Tanium Threat Response User Guide

2026H2 Semiannual Release

Version 4.24

November 17, 2026



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

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

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

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

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

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

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

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

©2026 Tanium Inc. All Rights Reserved

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

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

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

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

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

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

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

© 2026 Tanium Inc. All rights reserved.

Table of contents

Overview 13
- Investigation 13
- Detection 13
- Containment 13
- Tanium Autonomous IT Platform in Threat Response 13
- Supported languages 14
- Interoperability with other Tanium products 15

Gaining organizational effectiveness 17

Requirements 30
- Core platform dependencies 30
- Computer group dependencies 31
- Solution dependencies 31
  - Tanium recommended installation 31
  - Import specific solutions 31
  - Required dependencies 32
  - Feature-specific dependencies 32
- Client extensions and endpoint tools 33
- Tanium™ Module Server 33
- Endpoints 33
  - Disk space requirements 36
  - CPU and memory requirements 37
  - Tanium Driver 37
- Host and network security requirements 37
  - Ports 37
    - Ports for Threat Response communication 38
  - Security exclusions 39
  - Threat Response server exclusions 40
  - Threat Response endpoint exclusions 40

©2026 Tanium Inc. All Rights Reserved

User role requirements 50

Installing 63
Before you begin 63
Import Threat Response with default settings 64
Default settings for Threat Response 64
Threat Response import notes 64
Import Threat Response with custom settings 65
Manage solution dependencies 65
Upgrade the Threat Response version 66
Verify Threat Response version 66

Configuring 68
Install and configure Tanium Endpoint Configuration 68
Manage solution configurations with Tanium Endpoint Configuration 68
Threat Response Endpoint Configuration approvals 70
Configure Threat Response 70
Configure the Threat Response action group 70
Set up Threat Response users 72
Select a language 75

Getting started with Threat Response 76
Evidence and telemetry 77
Profiles 78
Live Response 79
Alerting and detection 80
Extended detections 80
3rd party intel feeds 82
Endpoint isolation 82
Tanium default quarantine profile 82
Create quarantine profile 83
Incident response automation 83
Tanium default alert reactions 83
Endpoint reactions 84
Automate playbooks 84
SIEM integration 84
Send stream data to SIEM 85

©2026 Tanium Inc. All Rights Reserved

Send alerts to SIEM 85
Send Audit Logs to SIEM 85

Adding intel 87
Signals 87
Signals do not always evaluate with the recorder database 88
Signals best practices 88
Intel safeguards 90
Configure Intel Safeguards 91
Disable Intel Safeguards for an intel document 92
Configure intel sources 92
Connect to the Tanium Signals feed 93
Configuring Tanium Signals feed in an airgapped environment 95
Connect to a TAXII server 96
Set up Connect and Wildfire 98
Use a local directory or remote share 98
Delete an intel source 100
Configure process injection 100
Reputation data 103
Configure reputation data in Tanium Connect 103
Add signals 104
Import and export signals 106
Export signals 106
Import signals 107
Upload intel documents 108
Create intel documents 108
Create IOCs 109
Label intel 111
Apply a label 111
Manage existing labels 111
Configure YARA files 112
View orphaned intel documents 113
Assign a reaction to an intel document 113
Testing Intel for deployment 113

Searching with threat navigator 115

©2026 Tanium Inc. All Rights Reserved

Search with intel 116
Quick filters 117
Pin artifacts to a search 118
Pin an artifact to a search 119
Unpin an artifact 119
Iterate on searches 120
Choose existing intel 120
Import intel 122
View search activity 122
View search results 124
Create hypotheses 125
Export a hypothesis 126
View MITRE techniques 126
Add MITRE techniques to a search 128
Manage MITRE techniques for multiple searches 128
Add MITRE techniques to a hypothesis 129

Creating reactions 130
Create a reaction 130
Assign a reaction to an intel document 134
Reaction statuses 135
Audit reaction data 136

Analyzing context 137
Analyze the context of artifacts 138
Export Context Analyzer results 139

Scanning endpoints 141
Background scans 142
On-demand scans 142

Creating configurations in Threat Response 144
Overview 144
Create detection configurations 144
Create index configurations 146
Create indexing exclusions 149
Create recorder configurations 149

©2026 Tanium Inc. All Rights Reserved

Create stream configurations 154
Create filters 164
Import and export configurations and filters 179
Export configurations 180
Export filters 180
Import configurations 180
Import filters 181

Creating profiles in Threat Response 182
Overview 182
Tanium Managed profiles 183
Create a profile 184
Prioritize profiles 186
Deploy a profile 186
Deploy intel 187
Configure the intel deployment setting 188
Immediately deploy intel to endpoints 188

Direct connecting to endpoints and exploring data 189
Direct connect to an endpoint 189
Add to investigation 190
Capture a snapshot 191
Close the connection 191
Browse the file system on connected endpoints 191
Search for events 192
View process details and hash ratings 194
Explore artifact and event details with Tanium Autonomous IT 195
Manage snapshots 196
Export a snapshot from an endpoint 196
Download a snapshot 196
Upload a snapshot 197
Save files and events 197
Download a file 198
Create Enforce rules 199
Export events 200
Manage IOCs 200

©2026 Tanium Inc. All Rights Reserved

Generate an IOC 200

Searching across the enterprise 202

Managing alerts 262
View alerts 263
Decode encoded text 263
Explore alert details with Tanium Autonomous IT 264
Alert enrichment 264
Alert analysis 265
Assign a status to an alert 265
View alerts by intel document 266
Microsoft Defender alerts 266
Deep Instinct alerts 267
Investigate reputation data 268
Investigate alerts 269
Distinguish between malicious and false positive alerts 270
Filter false positives 271
Add alerts to an investigation in Tanium Investigate 272
Deploy an action to an endpoint 272
Initiate a Response Action from an alert 273
Remediate alerts in Tanium Enforce 274
Export alerts 277
Delete alerts 278
Suppress alerts 278
Suppress an alert 280
Edit and delete suppression rules 280
View the status of a retroactive task 281
Import and export suppression rules 282
Export specific suppression rules 282
Export all suppression rules 282
Import suppression rules 282
Manage the impact of lateral movement with Tanium Impact 283
Set up Tanium Connect forwarding 283

Managing response activity 286

©2026 Tanium Inc. All Rights Reserved

Create a response action for an endpoint 286
Response Action: Download File 286
Response Action: Gather Snapshot 287
Response Action: Live Response 287
Response Action: Quarantine 290
Response Action: Unquarantine 290
Stop a response action 291

Collecting data from endpoints 292
Destinations 292
Destination types 294
Azure Destinations 294
S3 Destinations 295
SSH Destinations 296
SMB Destinations 297
Generate known_hosts and test connections 297
Collections 299
File Collector sets 302
Script sets 312
Collect data from endpoints 312
Collect logs 314
Regular expressions and environment variables 314

Quarantining compromised endpoints 317
Before you begin 320
Endpoint operating system requirements 321
Supported Windows versions 321
Supported Linux OS versions 322
Supported macOS versions 322
Create quarantine rules 323
Create a quarantine profile 324
Delete a profile 329
Duplicate a profile 329
Edit a profile 330
Export a profile 330
Export all profiles 330

©2026 Tanium Inc. All Rights Reserved

Import a profile 330
Generate Quarantine Packages 330
Test quarantine on endpoints 332
View quarantined endpoints 334
Remove endpoints from quarantine 334
Reference: Create custom quarantine rules 334
Reference: Custom rules and options 335
Custom rules format 336
Reference: Custom rules examples 337
Example for Custom Quarantine Rules field 337
taniumquarantine.dat sample file 337

Exporting audit data 339
Tanium Connect 342
Before you begin 342
Create a connection 342
Test a connection and review audit data 343
Schedule the connection 343

Maintaining 344
Review and remediate Tanium Threat Response issues 344
Get Threat Response endpoint tools status and configurations 345
Monitor and troubleshoot Threat Response coverage 349
Monitor and troubleshoot mean time to investigate threats 349
Monitor and troubleshoot mean time to remediate threats 350

Troubleshooting 351
Collect logs 353
Collect troubleshooting information from the Threat Response service 353
Collect troubleshooting information from endpoints 353
View notifications 354
View task status 355
View and export log data 356
Remove Threat Response tools from endpoints 358
My device has no profile or the wrong profile 360
No alerts are generated 362

©2026 Tanium Inc. All Rights Reserved

Too many alerts are generated 363
The lifetime of recorder events is too short 364
File, network, or security events are not displayed on Oracle Linux server 365
Identify Linux endpoints that are missing auditd 366
Start or stop the recorder 366
Files are not being hashed or indexed 367
Configure client disk space use 368
Cannot establish a live connection 368
Test Live Response connections manually 368
Stream is not sending data 369
Stream is sending too much data 370
Configuration not available or not updated to the latest settings when deploying package 371
Action not running on endpoint 371
Artifacts not being copied to destination 371
Custom configurations are missing 372
Live Connections are not working while quarantined 372
Live Response is not working to copy files to the destination while quarantined 372
Verify endpoint tools 373
Uninstall Threat Response 373
Contact Tanium Support 373

Reference: Common health check issues 374

Reference: Alert data 378

Reference: Set up the zone proxy service 400

Reference: Gateway examples for Threat Response 401
Assign Resolved status to an alert 401
Assign Resolved status to alert 401

©2026 Tanium Inc. All Rights Reserved

Threat Response overview

Use Threat Response to expedite incident response actions from hours or days to minutes. Detect, react, and recover quickly from attacks and the resulting business disruptions.

Investigation

Threat Response continuously records key system activity for forensic and historical analysis. You can look for specific activity across every endpoint in an enterprise and drill down into process and user activity on individual endpoints in both real-time and historical views. You can investigate alerts from external sources such as Microsoft Defender and Deep Instinct to leverage the endpoint visibility provided by Threat Response.

Detection

Threat Response monitors activity in real time and generates alerts when potential malicious behavior is detected. You can configure threat intelligence from a variety of reputable sources. Use threat intelligence to search endpoints for known indicators of compromise and perform reputation analysis. The reputation data that Threat Response uses constantly compares activity such as all processes run, autorun related files, and loaded modules against known malicious hashes defined by user hash lists or other services such as Palo Alto Wildfire, VirusTotal, and ReversingLabs.

Containment

Threat Response includes sensors and packages that provide endpoint visibility and remediation. With the sensors, you can search endpoint data quickly for evidence of compromise. When you have discovered compromised endpoints, you can use Threat Response packages to isolate incidents and prevent additional compromise, data leakage, and lateral movement.

Tanium Autonomous IT Platform in Threat Response

Tanium Autonomous IT Platform comprises a set of interrelated features across multiple Tanium solutions that collect real-time intelligence about conditions in your environment. Tanium Threat

©2026 Tanium Inc. All Rights Reserved

Response provides the following Autonomous IT Platform features:

- **Tanium Automate playbook steps**: Tanium Automate implements endpoint quarantine and quarantine removal in playbook steps. For more information, see Quarantining endpoints on page 317, Tanium Automate User Guide: Building playbooks, and Tanium Automate User Guide: Reference: Steps.

- **Default configuration**: Threat Response provides common configuration workflows to expedite the time to value and to simplify the initial configuration experience. Configuration categories that target specific end-to-end scenarios decrease the number of steps required to operationalize Threat Response without having a comprehensive knowledge of all of the functionality of the module.

Supported languages

You can select one of the languages in the following table for user interface (UI) text in the Threat Response workbench and Tanium documentation.

The language that you select for the workbench also sets the date and time format:

- Dates: In the table, the letters `dd`, `mm`, and `yyyy` represent the digits for day, month, and year respectively.
- Times: English (United States) times use the 12-hour clock in the format hh:mm:ss [AM|PM] <time zone>, where `hh`, `mm`, and `ss` represent the hour, minute, and second respectively. Other times use the 24-hour clock, where GMT-<#> indicates the offset from Greenwich Mean Time (GMT). For example, `GMT-7` indicates a time zone that is 7 hours ahead of GMT.

Supported languages with associated date and time formats

Language	Locale code	Date and time format
English (United States)	en-US	mm/dd/yyyy [AM|PM] <time zone>
French (France)	fr-FR	dd/mm/yyyy GMT- <#>
German (Germany)	de-DE	dd/mm/yyyy GMT- <#>
Japanese (Japan)	ja-JP	yyyy/mm/dd GMT- <#>
Korean (Korea, Republic of)	ko-KR	yyyy.mm.dd GMT- <#>
Spanish (Latin American)	es-LA	dd/mm/yyyy GMT- <#>

For information about language support, which types of text are translated, and the steps to select a language, see Tanium Console User Guide: Reference: Language support.

©2026 Tanium Inc. All Rights Reserved

Interoperability with other Tanium products

Threat Response works with Tanium™ Connect, Tanium™ Data Service, Tanium™ Enforce, Tanium™ Impact, and Tanium™ Investigate for additional alerting, remediation, and trending of incident related data.

Tanium Connect

Configure a Connect destination to export Threat Response data outside of Tanium. Connect can send information to security information and event management (SIEM) products and services including Micro Focus ArcSight, IBM QRadar, LogRhythm, McAfee SIEM, and Splunk. For more information, see Connect User Guide: Configuring SIEM destinations. Threat Response sends hash information from saved questions to Connect and reputation service providers to elaborate on process hashes for an at-a-glance reputation status. You can also configure incoming connections from sources such as Palo Alto Wildfire to create threat data.

Tanium Data Service

Tanium Data Service (TDS) is a Tanium shared service that enables you to view stored sensor results for endpoints that are offline at the moment you issue a question. For more information about TDS, see Managing Tanium Data Service.

Tanium Enforce

Use Threat Response findings to create process and network rule policies for endpoints to prevent future incidents across the network. Failing to identify and address more fundamental vulnerabilities exploited during an incident leaves the organization with no net improvement to their security posture.

Tanium Impact

Use alert integration with Impact to take a data-driven approach to manage lateral movement impact within your organization by identifying, prioritizing and remediating access rights dependencies to reduce attack surface, prioritize actions, and scope incidents.

©2026 Tanium Inc. All Rights Reserved

Tanium Investigate

From the sample details view in the context analyzer and the events grid on direct endpoint connections, you can add events to an investigation in Tanium Investigate. With Tanium Investigate you can identify the root cause of issues that arise on Tanium-managed endpoints and arrive at resolutions to issues more quickly. For more information, see Tanium Investigate User Guide.

©2026 Tanium Inc. All Rights Reserved

Gaining organizational effectiveness with Threat Response

There are four key organizational governance steps to maximizing the value delivered by Threat Response to enable time to value:

- Develop a dedicated change management process. For more information, see Change management on page 17.
- Define distinct roles and responsibilities. For more information, see RACI chart on page 18.
- Track operational maturity. For more information, see Operational metrics on page 24.
- Validate cross-functional alignment. For more information, see Organizational alignment on page 24.

Change management

Develop a tailored, dedicated change management process to set up any incident response tools for a streamlined process using Tanium Threat Response.

- Update service level agreements and align activities to key resources for Tanium Threat Response where applicable. For example, see Maturity / Metrics and RACI
- Designate change or maintenance windows for various scenarios, where applicable. For example, setting up a Reputation source, integration with a SIEM, Log Solution, or SOAR solution.
- Identify internal and external dependencies to incident response process. For example, to achieve effective integrations with a SIEM, Log Solution, or SOAR Solution.
- Create a Tanium Steering Group (TSG) for discovery activities to expedite reviews and approvals of processes that align with SLAs / incident response processes, as applicable.

