

Tanium™ Integrity Monitor User Guide

Autonomous IT. Unstoppable Business.

2026H1 Semiannual Release

Version 3.8

May 28, 2026

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

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

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

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

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

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

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

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

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

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

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

© 2026 Tanium Inc. All Rights Reserved

© 2026 Tanium Inc. All rights reserved.

Table of contents

Integrity Monitor overview **11**

File and registry monitoring 11

Rules and labels 11

Interoperability with other Tanium products 11

ServiceNow 11

Tanium Connect 12

Tanium™ Reporting 12

Integrity Monitor - Health 12

Integrity Monitor - Summary 12

Gaining organizational effectiveness with Integrity Monitor **13**

Change management 13

RACI chart 13

Organizational alignment 17

Operational metrics 18

Integrity Monitor maturity 18

Benchmark metrics 18

Integrity Monitor 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 24

Supported operating systems 24

© 2026 Tanium Inc. All Rights Reserved

Disk space requirements ... 26
CPU and memory requirements ... 26
Permission recording requirements ... 26
Client Recorder Extension ... 26
Tanium Event Recorder Driver ... 26
Third-party software ... 26
Host and network security requirements ... 27
Ports ... 27
Security exclusions ... 27
User role requirements ... 59
Installing Integrity Monitor ... 64
Before you begin ... 64
Import Integrity Monitor with default settings ... 64
Import Integrity Monitor with custom settings ... 65
Manage solution dependencies ... 66
Upgrade Integrity Monitor ... 66
Verify Integrity Monitor version ... 66
Configuring Integrity Monitor ... 67
Prepare Endpoints ... 67
(Windows) Configure permission recording ... 67
Remove legacy Client Recorder Extension ... 68
Install and configure Tanium Endpoint Configuration ... 68
Manage solution configurations with Tanium Endpoint Configuration ... 68
Configure Integrity Monitor ... 70
(Optional) Configure Automatic Deployment on Upgrade ... 70
Configure the Integrity Monitor action group ... 70
Organize computer groups ... 71
Set up Integrity Monitor users ... 71
Upgrading Integrity Monitor ... 74
Upgrading from a version earlier than 3.0 ... 74

© 2026 Tanium Inc. All Rights Reserved

Review changes related to removal of server-side storage of labels ... 74
Update sensors in saved questions ... 75
Add filters to saved questions for change types ... 76
Review monitor and watchlist targeting ... 76
Review monitor settings ... 77
Review paths that include symbolic links ... 78
Review registry paths, inclusions, and exclusions that specify values ... 78
Review path inclusions and exclusions that include wildcard characters ... 79
Deploy monitors, watchlists, and rules ... 79
Redeploy monitors, watchlists, and rules ... 79
Configure automatic redeployment of monitors ... 80
Verify Integrity Monitor version ... 80
Managing scan settings with monitors ... 81
Create or edit a monitor ... 81
Prioritize monitors ... 83
Deploy monitors ... 84
Check the status of deployed monitors ... 85
Managing watched paths with watchlists ... 86
Before you begin ... 86
Create or edit a watchlist ... 86
Add and edit paths ... 87
Paths ... 87
Inclusions and exclusions ... 88
Add a file path ... 89
(Windows) Add a registry path ... 90
Considerations for registry paths ... 92
Determining watched subkeys ... 92
Using an abbreviation for a subtree ... 92
Using the HKEY_CURRENT_USER subtree in a path ... 92
Using a redirected registry key in a path ... 92

© 2026 Tanium Inc. All Rights Reserved

Import a path ... 92
Add paths from a file ... 93
CSV format for path imports ... 93
Add paths from templates ... 94
(Windows path style only) Update the Permission change type setting for multiple paths ... 95
Review watchlist details ... 95
Deploy watchlists ... 96
Export a watchlist ... 97
Import a watchlist ... 97
Viewing events ... 98
View events for a monitor, label, or rule ... 98
Pause and resume the event view ... 98
Download the full list of events or selected events ... 98
Use sensors to view events or event counts ... 98
Labeling events with rules ... 101
Customize labels ... 101
Use rules to automatically label events ... 101
Create a rule ... 102
Import rules ... 103
Example Tanium CSV file used to import rules ... 103
Deploy rules ... 104
Deactivate a rule ... 105
Duplicate a rule ... 105
Delete a rule ... 105
Sending and reporting events ... 106
Use Connect to send events ... 106
Create incidents for unlabeled events in ServiceNow Incident Management ... 106
Monitor for unauthorized changes with ServiceNow ... 107
Integrating with IT workflows in ServiceNow ... 108
Before you begin ... 108

© 2026 Tanium Inc. All Rights Reserved

Requirements ... 108
ServiceNow permissions required for least-privilege access ... 108
Configure the integration with ServiceNow ... 109
Specify the connection information ... 109
Configure ServiceNow mappings ... 110
Configure the schedules to synchronize data with ServiceNow ... 110
Complete the configuration ... 111
Manage authorized events ... 111
ServiceNow change requests or tasks with an Open state ... 111
ServiceNow change requests or tasks with a Closed state ... 112
ServiceNow change requests or tasks with a Canceled state ... 112
Review events ... 112
Maintaining Integrity Monitor ... 113
Monitor and troubleshoot Integrity Monitor health ... 113
Troubleshooting Integrity Monitor ... 114
Collect logs ... 114
Change the logging level ... 114
Upgrading to Integrity Monitor 3.4.97 ... 114
File permission monitoring is configured for a Windows path, but file permission events are not recorded on an endpoint ... 115
Verify endpoint tools ... 115
Identify and resolve issues with Client Extensions ... 115
Review the Extensions log for an endpoint ... 117
Uninstall Integrity Monitor ... 118
Remove Integrity Monitor tools from endpoints ... 118
Resolve issues with legacy Client Recorder Extension installations ... 119
Contact Tanium Support ... 119
Reference: Integrity Monitor endpoint tools ... 120
Reference: Endpoint monitoring health check errors ... 121
Standard cross-platform endpoint health check error messages ... 121
Standard Windows-specific endpoint health check error messages ... 122

© 2026 Tanium Inc. All Rights Reserved

Standard Linux-specific endpoint health check error messages ... 123

Reference: Gateway examples for Integrity Monitor ... 125

Create Integrity Monitor monitor ... 125

Create Integrity Monitor monitor ... 125

Create Integrity Monitor watchlist ... 129

Create Integrity Monitor watchlist ... 129

Create Integrity Monitor watchlist Unix path ... 136

Create Integrity Monitor Unix-style watchlist path ... 136

Create Integrity Monitor watchlist Windows file path ... 138

Create Integrity Monitor Windows-style watchlist file path ... 138

Create Integrity Monitor watchlist Windows registry path ... 141

Create Integrity Monitor Windows-style watchlist registry path ... 141

Delete Integrity Monitor watchlist path ... 143

Delete Integrity Monitor watchlist path ... 143

Deploy Integrity Monitor monitors ... 144

Deploy all Integrity Monitor monitors ... 145

Deploy Integrity Monitor watchlists ... 145

Deploy all Integrity Monitor watchlists ... 145

Get Integrity Monitor monitor by ID ... 146

Get Integrity Monitor monitor by ID ... 146

Get Integrity Monitor service status ... 149

Get Integrity Monitor service status ... 149

Get Integrity Monitor watchlist by ID ... 150

Get Integrity Monitor watchlist by ID ... 150

Get multiple Integrity Monitor monitors ... 154

Get multiple Integrity Monitor monitors ... 154

Get multiple Integrity Monitor watchlists ... 160

Get multiple Integrity Monitor watchlists ... 160

Mark Integrity Monitor monitors for deletion ... 167

Mark Integrity Monitor monitor for deletion ... 167

© 2026 Tanium Inc. All Rights Reserved

Mark Integrity Monitor watchlists for deletion ... 168
Mark Integrity Monitor watchlist for deletion ... 168
Update Integrity Monitor monitor by ID ... 170
Update Integrity Monitor monitor ... 170
Update Integrity Monitor watchlist ... 174
Update Integrity Monitor watchlist ... 174
Update Integrity Monitor watchlist Unix path ... 178
Update Integrity Monitor Unix-style watchlist path ... 178
Update Integrity Monitor watchlist Windows file path ... 180
Update Integrity Monitor Windows-style watchlist file path ... 181
Update Integrity Monitor watchlist Windows registry path ... 183
Update Integrity Monitor Windows-style watchlist registry path ... 183
Reference: Watchlist paths, inclusions, and exclusions ... 186
Paths ... 186
File paths ... 186
Registry paths ... 187
Determining watched subkeys ... 188
Using an abbreviation for a subtree ... 188
Using the HKEY_CURRENT_USER subtree in a path ... 188
Using a redirected registry key in a path ... 188
Path inclusions ... 189
File path inclusions ... 189
Registry path inclusions ... 193
Path exclusions ... 195
File path exclusions ... 195
Registry path exclusions ... 197
Path inclusions and exclusions used together ... 199

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor overview

With Integrity Monitor, you can simplify regulatory compliance for your enterprise by consolidating tools and accomplishing the following tasks:

- Continuously monitor critical operating system (OS), application, and log files and critical Windows registry paths.
- Deploy continuous monitoring for common or new attack vectors to any dynamic group of computers or across the enterprise.
- Go from alert to active investigation using other modules on the Tanium platform. Automatically send emails to open incidents for suspicious events in incident response systems with Tanium™ Connect.
- Automatically identify approved events based on change requests or tasks by integrating with ServiceNow Change Management.
- Automatically send events to Security Information and Event Management (SIEM) solutions; Security Orchestration, Automation and Response (SOAR) solutions; and other data lakes or log solutions for analysis and auditing with Connect.

File and registry monitoring

Define scan settings for computer groups using monitors. Then, use watchlists to specify files, directories, or Windows registry paths that you want to monitor for changes, and target the Tanium Client managed endpoints where Integrity Monitor should watch those items. After you create and deploy watchlists and monitors, Integrity Monitor records events on the included endpoints.

All monitors perform hash monitoring for files included in specified watchlists. Hash monitoring uses periodic file index scans to check for changes to the file hash or metadata of files. Hash monitoring uses the Tanium™ Client Index Extension. For more information, see Tanium Client Index Extension User Guide.

On Windows or Linux endpoints, you can optionally perform event monitoring as well. Event monitoring records real-time change events, such as create, write, delete, or rename for files or Windows registry values in specified watchlists. This method records the specific operation and the associated user or process path. Event monitoring uses the Tanium™ Client Recorder Extension. For more information, see Tanium Client Recorder Extension User Guide.

Rules and labels

Create rules to automatically label events, which can help you identify events of concern. Labels can indicate events that are expected or planned, or which events might need investigation or remediation.

Interoperability with other Tanium products

ServiceNow

The Tanium™ File Integrity Monitoring integration can automatically label events based on change requests or change tasks in ServiceNow. You can then determine which events are authorized and filter out events within authorized change windows.

For more information, see Integrating with IT workflows in ServiceNow on page 108.

© 2026 Tanium Inc. All Rights Reserved

Tanium Connect

You can access events from Integrity Monitor in Connect using saved questions.

In Tanium Connect 5.8.54 and later, you can also configure Integrity Monitor as a connection source to export watchlist data to Connect.

For more information, see Tanium Connect User Guide: Connect overview.

Tanium™ Reporting

Integrity Monitor works with Reporting for additional reporting of related data. Integrity Monitor features reports that provide data visualization of Integrity Monitor concepts.

INTEGRITY MONITOR - HEALTH

The **Integrity Monitor - Health** board displays the health status of Integrity Monitor on monitored endpoints. The **Integrity Monitor - Health** board contains the **Endpoint Health** panel.

INTEGRITY MONITOR - SUMMARY

The **Integrity Monitor - Summary** board displays information about the operation and effectiveness of Integrity Monitor based on change events on endpoints. The following panels are in the **Integrity Monitor - Summary** board:

- Endpoints by OS Platform
- Active Watchlists
- Event Count

© 2026 Tanium Inc. All Rights Reserved

Gaining organizational effectiveness with Integrity Monitor

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

- Develop a dedicated change management process. For more information, see Change management on page 13.
- Define distinct roles and responsibilities. For more information, see RACI chart on page 13.
- Track operational maturity. For more information, see Operational metrics on page 18.
- Validate cross-functional alignment. For more information, see Organizational alignment on page 17.

Change management

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

- Update SLAs for file and registry integrity monitoring activities, from identification to remediation of unapproved changes.
- Identify key resources in the organization to review and approve changes to integrity monitoring requirements to ensure minimal unexpected or unapproved changes.
- Align activities to key resources for Tanium integrity monitoring activities across security, operations, and risk/compliance teams.
- Identify maintenance windows for all integrity monitoring changes to optimize integrity monitoring effectiveness.
- Create a Tanium steering group (TSG) for integrity monitoring activities, to expedite reviews and approvals of processes that align with SLAs.

RACI chart

A RACI chart identifies the team or resource who is **R**esponsible, **A**ccountable, **C**onsulted, and **I**nformed, 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 integrity monitoring. Use the following table as a baseline example.

© 2026 Tanium Inc. All Rights Reserved

RACI chart for Tanium Integrity Monitor

Task	Security	Operations	Risk/Compliance	Executive	Rationale
Define and deploy monitors	C	R/A	R/A	I	The risk/compliance and operations teams share the responsibility of creating monitors that define the scan settings and intervals used for each computer group, in consultation with the security team. The operations team deploys the monitors to Tanium Client managed endpoints.
Define and deploy watchlists	C	C	R/A	I	The risk/compliance team creates watchlists that identify files and registry paths to be monitored, with review and input from the security and operations teams, based on regulatory compliance (such as PCI or Sarbanes-Oxley) and security requirements. The operations team deploys the watchlists to endpoints.

© 2026 Tanium Inc. All Rights Reserved

RACI chart for Tanium Integrity Monitor (continued)

Task	Security	Operations	Risk/Compliance	Executive	Rationale
Monitor events in real time	C	C	R/A	I	The risk/compliance team owns real-time monitoring and review of the events that result from creation, deletion, and changes to files or registry paths in the deployed watchlists. The security and operations teams are consulted, and all three teams review results to make adjustments to watchlists as necessary.
Use rules to apply labels	C	C	R/A	-	Labels are automatically applied by rules and, optionally, by integration with IT workflows in ServiceNow Change Management. The risk/compliance team creates rules and labels, with review and input from the operations and security teams.
Investigate unexpected events	R/A	-	C	I	The security team performs active investigations of unexpected events in consultation with the risk/compliance team.

© 2026 Tanium Inc. All Rights Reserved

RACI chart for Tanium Integrity Monitor (continued)

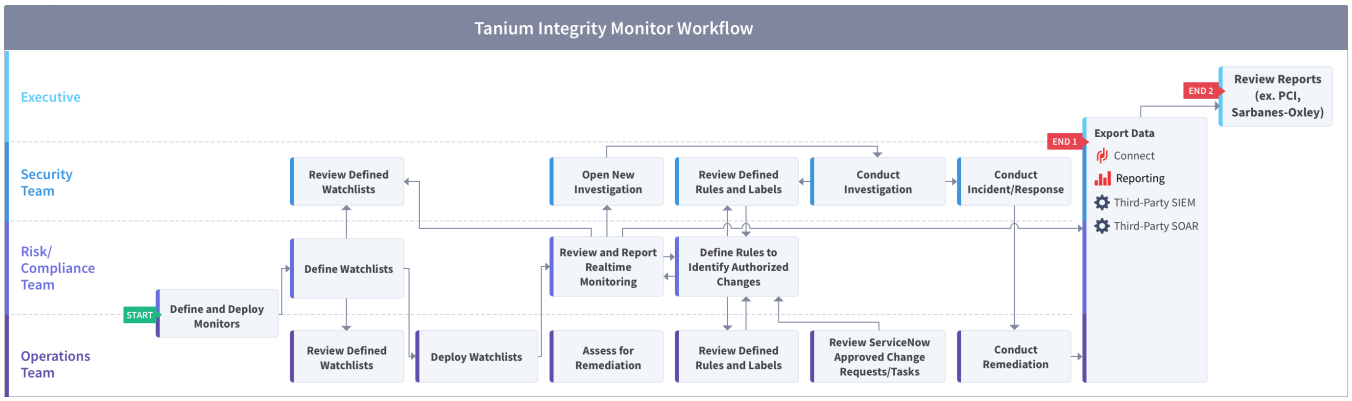
Task	Security	Operations	Risk/Compliance	Executive	Rationale
Remediate unapproved events	C	C	R/A	I	The operations team remediates events determined to be unapproved, in consultation with the security and risk/compliance teams. The executive team is informed of the final remediation.
Report compliance data	C	R/A	C	I	The risk/compliance team, with input from the security and operations teams, configures reporting of unexpected events (typically unlabeled events) and, optionally, expected events (typically events with specific labels). Using Connect, events can be sent to an external repository, such as a SIEM or SOAR solution, ServiceNow, or a SQL database.
Review status	I	I	I	I	Reporting boards show aggregated data from events and are reviewed by all teams.

© 2026 Tanium Inc. All Rights Reserved

RACI chart for Tanium Integrity Monitor (continued)

Task	Security	Operations	Risk/Compliance	Executive	Rationale
Routinely review compliance data from reports	-	-	R/A	I	The risk/compliance team is responsible for reporting compliance data from Reporting and Connect to the executive team and to auditors. External repositories such as a SIEM or a SQL database provide long-term storage for compliance data for auditing.

Integrity monitoring workflow



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 integrity monitoring.

© 2026 Tanium Inc. All Rights Reserved

Operational metrics

Integrity Monitor maturity

Managing an integrity monitoring 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 Integrity Monitor program are as follows:

Processes to measure Tanium Integrity Monitor maturity

Process	Description
Usage	How and when Tanium Integrity Monitor is used in your organization (for example, whether Integrity Monitor is supplemental for another legacy tool)
Automation	How Tanium Integrity Monitor is automated across endpoints, and how well it is leveraged in the automation of other systems
Functional Integration	How integrated Tanium Integrity Monitor is, across security, operations, and risk/compliance teams
Reporting	How Tanium Integrity Monitor reporting is automated and who the audience of Integrity Monitor reporting is

Benchmark metrics

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

© 2026 Tanium Inc. All Rights Reserved

Tanium Integrity Monitor maturity levels

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
Process	Usage	Integrity Monitor is configured and used by exception; some monitors are deployed to test groups or other small deployments	Integrity Monitor is used to audit the effectiveness of legacy tooling; simple watchlists are created and deployed	Integrity Monitor is used as the default tool for file and registry integrity monitoring only on systems in scope for regulatory compliance; legacy tooling might be used to audit file integrity monitoring effectiveness; multiple watchlists have been created and reused	Integrity Monitor is used as default tool for file and registry integrity monitoring on all critical endpoints; legacy tooling might be used to audit file integrity monitoring effectiveness; complex watchlists with includes and excludes have been created and reused	Integrity Monitor is used as default tool for file and registry integrity monitoring on all endpoints; watchlists are aligned to regulatory compliance requirements and surveys from business owners that identify critical and custom applications

© 2026 Tanium Inc. All Rights Reserved

Tanium Integrity Monitor maturity levels (continued)

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
	Automation	Rules are not used; review of events is fully manual	Rules are not used; review of events is fully manual	Rules are in use to apply labels to events	Well-tuned rules are in use to apply labels to all events	Well-tuned rules are in use to apply labels to all events; ServiceNow integration is used to label events associated with approved change requests or tasks
	Functional integration	Functionally siloed	Consult with or take direction from peers in first-level risk/compliance and security teams	Consult with or take direction from peers in first- and second-level risk/compliance and security teams; all data is sent to a SIEM, SOAR, or other data lake or log solution using Connect; default labels are used for events	Consult with or take direction from peers in first- and second-level risk/compliance, security, threat management, and security operations center teams; all data is sent to a SIEM, SOAR, or other data lake or log solution using Connect; custom labels are used for events	Consult with or take direction from peers in first- and second-level risk/compliance, security, threat management, and security operations center teams; only labeled events are sent to a SIEM, SOAR, or other data lake or log solution using Connect; remediation policies are in place in Tanium™ Enforce.
	Reporting	Manual	Manual; the Integrity Monitor Reporting gallery is imported	Automated; Reporting boards specific to your environment are created	Automated; Reporting boards specific to your environment are created, and Reporting reports are distributed automatically	Automated; Reporting boards specific to your environment are created, and Reporting reports are distributed automatically

© 2026 Tanium Inc. All Rights Reserved

Tanium Integrity Monitor maturity levels (continued)

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
Metrics	Integrity Monitor Server Coverage	0–79%	80–88%	89–94%	95–98%	99–100%
	Mean Unexpected Change Events per Endpoint	Frequent spikes or sharply upward trends in unexpected events	Occasional spikes or upward trends in unexpected events	Minimal spikes in unexpected events	Minimal spikes in unexpected events	No events are unexpected
	Expected vs Unexpected Change Events	21–100% of events are unexpected	11–20% of events are unexpected	6–10% of events are unexpected	1–5% of events are unexpected	No events are unexpected

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor requirements

Review the requirements before you install and use Integrity Monitor.

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium license that includes the Risk & Compliance Plus bundle. For more information about how to get a bundle, see Tanium Solutions & Bundles.
- Tanium™ Core Platform servers
- Tanium™ Client:

  Any supported version of Tanium Client. For more information, see Tanium Client Management User Guide: Client version and host system requirements.

  If you use a Client version that is not listed, certain product features might not be available, or stability issues can occur that can only be resolved by upgrading to one of the listed Client versions.

For more information, see Tanium Client Management User Guide: Client version and operating system requirements.

If you use a client version that is not listed, certain product features might not be available, or stability issues can occur that can only be resolved by upgrading to one of the listed client versions.

Computer group dependencies

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

- **All AIX**
- **All Linux**
- **All Solaris**
- **All Windows**
- **All Windows Servers**
- **All Windows Server 2022**
- **All Windows Server 2019**
- **All Windows Server 2016**
- **All Windows Server 2012 R2**
- **All Windows Server 2012**
- **All Windows Server 2008 R2**

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



Some Integrity Monitor dependencies have their own dependencies, which you can see by clicking the links in the lists of Required dependencies on page 23 and Feature-specific dependencies on page 24. Note that the links open the user guides for the latest version of each solution, not necessarily the minimum version that Integrity Monitor requires.

Tanium recommended installation

If you select **Tanium Recommended Installation** when you import Integrity Monitor, 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 Integrity Monitor 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 Integrity Monitor, the server automatically updates those dependencies to the latest available versions.

Required dependencies

Integrity Monitor has the following required dependencies:

- Tanium™ Client Index Extension*
- Tanium™ Client Recorder Extension*
- Tanium™ Endpoint Configuration
- Tanium™ Interact
- Tanium™ Data Service (TDS)
- Tanium™ RDB Service
- Tanium™ Secrets Service

*= The required version of this client extension is installed as part of Integrity Monitor. The Client Recorder Extension also includes the Tanium Driver.

© 2026 Tanium Inc. All Rights Reserved

Feature-specific dependencies

Integrity Monitor has the following feature-specific dependencies at the specified minimum versions:

- Tanium™ Connect 4.0 or later for event export
- Tanium Connect for watchlist data export
- Tanium Gateway to access Integrity Monitor from third-party integrations. For more information, see Reference: Gateway examples for Integrity Monitor on page 125.

Client extensions and endpoint tools

Tanium Endpoint Configuration installs Client Extensions and other tools for Integrity Monitor on endpoints. Client extensions perform tasks that are common to certain Tanium solutions. Each Client Extension and tool might have recommended security exclusions to allow them to run without interference. For more information, see Security exclusions. For a list of Integrity Monitor tools, see Reference: Integrity Monitor endpoint tools on page 120. For a list of all Client Extensions and tools, see Tanium Client Management User Guide: Reference: Client extensions used for Tanium solutions.

Endpoints

Supported operating systems

The following Tanium Client managed endpoint operating systems are supported with Integrity Monitor.

Supported operating systems for Tanium Client managed endpoints

Operating System	Version	Notes
Windows	• Windows 7 or later • Windows Server 2008 R2 or later	

© 2026 Tanium Inc. All Rights Reserved

Supported operating systems for Tanium Client managed endpoints (continued)

Operating System	Version	Notes
Linux	Same as Tanium Client support. For more information, see Tanium Client Management User Guide: Client version and operating system requirements.	Integrity Monitor uses the Client Recorder Extension when you enable the **Collect process and user attribution information** option for a monitor. The Client Recorder Extension does not support CentOS and Red Hat Enterprise Linux versions 5.3 and earlier. Endpoints require version 5.4 or later of CentOS or Red Hat Enterprise Linux. The Client Recorder Extension provides SELinux policies for the following distributions and versions: • Red Hat Enterprise Linux (RHEL) 5.4 and later, 6.x, 7.x, 8.x, and 9.x • CentOS 5.4 and later, 6.x, 7.x, 8.x, and 9.x • Amazon Linux 2 LTS (2017.12) At this time, SELinux is not supported on other Linux distributions. On endpoints where the recorder is not supported, event monitoring is unavailable, and only hash monitoring is supported. For Linux endpoints: • Install the most recent stable version of the audit daemon and audispd-plugins. For information on deprecated parameters in the audit daemon configuration, see Tanium Client Recorder Extension User Guide. See the specific operating system documentation for instructions. • Be aware that when using immutable "-e 2" mode, the recorder adds Tanium audit rules in front of the immutable flag. When using the -e 2 flag on Linux, the endpoint must be restarted after the recorder is enabled. • Be aware that when using the failure "-f 2" mode, the Linux kernel panics in the event that the auditd message is lost. The recorder does not add audit rules if this configuration is detected.
AIX	• AIX 7.1.4 or later	The IBM XL C++ runtime libraries file set (`xlC.rte`), version 16.1.0.0 or later, and the IBM LLVM runtime libraries file set (`libc++.rte`) must be installed. For more information, see Tanium Client Management User Guide: Deploy the Tanium Client to AIX endpoints using a package file.
Solaris	Same as Tanium Client support. For more information, see Tanium Client Management User Guide: Client version and operating system requirements.	

© 2026 Tanium Inc. All Rights Reserved

Disk space requirements

On managed endpoints, Integrity Monitor requires at least 1 GB of disk space. 3 GB is recommended.

CPU and memory requirements

The CPU demand on the endpoint averages less than 2.5% for each CPU core.

The Client Recorder Extension does not start on endpoints with a single logical core without updating the **CX.recorder.EnableSingleCpuRequirement** configuration setting to 0. To update CX.recorder.EnableSingleCpuRequirement to 0, edit the **Recorder - Set Recorder Extension Setting [*OS*]** package to add a parameter with the configuration key `EnableSingleCpuRequirement` and a value of `0`, and deploy the package to appropriate endpoints. Alternatively, you can run the following command from the Tanium Client directory on endpoints to update this configuration setting:

- (Windows) `TaniumClient.exe config set CX.recorder.EnableSingleCpuRequirement 0`
- (Linux) `./TaniumClient config set CX.recorder.EnableSingleCpuRequirement 0`

A minimum of 4 GB RAM is recommended on each endpoint device.

Permission recording requirements

Linux endpoints do not have any special requirements to monitor changes in file permissions.

To monitor changes in file permissions on Windows endpoints, you must configure the **Audit File System** permission under **Local Security Policy** on the endpoint. For more information, see Prepare Endpoints on page 67.

Client Recorder Extension

Integrity Monitor uses the Tanium Client Recorder Extension to gather data from endpoints when you enable the **Collect process and user attribution information** option for a monitor. For more information, see Client Recorder Extension User Guide.

Integrity Monitor does not use the Client Recorder Extension for Solaris and AIX endpoints.

Tanium Event Recorder Driver

Integrity Monitor uses the Tanium Event Recorder Driver to record file and registry events on supported Windows endpoints.

