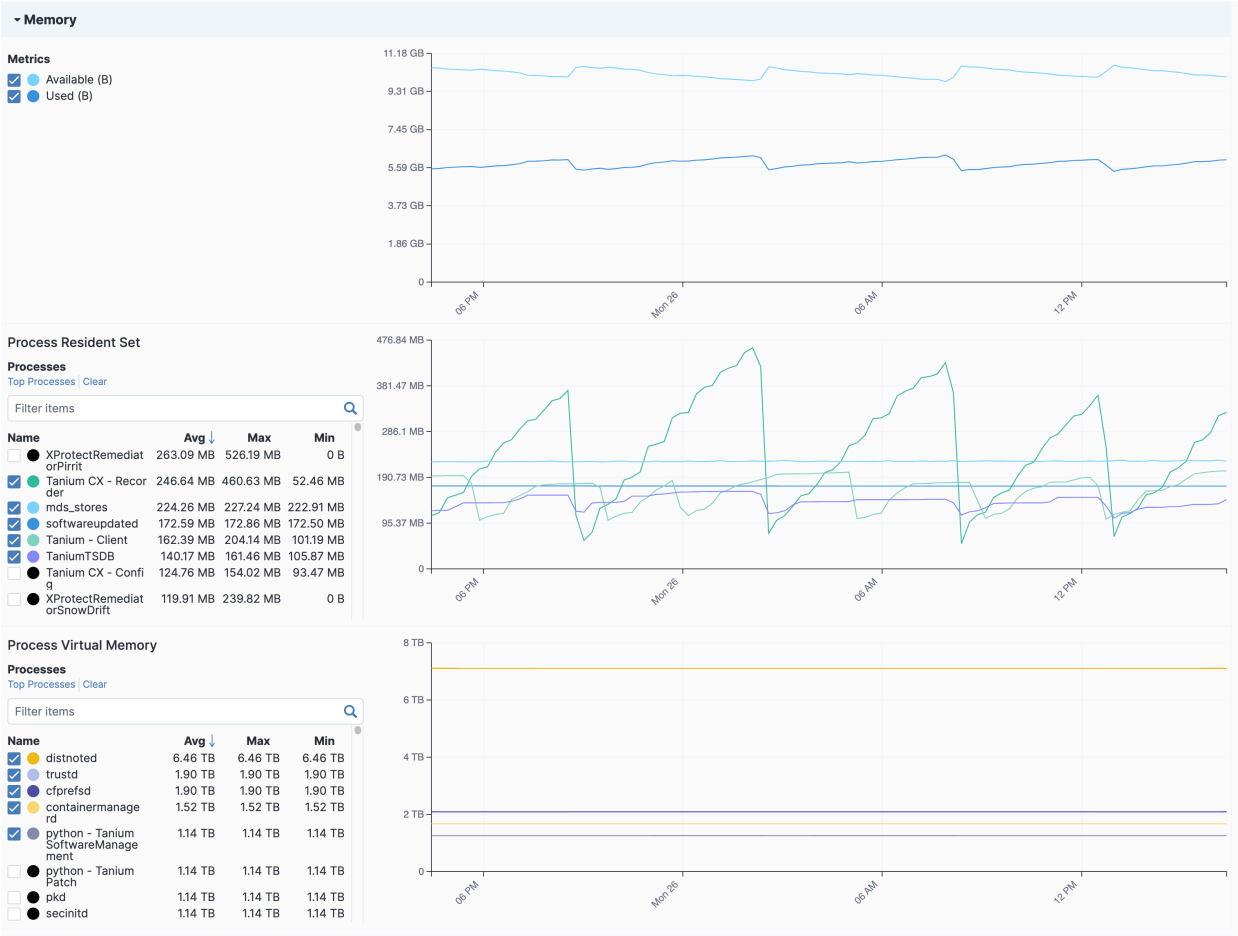
  Windows endpoints

  - **Process Working Set**: Shows the processes that were consuming physical memory on the endpoint during the selected time frame.
  - **Process Private Committed**: Shows the processes that were consuming private committed memory on the endpoint during the selected time frame.

  For all process charts, you can select the specific processes that you want to see in the chart. If the selected time frame is one day or less, click **Top Processes** to select only the top processes for the selected time frame. The top processes are the processes that consumed the highest amount of memory for the duration of the selected time frame.

  Figure 30. Memory Metrics and Processes sections

©2026 Tanium Inc. All Rights Reserved



Network

The **Network** section contains the following charts:

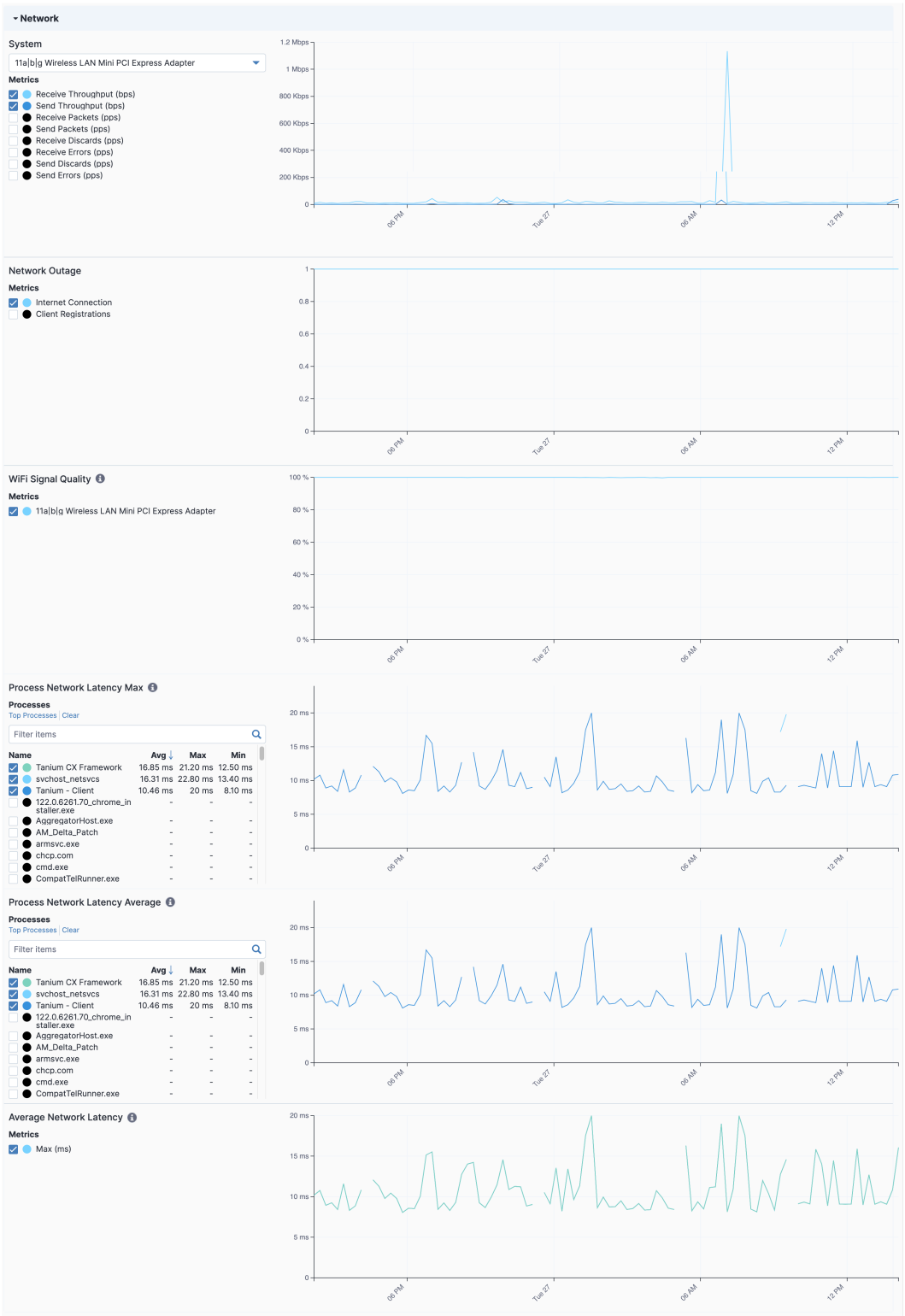
- **System**: Shows metrics for a network adapter. Select an adapter from the dropdown list. You can select the following metrics to show information about that adapter: **Receive Throughput (bps)**, **Send Throughput (bps)**, **Receive Packets (pps)**, **Send Packets (pps)**, **Receive Discards (pps)**, **Receive Errors (pps)**, **Send Discards (pps)**, and **Send Errors (pps)**.
- **Network Outage**: Shows metrics for events that cause network outages and failed Tanium Client registrations. You can select the following metrics to show:
    - **Internet Connection** (Windows and macOS endpoints): 1 indicates that the endpoint is connected to the Internet. 0 indicates that the endpoint is disconnected.
    - **Client Registrations**: 1 indicates that the Tanium Client on an endpoint successfully registered.

©2026 Tanium Inc. All Rights Reserved

- **WiFi Signal Quality**: (Windows and macOS endpoints) Shows signal strengths for any WiFi adapters. Hover over a signal strength in the chart to view the SSID of the WiFi adapter. The chart contains adapters only for endpoints that have at least one WiFi adapter.
- **Process Network Latency Max**: (Windows and macOS endpoints only) Shows metrics for the process of each name with the highest network latency. Click **Top Processes** to show metrics in the chart for the five processes with the highest average latency.
- **Process Network Latency Average**: (Windows and macOS endpoints only) Shows network latency metrics for all processes. Processes are grouped together by name. Click **Top Processes** to show metrics in the chart for the five processes with the highest average latency.
- **Average Network Latency**: (Windows and macOS endpoints only) Shows the overall network latency of the endpoint. It is calculated using the average value of the ten most latent processes. Use this chart to compare system-level latency to process latency.

Figure 31. Network section

©2026 Tanium Inc. All Rights Reserved



Disk

The **Disk** section contains the following charts:

©2026 Tanium Inc. All Rights Reserved

- **Physical Disk I/O**: The most active disk drive is selected by default. You can select a different disk drive from the dropdown list. You can select the following metrics to show information about that disk: **Active (%)**, **Read (%)**, **Write (%)**, **Read (Bps)**, **Write (Bps)**, **Read Latency (ms)**, **Write Latency (ms)**, **Reads (ops)**, and **Writes (ops)**. **Read Latency (ms)** and **Write Latency (ms)** are selected by default.

    - The **Active (%)** metric indicates the disk time spent servicing read and write requests. On Windows endpoints, this value is determined by the **Average Disk Queue Length** measurement in percentage format (multiplied by 100) reported by Windows Performance Monitoring (perfmon). For example, if the **Average Disk Queue Length** for an endpoint is 1, the **Active (%)** metric reports as `100%`. This value can be over 100% when the **Average Disk Queue Length** value is greater than 1. If the **Average Disk Queue Length** for an endpoint is 3, the **Active (%)** metric is `300%`. A value over 100% does not mean that processes are using 3 times more disk than available, nor that there is a bottleneck.

    - The **Read (%)** and **Write (%)** metrics are similar to **Active (%)**, but show only the operations read from or written to disk, respectively. These values are determined by the **Average Disk Read Queue Length** and **Average Disk Write Queue Length** values represented in percentages. As with **Active (%)**, values over 100% do not necessarily indicate a problem on the endpoint.

    - If you are investigating a storage issue on an endpoint, the primary indicator is usually disk latency. If the **Active (%)**, **Read (%)**, and **Write (%)** metrics for an endpoint are high, check to see whether disk latency is also high. If it is not, the endpoint is likely not experiencing a disk storage issue.

    - For more information, see Microsoft: Windows Performance Monitor Disk Counters Explained.

- **Total Disk I/O Read and Write**: Shows the IO usage by the processes that were running on the endpoint during the selected time frame. Select the specific processes that you want to see in the chart. If the selected time frame is one day or less, you can click **Show Top Processes** to select only the top processes for the selected time frame. The top processes are the processes that had the highest disk IO usage for the duration of the selected time frame.

- **Logical Disk Capacity**: Shows the used and free disk space for logical disks that are classified as fixed disks.

©2026 Tanium Inc. All Rights Reserved

Note: For Windows, **I/O** is generic and refers to file, network, and device I/O. For Linux, I/O is specific to storage and includes subprocesses.

Figure 32. Disk section



Process Diagnostics

About this task

The **Process Diagnostics** section contains the following charts:

- **Zombies**: The Zombie Count is the total number of zombie processes running on the endpoint. A zombie process is a process that has completed execution but is still listed in the process table. A relatively high number of zombie processes can lead to unresponsive applications and system instability. The Process Count is the total process count, including zombies.

  Note: Zombie Count and Process Count metrics are collected every four hours.

- **Process Handles**: The number of handles that a process has open.
- **Process Threads**: The thread count of a process.

Figure 33. Process Diagnostics section

©2026 Tanium Inc. All Rights Reserved



Working with charts

Scope

Click to zoom in the charts. The charts and associated time frame adjust to a shorter range. For example, if the time range is set to **Past Hour** and the current charts show 15 minute increments from 3:00 PM - 4:00 PM, they shift to show 5 minute increments from 3:15 PM - 3:45 PM.