©2026 Tanium Inc. All Rights Reserved

RACI chart

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

RACI chart for Threat Response roles and responsibilities

Task	SOC (Detection & Alerts) / L1	Hunting Team / L2	Incident Response (IR)	CISO	C-Level	Rationale
Unstructured Threat Investigation	C/I	R/A	C/I	-	-	One of three starts to an investigation. For example, you have a hypothesis or are not sure of specific indicators to look for. You have not yet identified a problem and use Enterprise Hunting or other tools to investigate and understand a problem.
Known Target/ Hypothesis	R/A	C/I	C/I	I	-	One of three starts to an investigation wherein a known target has been identified; for example, malware X or attacker Y uses this capability or technique for malicious intent in the environment. Use one of four techniques (Index, Incident Response Sensors, Live Connection, or Tanium Questions) to understand this known target. For example, use Tanium questions to show malware and what is relevant to that technique. You might not have a specific indicator or file you are looking for, but you know the attacker will put unusual things in outruns such as a technique - but not an indicator - and use for known target

©2026 Tanium Inc. All Rights Reserved

Task	SOC (Detection & Alerts) / L1	Hunting Team / L2	Incident Response (IR)	CISO	C-Level	Rationale
						for questions.
Enterprise Hunting: Index, Incident Response Sensors, Tanium Questions, Live Connections	CI	R/A	R/A	-	-	Using Tanium questions to gather enterprise-wide data to establish a hypothesis and establish what is normal activity.
Establish what is normal activity	R/A	R/A	R/A	-	-	Use autoruns to establish normal activity from abnormal activity. For example, if a network has 10 devices that all demonstrate the same conditions, or establish that 9 out of 10 are normal. Something might only be available on one endpoint demonstrating a need for investigation. If you have identified what is normal or abnormal, go to establishing the hypothesis of the activity; for example, an attacker created an autorun.
Establish hypothesis of activity	C/I	R/A	R/A	I	-	When you have established what is normal versus abnormal, you can establish a hypothesis of the activity and conduct additional hunting for more information or establish suspicious activity to take action or remediation.
Additional hunting	I	R/A	R/A	-	-	While working through what is normal versus abnormal activity, and establishing a

©2026 Tanium Inc. All Rights Reserved

Task	SOC (Detection & Alerts) / L1	Hunting Team / L2	Incident Response (IR)	CISO	C-Level	Rationale
required						hypothesis to perform actions or remediate, you might conduct additional hunting to understand the behavior.
Reputation and third-party validation	R/A	C/I	C/I	-	-	The reputation services provide the capability to compare information from the enterprise against lists of known bad at scale. The reputation service and Threat Response integrate to automatically search for relevant artifacts and then create IOCs from any malicious reputations discovered in the environment and then scan them to establish exposure.
Establish suspicious activity	R/A	R/A	R/A	I	I	When the suspicious activity has been established, decide on a course of action that might require further monitoring or investigation, or remediate the suspicious activity using Tanium and/or external tools.
Further Investigation: Live Connection	C/I	R/A	R/A	-	-	Further investigations might be required to establish the real cause of any activity discovered in the previous steps. This might be performed entirely in the Tanium platform or by gathering information for analysis in 3rd party applications.
Further Investigation: Live Response	C/I	R/A	R/A	-	-	Further investigations might be required to establish the real cause of any activity discovered on the previous steps. This might be performed entirely in the Tanium platform or by gathering information for analysis in 3rd party applications.

©2026 Tanium Inc. All Rights Reserved

Task	SOC (Detection & Alerts) / L1	Hunting Team / L2	Incident Response (IR)	CISO	C-Level	Rationale
Further Investigation: Questions	R/A	R/A	R/A	-	-	Further investigations might be required to establish the real cause of any activity discovered on the previous steps. This might be performed entirely in the Tanium platform or by gathering information for analysis in 3rd party applications.
Select Action/ Actions	R/A	R/A	R/A	I	-	Apply established process for further action or discuss and establish new course of action for previously undocumented activity.
Remediation: Operational Modules	C/I	C/I	C/I	-	-	When a suspicions activity has been established, and an action identified, remediation can be conducted using Tanium Operational Modules. This may often be outside of the realm of responsibility of the security organization who needs to hand off the requirement to the operations team or might involve some level of security team involvement in actions such as quarantining while further action is performed.
Remediation: Security/Risk Modules	R/A	C/I	C/I	-	-	When suspicious activity has been established, and an action identified, remediation can be conducted using Tanium Security Modules through Threat Response. For example, use built-in actions to kill processes, quarantine endpoints, delete files and folders, delete registry keys, or use Tanium Enforce for application allowlisting, firewall configuration, or security policy management.
Remediation:	C/I	C/I	C/I	I/R/A	I	When suspicious activity has been established,

©2026 Tanium Inc. All Rights Reserved

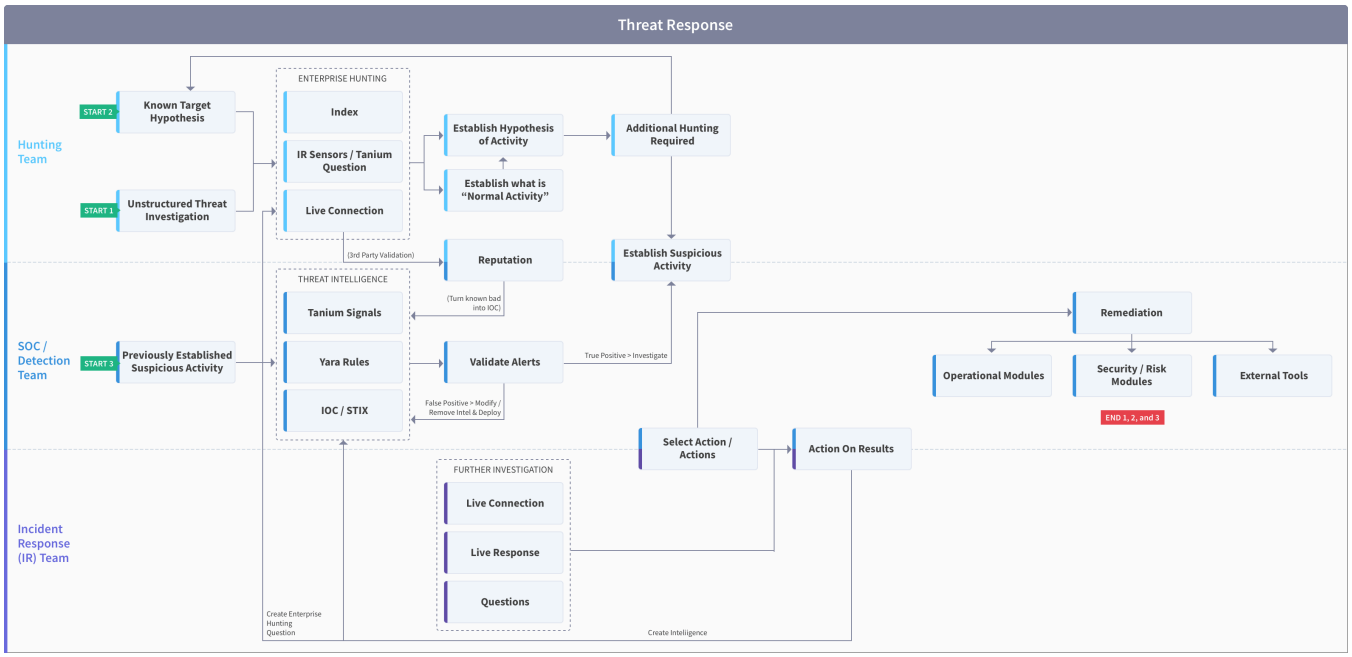
Task	SOC (Detection & Alerts) / L1	Hunting Team / L2	Incident Response (IR)	CISO	C-Level	Rationale
External Tools						and an action identified, remediation can be conducted using third-party capabilities and/or external organizations. This might often be outside the realm of responsibility of the security organization who need to hand off the requirement to the operations team or might involve some level of security team involvement in actions like quarantining while further action is performed.
Previously established suspicious activity	R/A	C/I	C/I	-	-	One of three starts to detection activity; for example, use Tanium Signals, YARA rules, and or IOC/STIX to validate alerts and identify true positives to further investigate and identify false positives to modify or remove intelligence and redeploy alerts.
Threat Intelligence: Tanium Signals	R/A	C/I	C/I	-	-	Install and deploy threat intelligence and then monitor systems for alerts from the environment.
Threat Intelligence: YARA Rules	R/A	C/I	C/I	-	-	Install and deploy threat intelligence and then monitor systems for alerts from the environment.
Threat Intelligence: IOC/STIX	R/A	C/I	C/I	-	-	Install and deploy threat intelligence and then monitor systems for alerts from the environment.
Validate Alerts: True Positive >	R/A	R/A	R/A	-	-	Activity that results as part of Threat Intelligence activities to validate an alert as a true positive and further investigate. This can

©2026 Tanium Inc. All Rights Reserved

Task	SOC (Detection & Alerts) / L1	Hunting Team / L2	Incident Response (IR)	CISO	C-Level	Rationale
Investigate						result in escalation to higher levels.
Validate Alerts: False Positive > Modify/ Remove Intelligence and Redeploy	R/A	R/A	R/A	-	-	SOC/L1 activity to analyze alert data and validate an alert as a false positive. This results in an action to modify or remove intelligence or to redeploy threat intelligence. Control of Threat Intelligence is often the responsibility of hunting or incident response teams.
Action on Results: Create Enterprise Hunting Question or Intelligence	C/I	R/A	R/A	I	-	Create alerts based on intelligence, hunting, or detection activities for automation. For example, Saved questions, alerts, or signals. Use the enterprise hunting dashboard to ask a saved question and have the results sent to SIEM or reputation tool.

Figure 1. Standard Threat Response workflow (click image to enlarge)

©2026 Tanium Inc. All Rights Reserved



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 on how to manage software and hardware assets.

Operational metrics

Threat Response maturity

Managing an incident response 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 Threat Response program are as follows:

©2026 Tanium Inc. All Rights Reserved

Threat Response maturity key processes

Process	Description
Usage	how and when Tanium Threat Response is used in your organization
Automation	how automated Tanium Threat Response is, across endpoints
Functional Integration	how integrated Tanium Threat Response is, across IT security, IT operations, and IT risk or compliance teams
Reporting	how automated Tanium Threat Response is and who the audience of Threat Response reporting is

Benchmark metrics

In addition to the key incident response processes, the three key benchmark metrics that align to the operational maturity of the Tanium Threat Response program to achieve maximum value and success are as follows:

Threat Response benchmark metrics

Executive Metrics	Threat Response Coverage	Mean Time to Investigate Threats	Mean Time to Remediate Threats
Description	The percentage of endpoints that are running Threat Response tools.	The average number of days to perform analysis of threats.	The average number of days to remediate threats.
Instrumentation	The number of endpoints with an active Threat Response profile.	The time it takes from an Alert was received, to when remediation work on the detected alert begins.	The time it takes to author an Action or Enforce Remediation Policy status to resolve applicable Alerts.
Why this metric matters	If you are not including the entirety of your estate when searching for specific activity, then you are at risk.	The more quickly you can evaluate the risk associated with a given activity, the more quickly you can begin remediating a threat.	The more quickly you can remediate a threat, the more you can contain the associated damage.

Use the following table to determine the maturity level for Tanium Threat Response in your

©2026 Tanium Inc. All Rights Reserved

organization.

Threat Response maturity levels by process and metric

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
Process	Usage	Threat Response installed; deployment profiles applied. Use of Threat Response questions and investigations. Components configured or in use: Index, Recorder, Detect.	Some Tanium Signals deployed; understanding of Tanium Signals syntax basics. Live Response Destinations configured and tested. Tanium IR Quarantine tested with default configuration. Components in use: Index, Recorder, Detect, Live Response, Trends.	Threat intelligence testing process created; tailoring Tanium Signals to the environment. Process injection alerting enabled. Multiple custom Live Response forensic data collection configurations created. Tanium IR Quarantine custom configuration setup and tested. Default Recorder filters implemented. Using Quick Scans and Background Scanning for Threat Response Intel. Components in	Tuned deployment strategy for profiles and intel documents, including intel testing and promotion. Process injection alerting enabled and tuned. Creation of suppression rules for Tanium Signals to reduce false positives. Threat Response Alert triage and remediation using Response Actions Custom Recorder filters. Enables longer data retention,	Proactive hunting for malicious activity (through Enterprise Hunting or Incident Response Sensors). Process injection alerting enabled and tuned. Generating custom YARA rules, IOCs, and Tanium Signals and sharing through the Threat Response community. Enables development and application of customized intel for given industry vertical and industry specific information

©2026 Tanium Inc. All Rights Reserved

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
				use: Index, Recorder, Detect, Live Response, Trends, IR Content, Reputation.	less noise when investigating events, and better performance of THR on endpoints. Components in use: Index, Recorder, Detect, Live Response, Trends, IR Content, Reputation, Connect, SIEM / Log Solution Integration, Tanium Impact	sharing and analysis centers (ISACs). Components in use: Index, Recorder, Detect, Live Response, Trends, IR Content, Reputation, Connect, SIEM / Log Solution Integration, Tanium Enforce.
	Automation	Some intelligence applied and imported (For example, a few Tanium Signals, OpenIOC Intel, etc.)	Additional threat intelligence applied, and intel sources added. Ex: out of the box Tanium Signals, OpenIOCs, and a subscription to a TAXII source has been configured to automate searching for malicious behavior.	Tanium Reputation and Tanium Connect saved question configured to automatically feed hashes to Reputation Providers.	Automated Threat Response scanning of malicious hashes found via Reputation providers. Using the Threat Response API to automate tasks.	Integration with a SOAR Solution to automate evidence gathering, response actions, intel management (adding/ removing/ scanning), remediation, etc.)

©2026 Tanium Inc. All Rights Reserved

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
	Functional integration	N/A	Trends Boards imported and / or integration with Reputation provider.	Threat Response is configured to surface alerts from Windows Defender and/or Deep Instinct.	Tanium Connect, SIEM / Log Solution integrated. Ex: Splunk and Yara rules set up or Splunk integration set up.	Creating remediation policies through Tanium Enforce and integration with a SOAR solution to automate data collection and performing actions.
	Reporting	Manual; through Threat Response workbench or dashboard for operators only.	Manual; Threat Response integration with Tanium Trends.	Automated; exporting data through file, email, or SQL to feed reports.	Automated; using SIEM / Log Solution; Ex: Splunk including the Tanium Splunk application.	Automated; using a SOAR solution for a holistic view of activity.
Metrics	Threat Response Coverage (% of Total)	0-60%	61-70%	71-85%	86-94%	>95%
	Mean Time to Investigate Threat (time)	>45 days	31-45 days	15-30 days	8-14 days	0-7 days
	Mean Time to Remediate	>45 days	31-45 days	15-30 days	8-14 days	0-7 days

©2026 Tanium Inc. All Rights Reserved

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
	Threat (time)					
	Historical Lookback Time	0 - 7 days	8 - 14 days	15 - 30 days	31 - 45 days	>45 days

©2026 Tanium Inc. All Rights Reserved

Threat Response requirements

Review the requirements before you install and use Threat Response.