The Tanium Event Recorder Driver is installed automatically when you deploy a monitor with the **Collect process and user attribution information** option enabled. For more information, see Create or edit a monitor on page 81.



If the Tanium Event Recorder Driver is updated, endpoints that use Integrity Monitor require a reboot to see the recorder status.

Third-party software

To integrate Integrity Monitor with an IT workflow in ServiceNow Change Management, ServiceNow Madrid or later is required.

© 2026 Tanium Inc. All Rights Reserved

To use Integrity Monitor with the ServiceNow Tanium File Integrity and Unauthorized Change Monitoring application, ServiceNow Tokyo or later is required.

Host and network security requirements

Specific ports and processes are needed to run Integrity Monitor.

Ports

The following ports are required for Integrity Monitor communication.

Ports for Integrity Monitor communication

Source	Destination	Port	Protocol	Purpose
Module Server	Module Server (loopback)	17456	TCP	Internal communication; firewall rules are not typically required



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

Security exclusions

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



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

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

Target Device	Notes	Exclusion Type	Process
Tanium Module Server		Process	`<Module Server>\services\integrity-monitor-service\node.exe`
		Process	`<Module Server>\services\endpoint-configuration-service\TaniumEndpointConfigService.exe`

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Process
Windows x86 and x64		File	`<Tanium Client>\extensions\TaniumIndex.dll`

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	`<Tanium Client>\extensions\TaniumIndex.dll.sig`

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	<*Tanium Client*>\extensions\TaniumIntegrityMonitor.dll

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	`<Tanium Client>\extensions\TaniumIntegrityMonitor.dll.sig`

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	<*Tanium Client*>\extensions\TaniumRecorder.dll

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	<*Tanium Client*>\extensions\TaniumRecorder.dll.sig

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	<*Tanium Client*>\extensions\recorder\proc.bin

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	<*Tanium Client*>\extensions\recorder\recorder.db

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	<*Tanium Client*>\extensions\recorder\recorder.db-shm

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	<*Tanium Client*>\extensions\recorder\recorder.db-wal

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	<*Tanium Client*>\extensions\index\index.db

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	<*Tanium Client*>\extensions\index\index.db-shm

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	<*Tanium Client*>\extensions\index\index.db-wal

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	<*Tanium Client*>\TaniumClientExtensions.dll

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	<*Tanium Client*>\TaniumClientExtensions.dll.sig

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
	Endpoints with Toolset version 2.7 or later	Folder	`<Tanium Client>\python312`

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
	Endpoints with Toolset version 2.7 or later	Folder	`<Tanium Client>\TPython312`

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
	Endpoints with a Toolset version earlier than 2.7	Process	`<Tanium Client>\Python38\TPython.exe`

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
	Endpoints with a Toolset version earlier than 2.7	Folder	<*Tanium Client*>\Python38
	Endpoints with Toolset version 2.7 or later	Process	<*Tanium Client*>\python312\TPython.exe
		Process	<*Tanium Client*>\TaniumCX.exe
		Folder	<*Tanium Client*>\extensions\index
		Folder	<*Tanium Client*>\extensions\integrity-monitor
		File	C:\Windows\System32\drivers\TaniumRecorderDrv.sys
		File	C:\Windows\system32\drivers\TaniumProcessMonitor.dll
		Process	<*Tanium Client*>\tools\driver\service\TaniumDriverSvc.exe
	x86 endpoints	Process	<*Tanium Client*>\tools\driver\TaniumDriverCtl.exe
	x86 endpoints	Process	<*Tanium Client*>\tools\driver\TaniumDriverSvc.exe
	x86 endpoints	File	<*Tanium Client*>\tools\driver\TaniumProcessMonitor.dll
	x64 endpoints	Process	<*Tanium Client*>\tools\driver\TaniumDriverCtl64.exe
	x64 endpoints	Process	<*Tanium Client*>\tools\driver\TaniumDriverSvc64.exe
	x64 endpoints	File	<*Tanium Client*>\tools\driver\TaniumProcessMonitor64.dll
	x64 endpoints	File	C:\Windows\SysWOW64\TaniumProcessMonitor.dll

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
Linux x86 and x64		Process	`<Tanium Client>/extensions/recorder/TaniumAuditPipe`

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	`<Tanium Client>/libTaniumClientExtensions.so`

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	`<Tanium Client>/libTaniumClientExtensions.so.sig`

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	`<Tanium Client>/extensions/libTaniumIndex.so`

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	`<Tanium Client>/extensions/libTaniumIndex.so.sig`

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	`<Tanium Client>/extensions/libTaniumIntegrityMonitor.so`

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	`<Tanium Client>/extensions/libTaniumIntegrityMonitor.so.sig`

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	`<Tanium Client>/extensions/libTaniumRecorder.so`

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	`<Tanium Client>/extensions/libTaniumRecorder.so.sig`

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	<*Tanium Client*>/extensions/recorder/proc.bin

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	`<Tanium Client>/extensions/recorder/recorder.db`

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	<*Tanium Client*>/extensions/recorder/recorder.db-shm
		File	<*Tanium Client*>/extensions/recorder/recorder.db-wal
		File	<*Tanium Client*>/extensions/recorder/recorder.auditpipe
		File	<*Tanium Client*>/extensions/index/index.db
		File	<*Tanium Client*>/extensions/index/index.db-shm
		File	<*Tanium Client*>/extensions/index/index.db-wal
		Process	<*Tanium Client*>/TaniumCX
	Endpoints with a Toolset version earlier than 2.7	Process	<*Tanium Client*>/python38/python
	Endpoints with Toolset version 2.7 or later	Folder	<*Tanium Client*>/python312
	Endpoints with Toolset version 2.7 or later	Folder	<*Tanium Client*>/TPython312
	Endpoints with Toolset version 2.7 or later	Process	<*Tanium Client*>/python312/python
	Endpoints with Toolset version 2.7 or later	Process	<*Tanium Client*>/python312/bin/pybin
		Folder	<*Tanium Client*>/extensions/index
		Folder	<*Tanium Client*>/extensions/integrity-monitor

© 2026 Tanium Inc. All Rights Reserved

User role requirements

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

- Integrity Monitor solution permissions on page 59
- Integrity Monitor requirements on page 22: The solution permissions automatically provide some of these permissions.

To review a summary of the predefined roles, see Set up Integrity Monitor users on page 71.

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

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



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

Integrity Monitor solution permissions

Privilege	Integrity Monitor Administrator[1]	Integrity Monitor Operator[1]	Integrity Monitor Author[1]	Integrity Monitor User[1]	Integrity Monitor Read Only User[1]	Integrity Monitor Endpoint Configuration Approver[1]
Integrity Monitor View the Integrity Monitor workbench	✓ SHOW TROUBLESHOOTING	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW
Integrity Monitor Admin Settings For internal purposes only	✓ WRITE	✗	✗	✗	✗	✗

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor solution permissions (continued)

Privilege	Integrity Monitor Administrator[1]	Integrity Monitor Operator[1]	Integrity Monitor Author[1]	Integrity Monitor User[1]	Integrity Monitor Read Only User[1]	Integrity Monitor Endpoint Configuration Approver[1]
Integrity Monitor API Perform Integrity Monitor operations using the API	✅ EXECUTE	✅ EXECUTE	✅ EXECUTE	✅ EXECUTE	✅ EXECUTE	✅ EXECUTE
Integrity Monitor Deploy MONITORS: Deploy monitors RULES: Deploy rules WATCHLISTS: Deploy watchlists	✅ MONITORS RULES WATCHLISTS	✅ MONITORS RULES WATCHLISTS	❌	❌	❌	❌
Integrity Monitor Endpoint Configuration Approve Integrity Monitor configuration changes in Tanium Endpoint Configuration	❌	❌	❌	❌	❌	✅ APPROVE
Integrity Monitor Execute Scheduled Run tasks in the IM service with the IM schedule plugin, including running ServiceNow scheduled tasks.	✅ TASK	❌	❌	❌	❌	❌

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor solution permissions (continued)

Privilege	Integrity Monitor Administrator[1]	Integrity Monitor Operator[1]	Integrity Monitor Author[1]	Integrity Monitor User[1]	Integrity Monitor Read Only User[1]	Integrity Monitor Endpoint Configuration Approver[1]
Integrity Monitor Integrations Create, edit, and schedule integrations with IT workflows	✓ ADMIN	✓ ADMIN	✗	✗	✗	✗
Integrity Monitor Labels View, create, and edit labels	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✓ READ
Integrity Monitor Monitor Event Labels View, create, edit, and delete monitor event labels and label notes Send labeled events to Connect manually[2]	✓ READ WRITE DELETE	✓ READ WRITE DELETE	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Integrity Monitor Monitor Events View monitor events	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ	✗
Integrity Monitor Monitors View, create, and edit monitors	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✓ READ
Integrity Monitor Reports Access reports in the Integrity Monitor content set	✓ READ	✓ READ	✗	✓ READ	✓ READ	✗

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor solution permissions (continued)

Privilege	Integrity Monitor Administrator[1]	Integrity Monitor Operator[1]	Integrity Monitor Author[1]	Integrity Monitor User[1]	Integrity Monitor Read Only User[1]	Integrity Monitor Endpoint Configuration Approver[1]
Integrity Monitor Rules View, create, and edit rules	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Integrity Monitor Settings View and update general settings, templates, and default labels	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✓ READ	✗
Integrity Monitor Watchlists View, create, and edit watchlists	✓ READ WRITE	✓ 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 Tanium Console User Guide: View effective role permissions.

[2] To send labeled events to Tanium Connect, you must have Connect installed. You must also have the **Integrity Monitor Monitor Event Labels Write** permission and the **Tanium Connect Connect Event Write** permission, which is provided through the Connect roles. The least privileged Connect role that an Administrator can assign to grant this privilege is Connect User.

Integrity Monitor administration and platform content permissions

Permission	Permission Type	Integrity Monitor Administrator	Integrity Monitor Operator	Integrity Monitor Author	Integrity Monitor User	Integrity Monitor Read Only User	Integrity Monitor Endpoint Configuration Approver
Action Group	Administration	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor administration and platform content permissions (continued)

Permission	Permission Type	Integrity Monitor Administrator	Integrity Monitor Operator	Integrity Monitor Author	Integrity Monitor User	Integrity Monitor Read Only User	Integrity Monitor Endpoint Configuration Approver
Action	Platform Content	✓ READ WRITE	✓ READ WRITE	✗	✗	✗	✗
Filter Group	Platform Content	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ
Own Action	Platform Content	✓ READ	✓ READ	✗	✗	✗	✗
Package	Platform Content	✓ READ WRITE	✓ READ WRITE	✗	✗	✗	✗
Plugin	Platform Content	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE
Saved Question	Platform Content	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✓ READ	✗
Sensor	Platform Content	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ	✗

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

© 2026 Tanium Inc. All Rights Reserved

Installing Integrity Monitor

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

- **Automatic configuration with default settings**: Integrity Monitor 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, see Import Integrity Monitor with default settings on page 64.
- **Manual configuration with custom settings**: After installing Integrity Monitor, you must manually configure required settings. Select this option only if Integrity Monitor requires settings that differ from the recommended default settings. For more information, see Import Integrity Monitor with custom settings on page 65.

Before you begin

- Read the release notes.
- Review the Integrity Monitor requirements on page 22.
- If you are upgrading from a previous version, see Upgrading Integrity Monitor on page 74.
- Assign the correct roles to users for Integrity Monitor. Review the User role requirements on page 59.
    - To import the Integrity Monitor solution, you must be assigned the Administrator reserved role or a role that has the **Import Signed Content** permission.
    - To configure the Integrity Monitor 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 Integrity Monitor with default settings

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

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

© 2026 Tanium Inc. All Rights Reserved

Tanium Integrity Monitor default settings

Setting	Default value
Action group	• Restricted targeting disabled (default): `All AIX`, `All Linux`, `All Solaris`, and `All Windows` computer groups • Restricted targeting enabled: `No Computers` computer group
Monitor creation	A monitor is created for each supported operating system (Windows, Linux, Solaris, and AIX). The Windows monitor is targeted only to Windows Server computer groups: **All Windows Server 2008 R2**, **All Windows Server 2012**, **All Windows Server 2012 R2**, **All Windows Server 2016**, **All Windows Server 2019**, and **All Windows Server 2022**. All other monitors are targeted to the associated **All <*Operating System*>** computer group: **All Linux**, **All AIX**, and **All Solaris**. TIP If one or more of the targeted operating systems are not used in your environment, delete the associated monitors.
Monitor deployments	The monitors are deployed to endpoints.
Watchlist	A watchlist is created for each supported operating system based on the **Critical System Files** template for the operating system. The Windows watchlist is targeted only to Windows Server computer groups: **All Windows Server 2008 R2**, **All Windows Server 2012**, **All Windows Server 2012 R2**, **All Windows Server 2016**, **All Windows Server 2019**, and **All Windows Server 2022**. All other watchlists are targeted to the associated **All <*Operating System*>** computer group: **All Linux**, **All AIX**, and **All Solaris**. TIP If one or more of the targeted operating systems are not used in your environment, delete the associated watchlists.
Watchlist deployments	The watchlists are deployed to endpoints.

To import Integrity Monitor 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 Integrity Monitor version on page 66.

Import Integrity Monitor with custom settings

To import Integrity Monitor without automatically configuring default settings, be sure to clear the **Apply 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 Integrity Monitor version on page 66.

© 2026 Tanium Inc. All Rights Reserved

Manage solution dependencies

When you start the Integrity Monitor workbench for the first time, the Tanium Server checks whether all the Tanium modules and shared services (solutions) that are required for Integrity Monitor are installed at the required versions. The Integrity Monitor workbench cannot load unless all required dependencies are installed. If you selected **Tanium Recommended Installation** when you imported Integrity Monitor, the Tanium Server automatically imported all your licensed solutions at the same time. Otherwise, if you manually imported Integrity Monitor and did not import all its dependencies, Tanium Console displays a banner that lists the dependencies and the required versions. For more information, see Solution dependencies.

Perform the following steps if a banner indicates any Integrity Monitor dependencies are not installed:

1. Install the dependencies as described in Tanium Console User Guide: Import or update specific solutions.
2. From the Main menu, go to **Modules > Integrity Monitor** to open the Integrity Monitor **Overview** page and verify that Console no longer displays a banner to list missing dependencies.

Upgrade Integrity Monitor

For the steps to upgrade Integrity Monitor, see Tanium Console User Guide: Managing Tanium solutions. After the upgrade, verify that the correct version is installed. For more information, see Verify Integrity Monitor version on page 66.



The Integrity Monitor event source is no longer available in Integrity Monitor 3.4.182 and later. After you upgrade to Integrity Monitor 3.4.182 or later, use saved questions to send Integrity Monitor data to external destinations. For more information, see Use Connect to send events on page 106.

After you upgrade Integrity Monitor, see Upgrading Integrity Monitor on page 74 for additional tasks.

Verify Integrity Monitor version

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

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

© 2026 Tanium Inc. All Rights Reserved

Configuring Integrity Monitor

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

Prepare Endpoints

Prepare endpoints to use Integrity Monitor by configuring the permission recording on Windows endpoints and removing the legacy Client Recorder Extension if needed.

(Windows) Configure permission recording

To monitor changes in file permissions, you must configure the **Audit File System** permission under **Local Security Policy** on the endpoint.

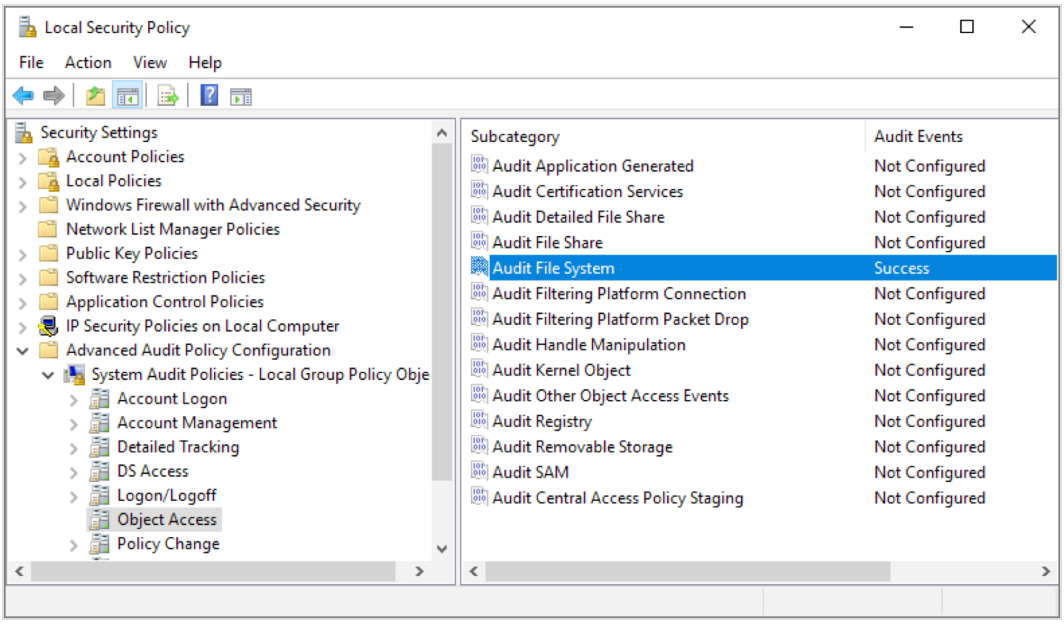
Endpoints that do not have this permission configured return `Recorder - Error: File permission auditing is disabled` when you ask a question using the `Client Extensions - Status` sensor, and they appear in the **Endpoint Health** panel on the Integrity Monitor Overview page.

To configure the **Audit File System** permission, complete the following steps. (These steps apply to Windows 10 and might vary for different versions of Windows.)

1. From the Control Panel, open **Administrative Tools > Local Security Policy**.
2. Go to **Security Settings > Advanced Audit Policy Configuration > System Audit Policies - Local Group Policy Object > Object Access**.

© 2026 Tanium Inc. All Rights Reserved

3. Double-click **Audit File System**.



4. Select **Configure the following audit events:** and then select **Success**.
5. Click **OK**.

> NOTE
>
> When you enable the **Permission** change type for a path in a watchlist, Integrity Monitor automatically configures the appropriate System Access Control List (SACL) audit settings for every file and folder in that path for that watchlist.

Remove legacy Client Recorder Extension

If Client Recorder Extension version 1.x exists on a targeted endpoint, you must remove it before you install Client Recorder Extension version 2.x tools. To target endpoints where Client Recorder Extension version 1.x exists, ask the question: `Recorder - Legacy Installed`. If the Supported Endpoints column displays **Yes**, you must remove Client Recorder Extension version 1.x from the endpoint before you install Client Recorder Extension 2.x tools. To remove Client Recorder Extension version 1.x, deploy the **Recorder - Remove Legacy Recorder [*Operating System*]** package to targeted endpoints.

Install and configure Tanium Endpoint Configuration

Manage solution configurations with Tanium Endpoint Configuration

Tanium Endpoint Configuration delivers configuration information and required tools for Tanium Solutions to endpoints. Endpoint Configuration consolidates the configuration actions that traditionally accompany additional Tanium functionality and eliminates

© 2026 Tanium Inc. All Rights Reserved

the potential for timing errors that occur between when a solution configuration is made and the time that configuration reaches an endpoint. Managing configuration in this way greatly reduces the time to install, configure, and use Tanium functionality, and improves the flexibility to target specific configurations to groups of endpoints.

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

IMPORTANT

When you upgrade Integrity Monitor, the change management feature enables you to perform a staged rollout of the endpoint tools associated with the new version of Integrity Monitor. Integrity Monitor 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 Integrity Monitor might not be available on these endpoints until they receive the upgraded tools.

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

NOTE

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

Optionally, you can use Endpoint Configuration to require approval of configuration changes. When configuration approvals are enabled, Endpoint Configuration does not deploy a configuration change to endpoints until a user with approval permission approves the change. For information about the roles and permissions that are required to approve configuration changes for Integrity Monitor, see User role requirements on page 59. For more information about how to enable and use configuration approvals in Endpoint Configuration, see Tanium Endpoint Configuration User Guide: 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 Tanium Console User Guide: Managing action locks.

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

If you enabled configuration approvals, the following configuration changes must be approved in Endpoint Configuration before they deploy to endpoints:

© 2026 Tanium Inc. All Rights Reserved

- Deploying monitors
- Deploying watchlists
- Deploying rules

Configure Integrity Monitor

(Optional) Configure Automatic Deployment on Upgrade

Select **Automatic Deployment on Upgrade** to automatically deploy monitors, watchlists, and rules after an upgrade. Deployment of each monitor, watchlist, or rule uses the management rights of the last user to deploy the item, but does not use any of that user's persona rights, even if the user changed to a persona to deploy.

Review any tools, watchlists, and monitors deployed to endpoints before you select this option, especially if changes were made since the last deployment.

1. From the Main menu, go to **Modules > Integrity Monitor > Overview**, and then click Settings .
2. Click the **General Settings** tab.
3. Select **Automatically deploy monitors, watchlists, and rules when upgrading the module** and click **Save**.

Configure the Integrity Monitor action group

Importing the Integrity Monitor 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 Integrity Monitor, the action group targets **No Computers**.

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

Select the computer groups to include in the Integrity Monitor action group.



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

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

© 2026 Tanium Inc. All Rights Reserved

Organize computer groups

You deploy watchlists and monitors by computer group. Target monitors as broadly as possible, and create more specific groups if you need different settings or intervals for scanning some endpoints. Create specific groups for watchlists, targeted more narrowly to watch only the necessary paths on the necessary endpoints.



When possible, avoid targeting different monitors to computer groups that contain some of the same endpoints. One monitor is deployed to each endpoint. You can prioritize monitors when computer groups overlap, but it is better to create non-overlapping computer groups to use with monitors for a more predictable deployment.

Create relevant computer groups to organize your endpoints for monitor and watchlist targeting. Some options include:

- Applications in use on an endpoint
- Endpoint type, such as servers with a specific function
- Endpoint compliance requirements, such as endpoints that must comply with Payment Card Industry Data Security Standard (PCI DSS) or the Sarbanes-Oxley Act (SOX)
- Endpoint location, such as by country or time zone
- Endpoint priority, such as business-critical machines
- Endpoint configuration needs, such as VDI machines

For more information, see Tanium Core Platform User Guide: Managing computer groups.

Set up Integrity Monitor users

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

For more information, see User role requirements on page 59.



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

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

Integrity Monitor Administrator

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

© 2026 Tanium Inc. All Rights Reserved

- Configure all Integrity Monitor settings, templates, and labels
- Execute scheduled tasks in the Integrity Monitor service using the schedule plugin
- Run and apply rules to events
- View, create, edit, and deploy monitors, rules, and watchlists
- Create, edit, and schedule integrations with IT workflows
- Delete labels and event labels

Integrity Monitor Operator

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

- Configure Integrity Monitor settings, templates, and labels
- Run and apply rules to events
- View, create, edit, and deploy monitors, rules, and watchlists
- Create, edit, and schedule integrations with IT workflows
- Delete labels and event labels

Integrity Monitor Author

Assign the **Integrity Monitor Author** role to users who manage monitors, rules, and labels in Integrity Monitor.
This role can perform the following tasks:

- View, create, and edit monitors, rules, and labels
- View Integrity Monitor events and settings

Integrity Monitor User

Assign the **Integrity Monitor User** role to users who manage event labels and rules in Integrity Monitor.
This role can perform the following tasks:

- View, create, and edit event labels and rules
- View Integrity Monitor monitors, events, labels, and settings

Integrity Monitor Read Only User

Assign the **Integrity Monitor Read Only User** role to users who need visibility into Integrity Monitor data.
This role can view **Integrity Monitor Read Only User** events, event labels, labels, monitors, rules, and settings.

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor Endpoint Configuration Approver

Assign the **Integrity Monitor Author** role to a user who approves or rejects **Integrity Monitor** configuration items in Tanium Endpoint Configuration.



Do not assign the **Integrity Monitor Service Account** role to users. This role is for internal purposes only.

© 2026 Tanium Inc. All Rights Reserved

Upgrading Integrity Monitor

For the steps to upgrade Integrity Monitor, see Tanium Console User Guide: Import or update specific solutions. After the upgrade, verify that the correct version is installed. For more information, see Verify Integrity Monitor version on page 80.

Read the release notes for a particular version before you upgrade Integrity Monitor.

IMPORTANT

In Integrity Monitor 3.4.97 and later, the steps required to configure the service account are no longer necessary due to the adoption of the System User Service, which performs these tasks automatically. Additionally, the Integrity Monitor database is migrated to RDB in this release. Consequently, after upgrading from version 3.1.9 or earlier to Integrity Monitor 3.4.97 or later, it might take time for the database migration to complete and for RBAC privileges and other updates to sync properly. This could lead to issues and error messages when you first query Tanium Console. These issues usually resolve on their own after a few minutes, but could take up to an hour or longer depending on system resources and the amount of data to migrate.

BEST PRACTICE

Perform some basic tests in Integrity Monitor before and after the upgrade to ensure that all operations are working as expected.

Upgrading from a version earlier than 3.0

IMPORTANT

Integrity Monitor 3.0 and later changes how labeled events are stored, how watchlists and monitors are targeted, and the sensors used, which requires certain manual changes. An upgrade from a version earlier than 3.0 to 3.0 or later does not automatically redeploy monitors and rules, regardless of the **Automatically deploy monitors and rules when upgrading the module** setting in the earlier version (see Redeploy monitors, watchlists, and rules on page 79), or deploy watchlists. Complete all upgrade-related tasks before you redeploy monitors and rules and deploy watchlists for the first time.

Review changes related to removal of server-side storage of labels

In Integrity Monitor 3.0 and later, all labels for events are stored on Tanium Client managed endpoints. To support this functionality, when you upgrade from a version earlier than 2.4, all existing labels become global labels. Any user-defined custom labels that were assigned to specific monitors are migrated to a matching global label. Any custom labels that have conflicting names are merged into a single global label. (These changes already occurred if you upgraded to version 2.4 or later.)

Additionally, when you upgrade from a version earlier than 3.0, the following changes occur:

© 2026 Tanium Inc. All Rights Reserved

- Legacy monitors that store events on the server (formerly known as *basic monitors*) are migrated to standard monitors.
- Legacy rules (formerly known as *basic rules*) are removed. You must recreate rules and apply them to migrated monitors to continue automatically labeling events for migrated monitors.
- The **Reports** tab is removed from legacy monitors.
- Manual labeling controls are removed from legacy monitors.
- Any existing labels are removed from events.

Update sensors in saved questions

Because Integrity Monitor 3.0 and later uses a different database to store recorded events, legacy sensors that were used with versions earlier than 3.0 are deprecated. Integrity Monitor 3.0 or later does not install these sensors in a new installation. If you are upgrading from a version earlier than 3.0, deprecated sensors remain available and continue to return events from before the upgrade, until those events are pruned from the database. Only the legacy sensors return these legacy events, and only the new sensors return new events that occur after you first deploy monitors after the upgrade. Events are pruned from a Tanium Client managed endpoint database according to the **Monitor Pruning Age** that is configured for the monitor that is deployed to that endpoint, which is six months by default. An endpoint automatically deletes the legacy event database and removes legacy Integrity Monitor tools after the full time of the **Monitor Pruning Age** has passed since you first deployed monitors after the upgrade.



The **Monitor Pruning Age** determines how long Integrity Monitor stores events in the endpoint database. Auditing this database requires the assistance of Tanium Support. When asking questions using Integrity Monitor sensors, you can view events as old as 250 hours.

To collect new event data, you must replace each sensor as directed in saved questions, including those used with Connect.



New sensors use different parameters and return data with groupings and columns that are different from legacy sensors. In addition to replacing sensors, you must review and update any saved question, connection, or logic at a connection destination that depends on the groupings and columns in the deprecated sensor. For more information about new event sensors, see Use sensors to view events or event counts on page 98. For more information about updating connections, see the Tanium Connect User Guide.