Click to zoom out the charts. The charts and associated time frame adjust to a longer range. For example, if the time range is set to **Past Hour** and the current charts show 15 minute increments from 3:00 PM - 4:00 PM, they shift to show 30 minute increments from 3:15 PM - 3:45 PM.

Click to pan left in the charts. The charts and associated time frame shift to earlier times in the predefined increments. For example, if the time range is set to **Past Hour** and the current charts show 15 minute increments from 3:00 PM - 4:00 PM, they shift to show 15 minute increments from 2:30 PM - 3:30 PM.

Click to pan right in the charts. The charts and associated time frame shift to later times in the predefined increments. For example, if the time range is set to **Past Hour** and the current charts show 15 minute increments from 3:00 PM - 4:00 PM, they shift to show 15 minute increments from 3:30 PM - 4:30 PM.

Resolution

©2026 Tanium Inc. All Rights Reserved

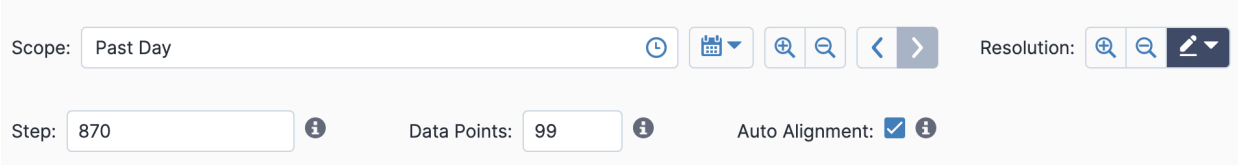
Click to increase the number of data points. This divides the step by 2 to increase the resolution, which increases the number of data points.

Click to decrease the number of data points. This multiplies the step by 2 to decrease the resolution, which decreases the number of data points.

Click Set query options to view the step and data points used for calculation and to optionally change them.

- **Step** is the interval, in seconds, used to query the data.
- **Data Points** are all data available within a scope of time.
- **Auto Alignment** is enabled by default to keep zoom-in and panning consistent in the frame. You can manually adjust the frame by clearing this checkbox and entering your own step and/or data point values.

Figure 34. Expanded Set query options



Note:

Performance prevents you from requesting over 11,000 data points. For example, if you enter a scope of "Past Day" and manually override the alignment to enter `1` as the step value, Performance automatically adjusts the step to be the lowest amount possible for that scope duration. For example, for "Past Day", the step would be 8.

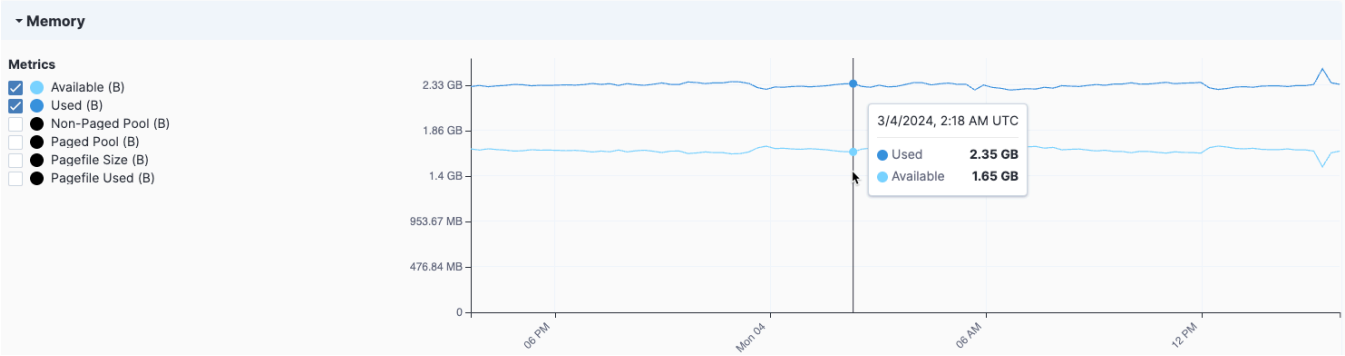
Also note that overriding the step or data points might break queries with multiple series. If this occurs, a notification appears informing you that you exceeded the threshold.

Events annotations

Events annotations highlight the time span when an event occurred in red. Click the annotation for more details about the event.

Figure 35. Event annotation on a chart

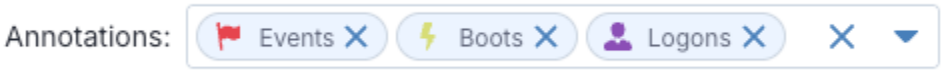
©2026 Tanium Inc. All Rights Reserved



Event annotations for **Application Crashes** and **System Crashes** appear on all charts. Annotations for all other event types appear only on the specific charts for which they are applicable.

You can turn events annotations on or off in the scope section. To turn on an annotation, select it from the list. To turn off an annotation, click its close icon ✕. To turn off all annotations, click the close icon ✕ in the **Annotations** row.

Figure 36. Events annotations in the Scope section



©2026 Tanium Inc. All Rights Reserved

Monitoring performance scores

About this task

Performance scores reflect the health of the endpoints in your environment. The Performance Score dashboard shows overall endpoint health and provides breakdowns by event type, endpoint count, and criticality level. For example, if users in a department report that their endpoints are running slowly, you can filter the dashboard by the relevant computer group to determine whether scores are declining, identify the event categories driving lower scores, and then review individual endpoint scores to find the most affected endpoints.

Note: Performance scores are driven by the number of performance-related events that occur on an endpoint. If an endpoint is idle and not actively in use, it might not generate new events, and its score remains unaffected.

Before you begin

- For each endpoint, the performance score is calculated based on the active profile for the endpoint. For more information about how to configure the performance score weight for a profile, see Create a profile on page 46.
- To filter dashboards by specific computer groups, you must enable data collection for the computer groups in Tanium Reporting. For information, see Tanium Reporting User Guide: Select computer groups for data collection.
- For more information about performance scores, see Performance scores on page 10.

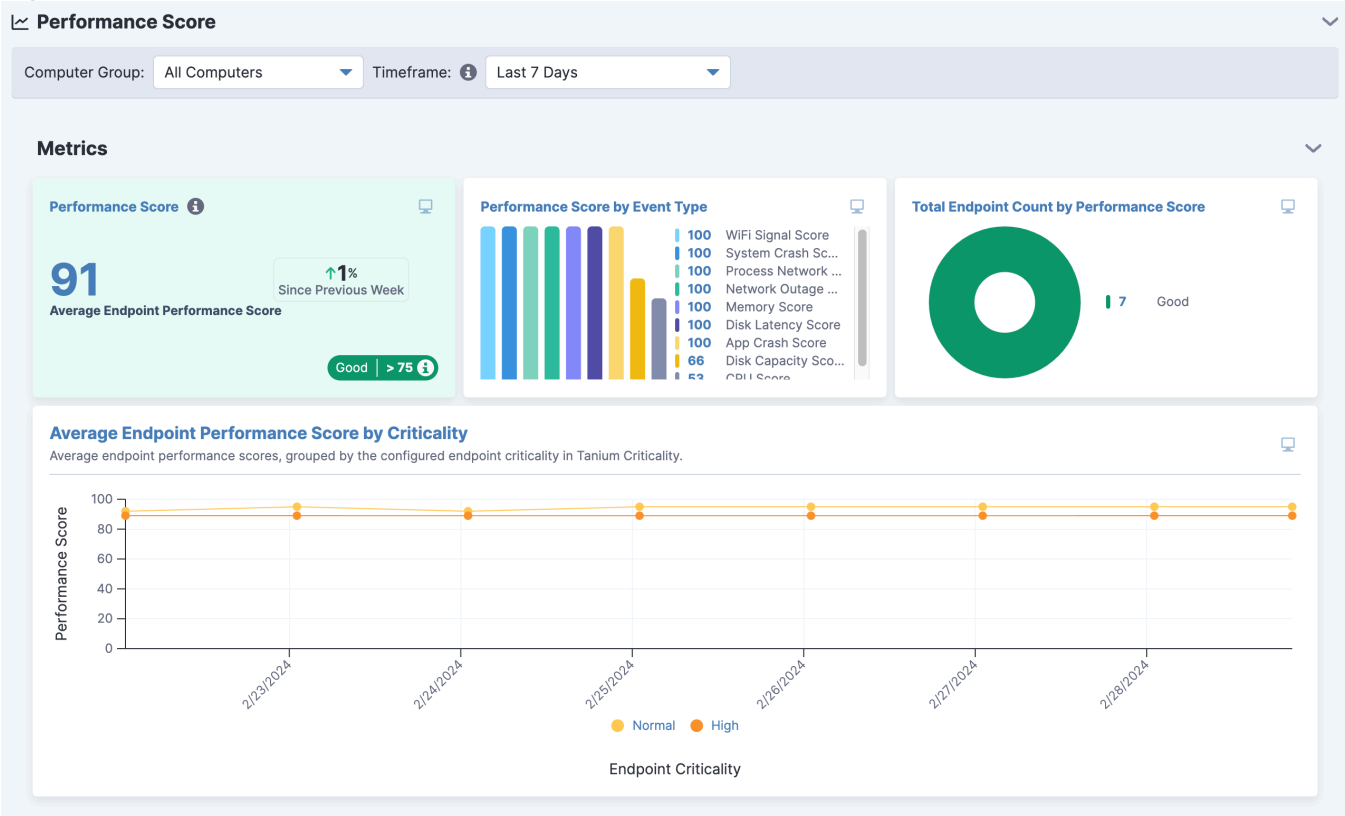
View the Performance Score dashboard

About this task

The **Performance Overview** page contains a dashboard with performance score metrics in a visual format.

©2026 Tanium Inc. All Rights Reserved

Figure 37. Tanium Performance Score dashboard



1. From the Main menu, go to **Modules** > **Performance** to open the **Overview** page.
2. Navigate to the **Performance Score** section to view the **Performance Score** dashboard. The dashboard contains the following charts:

Chart	Description
Performance Score	The overall score of your environment
Performance Score by Event Type	A breakdown of performance scores by event category.
Total Endpoint Count by Performance Score	The number of endpoints with each performance score.
Average Endpoint	The average performance score by criticality level. Criticality values are assigned to endpoints in Tanium Criticality, and define the amount of risk the endpoint presents to the organization. For

©2026 Tanium Inc. All Rights Reserved

Chart	Description
Performance Score by Criticality	information about criticality levels, see Tanium Criticality User Guide: Criticality overview . **Note:** A **Normal** level in Performance is equal to a **Medium** level in Criticality.

3. When viewing the performance scores, the following options are available:
    - In the header of the section, select a **Computer Group** and **Timeframe** to apply to all charts in the section. Note that some charts might not contain data for all time frames and computer groups.

      Note: To filter dashboards by specific computer groups, you must enable data collection for the computer groups in Tanium Reporting. For more information, see Tanium Reporting User Guide: Select computer groups for data collection.
    - Chart data automatically refreshes every two minutes when the browser tab is open.
    - Click the name of a chart to open the report that supplies the data to the chart. For more information about available options when viewing a report, see Tanium Reporting user guide: View reports.
    - Click any data point on a chart to view the data in a report.

Result

Tip: You can also view individual endpoint scores in the **Online Endpoints** section on the Performance **Overview** page.

View performance scores by event

1. From the Main menu, go to **Modules** > **Performance > Events**.
2. Select any filters in the **Targets** section.
    a. Specify the computer group for which you want to see events in the **Define Computer Groups** field.
    b. Select a time period for the events from the **Scope** menu. The default option is **Past Day**.

©2026 Tanium Inc. All Rights Reserved

c. If you change any values, click **Get Results** to update the charts and table in the **Events** section.

3. In the **Events** section, select an event category to show only events in the selected category. The report and charts that appear in the **Events** section contains a list of endpoints with matching events for the category.
4. (Optional) In the report, expand **Filters** and then select a model, platform, and process name to add additional filters to the report. To remove report filters, click **Clear Filters**.
5. (Optional) To connect to an endpoint, find the endpoint in the report, and then click Direct Connect to Endpoint in the **Action** column.

View performance scores by endpoint

1. From the Main menu, go to **Modules** > **Performance** > **Performance Score**.
2. Navigate to the **Endpoint Performance Scores** section. This section shows a table of endpoints that are tracked by Performance, including a column for **Performance Score**.



Tip: If the **Performance Score** column does not appear, click Customize Columns and select the **Performance Score** column to show the column in the table.

3. Use the search, filter, and sort controls to quickly find an endpoint in the table.
   - Rows must match all filters to appear in the table.
   - Enter a value in the **Filter items** field to show rows with matching text in any column.
   - To add advanced filters, expand **Filters** and then add individual or groups of filters. You can then add filters in rows and groups.
     - To add an individual filter, click **+ Row**, select a source, operator, and value that endpoints must match, and then click **Apply**.
     - To add related filters, click **+ Grouping**. For each filter, select a source, operator, and value that endpoints must match, and then click **Apply**. Select this option to nest a Boolean operator and then add rows or more groups to build the nested expression.

©2026 Tanium Inc. All Rights Reserved

- To filter the report by a particular cell, hover over the cell, click Options , and click Filter by value
- To copy the contents of a single cell, hover over the cell, click Options , and click Copy Cell Value .
- To view basic details for an endpoint, click Endpoint Details next to the name of an endpoint in the **Computer Name** column. From the basic details, you can then click **View Details** to view and manage the endpoint in Tanium Reporting. For more information, see Tanium Reporting user guide: View and manage a single endpoint.
- Click Export to CSV to download a copy of the table as a CSV file. The CSV file includes the table headers and table data.
- Click Refresh to show updated data.