Important: In Threat Response 4.0, the Detect and Event services have been deprecated and replaced by the Threat Response service. The integration with the Threat Response service and the Threat Response Client Extension on the endpoints provides performance improvements and provides a platform for future capability, intelligence, and workflows around intel and alerting. Threat Response 4.0 includes API changes that require customers and partners to reconfigure API integrations. The API data format may be changed for many existing routes. Most of these changes have been made for consistency in what each API returns. From the Threat Response Workbench, click **Help** > **API** > **See API documentation** to review the Threat Response 4.0 API documentation to adjust your integrations appropriately. For more information about the exact changes and required steps to ensure integrations work as intended, see Threat Response Version 4.0 API Changes.

Core platform dependencies

Make sure that your environment meets the following requirements:

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

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

  .

  Any supported version of Tanium Client. For more information, see Client version and host system requirements. If you use a Client version that is not listed, certain product features might not be available, or stability issues can occur that can only be resolved by upgrading to one of the listed Client versions.

©2026 Tanium Inc. All Rights Reserved

Computer group dependencies

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

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

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

Solution dependencies

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

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

Tanium recommended installation

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

Import specific solutions

©2026 Tanium Inc. All Rights Reserved

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

Required dependencies

About this task

Threat Response has the following required dependencies at the specified minimum versions:

- Tanium™ Client Index Extension*
- Tanium™ Client Recorder Extension*
- Tanium™ Connect
- Tanium™ Data Service (TDS)
- Tanium™ Reputation
- Tanium™ Investigate is required to add alerts to an Investigation
- Tanium™ IR Quarantine is required for isolating endpoints
- Tanium™ Direct Connect is required for live endpoint connections
- Tanium Interact
- Tanium Default Content
- Tanium Endpoint Configuration
- Tanium™ RDB Service
- Tanium Secrets

* = The required version of this client extension is installed as part of Threat Response.

Feature-specific dependencies

©2026 Tanium Inc. All Rights Reserved

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

- Tanium™ Enforce is required for alert remediation.
- Tanium Impact is required to display Impact ratings for alerts.

Client extensions and endpoint tools

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



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

Tanium™ Module Server

Threat Response is installed and runs as a service on the Module Server host computer. The impact on Module Server host computer sizing is minimal and depends on usage. For more information, see Contact Tanium Support on page 373. As a best practice, 250GB to 1TB of disk space is recommended to ensure available storage for snapshots and other saved Threat Response evidence.

Endpoints

The following endpoint operating systems are supported with Threat Response. Threat Response uses the Tanium™ Client Recorder Extension to gather data from endpoints.

Supported operating systems for Tanium Threat Response

Operating System	Version
Windows	A minimum of Windows 7 (SP1) or Windows Server 2008 R2 (with SP1) is required. Windows 8.1 provides DNS event

©2026 Tanium Inc. All Rights Reserved

Operating System	Version
	recording capability. Windows XP, Windows Server 2008, and Windows Server 2003 are not supported. Live Response is not supported on Windows 7 (SP1) and Windows Server 2008 R2 endpoints. The ability to collect forensic evidence from Windows 7 (SP1) and Windows Server 2008 R2 endpoints using Live Response will be deprecated in an upcoming version of Threat Response. Windows 7 and Windows Server 2008 R2 operating systems must have the following Microsoft KBs installed: • KB3033929 - "Availability of SHA-2 code signing support for Windows 7 and Windows Server 2008 R2." For more information regarding KB3033929, see https://support.microsoft.com/en-us/help/3033929/microsoft-security-advisory-availability-of-sha-2-code-signing-support. • KB4490628 - "Servicing stack update for Windows 7 SP1 and Windows Server 2008 R2 SP1." For more information regarding KB4490628, see https://support.microsoft.com/en-us/topic/servicing-stack-update-for-windows-7-sp1-and-windows-server-2008-r2-sp1-march-12-2019-b4dc0cff-d4f2-a408-0cb1-cb8e918feeba. • KB4474419 - "SHA-2 code signing support update for Windows Server 2008 R2, Windows 7, and Windows Server 2008." For more information regarding 4474419, see https://support.microsoft.com/en-us/topic/sha-2-code-signing-support-update-for-windows-server-2008-r2-windows-7-and-windows-server-2008-september-23-2019-84a8aad5-d8d9-2d5c-6d78-34f9aa5f8339. • KB4534310 or KB4539601 • KB4534310 - "January 14, 2020—KB4534310 (Monthly Rollup)" For more information, see https://support.microsoft.com/en-au/topic/january-14-2020-kb4534310-monthly-rollup-9ce32b1b-77ef-9a17-7ecb-2bcebcaa9ff5. • KB4539601 - "January 31, 2020—KB4539601 (Preview of Monthly Rollup)" For more information, see https://support.microsoft.com/en-gb/topic/january-31-2020-kb4539601-preview-of-monthly-rollup-1768e5a4-04bc-e964-a7a7-9509f91b0d1f. Windows 11 (Arm-based) endpoints running in emulation mode are supported. The following are areas where Windows 11 (Arm-based) running in emulation mode are not supported: • Deep Instinct alert integration. • Process Injection monitoring. • Live Response Memory collection may not be fully supported on Arm processors. Process injection monitoring is not supported on Windows 8.1 and Windows Server 2012 R2 and earlier. For Live Response, SSH destinations are not supported on Windows Server. SSH destinations are only supported on

©2026 Tanium Inc. All Rights Reserved

Operating System	Version
	Linux and macOS. The recorder forces a vacuum if the database size becomes too large to ensure that a continual vacuuming does not exist. The recorder checks to only vacuum once per day and at least one hour after system startup to make sure vacuum operations do not interfere with system boot.
macOS	Same as Tanium Client support. Live Response Memory Collection is not supported on macOS endpoints that use M-series ARM chips. The Dump System Memory module is not supported on macOS versions after Big Sur 11.X
Linux	Same as Tanium Client support with the exceptions noted below. For more information, see Tanium Client Management User Guide: Client version and host system requirements . Systemd is required for the Linux autorun sensor to collect data. 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. eBPF as an event source for the Client Recorder Extension requires specific operating systems. For more information, see Tanium Client Recorder Extension User Guide . The debugfs file system is required. By default this is mounted under sys/kernel/debug . Make sure that sys/kernel/debug is not unmounted. If you are building a custom kernel, make sure that the DEBUG_FS option is enabled. DNS event recording capability is provided on Linux endpoints where eBPF is enabled. 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. Live Response Memory Collection is not supported on Amazon Linux 2 (ARM) endpoints. Live Response is not supported on CentOS5 endpoints. For Linux endpoints:

©2026 Tanium Inc. All Rights Reserved

Operating System	Version
	• 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. • If using eBPF for event data, the entire kernel headers package and the entire kernel devel package must be enabled on RHEL and CentOS versions 7.8 to 8.1 endpoints. This is a requirement of BCC. eBPF adds a BCC library that is compiled on the endpoint. This library is recompiled every time the endpoint is restarted.

Disk space requirements

By default, the endpoint database for Threat Response is 1GB in size. On installation, 100MB is reserved on on disk, and the database increases in size to up to 1GB before event pruning occurs. 3GB is recommended. Free disk space is checked when a snapshot is requested.

If Indexing is enabled, space should also be reserved for the Index database. The size of the database depends on several factors, including the types of hashes recorded, the types and number of exclusions to indexing, and the number of files present on the volumes indexed.

For a rough estimate, the Index database uses approximately 1 GB of Index database for every 2 million items indexed. By default, Index extracts and indexes the contents of archive files. Archive files that contain a large number of files and folders can cause the Index database to consume additional space.

If you do not know the number of files, you can apply a rough estimate by using between 2-5 MB of Index database size per 1GB of used disk space. This estimate can vary across endpoints. Tanium Reveal quick search requires additional Index database space. When using Reveal Quick Search, budget approximately 20MB per 1GB.

©2026 Tanium Inc. All Rights Reserved

CPU and memory requirements

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. For more information about editing packages, see Tanium Console User Guide: Edit a Package. Alternatively, you can run the following command from the Tanium Client installation directory on endpoints to update this configuration setting:

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

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

Tanium Driver

The Tanium Driver records process and command-line events on supported Windows endpoints. The Tanium Driver is included in initial installations and any subsequent updates of Threat Response. To record event data from Windows endpoints, the Tanium Driver must be installed.

If you are deploying the Tanium Driver to endpoints for the first time, a reboot of endpoints is not required for the driver to capture events, but a reboot is required to view complete process tree data.

Host and network security requirements

Specific ports and processes are needed to run Threat Response.

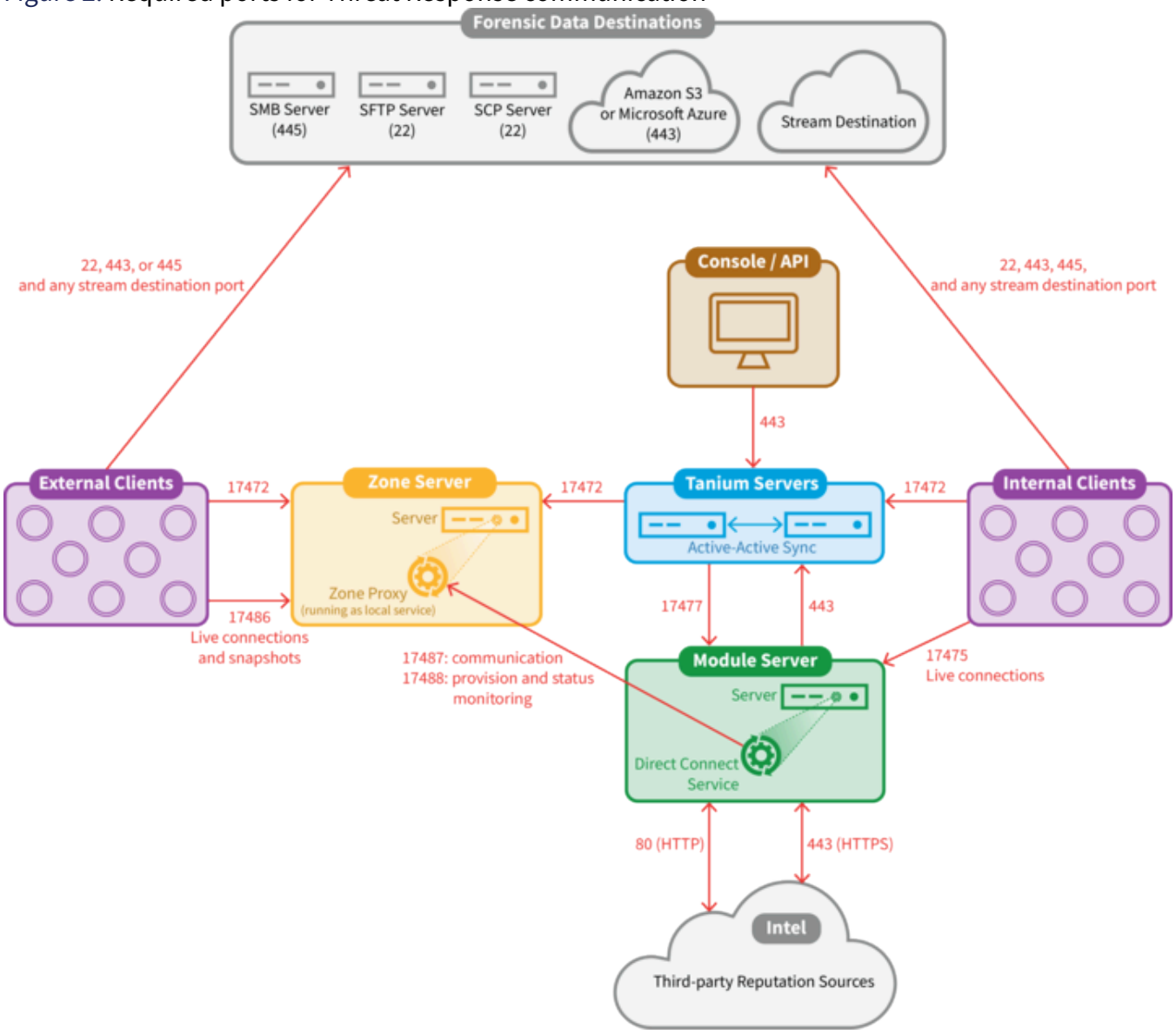
Ports

About this task

The following ports are required for Threat Response communication.

©2026 Tanium Inc. All Rights Reserved

Figure 2. Required ports for Threat Response communication



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

PORTS FOR THREAT RESPONSE COMMUNICATION

©2026 Tanium Inc. All Rights Reserved

Required ports for Tanium Threat Response communication

Source	Destination	Port	Protocol	Purpose
Module Server	Direct Connect Zone Proxy	17487 (Direct Connect communication port) and 17488 (Direct Connect provision and status monitoring port)	TCP	(Optional) Tanium Direct Connect connection to Direct Connect Zone Proxy
	Module Server (loopback)	17466	TCP	Internal purposes, not externally accessible
	Intel provider	80, 443	TCP	Integration of intel streams
Tanium Server	Module Server	17477	TCP	Tanium Server initiates connections to the Module Server on port 17477
Tanium Client	Direct Connect	17475 (Direct Connect on Module Server) 17486 (Direct Connect Zone Proxy)	TCP	Connections to the Module Server or the Direct Connect Zone Proxy for live connections
	Live Response destination	443 (S3/Azure), 22 (SFTP/SCP), or 445 (SMB)	TCP	Outbound connections over ports depending on how the collected data is being transferred
	Stream configurations to external destinations	A TCP port for an external destination that you select in a Stream configuration. For Splunk destinations this is provided by a Splunk administrator. For Sentinel destinations this is 514 by default but is configurable.	TCP	Stream events from clients to external destinations that you specify in a Stream configuration.

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

©2026 Tanium Inc. All Rights Reserved

Tanium processes to run without interference. This software can include security applications that are included with an endpoint operating system, such as fapolicyd on some Linux distributions, or Microsoft Defender on Windows. The configuration of these exclusions varies depending on the security software.