Tanium Integrity Monitor replacement sensors

Deprecated Sensor	Replacement Sensor
`Integrity Monitor - Coverage Status`	`Client Extensions - Status`
`Integrity Monitor Endpoint Config Monitor Status`	`Client Extensions - Status`
`Integrity Monitor Endpoint Config Priority`	`Client Extensions - Status`
`Integrity Monitor Endpoint ID`	`Client Extensions - Endpoint ID`

© 2026 Tanium Inc. All Rights Reserved

Tanium Integrity Monitor replacement sensors (continued)

Deprecated Sensor	Replacement Sensor
`Integrity Monitor Endpoint Process Restart Needed`	`Client Extensions - Status`
`Integrity Monitor Endpoint Tools Status`	`Client Extensions - Status`
`Integrity Monitor File Events Details`	`Integrity Monitor - Monitor Events`
`Integrity Monitor File Events Overview`	`Integrity Monitor - Monitor Events`
`Integrity Monitor Filtered Events Count`	`Integrity Monitor - Event Count`
`Integrity Monitor Filtered File Events Details`	`Integrity Monitor - Monitor Events`
`Integrity Monitor Filtered File Events Overview`	`Integrity Monitor - Monitor Events`
`Integrity Monitor Labeled File Events Details`	`Integrity Monitor - Monitor Events`
`Integrity Monitor Unlabeled File Events Details`	`Integrity Monitor - Monitor Events Unlabeled`
`Integrity Monitor Unlabeled File Events Overview`	`Integrity Monitor - Monitor Events Unlabeled`



After the **Monitor Pruning Age** has passed for all monitors and all legacy events have been pruned, delete the deprecated sensors to avoid confusion.

Add filters to saved questions for change types

In Integrity Monitor versions earlier than 3.0, you could select specific change types for Integrity Monitor to record for each path in a watchlist. Integrity Monitor 3.0 and later monitors all change types for all paths. If you want to limit saved questions to specific change types, including saved questions used with Connect, you must update those saved questions with a filter. For example, the following question returns only file creation events:

```
Get Integrity Monitor - Monitor Events[10,0,360,15,0,""] having Integrity Monitor - Monitor Events:Change Type equals CreateNewFile from all machines
```

Review monitor and watchlist targeting

Integrity Monitor versions earlier than 3.0 handled targeting exclusively through monitors, and you assigned watchlists to monitors for deployment. In Integrity Monitor 3.0 and later, you target and deploy watchlists and monitors separately, which lets you use fewer monitors and use watchlist targeting to more closely control which paths Integrity Monitor watches on each endpoint. You no longer assign watchlists to monitors, though each endpoint that you target in a watchlist must also be targeted in a monitor for the watchlist to take effect.

When you upgrade to Integrity Monitor 3.0 or later, the upgrade automatically adds computer groups to the targeting for each watchlist, based on the targeting of the monitors to which that watchlist was assigned in the earlier version. Before redeploying watchlists and monitors, review the targeting of each watchlist and monitor to determine whether it needs refinement to avoid watching unnecessary paths on some endpoints.

© 2026 Tanium Inc. All Rights Reserved

IMPORTANT

In certain cases where multiple monitors target the same endpoint, the automatic application of watchlist targeting can cause a watchlist to apply to an endpoint where it did not apply before the upgrade.

For example, assume the following conditions applied in the earlier version of Integrity Monitor:

- **Watchlist 1** was assigned only to **Monitor A**.
- **Watchlist 2** was assigned only to **Monitor B**.
- Both **Monitor A** and **Monitor B** targeted computer groups that contain **Endpoint Z**.
- **Monitor A** was above **Monitor B** in the priority list.

Because Integrity Monitor deploys only one monitor to each endpoint based on the priority list, it deploys only **Monitor A** to **Endpoint Z**, and this still applies in Integrity Monitor 3.0 and later. However, before the upgrade, **Watchlist 2** did not apply on **Endpoint Z** because **Monitor B** was not deployed there. The upgrade to Integrity Monitor 3.0 or later copies targeting from **Monitor A** to **Watchlist 1** and from **Monitor B** to **Watchlist 2**, and because watchlists are now deployed separately from monitors, both watchlists apply to **Endpoint Z** after the upgrade. If you redeploy watchlists and monitors without any adjustments to targeting, Integrity Monitor now watches paths in **Watchlist 2** on **Endpoint Z**.

If you use overlapping monitors, take extra care in reviewing watchlist targeting to avoid watching unnecessary paths on endpoints that are included in the targeting for multiple monitors.

BEST PRACTICE

Edit watchlists to apply narrow targeting and watch only the necessary paths on the necessary endpoints. Consolidate monitors, and target consolidated monitors as broadly as possible. Use additional monitors only to accommodate different scan settings, scan intervals, or rules.

Review monitor settings

In Integrity Monitor versions earlier than 3.0, you could select hash monitoring, event monitoring, or both for the monitoring method. Integrity Monitor 3.0 and later performs hash monitoring for all monitors, which uses Index CX to detect and record basic file and registry events. Monitors that were configured to perform event monitoring before the upgrade have the **Collect process and user attribution information** setting enabled after the upgrade. This setting uses Recorder CX to record the specific operation, as well as the associated user or process path. You can optionally disable this setting for a monitor if you do not need process and user information for events that the monitor records.

Additionally, the **Install Tanium Driver** setting has been removed, and Integrity Monitor 3.0 and later automatically installs the Tanium Driver on all targeted Windows endpoints when you deploy a monitor with the **Collect process and user attribution information** setting enabled.

IMPORTANT

After the driver is first installed on a targeted endpoint, you must reboot that endpoint before Integrity Monitor can record process and user information associated with file and registry operations.

© 2026 Tanium Inc. All Rights Reserved

Review paths that include symbolic links

Integrity Monitor 3.0 and later watches files and directories that are referenced by a symbolic link, if you directly specify a symbolic link in a path (including with the use of wildcard characters), whereas versions earlier than 3.0 watched only the symbolic link file itself. If an existing watchlist includes a path that directly specifies a symbolic link, Integrity Monitor starts watching referenced files and directories after the upgrade. If you want to continue watching only the symbolic link file itself, you can change the path to watch the parent directory that contains the symbolic link file, and specify the symbolic link file as an inclusion.



To avoid recursion, Integrity Monitor does not watch the referenced directories or files if the symbolic link is contained within a directory that the path specifies. For example, if you have a symbolic link at `/my/path/directory-symlink` that references `/other/path/referenced-directory`, then if you specify the path `/my/path/directory*`, Integrity Monitor watches the referenced directory `/other/path/referenced-directory`. If you specify the path `/my/path`, then Integrity Monitor watches the symbolic link file itself, but it does not watch the referenced directory.

If a watchlist includes paths that contain symbolic links but no paths that directly specify symbolic links, there is no change in behavior after the upgrade.

Review registry paths, inclusions, and exclusions that specify values

In Integrity Monitor versions earlier than 3.0, a double-backslash separator (`\\`) specified a registry value in a path, inclusion, or exclusion. Integrity Monitor 3.0 and later does not let you specify registry values, and all values are watched for each watched key. Watchlist paths, inclusions, and exclusions are not modified for this behavior during the upgrade, but Integrity Monitor 3.0 and later ignores anything after two backslashes (`\\`) in a registry path, inclusion, or exclusion.



This change in behavior can result in Integrity Monitor watching values and subkeys that it did not watch before the upgrade. Because a value in an existing registry path, inclusion, or exclusion is ignored after the upgrade, a path, inclusion, or exclusion that contains a value indicates the key immediately preceding the double-backslash separator (`\\`) after the upgrade.

This change results in the following behavior after the upgrade:

- For a path that contains a value, Integrity Monitor watches the key immediately preceding the double-backslash separator (`\\`), all subkeys of that key unless inclusions or exclusions specify otherwise, and all values of that key and watched subkeys, regardless of inclusions or exclusions.
- For an inclusion or exclusion that contains a key and a value, Integrity Monitor interprets the inclusion or exclusion as the key immediately preceding the double-backslash separator (`\\`).
- For an inclusion or exclusion that contains only a value, Integrity Monitor ignores the inclusion or exclusion.

If you use registry paths, inclusions, or exclusions that specify values, carefully review those items and make adjustments to avoid watching additional subkeys unnecessarily.

© 2026 Tanium Inc. All Rights Reserved

Review path inclusions and exclusions that include wildcard characters

In Integrity Monitor versions earlier than 3.0, a single asterisk wildcard character (`*`) matched path separators when used in an inclusion or exclusion. In Integrity Monitor 3.0 and later, a single asterisk (`*`) does not match path separators, and two asterisks together (`**`) do include path separators. When you upgrade from a version earlier than 3.0 to version 3.0 or later, each asterisk in an inclusion or exclusion is automatically changed to a pair of asterisks. Because this automatic change maintains the previous behavior for inclusions and exclusions, no manual updates are necessary. However, make sure you use two asterisks (`**`) in an inclusion or exclusion to match path separators when you add new inclusions or exclusions or import paths from a file.

Deploy monitors, watchlists, and rules

An upgrade from a version earlier than 3.0 to 3.0 or later does not automatically redeploy monitors and rules, regardless of the **Automatically deploy monitors and rules when upgrading the module** setting in the earlier version (see Redeploy monitors, watchlists, and rules on page 79), or deploy watchlists. After you complete all upgrade-related tasks and review your configuration, you must manually deploy monitors, watchlists, and rules. For more information, see Deploy monitors on page 84, Deploy watchlists on page 96, and Deploy rules on page 104.

NOTE

You must deploy both a monitor and at least one watchlist to each endpoint for Integrity Monitor to watch paths on that endpoint. You can ask questions to identify endpoints that are missing either a monitor or watchlist:

- To identify endpoints to which you have deployed one or more watchlists but no monitor, ask the question: `Get Computer Name and Client Extensions - Status matches "^integrity_monitor\|monitor_id\|.*$" from all machines with Client Extensions - Status matches "^integrity_monitor\|monitor_id\|0$"`.
- To identify endpoints to which you have deployed a monitor but no watchlists, ask the question: `Get Computer Name and Client Extensions - Status matches "^integrity_monitor\|monitor_id\|[^0].*$" and Integrity Monitor - Active Watchlists from all machines with ( Client Extensions - Status matches "^integrity_monitor\|.*$" and Integrity Monitor - Active Watchlists contains No Results Found )`.

Redeploy monitors, watchlists, and rules

After you upgrade Integrity Monitor, all monitors, rules, and watchlists must be redeployed. The default configuration automatically redeploys all items after an upgrade, or if the automatic deployment setting is not configured, you must manually redeploy them. For more information, see Deploy monitors on page 84, Deploy watchlists on page 96, and Deploy rules on page 104.

IMPORTANT

If you do not redeploy monitors, watchlists, and rules, the system might be left in a nonworking state.

© 2026 Tanium Inc. All Rights Reserved

Configure automatic redeployment of monitors

1. From the Integrity Monitor **Overview** page, click Settings.
2. Click the **General Settings** tab.
3. In the **Automatic Deployment on Upgrade** section, select **Automatically deploy monitors, watchlists, and rules when upgrading the module**.

Verify Integrity Monitor version

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

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

© 2026 Tanium Inc. All Rights Reserved

Managing scan settings with monitors

Use monitors to define scan settings for the endpoints in a targeted computer group. A monitor can be deployed to multiple computer groups.

IMPORTANT

Each Tanium Client managed endpoint that you target in a watchlist must also be targeted in a monitor for the watchlist to take effect when you deploy watchlists and monitors. To identify endpoints to which you have deployed a monitor but no watchlists, ask the question: `Get Computer Name and Client Extensions - Status matches "^integrity_monitor\|monitor_id\|[^0].*$" and Integrity Monitor - Active Watchlists from all machines with ( Client Extensions - Status matches "^integrity_monitor\|.*$" and Integrity Monitor - Active Watchlists contains No Results Found )`. For more information, see Managing watched paths with watchlists on page 86.

Create or edit a monitor

Create or edit a monitor to identify scan settings for a targeted computer group.

BEST PRACTICE

- Create as few monitors as possible, and target those monitors as broadly as possible. Create additional monitors only to accommodate different scan settings, scan intervals, or rules.
- When possible, avoid targeting different monitors to computer groups that contain some of the same endpoints. One monitor is deployed to each endpoint. You can prioritize monitors when computer groups overlap, but it is better to create non-overlapping computer groups to use with monitors for a more predictable deployment.
- Name each monitor based on the operating system, business unit, or application group for which you are configuring scan settings.
- Select the **Collect process and user attribution information** option to record real-time events and attribution data. This option subscribes the watchlist items to Tanium Recorder, and Tanium Index handles the items as high priority paths.

1. From the Main menu, go to **Modules > Integrity Monitor > Monitors**.
2. Click **Create Monitor**, or click Edit in the row for an existing monitor that you want to edit.
3. In the **Summary** section, enter a **Name** and **Description** for the monitor.

© 2026 Tanium Inc. All Rights Reserved

4. (Optional) For **Monitor Pruning Age**, configure the time that Integrity Monitor should keep each event that the monitor records in the database.

   NOTE

   The **Monitor Pruning Age** determines how long Integrity Monitor stores events in the endpoint database. Auditing this database requires the assistance of Tanium Support. You can adjust this setting to meet the requirements of any applicable compliance standards and manage the database size on endpoints, but do not set it lower than 250 hours. When asking questions using Integrity Monitor sensors, you can view events as old as 250 hours.

5. (Optional) For **Database Maximum Size**, enable and configure the maximum size in megabytes of the endpoint database. The endpoint attempts to prune the database after it reaches the **Database Maximum Size** or if an event reaches the **Monitor Pruning Age**, whichever occurs first. If the endpoint prunes the database due to reaching the **Database Maximum Size**, but pruned events are not older than the **Monitor Pruning Age**, a health check runs because the Integrity Monitor data is incomplete and cannot be recovered.

   NOTE

   For the best results, work with Tanium Support to monitor the Integrity Monitor database before implementing size restrictions.

6. To record real-time change events, such as create, write, delete, or rename operations, select **Collect process and user attribution information**. This method records the specific operation, as well as the associated user or process path.

   NOTE

   - This setting applies only to Windows and Linux endpoints. Solaris and AIX endpoints perform only hash monitoring, regardless of this setting.
   - If you disable this setting, the following behaviors apply:
     - Integrity Monitor records a rename operation as a delete operation followed by a create operation. On Solaris and AIX endpoints, Integrity Monitor always records a rename operation as a delete operation followed by a create operation.
     - Integrity Monitor does not return modifications to registry values as events. Create and delete operations are still recorded for individual registry values, regardless of this setting.

7. For **Index First Scan Distribute Over Time**, configure the time over which to randomize the first file index scan on targeted endpoints. Randomizing this scan over a period of time helps balance resource use.

8. For **Index Scan Frequency**, configure the interval between subsequent file index scans for all watchlists. This configuration acts as a fail-safe in case Tanium Recorder is unavailable. If another solution also uses Index, Integrity Monitor and the other solution maintain separate subscription and scan schedules.

© 2026 Tanium Inc. All Rights Reserved

NOTE

If the scan takes longer than the interval configured for this setting on an endpoint, the endpoint returns `Scan completion took longer than configured scan interval` from the `Client Extensions - Status` sensor and appears in the **Endpoint Health** panel on the Integrity Monitor Overview page. To resolve this condition, make sure that the endpoint meets the minimum system requirements for Integrity Monitor, and adjust this setting as necessary.

9. In the **Targeting** section, click **Select Computer Groups**, select the computer groups to target, and click **Save**. For more information, see Tanium Platform User Guide: Managing computer groups.
10. Click **Create** (for a new monitor) or **Save** (for an existing monitor).
11. After you create or edit a monitor, you must deploy all monitors. For more information, see Deploy monitors on page 84. If you are using rules, you must also redeploy all rules. For more information, see Deploy rules on page 104.

IMPORTANT

When you first deploy a monitor with the **Collect process and user attribution information** option enabled, Integrity Monitor installs the Tanium Driver on targeted Windows endpoints, unless another Tanium solution has already installed the driver. After the driver is first installed on a targeted endpoint, you must reboot that endpoint before Integrity Monitor can record process and user information associated with file and registry operations.

Prioritize monitors

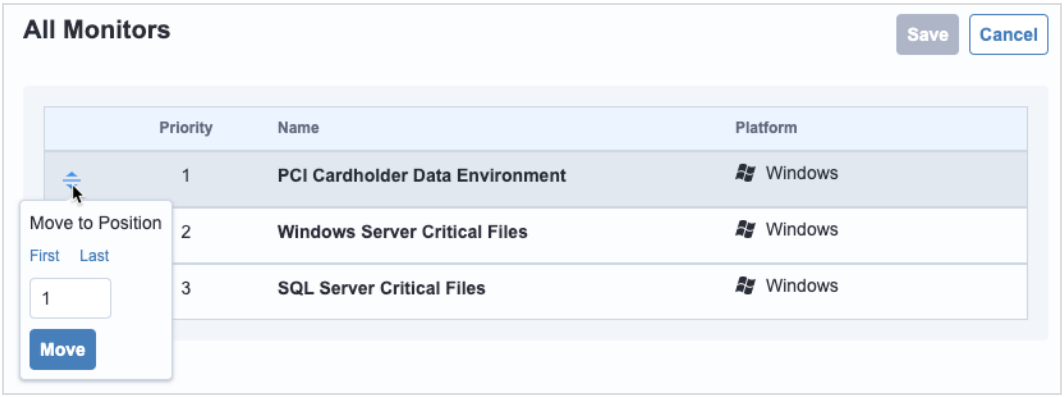
One monitor is deployed to each endpoint. If an endpoint belongs to the targeted computer groups for two or more monitors, the monitor priority list determines which monitor is deployed to the endpoint.

BEST PRACTICE

When possible, avoid targeting different monitors to computer groups that contain some of the same endpoints. One monitor is deployed to each endpoint. You can prioritize monitors when computer groups overlap, but it is better to create non-overlapping computer groups to use with monitors for a more predictable deployment.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules > Integrity Monitor > Monitors**.
2. Click **Prioritize**.
3. Drag monitors into the order you want to prioritize them, or click Move to Position in the row for a monitor you want to reorder, enter the new position, and click **Move**. After you have reordered the monitors, click **Save**.



4. After you re-prioritize, you must deploy all monitors. For more information, see Deploy monitors on page 84.

Deploy monitors

After you create, edit, reprioritize, or delete monitors, you must deploy all monitors to the endpoints. A **Deploy Now** banner appears, and **Pending Deployment** (new monitors), **Pending Deployment** (changed monitors), or **Pending Deletion** (deleted monitors) appears in the **Status** column for the monitor on the **All Monitors** page.

If you have more than one monitor, all monitors are deployed each time you deploy monitors.

BEST PRACTICE

When you deploy a monitor, you deploy all monitors. When you take an action on monitors (such as creating, modifying, or reprioritizing monitors) you are prompted to deploy all monitors. For best results, create all planned monitors, and then deploy them at the same time. If you deploy a monitor with restricted management rights, the set of management rights is applied to all deployed monitors. The monitor or Integrity Monitor tools are removed from any endpoints that are not a member of the updated computer management group.

NOTE

You cannot deploy monitors to endpoints with action locks turned on, unless Endpoint Configuration is configured to ignore action locks. For more information, see Install and configure Tanium Endpoint Configuration and Tanium Console User Guide: Managing action locks.

1. Click **Deploy Now** in the banner or **Deploy All Monitors** on the **All Monitors** page.
2. Confirm the deployment. If you have more than one monitor, all monitors are deployed.

© 2026 Tanium Inc. All Rights Reserved

NOTE

- If you enabled Endpoint Configuration approval, monitor deployment must be approved in Endpoint Configuration before monitors deploy to endpoints.
- If you delete a monitor, any rules assigned only to that monitor are automatically deleted from the Integrity Monitor workbench. The rules are no longer active on endpoints, but they are not removed from endpoints. Therefore, you will not see an approval in Endpoint Configuration.

Check the status of deployed monitors

To check the status of deployed monitors on endpoints, ask the question: `Get Client Extensions - Status having Client Extensions - Status:Domain contains integrity_monitor and Computer Name from all machines`.

TIP

To view additional filter options, from the Main menu, go to **Modules > Integrity Monitor > Overview**. In the **Health** section, click the title of the **Endpoint Health** chart. Review the filters In the **Integrity Monitor - Endpoint Health** report that appears.

For more information, see Troubleshooting Integrity Monitor on page 114.

© 2026 Tanium Inc. All Rights Reserved

Managing watched paths with watchlists

Watchlists define a set of files, directories, and Windows registry paths that you want to monitor for changes. Create specific watchlists that target the Tanium Client managed endpoints where Integrity Monitor should watch the specified paths.

IMPORTANT

Use monitors to configure scan settings for endpoints. Each Tanium Client managed endpoint that you target in a watchlist must also be targeted in a monitor for the watchlist to take effect when you deploy watchlists and monitors. To identify endpoints to which you have deployed one or more watchlists but no monitor, ask the question: `Get Computer Name and Client Extensions - Status matches "^integrity_monitor\|monitor_id\|.*$" from all machines with Client Extensions - Status matches "^integrity_monitor\|monitor_id\|0$"`. For more information, see Managing scan settings with monitors on page 81.

Before you begin

- On Windows endpoints, the **Audit File System** operating system permission must be configured to record permission changes. For more information, see Prepare Endpoints on page 67.
  When you enable the **Permission** change type for a path in a watchlist, Integrity Monitor automatically configures the appropriate System Access Control List (SACL) audit settings for every file and folder in that path for that watchlist.
- To specifically record file or registry rename operations on an endpoint, or to specifically record modifications to individual registry values on an endpoint, you must enable the **Collect process and user attribution information** setting in the monitor that you deploy to that endpoint. For more information, see Create or edit a monitor on page 81.
  If you disable this setting, these operations are recorded as follows:
  - Integrity Monitor records a rename operation as a delete operation followed by a create operation. On Solaris and AIX endpoints, Integrity Monitor always records a rename operation as a delete operation followed by a create operation.
  - Integrity Monitor does not return modifications to registry values as events. Create and delete operations are still recorded for individual registry values, regardless of this setting.

Create or edit a watchlist

Create or edit a watchlist to identify the name, path style, and optional watchlist templates. Integrity Monitor includes watchlist templates that contain critical files and directories that are typically monitored for Windows and Linux, and registry paths that are typically monitored for Windows.

© 2026 Tanium Inc. All Rights Reserved

BEST PRACTICE

- Create as many watchlists as necessary, targeted narrowly to watch only the necessary paths on the appropriate endpoints.
- Name each watchlist based on the application, business unit, or compliance standard you want to monitor.
- Use a template as a starting point, and modify the watchlist to suit the needs of your environment. Monitors that use the default watchlists from the included templates might record a significant number of events that are not necessarily cause for concern.

1. From the Main menu, go to **Modules > Integrity Monitor > Watchlists**.
2. Click **Create Watchlist**, or click Edit in the row for an existing watchlist that you want to edit.
3. Enter a **Name** and **Description** for the watchlist.
4. For **Path Style**, select **Windows** or **Unix**.

   NOTE

   The target endpoint operating system and path style must be consistent within a watchlist. For example, you cannot add a Windows file path or a Windows registry path to a watchlist that uses the Unix path style.

5. (Optional) In the **Watchlist Templates** section, select templates from which to add initial paths to the watchlist.
6. In the **Targeting** section, click **Select Computer Groups**, select the computer groups to target, and click **Save**.

   NOTE

   If you edit the targeting for an existing watchlist, you must redeploy all watchlists. For more information, see Deploy watchlists on page 96.

7. Click **Create** (for a new watchlist) or **Save** (for an existing watchlist).

Add and edit paths

After you create a watchlist, you add paths to determine the files, directories, and Windows registry paths that are monitored. If you used a template when creating a watchlist, you can edit the paths that were defined in the template.

Paths

The paths you add to a watchlist determine the files, directories, and registry paths that are monitored on endpoints where the watchlist is deployed. You can configure each path in a watchlist to trigger events for changes in files or registry keys. Integrity Monitor records create, write, delete, or rename operations for files, directories, or registry keys, as well as changes to permission for files or directories.

© 2026 Tanium Inc. All Rights Reserved

To refine the files, directories, and registry paths that are monitored for a watchlist, add *path inclusions* or *path exclusions*. Without inclusions or exclusions defined, the path matches all files and subdirectories in a file path or all subkeys in a registry path. By default, a file path that specifies a directory includes subdirectories recursively, and a registry path that specifies a registry key includes subkeys recursively.

If you directly specify a symbolic link in a path (including with the use of wildcard characters), Integrity Monitor watches the directories or files that the symbolic link references. It also follows symbolic links nested within that referenced directory. To avoid recursion, Integrity Monitor does not watch the referenced directories or files if the symbolic link is contained within a directory that you specify in a path. For example, assume you have a symbolic link at `/my/path/directory-symlink` that references `/other/path/referenced-directory`. If you specify the path `/my/path/directory*`, Integrity Monitor watches the referenced directory `/other/path/referenced-directory`, and it also follows any additional symbolic links contained within `/other/path/referenced-directory`. If you specify the path `/my/path`, then Integrity Monitor watches the symbolic link file itself, but it does not watch the referenced directory.



If a path has a trailing `/*` and you then remove `/*` from the path, Integrity Monitor rescans the top-level directory and subdirectories and creates events for all symbolic links it did not previously see. The timestamp indicates the time that the events were written to the database.

Inclusions and exclusions

If you define path inclusions, the path matches *only* subdirectories, files, or registry subkeys that match the inclusions.

If you define path exclusions, the path does *not* match subdirectories, files, or registry subkeys that match the exclusions.

Exclusions take precedence over inclusions. If you define both inclusions and exclusions, the path matches all directories, files, or registry keys that match the inclusions, *except* those that match exclusions.

For more information, see Reference: Watchlist path inclusions and exclusions.



- Be specific when defining watchlists. For example, watching the `C:\` or `/` directories on endpoints results in a large number of events that are not cause for concern. To help focus on events of concern, follow these guidelines:
    - When possible, add multiple specific file paths instead of a single directory path. Add multiple specific registry subkey paths instead of higher-level registry keys.
    - If you add a directory path, add inclusions for specific file types to watch, such as `*.exe` and `*.dll`.
    - Create multiple, focused watchlists for different types of applications, software components, system configuration areas, or compliance standards. For example, if you need to monitor critical

© 2026 Tanium Inc. All Rights Reserved

BEST PRACTICE

operating system files for Windows, and SQL Server critical files, directories, and registry entries, create separate watchlists for Windows and SQL Server. You can target different computer groups with these watchlists for different monitoring needs.

- Rely primarily on inclusions to refine paths, and try to limit the number of exclusions for cleaner watchlists and more predictable monitoring.

Add a file path

Add file paths to a watchlist to define the files and directories that you want to monitor for changes on certain endpoints.

1. From the Main menu, go to **Modules > Integrity Monitor > Watchlists**.
2. Click the name of the watchlist.
3. (For Windows watchlist path style) Make sure the **File Paths** tab is active.
4. Click **Add Paths > New**.
5. In the **Details** section, provide the information for the path:
   - Enter the absolute path for the file or directory.

     NOTE

     - You can use wildcard characters within a directory or file name in a path, but you cannot use wildcard characters to specify path separators or multiple directory or subkey levels. For example, if you specify the path `/a/*/z`, the path `a/b/z` is monitored, but not `a/b/c/z`.
     - If you specify a root directory, you must include the slash. For example: `D:\`
   - (For Windows watchlist path style) In the **Change Type** section, if you want to record process and user information for permission changes, select **Permission**.
6. In the **Inclusions and Exclusions** section, expand the **Path Inclusions** or **Path Exclusions** section to add path inclusions or exclusions.