Tip: You can also view individual endpoint scores in the **Online Endpoints** section on the Performance **Overview** page.

©2026 Tanium Inc. All Rights Reserved

Monitoring applications

About this task

Application monitoring allows you to monitor the performance of key applications with real-time metrics whether endpoints are online or offline. With the continuous monitoring of specific processes, you can ensure applications are functioning properly while maintaining visibility into issues that may impact endpoints. Use the provided common applications or configure your own custom applications to monitor a wide range of process groups, including single applications, software suites, task management tools, communication platforms, or IT deployed agents.

Before you begin

- To filter dashboards by specific computer groups, you must enable data collection for the computer groups in Tanium Reporting. For information, see Tanium Reporting User Guide: Select computer groups for data collection.
- To ensure the configuration is targeting the correct processes, Tanium Performance application monitoring uses the process group name because it is not always possible to derive the name of the process based on the application name. Endpoints can alter process names based on the process group configuration. For more information, see Configure application monitoring on page 102.



Best Practice: Application monitoring introduces new metric types designed to provide more granular visibility into the performance of applications. Although this monitoring should have minimal impact on endpoints, it is recommended you begin by monitoring only a few applications and then gradually expanding to more.

Configure application monitoring

1. From the Main menu, go to **Modules** > **Performance > Dashboards** > **Application Monitoring**, and then click **Add Application**.
2. In the **Definition** section, configure the following:

©2026 Tanium Inc. All Rights Reserved

- **Common Applications** - Select from the provided list of applications. When you select an application, the Name and Processes fields are automatically populated with data.
    - **Name** - The name of the selected application appears here.
    - **Processes** - This is the process group name for the selected application. Click the **Add Process** button to manually enter another process group name to the list for this application.
    - Under **Process Matching**, the **Ignore Case** checkbox is selected by default and therefore process group names are not case sensitive.

      Important: When entering the process group name, note that matching is not case sensitive when the Ignore Case checkbox is selected. If you clear the Ignore Case checkbox, process group names are matched exactly as entered, including case.
- **Custom** - Select Custom from the list of applications to configure your own applications.
    - Enter a **Name** for the application.

      Important: Enter a Name that matches the name found by the Installed Applications sensor. The Installed Applications sensor uses this name to match the application to its version number. If the name of the application and Installed Applications sensor results don't match, the application version column in the report will remain empty.

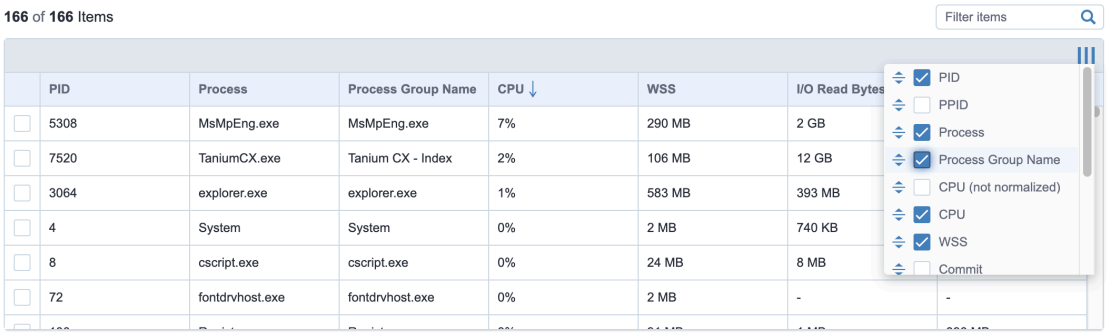
      Important: You cannot change the name of a monitored application once it has been enabled. You can update the processes associated with the application and toggle monitoring to enable and disable monitoring, but you cannot change the name. Changing the name could cause inconsistencies in the metrics.
    - Enter one or more process groups in the **Processes** section. Process group name is case sensitive.

If you're unsure of the process group name, use Tanium Direct Connect to find the

©2026 Tanium Inc. All Rights Reserved

name of the process group running on the endpoint. You may need to unhide the **Process Group Name** column.

Figure 38. Process Group Name column

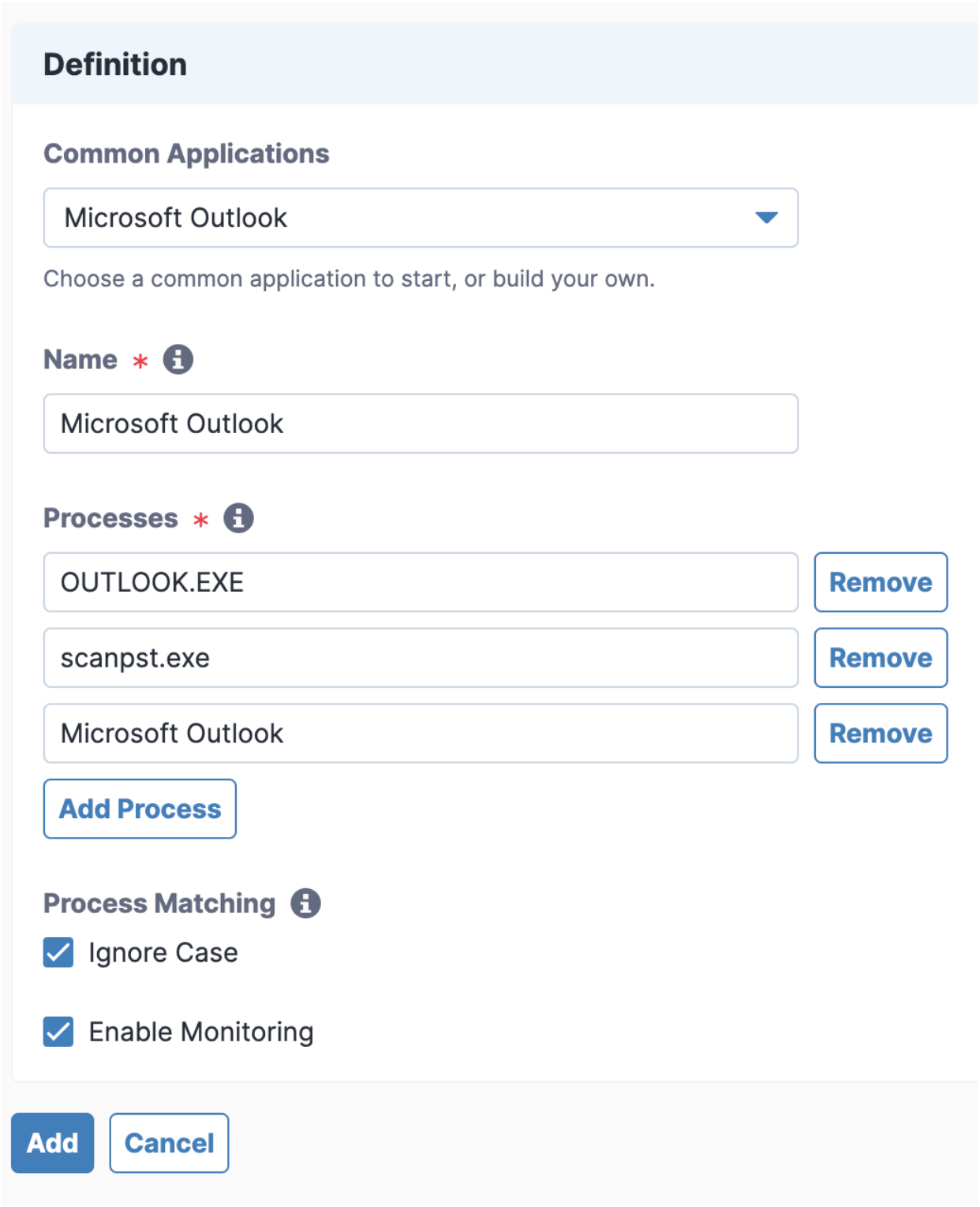


Best Practice: You cannot configure more than 30 monitored applications by default. It is recommended that you do not change this limit, however, it is configurable in Performance Settings, with an upper limit of 100.

3. Leave the **Enable Monitoring** checkbox selected to initiate monitoring when profiles are deployed. Clear the checkbox to save the configuration but begin monitoring at a later time. You can enable or disable monitoring at any time by selecting the Edit button for the application in the list view and toggling the **Enable Monitoring** checkbox.

4. Click **Add**.
   Figure 39. Completed application Definition form

©2026 Tanium Inc. All Rights Reserved



Result

Important: Configuration changes do not take effect until profiles are deployed to targeted endpoints. Click **Deploy All Profiles** when the message appears on the Application Monitoring page or go to **Performance > Management > Profiles**.

©2026 Tanium Inc. All Rights Reserved

Note: When you delete or disable an application, historical data for that application's processes will continue to appear in the charts for a period of time.

View the monitoring applications dashboard

About this task

The Application Monitoring **Dashboard** tab contains charts with metrics in a visual format for monitored applications. You can filter the charts by Computer Groups, Applications, and Timeframe.

Note: For more information about how metrics are collected and calculated, see the Reference on page 111 section.

1. From the Main menu, go to **Modules** > **Performance > Application Monitoring**.
2. In the **Dashboard** tab, view the following charts:

   Applications with Most Crashes

   This chart provides information about applications on endpoints in the defined computer groups that reported the most crashes. Data displayed here represents the last recorded data point for the selected timeframe. Click on an application in the list to go to another view with more details on that application. If there have been no application crashes, this chart displays a zero.

   Total Daily Application Crashes Over Time

   This graph illustrates the number of crashes listed by date. Data displayed here represents all available data points for the selected timeframe. Hover over a date to see the list of applications that crashed. Click on an application to go to another view with more details on that application.

   Applications with Highest CPU Usage

   This chart provides information about applications on endpoints in the defined computer groups that reported the most CPU usage (percent utilization, out of 100). Data displayed here represents the last recorded data point for the selected timeframe. Click on an application in the list or hover over a bar in the chart and click to go to another view with more details on that application.

©2026 Tanium Inc. All Rights Reserved

Average Daily CPU Usage Over Time

This graph illustrates the percentage of CPU usage by date (percent utilization, out of 100). Hover over a date to see the list of applications sorted by CPU usage. Data displayed here represents all available data points for the selected timeframe. Click on an application to go to another view with more details on that application.

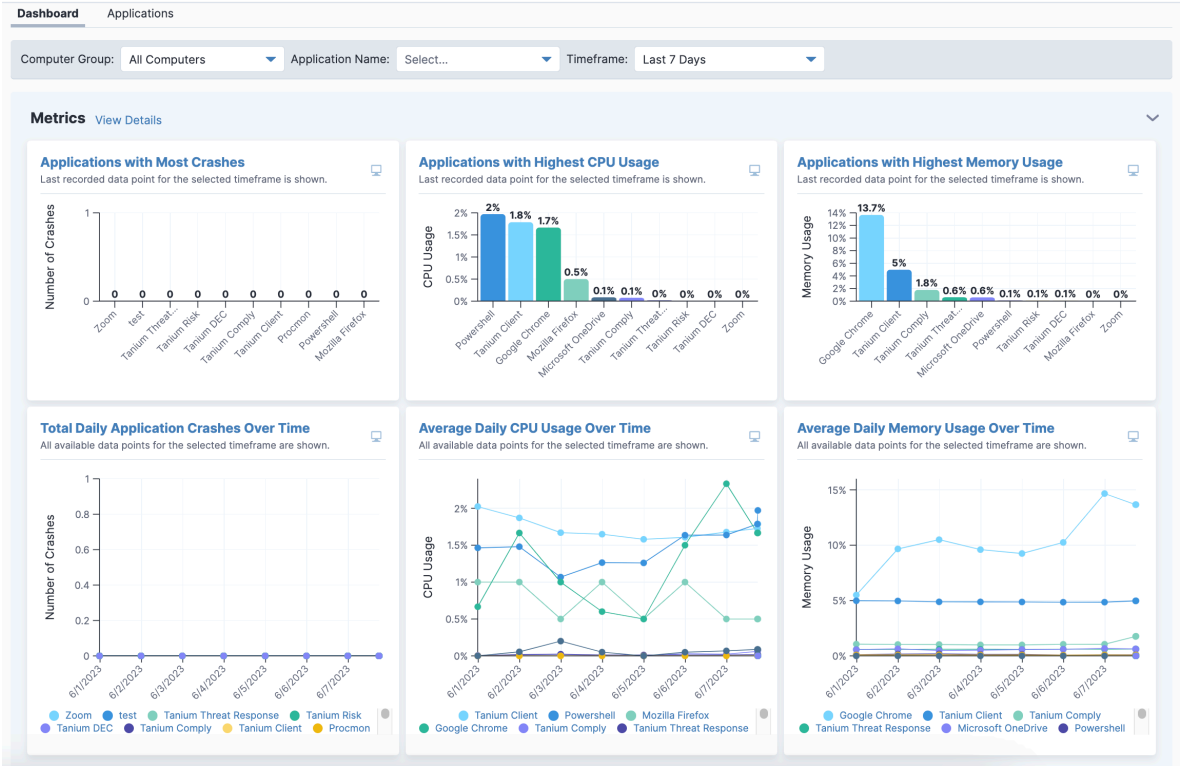
Applications with Highest Memory Usage

This chart provides information about applications on endpoints in the defined computer groups that reported the most memory usage (percent utilization, out of 100). Data displayed here represents the last recorded data point for the selected timeframe. Click on an application in the list hover over a bar in the chart and click to go to another view with more details on that application.