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

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

Threat Response server exclusions

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

Target Device	Notes	Exclusion Type	Exclusion
Tanium Module Server		Process	*<Module Server>* \services\threat-response-service\node.exe
		Process	*<Module Server>* \services\twsm-v1\twsm.exe
		Process	*<Module Server>* \services\endpoint-configuration-service\ TaniumEndpointConfigService.exe
Tanium Zone Server		Process	<Tanium Installation Directory>\Tanium Direct Connect Zone Proxy\node.exe
		Process	<Tanium Installation Directory>\Tanium Direct Connect Zone Proxy\twsm.exe

Threat Response endpoint exclusions

©2026 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows x86 and x64		Process	*<Tanium Client>* \Tools\IR\TaniumExecWrapper.exe
		Process	*<Tanium Client>* \Tools\IR\TaniumFileInfo.exe
		Process	*<Tanium Client>* \Tools\IR\TaniumHandle.exe
		File	*<Tanium Client>* \extensions\TaniumIndex.dll
		File	*<Tanium Client>* \extensions\TaniumIndex.dll.sig
		Process	*<Tanium Client>* \Tools\recorder\TaniumRecorderCtl.exe
		File	*<Tanium Client>* \extensions\TaniumRecorder.dll
		File	*<Tanium Client>* \extensions\TaniumRecorder.dll.sig
		File	*<Tanium Client>* \extensions\SupportCX.dll
		File	*<Tanium Client>* \extensions\SupportCX.dll.sig
		File	*<Tanium Client>* \extensions\recorder\proc.bin
		File	*<Tanium Client>* \extensions\recorder\recorder.db
		File	*<Tanium Client>* \extensions\recorder\recorder.db-shm
		File	*<Tanium Client>* \extensions\recorder\recorder.db-wal
		File	*<Tanium Client>* \extensions\index\index.db
		File	*<Tanium Client>* \extensions\index\index.db-shm
		File	*<Tanium Client>* \extensions\index\index.db-wal
		File	*<Tanium Client>* \extensions\TaniumStream.dll

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* \extensions\TaniumStream.dll.cfg
		File	*<Tanium Client>* \extensions\TaniumStream.dll.sig
		File	*<Tanium Client>* \extensions\TaniumExtras.dll
		File	*<Tanium Client>* \extensions\TaniumExtras.dll.cfg
		File	*<Tanium Client>* \extensions\TaniumExtras.dll.sig
	x86 endpoints	Process	*<Tanium Client>* \tools\driver\TaniumDriverCtl.exe
	x64 endpoints	Process	*<Tanium Client>* \tools\driver\TaniumDriverCtl64.exe
	x86 endpoints	Process	*<Tanium Client>* \tools\driver\TaniumDriverSvc.exe
	x64 endpoints	Process	*<Tanium Client>* \tools\driver\TaniumDriverSvc64.exe
		Process	*<Tanium Client>* \tools\driver\service\TaniumDriverSvc.exe
		File	*<Tanium Client>* \tools\driver\TaniumProcessMonitor.dll
		File	*<Tanium Client>* \tools\driver\TaniumProcessMonitor64.dll
		File	*<Tanium Client>* \extensions\TaniumThreatResponse.dll
		File	*<Tanium Client>* \extensions\TaniumThreatResponse.dll.sig
		File	*<Tanium Client>* \extensions\core\TaniumPythonCx.dll
		File	*<Tanium Client>* \extensions\core\TaniumPythonCx.dll.sig
		Folder	*<Tanium Client>* \extensions\stream
		File	*<Tanium Client>* \TaniumClientExtensions.dll
		File	*<Tanium Client>* \TaniumClientExtensions.dll.sig
		Process	*<Tanium Client>* \Tools\IR\TaniumPersistenceAnalyzer.exe

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* \Tools\IR\PowerForensics\PowerForensics.dll
	Where * corresponds to the action ID or the version of linpmem.	File	*<Tanium Client>* \Tools\IR\data\Action_*\PowerForensics.dll
	Where * corresponds to the action ID or the version of linpmem.	File	*<Tanium Client>* \Tools\IR\data\Action_*\PSTaniumFileTransfer_64.dll
	Where * corresponds to the action ID or the version of linpmem.	Process	*<Tanium Client>* \Tools\IR\data\Action_*\taniumfiletransfer_32.exe
	Where * corresponds to the action ID or the version of linpmem.	Process	*<Tanium Client>* \Tools\IR\data\Action_*\taniumfiletransfer_64.exe
	Where * corresponds to the action ID or the version of linpmem.	Process	*<Tanium Client>* \Tools\IR\data\Action_*\TaniumHandle_32.exe
	Where * corresponds to the action ID or the version of linpmem.	Process	*<Tanium Client>* \Tools\IR\data\Action_*\TaniumHandle_64.exe
	Where * corresponds to the action ID or the version of linpmem.	Process	*<Tanium Client>* \Tools\IR\data\Action_*\winpmem_mini_x64_rc2.exe
		File	*<Tanium Client>* \Tools\IR\PSTaniumFileTransfer.dll
		Process	*<Tanium Client>* \Tools\IR\TanFileInfo.exe
		Process	*<Tanium Client>* \Tools\IR\taniumfiletransfer.exe
		Process	*<Tanium Client>* \Tools\Copy\taniumfiletransfer.exe

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	*<Tanium Client>* \Tools\IR\py\incident_response_deps_platform\38-cp38-win32\taniumfiletransfer\taniumfiletransfer.exe
		Process	*<Tanium Client>* \Tools\IR\py\incident_response_deps_platform\312-cp312-win32\taniumfiletransfer\taniumfiletransfer.exe
		Process	*<Tanium Client>* \Tools\IR\TaniumHandle.exe
		Process	*<Tanium Client>* \Tools\IR\TaniumListModules.exe
		Process	*<Tanium Client>* \Tools\IR\TaniumPersistenceAnalyzer.exe
		File	*<Tanium Client>* \TPython\TPython.bat
		Folder	*<Tanium Client>* \TPython312
		Folder	*<Tanium Client>* \python312
		Process	*<Tanium Client>* \python312\TPython.exe
		Process	*<Tanium Client>* \TaniumCX.exe
		File	*<Tanium Client>* \extensions\TaniumDEC.dll
		File	*<Tanium Client>* \extensions\TaniumDEC.dll.sig
		File	C:\Windows\System32\drivers\TaniumRecorderDrv.sys
		File	C:\Windows\SysWOW64\TaniumProcessMonitor.dll
		File	C:\Windows\system32\drivers\TaniumProcessMonitor.dll
Linux x86 and x64		Process	*<Tanium Client>* /extensions/recorder/TaniumAuditPipe
		Process	*<Tanium Client>* /TaniumCX
		Process	*<Tanium Client>* /Tools/IR/TaniumExecWrapper
		File	*<Tanium Client>* /extensions/libTaniumIndex.so

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* /extensions/libTaniumIndex.so.sig
		Folder	*<Tanium Client>* /python312
		Process	*<Tanium Client>* /python312/python
		Process	*<Tanium Client>* /python312/bin/pybin
		Process	*<Tanium Client>* /TPython/TPython
		Folder	*<Tanium Client>* /TPython312
		File	*<Tanium Client>* /libTaniumClientExtensions.so
		File	*<Tanium Client>* /libTaniumClientExtensions.so.sig
		File	*<Tanium Client>* /extensions/libSupportCX.so
		File	*<Tanium Client>* /extensions/libSupportCX.so.sig
		File	*<Tanium Client>* /extensions/libTaniumThreatResponse.so
		File	*<Tanium Client>* /extensions/libTaniumThreatResponse.so.sig
		File	*<Tanium Client>* /extensions/libTaniumRecorder.so
		File	*<Tanium Client>* /extensions/libTaniumRecorder.so.sig
		File	*<Tanium Client>* /extensions/recorder/proc.bin
		File	*<Tanium Client>* /extensions/recorder/recorder.db
		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

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* /extensions/index/index.db-shm
		File	*<Tanium Client>* /extensions/index/index.db-wal
		File	*<Tanium Client>* /extensions/core/libTaniumPythonCx.so
		File	*<Tanium Client>* /extensions/core/libTaniumPythonCx.so.sig
		File	*<Tanium Client>* /extensions/libTaniumDEC.so
		File	*<Tanium Client>* /extensions/libTaniumDEC.so.sig
		Folder	*<Tanium Client>* /extensions/stream
		File	*<Tanium Client>* /extensions/libTaniumStream.so
		File	*<Tanium Client>* /extensions/libTaniumStream.so.cfg
		File	*<Tanium Client>* /extensions/libTaniumStream.so.sig
		File	*<Tanium Client>* /extensions/TaniumExtras.so
		File	*<Tanium Client>* /extensions/TaniumExtras.so.cfg
		File	*<Tanium Client>* /extensions/TaniumExtras.so.sig
	Where * corresponds to the action ID or the version of linpmem.	File	<Tanium Client>/Downloads/Action_*/linpmem-*.bin
	Where * corresponds to the action ID or the version of linpmem.	Process	*<Tanium Client>* /Tools/IR/taniumfiletransfer
		File	*<Tanium Client>* /Tools/IR/linpmem_3.0rc2.bin
	Where * corresponds to the action ID or the version of	File	*<Tanium Client>* /Downloads/Action_*/linpmem_3.0rc2.bin

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	linpmem.		
		Process	*<Tanium Client>* /Tools/IR/py/incident_response/_deps/_platform/38-cp38-linux_x86_64/taniumfiletransfer/taniumfiletransfer
		Process	*<Tanium Client>* /Tools/IR/py/incident_response/_deps/_platform/312-cp312-linux_x86_64/taniumfiletransfer/taniumfiletransfer
macOS		Process	*<Tanium Client>* /TaniumCX
	For macOS Universal only	Process	*<Tanium Client>* /TaniumCX.app/Contents/MacOS/TaniumCX
		Process	*<Tanium Client>* /Tools/IR/TaniumExecWrapper
		File	*<Tanium Client>* /extensions/libTaniumIndex.dylib
		File	*<Tanium Client>* /extensions/libTaniumIndex.dylib.sig
		Folder	*<Tanium Client>* /python312
		Process	*<Tanium Client>* /python312/python
		Process	*<Tanium Client>* /python312/bin/pybin
		Process	*<Tanium Client>* /TPython/TPython
		Folder	*<Tanium Client>* /TPython312
		File	*<Tanium Client>* /libTaniumClientExtensions.dylib
		File	*<Tanium Client>* /libTaniumClientExtensions.dylib.sig
		File	*<Tanium Client>* /extensions/libTaniumThreatResponse.dylib
		File	*<Tanium Client>* /extensions/libTaniumThreatResponse.dylib.sig
		File	*<Tanium Client>* /extensions/libTaniumRecorder.dylib
		File	*<Tanium Client>* /extensions/libTaniumRecorder.dylib.sig

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* /extensions/recorder/proc.bin
		File	*<Tanium Client>* /extensions/recorder/recorder.db
		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/core/libTaniumPythonCx.dylib
		File	*<Tanium Client>* /extensions/index/index.db
		File	*<Tanium Client>* /extensions/index/index.db-shm
		File	*<Tanium Client>* /extensions/index/index.db-wal
		File	*<Tanium Client>* /extensions/core/libTaniumPythonCx.dylib.sig
		Folder	*<Tanium Client>* /extensions/stream
		File	*<Tanium Client>* /extensions/libTaniumDEC.dylib
		File	*<Tanium Client>* /extensions/libTaniumDEC.dylib.sig
		File	*<Tanium Client>* /extensions/libSupportCX.dylib
		File	*<Tanium Client>* /extensions/libSupportCX.dylib.sig
		File	*<Tanium Client>* /extensions/libTaniumStream.dylib
		File	*<Tanium Client>* /extensions/libTaniumStream.dylib.cfg
		File	*<Tanium Client>* /extensions/libTaniumStream.dylib.sig
		File	*<Tanium Client>* /extensions/libTaniumExtras.dylib
		File	*<Tanium Client>* /extensions/libTaniumExtras.dylib.cfg

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* /extensions/libTaniumExtras.dylib.sig
		Process	*<Tanium Client>* /Tools/IR/taniumfiletransfer
	Where * corresponds to the action ID or the version of linpmem.	Process	*<Tanium Client>* /Tools/IR/data/Action_*/osxpmem.app
	Where * corresponds to the action ID or the version of linpmem.	File	*<Tanium Client>* /Tools/IR/data/Action_*/osxpmem.app/libs/libaff4.0.dylib
	Where * corresponds to the action ID or the version of linpmem.	File	*<Tanium Client>* /Tools/IR/data/Action_*/osxpmem.app/libs/libpcre.1.dylib
	Where * corresponds to the action ID or the version of linpmem.	File	*<Tanium Client>* /Tools/IR/data/Action_*/osxpmem.app/libs/libpcre++.0.dylib
	Where * corresponds to the action ID or the version of linpmem.	File	*<Tanium Client>* /Tools/IR/data/Action_*/osxpmem.app/libs/libraptor2.0.dylib
	Where * corresponds to the action ID or the version of linpmem.	File	*<Tanium Client>* /Tools/IR/data/Action_*/osxpmem.app/libs/libsnappy.1.dylib
	Where * corresponds to the action ID or the version of linpmem.	File	*<Tanium Client>* /Tools/IR/data/Action_*/osxpmem.app/libs/liburiparser.1.dylib
	Where * corresponds to the action ID or the version of linpmem.	File	*<Tanium Client>* /Tools/IR/data/Action_*/osxpmem.app/libs/libuuid.16.dylib
	Where * corresponds to the	File	*<Tanium Client>* /Tools/IR/data/Action_*/osxpmem.app/libs/libyaml-cpp.0.6.dylib

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	action ID or the version of linpmem.		
		Procress	*<Tanium Client>* /Tools/IR/py/incident_response/_deps/_platform/312-cp312-macosx_10_11_x86_64/taniumfiletransfer/taniumfiletransfer
		Process	*<Tanium Client>* /Tools/IR/py/incident_response/_deps/_platform/38-cp38-macosx_10_11_x86_64/taniumfiletransfer/taniumfiletransfer

User role requirements

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

- Table 10. Threat Response solution permissions on page 51
- Table 11. Threat Response administration and platform content permissions on page 60: The solution permissions automatically provide some of these permissions.

For more information and to review a summary of the predefined roles, see Set up Threat Response users on page 72.