   TIP

   You can use wildcard characters. Use a single asterisk (`*`) to represent a string of characters within a directory, file, or registry key name, just as you can in a path. In inclusions or exclusions, you can use two asterisks together (`**`) to include path separators (and therefore multiple directory or subkey levels) in the match. For example, if the path is `/a` and an inclusion is `**/z`, this inclusion matches `/a/b/z`, `/a/b/c/z`, or `/a/b/c/d/e/f/g/z`. For more information, see Reference: Watchlist path inclusions and exclusions.

© 2026 Tanium Inc. All Rights Reserved

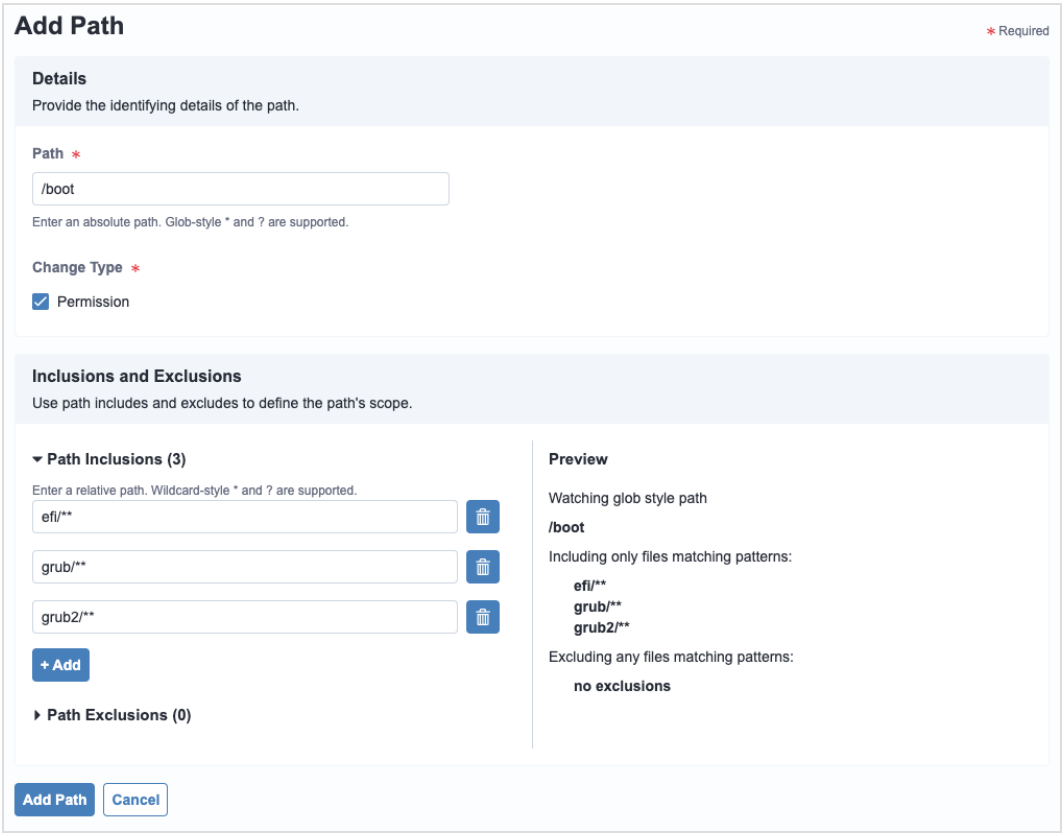
NOTE

If a symbolic link is referenced by a path inclusion or exclusion, it applies only to the symbolic link name itself, not the target of the link.

To add an additional path inclusion or exclusion, click **Add** in the corresponding section.

To delete an inclusion or exclusion, click .

7. Click **Add Path**.



(Windows) Add a registry path

Add registry paths to a watchlist to define the registry keys that you want to monitor for changes on certain endpoints. Registry paths are available only for watchlists with a **Windows** path style.

1. From the Main menu, go to **Modules > Integrity Monitor > Watchlists**.
2. Click the name of the watchlist and then click the **Registry Paths** tab.
3. Click **Add Paths > New**.

© 2026 Tanium Inc. All Rights Reserved

4. For **Path**, enter the absolute path for the registry key.

> NOTE
>
> You can use wildcard characters within a key name in a path, but you cannot use them to specify path separators or multiple key levels. For example, if you have a path `HKEY_LOCAL_MACHINE\*\z`, the path `HKEY_LOCAL_MACHINE\a\z` is monitored, but not `HKEY_LOCAL_MACHINE\a\b\z`.

For more information, see Considerations for registry paths on page 92.

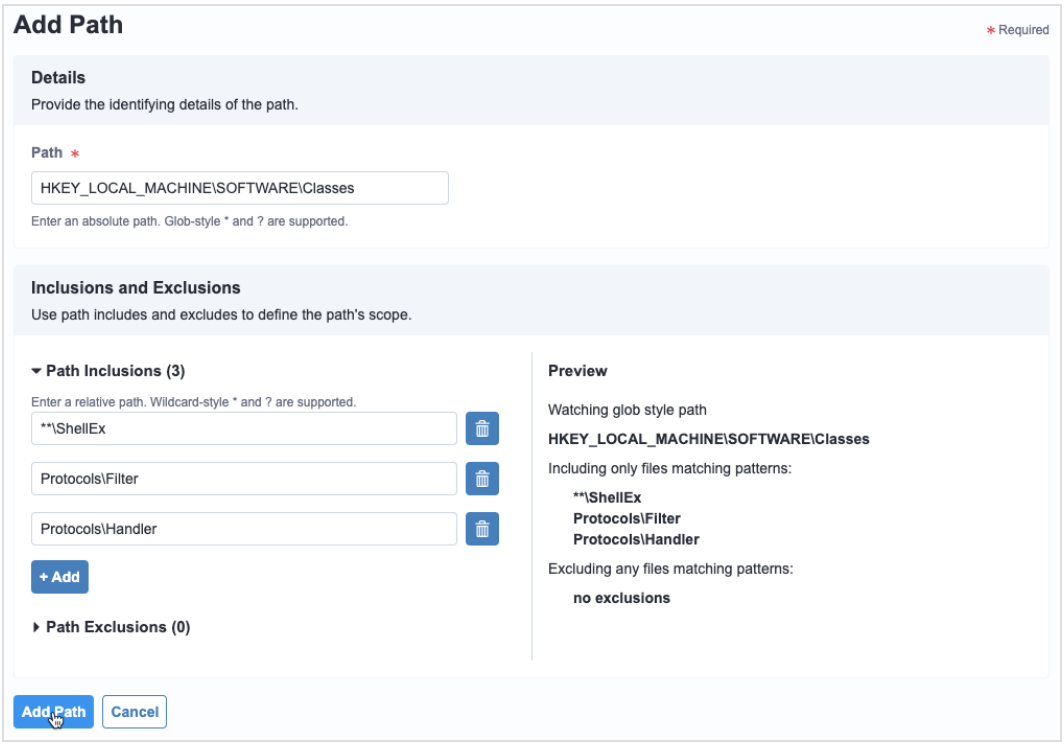
5. In the **Inclusions and Exclusions** section, expand the **Path Inclusions** or **Path Exclusions** section to add path inclusions or exclusions.

> TIP
>
> You can use wildcard characters. Use a single asterisk (*) to represent a string of characters within a directory, file, or registry key name, just as you can in a path.In inclusions or exclusions, you can use two asterisks together (**) to include path separators (and therefore multiple directory or subkey levels) in the match. For example, if the path is `HKEY_LOCAL_MACHINE\a` and an inclusion is `**\z`, this inclusion matches `HKEY_LOCAL_MACHINE\a\b\z`, `HKEY_LOCAL_MACHINE\a\b\c\z`, or `HKEY_LOCAL_MACHINE\a\b\c\d\e\f\g\z`. For more information, see Reference: Watchlist path inclusions and exclusions.

To add an additional path inclusion or exclusion, click **Add** in the corresponding section.

To delete an inclusion or exclusion, click .

6. Click **Add Path**.



© 2026 Tanium Inc. All Rights Reserved

CONSIDERATIONS FOR REGISTRY PATHS

Determining watched subkeys

A path matches all subkeys recursively under a key or keys that are specified by the path. For example, if you specify the path `HKEY_LOCAL_MACHINE\a`, then the path matches all subkeys of the `a` key (such as `HKEY_LOCAL_MACHINE\a\x`, `HKEY_LOCAL_MACHINE\a\x\y`, and `HKEY_LOCAL_MACHINE\a\z`), unless you otherwise exclude them. If the **Collect process and user attribution information** setting is enabled in the monitor that you deploy to that endpoint, all values of matching subkeys are watched.

You cannot monitor an entire subtree, such as `HKEY_LOCAL_MACHINE`, and you cannot specify individual values within a key.

Using an abbreviation for a subtree

You can use the abbreviation for the subtree in a path. Integrity Monitor expands the subtree name when you save your changes. For example, you can enter the path `HKLM\MyKey`, which is saved as `HKEY_LOCAL_MACHINE\MyKey`.

Subtree abbreviations

Subtree name	Abbreviation
`HKEY_LOCAL_MACHINE`	`HKLM`
`HKEY_USERS`	`HKU`

Using the HKEY_CURRENT_USER subtree in a path

When you add a path in the `HKEY_CURRENT_USER` subtree, such as `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy`, Integrity Monitor changes the `HKEY_CURRENT_USER` subtree in the path to `HKEY_USERS\*` when you save your changes (for example, `HKEY_USERS\*\Software\Microsoft\Windows\CurrentVersion\Group Policy`). Because the Tanium Client uses the SYSTEM account, the `HKEY_CURRENT_USER` subtree applies to the SYSTEM account rather than the user account that is currently signed in to Windows. Using `HKEY_USERS\*` instead lets Integrity Monitor record events for all users, including the user account that is currently signed in to Windows.

Using a redirected registry key in a path

For 64-bit Windows, the registry redirector maps some keys, such as `HKEY_LOCAL_MACHINE\SOFTWARE\`, to a `WOW6432Node` subkey (for example, `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node`) for use by 32-bit applications. When you add key paths that are redirected under WOW64, the watchlist does not automatically include the parallel key paths under the `WOW6432Node` keys. If you want to monitor keys under these paths, you must enter them separately.

Import a path

You can import paths to a watchlist from a file that you created in another monitoring tool or from a template that is provided with Integrity Monitor.

© 2026 Tanium Inc. All Rights Reserved

ADD PATHS FROM A FILE

Tanium provides limited support for importing paths from Tripwire configurations, Open Source HIDS Security (OSSEC) configurations, Log Correlation Engine (LCE) Client policies, or CSV files. For more information, see CSV format for path imports. An imported file can contain either file and directory or registry paths.



Use a backslash (\) to escape backslashes in Windows paths.

1. From the Main menu, go to **Modules > Integrity Monitor > Watchlists**.
2. Click the name of the watchlist.
3. Click **Add Paths > Import From File**.
4. Click **Choose Files**.
5. Browse to and select the path file or files and click **Open**.
6. Click **Import** to import the file or files.

CSV format for path imports

The first line of a CSV file specifies the field names and defines the order of the values in the subsequent rows. The import uses the following fields:

Fields for importing a path

Field	Description
`path`	The file, directory, or registry path
`ops_permission`	Whether to monitor a Windows file path for changes in permission (`on` or `off`)
`excludes_spec`	An exclusion to apply to the path

You can add additional exclusions to a path by adding subsequent lines with all fields empty except for `excludes_spec`. These lines inherit the blank field values from the parent entry.

The following example CSV file demonstrates the structure to use to import paths to Integrity Monitor.

```
path,ops_permission,excludes_spec
C:\\autoexec.bat,on,
C:\\Windows\\logs,off,**
C:\\Windows,on,NtServicePackUninstall
,,NtServicePackUninstall\\**
,,NtUninstall
,,NtUninstall\\**
,,Help
,,Help\\**
C:\\Windows\\assembly,on,**
```

© 2026 Tanium Inc. All Rights Reserved

Line descriptions for example CSV file

In the preceding example, this line adds the path `C:\autoexec.bat` and enables monitoring file permission changes:

```
C:\\autoexec.bat,on,
```

This line adds the path `C:\Windows\logs`, disables monitoring file permission changes, and adds the exclusion `\**`, which excludes any subdirectories within `C:\Windows\logs`:

```
C:\\Windows\\logs,off,\\**
```

These lines add the path `C:\Windows`, enable monitoring file permission changes, and add exclusions for three directories and their subdirectories (`NtServicePackUninstall`, `NtUninstall`, and `Help`):

```
C:\\Windows,on,NtServicePackUninstall
,,NtServicePackUninstall\\**
,,NtUninstall
,,NtUninstall\\**
,,Help
,,Help\\**
```

Finally, this line adds the path `C:\Windows\assembly`, enables monitoring file permission changes, and adds the exclusion `\**`:

```
C:\\Windows\\assembly,on,\\**
```

ADD PATHS FROM TEMPLATES

Integrity Monitor includes watchlist templates that contain critical files and directories that are typically watched for Windows and Linux. You can use these templates when creating new watchlists, and you can also use them to add paths to existing watchlists.

1. From the Main menu, go to **Modules > Integrity Monitor > Watchlists**.
2. Click the name of the watchlist.
3. Click **Add Paths > Import From Templates**.
4. Select one or more templates and click **Import**.

© 2026 Tanium Inc. All Rights Reserved

BEST PRACTICE

Use a template as a starting point, and modify the watchlist to suit the needs of your environment. Monitors that use the default watchlists from the included templates might record a significant number of events that are not necessarily cause for concern.

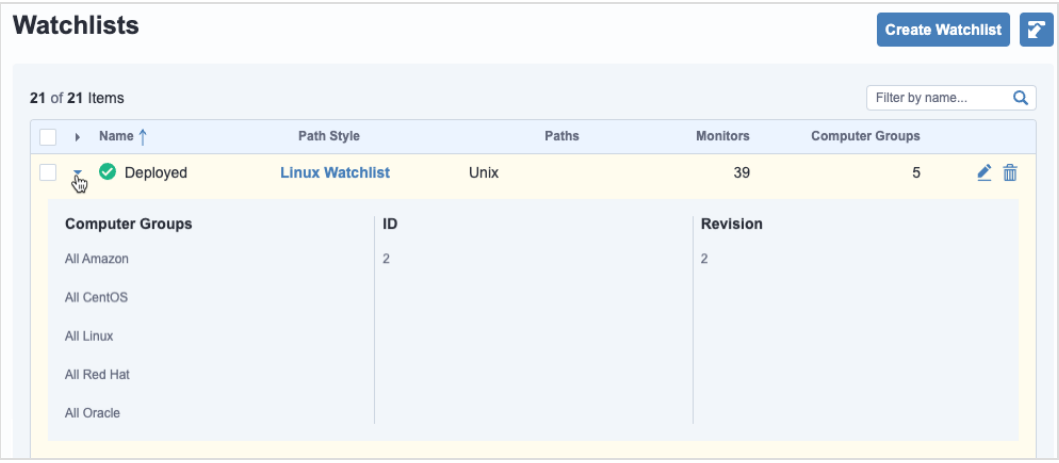
(Windows path style only) Update the Permission change type setting for multiple paths

1. From the Main menu, go to **Modules > Integrity Monitor > Watchlists**.
2. Click the name of the watchlist.
3. Select one or more paths.
4. Click **Manage Change Type**.
5. Update the selection for **Permission** and click **Save**.

Review watchlist details

On the **Watchlists** page, click Expand for a watchlist to view the monitors that target the same endpoints, computer groups that the watchlist targets, and the revision number of the watchlist.

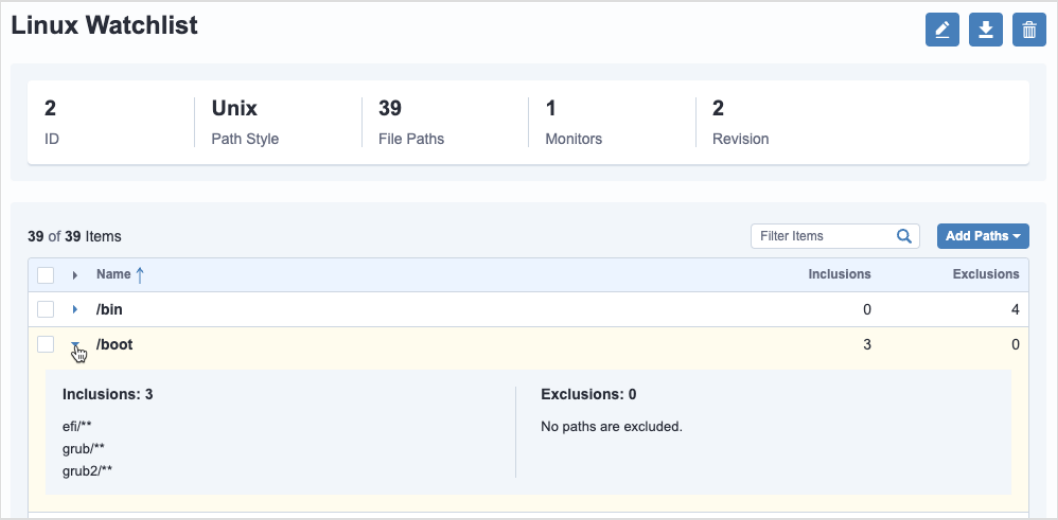
Watchlist details



To view paths for a watchlist, click the name of the watchlist. From the details page for the watchlist, click Expand for a path to view inclusions and exclusions for that path.

Linux watchlist paths

© 2026 Tanium Inc. All Rights Reserved



To determine the watchlists that apply to particular endpoints, ask a question using the `Integrity Monitor - Active Watchlists` sensor.

Deploy watchlists

After you create, edit, or delete watchlists, you must deploy all watchlists to the endpoints. A **Deploy Now** banner appears, and **Pending Deployment** (new watchlists), **Needs Deployment** (changed watchlists), or **Pending Deletion** (deleted watchlists) appears in the **Status** column for the watchlist on the **Watchlists** page.

If you have more than one watchlist, all watchlists are deployed each time you deploy watchlists.

BEST PRACTICE

When you deploy a watchlist, you deploy all watchlists. When you create, edit, or delete a watchlist, you are prompted to deploy all watchlists. For best results, create all planned watchlists, and then deploy them at the same time. If you deploy watchlists as a user with restricted management rights, the set of management rights is applied to all deployed watchlists. All watchlists are removed from any endpoints that are not a member of the updated computer management groups. Ensure the same set of computer management groups are assigned to all users who deploy watchlists.

NOTE

You cannot deploy watchlists to endpoints with action locks turned on, unless Endpoint Configuration is configured to ignore action locks. For more information, see Install and configure Tanium Endpoint Configuration and Tanium Console User Guide: Managing action locks.

1. Click **Deploy Now** in the banner or **Deploy Watchlists** on the **Watchlists** page.
2. Confirm the deployment. If you have more than one watchlist, all watchlists are deployed.

© 2026 Tanium Inc. All Rights Reserved

NOTE

If you enabled Endpoint Configuration approval, watchlist deployment must be approved in Endpoint Configuration before watchlists deploy to endpoints.

IMPORTANT

Each Tanium Client managed endpoint that you target in a watchlist must also be targeted in a monitor for the watchlist to take effect when you deploy watchlists and monitors. For more information, see Managing scan settings with monitors on page 81.

Export a watchlist

You can export a watchlist to transfer it to another environment (for example, if you created the watchlist in a QA or lab environment and you want to move it to a production environment) or for backup.

1. From the Main menu, go to **Modules > Integrity Monitor > Watchlists**.
2. Click the name of a watchlist.
3. Click Export Watchlist .

   The exported watchlist downloads in your browser in JSON format.

Import a watchlist

You can import a watchlist into another environment (for example, you want to add the watchlist to a production environment) or for backup.

1. From the Main menu, go to **Modules > Integrity Monitor > Watchlists**.
2. Click Import Watchlist .
3. Click **Choose File**.
4. Browse to the watchlist file and click **Open**.
5. Click **Import** to import the file.

© 2026 Tanium Inc. All Rights Reserved

Viewing events

After a monitor and watchlists deploy to Tanium Client managed endpoints, events get returned that match the deployed watchlists.

View events for a monitor, label, or rule

You can view an overview of events that are returned by a monitor or that have a specific label.

- **To view events returned by a monitor in the past day:** From the Main menu, go to **Modules > Integrity Monitor > Monitors** and click the name of the monitor for which you want to see events.
- **To view events from the past day that have a specific label:** From the Main menu, go to **Modules > Integrity Monitor > Labels**, click the name of the label for which you want to see events, and click the **Events** tab.

In this view, Integrity Monitor aggregates events that share the same path, user, process, and operation every 15 minutes to help you identify common events on monitored endpoints. To retrieve more specific information about events and the endpoints where they occurred, you can select events and then click **Drill Down**. For more information, see Tanium Interact User Guide: Drill down.

To filter the events, use the **Filter by text** box, or expand the **Filters** section.

To view earlier events, ask a question using one of the Integrity Monitor sensors. For more information, see Use sensors to view events or event counts on page 98. You can view events from the past 250 hours.



Tanium Client Recorder Extension disregards events caused by the Tanium Client, even on watched paths.

Pause and resume the event view

To temporarily stop incoming events from being added to the results grid, click Pause in the results grid. To resume viewing incoming events in real time, click Resume.

The event view automatically pauses when you select events.

Download the full list of events or selected events

To download the full list of events in CSV format, click Export in the results grid.

To download the information from specific events in CSV format, select events from the results grid, and click **Export**.

Use sensors to view events or event counts

You can ask questions in Interact with the Integrity Monitor sensors to view events with specific criteria or event counts. For more information, see Tanium Interact User Guide: Asking questions and searching endpoints in Interact.

© 2026 Tanium Inc. All Rights Reserved

Sensors provided by Integrity Monitor to view events and event counts

Sensor	Description	Parameters	Returned Columns

Integrity Monitor - Monitor Events	Returns recorded events. The sensor combines events that share the same path, user, process, and change type into groups by time period.	• **Row Limit:** The maximum number of rows to return. Each row is a group of matching events for a time period.
		• **Monitor ID:** The monitor from which you want to return events. The ID for each monitor appears on its detail page. Specify `0` to return events from all monitors.
		• **Rolling Minute Offset:** The number of minutes into the past from which to return events. You can view events as old as 15,000 minutes (250 hours).
		• **Timestamp minute resolution:** The number of minutes to use in grouping matching events.
		• **Exclude label list:** Specifies whether the **CSV Label Search** field contains labels that should be excluded from the returned results.
		• **CSV Label Search:** Labels to include or exclude in the results, depending on whether you enable **Exclude label list**:
		  ◦ **Disabled:** The returned results include only events with the labels you specify.
		  ◦ **Enabled:** The returned results include only events that do not have the
			• **Event Time**: The date and time when the event occurred.
			• **File Path**: The file path or registry path where the event occurred.
			• **Change Type**: The change types applied to the event based on rules. For more information, see Create a rule on page 102.
			• **Process Path**: If the event is a process change, the path where the event occurred.
			• **User**: The user who performed the change.
			• **Detail**: The detected change, for example, `user_name=root group_name=root`. The details provide context for what triggered the event, such as a modified file or updated registry key.
			• **Hash**: A cryptographic fingerprint of the file or object at the time of the event. The hash is used to verify integrity and help detect tampering.
			• **Hashed At**: The date and time when the hash was created.
			• **Labels**: The labels applied to the event.
			• **Watchlists**: The watchlists that identified the event.
			• **ServiceNow Change IDs**: ServiceNow change request IDs. Use the IDs to help correlate detected changes with approved or planned activities.

Sensors provided by Integrity Monitor to view events and event counts (continued)

Sensor	Description	Parameters	Returned Columns
Integrity Monitor - Monitor Events Unlabeled	Returns recorded events that do not have labels applied. The sensor combines events that share the same path, user, process, and change type into groups by time period. For more information, see Labeling events with rules on page 101.	• **Row Limit:** The maximum number of rows to return. Each row is a group of matching events for a time period. • **Monitor ID:** The monitor from which you want to return events. The ID for each monitor appears on its detail page. Specify `0` to return events from all monitors. • **Rolling Minute Offset:** The number of minutes into the past from which to return events. You can view events as old as 15,000 minutes (250 hours). • **Timestamp minute resolution:** The number of minutes to use in grouping matching events.	• Event Time • File Path (returns a registry path when applicable) • Change Type • Process Path • User • Detail • Hash • Hashed At • Watchlists
Integrity Monitor - Event Count	Returns ranges of event counts. You can use this sensor in questions to help identify which endpoints have high numbers of events and might require investigation.	**Rolling Minute Offset**: The number of minutes into the past from which to return events. You can view events as old as 15,000 minutes (250 hours).	Integrity Monitor - Event Count
Integrity Monitor - Event Count By Watchlist	Returns ranges of event counts specific to each watchlist. You can use this sensor in questions to help identify which endpoints have high numbers of events for certain watchlists and might require investigation, or which watchlists generate high numbers of events and might require tuning.	**Rolling Minute Offset**: The number of minutes into the past from which to return events. You can view events as old as 15,000 minutes (250 hours).	• Watchlist ID • Event Count

© 2026 Tanium Inc. All Rights Reserved

Labeling events with rules

Configure labels to annotate events or to indicate which events need investigation or remediation, and use rules to automatically label events based on their attributes.

Integrity Monitor includes the following default labels:

- **Important**
- **Suspicious**
- **Expected**
- **Ignored**
- **Planned**

Customize labels

You can customize the default labels or create your own labels. After you define labels, you can associate the labels with rules.

> NOTE
> Any change to a default label affects every monitor.

1. From the Main menu, go to **Modules > Integrity Monitor > Labels**.
2. Click **Create Label** to create a label, or click Edit in the row for the label you want to edit.
3. Enter a **Name** and **Description**.

   > NOTE
   > You cannot edit the name of an existing label.

4. Click **Create** (for a new label) or **Update** (for an existing label).

To delete a label, click Delete in the row for the label.

Use rules to automatically label events

Create rules to automatically label events based on their attributes. You can configure rules to help differentiate among planned, expected, ignored, or suspicious changes, or you can use rules to apply custom labels to suit your environment.

Each rule applies to either a single monitor or all monitors and applies a single label based on the criteria you specify.

© 2026 Tanium Inc. All Rights Reserved

Create a rule

BEST PRACTICE

Create rules to apply default labels as appropriate:

- Create rules that apply the **Planned** label to events that occur during an approved change window. You can also integrate Integrity Monitor with your IT workflow in ServiceNow Change Management to determine change windows based on change requests or change tasks. For more information, see Integrating with IT workflows in ServiceNow on page 108.
- Create rules that apply the **Expected** label to events for changes performed by approved administrator or service accounts.
- Create rules that apply the **Suspicious** label to events for changes that normally should not occur.

1. From the Main menu, go to **Modules > Integrity Monitor > Rules** and click **Create Rule**.
2. In the **Summary** section, enter a **Name** and **Description**.
3. In the **Rule Criteria** section, select an attribute and operator, enter the appropriate criteria, and click **Apply**.

NOTE

- Text that you enter for the criteria value is case sensitive. For example, the value `/mypath` for the attribute **File/Registry Path** does not match the path `/MyPath` on a Tanium Client managed endpoint.
- If you select the **Change Type** attribute, enter one of the following values:
  - `ChangedTime`
  - `CreateNewFile`
  - `DeletePath`
  - `FileOwnershipChange`
  - `FilePermissionChange`
  - `RegistryCreate`
  - `RegistryDelete`
  - `RegistryRename`
  - `RegistrySet`
  - `RenamePath`
  - `Write`
- If you select the **Process Path** or **User Name (event)** attributes, you can select the **exists** operator with a **True** or **False** value to match on the existence of those attributes in the events.