Average Daily Memory Usage Over Time

This graph illustrates the percentage of memory usage by date (percent utilization, out of 100). Data displayed here represents all available data points for the selected timeframe. Hover over a date to see the list of applications sorted by memory usage. Click on an application to go to another view with more details on that application.

Figure 40. Application Monitoring Dashboard



3. When viewing the application monitoring charts, the following options are available:

©2026 Tanium Inc. All Rights Reserved

- In the header of the section, select a **Computer Group**, **Application**, and **Timeframe** to apply to all charts in the section. Note that in the bar charts, only the state at the end of the selected timeframe is shown. Also note that some charts might not contain data for the selected filters.
- Chart data automatically refreshes every two minutes when the browser tab is open.
- Click the name of a chart to open the report that supplies the data to the chart. For more information about available options when viewing a report, see Tanium Reporting user guide: View reports.
- Click any data point on a chart to view the data in a report.

View metrics by application

1. From the Main menu, go to **Modules** > **Performance > Application Monitoring**.
2. In the **Dashboard** tab, click on an application that appears in any of the charts to view more in-depth details. The following tabs are available in the application details view:

   Note: Empty cells in a report indicate that the application being monitored has not run on the endpoint.

   Dashboard

   The same charts available for all monitored applications are available for the selected application. You can filter by Computer Groups and Timeframe.

   The **Total Daily Application Crashes**, **Average Daily CPU Usage**, and **Average Daily Memory Usage** charts include a trending indicator that shows the percent of change between the metric value for the previous week and its current value. Click the current value beside the trending indicator to view the report that supplies data for the chart. For more information about viewing a report, see Tanium Reporting user guide: View reports.

   Report - Crashes

   View a table of application crashes with data listed by Computer Name, Performance Score, Daily Application Crashes, Criticality, OS Platform, and Model. Click the Customize columns icon to select additional columns to be included. For information about criticality levels, see Tanium Criticality User Guide: Criticality overview. Click the Export icon to export data to a CSV file.

©2026 Tanium Inc. All Rights Reserved

Report - CPU Usage

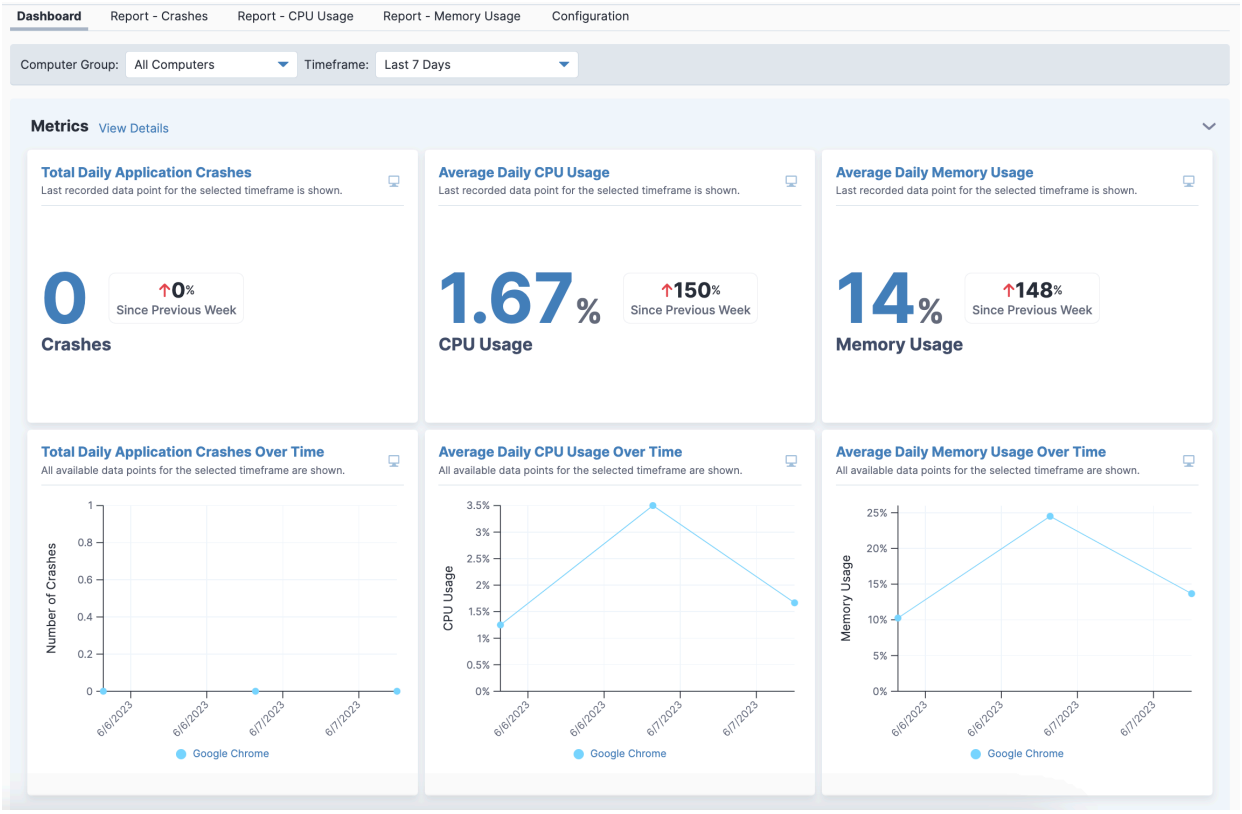
View a table of CPU usage with data listed by Computer Name, Performance Score, Average Daily CPU, CPU Details-Total Logical Processors, Criticality, OS Platform, and Model. Click the Customize columns icon to select additional columns to be included. For more information about criticality levels, see Tanium Criticality User Guide: Criticality overview. Click the Export icon to export data to a CSV file.

Report - Memory Usage

View a table of memory usage with data listed by Computer Name, Performance Score, Average Daily Memory, Total Memory, RAM Max Capacity, RAM Slots Used and Unused, Criticality, OS Platform, and Model. Click the Customize columns icon to select additional columns to be included. For information about criticality levels, see Tanium Criticality User Guide: Criticality overview. Click Export to export data to a CSV file.

Configuration

View a summary of the application configuration, including monitored processes and monitoring dates.



Use report controls

©2026 Tanium Inc. All Rights Reserved

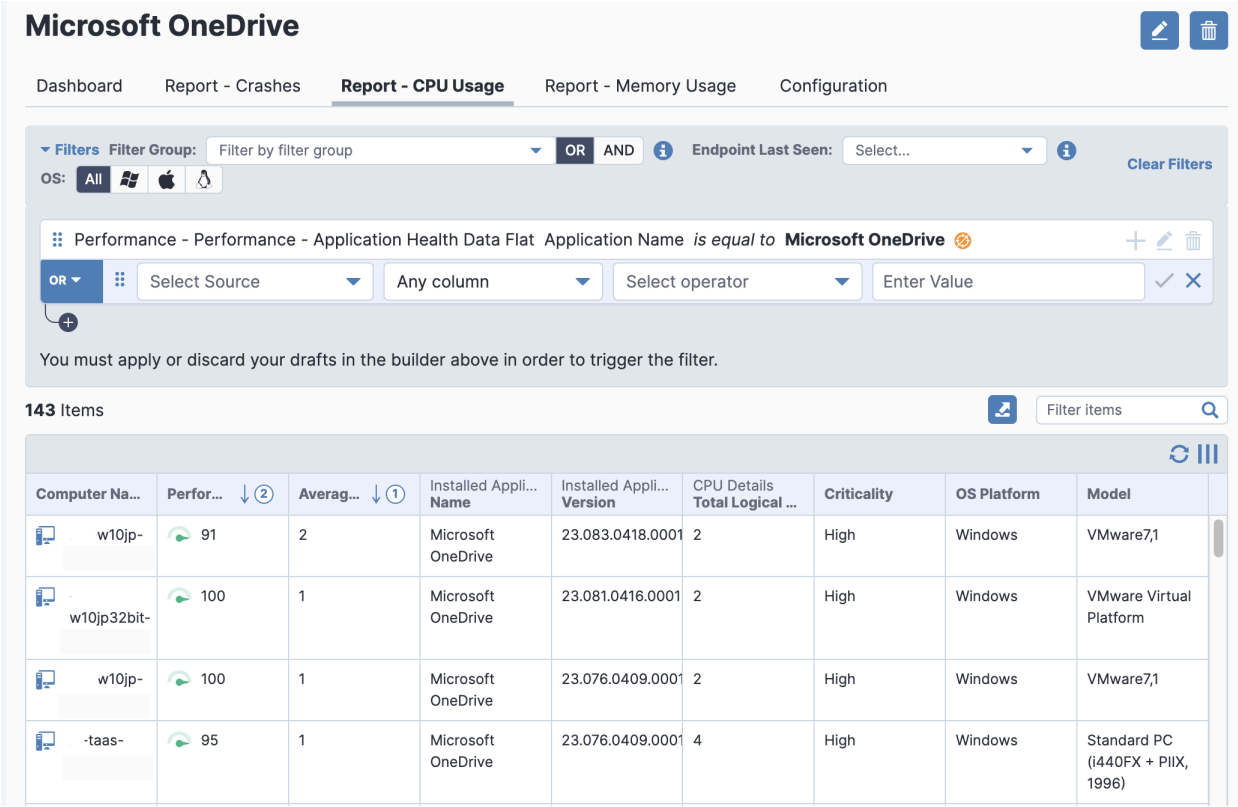
About this task

The tabs that contain reports use filters and controls found in reports throughout Tanium. For available options when viewing a report, see Tanium Reporting user guide: View reports. Use the search, filter, and sort controls to quickly find information in the table.

- Enter a value in the **Filter items** field to show rows with matching text in any column.
- Filter by **Endpoints Last Seen** within a specified time frame.
- To add advanced filters, expand **Filters** and then add individual or groups of filters. You can then add filters in rows and groups.
    - To add an individual filter, click **+ Row**, select a source, operator, and value that endpoints must match, and then click **Apply**.
    - To add related filters, click **+ Grouping**. For each filter, select a source, operator, and value that endpoints must match, and then click **Apply**. Select this option to nest a Boolean operator and then add rows or more groups to build the nested expression.
- To filter the report by a particular cell, hover over the cell, click Options , and click Filter by value
- To copy the contents of a single cell, hover over the cell, click Options , and click Copy Cell Value .

Figure 41. Filters on Application Monitoring page

©2026 Tanium Inc. All Rights Reserved



Reference

This section is intended to provide an overview of how application metrics are collected and calculated.

Note: Application monitoring and metrics collection begin when the configuration is received by the endpoint. Metrics cannot be collected retroactively.

For application monitoring, the endpoint collects CPU and memory metrics for all processes (grouped by process group) every 15 seconds and stores those in the Time Series Database (TSDB). Then every 5 minutes, averages for CPU and memory for each monitored application are collected by aggregating the stored values found in the TSDB.

The following metrics are calculated as described below:

- Application crashes - Every 5 minutes the Tanium Client checks the count of crashes that occurred for an application counted back to midnight UTC. This count includes zeros. Note that a value of zero application crashes does not imply that an application has run on the

©2026 Tanium Inc. All Rights Reserved

endpoint.

- CPU usage - Every 5 minutes the Tanium Client calculates the average CPU usage rate for an application back to midnight UTC in 60 second blocks. This rate excludes zeros, and therefore if there are spans of time without application usage, that will not cause the average to approach zero.

- Memory usage - Every 5 minutes the Tanium Client checks the resident memory usage for an application back to midnight UTC in 60 second blocks. This rate excludes zeros, and therefore if there are spans of time without application usage, that will not cause the average to approach zero.

For reporting, TDS harvests performance application health data every 30 minutes. The data in TDS is reflected in the reports. Graphs that display time series data are updated once a day. Bar charts that use TDS directly update along with the reporting information.

©2026 Tanium Inc. All Rights Reserved

Monitoring boot times

About this task

Use the Performance Boot Time dashboard to identify potential endpoint start up performance degradation over time. Boot time degradation could indicate issues with hardware, software, or system configurations. You can also monitor boot times for the following purposes:

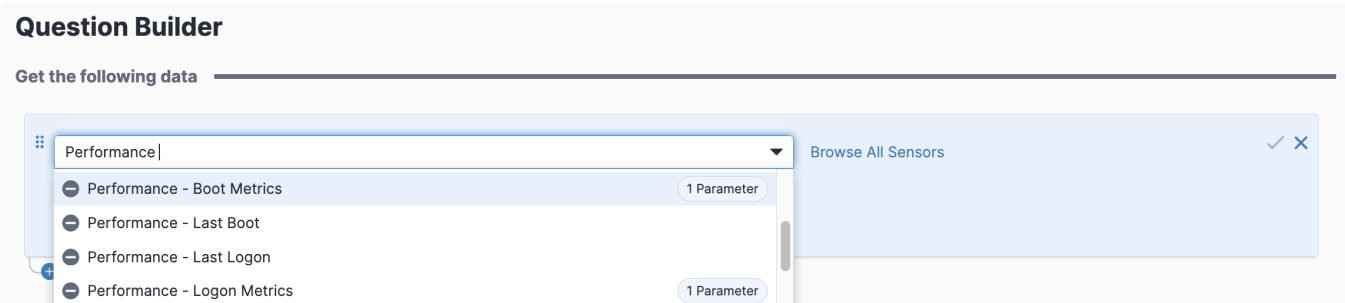
- **Troubleshooting**: Detect potential issues, such as software issues, hardware issues, or system update issues if you notice sudden increases in boot times.
- **Improving user experience**: Analyze boot times to understand the user experience. Quick boot times can contribute to positive employee experiences. Slow boot times can contribute to negative experiences.
- **Managing resources**: Allocate resources more effectively to improve boot times, such as upgrading hardware.