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

©2026 Tanium Inc. All Rights Reserved

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

Threat Response solution permissions

Permission	Threat Response Administrator [1]	Threat Response Operator [1]	Threat Response User [1]	Threat Response Read Only User [1,3]	Threat Response Endpoint Configuration Approver [1]
Threat Response Access to the Threat Response workbench	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW
Threat Response Alert Deploy Allows for action deployment from a Threat Response alert	✓ ACTION	✓ ACTION	✓ ACTION	✗	✗
Threat Response Alerts Access to read and modify alerts	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Threat Response All Signals Suppression Rules Access to modify all signals suppression rules in Threat Response	✓ WRITE	✓ WRITE	✓ WRITE	✗	✗
Threat Response API Perform Threat Response operations using the API	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE
Threat Response API Doc View and list API Docs	✓ READ	✓ READ	✓ READ	✓ READ	✗
Threat Response Audit Allows viewing and exporting	✓ READ	✓ READ	✗	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Threat Response Administrator [1]	Threat Response Operator [1]	Threat Response User [1]	Threat Response Read Only User [1,3]	Threat Response Endpoint Configuration Approver [1]
Threat Response Audit data					
Threat Response Configs Access to read and create configurations	✓ READ WRITE	✓ READ WRITE	✓ READ	✗	✓ READ
Threat Response Content Provides content privileges for Threat Response users	✓ USER	✓ USER	✓ USER	✗	✗
Threat Response Content Incident Response Provides content privileges for Threat Response Incident Response users	✓ USER	✓ USER	✓ USER	✗	✗
Threat Response Content Incident Response Administrator Provides content privileges for Threat Response Incident Response administrators	✓ ADMINISTRATOR	✓ ADMINISTRATOR	✗	✗	✗
Threat Response Content Incident Response Readonly Provides content privileges for Threat Response Incident Response read only users	✓ USER	✓ USER	✓ USER	✓ USER	✗
Threat Response Content Index Provides content privileges for Threat Response Index users	✓ USER	✓ USER	✓ USER	✓ USER	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Threat Response Administrator [1]	Threat Response Operator [1]	Threat Response User [1]	Threat Response Read Only User [1,3]	Threat Response Endpoint Configuration Approver [1]
Threat Response Content Index Administrator Provides content privileges for Threat Response Index administrators	✓ ADMINISTRATOR	✓ ADMINISTRATOR	✗	✗	✗
Threat Response Content Readonly Provides content privileges for Threat Response Readonly users	✓ USER	✓ USER	✓ USER	✓ USER	✗
Threat Response Context Analyzer Provides content privileges to use Context Analyzer	✓ WRITE	✓ WRITE	✓ WRITE	✗	✗
Threat Response Data Collection Identify Allows the user to use the TDS Oracle service to get EIDs	✓ WRITE	✗	✗	✗	✗
Threat Response Direct Connect Allows bypassing Direct Connect action approvals	✓ BYPASS	✓ BYPASS	✓ BYPASS	✗	✗
Threat Response Downloads Read and manage downloaded files from live connections	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Threat Response Endpoint Configuration Enables approver privileges in Tanium Endpoint	✗	✓ DISMISS REJECT	✗	✗	✓ APPROVE

©2026 Tanium Inc. All Rights Reserved

Permission	Threat Response Administrator [1]	Threat Response Operator [1]	Threat Response User [1]	Threat Response Read Only User [1,3]	Threat Response Endpoint Configuration Approver [1]
Configuration for Threat Response configuration changes					
Threat Response Enterprise Hunting View and list sensors for enterprise hunting	✓ READ	✓ READ WRITE	✓ READ	✓ READ	✓ READ
Threat Response Exports Create, view, and delete exported events	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Threat Response Filters Access to read and create filters	✓ READ WRITE	✓ READ WRITE	✓ READ	✗	✓ READ
Threat Response Health Status Allows use of health status actions	✓ WRITE	✗	✗	✗	✗
Threat Response Intel Allows creating, viewing, and deploying Threat Response Intel	✓ DEPLOY READ WRITE	✓ DEPLOY READ WRITE	✓ READ	✓ READ	✗
Threat Response Intel Reaction Allows reading and modifying Intel reaction related	✓ WRITE	✓ WRITE	✓ WRITE	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Threat Response Administrator [1]	Threat Response Operator [1]	Threat Response User [1]	Threat Response Read Only User [1,3]	Threat Response Endpoint Configuration Approver [1]
attributes in Threat Response.					
Threat Response Intel Safeguards Allows reading and modifying Intel Safeguard related attributes in Threat Response.	✓ WRITE	✓ WRITE	✗	✗	✗
Threat Response Labels Access to read and modify intel labels	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Threat Response Live Connection Allows setting and viewing live connections to endpoints	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗
Threat Response Live Connection File Allows deletion of a file on the endpoint during a live connection	✓ DELETE	✓ DELETE	✗	✗	✗
Threat Response Live Connections Filesystem Browse the filesystem on live connections	✓ BROWSE	✓ BROWSE	✓ BROWSE	✓ BROWSE	✗
Threat Response Live Response Collection Configs Access to read and create Threat Response Live Response Collection configurations	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Threat Response Administrator [1]	Threat Response Operator [1]	Threat Response User [1]	Threat Response Read Only User [1,3]	Threat Response Endpoint Configuration Approver [1]
Threat Response Live Response Destinations Access to read and createThreat Response Live Response destinations	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗
Threat Response Live Response File Collector Sets Access to read and create Threat Response Live Response file collector set configurations	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗
Threat Response Live Response Modules Access to read Threat Response Live Response module configuration information	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗
Threat Response Live Response Packages Access to create Threat Response Live Response packages	✓ GENERATE	✓ GENERATE	✗	✗	✗
Threat Response Live Response Script Sets Access to read and create Threat Response Live Response script set configuration information	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗
Threat Response Logs Allows viewing Threat	✓	✗	✗	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Threat Response Administrator [1]	Threat Response Operator [1]	Threat Response User [1]	Threat Response Read Only User [1,3]	Threat Response Endpoint Configuration Approver [1]
Response logs	READ				
Threat Response Notification Access to read and modify notifications	✓ READ WRITE	✓ READ WRITE	✗	✗	✗
Threat Response On Demand Scans [2] Access to run and read the results of on-demand scans	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Threat Response Operator Settings Allows the operator to read and modify available settings	✓ READ WRITE	✓ READ WRITE	✗	✗	✗
Threat Response Operator Status Allows the operator to view the module status	✓ READ	✗	✓ READ	✓ READ	✗
Threat Response Override Scan Allows for overriding scan blockout windows on endpoints.	✓ BLOCKOUTS	✓ BLOCKOUTS	✗	✗	✗
Threat Response Profiles Access to read, create, and deploy profiles	✓ READ WRITE DEPLOY	✓ READ WRITE DEPLOY	✓ READ	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Threat Response Administrator [1]	Threat Response Operator [1]	Threat Response User [1]	Threat Response Read Only User [1,3]	Threat Response Endpoint Configuration Approver [1]
Threat Response Quarantine Packages Allows for the generation of Threat Response Quarantine Packages	✓ GENERATE	✓ GENERATE	✓ READ	✗	✗
Threat Response Quarantine Profile Allows users to read and write quaranting profiles and rules	✓ READ WRITE	✓ READ WRITE	✗	✗	✗
Threat Response Reputation Allows operations against Reputation	✓ READ INTEGRATIONS	✓ READ INTEGRATIONS	✓ READ	✓ READ	✗
Threat Response Response Actions Enables users to view, create, and stop response actions	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Threat Response Saved Evidence View and save events from live endpoint connections	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✗	✗
Threat Response Settings Allows viewing and editing Threat Response settings	✓ READ WRITE	✗	✓ READ	✓ READ	✗
Threat Response Snapshot Capture,view, and delete snapshots	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Threat Response Administrator [1]	Threat Response Operator [1]	Threat Response User [1]	Threat Response Read Only User [1,3]	Threat Response Endpoint Configuration Approver [1]
Threat Response Sources [2] Access to read and modify sources	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Threat Response Stats Allows viewing Threat Response stats	✓ READ	✓ READ	✓ READ	✓ READ	✗
Threat Response Status Allows the operator to view status information	✓ READ	✓ READ	✓ READ	✓ READ	✗
Threat Response Suppression Rules Create, edit, view, list, and delete suppression rules	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Threat Response Tasks Access to read Threat Response tasks	✓ READ	✓ READ	✗	✗	✗
Threat Response Threat Navigator Enables users to create, edit, and read threat navigator searches	✓ READ WRITE BYPASS	✓ READ WRITE BYPASS	✗	✗	✗
Threat Response Trends Board Allows the user to view Trends data	✓ READ	✓ WRITE	✗	✗	✗
Threat Response Visibility	✓	✓	✗	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Threat Response Administrator [1]	Threat Response Operator [1]	Threat Response User [1]	Threat Response Read Only User [1,3]	Threat Response Endpoint Configuration Approver [1]
Bypass Enables users to view all alerts and saved evidence regardless of computer group membership	READ	READ			

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

[2] Requires permissions for other modules or solutions to complete all tasks in other modules and see all content; such as Protect (version 1.3.0 or later), Connect (version 4.3.0 or later), or Interact. You can assign a role for another product, or create a custom role that lists just the specific privileges needed.

[3] The Threat Response Read Only User role does not have the ability to create live endpoint direct connections. The Threat Response User role is required as a minimum for creating live endpoint connections.

Threat Response administration and platform content permissions

Permission	Permission Type	Threat Response Administrator [1]	Threat Response Operator	Threat Response User	Threat Response Read Only User	Threat Response Endpoint Configuration Approver
Action Group	Administration	✓ READ	✓ READ	✓ READ	✗	✗
Computer Group	Administration	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ
User	Administration	✓ READ	✗	✗	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Permission Type	Threat Response Administrator [1]	Threat Response Operator	Threat Response User	Threat Response Read Only User	Threat Response Endpoint Configuration Approver
Allowed URLs	Administration	✗	✗	✗	✗	✗
Action	Platform Content	✓ READ WRITE	✓ READ WRITE	✓ WRITE	✗	✗
Dashboard	Platform Content	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗
Dashboard Group	Platform Content	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗
Filter Group	Platform Content	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ
Own Action	Platform Content	✓ READ	✓ READ	✓ READ	✗	✗
Package	Platform Content	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗
Plugin	Platform Content	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE

©2026 Tanium Inc. All Rights Reserved

Permission	Permission Type	Threat Response Administrator [1]	Threat Response Operator	Threat Response User	Threat Response Read Only User	Threat Response Endpoint Configuration Approver
Saved Question	Platform Content	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗
Sensor	Platform Content	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗

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

©2026 Tanium Inc. All Rights Reserved

Installing Threat Response

About this task

Use the **Solutions** page to install Threat Response and choose between automatic and manual configuration:

- **Automatic configuration with default settings**: Threat Response is installed with any required dependencies and other selected products. After installation, the Tanium Server automatically configures the recommended default settings. This option is the best practice for most deployments. For more information about the automatic configuration for Threat Response, see Import Threat Response with default settings on page 64.
- **Manual configuration with custom settings**: After installing Threat Response, you must manually configure required settings. Select this option only if Threat Response requires settings that differ from the recommended default settings. For more information, see Import Threat Response with custom settings on page 65.

Before you begin

- Read the Release Notes.
- Review the Threat Response requirements on page 30.
- If you are upgrading from a previous version, see Upgrade the Threat Response version on page 66.
- If the Tanium Server uses a self-signed certificate, you must add localhost to the TrustedHostList.
- Assign the correct roles to users for Threat Response. Review the User role requirements on page 50.
    - To import the Threat Response solution, you must be assigned the Administrator reserved role.
    - To configure the Threat Response action group, you must be assigned the

©2026 Tanium Inc. All Rights Reserved

Administrator reserved role, Content Administrator reserved role, or a role that has the **Action Group** write permission.

Import Threat Response with default settings

Default settings for Threat Response

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

Default settings for Tanium Threat Response

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

Tanium Signals are imported.

Tanium Managed profiles are provided that contain updated configurations. These profiles are the result of Tanium data and experience and have been designed to use settings that are considered safer and to provide more real-time visibility with Index and Recorder data. You cannot delete Tanium Managed profiles.

Threat Response import notes

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

To import Threat Response and configure default settings, be sure to select the **Apply Tanium recommended configurations** checkbox while performing the steps in Tanium Console User Guide: Manage Tanium modules . After the import, verify that the correct version is installed: see Verify

©2026 Tanium Inc. All Rights Reserved

Threat Response version on page 66.

Import Threat Response with custom settings

About this task

To import Threat Response without automatically configuring default settings, be sure to clear the **Apply All Tanium recommended configurations** checkbox while performing the steps in Tanium Console User Guide: Import or update specific solutions. After the import, verify that the correct version is installed: see Verify Threat Response version on page 66.

To configure the Threat Response action group, see Configure the Threat Response action group on page 70.

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.

Manage solution dependencies

About this task

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

Perform the following steps if a banner indicates any Threat Response dependencies are not installed:

1. Install the dependencies as described in Tanium Console User Guide: Import or update specific solutions.

©2026 Tanium Inc. All Rights Reserved

2. From the Main menu, go to **Modules** > **Threat Response** to open the **Overview** page. to open the Threat Response **Overview** page and verify that Console no longer displays a banner to list missing dependencies.

Upgrade the Threat Response version

Upgrade Threat Response to the latest version by importing an update to the solution and migrating any existing intel.

Before you upgrade, use Tanium Health Check to generate a report that you can use to resolve any issues or risks associated with the Tanium environment. Fix any issues reported by Tanium Health Check to mitigate problems that you encounter during an upgrade. You can also use this report to discover opportunities for improving the performance of the Tanium environment. For more information, see Tanium Health Check User Guide: Health Check overview.

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

If Tanium Reveal and Tanium Threat Response exist in the same environment, both solutions must be on a version that is running the same architecture of Tanium Index. Threat Response 3.4 and later must be installed in the same environment as Reveal 1.15 and later. Threat Response versions earlier than Threat Response 3.4 can be installed in the same environment as Reveal 1.14 and earlier.

When upgrading Threat Response, you can select to automatically upgrade the Threat Response tools package on all of the endpoints in an environment to ensure that the latest version of the Threat Response tools are distributed.

Important: When Endpoint Change Management (ECM) is enabled, endpoint tools get upgraded according to upgrade workflows defined in Endpoint Change Management. When ECM is enabled, the option to control Threat Response tools deployment automatically or through Threat Response profile deployment is not available. Endpoint Change Management is enabled by default in Tanium Cloud and beginning with the 2024H1 Semi-Annual Release.

Verify Threat Response version

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

©2026 Tanium Inc. All Rights Reserved

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

©2026 Tanium Inc. All Rights Reserved

Configuring Threat Response

About this task

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

Install and configure Tanium Endpoint Configuration

Manage solution configurations with Tanium Endpoint Configuration

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

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

©2026 Tanium Inc. All Rights Reserved

Important:

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

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

Note: For information about how to install Endpoint Configuration, see Installing Endpoint Configuration.

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

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

©2026 Tanium Inc. All Rights Reserved

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

Threat Response Endpoint Configuration approvals

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

- Associating a response action with an alert
- Deleting profiles
- Deploying profiles
- Gathering snapshots
- Initiating on-demand scans

Important: When Endpoint Change Management (ECM) is enabled, endpoint tools get upgraded according to upgrade workflows defined in Endpoint Change Management. When ECM is enabled, the option to control Threat Response tools deployment automatically or through Threat Response profile deployment is not available. Endpoint Change Management is enabled by default in Tanium Cloud and beginning with the 2024H1 Semi-Annual Release.

Configure Threat Response

Configure the Threat Response action group

About this task

Importing the Threat Response 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 Threat Response, the action group targets **No Computers**.

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

Select the computer groups to include in the Threat Response action group.

©2026 Tanium Inc. All Rights Reserved

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

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

Result

When you have the **Threat Response Reputation Integrations** permission, you can auto-create Saved Questions and Connections for Tanium Reputation.

1. From the Threat Response overview page, click Settings.
2. Click **Service** > **Reputation**.
3. Click **Configure Reputation** to generate the saved questions and connections that are required to provide reputation intel to Threat Response.

When you click **Configure Reputation**, the following saved questions are generated:

- Reputation - Driver Details (SHA 256) [Tanium Default]
- Reputation - MS EXE Recently Changed [Tanium Default]
- Reputation - Windows AutoRuns (SHA 256) [Tanium Default]
- Reputation - Running Processes with Hash (SHA256) [Tanium Default]
- Reputation - Mac Autoruns (MD5) [Tanium Default]
- Reputation - Linux Autoruns (MD5) [Tanium Default]
- Reputation - Trace Executed Process Hashes (MD5) [Tanium Default]
- Reputation - Service Module Details (SHA256) [Tanium Default]
- Reputation - Loaded Modules (SHA256) [Tanium Default]

©2026 Tanium Inc. All Rights Reserved

- Reputation - Recently Changed MACHO 32 Bit [Tanium Default]
- Reputation - Recently Changed MACHO 64 Bit [Tanium Default]
- Reputation - Recently Changed ELF [Tanium Default]

When you click **Configure Reputation**, the following Tanium Connect connections are generated to provide reputation intel to Threat Response:

- Reputation - Recently Changed MACHO 64 Bit [Tanium Default]
- Reputation - Recently Changed ELF [Tanium Default]
- Reputation - Recently Changed MACHO 32 Bit [Tanium Default]
- Reputation - Trace Executed Process Hashes (MD5) [Tanium Default]
- Reputation - Loaded Modules (SHA256) [Tanium Default]
- Reputation - Service Module Details (SHA256) [Tanium Default]
- Reputation - Linux Autoruns (MD5) [Tanium Default]
- Reputation - Mac Autoruns (MD5) [Tanium Default]
- Reputation - Running Processes with Hash (SHA256) [Tanium Default]
- Reputation - MS EXE Recently Changed [Tanium Default]
- Reputation - Windows AutoRuns (SHA 256) [Tanium Default]
- Reputation - Driver Details (SHA 256) [Tanium Default]

Clicking **Configure Reputation** does not recreate any existing connections or saved questions. If any connections or saved questions do not exist in the environment, they are created. Saved questions are recreated when the Threat Response service is restarted.