© 2026 Tanium Inc. All Rights Reserved

NOTE

- Wildcard characters (`*`, `?`) are evaluated as a literal character. To simulate wildcard characters, use a grouping with an `AND` operator.

4. Click **Row** or **Grouping** to add additional criteria and groups of conditions as necessary, and select **AND** or **OR** to determine how the conditions are applied.
5. In the **Actions** section, select the **Monitor** to which you want to apply this rule and the **Label** you want to apply to events that match the rule.
6. Click **Create**.

NOTE

- Newly created rules only affect new events. Past events cannot be labeled by a new rule.
- Events are labeled by rules as they occur and appear within approximately two minutes.
- To support consistent auditing, you cannot directly edit a rule. If you want to modify a rule, you must deactivate it, duplicate it, and save the new rule. For more information, see Deactivate a rule on page 105 and Duplicate a rule on page 105.

Import rules

You can import multiple rules from a CSV file.

1. From the Main menu, go to **Modules > Integrity Monitor > Rules**.
2. Click Import Rules .
3. Click **Choose File**.
4. Browse to a CSV file and click **Open**.
5. Click **Import**.

EXAMPLE TANIUM CSV FILE USED TO IMPORT RULES

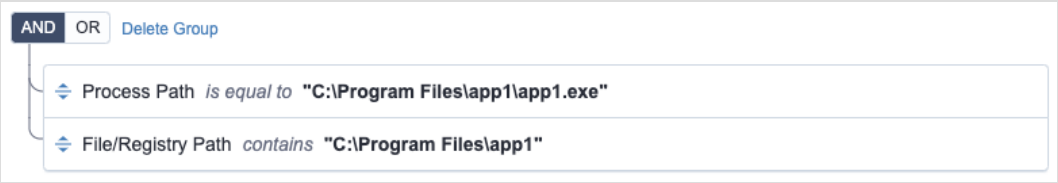
```
name,description,note,monitor_id,label_id,field,operator,value
app1 generated events,events generated by app1,CR12345,1,5,,,
,,,,,process,eq,C:\Program Files\app1\app1.exe
,,,,,file,contains,C:\Program Files\app1
rule 2,rule 2 description,rule 2 note,1,5,,,
,,,,,event_timestamp,gt,2018-06-01T06:00:00.000Z
,,,,,event_timestamp,lt,2018-07-01T06:00:00.000Z
,,,,,file,contains,C:\Program Files
```

© 2026 Tanium Inc. All Rights Reserved

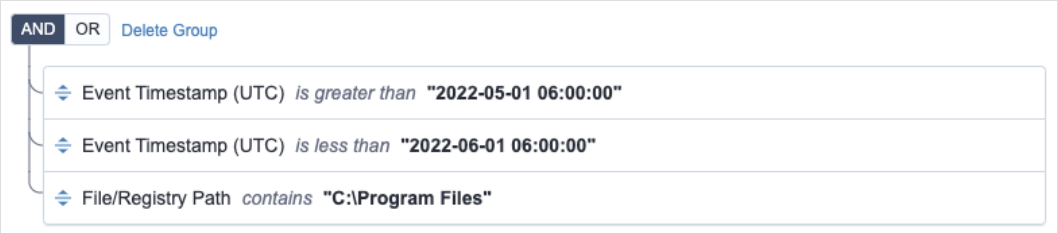
The first line of the file defines the field names of `name`, `description`, `note`, `monitor_id`, `label_id`, `field`, `operator`, and `value`. The first line for a rule defines the settings for a rule using the `name`, `description`, `note`, `monitor_id`, and `label_id`, and the values for `field`, `operator`, and `value` are left blank. The subsequent lines have blank values for `name`, `description`, `note`, `monitor_id`, and `label_id`, and define each condition for the rule using the `field`, `operator`, and `value` fields. Imported conditions are in a single group and use the `AND` operator.

The preceding CSV example contains two rules that each apply to the monitor with ID 1 and apply the label with ID 5:

- The rule named `app1 generated events` defines two conditions.



- The rule named `rule 2` defines three conditions.



Deploy rules

Deploy rules to endpoints so that Integrity Monitor can apply labels to events directly on endpoints.

After you create, delete, or save updates to a rule, a **Deploy Now** banner appears, and **Pending Active** appears in the **Status** column for the rule on the **Rules** page. To deploy the updates to the configured endpoints, click **Deploy Now** in the banner or **Deploy Rules** on the **Rules** page.

BEST PRACTICE

When you deploy rules, you deploy all rules. When you take an action on rules (such as creating, deactivating, or deleting), you are prompted to deploy all rules. For best results, create all planned rules and then deploy them at the same time. If you deploy a rule with restricted management rights, the set of management rights is applied to all deployed rules. The rule or Integrity Monitor tools are removed from any endpoints that are not a member of the updated computer management group.

NOTE

- You cannot deploy rules to endpoints with action locks turned on, unless Endpoint Configuration is configured to ignore action locks. For more information, see Install and configure Tanium Endpoint Configuration and Tanium Console User Guide: Managing action locks.

© 2026 Tanium Inc. All Rights Reserved

NOTE

- If you enabled Endpoint Configuration approval, rule deployment must be approved in Endpoint Configuration before rules deploy to endpoints.

Deactivate a rule

Deactivate a rule if you no longer want the rule to run. On the **Rules** page, select the rule you want to deactivate and click **Deactivate**.

Deactivating a rule does not delete any labeled events associated with the rule.

NOTE

- To support consistent auditing, deactivation is permanent. If you want to reactivate the rule, you must duplicate it and save the new rule.
- You cannot deactivate a rule that is not deployed. You can delete the rule if you no longer want to deploy it. For more information, see Delete a rule on page 105.

Duplicate a rule

To support consistent auditing, you cannot directly edit a rule or reactivate a deactivated rule. However, you can duplicate an existing rule, modify settings, and save the new rule.

1. From the **Rules** page, click Duplicate in the row for the rule you want to duplicate.
2. On the **Create Rule** page, the settings are pre-populated to match the rule you copied, and the default **Name** indicates it is a duplicated rule.
3. Edit the rule settings as necessary and click **Create**.

Delete a rule

To delete a rule, on the **Rules** page, select the rule and click Delete. The deletion is pending until the next time you deploy rules.

NOTE

If you delete a rule, any labels that Integrity Monitor applied to events based on that rule remain in place for those existing events. Events that occur after you delete the rule and redeploy all rules are not labeled.

© 2026 Tanium Inc. All Rights Reserved

Sending and reporting events

Send events to a SIEM, SOAR, or other data lake or log solution using Connect.

Use Connect to send events

You can create saved questions that include any of the sensors provided by Integrity Monitor and then use those saved questions as connection sources in Connect.



When you send events to a SIEM, SOAR, or other data lake, send only unlabeled events and events that are required for regulatory compliance and auditing. (In some cases, all events might be required.)

1. Create a saved question that returns the events you want to report using the `Integrity Monitor - Monitor Events` or `Integrity Monitor - Monitor Events Unlabeled` sensor. Include any other sensors you want to include as columns in the data. For more information, see Tanium Interact User Guide: Managing saved questions in Interact.
2. Create a connection in Connect. Use Saved Question for the source type, and select the saved question that you created. For more information, see Tanium Connect User Guide: Connect overview.

Create incidents for unlabeled events in ServiceNow Incident Management

If you use ServiceNow Incident Management, you can create incidents based on unlabeled events by using an email destination in Connect and configuring email actions in ServiceNow to create incidents.

1. Configure inbound email actions in ServiceNow to create incidents based on emails from Tanium. For more information, see ServiceNow Product documentation: Inbound email actions.
2. Create a saved question using the `Integrity Monitor - Monitor Events Unlabeled` sensor. For more information, see Tanium Interact User Guide: Managing saved questions in Interact.
3. From the Main menu, go to **Modules > Connect > Connections** and click **Create Connection**.
4. Configure the following settings in the connection:
    - Specify a **Name** and optional **Description** for the connection.
    - For **Source**, select **Saved Question**.
    - In the **Saved Question Name** list, select the saved question you created.
    - Select the appropriate **Computer Group**.
    - Select **Flatten Results**.
    - For **Destination**, select **Email (O365)** or **Email (SMTP)**.

© 2026 Tanium Inc. All Rights Reserved

- Complete the Email configuration by following the steps in the corresponding topic in the Connect User Guide:
  - **Email (O365):** Connect User Guide: Configure the email results destination
  - **Email (SMTP):** Connect User Guide: Configure the email (SMTP) results destination. In the **Advanced** section, select **Attachment**, and enter an **Attachment File Name** that ends with `.csv`.
- In the **Configure Output** section, for **Format**, select **CSV**.
- In the **Schedule** section, configure a schedule for the connection.

5. Click **Save**.

BEST PRACTICE

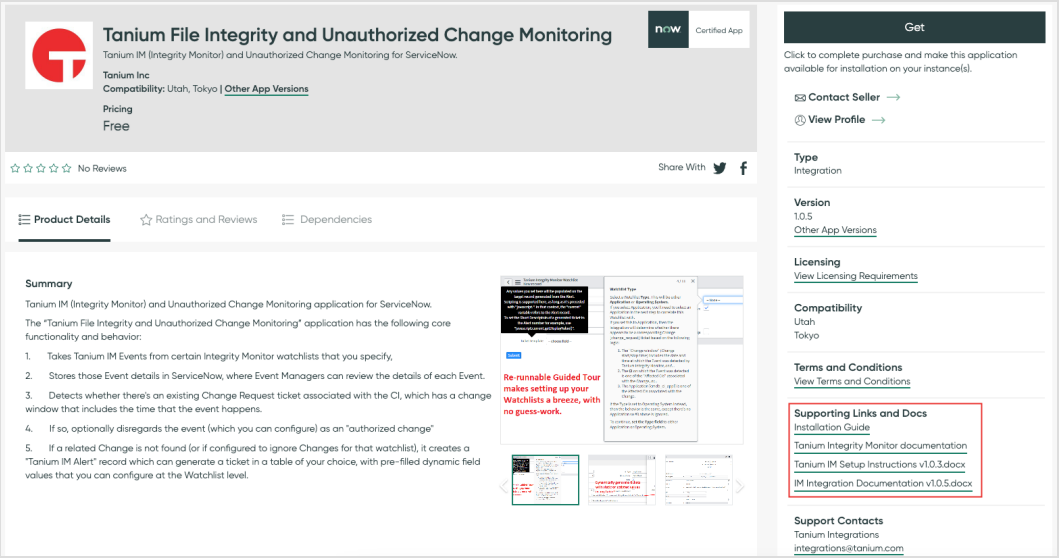
Manually run the new email connection while monitoring incidents in ServiceNow to make sure that new incidents are successfully created. Open the first new incident and confirm that it includes a CSV file with the expected information.

Monitor for unauthorized changes with ServiceNow

If you install the Tanium File Integrity and Unauthorized Change Monitoring ServiceNow application, you can send events from Integrity Monitor to ServiceNow to correlate them with Change Requests.

For more information, see Tanium Data Sheet: Tanium File Integrity and Unauthorized Change Monitoring for ServiceNow.

To download the application from the ServiceNow Store, see ServiceNow: Tanium File Integrity and Unauthorized Change Monitoring. You can download the setup instructions from the **Supporting Links and Docs** section on the application page: **Tanium File Integrity and Unauthorized Change Monitoring ServiceNow details**



© 2026 Tanium Inc. All Rights Reserved

Integrating with IT workflows in ServiceNow

The Tanium™ File Integrity Monitoring integration can automatically label events based on change requests or change tasks in ServiceNow. You can then determine which events are authorized and filter out events within authorized change windows.

You can also automatically create incidents in ServiceNow Incident Management for unexpected events by using inbound email actions in ServiceNow and an email destination in Connect. For more information, see Create incidents for unlabeled events in ServiceNow Incident Management on page 106.

You can configure Integrity Monitor to synchronize change requests, change tasks, or both. The change requests or change tasks determine the authorized change windows for specific Tanium Client managed endpoints (which are synchronized with ServiceNow configuration items). For events that occur on endpoints that are mapped to those configuration items during an authorized change window, Integrity Monitor automatically applies the **ServiceNow** label and records the ID of the change request or change task from ServiceNow.

Before you begin

Requirements

- ServiceNow Madrid release or later.
- Endpoints must be defined in ServiceNow as configuration items (CIs). One method to create configuration items for endpoints is by exporting data from Tanium™ Asset to your ServiceNow CMDB. For more information, see Tanium Asset User Guide: Exporting data.
- Your ServiceNow account must be configured with the appropriate permissions. For more information, see ServiceNow permissions required for least-privilege access.

ServiceNow permissions required for least-privilege access

Tanium Integrity Monitor must have the following access for integration with ServiceNow. For specific configuration in ServiceNow, work with your ServiceNow administrator, and consult the ServiceNow Documentation.

Least-privilege ServiceNow permissions for Tanium Integrity Monitor

Access control type	Operation	Name
REST_Endpoint	execute	`/api/now/cmdb/meta`[1]
record	read	`change_request.end_date`
record	read	`change_request.number`
record	read	`change_request.start_date`

© 2026 Tanium Inc. All Rights Reserved

Least-privilege ServiceNow permissions for Tanium Integrity Monitor (continued)

Access control type	Operation	Name
record	read	`change_request.state`
record	read	`change_request.sys_id`
record	read	`change_task.change_request`
record	read	`change_task.planned_end_date`
record	read	`change_task.planned_start_date`
record	read	`change_task.number`
record	read	`change_task.state`
record	read	`change_task.sys_id`
record	read	`cmdb_ci_hardware.sys_id`
record	read	`sys_choice.element`
record	read	`sys_choice.label`
record	read	`sys_choice.value`
record	read	`task_ci.ci_item`
record	read	`task_ci.task`

[1] Access to the CMDB Meta API typically requires the ITIL role, but you can explicitly grant it to another role for the purpose of Integrity Monitor access.

Configure the integration with ServiceNow

To create a ServiceNow integration, you need to specify connection information, the ServiceNow mappings, and the schedules to synchronize data with ServiceNow.

Specify the connection information

1. From the Integrity Monitor **Overview** page, click Settings, and then click the **Integrations** tab.
2. Click **Create Integration**.
3. In the **Summary** section, enter a **Name** for the integration.
4. In the **Destination** section, enter the **Host URL** of your ServiceNow instance.

© 2026 Tanium Inc. All Rights Reserved

5. Enter the **User Name** and **Password** for a ServiceNow account that has read privileges to query Change Management and CMDB data. To create a ServiceNow user with the minimum privileges necessary, see ServiceNow permissions required for least-privilege access on page 108.
6. Click **Establish Connection**.

Configure ServiceNow mappings

Integrity Monitor uses the statuses of Open, Closed, and Canceled to manage authorized change windows. You must map these statuses to the states used in your ServiceNow change requests and change tasks. You must also map the attributes that identify an endpoint in ServiceNow to the appropriate Integrity Monitor sensors.

1. For **Create rules from**, select **Change Requests and Tasks**, **Change Requests**, or **Change Tasks**. This setting determines whether authorized change windows are determined by ServiceNow change requests, change tasks, or both.
2. If you are mapping change requests, in the **Change Requests** section select the appropriate ServiceNow states for **Open States**, **Closed States**, and **Canceled States**. If you use the default change request states in ServiceNow, you can leave the default mapping in place.

   You must have at least one ServiceNow state selected for each Integrity Monitor status.
3. If you are mapping change tasks, in the **Change Tasks** section select the appropriate ServiceNow states for **Open States**, **Closed States**, and **Canceled States**. Select the ServiceNow **Task Type** to use to define authorized change windows.

   You must have at least one ServiceNow state selected for each Integrity Monitor status, and you must select at least one **Task Type**.
4. In the **Endpoints** section, select each **Tanium Sensor** to identify endpoints, and select the corresponding **ServiceNow Attribute** for each sensor. By default, the `Computer Name` and `Computer Serial Number` sensors are mapped to the `Name` and `Serial Number` ServiceNow attributes.

   To add more attribute mappings to help identify endpoints, click Add Mapping . To remove an attribute mapping, click Remove Mapping .

Configure the schedules to synchronize data with ServiceNow

To enable the integration, you must enable and configure schedules to synchronize change data from ServiceNow.

1. In the **Schedule** section, select **Sync this mapping on a defined schedule**.
2. Configure the **ServiceNow Sync** schedule, which determines when the Tanium Server synchronizes change windows from ServiceNow, maps configuration items from ServiceNow to Tanium endpoints, and generates rules.
3. Configure the **Tanium Endpoint Sync Schedule**, which determines when the Tanium Server gathers identification data from endpoints. For best results, this synchronization should be more frequent than the ServiceNow synchronization. The data is

© 2026 Tanium Inc. All Rights Reserved

synchronized with ServiceNow during the following ServiceNow synchronization.

4. Configure the remaining advanced settings as necessary.

Tanium Integrity Monitor advanced settings for ServiceNow data synchronization

Setting	Description
Request Timeout	The time in seconds that Integrity Monitor waits for a response from ServiceNow. Valid values range from 30 to 180 seconds.
Batch Size	The number of records to request from ServiceNow at one time. Valid values range from 500 to 10000 records.
Look Back Days / Look Ahead Days	The number of days into the past and future for which Integrity Monitor should synchronize change requests or change tasks. Valid values range from 1 to 14 days.
Concurrent Requests	The number of concurrent requests to submit to ServiceNow. A lower value might lessen the performance impact on your ServiceNow instance. Valid values range from 1 to 8 requests.
Distribute Rules Over	The number of minutes over which the Tanium server should distribute the automatically generated rules that apply the ServiceNow label. The distribution is randomized over the specified duration to avoid spikes in network or other resource utilization. Valid values range from 5 to 30 minutes.
Change Window Extension	The number of hours to extend the beginning and end of a change window determined from ServiceNow. The **ServiceNow** label is still applied during this extended time. Changing this value affects only newly synchronized change windows; any existing change windows keep the extended time that was configured when they were first synchronized. Valid values range from 1 to 24 hours.

Complete the configuration

After you configure the necessary settings, click **Create**.



ServiceNow rules deploy to endpoints on the next synchronization determined by the ServiceNow Sync schedule. If you enabled Endpoint Configuration approvals, ServiceNow rule deployment must be approved in Endpoint Configuration before ServiceNow rules deploy to endpoints. For more information, see Tanium Endpoint Configuration User Guide: Managing approvals.

Manage authorized events

Review events to identify authorized ServiceNow change requests or tasks.

ServiceNow change requests or tasks with an Open state

When Integrity Monitor synchronizes data with ServiceNow, it determines authorized change windows from change requests, change tasks, or both (depending on the settings) with a state that you mapped to the Open status during configuration.

© 2026 Tanium Inc. All Rights Reserved

Integrity Monitor applies the **ServiceNow** label to events that fall within these authorized change windows on associated Tanium endpoints.

ServiceNow change requests or tasks with a Closed state

For change requests or change tasks with a ServiceNow state that you have mapped to the Closed status, Integrity Monitor no longer applies the **ServiceNow** label to associated events.

ServiceNow change requests or tasks with a Canceled state

For change requests or change tasks with a ServiceNow state that you have mapped to the Canceled status, Integrity Monitor removes the **ServiceNow** label from associated events if it has previously been applied.

Review events

When you view events, you can apply a filter to include only events that do not contain the **ServiceNow** label. The resulting list of events then includes only those that are not associated with approved changes in ServiceNow Change Management. For more information about viewing events, see Viewing events on page 98. For more information, see Tanium Interact User Guide: Filter question results.

When you review events with the **ServiceNow** label, you can use the change request or change task from the ID of the event to locate the associated change request or change task in ServiceNow Change Management.

© 2026 Tanium Inc. All Rights Reserved

Maintaining Integrity Monitor

Perform monthly maintenance tasks to ensure that Integrity Monitor successfully performs scheduled activities on all the targeted Tanium Client managed endpoints and does not overuse endpoint or network resources. If Integrity Monitor is not performing as expected, you might need to troubleshoot issues or change settings. For more informaiton, see Troubleshooting Integrity Monitor on page 114 for related procedures.

1. From the Main menu, go to **Modules > Integrity Monitor > Overview**.
2. Scroll to the **Health** dashboard to review any health check errors.
3. To investigate issues with client extensions that appear in the panel, click **Health Check**. For specific troubleshooting steps, see Identify and resolve issues with Client Extensions on page 115.
4. To see detailed health information about endpoints that are included in an error category, click the bar for that category in the chart. For specific troubleshooting steps, see Reference: Endpoint monitoring health check errors on page 121.

Monitor and troubleshoot Integrity Monitor health

Endpoints with errors appear in the **Endpoint Health** panel on the Integrity Monitor **Overview** page. To see all endpoint health errors that are relevant to Integrity Monitor, click the title of the chart. To get detailed health information about endpoints that are included in an error category, click the bar for the category in the chart.

For issues with client extensions that appear in the chart, see Identify and resolve issues with Client Extensions on page 115.

For help resolving a specific error, see Reference: Endpoint monitoring health check errors on page 121, and Contact Tanium Support for further assistance.

© 2026 Tanium Inc. All Rights Reserved

Troubleshooting Integrity Monitor

Collect logs

Server logs might be required by Tanium to assist you with troubleshooting. The information is saved as a ZIP file that you can download with your browser. The zip file is also known as a support bundle.



You must have either an Administrator or Content Administrator role in Integrity Monitor to collect server logs.

1. From the Integrity Monitor **Overview** page, click Help .
2. Click the **Troubleshooting** tab.
3. Click **Collect** and then click **Download** to download a ZIP file containing the logs.

Change the logging level

1. To specify minimum log level, from the Integrity Monitor **Overview** page, click Help .
2. Click the **Troubleshooting** tab.
3. Select a **Log Level**. The default setting is **Info**.



This update changes the log level for future logging. It does not affect the data that is available in the support package for previously logged events.

Upgrading to Integrity Monitor 3.4.97



In Integrity Monitor 3.4.97 and later, the steps required to configure the service account are no longer necessary due to the adoption of the System User Service, which performs these tasks automatically. Additionally, the Integrity Monitor database is migrated to RDB in this release. Consequently, after upgrading from version 3.1.9 or earlier to Integrity Monitor 3.4.97 or later, it might take time for the database migration to complete and for RBAC privileges and other updates to sync properly. This could lead to issues and error messages when you first query Tanium Console. These issues usually resolve on their own after a few minutes, but could take up to an hour or longer depending on system resources and the amount of data to migrate.

© 2026 Tanium Inc. All Rights Reserved

File permission monitoring is configured for a Windows path, but file permission events are not recorded on an endpoint

If you deployed a watchlist that includes a Windows-style path that is configured to record permission changes, but file permission events are not recorded on a Windows Tanium Client managed endpoint, make sure the **Audit File System** permission is configured properly on the endpoint. For more information, see Prepare Endpoints on page 67.

Endpoints that do not have this permission configured return `Recorder - Error: File permission auditing is disabled` when you ask a question using the `Client Extensions - Status` sensor, and they appear in the **Endpoint Health** panel on the Integrity Monitor **Overview** page.

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. For more information about Integrity Monitor tools, see Reference: Integrity Monitor endpoint tools on page 120.

Identify and resolve issues with Client Extensions

Use the following steps to troubleshoot issues with the Client Extensions that Integrity Monitor installs and uses. During troubleshooting, consider environmental factors such as security exclusions, file locks, CPU usage, RAM usage, and disk failures.

For more information about the Client Extensions that Integrity Monitor installs and uses, see Client Extensions.

1. If endpoints have Client Extension shared process mode enabled and you need to troubleshoot resource usage or crashes in the combined `TaniumCX.exe` or `TaniumCX` process, disable shared process mode on the affected endpoints, and then reproduce the issue if possible. For more information, see Endpoint Configuration User Guide: Manage Client Extension shared process mode.
2. To review the health of Client Extensions or to start an investigation into an existing error, ask a question using the `Client Extensions - Status` sensor.
   The results of these questions help to identify endpoints with errors and provide a starting point to deploy actions that might help correct the issue. Filter the results and drill down as necessary to investigate results that indicate errors.

   Consider whether endpoints with errors share common characteristics, such as operating system, domain or organization unit, or the antivirus software that is installed.

© 2026 Tanium Inc. All Rights Reserved

3. Target one or more endpoints with errors, and uninstall tools that report errors without blocking reinstallation. For more information, see Remove Integrity Monitor tools from endpoints and Endpoint Configuration User Guide: Uninstall a tool installed by Endpoint Configuration.

   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.

   Wait for automatic reinstallation of the tool. If the reinstallation does not resolve the issue, continue to the next step.

4. Ask a question using the `Endpoint Configuration - Tools Status Details` sensor, and include filters to limit the results to the tool that you are investigating. For example:

   ```
   Get Endpoint Configuration - Tools Status Details having Endpoint Configuration - Tools Status Details:Tool Name contains Integrity Monitor from all machines with Endpoint Configuration - Tools Status:Tool Name contains Integrity Monitor
   ```

   Review the columns in the results for specific information about errors. The following table provides guidance for some common error conditions:

   Potential errors returned by the Ednpoint Configuration - Tools Status Details sensor

Error Condition	Possible Resolution
No error appears, but an available new version has not been installed	Review the **Targeted Version** column to make sure that the endpoint has received the latest manifest. If the targeted version does not yet show the updated version, the Endpoint Configuration manifest has not updated on the endpoint, usually for one of the following reasons: • The manifest update is still pending. Either wait for the manifest to update and then review the results again, or follow the steps in Endpoint Configuration User Guide: Verify and manually update the Endpoint Configuration manifest. • Action lock is enabled on the endpoint. Follow the steps in Endpoint Configuration User Guide: Verify and manually update the Endpoint Configuration manifest to identify endpoints with action lock turned on. • Integrity Monitor is no longer installed, or it is no longer targeting the endpoint. In some cases, Integrity Monitor might stop targeting an endpoint because it no longer needs the endpoint for a particular workload. Consider whether Integrity Monitor should still target the endpoint: ◦ If it is expected or intentional that Integrity Monitor no longer targets the endpoint, you can optionally uninstall Integrity Monitor tools and dependencies. For more information, see Remove Integrity Monitor tools from endpoints. ◦ If Integrity Monitor should still target the endpoint, make sure that the Integrity Monitor action group includes the endpoint, and make sure Integrity Monitor targets the endpoint in any expected configurations or profiles. Then, either wait for the manifest to update and then review the results again, or follow the steps in Endpoint Configuration User Guide: Verify and manually update the Endpoint Configuration manifest.

© 2026 Tanium Inc. All Rights Reserved

Potential errors returned by the Ednpoint Configuration - Tools Status Details sensor (continued)

Error Condition	Possible Resolution
Installation Blocker:`Unmet Dependencies: [Tool name]`	If no **Failure Message** or **Failure Step** appears, the endpoint might be waiting for the dependencies to install. Wait to see if the condition resolves on its own. If this condition remains for an extended period, ask the question again and review any error information in other columns, especially the **Failing Dependency** column.
Failing Dependency: *[Tool name]*	Ask the question: `Endpoint Configuration - Tools Status Details having Endpoint Configuration - Tools Status Details:Tool Name contains [Tool name] from all machines with Endpoint Configuration - Tools Status:Tool Name contains [Tool name]` Investigate further errors with the tool. If the dependency has not been installed on an endpoint, ask the question: `Get Endpoint Configuration - Tools Retry Status from all machines with Computer Name equals Computer_Name` to review the retry status for the tool installation. For more information, see Endpoint Configuration User Guide: Review tool installations that are scheduled for a retry.
Manually Blocked:`blocked`	The tool was previously blocked, either manually or during a previous uninstallation. Unblock the tool. For more information, see Endpoint Configuration User Guide: Block or unblock tools from installing on an endpoint.

5. Review the Extensions logs on the endpoint. Take note of entries that include `fail` or `error`. For more information, see Review the Extensions log for an endpoint on page 117.

For additional help, collect all logs for Tanium Integrity Monitor, and contact Tanium Support.