Boot sensors

In addition to the **Performance Boot sensors**, Tanium provides Core Content boot sensors that you can use to ask questions. For more information, see Tanium Console User Guide: Asking questions and searching endpoints in Console and Interact. Ensure that you are aware of the differences between **Performance Boot sensors** and **Core Content Boot sensors**.

The following image shows the Performance boot and logon sensors in **Question Builder**:

Figure 42. Performance boot and logon sensors in Question Builder



- **Performance – Boot Metrics**: Returns the average duration, minimum duration, and

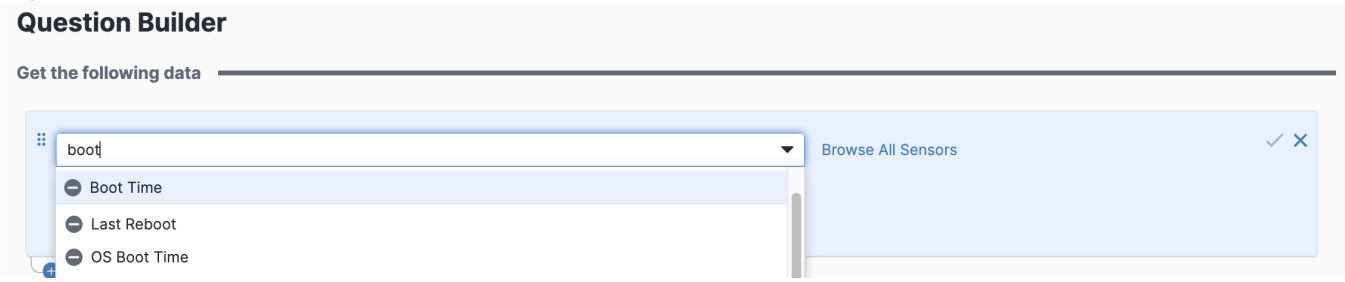
©2026 Tanium Inc. All Rights Reserved

maximum duration for boot activities across a given timeframe.

- **Performance – Last Boot**: Returns the time stamp when an endpoint last turned on, in GMT time. Boot duration is from when the endpoint is turned on to when the endpoint prompts the user to sign in.
- **Performance – Last Logon**: Returns the time stamp of the last logon, the logon duration, and the user. Logon duration is from when a user signs in to the endpoint to when the endpoint presents a usable desktop.
- **Performance – Logon Metrics**: Returns the average duration, minimum duration, and maximum duration for logon activities across a given timeframe.

The following image shows the various Core Content boot sensors in **Question Builder**:

Figure 43. Core Content boot sensors in Question Builder



- **(Core Content) Boot Time**: Returns the time elapsed from when the Windows logo appears to when the desktop appears for 10 seconds. This duration includes the idle time that passes before a user enters their credentials.
- **(Core Content) Last Reboot**: Returns the time stamp when an endpoint last turned on, including a UTC offset. For Windows endpoints, the offset is in hours. For example, `+0540` is UTC+9. For Linux and Mac endpoints, the offset is in hours and minutes. For example, `+0100` is UTC+1.
- **(Core Content) OS Boot Time**: Returns the time stamp when an endpoint last turned on in GMT time (+0000 offset).

Prerequisite

Configure at least one profile to collect boot time and logon time data. For more information, see Managing profiles on page 46.

©2026 Tanium Inc. All Rights Reserved

View the Boot Times dashboard

1. From the Main menu, go to **Modules** > **Performance** > **Dashboards** > **Boot Time**.
2. In the **Computer Groups** menu, specify the computer group for which you want to analyze boot times.
3. In the **Timeframe** menu, select a period to see metrics that occurred within that timeframe. The following information appears on the page:
    - **Average Last Boot Time**: The average boot time, based on each endpoint's last boot duration. The average is calculated by adding the last boot durations of all endpoints and then dividing by the number of endpoints. This metric refreshes approximately every 30 minutes.
    - **Average Last Boot Time by OS**: The Average Last Boot Time, grouped by operating system. This metric refreshes approximately every 30 minutes.
    - **Last Boot Time Health**: A donut chart with counts of endpoints grouped by boot health. This metric refreshes approximately every 30 minutes.
        - **Poor**: Boot time was longer than 60 seconds
        - **Fair**: Boot time was between 31 and 60 seconds
        - **Good**: Boot time was between 0 and 30 seconds
    - **Average Last Boot Times**: The average last boot times plotted daily.
    - **Average Last Boot Time by Start Up Program Count**: The average last boot time grouped by endpoints with similar number of configured startup programs. The groups are separated by program count. For example, the **0 – 5** interval on the x-axis indicates the average boot time for endpoints that have zero to five applications that are configured to automatically run at startup. This metric refreshes approximately every 30 minutes.
    - **Average Last Boot Time by Model**: The longest average last boot times grouped by model. The chart can include up to ten models. This metric refreshes approximately every 30 minutes.
    - **Average Last Boot Time by Chassis Type**: The longest average last boot times grouped by chassis type. The chart can include up to ten chassis types. This metric

©2026 Tanium Inc. All Rights Reserved

refreshes approximately every 30 minutes.

- **Average Last Boot Time by Disk Type**: The longest average last boot times grouped by disk type. The chart can include up to ten disk types. This metric refreshes approximately every 30 minutes.
- **Last Boot Times**: A table with last boot time information for all endpoints.

©2026 Tanium Inc. All Rights Reserved

Monitoring logon times

About this task

Use the Logon Time dashboard to identify potential bottlenecks or inefficiencies in sign in processes, such as authentication procedures. You can also monitor logon times for the following purposes:

- **Troubleshooting**: Detect potential issues such as network problems, authentication delays, or filesystem issues if you notice sudden increases in logon times.
- **Improving user experience**: Analyze logon times to understand the user experience. Quick logon times can contribute to positive employee experiences. Slow logon times can contribute to negative experiences.
- **Managing resources**: Allocate resources more effectively to improve logon times, such as upgrading hardware.

Prerequisite

Configure at least one profile to collect boot time and logon time data. For more information, see Managing profiles on page 46.

View the Logon Times dashboard

1. From the Main menu, go to **Modules** > **Performance** > **Dashboards** > **Logon Time**.
2. In the **Computer Groups** menu, specify the computer group for which you want to analyze logon times.
3. In the **Timeframe** menu, select a period to see metrics that occurred within that timeframe. The following information appears on the page:
    - **Average Last Logon Time**: The average last logon time, based on each endpoint's last logon duration. The average is calculated by adding the last logon durations of all endpoints and then dividing by the number of endpoints. This metric refreshes approximately every 30 minutes.

©2026 Tanium Inc. All Rights Reserved

- **Average Last Logon Time by OS**: The Average Last Logon Time, grouped by operating system. This metric refreshes approximately every 30 minutes.
- **Last Logon Time Health**: A donut chart with counts of endpoints grouped by logon health. This metric refreshes approximately every 30 minutes.
    - **Poor**: Logon time was longer than 181 seconds
    - **Fair**: Logon time was between 121 and 180 seconds
    - **Good**: Logon time was between 0 and 120 seconds
- **Average Last Logon Times**: The average last logon times calculated and plotted daily.
- **Average Last Logon Time by Start Up Program Count**: The average last logon time grouped by endpoints with similar number of configured startup programs. The groups are separated by program count. For example, the **0 – 5** interval on the x-axis indicates the average logon time for endpoints that have zero to five programs that are configured to automatically run at startup. This metric refreshes approximately every 30 minutes.
- **Average Last Logon Time by Model**: The longest average last logon times grouped by model. The chart can include up to ten models. This metric refreshes approximately every 30 minutes.
- **Average Last Logon Time by Chassis Type**: The longest average last logon times grouped by chassis type. The chart can include up to ten chassis types. This metric refreshes approximately every 30 minutes.
- **Average Last Logon Time by Disk Type**: The longest average last logon times grouped by disk type. The chart can include up to ten disk types. This metric refreshes approximately every 30 minutes.
- **Last Logon Times**: A table with last logon time information for all endpoints.

©2026 Tanium Inc. All Rights Reserved

Monitoring Performance Trends

The Performance Trends dashboard provides insight into operational health through current and historical endpoint data. Visualizations show Performance coverage, event trends, process resource usage, and CPU and memory distribution across your environment. You can use this dashboard in the following scenarios:

- **Auditing coverage after a rollout**: After deploying Performance profiles to new computer groups, confirm that Performance coverage includes all target endpoints.
- **Investigating crash patterns**: When users report recurring application or system failures, use the Application and System Crashes section to identify which applications are crashing most frequently and on how many endpoints.
- **Identifying resource-intensive processes**: When endpoints experience slowdowns, use the Top Processes section to identify processes consuming the most CPU, memory, or handles across your environment.
- **Analyzing resource trends**: When you want to analyze CPU and memory utilization patterns, use the Enterprise System Metrics section to view the current distribution and historical trends across your environment.

Prerequisites

Deploy at least one profile that targets the computer groups you want to monitor. For **Boot Time**, **Logon Time**, **Application Crashes**, and **System Crashes** data to appear in the dashboard, configure the profile to collect the corresponding data. For more information, see Managing profiles on page 46.

View the Performance Trends dashboard

Monitor endpoint health, investigate event patterns, and track resource utilization across your environment from the Performance Trends dashboard. You can export the dashboard as an HTML file to preserve as a point-in-time snapshot.

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Performance > Dashboards** > **Trends**.
2. (Optional) Filter the dashboard by **Computer Group** or **Timeframe**.

   > **Note:** To override the computer group filter for an individual chart, select the monitor icon  in the chart header and then select a computer group.

3. View the **Endpoint Status** section to review Performance deployment coverage and database usage across your environment:

   - **Performance Coverage**: Endpoints with Performance installed and active. Status values include **Optimal** and **Initializing**. An **Optimal** endpoint is actively collecting and reporting data. An **Initializing** endpoint has received a profile but has not yet begun reporting data.
   - **Performance Database Enabled**: Endpoints with the Tanium Time Series Database (Tanium TSDB) enabled, grouped by enabled status.
   - **Performance Database Size**: Tanium TSDB database size distribution across endpoints, in MB ranges.

4. View the **Events** section to see active performance event data, affected hardware models, and event trends over time:

   - **Event Composition**: Breakdown of endpoints with performance events by event category, such as **Disk Capacity**, **Disk Latency**, **CPU**, **Memory**, and **Application Crashes**.
   - **Models with Performance Events**: Hardware models with active performance events, by number of endpoints.
   - **Endpoints with Performance Events**: Performance event trends over time, with a line for each event category. Categories that require specific profile configuration, such as **Boot Time**, **Logon Time**, and **System Crashes**, appear only when the profile is configured to collect that data. For more information, see Managing profiles on page 46.

5. View the **Application and System Crashes** section to identify the most frequently occurring

©2026 Tanium Inc. All Rights Reserved

application and system crashes across your environment.

> **Note:** If no crashes have been recorded for the selected timeframe and computer group, a chart shows no data. An empty state indicates that no crashes have occurred during the selected timeframe.

The following charts are available:

- **Top Application Crashes**: Applications that crashed most frequently, by application name, version, and number of endpoints affected.
- **Top System Crashes**: System crashes that occurred most frequently, by number of endpoints affected.

6. View the **Top Processes** section to identify processes consuming the most CPU, memory, or handles across your environment. Each chart shows only processes that exceed the specified threshold:
   - **Top CPU Consumers**: Processes with average CPU utilization above 10%, by number of endpoints.
   - **Top Memory Consumers**: Processes with average resident memory above 500 MB, by number of endpoints.
   - **Top Handle Consumers**: Processes with average handle count above 10,000, by number of endpoints.
7. View the **Enterprise System Metrics** section. For each metric, a current distribution chart shows the number of endpoints in each percentage-range bucket (0–9%, 10–19%, and so on). A historical trend chart shows how those endpoint counts change daily over the selected timeframe, with each stacked layer representing one percentage-range bucket. The following charts are available:
   - Average CPU Usage
   - Minimum CPU Usage
   - Maximum CPU Usage
   - Average Memory Usage

©2026 Tanium Inc. All Rights Reserved

- Minimum Memory Usage
- Maximum Memory Usage

©2026 Tanium Inc. All Rights Reserved

Managing Performance alerts

About this task

Performance alerts surface high-impact or large-scale performance issues across your environment. While events provide fine-grained visibility into all occurrences of performance issues matching defined thresholds on individual endpoints, alerts generate an additional notification when specific events occur regularly on one or more endpoints.