Set up Threat Response users

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

To review specific permissions for each role, see User role requirements on page 50.

©2026 Tanium Inc. All Rights Reserved

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

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

Tip: To provide just-in-time access or scalable standing access to Threat Response functionality, you can use SCIM provisioning combined with Tanium user groups. This approach lets you manage user access at scale or ad hoc through your identity provider, without creating users individually in Tanium. For more information, see Provision users into Tanium user groups with SCIM.

Threat Response Administrator

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

- Configure Threat Response service settings
- Read and modify Threat Response configurations
- Take action on alerts
- Connect to remote endpoints
- Dismiss or reject approvals for Threat Response tasks in Tanium Endpoint Configuration

Threat Response Operator

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

- Configure Threat Response service settings
- Read and modify Threat Response configurations
- Take action on alerts

©2026 Tanium Inc. All Rights Reserved

- Connect to remote endpoints
- Dismiss or reject approvals for Threat Response tasks in Tanium Endpoint Configuration

Threat Response User

Assign the **Threat Response User** role to users who work with alerts and performing analysis on remote endpoints. This role can perform the following tasks:

- View service settings
- View and modify alerts and intel documents
- Suppress and take action on alerts
- Run and review on-demand scans
- Connect to remote endpoints and manage downloads from them, and read configurations and profiles

Threat Response Read Only User

Assign the **Threat Response Read Only User** role to users who need visibility into Threat Response data and Threat Response findings on endpoints. This role can perform the following tasks:

- View service settings, alerts, and intel documents
- Review on-demand scans
- Read connections to remote endpoints
- Read configurations and profiles

Threat Response Endpoint Configuration Approver

Assign the **Threat Response Endpoint Configuration Approver** role to a user who approves or rejects Threat Response configuration items in Tanium Endpoint Configuration. This role approves, rejects, or dismisses changes that target endpoints where Threat Response is installed.

©2026 Tanium Inc. All Rights Reserved

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

Select a language

Select one of the supported languages for the Threat Response workbench and Threat Response user guide, as described in Tanium Console User Guide: Reference: Language support.

©2026 Tanium Inc. All Rights Reserved

Getting started with Tanium™ Threat Response

About this task

Threat Response provides common configuration workflows to expedite the time to value and to simplify the initial configuration experience. Configuration workflows that target specific end-to-end scenarios ease the implementation of Threat Response without the need for comprehensive knowledge of the full functionality of the module. Initial configuration is not intended to replace existing workflows, but instead provide a path for configuring the operation of Threat Response as quickly as possible without having extensive Tanium experience or subject matter expert guidance. Configuration workflows also provide a sample of the functionality of Threat Response and the different types of scenarios that are possible.

The following read permissions are required to view the configuration workflows on the Threat Response overview page:

- Threat Response Profiles
- Threat Response Configs
- Threat Response Live Response Destinations
- Threat Response Quarantine Profile
- Threat Response Labels
- Threat Response Sources
- Threat Response Intel

These permissions are granted to Threat Response Administrators by default.

©2026 Tanium Inc. All Rights Reserved

Note: Configuration workflows only appear to new users of Threat Response. If you are an existing user, Click **Customize Page** at the top of the Overview page of the Threat Response workbench, select **Configuration**, and click **Save** to view the configuration workflows.

Threat Response provides configuration workflows for the following functional areas:

- Evidence and telemetry on page 77
- Alerting and detection on page 80
- Endpoint isolation on page 82
- Incident response automation on page 83
- SIEM integration on page 84

On the overview page, click **Next** to navigate through the provided workflows. After you navigate to any specific workflow, the navigation item becomes a link that you can use to go to the workflow directly. Click **Previous** to move to the previous workflow.

Evidence and telemetry

About this task

The evidence and telemetry section contains workflows for the configuration of Threat Response profiles and Live Response.

Profiles

Profiles are a collection of intel documents and settings that are distributed to endpoints. Threat Response uses a cascading model when deploying profiles to endpoints. For example, the profile with the highest priority targets endpoints with low resources, followed by more distinct categories of Windows domain controllers, servers, and workstations to ensure both broad coverage and optimal performance. The displayed profiles are Tanium Managed profiles. For more information about Tanium Managed profiles, see Tanium Managed profiles on page 183.

Live Response

Live Response enables you to collect specific information from endpoints to use for forensic analysis, data correlation, and to investigate potentially compromised systems with a

©2026 Tanium Inc. All Rights Reserved

customizable and extensible framework. You can specify a network location to transfer data that you collect.

Profiles

> **Note:** Initial configuration is not intended to replace existing workflows. For more information about profile configuration, see Creating profiles in Threat Response on page 182. The displayed profiles are Tanium Managed profiles. For more information about Tanium Managed profiles, see Tanium Managed profiles on page 183.

1. From the Main menu, go to **Modules** > **Threat Response** > **Evidence and Telemetry** > **Profiles**.
2. Select **Enable** or **Disable** for any displayed profile.

   > **Note:** When you disable a profile, the profile's computer group targeting is preserved but the profile is not deployed to those endpoints. Endpoints previously targeted by the disabled profile move to their next applicable enabled profile based on priority. Any configurations deployed by the profile before it was disabled are removed if no other profile is applicable.

3. If you disable a currently enabled profile, click **Save and Deploy** to apply the change to endpoints.
4. Click **Edit** to make changes to a profile.
5. In the Index Configuration section, you can select the hashes that you want to calculate for each file in disk to allow you to quickly search across all file systems, the frequency to receive updates for files in certain regions of the disk, the frequency to scan the entire disk on an endpoint, and the delay time after Index starts before starting the initial index scan.

   ### High Priority Path

   Use high priority path scanning to receive more frequent updates for files in certain regions of the disk. In addition to the baseline disk scan, you can specify high priority paths that use recorder events to update data. High Priority Paths are indexed more frequently. Performance impacts on the endpoint increase with the frequency of

©2026 Tanium Inc. All Rights Reserved

indexing and the size of the path. Using the root directory as a High Priority Path is discouraged as this can quickly consume resources.

Scan Frequency

Threat Response uses Tanium Index to scan the entire disk on an endpoint at regular intervals that typically occur between once a day and once a week. Index does not use recorder events to update file data across the entire disk. Enter a value for how often the Index scan runs.

Scan Distribution

The delay time after Index starts before starting the initial index scan. This time is randomized over a 24 hour period.

For more information about Index configurations, see Create index configurations on page 146.

6. In the Recorder Configuration section, you can add and remove the historical events Threat Response stores locally on the endpoint for triage and investigation. An exhaustive reference for event types is available in the Threat Response Intel Support documentation. To access the Threat Response Intel Support documentation, click the help icon from the Threat Response overview page and click the **Recorder Security Event Details** tab. For more information about recorder configurations and events, see Create recorder configurations on page 149.

7. In the Recorder Configuration section, you can view the number of active filters that are associated with the configuration. Click the number of filters to view all the existing filters to see which individual filters are applied. For more information about filters, see Create filters on page 164.

Live Response

About this task

Note: Initial configuration is not intended to replace existing workflows. For more information about Live Response, see Collecting data from endpoints with Live Response on page 292.

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Threat Response** > **Evidence and Telemetry** > **Live Response**.
2. In the Destinations row, click **Create** to create a destination. For more information about destinations and a procedure for creating a destination, see Destinations on page 292.

   Note: You must create an external destination to use Live Response.
3. In the Collections row, click **Create** to create a collection. Collections are pre-defined common triage artifact captures. For more information about collections and a procedure for creating a collection, see Collections on page 299.
4. In the File Collector Sets row, click **Create** to create a file collector set. File Collector Sets enable you to use Live Response to capture any arbitrary file for your review. For more information about File Collector Sets and a procedure for creating a File Collector Sets, see File Collector sets on page 302.
5. In the Script Sets row, click **Create** to create a Script Set. Script Sets enable you to use PowerShell and Python scripts to programmatically collect triage evidence. For more information about Script Sets and a procedure for creating a Script Set, see Script sets on page 312.

Alerting and detection

The alerting and detection section contains workflows for configuring intel documents and subscriptions to third-party threat intelligence data, and Tanium Signal Intel documents. Extended detections include intel documents for Deep Instinct, Microsoft Defender, Process Injection, and Reputation.

Extended detections

About this task

Note: Initial configuration is not intended to replace existing workflows. For more information about Intel, see Adding intel on page 87.

1. From the Main menu, go to **Modules** > **Threat Response** > **Alerting and Detection** >

©2026 Tanium Inc. All Rights Reserved

Detections.

2. (Optional) For **Tanium Signals**, select to distribute the **Initial Set** or **All Signals**. The **Initial Set** of signals is a set of Tanium Signals that are curated and tested to ensure fewer false positive alerts. Tanium Signals in the **Initial Set** are assigned to the detection configuration in the profile that Threat Response deploys to endpoints and these signals have the **Tanium Initial Intel** label applied. Select **All Signals** to assign all Tanium Signals to the detection configuration in the profile that Threat Response deploys to endpoints. The **All Signals** option provides a more exhaustive set of alerts at the expense of more attentive analysis of the alerts that are generated. For more information about Tanium Signals, see Signals on page 87.

3. (Optional) For **Process Injection**, select **Enable** or **Disable**. Enable Process Injection to deploy the Process Injection intel document to endpoints that are targeted by the Threat Response profile. The Process Injection intel document provides a way to alert on incidents that involve techniques such as process injection and credential dumping. If you select **Disable**, you can save and optionally deploy the changes to the profile to endpoints. Click Edit to select the profiles to which you want to apply Process Injection. For more information about Process Injection, see Configure process injection on page 100.

4. (Optional) For **Reputation**, select **Enable** or **Disable**. Enable Reputation data to gain insight into which alerts might be good candidates to save for further analysis and action. If you select **Disable**, you can save and optionally deploy the changes to the profile to endpoints. Click Edit to select the profiles to which you want to apply Reputation. For more information about Reputation, see Reputation data on page 103. Reputation requires either a configuration with a reputation provider, or that malicious and non-malicious hashes be added to Reputation manually.

5. (Optional) For **Defender**, select **Enable** or **Disable**. Enable Microsoft Defender to gain visibility into common areas of Windows for changes which might have been caused by spyware, malware, and general security events. If you select **Disable**, you can save and optionally deploy the changes to the profile to endpoints. Click Edit to select the profiles to which you want to apply Defender. For more information about Defender, see Microsoft Defender alerts on page 266. Defender requires Defender AV to be installed and running on the endpoint.

6. (Optional) For **Deep Instinct**, select **Enable** or **Disable**. Enable Deep Instinct to apply deep learning and adds next-generation AV capabilities to Threat Response by integrating the investigative abilities of Threat Response to Deep Instinct alerts. If you select **Disable**, you can save and optionally deploy the changes to the profile to endpoints. Click Edit to select

©2026 Tanium Inc. All Rights Reserved

the profiles to which you want to apply Deep Instinct. For more information about Deep Instinct, see Deep Instinct alerts on page 267. Deep Instinct must be installed and running on the endpoint.

3rd party intel feeds

1. From the Main menu, go to **Modules** > **Threat Response** > **Alerting and Detection** > **3rd Party Intel Feeds**.
2. Click **Create**. An intel source is a series of intel documents from an external source. Sources can be a vendor or a folder in your network. You can import sources manually or based on subscription settings.
3. Subscribe to 3rd party intel feeds. For more information about subscribing to 3rd party intel feeds, see Adding intel on page 87.
4. If you create one or more 3rd party intel feed subscriptions, you can click **View** to review the details of the subscriptions.

Endpoint isolation

The endpoint isolation section contains workflows for configuring the quarantine of a Windows, Linux, or Mac endpoint that shows evidence of compromise or other suspicious activity. When an endpoint is quarantined, traffic that is allowed on the quarantined endpoint is between Tanium Client on the quarantined endpoint and Tanium Server over port 17472. Additionally, you can Direct Connect to the endpoint and use Live Response destinations.

Note: Initial configuration is not intended to replace existing workflows. For more information about Quaratine, see Quarantining endpoints on page 317.

Tanium default quarantine profile

1. From the Main menu, go to **Modules** > **Threat Response** > **Endpoint Isolation** > **Tanium Default Quarantine Profile**.
2. Click edit to edit specific values in the Default Quarantine Profile.

©2026 Tanium Inc. All Rights Reserved

3. Specify the allowances that you want to enable. The allowances that you select enable various types of traffic. You can select:

    a. **All DHCP** - Allows DHCP traffic to any destination.

    b. **DNS** - Allows DNS traffic to any destination when you select All. Allows DNS traffic only to the DNS servers currently configured on the endpoint being quarantined when you select **Current Only**.

    c. **Direct Connect** - Allows Direct Connect to access quarantined endpoints.

    d. **Live Response** - Allows Live Response to collect data from quarantined endpoints.

4. Click **Save and Deploy** to make any changes to the Tanium Default Quarantine Profile. For more information about the Tanium Default Quarantine Profile, see Quarantining endpoints on page 317.

Create quarantine profile

1. From the Main menu, go to **Modules** > **Threat Response** > **Endpoint Isolation** > **Create Quarantine Profile**.
2. Click **Create**. For a detailed overview of profile creation, see Quarantining endpoints on page 317.

Incident response automation

The incident response automation section contains workflows for managing and creating automated responses to alerts that result from an intel match. You can manage automated reactions to delete files, kill responsible processes, and quarantine endpoints. Additionally, you can create playbooks for Tanium Automate.



Note: Initial configuration is not intended to replace existing workflows. For more information about reactions, see Creating reactions on page 130.

Tanium default alert reactions

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Threat Response** > **Incident Response Automation** > **Tanium Default Alert Reactions**.

2. View the default reactions. Reactions automate one or more actions on an endpoint based on alerts from intel documents. For example, delete one or more files, kill a process, or quarantine an endpoint.

3. View the intel documents that are associated with each reaction. The associated intel documents are the documents that initiate the reaction if the intel definitions they contain are matched on an endpoint.

4. (Optional) Click **View** to view the reactions page in the Threat Response workbench to view all reactions.

Endpoint reactions

1. From the Main menu, go to **Modules** > **Threat Response** > **Incident Response Automation** > **Endpoint Reactions**.

2. Click **Create**.

3. The reactions page in the Threat Response workbench appears. For more information about creating reactions, see Creating reactions on page 130. After creating a new reaction, you must associate that reaction with an Intel Document.

Automate playbooks

1. From the Main menu, go to **Modules** > **Threat Response** > **Incident Response Automation** > **Automate Playbooks**.

2. Click **Create**.

3. The create playbook page in the Automate workbench appears. For more information about creating playbooks, see Tanium Automate User Guide: Building playbooks.