Review the Extensions log for an endpoint

Use Client Management to directly connect to an endpoint and view and download extension logs.

1. From the Main menu, go to **Shared Services > Client Management**.
2. From the Client Management menu, click **Client Health**.
3. In the **Direct Connect** search box, enter all or part of an IP address or a computer name.
   Matching results are displayed after the search completes.
4. From the search results, click the computer name to connect to the endpoint.
5. Click the **Logs** tab, and select an **extensions*[#]*.log** file.
6. (Optional) To download the log, click **Download**.

For additional help, collect all logs for Tanium Integrity Monitor, and contact Tanium Support.

© 2026 Tanium Inc. All Rights Reserved

Uninstall Integrity Monitor

IMPORTANT

Contact Tanium Support before you uninstall Integrity Monitor in a production environment so that you understand the potential repercussions.

1. From the Main menu, go to **Administration > Configuration > Solutions**.
2. Select Integrity Monitor and click **Uninstall**. Click **Yes** to complete the process.
3. Delete any remaining Integrity Monitor related scheduled actions and action groups.
4. Remove Integrity Monitor tools from your endpoints. For more information, see Remove Integrity Monitor tools from endpoints on page 118.
5. The uninstall process creates a folder with a backup of the Integrity Monitor files called `integrity-monitor-service-files`. If you have access to the file system on the machine hosting the Module Server, you can keep or delete this folder. If any other Integrity Monitor artifacts remain on your Module Server, Contact Tanium Support.

Remove Integrity Monitor tools from endpoints

You can deploy an action to remove Integrity Monitor 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 , drill down as necessary, and select the targets from which you want to remove Integrity Monitor 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 .
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 Integrity Monitor 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.

© 2026 Tanium Inc. All Rights Reserved

7. (Optional) To remove all Integrity Monitor databases and logs from the endpoints, clear the selection for **Soft uninstall**.

   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 Integrity Monitor tools (such as Recorder and Index) 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.

   BEST PRACTICE

   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.

Resolve issues with legacy Client Recorder Extension installations

If Tanium Endpoint Configuration detects endpoints that have legacy versions of the Client Recorder Extension installed, it reports the endpoint as **Unsupported** in the recorder column of the results grid when you ask the question: `Get Endpoint Configuration - Tools Status`. If Client Recorder Extension version 1.x exists on a targeted endpoint, you must remove it before you install Client Recorder Extension version 2.x tools. To target endpoints where Client Recorder Extension version 1.x exists, ask the question: `Recorder - Legacy Installed`. If the Supported Endpoints column displays **Yes**, you must remove Client Recorder Extension version 1.x from the endpoint before you install Client Recorder Extension 2.x tools. To remove Client Recorder Extension version 1.x, deploy the **Recorder - Remove Legacy Recorder [*Operating System*]** package to targeted endpoints.

Contact Tanium Support

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

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

© 2026 Tanium Inc. All Rights Reserved

Reference: Integrity Monitor endpoint tools

NOTE

Each solution includes a tool with the same name as the solution that appears in the Endpoint Configuration Toolset manifest but that does not appear in the following table. This tool is not deployed to the endpoint itself, but it manages the endpoint tooling dependencies for the solution, as listed in the table.

Endpoint tools for Tanium Integrity Monitor

Tool	Description
core-cx	Provides a management framework API for all other Client Extensions and exposes operating system metrics
cx-config	Provides installation and configuration of extensions on an endpoint
Driver	The Tanium Driver, which records process and command-line events on supported Windows endpoints
extras-cx	Provides a helper library that contains re-usable functions for various client extensions to use
index-cx	Provides the ability to index the local file systems on an endpoint
integrity-monitor-cx	Provides Integrity Monitor functions on an endpoint
python312	Provides TPython binary and libraries
Recorder	Provides the ability to save event data on each endpoint and monitor the endpoint kernel and other low-level subsystems to capture a variety of events
Recorder BPF Support	Provides the ability to save event data using eBPF on Linux endpoints

© 2026 Tanium Inc. All Rights Reserved

Reference: Endpoint monitoring health check errors

Review cross-platform and operating system specific endpoint health check error messages and potential solutions to help with troubleshooting.

Standard cross-platform endpoint health check error messages

The following section contains standard cross-platform endpoint health check error messages and potential resolutions. Use the information to troubleshoot the errors.

Scan completion took longer than configured scan interval. Maybe under spec or subscription misconfigured? Scan:integrity_monitor.watched_paths:<*path*>

*The indicated scan took longer than the **Index Scan Frequency** configured for the monitor that is deployed to the Tanium Client managed endpoint. This might be a temporary condition because of other processes running on the endpoint.*

Make sure that the endpoint meets the minimum system requirements for Integrity Monitor, review other processes that run on the endpoint, and increase the interval that is specified for the **Index Scan Frequency** setting as necessary in the monitor that is deployed endpoint. For more information, see Create or edit a monitor on page 81.

subscription has dropped events: <Recorder/Index/Integrity-monitor.journal>

The endpoint did not have sufficient resources to capture all events. This might be a temporary condition because of other processes running on the endpoint, or watchlists that are deployed to the endpoint might result in an excessive number of recorded events.

Make sure that the endpoint meets the minimum system requirements for Integrity Monitor, review other processes that run on the endpoint, and tune watchlists to reduce events that you do not need to record. For more information, see Add and edit paths on page 87.

Dropped high priority path events from recorder

The endpoint did not have sufficient resources to capture all events. This might be a temporary condition because of other processes running on the endpoint, or watchlists that are deployed to the endpoint might result in an excessive number of recorded events.

Make sure that the endpoint meets the minimum system requirements for Integrity Monitor, review other processes that run on the endpoint, and tune watchlists to reduce events that you do not need to record. For more information, see Add and edit paths on page 87.

© 2026 Tanium Inc. All Rights Reserved

Recorder - Error: Tanium Driver requires system reboot

The Tanium Event Recorder Driver was installed, but the endpoint has not been rebooted. After the driver is first installed on a targeted endpoint, you must reboot that endpoint before Integrity Monitor can record process and user information associated with file and registry operations.

Reboot the endpoint to enable the Tanium Event Recorder Driver.

Recorder - Error: Recorder not installed / Install Needed: Recorder not installed *(Both messages appear together.)*

The Client Recorder Extension is not installed.

Redeploy monitors action to attempt reinstallation of Recorder. For more information, see Deploy monitors on page 84. For more information about working with the recorder, see Tanium Client Recorder Extension User Guide.

Recorder - Error: Client Recorder Extension 2.0 previously installed but is no longer installed

The Client Recorder Extension was installed but is not running or was uninstalled.

Redeploy monitors action to attempt reinstallation of Recorder. For more information, see Deploy monitors on page 84. If the error still occurs, Contact Tanium Support.

Recorder - Error: System minimum requirements not met to enable features: Single CPU detected. Not loading rules *(This message is reported only if you are using Recorder 2.3 or later.)*

The Client Recorder Extension 2.3 and later requires a minimum of two CPUs per endpoint.

The recorder cannot be used on single-core endpoints. Deploy a monitor that has the **Collect process and user attribution information** setting disabled to the endpoint. For more information, see Create or edit a monitor on page 81.

Standard Windows-specific endpoint health check error messages

The following section contains standard Windows-specific endpoint health check error messages and potential resolutions. Use the information to troubleshoot the errors.

Recorder - Error: Missing "TaniumSystemMonitor" from Event Tracing sessions / Install Needed: Missing "TaniumSystemMonitor" from Event Tracing sessions *(Both messages appear together.)*

The recorder is not registered with Event Tracing for Windows (ETW). No events will be recorded.

Make sure that the Tanium Client is running with appropriate credentials, and restart the recorder by deploying the `Recorder - Disable Recorder Extension [OS]` action, followed by the `Recorder - Enable Recorder Extension [OS]` action.

© 2026 Tanium Inc. All Rights Reserved

Recorder - Error: Event Tracing for Windows checks timed out

Integrity Monitor could not determine if the recorder was correctly registered with ETW. The recorder might miss events in this state.

Make sure that the Tanium Client is running with appropriate credentials, and restart the recorder by deploying the `Recorder - Disable Recorder Extension [OS]` action, followed by the `Recorder - Enable Recorder Extension [OS]` action.

Recorder - Error: File permission auditing is disabled

*The **Audit File System** permission is not set correctly on the endpoint.*

For steps to configure the necessary permission, see Prepare Endpoints on page 67.

Standard Linux-specific endpoint health check error messages

The following section contains standard Linux-specific endpoint health check error messages and potential resolutions. Use the information to troubleshoot the errors.

Recorder - Error: im_recorder.json file not found / Install Needed: im_recorder.json file not found *(Both messages appear together.)*

A necessary configuration file for the recorder is missing.

Redeploy monitors action to reinstall Recorder and restore the configuration file. For more information, see Deploy monitors on page 84.

Recorder - Error: The "service" binary is not installed on this system. Please install it first.

The recorder cannot run because the system is missing the standard Linux `service` binary file.

Install the `service` binary.

Recorder - Error: auditd is not installed on this system. Please install first.

The recorder cannot run because the system is missing the `auditd` package.

Install the `auditd` package.

Recorder - Error: auditd raw logging is enabled

Raw logging is enabled in `auditd.conf`, which might reduce performance and prevent audit rules from loading.

Unless the system has excess resources and raw logging is necessary for other applications, consider disabling raw logging to improve performance. To disable raw logging, deploy the `Recorder - Disable Raw Logging [Linux]` action.

© 2026 Tanium Inc. All Rights Reserved

Recorder - Error: systemd raw logging is enabled

Raw logging is enabled for `systemd`, which might reduce performance and prevent audit rules from loading.

Unless the system has excess resources and raw logging is necessary for other applications, consider disabling raw logging to improve performance. To disable raw logging, deploy the `Recorder - Disable Raw Logging [Linux]` action.

Recorder - Error: Trouble loading recorder audit rules ("key=TaniumRecorder" missing from "auditctl -l" output)

Recorder `auditd` rules are not configured correctly. Audit rules might not be loaded if raw logging is enabled. No events will be recorded.

Deploy the `Recorder - Disable Raw Logging [Linux]` action to disable raw logging. If the problem persists, Contact Tanium Support.

© 2026 Tanium Inc. All Rights Reserved

Reference: Gateway examples for Integrity Monitor

The following requests require Integrity Monitor 3.6 or later to create, retrieve, update, deploy, and delete Integrity Monitor monitors and watchlists.

For more information, see Tanium Gateway User Guide: Reference: Filter syntax and Tanium Gateway User Guide: Reference: Gateway examples.

Create Integrity Monitor monitor

(`mutation.integrityMonitorMonitorCreate`)

CREATE INTEGRITY MONITOR MONITOR

The `integrityMonitorMonitorCreate` mutation requires Integrity Monitor 3.6 or later and the **Integrity Monitor Monitors write** permission.

The following mutation creates a monitor.

```
mutation exampleCreateIMMonitor($input: IntegrityMonitorMonitorCreateInput!) {
  integrityMonitorMonitorCreate(input: $input) {
    monitor {
      id
      collectProcessInformation
      computerGroups {
        edges {
          node {
            id
            contentSetV2 {
              id
              name
              description
            }
            expression
            filterEnabled
            managementRightsEnabled
```

© 2026 Tanium Inc. All Rights Reserved

```
            modifiedTime
            name
            type
          }
        }
      }
      databaseMaximumSizeMegabytes
      deploymentStatus
      description
      indexFirstScanDistributeOverTime {
        nanoseconds
        seconds
      }
      indexScanFrequency {
        nanoseconds
        seconds
      }
      monitorPruningAge {
        nanoseconds
        seconds
      }
      name
      priority
      revision
    }
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Include the input variables in the **Variables** panel or in your variables dictionary:

© 2026 Tanium Inc. All Rights Reserved

```
{
  "input": {
    "collectProcessInformation": true,
    "computerGroups": {
      "id": "123"
    },
    "databaseMaximumSizeMegabytes": 512,
    "description": "example monitor",
    "indexFirstScanDistributeOverTime": {
      "nanoseconds": 0,
      "seconds": 14400
    },
    "indexScanFrequency": {
      "nanoseconds": 0,
      "seconds": 43200
    },
    "monitorPruningAge": {
      "nanoseconds": 0,
      "seconds": 86400
    },
    "name": "Example monitor",
    "priority": 1
  }
}
```

Example response:

```
{
  "data": {
    "integrityMonitorMonitorCreate": {
      "monitor": {
        "id": "123",
        "collectProcessInformation": true,
        "computerGroups": {
```

© 2026 Tanium Inc. All Rights Reserved

```
      "edges": [
        {
          "node": {
            "id": "123",
            "contentSetV2": {
              "id": "3",
              "name": "Default Filter Groups",
              "description": null
            },
            "expression": " Operating System Generation equals Windows 10",
            "filterEnabled": true,
            "managementRightsEnabled": true,
            "modifiedTime": null,
            "name": "All Windows 10",
            "type": "STANDARD"
          }
        }
      ]
    },
    "databaseMaximumSizeMegabytes": 512,
    "deploymentStatus": "PendingDeployment",
    "description": "example monitor",
    "indexFirstScanDistributeOverTime": {
      "nanoseconds": 0,
      "seconds": 14400
    },
    "indexScanFrequency": {
      "nanoseconds": 0,
      "seconds": 43200
    },
    "monitorPruningAge": {
      "nanoseconds": 0,
      "seconds": 86400
    },
```


© 2026 Tanium Inc. All Rights Reserved

```
        "name": "Example monitor",
        "priority": 1,
        "revision": 1
      },
      "error": null
    }
  }
}
```

Create Integrity Monitor watchlist

(`mutation.integrityMonitorWatchlistCreate`)

CREATE INTEGRITY MONITOR WATCHLIST

The `integrityMonitorWatchlistCreate` mutation requires Integrity Monitor 3.6 or later and the **Integrity Monitor Watchlists write** permission.

The following mutation creates a Windows-style watchlist. Associated watchlist paths use backslashes (`\`).

```
mutation exampleCreateIMWatchlist($input: IntegrityMonitorWatchlistCreateInput!) {
  integrityMonitorWatchlistCreate(input: $input) {
    watchlist {
      id
      name
      computerGroups {
        edges {
          node {
            id
            name
            managementRightsEnabled
            filterEnabled
            contentSetV2 {
              id
              name
```

© 2026 Tanium Inc. All Rights Reserved

```
              description
            }
            type
            expression
          }
        }
      }
      deploymentStatus
      description
      paths {
        edges {
          node {
            path
            watchlistPathType
            includeFilePermissionChanges
            inclusions {
              edges {
                cursor
                node
              }
            }
            exclusions {
              edges {
                cursor
                node
              }
            }
          }
        }
      }
      pathStyle
      revision
    }
    error {
```

© 2026 Tanium Inc. All Rights Reserved

```
      message
      retryable
      timedOut
    }
  }
}
```

Include the input variables in the **Variables** panel or in your variables dictionary:

```
{
  "input": {
    "computerGroups": [
      {
        "name": "All Computers"
      },
      {
        "id": "123"
      }
    ],
    "description": "example watchlist",
    "name": "Example watchlist",
    "pathStyle": "Windows"
  }
}
```

Example response:

```
{
  "data": {
    "integrityMonitorWatchlistCreate": {
      "watchlist": {
        "id": "123",
        "name": "Example watchlist",
```

© 2026 Tanium Inc. All Rights Reserved

```
        "computerGroups": {
          "edges": [
            {
              "node": {
                "id": "345",
                "name": "All Computers",
                "managementRightsEnabled": true,
                "filterEnabled": true,
                "contentSetV2": {
                  "id": "1",
                  "name": "Reserved",
                  "description": "Built in sensors which can not be edited or removed."
                },
                "type": "STANDARD",
                "expression": " any Computer Name not matches .*"
              }
            }
          ]
        },
        "deploymentStatus": "PendingDeployment",
        "description": "example watchlist",
        "paths": [],
        "pathStyle": "Windows",
        "revision": 1
      },
      "error": null
    }
  }
}
```

The following mutation creates a Unix-style watchlist. Associated watchlist paths use forward slashes (`/`).

```
mutation examplecreateIMWatchlist($input: IntegrityMonitorWatchlistCreateInput!) {
  integrityMonitorWatchlistCreate(input: $input) {
```

© 2026 Tanium Inc. All Rights Reserved

```
    watchlist {
      id
      name
      computerGroups {
        edges {
          node {
            id
            name
            managementRightsEnabled
            filterEnabled
            contentSetV2 {
              id
              name
              description
            }
            type
            expression
          }
        }
      }
      deploymentStatus
      description
      paths {
        edges {
          node {
            path
            watchlistPathType
            includeFilePermissionChanges
            inclusions {
              edges {
                node
              }
            }
            exclusions {
```

© 2026 Tanium Inc. All Rights Reserved

```
              edges {
                node
              }
            }
          }
        }
      }
      pathStyle
      revision
    }
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Include the input variables in the **Variables** panel or in your variables dictionary:

```
{
  "input": {
    "computerGroups": [
      {
        "name": "All Computers"
      },
      {
        "id": "123"
      }
    ],
    "description": "example watchlist",
    "name": "Example watchlist Unix",
    "pathStyle": "Unix"
  }
```

© 2026 Tanium Inc. All Rights Reserved

```
}
```

Example response:


```
{
  "data": {
    "integrityMonitorWatchlistCreate": {
      "watchlist": {
        "id": "234",
        "name": "Example watchlist",
        "computerGroups": {
          "edges": [
            {
              "node": {
                "id": "345",
                "name": "All Computers",
                "managementRightsEnabled": true,
                "filterEnabled": true,
                "contentSetV2": {
                  "id": "1",
                  "name": "Reserved",
                  "description": "Built in sensors which can not be edited or removed."
                },
                "type": "STANDARD",
                "expression": " any Computer Name not matches .*"
              }
            }
          ]
        }
        "deploymentStatus": "PendingDeployment",
        "description": "example watchlist",
        "paths": [],
        "pathStyle": "Unix",
        "revision": 1
```


© 2026 Tanium Inc. All Rights Reserved

```
      },
      "error": null
    }
  }
}
```

Create Integrity Monitor watchlist Unix path

(`mutation.integrityMonitorWatchlistUnixPathCreate`)

CREATE INTEGRITY MONITOR UNIX-STYLE WATCHLIST PATH

The `integrityMonitorWatchlistUnixPathCreate` mutation requires Integrity Monitor 3.6 or later and the **Integrity Monitor Watchlists write** permission.

The following mutation creates a Unix-style watchlist path that uses forward slashes (`/`). This path is associated with the watchlist that matches the ID `123`.



The response returns an error if no watchlist matches the input ID, if the watchlist does not use Unix-style paths, or if the path is not unique in the watchlist.

```
mutation exampleCreateIMUnixPath($input: IntegrityMonitorWatchlistUnixPathCreateInput!) {
  integrityMonitorWatchlistUnixPathCreate(input: $input) {
    watchlistPath {
      id
      exclusions {
        edges {
          node
        }
      }
      inclusions {
        edges {
          node
        }
      }
```

© 2026 Tanium Inc. All Rights Reserved

```
      path
      watchlistPathType
    }
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Include the input variables in the **Variables** panel or in your variables dictionary:

```
{
  "input": {
    "watchlistID": "12",
    "path": "/a/b*/c",
    "inclusions": [
      ".ssh/\\*\\*"
    ],
    "exclusions": [
      "\\*\\*.log",
      "\\*\\*.db"
    ]
  }
}
```

Example response:

```
{
  "data": {
    "integrityMonitorWatchlistUnixPathCreate": {
      "watchlistPath": {
```

© 2026 Tanium Inc. All Rights Reserved

```
        "id": "123",
        "exclusions": {
          "edges": [
            {
              "node": "\\*\\*.db"
            },
            {
              "node": "\\*\\*.log"
            }
          ]
        },
        "inclusions": {
          "edges": [
            {
              "node": ".ssh/\\*\\*"
            }
          ]
        },
        "path": "/a/b*/c",
        "watchlistPathType": "File"
      },
      "error": null
    }
  }
}
```

Create Integrity Monitor watchlist Windows file path

(`mutation.integrityMonitorWatchlistWindowsFilePathCreate`)

CREATE INTEGRITY MONITOR WINDOWS-STYLE WATCHLIST FILE PATH

The `integrityMonitorWatchlistWindowsFilePathCreate` mutation requires Integrity Monitor 3.6 or later and the **Integrity Monitor Watchlists write** permission.

The following mutation creates a Windows-style watchlist file path that uses backslashes (`\`). This path is associated with the watchlist that matches the ID `123`.

© 2026 Tanium Inc. All Rights Reserved

NOTE

The response returns an error if no watchlist matches the input ID, if the watchlist does not use Windows-style paths, or if the path is not unique in the watchlist.

```
mutation exampleCreateIMWinFilePath($input:
IntegrityMonitorWatchlistWindowsFilePathCreateInput!) {
  integrityMonitorWatchlistWindowsFilePathCreate(input: $input) {
    watchlistPath {
      id
      exclusions {
        edges {
          node
        }
      }
      includeFilePermissionChanges
      inclusions {
        edges {
          node
        }
      }
      path
      watchlistPathType
    }
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Include the input variables in the **Variables** panel or in your variables dictionary:

```
{
```

© 2026 Tanium Inc. All Rights Reserved

```
  "input": {
    "watchlistID": "123",
    "path": "C:\\Program Files",
    "inclusions": [
      "**.pem"
    ],
    "exclusions": [
      "**.log",
      "**.db"
    ],
    "includeFilePermissionChanges": true
  }
}
```

Example response:

```
{
  "data": {
    "integrityMonitorWatchlistWindowsFilePathCreate": {
      "watchlistPath": {
        "id": "2345",
        "exclusions": {
          "edges": [
            {
              "node": "**.db"
            },
            {
              "node": "**.log"
            }
          ]
        },
        "includeFilePermissionChanges": true,
        "inclusions": {
          "edges": [
```

© 2026 Tanium Inc. All Rights Reserved

```
            {
              "node": "**.pem"
            }
          ]
        },
        "path": "C:\\Program Files",
        "watchlistPathType": "File"
      },
      "error": null
    }
  }
}
```

Create Integrity Monitor watchlist Windows registry path

(`mutation.integrityMonitorWatchlistWindowsRegistryPathCreate`)

CREATE INTEGRITY MONITOR WINDOWS-STYLE WATCHLIST REGISTRY PATH

The `integrityMonitorWatchlistWindowsRegistryPathCreate` mutation requires Integrity Monitor 3.6 or later and the **Integrity Monitor Watchlists write** permission.

The following mutation creates a Windows-style watchlist registry path that uses backslashes (`\`). This path is associated with the watchlist that matches the ID `123`.

> **NOTE** The response returns an error if no watchlist matches the input ID, if the watchlist does not use Windows-style paths, or if the path is not unique in the watchlist.

```
mutation exampleCreateIMWinRegPath($input:
IntegrityMonitorWatchlistWindowsRegistryPathCreateInput!) {
  integrityMonitorWatchlistWindowsRegistryPathCreate(input: $input) {
    watchlistPath {
      id
      exclusions
      inclusions
```

© 2026 Tanium Inc. All Rights Reserved

```
      path
      watchlistPathType
    }
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Include the input variables in the **Variables** panel or in your variables dictionary:

```
{
  "input": {
    "watchlistID": "123",
    "path": "HKEY_LOCAL_MACHINE\\a\\b*\\c",
    "inclusions": [
      "Classes\\*\\ShellEx\\*\\*"
    ],
    "exclusions": [
      ".NETFramework\\*\\NGenService\\**",
      "Cryptography\\CertificateTemplateCache\\*"
    ]
  }
}
```

Example response:

```
{
  "data": {
    "integrityMonitorWatchlistWindowsRegistryPathCreate": {
      "watchlistPath": {
```

© 2026 Tanium Inc. All Rights Reserved

```
        "id": "12345",
        "exclusions": {
          "edges": [
            {
              "node": "Cryptography\\CertificateTemplateCache\\*"
            },
            {
              "node": ".NETFramework\\*\\NGenService\\**"
            }
          ]
        },
        "inclusions": {
          "edges": [
            {
              "node": "Classes\\*\\ShellEx\\*\\*"
            }
          ]
        },
        "path": "HKEY_LOCAL_MACHINE\\a\\b*\\c",
        "watchlistPathType": "Registry"
      },
      "error": null
    }
  }
}
```

Delete Integrity Monitor watchlist path

(`mutation.integrityMonitorWatchlistPathDelete`)

DELETE INTEGRITY MONITOR WATCHLIST PATH

The `integrityMonitorWatchlistPathDelete` mutation requires Integrity Monitor 3.6 or later and the **Integrity Monitor Watchlists write** permission.

The following mutation deletes a watchlist path that matches the ID `123`.

© 2026 Tanium Inc. All Rights Reserved

```
mutation exampleDeleteIMPath($ref: IdRefInput!) {
  integrityMonitorWatchlistPathDelete(input: $ref) {
    pathID
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Include the input variables in the **Variables** panel or in your variables dictionary:

```
{
  "ref": {
    "id": "123"
  }
}
```

Example response:

```
{
  "data": {
    "integrityMonitorWatchlistPathDelete": {
      "pathID": "123",
      "error": null
    }
  }
}
```

Deploy Integrity Monitor monitors

(`mutation.integrityMonitorStartMonitorDeployment`)

© 2026 Tanium Inc. All Rights Reserved

DEPLOY ALL INTEGRITY MONITOR MONITORS

The `integrityMonitorStartMonitorDeployment` mutation requires Integrity Monitor 3.6 or later and the **Integrity Monitor Deploy Monitors** permission.

The following mutation deploys all monitors. Monitors marked for deletion are deleted during this deployment.

```
mutation exampleStartMonitorDeployment {
  integrityMonitorStartMonitorDeployment {
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Example response:

```
{
  "data": {
    "integrityMonitorStartMonitorDeployment": {
      "error": null
    }
  }
}
```

Deploy Integrity Monitor watchlists

(`mutation.integrityMonitorStartWatchlistDeployment`)

DEPLOY ALL INTEGRITY MONITOR WATCHLISTS

The `integrityMonitorStartWatchlistDeployment` mutation requires Integrity Monitor 3.6 or later and the **Integrity Monitor Deploy Watchlists** permission.

The following mutation deploys all watchlists. Watchlists marked for deletion are deleted during this deployment.

© 2026 Tanium Inc. All Rights Reserved

```
mutation exampleStartWatchlistDeployment {
  integrityMonitorStartWatchlistDeployment {
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Example response:

```
{
  "data": {
    "integrityMonitorStartWatchlistDeployment": {
      "error": null
    }
  }
}
```

Get Integrity Monitor monitor by ID

(`query.integrityMonitorMonitor`)

GET INTEGRITY MONITOR MONITOR BY ID

The `integrityMonitorMonitor` query requires Integrity Monitor 3.6 or later and the **Integrity Monitor Monitor read** permission.