An alert monitor is created for each event rule that you enable on a Performance profile. When an alert monitor detects that the alerting threshold for the event rule is met, it generates an alert and sends the alert to Performance.

For example, if a software update causes CPU events to occur repeatedly across a large number of endpoints, an alert monitor for the CPU Critical event rule notifies you when the number of affected endpoints crosses the configured threshold. You can then act on the widespread issue rather than discover it by manually reviewing the Events page.

Monitor, manage, and configure alerts from the following locations:

- **Performance** > **Management > Profiles**: Enable alert monitors in the profile configuration for each event rule type. For more information, see Managing profiles on page 46.
- **Performance** > **Management > Alert Monitors**: When you enable an alert for an event rule in a Performance profile, Performance creates an alert monitor. For more information, see Manage alert monitors on page 124.
- **Performance** > **Alerts**: Alerts are listed by type on the **Grouped Alerts** and **Individual Alerts** tabs. For more information, see Manage alerts on page 127.

Before you begin

- Confirm that Tanium™ Findings is installed.
- Confirm that Tanium™ Messaging Service is installed.
- Confirm that Tanium™ Connect is installed so you can export alert data.

©2026 Tanium Inc. All Rights Reserved

Manage alert monitors

About this task

Performance creates alert monitors after you enable and configure alerts for a profile. Alert monitor names are derived from their associated profile title and event rule type. For example, **<profile-title> - Disk Capacity**.

View alert monitors

About this task

View alert monitors to check their status and ensure that they are healthy and receiving findings. You can also open each alert monitor to view details including alert summaries and event rule configuration.

1. From the Main menu, go to **Performance** > **Management > Alert Monitors**.
2. (Optional) Filter the grid with the following methods. The grid lists only the rows that match all filters that you specify:
   - Click a status or health status.
   - Expand the **Filters** section and enter text in a filter field to match text to the corresponding grid column.
3. View information about the alert monitors in the grid, including the alert monitor status.

Icon	Status	Description
	Triggered	The alert monitor is active and is currently alerting.
	Idle	The alert was dismissed or is not yet triggered.
	Silenced	The alert monitor was dismissed or silenced. Performance does not receive alerts for the selected amount of time: 1 hour, 12 hours, 1 day, 3 days or 7 days.  **Note:** Auto-silencing: When an alert is dismissed, the alert monitor automatically silences for an hour. This hour gives the Tanium platform enough time to deploy a Tanium action that dismisses the alert on the impacted endpoints.

©2026 Tanium Inc. All Rights Reserved

Icon	Status	Description
	Disabled	The alert configuration is not enabled in the profile.

4. Review the health of each alert monitor.

Icon	Status	Description
	Healthy	The alert monitor is healthy and receiving findings for alerting endpoints.
	Unhealthy	The alert monitor has reached its maximum of 1,000 findings and cannot receive new findings. Dismiss or resolve alerts to receive new findings and restore it to a healthy state.

5. Click the title of an alert monitor to go to **Alert Monitor Details**. This page provides information about the alert monitor and lets you take action on the endpoints that triggered the alert monitor. The following tabs provide status, configuration, and diagnostic information:
    - **Alerts Summary**: This tab provides an overview of the alerts that were triggered by the alert monitor. The **Alert Summary** section provides a grid that lists the alerts. You can filter by alert status, and you can filter individual alerts by online status. You can also expand the **Filters** section to filter by **Rule Type** and **Profile**. To view information about an alert, click Alert Detail to open a side panel that shows a summary of the alert.

      You can select the checkbox on one or more alert rows to show options to update the alert status, including **Mark as In Progress**, **Dismiss**, and **Resolve**. For individual alerts, you can click Direct Connect to Endpoint in the **Actions** column to open a Direct Connect session to the endpoint. For more information, see Connecting directly to endpoints on page 76.

      Monitor Timeline shows each change in alert monitor status over the period selected in **Timeframe**. You can filter timeline data by status. To see when the status of the monitor changed, hover over an icon to view the date, time, and user who changed the status.

    - **Configuration**: This tab provides an overview of the event rule configuration for the event that triggered the alert and the configured thresholds for triggering the alert.

    - **Group Diagnostics** (grouped alerts only): Before an alert is triggered, this tab shows

©2026 Tanium Inc. All Rights Reserved

the **Ungathered Endpoint Summary** section that provides a dashboard that tracks endpoint performance as the endpoints in the group approaches alert thresholds. The dashboard includes the following charts.

Chart	Description
Total Alerts Triggered	Total number of alerts that the alert monitor triggered
Online Endpoints with Findings	Total number of online endpoints with findings **Note:** This number includes all endpoints, not only those that are visible to you through RBAC permissions. This number might differ from the number that appears in the **Endpoint Findings** section, which is subject to RBAC permissions.
Maximum Endpoint Count Over the Last Week	Maximum number of endpoints in the last week, aggregated every hour
Maximum Endpoint Count Over the Last 30 Days	Maximum number of endpoints in the last 30 days, aggregated every 24 hours

After a grouped alert is triggered, the **Grouped Diagnostics** tab shows **Ungathered Endpoint with Findings**. Go to **Alert Summary** to view details about the alert.

Silence or disable an alert monitor

You can silence or disable an alert monitor on the **Alerts Monitor Detail** page. For example, you might want to silence an alert monitor before you perform maintenance that might trigger alerts.

1. From the Main menu, go to **Modules** > **Performance > Management** > **Alert Monitors**, and then click the title of an alert monitor.
2. Review the **Alert Summary**, **Configuration**, and **Grouped Diagnostics** (grouped alerts only) tabs. For more information, see View alert monitors on page 124.
3. (Optional) To silence the alert monitor temporarily, click **Silence** and select a time period.

©2026 Tanium Inc. All Rights Reserved

When you silence an alert monitor, no further alerts are sent to Performance for the selected period of time. You might want to do this if you are pushing out changes to endpoints that might cause alerts to trigger.

You can view how much longer alert monitor is silenced in the **Silence Time Remaining** field located at the top of the **Alert Summary** tab on **Alert Monitor Details**.

> **Note:** After you silence an alert monitor, an **Unsilence Monitor** option appears. Unsilence an alert monitor only if you silenced the monitor yourself, as opposed to Tanium auto-silencing the monitor. If you unsilence a monitor before the silence time frame passes, it is possible that the alert triggers again within a few minutes.

4. (Optional) To disable the alert monitor, click **Disable**. When you disable an alert monitor, the **Alert Monitor Configuration** option in the profile that enabled this alert clears and the alert monitor configuration for the event rule is no longer active.

Manage alerts

View alerts

About this task

You can view the status and details about grouped and individual alerts. This information helps you manage, triage, and remediate issues in your environment.

1. From the Main menu, go to **Performance** > **Alerts**. You can also view a specific alert on the **Alert Summary** tab of the alert monitor that triggered the alert.
2. (Optional) Filter alerts by **Computer Group** or **Timeframe**.
3. Review the **Metrics** section for high-level data insights about the alerts. You can hover over the charts to see what percentage of the total alerts the data represents.
4. View information about the alerts in the alerts grid, including the alert status.

Icon	Status	Description
	Unresolved	The alert was opened and is ready for review.

©2026 Tanium Inc. All Rights Reserved

Icon	Status	Description
	In Progress	The alert was moved to the in-progress status.
	Resolved	The alert was moved to the resolved status.
	Dismissed	The alert was moved to the dismissed status. **Note:** Auto-silencing: When an alert is dismissed, the alert monitor is automatically silenced for an hour. This hour gives the Tanium platform enough time to deploy a Tanium action that dismisses the alert on the impacted endpoints.

5. Review alerts on the **Grouped Alerts** tab.
    a. In the alerts grid, click Alert Details to open a side panel to view information about the grouped alert, including the alert status, event rule configuration, total endpoint count, and the health status of its alert monitor.
    b. Click the alert ID to view details about endpoints that are sending the grouped alert, including alert details, event rule configuration information, and endpoint findings. The **Endpoint Findings** section has a summary section and a findings grid. You can filter the grid by **Online** status, **OS Platform**, **Performance Score**, and **Criticality**. For more information about performance scores, see Performance scores on page 10. For more information about criticality levels, see Endpoint Criticality.

    In the findings grid, click Finding Details to open a side panel to view information about the endpoint findings, including alert evidence from the most recent event that triggered the alert. To view all event findings that triggered an alert, click **Actions** and open a Direct Connect session to the endpoint.

    Note: The numbers in **Endpoint Findings** include only endpoints that are visible to you through RBAC permissions.

6. Review alerts on the **Individual Alerts** tab.
    a. You can click **Actions** and select **Direct Connect to Endpoint** to open a Direct Connect session to the endpoint.
    b. In the alerts grid, click Alert Details to open a side panel to view information about the alert, including the alert status, performance score, criticality, event rule configuration, and the health status of its alert monitor.

©2026 Tanium Inc. All Rights Reserved

Change the status of an alert

About this task

You can update the status of an alert to reflect whether the alert is being addressed or has already been resolved. This helps you track and manage alerts more effectively.

1. From the Main menu, go to **Modules** > **Performance > Alerts** and find the grouped or individual alert that you want to change.
2. Review alert, configuration, and endpoint details. For more information, see View alerts on page 127.
    - For grouped and individual alerts, click Alert Details to open a side panel with a summary of the alert.
    - For grouped alerts, click the **Alert ID**.
3. When you select the checkbox on one or more alert rows, the **Mark as In Progress**, **Dismiss**, and **Resolve** buttons appear. Click **Mark as In Progress** to move an alert into the In Progress status, which makes the **Unresolve** option available. Click **Dismiss** to move an alert into the Dismissed status. Click **Resolve** to move an alert into the Resolved status.

Result

Note: When you close an alert, all options become unavailable and online endpoints are no longer visible.

Export alert data to a Connect destination

About this task

Create a connection in Tanium Connect to send alert data to Connect destinations, such as Email, File, and HTTP.

Important: You must have access to Tanium Connect with the Connect User role.

1. From the Main menu, go to **Connect** > **Connections** and then click **Create Connection**.
2. Configure the **General Information** section.

©2026 Tanium Inc. All Rights Reserved

a. Enter a name and optional description for your connection.
b. Expand the **Advanced** section and set the following options:
    - **Log level**: By default, the logging is set to **Information**. To reduce the amount of logging, you can set the log level to **Warning**, **Error**, or **Fatal**.
    - **Minimum Pass Percentage**: Minimum percentage of the expected rows that must be processed for the connection to succeed.
    - **Memory Ceiling**: Maximum memory (GB) to run the connection.

3. In the **Configuration** section, set the **Source** and **Destination** as follows:
    a. For the **Source**, select **Event**.
    b. For the **Event Group**, choose from the following options:
        - To send alert data, select **Tanium Performance** and then enable the **New Performance Alert** option.
        - To send alert monitor data, select **Tanium Performance - Alert Monitors** and then select one or more alert monitors.
    c. Select a connection destination from the **Destination** list. Provide the configuration information for the destination that you selected. For more information on configuring destinations, see Tanium Connect User Guide: Connection destinations.
4. Configure the **Configure Output** section:
    a. (Optional) Configure a **Filter**.
    You can use filters to modify the data that you are getting from your connection source before it is sent to the destination.

    For more information about the types of filters you can configure, see Tanium Connect User Guide: Reference: Filtering options.

    b. Configure the **Format** for the data. For information on configuring the format, see the section on the destination type that you selected in Tanium Connect User Guide: Reference: Format types.
    c. (Optional) Expand **Columns** to customize columns for the exported data. Select the available **Source** items and configure the **Destination Label**, **Value Type**, and **Customization**. For more information on customizing columns, see the **Format Data for <destination type>** section for the destination type. For example, for more information about customizing columns for Email (SMTP), see Tanium Connect User Guide: Format data for email.

©2026 Tanium Inc. All Rights Reserved

> **Note:** Customizing columns does not add new rows, but rather adds columns to existing rows.

5. In the **Enablement** section, select **Listen for this Event**. In this case, the connection runs when a configured event is detected. Connections for this event type cannot be scheduled or run manually.
6. Click **Save**.

©2026 Tanium Inc. All Rights Reserved

Managing stream configurations

About this task

Use stream configurations to define an external destination to which Performance can stream events. After you create a stream configuration, you can select to use the configuration in new and existing profiles.

- You must have a role with the **Performance Stream read** permission to view stream configurations.
- You must have a role with the **Performance Stream write** permission to create and modify stream configurations.

By default, Performance streams data to the destination every five minutes. If the data cannot be sent to the destination successfully, it is cached on the endpoint. By default, up to 10 events can be cached before events are dropped.

If multiple events occurred on an endpoint in the previous five minutes, then these events are sent in a single message to the stream destination. The data is sent in JSON format. Multiple events are sent in newline delimited JSON (NDJSON) format.

If an event is ongoing, Performance continues to stream data about the event every five minutes until the event is over. For example, if a disk space event started three days ago and is still ongoing, Performance streamed data about this event every five minutes for the past three days.

View stream configurations

To view the **Stream Configurations** page, go to **Performance** > **Management > Stream Configurations**.