SIEM integration

The SIEM (Security Information and Event Management) integration section contains workflows for adding stream configurations to profiles that you can use to stream recorder data to external sources

©2026 Tanium Inc. All Rights Reserved

that includes process, network, file, driver events. You can use stream data to investigate incidents, enrich other workflows, or perform custom analytics. Stream configurations enable you to specify and filter recorder events for the endpoints in an environment, and provide instructions for exporting or streaming these events directly to an SIEM for analysis in JSON format. Additionally, you can create workflows to send alert and audit data to a SIEM using Tanium Connect.

Note: Initial configuration is not intended to replace existing workflows. For more information about stream configurations, see Create stream configurations on page 154. For more information about setting up alert forwarding in Tanium Connect, see Set up Tanium Connect forwarding on page 283. For more information about sending audit logs to a SIEM, see Tanium Connect User Guide: Managing connections.

Send stream data to SIEM

1. From the Main menu, go to **Modules** > **Threat Response** > **SIEM Integration**.
2. (Optional) Click **Create**. For more information about creating Stream configurations, see Create stream configurations on page 154.
3. Once you have created one or more stream destinations, for each profile, select a Stream configuration to apply to the profile. The available configurations that you can add are listed in the dropdown list. To create a new Stream configuration, click **Create**. If you do not include a Stream configuration, no data is streamed to a destination outside of Tanium.

Send alerts to SIEM

1. From the Main menu, go to **Modules** > **Threat Response** > **SIEM Integration** > **Send Audit Logs and Alerts to SIEM**.
2. Click **Create**. For more information about setting up alert forwarding in Tanium Connect, see Set up Tanium Connect forwarding on page 283.

Send Audit Logs to SIEM

1. From the Main menu, go to **Modules** > **Threat Response** > **SIEM Integration** > **Send Audit Logs and Alerts to SIEM**.
2. Click **Create**. For more information about sending audit logs to a SIEM, see Tanium Connect

©2026 Tanium Inc. All Rights Reserved

User Guide: Managing connections.

©2026 Tanium Inc. All Rights Reserved

Adding intel

Intel defines one or more conditions that might indicate malicious behavior on endpoints. Threat Response can leverage multiple sources of intel to identify and alert on potential threats in an environment. In addition to supporting third-party intelligence sources, Tanium provides threat intelligence called signals. Intel documents and signals, generally referred to as intel, interact with Threat Response to provide comprehensive monitoring and alerting.

Some intel document types, such as OpenIOC, STIX, CybOX, and YARA, search against existing or historical artifacts on the endpoint. There are a number of providers for these documents. You can upload them directly or configure source streams.

Supported intel document formats and versions

Format	Supported version(s)	Notes
CybOX	2.1	
OpenIOC	1.0, 1.1	
STIX	1.2	
YARA	4.5	Default modules: pe, elf, dotnet, hash, cuckoo, math, macho, dex, string, time

Note: STIX 2.0 requires TAXII 2.0, which is not currently supported.

Best Practice: Always use mutual (two-way) authentication and TLS encryption when connecting to intel feeds. Two-way authentication and data encryption provide additional privacy-related benefits, for example, ensuring that encryption keys that become compromised cannot decrypt TLS communications that were recorded in the past.

Signals

©2026 Tanium Inc. All Rights Reserved

Signals provide real-time monitoring of endpoint telemetry events; for example, process, network, registry, and file events for malicious behaviors and methodologies of attack. Unlike other static forms of intel which focus on specific indicators, signals are evergreen heuristics; they are perpetually relevant.

Signals interact with the engine differently; they can evaluate continuously with the recorder and match on live process events on endpoints. Signals help to identify malicious activity by correlating events and searching for behavior-based indicators that something is awry. You can use signals as a source directly from Tanium, or you can write your own signals. See Reference: Authoring Signals on page 403 for more information.

Important: Adding signals to an intel configuration enables the recorder process on endpoints, and loads the Tanium audit rules. This happens even if you do not enable a recorder configuration.

When a signal evaluates with the recorder database and an event matches, the resulting alert shows the context of the match. If you have filters for specific events in a recorder configuration, signals that match the events can still generate alerts. For a signal to evaluate with the recorder database, you need to enable both intel and recorder configurations in an active profile.

The events of a signal match are always written to the database, and override any filters that are included in a recorder configuration.

An exhaustive reference to signals syntax - including supported objects, properties, and conditions - is available in the Threat Response Intel Support documentation. To access the Threat Response Intel Support documentation, click ? from the Threat Response overview page and click the Threat Response Intel Support tab.

Signals do not always evaluate with the recorder database

There are times when signals cannot be evaluated with the recorder database. For example, it is possible for the recorder to generate signals, but not record them in the recorder database. Additionally, there are cases where events have been recorded, but one or more of the events in the signal match occurred too far in the past that the event has been purged from the recorder database.

Signals best practices

©2026 Tanium Inc. All Rights Reserved

Important: Signals should have a narrow scope, specific targets, and a clear intended use. The goal of an alert from a signal is for it to be actionable. They are not designed for broad data collection or hunting. Consider using recorder questions for data gathering and hunting activities.

- Test any update prior to full deployment. Test intel in a lab or test environment and deploy intel in a ring-based deployment to a production environment. For more information, see Testing intel for deployment.
- When testing signals, pay close attention to the false positive rate. For more information, see Filter false positives and Distinguish between malicious and false positive alerts.
- When you test for True and False positive rate, it is important to test on as many system types and workloads as possible. If workload is not tested against, it can generate unexpected false positives. Production workloads often differ significantly from test workloads, thus production is critical. As a best practice, test intel in a lab or test environment and deploy intel in a ring-based deployment before deploying to a production environment.
- There are multiple methods of getting random computer groups. Use the computer ID to generate a random sample instead of using the Online Random Sample sensor, as systems come in and out of groups on every evaluation.
- Throttle configuration is enabled by default and prevents an overabundance of alerts in production installations. Enable it for all production deployments and keep it enabled, regardless of the testing process.
- When using any intelligence feed (including Tanium Signals), do not directly deploy new intelligence to the production environment. Send new intelligence through the testing processes you have defined and that are outlined in the first item in this list. In the case of Tanium Signals, use a custom label to include signals in the production deployment configurations.
- Intel is not a one-time effort. Regardless of the testing process, a large accumulation of intel causes performance impact on endpoints. After rolling out intel, continue to monitor for performance changes, and opportunities to tailor definitions for your environment, as all environments are different and constantly changing.
- Use suppression rules to reduce false positives for process events if they are not causing throttling or high numbers of alerts. If events are throttled or non-process events are needed, modify the signal.

©2026 Tanium Inc. All Rights Reserved

- It is not possible to directly modify signals provided from the Tanium Signal Feed. You can add suppression rules, but if you need to modify the signal, make a copy and modify the copy.
- The intel document development workflow requires suppression rules, but suppression rules cannot compensate for truly poor intel. For example, do not create intel documents that alert on all instances of PowerShell and use suppression rules to allow for exceptions. Focus the signal on the positive alerting criteria.

Intel safeguards

Poorly tested or low-fidelity intel can cause a rapid influx of false-positive alerts that can be time consuming to review. By evaluating the fidelity of intel documents and disabling intel documents that generate high volumes of alerts, Threat Response can provide safeguards which help reduce false positive matches that overwhelm analysts. Intel safeguards provide the option to set thresholds across the environment for intel and to suppress intel that generates amounts of alerts that exceed the thresholds.

There are two types of thresholds that you can set; a per-endpoint alert rate before Threat Response disables the intel that initiated the alert, and a maximum percentage of disabled endpoints before Threat Response disables the intel document that initiated the alert.

Intel Safeguards is designed to only occur on Intel that is already being throttled. It only shuts down intel that is repeatedly and continuously throttled. Adjusting throttle settings impacts Intel safeguard settings.

In the Intel page of the Threat Response workbench, you can filter for intel documents that have the following states of intel safeguards:

Enabled

This designation is assigned to any intel documents that are not assigned another state.

Reduced

This designation is assigned to intel documents that any single endpoint has disabled. The result of an intel document being assigned this designation is that it no longer provides the complete visibility expected from a high-fidelity intel document. A system notification appears in the audit browser to show which endpoints are in a reduced state.

©2026 Tanium Inc. All Rights Reserved

Disabled

This designation is assigned to intel documents that are disabled enterprise-wide. Such intel documents have initiated alerts that have throttled over 250 times. 250 is a default value that you can configure to a more appropriate value for an environment. Intel documents with this designation require tuning and reevaluation to be effective.

Pending

This designation is for new or recently modified intel documents that have not been deployed and consequently have no basis for any other designation. If intel is deployed, but the intel document is not applicable to any endpoints, it continues to display as Pending indefinitely. Intel must be included in a Detection configuration to be applied to an endpoint. If an Intel document does not move to a Reduced or Disabled status, Intel remains in a pending state for up to two hours (by default) after Intel is deployed before moving to an Enabled state. This two hour timeframe is based on the Endpoint Safeguard Setting, which is 120 minutes by default.

No Safeguards

This designation means that automatic management of Enabled, Reduced, or Disabled states is turned off for an Intel document. This designation can be only for a specific intel document, or it could be turned off for the entire environment.



Note: You can re-enable Intel documents after they have become disabled or reduced by updating the intel document and deploying to reset the state. Saving any changes to the name, any suppression rules, or edits to the definition, or labels associated with the intel document constitute a change. Alternatively, you can also turn off safeguards for an individual document and redeploy intel to re-enable a reduced or disabled document. To re-enable all disabled intel documents, disable the **Intel Safeguards** setting in the **Intel Safeguards** section from the Settings  available from the Threat Response overview page.

Configure Intel Safeguards

1. From the Main menu, go to **Modules** > **Threat Response**. Click Settings .
2. Click **Service** > **Intel**.
3. In the **Intel Safeguards** section, enable or disable the **Intel Safeguards** setting.

©2026 Tanium Inc. All Rights Reserved

Enabling this setting causes intel documents that initiate a volume of alerts to become disabled. Default: Enabled.

4. In **Endpoint Safeguard Setting**, specify a number of throttle events that must occur in a time period for the intel document that is initiating the alerts to be disabled on the endpoint where alerts are being initiated.
   Default: 2 throttle events in 120 minutes. By default, individual endpoints throttle alerts for one hour if an Intel document alerts five times in five minutes. If this happens twice in a row, Intel Safeguards disables that intel document on that specific endpoint. Alerts from all other endpoints continue to be received.

5. In **Global Safeguard Setting**, set a threshold for continually throttled events across the enterprise that must occur for an intel document to be disabled.
   For example, if an intel document, at the service level, throttles 250 events consecutively, that intel document is disabled. Default: 250. By default, the service begins throttling alerts if an Intel document has more than 100 alerts in 20 minutes. If the number of alerts continues above this level, and the service counts 250 additional continuously throttled alerts after the throttle is initiated with no break in the throttling, Intel Safeguards will shut down that intel document across the entire environment.

Disable Intel Safeguards for an intel document

About this task

You can disable Intel Safeguards for individual intel documents of the following types: Open IOC, YARA, STIX, and signals that are part of the Tanium Signal feed.

1. From the Main menu, go to **Modules** > **Threat ResponseIntel** > **Documents**.
2. In the **Advanced Settings** section, deselect **Set to Active**.

Configure intel sources

An intel source provides a set of intel documents from an external source. Sources can be a vendor or a folder in your network. You can import sources manually or use sources that are based on subscription settings.

Intel sources are updated from the Threat Response service, which runs on the Module Server. If security software is deployed in the environment to monitor and block unknown URLs, your security

©2026 Tanium Inc. All Rights Reserved

administrator must allow the intel provider URLs on the Module Server.

Threat Response can use several data formats, with the following available source types:

- Connect to the Tanium Signals feed on page 93
- Connect to a TAXII server on page 96
- Set up Connect and Wildfire on page 98
- Use a local directory or remote share on page 98

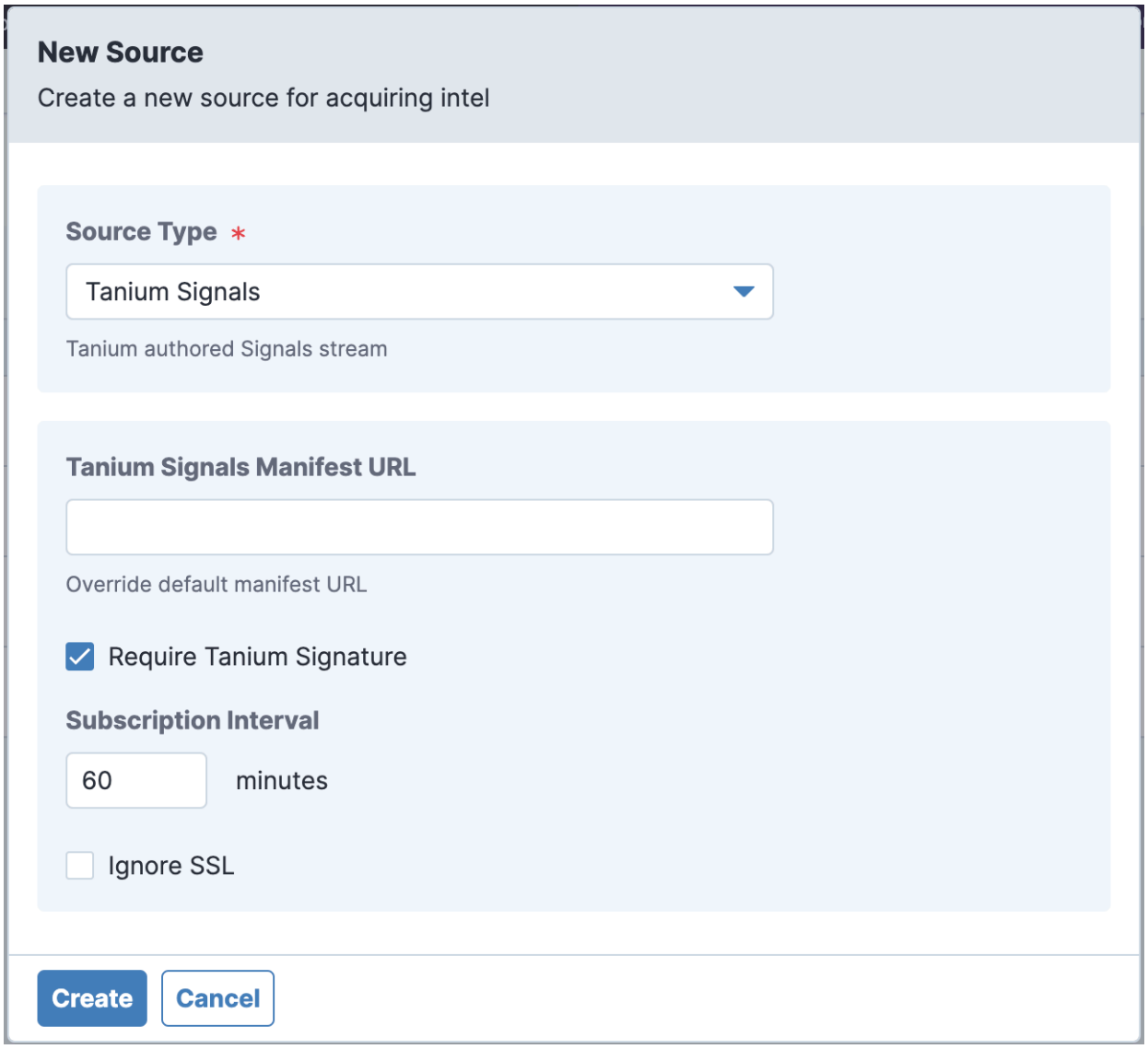
Connect to the Tanium Signals feed

About this task

You can configure one or more Tanium Signals sources to consume signals from different feeds. The default source is the Tanium Signal Feed, which provides a stream of regularly updated signals that are designed to detect common patterns of attack on Windows endpoints. Each signal is mapped to one or more categories in the MITRE ATT&CK Framework.