The following query retrieves the monitor that matches the ID.

```
query exampleGetIMMonitorByID($id: ID!) {
  integrityMonitorMonitor(ref: {id: $id}) {
    id
    collectProcessInformation
    computerGroups {
```

© 2026 Tanium Inc. All Rights Reserved

```
      edges {
        node {
          id
          contentSetV2 {
            id
            name
            description
          }
          expression
          filterEnabled
          managementRightsEnabled
          modifiedTime
          name
          type
        }
      }
    }
    databaseMaximumSizeMegabytes
    deploymentStatus
    description
    indexFirstScanDistributeOverTime {
      seconds
      nanoseconds
    }
    indexScanFrequency {
      seconds
      nanoseconds
    }
    monitorPruningAge {
      seconds
      nanoseconds
    }
    name
    priority
```

© 2026 Tanium Inc. All Rights Reserved

```
    revision
  }
}
```

Include the ID variable in the **Variables** panel or in your variables dictionary:

```
{
  "id": "123"
}
```

Example response:

```
{
  "data": {
    "integrityMonitorMonitor": {
      "id": "123",
      "collectProcessInformation": true,
      "computerGroups": {
        "edges": [
          {
            "node": {
              "id": "75",
              "contentSetV2": {
                "id": "3",
                "name": "Default Filter Groups",
                "description": null
              },
              "expression": " Is Linux equals True",
              "filterEnabled": true,
              "managementRightsEnabled": true,
              "modifiedTime": null,
              "name": "All Linux",
              "type": "STANDARD"
```

© 2026 Tanium Inc. All Rights Reserved

```
            }
          }
        ]
      },
      "databaseMaximumSizeMegabytes": null,
      "deploymentStatus": "PendingDeployment",
      "description": "",
      "indexFirstScanDistributeOverTime": {
        "seconds": 14400,
        "nanoseconds": 0
      },
      "indexScanFrequency": {
        "seconds": 43200,
        "nanoseconds": 0
      },
      "monitorPruningAge": {
        "seconds": 2592000,
        "nanoseconds": 0
      },
      "name": "Linux Monitor",
      "priority": 3,
      "revision": 5
    }
  }
}
```


Get Integrity Monitor service status

(`query.integrityMonitorStatus`)

GET INTEGRITY MONITOR SERVICE STATUS

The `integrityMonitorStatus` query requires Integrity Monitor 3.6 or later and the following permissions:

© 2026 Tanium Inc. All Rights Reserved

- **Integrity Monitor Monitors read** and **Integrity Monitor Watchlists read** permissions to submit the query request
- **Integrity Monitor Deploy Monitors** permission to get monitor deployment status (`isDeployingMonitors`)
- **Integrity Monitor Deploy Watchlists** permission to get watchlist deployment status(`isDeployingWatchlists`)

The following query retrieves the Integrity Monitor service status.

```
query exampleGetIMServiceStatus {
  integrityMonitorStatus {
    isDeployingMonitors
    isDeployingWatchlists
  }
}
```

Example response:

```
{
  "data": {
    "integrityMonitorStatus": {
      "isDeployingMonitors": true,
      "isDeployingWatchlists": true
    }
  }
}
```

Get Integrity Monitor watchlist by ID

(`query.integrityMonitorWatchlist`)

GET INTEGRITY MONITOR WATCHLIST BY ID

The `integrityMonitorWatchlist` query requires Integrity Monitor 3.6 or later and the **Integrity Monitor Watchlists read** permission.

The following query retrieves the watchlist that matches the ID.

```
query exampleGetIMWatchlistByID($id: ID!) {
```

© 2026 Tanium Inc. All Rights Reserved

```
  integrityMonitorWatchlist(ref: {id: $id}) {
    id
    name
    computerGroups {
      edges {
        node {
          id
          name
          managementRightsEnabled
          filterEnabled
          contentSetV2 {
            id
            name
            description
          }
          type
          expression
        }
      }
    }
    deploymentStatus
    description
    paths {
      edges {
        node {
          path
          watchlistPathType
          includeFilePermissionChanges
          inclusions {
            edges {
              node
            }
          }
          exclusions {
```

© 2026 Tanium Inc. All Rights Reserved

```
            edges {
              node
            }
          }
        }
      }
      pathStyle
      revision
    }
  }
```

Include the ID variable in the **Variables** panel or in your variables dictionary:

```
{
  "id": "123"
}
```

Example response:

```
{
  "data": {
    "integrityMonitorWatchlist": {
      "id": "123",
      "name": "Example watchlist update",
      "computerGroups": {
        "edges": [
          {
            "node": {
              "id": "1",
              "name": "All Computers",
              "managementRightsEnabled": true,
              "filterEnabled": true,
```

© 2026 Tanium Inc. All Rights Reserved

```
              "contentSetV2": {
                "id": "1",
                "name": "Reserved",
                "description": "Built in sensors which can not be edited or removed."
              },
              "type": "STANDARD",
              "expression": " All Computers"
            }
          },
          {
            "node": {
              "id": "123",
              "name": "All Debian 9",
              "managementRightsEnabled": true,
              "filterEnabled": true,
              "contentSetV2": {
                "id": "3",
                "name": "Default Filter Groups",
                "description": null
              },
              "type": "STANDARD",
              "expression": " Operating System Generation equals Debian 9"
            }
          }
        ]
      },
      "deploymentStatus": "PendingDeployment",
      "description": "example watchlist update",
      "paths": {
        "edges": [
          {
            "node": {
              "path": "/a/b*/c",
              "watchlistPathType": "File",
```


© 2026 Tanium Inc. All Rights Reserved

```
                "includeFilePermissionChanges": true,
                "inclusions": {
                  "edges": [
                    {
                      "node": ".ssh/\\*\\*"
                    }
                  ]
                },
                "exclusions": {
                  "edges": []
                }
              }
            }
          ]
        },
        "pathStyle": "Unix",
        "revision": 3
      }
    }
}
```

Get multiple Integrity Monitor monitors

(`query.integrityMonitorMonitors`)

GET MULTIPLE INTEGRITY MONITOR MONITORS

The `integrityMonitorMonitors` query requires Integrity Monitor 3.6 or later and the **Integrity Monitor Monitor read** permission.

The following query retrieves the first `2` monitors.

```
query exampleGetMultipleIMMonitors($first: Int) {
  integrityMonitorMonitors(first: $first) {
    edges {
```

© 2026 Tanium Inc. All Rights Reserved

```
      node {
        id
        collectProcessInformation
        computerGroups {
          edges {
            node {
              id
              contentSetV2 {
                id
                name
                description
              }
              expression
              filterEnabled
              managementRightsEnabled
              modifiedTime
              name
              type
            }
          }
        }
        databaseMaximumSizeMegabytes
        deploymentStatus
        description
        indexFirstScanDistributeOverTime {
          seconds
          nanoseconds
        }
        indexScanFrequency {
          seconds
          nanoseconds
        }
        monitorPruningAge {
          seconds
```

© 2026 Tanium Inc. All Rights Reserved

```
            nanoseconds
          }
          name
          priority
          revision
        }
      }
    }
}
```

Include the pagination variable in the **Variables** panel or in your variables dictionary:

```
{
  "first": 2
}
```

Example response:

```
{
  "data": {
    "integrityMonitorMonitors": {
      "edges": [
        {
          "node": {
            "id": "123",
            "collectProcessInformation": true,
            "computerGroups": {
              "edges": []
            },
            "databaseMaximumSizeMegabytes": null,
            "deploymentStatus": "PendingDeployment",
            "description": "",
            "indexFirstScanDistributeOverTime": {
```

© 2026 Tanium Inc. All Rights Reserved

```
                "seconds": 0,
                "nanoseconds": 0
              },
              "indexScanFrequency": {
                "seconds": 600,
                "nanoseconds": 0
              },
              "monitorPruningAge": {
                "seconds": 2592000,
                "nanoseconds": 0
              },
              "name": "example monitor",
              "priority": 1,
              "revision": 6
            }
          },
          {
            "node": {
              "id": "234",
              "collectProcessInformation": true,
              "computerGroups": {
                "edges": [
                  {
                    "node": {
                      "id": "234",
                      "contentSetV2": {
                        "id": "3",
                        "name": "Default Filter Groups",
                        "description": null
                      },
                      "expression": "
Operating System Generation equals Windows Server 2008 R2",
                      "filterEnabled": true,
                      "managementRightsEnabled": true,
                      "modifiedTime": null,
```


© 2026 Tanium Inc. All Rights Reserved

```
                    "name": "All Windows Server 2008 R2",
                    "type": "STANDARD"
                  }
                },
                {
                  "node": {
                    "id": "345",
                    "contentSetV2": {
                      "id": "3",
                      "name": "Default Filter Groups",
                      "description": null
                    },
                    "expression": "Operating System Generation equals Windows Server 2016",
                    "filterEnabled": true,
                    "managementRightsEnabled": true,
                    "modifiedTime": null,
                    "name": "All Windows Server 2016",
                    "type": "STANDARD"
                  }
                },
                {
                  "node": {
                    "id": "456",
                    "contentSetV2": {
                      "id": "3",
                      "name": "Default Filter Groups",
                      "description": null
                    },
                    "expression": "Operating System Generation equals Windows Server 2019",
                    "filterEnabled": true,
                    "managementRightsEnabled": true,
                    "modifiedTime": null,
                    "name": "All Windows Server 2019",
```


© 2026 Tanium Inc. All Rights Reserved

```
                    "type": "STANDARD"
                  }
                },
                {
                  "node": {
                    "id": "567",
                    "contentSetV2": {
                      "id": "3",
                      "name": "Default Filter Groups",
                      "description": null
                    },
                    "expression": "Operating System Generation equals Windows Server 2022",
                    "filterEnabled": true,
                    "managementRightsEnabled": true,
                    "modifiedTime": null,
                    "name": "All Windows Server 2022",
                    "type": "STANDARD"
                  }
                },
                {
                  "node": null
                }
              ]
            },
            "databaseMaximumSizeMegabytes": null,
            "deploymentStatus": "PendingDeployment",
            "description": "",
            "indexFirstScanDistributeOverTime": {
              "seconds": 14400,
              "nanoseconds": 0
            },
            "indexScanFrequency": {
              "seconds": 43200,
              "nanoseconds": 0
```


© 2026 Tanium Inc. All Rights Reserved

```
            },
            "monitorPruningAge": {
              "seconds": 2592000,
              "nanoseconds": 0
            },
            "name": "Windows Monitor",
            "priority": 2,
            "revision": 6
          }
        }
      ]
    }
  }
}
```

Get multiple Integrity Monitor watchlists

(`query.integrityMonitorWatchlists`)

GET MULTIPLE INTEGRITY MONITOR WATCHLISTS

The `integrityMonitorWatchlists` query requires Integrity Monitor 3.6 or later and the **Integrity Monitor Watchlists read** permission.

The following query retrieves the first `2` watchlists.

```
query exampleGetIMWatchlists($first: Int) {
  integrityMonitorWatchlists(first: $first) {
    edges {
      node {
        id
        name
        computerGroups {
          edges {
            node {
```

© 2026 Tanium Inc. All Rights Reserved

```
            id
            name
            managementRightsEnabled
            filterEnabled
            contentSetV2 {
              id
              name
              description
            }
            type
            expression
          }
        }
      }
      deploymentStatus
      description
      paths {
        edges {
          node {
            path
            watchlistPathType
            includeFilePermissionChanges
            inclusions {
              edges {
                node
              }
            }
            exclusions {
              edges {
                node
              }
            }
          }
        }
```

© 2026 Tanium Inc. All Rights Reserved

```
          }
          pathStyle
          revision
        }
      }
    }
  }
```

Include the pagination variable in the **Variables** panel or in your variables dictionary:

```
{
  "first": 2
}
```

Example response:

```
{
  "data": {
    "integrityMonitorWatchlists": {
      "edges": [
        {
          "node": {
            "id": "12",
            "name": "Example AIX Watchlist",
            "computerGroups": {
              "edges": [
                {
                  "node": {
                    "id": "33",
                    "name": "All AIX",
                    "managementRightsEnabled": true,
                    "filterEnabled": true,
                    "contentSetV2": {
```

© 2026 Tanium Inc. All Rights Reserved

```
                        "id": "3",
                        "name": "Default Filter Groups",
                        "description": null
                      },
                      "type": "STANDARD",
                      "expression": " Is AIX equals True"
                    }
                  }
                ]
              },
              "deploymentStatus": "Deployed",
              "description": "",
              "paths": {
                "edges": [
                  {
                    "node": {
                      "path": "/bin",
                      "watchlistPathType": "File",
                      "includeFilePermissionChanges": true,
                      "inclusions": {
                        "edges": []
                      },
                      "exclusions": {
                        "edges": [
                          {
                            "node": "**.db"
                          },
                          {
                            "node": "**.log"
                          },
                          {
                            "node": "**.state"
                          },
                          {
```


© 2026 Tanium Inc. All Rights Reserved

```
                        "node": "**.tmp"
                      }
                    ]
                  }
                }
              },
              {
                "node": {
                  "path": "/boot",
                  "watchlistPathType": "File",
                  "includeFilePermissionChanges": true,
                  "inclusions": {
                    "edges": [
                      {
                        "node": "efi/**"
                      },
                      {
                        "node": "grub/**"
                      },
                      {
                        "node": "grub2/**"
                      }
                    ]
                  },
                  "exclusions": {
                    "edges": []
                  }
                }
              },
              {
                "node": {
                  "path": "/etc/shells",
                  "watchlistPathType": "File",
                  "includeFilePermissionChanges": true,
```

© 2026 Tanium Inc. All Rights Reserved

```
                    "inclusions": {
                      "edges": []
                    },
                    "exclusions": {
                      "edges": []
                    }
                  }
                }
              ]
            },
            "pathStyle": "Unix",
            "revision": 2
          }
        },
        {
          "node": {
            "id": "23",
            "name": "Example watchlist",
            "computerGroups": {
              "edges": [
                {
                  "node": {
                    "id": "1",
                    "name": "All Computers",
                    "managementRightsEnabled": true,
                    "filterEnabled": true,
                    "contentSetV2": {
                      "id": "1",
                      "name": "Reserved",
                      "description": "Built in sensors which can not be edited or
removed."
                    },
                    "type": "STANDARD",
                    "expression": " All Computers"
                  }
```


© 2026 Tanium Inc. All Rights Reserved

```
        }
      ]
    },
    "deploymentStatus": "Deployed",
    "description": "",
    "paths": {
      "edges": [
        {
          "node": {
            "path": "C:\\example",
            "watchlistPathType": "File",
            "includeFilePermissionChanges": true,
            "inclusions": {
              "edges": []
            },
            "exclusions": {
              "edges": []
            }
          }
        },
        {
          "node": {
            "path": "HKEY_LOCAL_MACHINE\\SYSTEM\\EXAMPLE",
            "watchlistPathType": "Registry",
            "includeFilePermissionChanges": false,
            "inclusions": {
              "edges": []
            },
            "exclusions": {
              "edges": []
            }
          }
        }
      ]
```


© 2026 Tanium Inc. All Rights Reserved

```
            },
            "pathStyle": "Windows",
            "revision": 3
          }
        }
      ]
    }
  }
}
```

Mark Integrity Monitor monitors for deletion

(`mutation.integrityMonitorMonitorMarkForDeletion`)

MARK INTEGRITY MONITOR MONITOR FOR DELETION

The `integrityMonitorMonitorMarkForDeletion` mutation requires Integrity Monitor 3.6 or later and the **Integrity Monitor Monitors write** permission.

The following mutation marks the monitor that matches the ID `123` for deletion. Monitors marked for deletion are deleted during the next monitor deployment.

```
mutation exampleMarkIMMonitorForDeletion($ref: IdRefInput!) {
  integrityMonitorMonitorMarkForDeletion(input: $ref) {
    monitor {
      id
      name
      }
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Include the input variables in the **Variables** panel or in your variables dictionary:

© 2026 Tanium Inc. All Rights Reserved

```
{
  "ref": {
    "id": "123"
  }
}
```

Example response:

```
{
  "data": {
    "integrityMonitorMonitorMarkForDeletion": {
      "monitor": {
        "id": "123",
        "name": "example monitor"
      },
      "error": null
    }
  }
}
```

Mark Integrity Monitor watchlists for deletion

(`mutation.integrityMonitorWatchlistMarkForDeletion`)

MARK INTEGRITY MONITOR WATCHLIST FOR DELETION

The `integrityMonitorWatchlistMarkForDeletion` mutation requires Integrity Monitor 3.6 or later and the **Integrity Monitor Watchlists write** permission.

The following mutation marks the watchlist that matches the ID `123` for deletion. Watchlists marked for deletion are deleted during the next watchlist deployment.

```
mutation exampleDeleteWatchlist($ref: IdRefInput!) {
  integrityMonitorWatchlistMarkForDeletion(input: $ref) {
    watchlist {
```

© 2026 Tanium Inc. All Rights Reserved

```
      id
      name
    }
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Include the input variables in the **Variables** panel or in your variables dictionary:

```
{
  "ref": {
    "id": "123"
  }
}
```

Example response:

```
{
  "data": {
    "integrityMonitorWatchlistMarkForDeletion": {
      "watchlist": {
        "id": "123",
        "name": "example watchlist"
      },
      "error": null
    }
  }
}
```

© 2026 Tanium Inc. All Rights Reserved

Update Integrity Monitor monitor by ID

(`mutation.integrityMonitorMonitorUpdate`)

UPDATE INTEGRITY MONITOR MONITOR

The `integrityMonitorMonitorUpdate` mutation requires Integrity Monitor 3.6 or later and the **Integrity Monitor Monitors write** permission.

The following mutation updates a monitor that matches the ID. Note the following:

- The response returns an error if no monitor matches the ID, the `name` value is an empty string or `null`, or the `name` value is updated to a name that matches another monitor.
- Fields defined with a value overwrite the existing field value with the defined value. Defining an array with at least one value for the `computerGroups` field overwrites all existing array values with the defined array values.
- Fields defined with a `null` value are not updated, if `null` is allowed.
- Fields defined with an empty string or empty array replace any existing value with the empty string or empty array, if an empty string or empty array are allowed.

```
mutation exampleUpdateIMMonitor($input: IntegrityMonitorMonitorUpdateInput!) {
  integrityMonitorMonitorUpdate(input: $input) {
    monitor {
      id
      collectProcessInformation
      computerGroups {
        edges {
          node {
            id
            contentSetV2 {
              id
              name
              description
            }
            expression
            filterEnabled
            managementRightsEnabled
            modifiedTime
            name
```

© 2026 Tanium Inc. All Rights Reserved

```
            type
          }
        }
      }
      databaseMaximumSizeMegabytes
      deploymentStatus
      description
      indexFirstScanDistributeOverTime {
        nanoseconds
        seconds
      }
      indexScanFrequency {
        nanoseconds
        seconds
      }
      monitorPruningAge {
        nanoseconds
        seconds
      }
      name
      priority
      revision
      }
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Include the input variables in the **Variables** panel or in your variables dictionary:

```
{
```

© 2026 Tanium Inc. All Rights Reserved

```
  "input": {
    "id": "12",
    "collectProcessInformation": true,
    "computerGroups": {
      "id": "123"
    },
    "databaseMaximumSizeMegabytes": 1024,
    "description": "example monitor",
    "indexFirstScanDistributeOverTime": {
      "seconds": 14400,
      "nanoseconds": 0
    },
    "indexScanFrequency": {
      "seconds": 43200,
      "nanoseconds": 0
    },
    "monitorPruningAge": {
      "seconds": 86400,
      "nanoseconds": 0
    },
    "name": "Example monitor",
    "priority": 1
  }
}
```

Example response:

```
{
  "data": {
    "integrityMonitorMonitorUpdate": {
      "monitor": {
        "id": "12",
        "collectProcessInformation": true,
        "computerGroups": {
```

© 2026 Tanium Inc. All Rights Reserved

```
        "edges": [
          {
            "node": {
              "id": "123",
              "contentSetV2": {
                "id": "3",
                "name": "Default Filter Groups",
                "description": null
              },
              "expression": " Operating System Generation equals Windows 10",
              "filterEnabled": true,
              "managementRightsEnabled": true,
              "modifiedTime": null,
              "name": "All Windows 10",
              "type": "STANDARD"
            }
          }
        ]
      },
      "databaseMaximumSizeMegabytes": 1024,
      "deploymentStatus": "PendingDeployment",
      "description": "example monitor",
      "indexFirstScanDistributeOverTime": {
        "nanoseconds": 0,
        "seconds": 14400
      },
      "indexScanFrequency": {
        "nanoseconds": 0,
        "seconds": 43200
      },
      "monitorPruningAge": {
        "nanoseconds": 0,
        "seconds": 86400
      },
```


© 2026 Tanium Inc. All Rights Reserved

```
        "name": "Example monitor",
        "priority": 1,
        "revision": 2
      },
      "error": null
    }
  }
}
```

Update Integrity Monitor watchlist

(`mutation.integrityMonitorWatchlistUpdate`)

UPDATE INTEGRITY MONITOR WATCHLIST

The `integrityMonitorWatchlistUpdate` mutation requires Integrity Monitor 3.6 or later and the **Integrity Monitor Watchlists write** permission.

The following mutation updates a watchlist that matches the ID. Note the following:

- The response returns an error if no watchlist matches the ID, the `name` value is an empty string or `null`, or the `name` value is updated to a name that matches another watchlist with the same `pathStyle` value.
- Fields defined with a value overwrite the existing field value with the defined value. Defining an array with at least one value for the `computerGroups` field overwrites all existing array values with the defined array values.
- Fields defined with a `null` value are not updated, if `null` is allowed.
- Fields defined with an empty string or empty array replace any existing value with the empty string or empty array, if an empty string or empty array are allowed.
- If you change the `pathStyle` of a watchlist, all of the watchlist paths are deleted because paths must match the watchlist path style.

```
mutation exampleUpdateIMWatchlist($input: IntegrityMonitorWatchlistUpdateInput!) {
  integrityMonitorWatchlistUpdate(input: $input) {
    watchlist {
      id
      name
      computerGroups {
        edges {
```

© 2026 Tanium Inc. All Rights Reserved

```
        node {
          id
          name
          managementRightsEnabled
          filterEnabled
          contentSetV2 {
            id
            name
            description
          }
          type
          expression
        }
      }
    }
    deploymentStatus
    description
    paths {
      edges {
        node {
          path
          watchlistPathType
          includeFilePermissionChanges
          inclusions {
            edges {
              node
            }
          }
          exclusions {
            edges {
              node
            }
          }
        }
```

© 2026 Tanium Inc. All Rights Reserved

```
        }
      }
      pathStyle
      revision
    }
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Include the input variables in the **Variables** panel or in your variables dictionary:

```
{
  "input": {
    "id": "10",
    "computerGroups": [
      {
        "name": "All Computers"
      },
      {
        "id": "123"
      }
    ],
    "description": "example watchlist update",
    "name": "Example watchlist update",
    "pathStyle": "Windows"
  }
}
```

Example response:

© 2026 Tanium Inc. All Rights Reserved

```
{
  "data": {
    "integrityMonitorWatchlistUpdate": {
      "watchlist": {
        "id": "123",
        "name": "Example watchlist update",
        "computerGroups": {
          "edges": [
            {
              "node": {
                "id": "1",
                "name": "All Computers",
                "managementRightsEnabled": true,
                "filterEnabled": true,
                "contentSetV2": {
                  "id": "1",
                  "name": "Reserved",
                  "description": "Built in sensors which can not be edited or removed."
                },
                "type": "STANDARD",
                "expression": " All Computers"
              }
            },
            {
              "node": {
                "id": "123",
                "name": "All Windows 8.1",
                "managementRightsEnabled": true,
                "filterEnabled": true,
                "contentSetV2": {
                  "id": "3",
                  "name": "Default Filter Groups",
                  "description": null
                },
```


© 2026 Tanium Inc. All Rights Reserved

```
                "type": "STANDARD",
                "expression": " Operating System Generation equals Windows 8.1"
              }
            }
          ]
        },
        "deploymentStatus": "PendingDeployment",
        "description": "example watchlist update",
        "paths": {
          "edges": []
        },
        "pathStyle": "Windows",
        "revision": 5
      },
      "error": null
    }
  }
}
```

Update Integrity Monitor watchlist Unix path

(`mutation.integrityMonitorWatchlistUnixPathUpdate`)

UPDATE INTEGRITY MONITOR UNIX-STYLE WATCHLIST PATH

The `integrityMonitorWatchlistUnixPathUpdate` mutation requires Integrity Monitor 3.6 or later and the **Integrity Monitor Watchlists write** permission.

The following mutation updates a Unix-style watchlist path that uses forward slashes (`/`). This path matches the ID `123`.



The response returns an error if no Unix-style watchlist path matches the input ID.

```
mutation exampleUpdateIMUnixPath($input: IntegrityMonitorWatchlistUnixPathUpdateInput!) {
  integrityMonitorWatchlistUnixPathUpdate(input: $input) {
    watchlistPath {
```

© 2026 Tanium Inc. All Rights Reserved

```
      id
      exclusions {
        edges {
          node
        }
      }
      inclusions {
        edges {
          node
        }
      }
      path
      watchlistPathType
    }
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Include the input variables in the **Variables** panel or in your variables dictionary:

```
{
  "input": {
    "id": "1234",
    "path": "/a/b*/c",
    "inclusions": [
      ".ssh/\\*\\*"
    ],
    "exclusions": [
      "\\*\\*.log"
    ]
```

© 2026 Tanium Inc. All Rights Reserved

```
  }
}
```

Example response:

```
{
  "data": {
    "integrityMonitorWatchlistUnixPathUpdate": {
      "watchlistPath": {
        "id": "1234",
        "exclusions": {
          "edges": [
            {
              "node": "\\*\\*.log"
            }
          ]
        },
        "inclusions": {
          "edges": [
            {
              "node": ".ssh/\\*\\*"
            }
          ]
        },
        "path": "/a/b*/c",
        "watchlistPathType": "File"
      },
      "error": null
    }
  }
}
```

Update Integrity Monitor watchlist Windows file path

(`mutation.integrityMonitorWatchlistWindowsFilePathUpdate`)

© 2026 Tanium Inc. All Rights Reserved

UPDATE INTEGRITY MONITOR WINDOWS-STYLE WATCHLIST FILE PATH

The `integrityMonitorWatchlistWindowsFilePathUpdate` mutation requires Integrity Monitor 3.6 or later and the **Integrity Monitor Watchlists write** permission.

The following mutation creates a Windows-style watchlist file path that uses backslashes (`\`). This path matches the ID `123`.



The response returns an error if no Windows-style watchlist file path matches the input ID.

```
mutation exampleUpdateIMWinFilePath($input:
IntegrityMonitorWatchlistWindowsFilePathUpdateInput!) {
  integrityMonitorWatchlistWindowsFilePathUpdate(input: $input) {
    watchlistPath {
      id
      exclusions {
        edges {
          node
        }
      }
      includeFilePermissionChanges
      inclusions {
        edges {
          node
        }
      }
      path
      watchlistPathType
    }
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Include the input variables in the **Variables** panel or in your variables dictionary:

© 2026 Tanium Inc. All Rights Reserved

```
{
  "input": {
    "id": "2345",
    "path": "C:\\Program Files",
    "inclusions": [
      "**.pem",
      "**.log"
    ],
    "exclusions": [
      "**.db"
    ],
    "includeFilePermissionChanges": true
  }
}
```

Example response:

```
{
  "data": {
    "integrityMonitorWatchlistWindowsFilePathUpdate": {
      "watchlistPath": {
        "id": "2345",
        "exclusions": {
          "edges": [
            {
              "node": "**.db"
            }
          ]
        },
        "includeFilePermissionChanges": true,
        "inclusions": {
          "edges": [
            {
              "node": "**.log"
```

© 2026 Tanium Inc. All Rights Reserved

```
            },
            {
              "node": "**.pem"
            }
          ]
        },
        "path": "C:\\Program Files",
        "watchlistPathType": "File"
      },
      "error": null
    }
  }
}
```

Update Integrity Monitor watchlist Windows registry path

(`mutation.integrityMonitorWatchlistWindowsRegistryPathUpdate`)

UPDATE INTEGRITY MONITOR WINDOWS-STYLE WATCHLIST REGISTRY PATH

The `integrityMonitorWatchlistWindowsRegistryPathUpdate` mutation requires Integrity Monitor 3.6 or later and the **Integrity Monitor Watchlists write** permission.

The following mutation creates a Windows-style watchlist registry path that uses backslashes (`\`). This path matches the ID `123`.