The following actions are available:

©2026 Tanium Inc. All Rights Reserved

Stream Configuration options

Option	Description
View stream configuration	In the **Stream Configuration Name** column, click the configuration to view configuration details.
View associated profile	In the **Associated Profiles** column, click the name of a profile to open the **Profile Details** page for the profile.
View result metrics	In the **Result Metrics** column, click View Metrics in Interact to view daily stream statistics.
Create stream configuration	Click **Add Stream Configuration** . For more information, see Create a stream configuration on page 133 .
Edit stream configuration	In the **Actions** column of the stream configuration that you want to edit, click Edit . For more information, see Edit a stream configuration on page 135 .
Delete stream configuration	In the **Actions** column of the stream configuration that you want to delete, click Delete . For more information, see Delete a stream configuration on page 135 .
Filter by text	Enter an alphanumeric string in the **Filter items** field to match text in any column.

Create a stream configuration

1. From the Performance menu, go to **Management** > **Stream Configurations** and then click **Add Stream Configuration**.
2. In the **Summary** section, enter a **Name** and optional **Description**.
3. By default, the **Dry Run** option is enabled when you create a stream configuration. When this setting is enabled, no data is streamed to a destination, but you can analyze the amount of event data that would be streamed to a destination. If you want to run the stream configuration without testing, clear the **Dry Run** option.

   Tip: Use the sensor to gain an understanding of the amount of data that would be sent.

©2026 Tanium Inc. All Rights Reserved

4. In the **Configuration** section, select a **Destination Type**. The **Destination Type** that you select determines the additional required configuration settings.

   ELK

   - URL: The URL for Logstash HTTP input.
   - Allow Untrusted Certificate (less secure): Select to disable the validation of the certificate presented by the destination.
   - Proxy Enabled: If a proxy is in use, select this option and then provide the proxy details.

   Splunk HEC

   - URL: The URL to access the Splunk REST API.
   - Authorization Token: The authorization token to access your Splunk environment. Do not include the `Splunk` prefix in this token.
   - Allow Untrusted Certificate (less secure): Select to disable the validation of the certificate presented by the destination. By default certificate validation is performed.
   - Proxy Enabled: If a proxy is in use, select this option and then provide the proxy details.

   Splunk TCP

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

   Tip: If security software is in use in the environment to monitor and block unknown host system processes or ports, ensure that a security administrator creates exclusions to allow the stream configurations to run without interference.

5. When finished, click **Submit**.

Result

You can now use the new stream configuration in profiles. For more information, see Managing

©2026 Tanium Inc. All Rights Reserved

profiles on page 46.

Tip: If you selected the **Dry Run** option to test the stream configuration, you can edit the stream configuration later and clear the **Dry Run** option to begin sending data to the destination. For more information about how to edit a stream configuration, see Edit a stream configuration on page 135.

Edit a stream configuration

About this task

When you update a stream configuration that is in use by any profiles, the profiles automatically update with the changes. The profile changes are then sent to Endpoint Configuration to distribute the profiles to endpoints. Updated profiles should be distributed within an hour, and metric monitoring and collection begins after the profile is placed on an endpoint. To immediately deploy profiles, go to the **Management** > **Profiles** page and click **Deploy All Profiles**.

Note: If you enabled configuration approvals in Endpoint Configuration, profile changes must be approved in Endpoint Configuration before they deploy to endpoints.

1. From the Performance menu, go to **Management** > **Stream Configurations**.
2. In the **Actions** column of the stream configuration that you want to edit, click Edit.
3. Modify the stream configuration as needed and then click **Submit**.

Delete a stream configuration

About this task

When you delete a stream configuration that is in use by any profiles, event streaming is automatically disabled for those profiles. The profile changes are then sent to Endpoint Configuration to distribute the profiles to endpoints. Updated profiles should be distributed within an hour, and metric monitoring and collection begins after the profile is placed on an endpoint. To immediately deploy profiles, go to the **Management** > **Profiles** page and click **Deploy All Profiles**.

©2026 Tanium Inc. All Rights Reserved

Tip: You can see which profiles use the stream configuration in the **Associated Profiles** column on the **Stream Configurations** page. You can edit the profiles to re-enable streaming with a different stream configuration.

1. From the Performance menu, go to **Management** > **Stream Configurations**.
2. In the **Actions** column of the stream configuration that you want to delete, click Delete .

©2026 Tanium Inc. All Rights Reserved

Maintaining Performance

About this task

Perform regular maintenance tasks to ensure that Performance successfully performs scheduled activities on all the targeted endpoints and does not overuse endpoint or network resources. If Performance is not performing as expected, you might need to troubleshoot issues or change settings. For more information about related procedures, see Troubleshooting Performance on page 141.

Performance monthly maintenance

1. From the Main menu, go to **Modules** > **Performance** to open the Tanium™ Performance **Overview** page.
2. Scroll to the **Health** dashboard to verify that Performance tools are installed on all endpoints and to review which profiles are applied to endpoints.
3. To investigate endpoints that do not have Performance tools installed, click the number above **Needs Attention** or **Unsupported** in the **Performance Coverage** panel. The Tanium Server issues a question that returns the computer name, operating system, IP address, and Performance coverage status for the affected endpoints.

   Tip: You can also issue the question `Get Performance - Configured from all machines` through the **Ask a Question** field in Interact and then drill down on results to investigate endpoints that have issues with Performance tools or configuration. For more information, see Managing question results.
4. To review the status, priority, and endpoint targeting of all profiles, click **Active Profiles**. For more information, see Managing profiles.
5. To review the entire configuration of a specific profile, click its name in the **Active Profiles** panel.
6. For more information about how to troubleshoot installation issues related to Performance tools or profiles, see Monitor and troubleshoot Performance coverage.

©2026 Tanium Inc. All Rights Reserved

Monitor and troubleshoot Performance Coverage

The following table lists contributing factors into why the Performance coverage metric might report endpoints as **Needs Attention** or **Unsupported**, and corrective actions you can make.

Tanium Performance coverage metric issues and resolutions

Contributing factor	Corrective action
Endpoints do not have a Performance profile installed	In Interact, ask the **Get Performance - Configured from all machines** question. The results from this question will tell you why an endpoint was classified as **Needs Attention**. If the status for the endpoint is **Needs Profile**, check that the computer groups in your profiles cover all of the endpoints that you want to monitor.
Endpoints do not have the Performance tools installed	In Interact, ask the **Get Performance - Configured from all machines** question. The results from this question will tell you why an endpoint was classified as **Needs Attention**. If the status for the endpoint is **Needs Tools**, ensure that all operating systems supported by Performance are included in the Performance and Direct Connect action groups. Membership in these action groups determines which endpoints receive the Performance and Direct Connect tools, which are required for Performance operations.
Endpoints do not have a supported version of the Tanium Client installed	In Interact, ask the **Get Performance - Configured from all machines** question. The results from this question will tell you why an endpoint was classified as **Needs Attention**. If the status for the endpoint is **Not Configured** with details that state **Needs Tanium Client Upgraded**, upgrade the Tanium Client on the endpoint to a version that is supported by Performance. For more information about supported versions, see Performance requirements on page 22.
Endpoints do not have enough free disk space	In Interact, ask the **Get Performance - Configured from all machines** question. The results from this question will tell you why an endpoint was classified as **Needs Attention**. If the status for the endpoint is **Not Configured** with details that state **Needs More Disk Space**, free up disk space on the endpoint. For more information on disk space requirements, see Disk space requirements on page 26.
The Tanium TSDB is disabled on the endpoint	In Interact, ask the **Get Performance - Configured from all machines** question. The results from this question will tell you why an endpoint was classified as **Needs Attention**. If the status for the endpoint is **Not Configured** with details that state that **Tanium TSDB is disabled**, check

©2026 Tanium Inc. All Rights Reserved

Contributing factor	Corrective action
	to confirm that the endpoint is currently targeted by a profile. If the endpoint is currently targeted by a profile, but the **Performance - Configured** sensor still reports that Tanium TSDB is disabled on the endpoint, contact Tanium Support for assistance. For more information, see Contact Tanium Support on page 147 .
Endpoints are not running a supported operating system	In Interact, ask the **Get Performance - Configured from all machines** question. If the result of this question is **Unsupported** , the endpoint operating system is not supported by Performance. For more information about supported operating system versions, see Supported operating systems on page 25 .

Monitor and troubleshoot endpoints with performance events

The following table lists contributing factors into why endpoints might have a higher number of performance events, and corrective actions you can make.

Tanium Performance performance events issues and resolutions

Contributing factor	Corrective action
Resource intensive software	• Consult the vendor. • Investigate other software interference (security software exclusions). • Investigate commonalities in software versions on affected machines.
Poorly performing hardware	Consider replacing the models or upgrading their hardware.
Event thresholds poorly defined	Consider raising thresholds and durations in one or more profiles.
System Crashes	• Check for out-of-date driver versions. • Research causes of numerous bugcheck IDs. • Out of date BIOS or Firmware versions. • Out of date or known bad kernel-mode drivers. • Faulty hardware.

©2026 Tanium Inc. All Rights Reserved

Contributing factor	Corrective action
Low Disk Capacity	• Investigate what is using disk space. • Free up disk space. • Increase disk space available to users. • Expand virtual volumes. • Upgrade disks in physical machines.
Application Crashes	• Consult the software vendor • Use the file browser in Direct Connect sessions to retrieve log or dump files and investigate them.

©2026 Tanium Inc. All Rights Reserved

Troubleshooting Performance

About this task

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

Collect logs

About this task

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

1. From the Main menu, go to **Modules** > **Performance** to open the **Overview** page.
2. Click Help ? and then click the **Troubleshooting** tab if needed.
3. Collect the troubleshooting package. Click **Generate Support Package**. When the ZIP file is ready, click **Download Support Package**.
4. Contact Tanium Support to determine the best option to send the ZIP file. For more information, see Contact Tanium Support on page 147.

Collect troubleshooting information from endpoints

About this task

You can use Client Management to directly connect to an endpoint and collect a bundle of logs and other artifacts, sometimes referred to as an *Endpoint Must Gather* (EMG).

1. From the Main menu, go to **Shared Services** > **Client Management**.
2. From the Client Management menu, click **Client Health**.
3. In the **Single Endpoint View** search box, enter all or part of an IP address or a computer name.
   Matching results appear after the search completes.
4. From the search results, click the computer name.

©2026 Tanium Inc. All Rights Reserved

Client Management opens the Endpoint Details page in Single Endpoint View (SEV).

5. Click the **Client Health** tab and, if the endpoint is not yet **Connected**, click **Direct Connect**.
6. In the **Available Steps** grid, select the domains (types of logs and artifacts) for which you want to gather troubleshooting information.
   For Patch information, select the **Core** and **Patch** domains.

   For Comply information, select the **Comply** domain and then select **Comply Database**, **Comply Extension Data**, and **Comply Intel**.

   For Endpoint Management for Operational Technology entity provider information, select the **Core** domain and then select **Tanium Client Logs**. Select the **Entity** domain and then select **Config Data**, **Entity Log**, and **Entity Provider Metadata**.
7. Click **Gather from Endpoint**.
   The selected logs and artifacts are gathered from the endpoint. The package appears in the **Must Gathers** section, and the name of the package corresponds with its time stamp.
8. When **Finished** appears in the **Run State** column, select the package and click **Download** to download a ZIP file that contains the troubleshooting information.
   For more information about collecting troubleshooting information in Single Endpoint View, see Tanium Reporting User Guide: Collect troubleshooting information.

   For more information about how to connect directly to endpoints, see Tanium Direct Connect User Guide.

   For more information about Client health features in Client Management, see Tanium Client Management User Guide: Monitor the Client health overview in Client Management and Tanium Client Management User Guide: Access detailed Client health and troubleshooting information on an endpoint.

Alerts are not triggering

If you enabled alerts, and they are not triggering, check the following possible issues:

Configuration issue

If you are not receiving alerts, you can check the following configuration items:

©2026 Tanium Inc. All Rights Reserved

- Confirm the profile that has alerts enabled has been deployed. There should be a green check in the **Status** column on the **Profiles** list page.
- Confirm the alert monitor is not silenced or disabled. Check the **Status** column on the **Alert Monitor** list page.
- In the **Profile** configuration, check that the threshold settings are not set too high. Default threshold settings for alerts are 5 triggered events on at least one endpoint over a period of one hour.

Service issue

If you are not receiving alerts, you can check the services:

INFORMATION FLOW OVERVIEW

When the alerting criteria configured in a Performance Profile is met on the endpoint, the match of that criteria is a Finding. The Findings Service monitors endpoints for active findings and broadcasts that information over the Message Bus Service. The Performance Service listens to the Message Bus Service for the Findings counts and triggers alerts based on those counts. When an alert is acknowledged, the Performance Service tells the Findings Service to dismiss the finding, which in turn, causes the endpoint to stop reporting the finding.

Check the Message Bus Service connection to the Findings Service:

1. From the Main menu, go to **Modules** > **Performance** to open the **Overview** page.
2. Click Info and verify that the **Message Bus** section shows the following information:
    - Connected: **Yes**
    - Subject: **tanium.findings.heartbeat** should be received every minute
    - Subject: **tanium.findings.performance.summary** should be received whenever an alert monitor has a nonzero endpoint count

Sync alert data

About this task

©2026 Tanium Inc. All Rights Reserved

Important:

Review the following considerations before you sync alert data:

- You must have a role with the **Performance Settings Writer** permission to sync alert data. Roles with this permission include **Performance Administrator** and **Performance Operator**.
- Syncing alert data might consume significant system resources.