NOTE

The response returns an error if no Windows-style watchlist registry path matches the input ID.

```
mutation exampleUpdateIMWinRegPath($input:
IntegrityMonitorWatchlistWindowsRegistryPathUpdateInput!) {
  integrityMonitorWatchlistWindowsRegistryPathUpdate(input: $input) {
    watchlistPath {
      id
      exclusions {
        edges {
          node
```

© 2026 Tanium Inc. All Rights Reserved

```
        }
      }
      inclusions {
        edges {
          node
        }
      }
      path
      watchlistPathType
    }
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Include the input variables in the **Variables** panel or in your variables dictionary:

```
{
  "input": {
    "id": "12345",
    "path": "HKEY_LOCAL_MACHINE\\a\\b*\\c",
    "inclusions": [
      "Classes\\*\\ShellEx\\*\\*",
      ".NETFramework\\*\\NGenService\\**"
    ],
    "exclusions": [
      "Cryptography\\CertificateTemplateCache\\*"
    ]
  }
}
```

Example response:

© 2026 Tanium Inc. All Rights Reserved

```
{
  "data": {
    "integrityMonitorWatchlistWindowsRegistryPathUpdate": {
      "watchlistPath": {
        "id": "12345",
        "exclusions": {
          "edges": [
            {
              "node": "Cryptography\\CertificateTemplateCache\\*"
            }
          ]
        },
        "inclusions": {
          "edges": [
            {
              "node": "Classes\\*\\ShellEx\\*\\*"
            },
            {
              "node": ".NETFramework\\*\\NGenService\\**"
            }
          ]
        },
        "path": "HKEY_LOCAL_MACHINE\\a\\b*\\c",
        "watchlistPathType": "File"
      },
      "error": null
    }
  }
}
```


© 2026 Tanium Inc. All Rights Reserved

Reference: Watchlist paths, inclusions, and exclusions

Add paths to a watchlist to determine the files, directories, and Windows registry paths that a monitor watches for changes. You can refine the paths in a watchlist by adding path inclusions and path exclusions. If you define path inclusions, the path matches *only* subdirectories, files, or registry subkeys that match the inclusions. If you define path exclusions, the path does *not* match subdirectories, files, or registry subkeys that match the exclusions. Exclusions take precedence over inclusions. If you define both inclusions and exclusions, the path matches all directories, files, or registry keys that match the inclusions, *except* those that match exclusions.



Rely primarily on inclusions to refine paths, and try to limit the number of exclusions for cleaner watchlists and more predictable monitoring.

For more information, see Managing watched paths with watchlists on page 86.

Paths

A path is an absolute file or Windows registry path that provides the basis for determining directories, files, or registry keys that a watchlist defines. Without inclusions or exclusions defined, the path matches all files and subdirectories in a file path or all subkeys in a registry path. By default, a file path that specifies a directory includes subdirectories recursively, and a registry path that specifies a registry key includes subkeys recursively.

You can use a question mark (`?`) wildcard character to match any single character or an asterisk (`*`) wildcard character to match any number of any characters. In a path, you can use wildcard characters within a directory, file, or registry key name, but you cannot use wildcard characters to match path separators or specify multiple directory or subkey levels.

File paths

A file path specifies a directory or file. If you specify a root directory, you must include the slash. For example: `D:\`.

© 2026 Tanium Inc. All Rights Reserved

Example file paths

Example path and explanation	Examples of watched directories and files

Path (Windows):
`C:\Program Files`
 	
A path that specifies a directory without using wildcards matches that directory itself, as well as all files in that directory, and all subdirectories and files recursively.
	Examples of watched directories and files (without inclusions or exclusions defined):
	`C:\Program Files\`
	`C:\Program Files\My Program\`
	`C:\Program Files\My Program\myprogram.exe`
	`C:\Program Files\Another Program\`
	
	Examples of directories that are not watched (when only this path is specified):
	`C:\Program Files (x86)\`
	`D:\Program Files\`
	`D:\Program Files (x86)\`

Path (Unix):
`/a/b*/c`
 	
The `*` wildcard character represents zero or more characters within the directory name, but it does not match path separators.
	Examples of watched directories and files (without inclusions or exclusions defined):
	`/a/b/c/`
	`/a/b/c/myfile.txt`
	`/a/bin/c/`
	`/a/bin/c/myfile.txt`
	`/a/b/c/d/myfile.txt`
	
	Examples of directories and files that are not watched (when only this path is specified):
	`/a/b/`
	`/a/b/c.txt`
	`/a/b/d/c/`

Registry paths

A registry path specifies a Windows registry key.

© 2026 Tanium Inc. All Rights Reserved

NOTE

To specifically record registry rename operations on an endpoint, or to specifically record modifications to individual registry values on an endpoint, you must enable the **Collect process and user attribution information** setting in the monitor that you deploy to that endpoint. For more information, see Create or edit a monitor on page 81.

If you disable this setting, Integrity Monitor does not return modifications to registry values as events. Create and delete operations are still recorded for individual registry values, regardless of this setting.

Determining watched subkeys

A path matches all subkeys recursively under a key or keys that are specified by the path. For example, if you specify the path `HKEY_LOCAL_MACHINE\a`, then the path matches all subkeys of the `a` key (such as `HKEY_LOCAL_MACHINE\a\x`, `HKEY_LOCAL_MACHINE\a\x\y`, and `HKEY_LOCAL_MACHINE\a\z`), unless you otherwise exclude them. If the **Collect process and user attribution information** setting is enabled in the monitor that you deploy to that endpoint, all values of matching subkeys are watched.

You cannot monitor an entire subtree, such as `HKEY_LOCAL_MACHINE`, and you cannot specify individual values within a key.

Using an abbreviation for a subtree

You can use the abbreviation for the subtree in a path. Integrity Monitor expands the subtree name when you save your changes. For example, you can enter the path `HKLM\MyKey`, which is saved as `HKEY_LOCAL_MACHINE\MyKey`.

Subtree abbreviations

Subtree name	Abbreviation
`HKEY_LOCAL_MACHINE`	`HKLM`
`HKEY_USERS`	`HKU`

Using the HKEY_CURRENT_USER subtree in a path

When you add a path in the `HKEY_CURRENT_USER` subtree, such as `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy`, Integrity Monitor changes the `HKEY_CURRENT_USER` subtree in the path to `HKEY_USERS\*` when you save your changes (for example, `HKEY_USERS\*\Software\Microsoft\Windows\CurrentVersion\Group Policy`). Because the Tanium Client uses the SYSTEM account, the `HKEY_CURRENT_USER` subtree applies to the SYSTEM account rather than the user account that is currently signed in to Windows. Using `HKEY_USERS\*` instead lets Integrity Monitor record events for all users, including the user account that is currently signed in to Windows.

Using a redirected registry key in a path

For 64-bit Windows, the registry redirector maps some keys, such as `HKEY_LOCAL_MACHINE\SOFTWARE\`, to a `WOW6432Node` subkey (for example, `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node`) for use by 32-bit applications. When you add key paths that are redirected under WOW64, the watchlist does not automatically include the parallel key paths under the `WOW6432Node` keys. If you want to monitor keys under these paths, you must enter them separately.

© 2026 Tanium Inc. All Rights Reserved

Example registry path

Example path and explanation	Examples of watched subkeys

Path (registry):
`HKEY_LOCAL_MACHINE\a\b*\c`
 	
The `*` wildcard character represents zero or more characters within a key name, but it does not match path separators.
	Examples of watched subkeys (without inclusions or exclusions defined):
	
	`HKEY_LOCAL_MACHINE\a\b\c\`
	`HKEY_LOCAL_MACHINE\a\BCD00000000\c\`
	`HKEY_LOCAL_MACHINE\a\b\c\d\`
	`HKEY_LOCAL_MACHINE\a\BCD00000000\c\d\`
	
	Examples of subkeys that are not watched (when only this path is specified):
	
	`HKEY_LOCAL_MACHINE\a\`
	`HKEY_LOCAL_MACHINE\a\b\d\c`

Path inclusions

If you define path inclusions, the path matches *only* subdirectories, files, or registry subkeys that match the inclusions. When you specify an inclusion with no wildcards, it limits the path to a specific subdirectory, file, or registry subkey that matches the path together with the inclusion. In an inclusion, you can use an asterisk wildcard character (`*`) to match a string of characters within a directory, file, or registry key name, or you can use two asterisks together (`**`) to include path separators (and therefore multiple directory or subkey levels) in the match.

File path inclusions

File path inclusions refine a file path to match a subset of the subdirectories and files that match the file path itself.

© 2026 Tanium Inc. All Rights Reserved

Example file path inclusions

Example path, inclusion, and explanation	Examples of watched directories and files

Path (Unix):
`/mypath`
Inclusion:
`test`
Because this example does not use wildcard characters in the inclusion, the path matches only the single subdirectory, non-recursively.
	Watched directory (without exclusions defined):
	`/mypath/test/`
	Examples of directories and files that are not watched (when only this path and inclusion are specified):
	`/mypath/test.txt`
	`/mypath/test1/`
	`/mypath/test/myfile.txt`
	`/mypath/mydir/test/`
	`/myotherpath/test/`

Path (Unix):
`/mypath`
Inclusion:
`test*`
Because this example uses a single `*` wildcard character at the end of the inclusion, the path matches any combination of valid path characters at the end of `/mypath/test`, but not directory separators.
	Examples of watched directories and files (without exclusions defined):
	`/mypath/test/`
	`/mypath/test.txt`
	`/mypath/test1/`
	Examples of directories and files that are not watched (when only this path and inclusion are specified):
	`/mypath/test/mydir/myfile.txt`
	`/mypath/test/myfile.txt`
	`/mypath/mydir1/test/`
	`/mypath/myfile.txt`
	`/mypath/Xtest/`

© 2026 Tanium Inc. All Rights Reserved

Example file path inclusions (continued)

Example path, inclusion, and explanation	Examples of watched directories and files

Path (Unix):
`/mypath`
 	
Inclusion:
`test**`
 	
Because this example uses two `*` wildcard characters at the end of the inclusion, the path matches any combination of directory separators and valid path characters at the end of `/mypath/test`.
	Examples of watched directories and files (without exclusions defined):
	
	`/mypath/test/`
	`/mypath/test.txt`
	`/mypath/test1/`
	`/mypath/test/myfile.txt`
	`/mypath/test/mydir/myfile.txt`
	
	Examples of directories and files that are not watched (when only this path and inclusion are specified):
	
	`/mypath/mydir1/test/`
	`/mypath/myfile.txt`
	`/mypath/Xtest/`

Path (Unix):
`/mypath`
 	
Inclusion:
`*test`
 	
Because this example uses a single `*` wildcard character at the beginning of the inclusion, the path matches any combination of valid path characters after `/mypath` that end with `test`, but not directory separators.
	Examples of watched directories and files (without exclusions defined):
	
	`/mypath/test/`
	`/mypath/Xtest/`
	`/mypath/myfile.test`
	
	Examples of directories and files that are not watched (when only this path and inclusion are specified):
	
	`/mypath/mydir1/mydir2/test/`
	`/mypath/mydir1/mydir2/Xtest/`
	`/mypath/myfile.txt`
	`/mypaty/test1/`
	`/mypath/test/mydir1/`
	`/mypath/test/myfile.txt`
	`/mypath/test.txt/`

© 2026 Tanium Inc. All Rights Reserved

Example file path inclusions (continued)

Example path, inclusion, and explanation	Examples of watched directories and files

Path (Unix):
`/mypath`
 	
Inclusion:
`**test`
 	
Because this example uses two `*` wildcard characters at the beginning of the inclusion, the path matches any combination of directory separators and valid path characters after `/mypath` that end with `test`.
	Examples of watched directories and files (without exclusions defined):
	
	`/mypath/test/`
	`/mypath/mydir1/mydir2/test/`
	`/mypath/Xtest/`
	`/mypath/mydir1/mydir2/Xtest/`
	`/mypath/myfile.test`
	
	Examples of directories and files that are not watched (when only this path and inclusion are specified):
	
	`/mypath/myfile.txt`
	`/mypaty/test1/`
	`/mypath/test/mydir1/`
	`/mypath/test/myfile.txt`
	`/mypath/test.txt/`

Path (Unix):
`/mypath`
 	
Inclusion:
`test?`
 	
Because this example uses a `?` wildcard character at the end of the inclusion, the path matches any directories and files after `/mypath` that match `test` plus one additional character.
	Examples of watched directories (without exclusions defined):
	
	`/mypath/test1/`
	`/mypath/testX/`
	
	NOTE Though a trailing path separator (`/`) is shown here to denote a directory, it is not included as part of the match for the `?` wildcard character in the inclusion.
	
	Examples of directories and files that are not watched (when only this path and inclusion are specified):
	
	`/mypath/test/`
	`/mypath/Xtest/`
	`/mypath/test.txt`

© 2026 Tanium Inc. All Rights Reserved

Example file path inclusions (continued)

Example path, inclusion, and explanation	Examples of watched directories and files

Path (Unix):
`/mypath`
Inclusion:
`**/**.log`
This example uses an inclusion with a path separator to specify that a matching file or directory must be in a directory that is at least one directory level below the path. The file or directory must end with `.log` but can otherwise include any combination of characters.
	Examples of watched directories (without exclusions defined):
	`/mypath/mydir1/mylog.log`
	`/mypath/mydir2/anotherlog.log`
	`/mypath/mydir1/mysubdir/mylog.log`
	Examples of directories and files that are not watched (when only this path and inclusion are specified):
	`/mypath/mylog.log`
	`/mypath/mydir/mylog.txt`

Registry path inclusions

Registry path inclusions refine a registry path to match a subset of the subkeys that match the registry path itself. Inclusions do not restrict value names; all values of matching keys are still watched.

Example registry path inclusions

Example path, inclusions, and explanation	Examples of watched subkeys

Path (registry):
`HKEY_LOCAL_MACHINE\MyKey`
Inclusion:
`test`
Because this example does not use wildcard characters in the inclusion, the path matches only the single subkey, non-recursively.
	Watched subkey (without exclusions defined):
	`HKEY_LOCAL_MACHINE\MyKey\test\`
	Examples of subkeys that are not watched (when only this path and inclusion are specified):
	`HKEY_LOCAL_MACHINE\MyKey\AnotherKey\test\`
	`HKEY_LOCAL_MACHINE\MyKey\test\AnotherKey\`

© 2026 Tanium Inc. All Rights Reserved

Example registry path inclusions (continued)

Example path, inclusions, and explanation	Examples of watched subkeys

Path (registry):
`HKEY_LOCAL_MACHINE\MyKey`
 	
Inclusion:
`test*`
 	
Because this example uses a single `*` wildcard character at the end of the subkey inclusion, the path matches any combination of valid path characters at the end of `HKEY_LOCAL_MACHINE\MyKey`, but not path separators.
	Examples of watched subkeys (without exclusions defined):
	
	`HKEY_LOCAL_MACHINE\MyKey\test\`
	`HKEY_LOCAL_MACHINE\MyKey\test1\`
	
	Examples of subkeys that are not watched (when only this path and inclusion are specified):
	
	`HKEY_LOCAL_MACHINE\MyKey\test\AnotherKey\`
	`HKEY_LOCAL_MACHINE\MyKey\AnotherKey\test\`
	`HKEY_LOCAL_MACHINE\MyKey\xtest\test\`

Path (registry):
`HKEY_LOCAL_MACHINE\MyKey`
 	
Inclusion:
`test**`
 	
Because this example uses two `*` wildcard characters at the end of the subkey inclusion, the path matches any combination of path separators and valid path characters at the end of `HKEY_LOCAL_MACHINE\MyKey`.
	Examples of watched subkeys (without exclusions defined):
	
	`HKEY_LOCAL_MACHINE\MyKey\test\`
	`HKEY_LOCAL_MACHINE\MyKey\test\AnotherKey\`
	`HKEY_LOCAL_MACHINE\MyKey\test1\`
	
	Examples of subkeys that are not watched (when only this path and inclusion are specified):
	
	`HKEY_LOCAL_MACHINE\MyKey\AnotherKey\test\`
	`HKEY_LOCAL_MACHINE\MyKey\xtest\test\`

© 2026 Tanium Inc. All Rights Reserved

Example registry path inclusions (continued)

Example path, inclusions, and explanation	Examples of watched subkeys

Path (registry):
`HKEY_LOCAL_MACHINE\MyKey`
 	
Inclusion:
`*test`
 	
Because this example uses a `*` wildcard character at the beginning of the inclusion, the path matches any combination of valid path characters after `/mypath` that end with `test`, but not path separators.
	Examples of watched subkeys (without exclusions defined):
	
	`HKEY_LOCAL_MACHINE\MyKey\test\`
	`HKEY_LOCAL_MACHINE\MyKey\xtest\`
	
	Examples of subkeys that are not watched (when only this path and inclusion are specified):
	
	`HKEY_LOCAL_MACHINE\MyKey\test\AnotherKey\`
	`HKEY_LOCAL_MACHINE\MyKey\AnotherKey\test\`
	`HKEY_LOCAL_MACHINE\MyKey\test1\`

Path (registry):
`HKEY_LOCAL_MACHINE\MyKey`
 	
Inclusion:
`**test`
 	
Because this example uses two `*` wildcard characters at the beginning of the inclusion, the path matches any combination of path separators and valid path characters after `/mypath` that end with `test`.
	Examples of watched subkeys (without exclusions defined):
	
	`HKEY_LOCAL_MACHINE\MyKey\test\`
	`HKEY_LOCAL_MACHINE\MyKey\test\AnotherKey\`
	
	Examples of subkeys that are not watched (when only this path and inclusion are specified):
	
	`HKEY_LOCAL_MACHINE\MyKey\AnotherKey\test\`
	`HKEY_LOCAL_MACHINE\MyKey\test1\`

Path exclusions

If you define path exclusions, the path does *not* match subdirectories, files, or registry subkeys that match the exclusions. When you specify an exclusion with no wildcards, it excludes a specific subdirectory, file, or registry subkey that matches the path together with the exclusion. In an exclusion, you can use an asterisk wildcard character (`*`) to match a string of characters within a directory, file, or registry key name, or you can use two asterisks together (`**`) to include path separators (and therefore multiple directory or subkey levels) in the match. Keep in mind that when you exclude a particular directory using a single asterisk (`*`), the subdirectories of that directory are still watched.

File path exclusions

File path exclusions define subdirectories or files within a path that are excluded from matching the path.

© 2026 Tanium Inc. All Rights Reserved

Example file path exclusions

Example path, exclusion, and explanation	Examples of excluded directories and files

Path (Unix):
`/mypath`
Exclusion:
`test`
This example does not use wildcard characters, so it excludes only a single directory.
	Example excluded directory:
	`/mypath/test/`
	Examples of directories that are still watched:
	`/mypath/test.txt`
	`/mypath/test1/`
	`/mypath/test1/myfile.txt`
	`/mypath/mydir/test/`

Path (Windows):
`C:\Windows\System32`
Exclusion:
`*\logs`
Because this exclusion begins with the characters `*\`, it excludes directories with the name `logs` that are exactly two levels below the `System32` directory.
	Example excluded directories:
	`C:\Windows\System32\script\Logs\`
	`C:\Windows\System32\winevt\Logs\`
	`C:\Windows\System32\winevt\Logs\Application.evtx`
	Examples of directories that are still watched:
	`C:\Windows\System32\`
	`C:\Windows\System32\cmd.exe`
	`C:\Windows\System32\GroupPolicy\`
	`C:\Windows\System32\Logs\`

Path (Windows):
`C:\Windows\System32`
Exclusion:
`**\logs`
Because this exclusion begins with the characters `**\`, it excludes directories with the name `logs` that are at least two levels below the `System32` directory.
	Example excluded directories:
	`C:\Windows\System32\script\Logs\`
	`C:\Windows\System32\winevt\Logs\`
	`C:\Windows\System32\winevt\Logs\Application.evtx`
	Examples of directories that are still watched:
	`C:\Windows\System32\`
	`C:\Windows\System32\cmd.exe`
	`C:\Windows\System32\GroupPolicy\`
	`C:\Windows\System32\Logs\`

© 2026 Tanium Inc. All Rights Reserved

Example file path exclusions (continued)

Example path, exclusion, and explanation	Examples of excluded directories and files

Path (Unix):
`/mypath`
Exclusion:
`*`
When you specify a single `*` wildcard as the entire exclusion, it excludes subdirectories at the first level but still watches subdirectories at lower levels.
	Example excluded directories:
	`/mypath/test/`
	`/mypath/mydir/`
	Watched directories:
	`/mypath/`
	`/mypath/test/subdirectory/`
	`/mypath/mydir/mydir2/`
	`/mypath/mydir/mydir2/mydir3/`

Path (Unix):
`/mypath`
Exclusion:
`**`
When you specify two `*` wildcard characters as the entire exclusion, it restricts the path to only the exact directory that you specify.
	Example excluded directories:
	`/mypath/test/`
	`/mypath/mydir/`
	Watched directory:
	`/mypath/`

Registry path exclusions

Registry path exclusions define subkeys within a path that are excluded from matching the path. Exclusions do not apply to value names; all values of matching keys that are not excluded are still watched.

Example registry path exclusions

Example path, exclusion, and explanation	Examples of excluded directories and files

Path (registry):
`HKEY_LOCAL_MACHINE\MyKey`
Exclusion:
`test`
This example does not use wildcard characters, so it excludes only a single directory, non-recursively.
	Excluded subkey:
	`HKEY_LOCAL_MACHINE\MyKey\test\`
	Examples of subkeys that are not excluded:
	`HKEY_LOCAL_MACHINE\MyKey\`
	`HKEY_LOCAL_MACHINE\MyKey\test1\`
	`HKEY_LOCAL_MACHINE\MyKey\SomeSubkey\test\`

© 2026 Tanium Inc. All Rights Reserved

Example registry path exclusions (continued)

Example path, exclusion, and explanation	Examples of excluded directories and files

Path (registry):
`HKEY_LOCAL_MACHINE\MyKey`
Exclusion:
`test*`
This example uses a single `*` wildcard character at the end of the exclusion. It excludes any combination of valid path characters at the end of `HKEY_LOCAL_MACHINE\MyKey\test`, but it does not match path separators.
	Examples of excluded subkeys:
	`HKEY_LOCAL_MACHINE\MyKey\test\`
	`HKEY_LOCAL_MACHINE\MyKey\test1\`
	Examples of subkeys that are not excluded:
	`HKEY_LOCAL_MACHINE\MyKey\test\AnySubkey\`
	`HKEY_LOCAL_MACHINE\MyKey\test1\AnySubkey\`
	`HKEY_LOCAL_MACHINE\MyKey\SomeSubkey\AnotherLevel\`
	`KEY_LOCAL_MACHINE\MyKey\SomeSubkey\test\`
	`HKEY_LOCAL_MACHINE\MyKey\AnotherSubkey\AnotherLevel\`

Path (registry):
`HKEY_LOCAL_MACHINE\MyKey`
Exclusion:
`test**`
This example uses two `*` wildcard characters at the end of the exclusion. It excludes any combination of path separators and valid path characters at the end of `HKEY_LOCAL_MACHINE\MyKey\test`.
	Examples of excluded subkeys:
	`HKEY_LOCAL_MACHINE\MyKey\test\`
	`HKEY_LOCAL_MACHINE\MyKey\test\AnySubkey\`
	`HKEY_LOCAL_MACHINE\MyKey\test1\`
	`HKEY_LOCAL_MACHINE\MyKey\test1\AnySubkey\`
	Examples of subkeys that are not excluded:
	`HKEY_LOCAL_MACHINE\MyKey\SomeSubkey\AnotherLevel\`
	`KEY_LOCAL_MACHINE\MyKey\SomeSubkey\test\`
	`HKEY_LOCAL_MACHINE\MyKey\AnotherSubkey\AnotherLevel\`

© 2026 Tanium Inc. All Rights Reserved

Example registry path exclusions (continued)

Example path, exclusion, and explanation	Examples of excluded directories and files

Path (registry):
`HKEY_LOCAL_MACHINE\MyKey`
 	
Exclusion:
`**\**`
 	
This example demonstrates the pattern you can use to limit the number of levels watched. This example limits the path to matching one subkey level. You can use another `\**` character combination in the exclusion for each level you want to exclude. For example, to monitor two levels of subkeys under the specified path, add the exclusion `**\**\**` instead.
	Examples of excluded subkeys:
	
	`HKEY_LOCAL_MACHINE\MyKey\SomeSubkey\AnotherLevel\`
	`HKEY_LOCAL_MACHINE\MyKey\AnotherSubkey\AnotherLevel\`
	
	Examples of subkeys that are not excluded:
	
	`HKEY_LOCAL_MACHINE\MyKey\`
	`HKEY_LOCAL_MACHINE\MyKey\SomeSubkey\`
	`HKEY_LOCAL_MACHINE\MyKey\AnotherSubkey\`

Path inclusions and exclusions used together

Exclusions take precedence over inclusions. If you define both inclusions and exclusions, the path matches all directories, files, or registry keys that match the inclusions, *except* those that match exclusions.

Example file paths with inclusions and exclusions

Example path, inclusion, exclusion, and explanation	Examples of watched directories and files

Path (Unix):
`/mypath`
 	
Inclusion:
`mydir/**`
 	
Exclusion:
`**.log`
 	
The inclusion specifies files and directories within the `/mypath/mydir` subdirectory, and the exclusion keeps any files with the `log` extension within this directory structure from being watched.
	Example watched directories and files:
	
	`/mypath/mydir/myfile.txt`
	`/mypath/mydir/mysubdir/`
	`/mypath/mydir/mysubdir/myscript.sh`
	
	Examples of directories and files that are not watched:
	
	`/mypath/someotherdir/`
	`/mypath/someotherdir/anyfile.txt`
	`/mypath/mydir/myprogram.log`
	`/mypath/mydir/mysubdir/anotherprogram.log`

© 2026 Tanium Inc. All Rights Reserved

Example file paths with inclusions and exclusions (continued)

Example path, inclusion, exclusion, and explanation	Examples of watched directories and files

Path (Windows):
`C:\Windows`
 	
Inclusion:
`System32\**`
 	
Exclusion:
`System32\**\**`
 	
The inclusion with a trailing wildcard character is paired with a matching exclusion ending in `**\**` to end the recursion at a specified depth. If you want to monitor files in subdirectories with depth `n`, add `n+1` pairs of asterisks (`**`) separated by path separators (`\` or `/`, depending on the target Tanium Client managed endpoint operating system).
	Example watched files:
	
	`C:\Windows\System32\ARP.exe`
	`C:\Windows\System32\cmd.exe`
	`C:\Windows\System32\wwapi.dll`
	
	Examples of files that are not watched:
	
	`C:\Windows\System32\drivers\acpi.sys`
	`C:\Windows\System32\winevt\Logs\Application.evtx`
	`C:\Windows\System32\WinMetadata\Windows.Data.winmd`

Example registry path with inclusions and exclusions

Example path, inclusion, exclusion, and explanation	Examples of watched subkeys

Path (registry):
`HKEY_LOCAL_MACHINE\MyKey`
 	
Inclusion:
`Test**`
 	
Exclusion:
`TestTwo**`
 	
The inclusion specifies any subkey that begins with `Test` within the `MyKey` key, but the exclusion keeps any subkey that begins with `TestTwo` from being watched.
	Example watched subkeys:
	
	`HKEY_LOCAL_MACHINE\MyKey\Test\`
	`HKEY_LOCAL_`
	`MACHINE\MyKey\Test\AnySubkey\`
	`HKEY_LOCAL_MACHINE\MyKey\TestOne\`
	`HKEY_LOCAL_`
	`MACHINE\MyKey\TestOne\AnySubkey\`
	
	Examples of subkeys that are not watched:
	
	`HKEY_LOCAL_MACHINE\MyKey\TestTwo\`
	`HKEY_LOCAL_`
	`MACHINE\MyKey\TestTwo\AnySubkey\`
	`HKEY_LOCAL_MACHINE\MyKey\TestTwoThree\`

© 2026 Tanium Inc. All Rights Reserved