If Performance alerts do not reflect the most current information from your environment, manually sync alert data:

1. From the Main menu, go to **Performance** > **Overview**.
2. Click Settings.
3. Under **Alerts**, click **Sync Alerts**. This synchronizes all alert data and removes any stale or corrupted alert data.

Unable to configure Retention Settings

Note: You can configure **Retention Settings** to specify the **Database maximum size** and **Database maximum days** in profiles. If you do not see these settings in an existing profile, edit the profile to specify the **Retention Settings** and then save the profile.

Error when connecting to endpoints

You must have the **Performance Direct Connect read** permission, which is provided by the Performance Administrator, Performance Read Only User, and Performance User roles, to connect directly to endpoints. You must also have the **Data Collection Registration read** Interact permission to connect directly to endpoints.

If you do not have sufficient privileges, the connection attempt fails with this error: Failed to connect to endpoint <*endpoint-computer-name*>. Failed to query for endpoints. Request failed with status code 500.

©2026 Tanium Inc. All Rights Reserved

Remove Performance tools from endpoints

About this task

You can deploy an action to remove Performance tools from an endpoint or computer group. Separate actions are available for Windows and non-Windows endpoints.

1. In Interact, target the endpoints from which you want to remove the tools. For example, ask a question that targets a specific operating system:`Get Endpoint Configuration - Tools Status from all machines with Is Windows equals true`
2. In the results, select the row for Performance, drill down as necessary, and select the targets from which you want to remove Performance tools. For more information, see Tanium Interact User Guide: Drill Down.
3. Click **Deploy Action**.
4. For the **Deployment Package**, select **Endpoint Configuration - Uninstall Tool [Windows]** or **Endpoint Configuration - Uninstall Tool [Non-Windows]**, depending on the endpoints you are targeting.
5. For **Tool Name**, select Performance.
6. (Optional) By default, after the tools are removed they cannot be reinstalled. To allow tools to be automatically reinstalled, clear the selection for **Block reinstallation**. Re-installation occurs almost immediately.

   Note:

   If reinstallation is blocked, you must unblock it manually:

   - To allow Performance to reinstall tools, deploy the **Endpoint Configuration - Unblock Tool [Windows]** or **Endpoint Configuration - Unblock Tool [Non-Windows]** package (depending on the targeted endpoints).
   - If you reinstall tools manually, select **Unblock Tool** when you deploy the **Endpoint Configuration - Reinstall Tool [Windows]** or **Endpoint Configuration - Reinstall Tool [Non-Windows]** package.
7. (Optional) To remove all Performance databases and logs from the endpoints, clear the selection for **Soft uninstall**.

©2026 Tanium Inc. All Rights Reserved



CAUTION: When you perform a hard uninstallation of some tools, the uninstallation also removes data that is associated with the tool from the endpoint. This data might include important historical or environmental data. If data that you want to keep is associated with the tool, make sure you perform only a soft uninstallation of the tool.

8. (Optional) To also remove any tools that were dependencies of the Performance tools that are not dependencies for tools from other solutions, select **Remove unreferenced dependencies**.
9. (Optional) In the **Deployment Schedule** section, configure a schedule for the action.

Tip: If some target endpoints might be offline when you initially deploy the action, select **Recurring Deployment** and set a reissue interval.

10. Click **Show preview to continue**.
11. A results grid appears at the bottom of the page showing you the targeted endpoints for your action. If you are satisfied with the results, click **Deploy Action**.



Note: If you have enabled Endpoint Configuration approval, tool removal must be approved in Endpoint Configuration before tools are removed from endpoints.

Verify endpoint tools

If you are experiencing issues such as a feature not working on an endpoint or seeing incorrect data in the workbench, confirm that your endpoints have the latest toolset version.

For more information, see Tanium Endpoint Configuration User Guide: Identify and resolve issues with endpoint tools or Client Extensions and Reference: Client extensions and endpoint tools used for Tanium solutions.

Uninstall Performance

1. From the Main menu, go to **Administration** > **Configuration** > **Solutions**.
2. Select the checkbox in the Performance section, and then click **Uninstall**.

©2026 Tanium Inc. All Rights Reserved

3. Review the content that will be removed and click **Uninstall**.

4. Return to the **Solutions** page and verify that the **Import** button is available for Performance.

> **Note:** By design, the uninstall process does not remove Performance content (packages, saved questions, and sensors) so that other solutions are not impacted if they use this content. If you are sure that this content is not being used by any other solutions, you can manually remove it.

Contact Tanium Support

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

For more information about submitting a support case, see Case Submission Form.

©2026 Tanium Inc. All Rights Reserved

Reference: Performance Advanced Settings

You can manage settings that control Tanium Performance such as configuring process groups.

Configure process groups

By default, Performance aggregates metrics collected for processes with the same name and displays the aggregated metrics. For example, if an endpoint has multiple named BusinessApp processes running, after you establish a direct connection to the computer and viewing historical performance information, only one BusinessApp process displays.

> **Note:** Processes with the same name are aggregated, even if each process runs from a different command line filepath.

Process groups affect the collection and display names of processes, which change how Performance aggregates and displays metrics. Process groups have two primary purposes:

- The most common purpose is to separate processes which would be grouped together by default, to view separate metrics for each process. This is most useful when troubleshooting specific applications that might run multiple processes with the same name, each of which does different things. For example, Windows runs multiple svchost.exe processes during normal operation. You can display separate metrics for each individual svchost.exe process.
- The next most common purpose is to group processes with different names when Performance aggregates metrics. The process name displayed is the **Replacement** text that the user enters. For example, a process named foo and a process named bar can have their metrics combined and shown as a single process named baz. All metrics views and Performance sensors display the name baz for this process group, instead of foo or bar.

©2026 Tanium Inc. All Rights Reserved

Note: The `Performance - Application Metric Analysis` sensor allows users to graph or report on metrics from multiple processes that might comprise a single application without affecting the underlying data that Performance captures.

Important: A process group is an advanced setting in Performance. For assistance with any process group configuration, Contact Tanium Support on page 147.

1. From the Main menu, go to **Modules** > **Performance > Management** > **Process Groups** and then click **Create Process Group**.
2. In the **When** section, select a replacement process name definition:
   - To match a command run at a command prompt, select **Command Line**.
   - To match a process name, select **Process Name**.
3. In the **Matches** section, enter a **Regular Expression** to match the command or process. You can enter either a regular expression or a URL to a website that validates regular expressions.

   For example, if the command line for a process is TestProcess.exe --test-cmd, then a matching regular expression is:

   ```
   ^.*TestProcess(?:\.exe)?.+--test-cmd.*$
   ```

   The following example regular expression validation URL matches the process string TestProcess.exe --test-cmd:

   ```
   https://regex101.com/r/wMVNFd/1
   ```
4. In the **Replace With** section, enter **Replacement** text if the regular expression matches a process or command.
5. Click **Submit**.
6. Update the profile targeting the computer group. For more information, see Modify a profile on page 51.
7. To verify that the process group works, establish a direct connection with a targeted

©2026 Tanium Inc. All Rights Reserved

endpoint and view the Live Process Monitor. Add the **Process Group Name** and **Command Line** columns to the view. For more information, see Create a direct connection on page 77 and View the Live Process Monitor on page 79.

©2026 Tanium Inc. All Rights Reserved

Reference: Event Rules

Use event rules to specify the heuristic parameters for which the targeted endpoints report performance events.

You can configure these event rules:

- Application Crashes on page 152
- Available Memory on page 152
- CPU Critical on page 152
- Disk Capacity on page 153
- Disk Latency on page 153
- System Crashes on page 154
- Process Network Latency on page 154
- Network Outage on page 154
- WiFi Signal on page 155
- Boot Time on page 155
- Logon Time on page 155

Profiles and the event rules that they contain do not determine what data is collected on endpoints. The same data is monitored on all endpoints that a profile targets. Profiles determine which conditions on the endpoint generate a negative performance event.

After you add an event rule to a profile, select and configure the heuristics that you want to monitor.

©2026 Tanium Inc. All Rights Reserved

Application Crashes

You can monitor this event rule on Windows and macOS endpoints.

This event rule monitors the Windows Event Log for targeted Windows endpoints and DiagnosticsReports for targeted macOS endpoints. An event occurs if an application crashes.

Available Memory

You can monitor this event rule on Windows, macOS, and Linux endpoints.

Create event rules for available memory by MB, percentage of total memory, or both.

Available Memory is a measurement of the amount of memory available to be immediately allocated to programs. Paging occurs when an endpoint runs low on available memory, which puts a load on disks and might result in workstation slowdowns or hangs. Monitor available memory to detect when programs might not have enough available memory to run without paging.

In the **Duration** field, specify the amount of time that the specified conditions must be present to trigger a performance event.

CPU Critical

The **CPU Critical** event rule contains three heuristics:

1. **CPU Utilization** and **Kernel Time** monitoring is supported Windows, macOS, and Linux endpoints. With this heuristic, you can monitor:

    - **CPU Utilization**: Monitor CPU utilization to detect CPU contention.
    - **Kernel Time**: Monitor kernel time to detect when the CPU is spending too much time on kernel mode operations.

      CPUs operate in two modes: kernel mode and user mode. Kernel mode is typically used for core operating system functions, I/O, and filter driver operations. If the CPU on an endpoint spends the majority of time on kernel mode operations, little CPU time is available for user mode operations, which might cause a negative

©2026 Tanium Inc. All Rights Reserved

performance condition.

2. **DPC time** monitoring is supported only for Windows endpoints.

   If you configure an event rule for **DPC time**, processor DPC for targeted endpoints is monitored. Specify the highest DPC time that is allowed on an endpoint before a performance event occurs. An unusually high amount of time spent on deferred procedure calls on an endpoint could indicate a processor bottleneck or driver problem.

3. **Load Average** monitoring is supported only for macOS and Linux endpoints.

   If you configure an event rule for **Load Average**, the load average for targeted endpoints is monitored. Specify the load average that is allowed on an endpoint before a performance event occurs.

   The load average is an exponential average of the number of processes in a running or waiting state. This metric is a standard UNIX method for detecting CPU contention. This rule monitors the 15 minute load average for the CPU. If the load average is equal to the number of cores on an endpoint, the CPU usage is at its maximum capacity.

In the **Duration** field, specify the amount of time that the specified conditions must be present to trigger a performance event.

Disk Capacity

You can monitor this event rule on Windows, macOS, and Linux endpoints.

You can create an event rule for free disk space by MB, percentage of total disk capacity, or both.

Disk capacity is a measurement of the free disk space on a logical drive. When disks run low on space, fragmentation increases. Fragmented disks contribute to slow response times.

Disk Latency

You can monitor this event rule on Windows, macOS, and Linux endpoints.

Create event rules for **Read Latency**, **Write Latency**, or both.

©2026 Tanium Inc. All Rights Reserved

Disk latency is a measurement of the average amount of time that an operation (read or write) takes to complete on a physical drive.

In the **Duration** field, specify the amount of time that the specified conditions must be present to trigger a performance event.

System Crashes

You can monitor this event rule only on Windows endpoints.

This event rule monitors the Windows System and Event Logs for targeted endpoints. An event occurs if the system crashes.

Process Network Latency

You can monitor this event rule only on Windows and macOS endpoints.

This event rule uses the 10 slowest processes running on the system to calculate the average process latency. An event triggers if the latency of a process is greater than the set amount, and it exceeds the calculated the average process latency on the system.

Network Outage

Create an event rule for client registration failures, internet disconnects, or both.

Client Registration Failures

A network outage event is created when the Tanium Client fails to register.

Internet Disconnected

You can monitor this event rule only on Windows and macOS endpoints.

A network outage event occurs when an endpoint is disconnected from the Internet for the selected

©2026 Tanium Inc. All Rights Reserved

duration.

> **Note:** To determine when internet disconnects occur, Performance monitors the network properties returned by the Windows Network Location Awareness (NLA) service. If your security settings block the sites that the NLA service uses to detect internet connectivity, a network outage event is created. For more information, see Microsoft Learn: NCSI active probes and the network status alert.

WiFi Signal

You can monitor this event rule only on Windows and macOS endpoints that have WiFi adapters. If there are no WiFi metrics available, the WiFi charts will not appear.

This event type monitors WiFi signal quality and triggers if the quality drops below the specified percentage for a set period of time.

Boot Time

You can monitor this event rule to detect when endpoints take too long to start. Performance Boot Time is the duration from when the endpoint is turned on to when the endpoint prompts the user to sign in.

You can configure the boot time threshold to determine when to capture a boot time event. To configure boot time threshold, you must enable **Data Collection: Boot Time and Logon Time** in a profile. For more information, see Managing profiles on page 46.

Logon Time

You can monitor this event rule to detect when Windows endpoints take too long to sign in. Performance Logon Time is the duration from when a user submits credentials at a sign in screen to when the endpoint presents a usable desktop, as indicated by the presence of the Windows start bar. Locking and unlocking the workstation does not contribute to a logon event.

You can configure the logon time threshold to determine when to capture a logon event. To configure

©2026 Tanium Inc. All Rights Reserved

logon time threshold, you must enable **Data Collection: Boot Time and Logon Time** in a profile. For more information, see Managing profiles on page 46.

©2026 Tanium Inc. All Rights Reserved