1. From the Main menu, go to **Modules** > **Threat ResponseIntel** > **Sources**. Click **Create**.
2. Enter a **Name** for the source that distinguishes it from other Tanium Signals sources.
3. (Optional) Enter a **Description** for the source.
4. From the **Type** drop-down menu, select **Tanium Signals**.

©2026 Tanium Inc. All Rights Reserved



5. (Optional) If you do not want to use the default feed, enter a different content manifest URL. Use this field for testing beta signals in non-production environments or to consume signals from a separate Tanium Signals feed such as Tanium HuntIQ. Each source requires a unique manifest URL. You cannot create a source using a URL that another Tanium Signals source already uses. If you require support for a different feed, see Contact Tanium Support on page 373.
6. Select **Require Tanium Signature** to only use Tanium-verified signals.
7. Select the **Subscription Interval**, in minutes.
8. (Optional) Click **Ignore SSL** to skip the certificate validation.
9. Click **Create**.

Result

©2026 Tanium Inc. All Rights Reserved

Note: If identical intel content exists in more than one Tanium Signals source, Threat Response keeps each occurrence as a separate signal instead of merging them into one.

When the Tanium Signals feed gets updated, system notifications get generated that include the release notes about the updates.

Configuring Tanium Signals feed in an airgapped environment

About this task

To configure the Tanium Signals feed in an airgapped environment on the Tanium Appliance, see Reference: Air gap support: Install or update Tanium Threat Response Signals.

If you are using one of the following versions of Threat Response, download Tanium Detect Signals v4:

- Threat Response version 3.10.59 or later 3.10 versions
- Threat Response version 4.0.1116 or later 4.0 versions
- Threat Response version 4.2.29 or later 4.2 versions
- Threat Response version 4.3.176 or later

If you are using Threat Response version 1.4 to any earlier 3.10, 4.0, 4.2, or 4.3 than listed above, download Tanium Detect Signals v3.

To deploy signals in an airgapped environment, navigate to https://content.tanium.com/files/published/thr/signals/refs/ga/DetectSignalsV4.zip and download Tanium Detect Signals from a computer that can access the internet. If you encounter a problem, see Contact Tanium Support on page 373.

When the download completes, host the .ZIP file on a Web server that is accessible by Threat Response. You can use the Tanium server to host this content. When this content is hosted, follow the instructions for connecting to the Tanium Signals feed.

For example, you can save the .ZIP file in a sub directory of the Tanium Server HTTP directory named signals. In this example, the URL to use when you create the signals feed is:

https://my.tanium.server/signals/DetectSignalsV4.zip

©2026 Tanium Inc. All Rights Reserved

In this scenario, content downloads directly from the Tanium Server, so the **Require Tanium Signature** option should be deselected. If the environment uses self-signed certificates select the **Ignore SSL** option.

All downloads of signals are logged on the module server.

Connect to a TAXII server

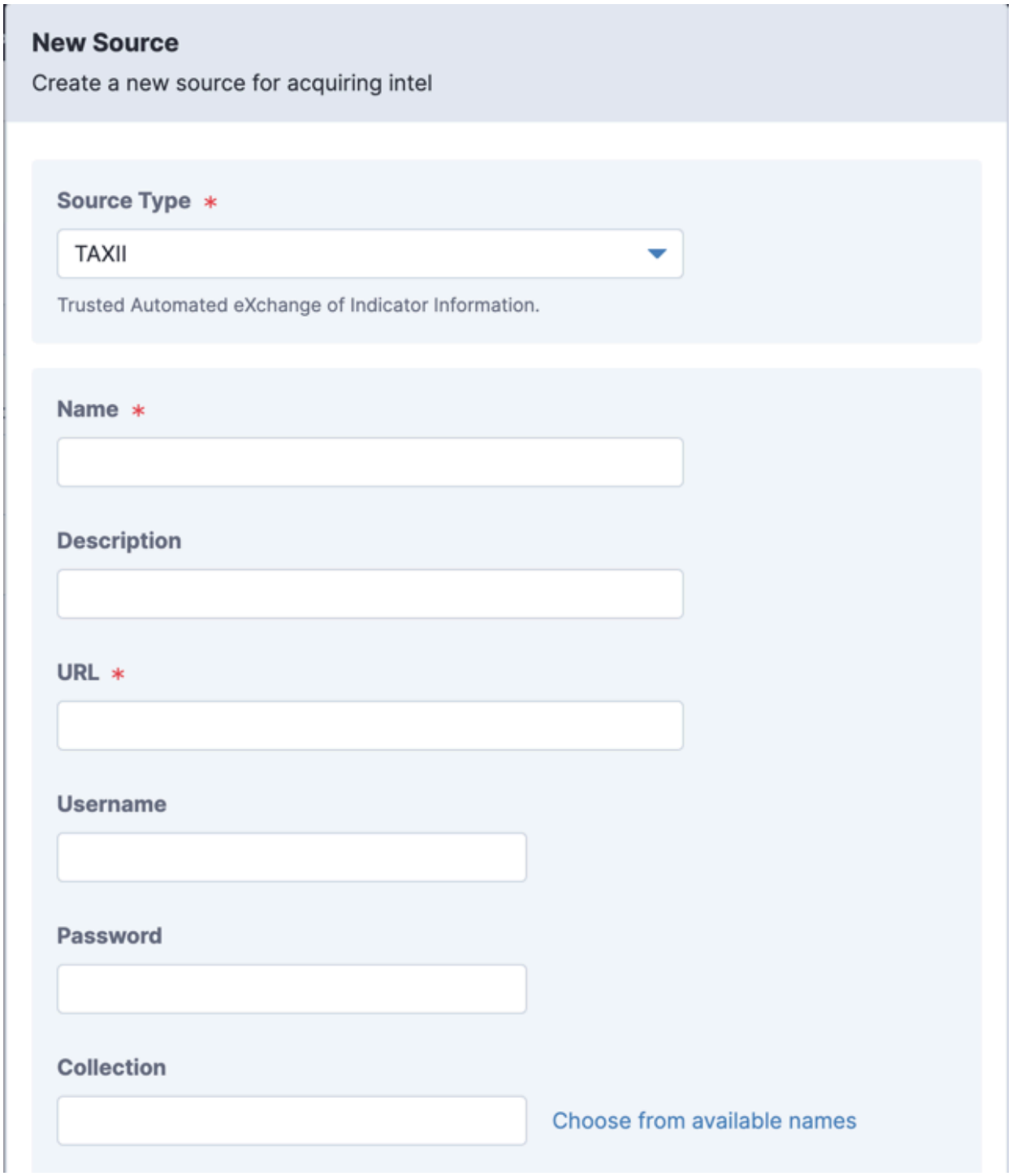
About this task

TAXII intelligence is always in STIX format. Unlike other streams, TAXII also sorts intel documents into collections, and a document only appears in one collection. Configure a source for each collection. Tanium does not support Subscription Based TAXII Servers; TAXII servers must be collection based.

> **Note:** The current supported version of STIX is 1.2. STIX 2.0 is required for TAXII 2.0 support. Consequently, TAXII 2.0 is not currently supported.

1. From the Main menu, go to **Modules** > **Threat Response Intel** > **Sources**. Click **Create**.
2. From the **Type** drop-down menu, select **TAXII**.

©2026 Tanium Inc. All Rights Reserved



3. Add a name and description.
4. Type in the case-sensitive collection name or select from available collections.
5. Select the **Initial History** in days, and the **Subscription Interval** in minutes.
6. Make optional security selections.
    a. If you want two-way SSL validation, paste the certificate and private key for your

©2026 Tanium Inc. All Rights Reserved

subscription.

b. Click **Ignore SSL** to skip the certificate validation.

7. (Optional) Click **Allow schema invalid documents** to enable the import of intel that might be formatted incorrectly. Invalid documents show a warning next to their type on the individual intel page.

8. Click **Create**.

Set up Connect and Wildfire

Important: The Palo Alto Networks Wildfire connection source is deprecated. Customers who need to integrate Palo Alto Networks WildFire and Tanium Threat Response should configure the Tanium Reputation source instead. For more information, see Tanium Reputation User Guide: Configure Palo Alto Networks WildFire reputation source.

For more information about configuring the reputation service, see Reputation data on page 103.

Use a local directory or remote share

About this task

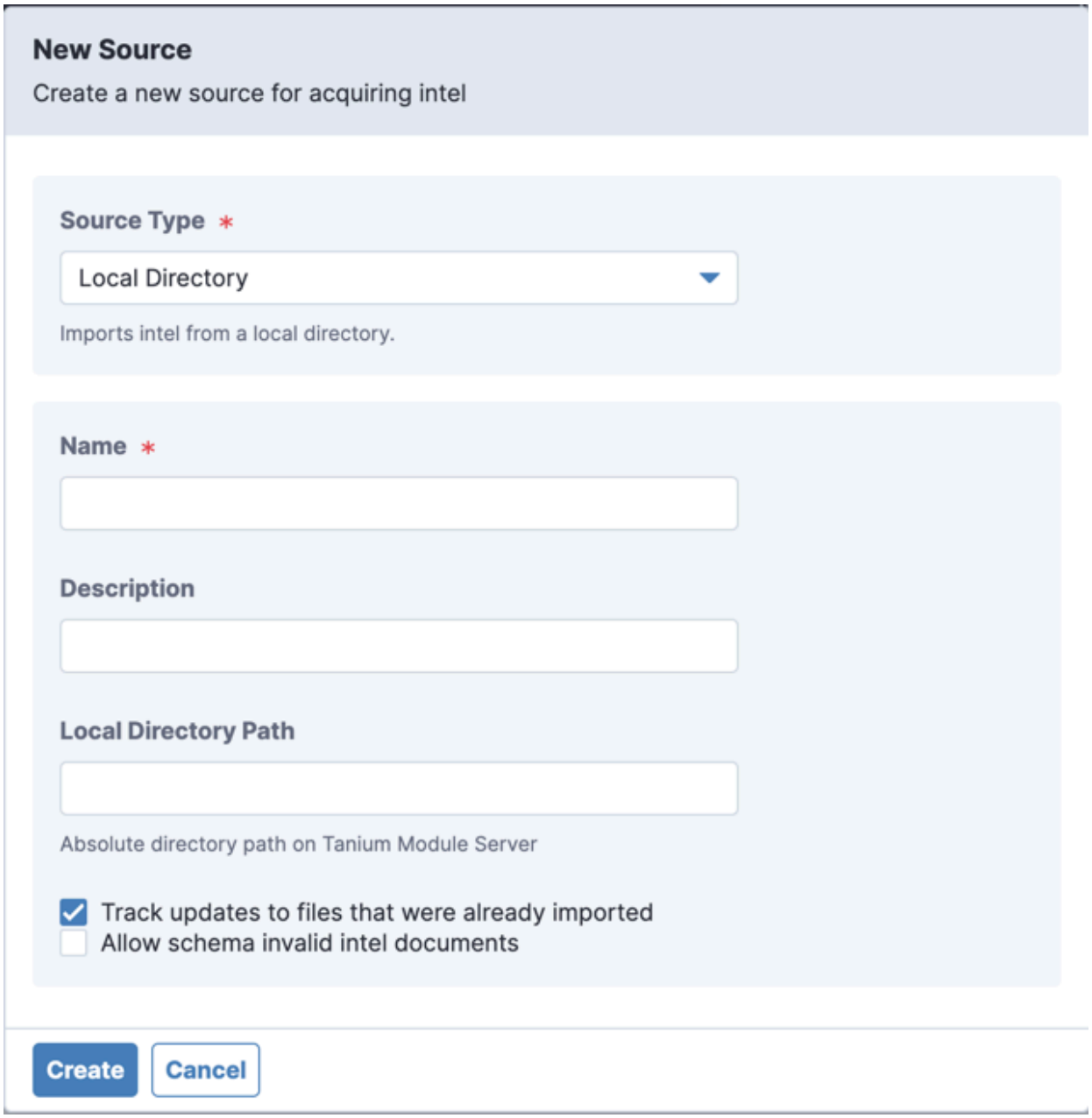
Stream intel from a set of local directories on the Module Server. The System Administrator for the computer where the Module Server is hosted must authorize a directory for streaming.

Note: In Threat Response 4.0 and later, local directories on the Module Server are no longer stored in the folder-stream-roots.conf file. All directory content is stored in the Threat Response database and all paths in the database are editable by using API routes. The API routes to view, add, or replace paths are available to users with the Tanium Administrator role. Any existing paths in the folder-stream-roots.conf file will be migrated to the Threat Response database when upgrading to Threat Response 4.0 from earlier versions.

To view the allowed paths, use the GET source-types/folder/allowed-roots route. To add or replace paths use the PUT source-types/folder/allowed-roots route. Both routes are only available to users who are assigned the Tanium Administrator role. For more information about using the Threat Response API, click **Help** > **API** > **See API documentation** from the Threat Response workbench.

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Threat Response Intel** > **Sources**. Click **Create**.
2. From the **Type** drop-down menu, select **Local Directory**.



3. Add a name and description.
4. In the **Local Directory Path** field, specify the absolute directory path on the Module Server. The folder must be explicitly authorized for stream activity.
5. (Optional) Disable update tracking for imported files.
6. (Optional) Click **Allow schema invalid documents** to enable the import of intel that might be formatted incorrectly. Invalid documents show a warning next to their type on the

©2026 Tanium Inc. All Rights Reserved

individual intel page.

7. Click **Create**.

Result

To mount a file share on a Tanium Appliance, see Tanium Appliance User Guide: Configure solution module file share mounts. After configuring the Detect file share mount, use the absolute path value /opt/mounts/detect as the **Local Directory Path**.

If you edit an existing source, for example, by adding subscription choices, Threat Response indexes and downloads new intel documents every 60 seconds. The intel gets pushed to the endpoint during the next intel publication interval.

For more information about registry settings to use sources with a proxy server, see Tanium Core Platform Installation Guide: Server Proxy Settings.

Delete an intel source

About this task

When you delete an intel source, all intel documents that are associated with the source are moved to the **Orphaned** source. The **Orphaned** source is not displayed on the sources page. To identify intel documents associated with the **Orphaned** source, you can filter all intel. Alerts that are associated with the intel from the source you are deleting are not deleted.

1. From the Main menu, go to **Modules** > **Threat Response Intel** > **Sources**.
2. Click the intel source that you want to delete.
3. Click Delete . Confirm that you want to delete the intel source.

Result

Any intel documents that were associated with the source you deleted are now associated with the **Orphaned** source. To manage intel in the **Orphaned** source, see View orphaned intel documents on page 113.

Configure process injection

About this task

©2026 Tanium Inc. All Rights Reserved

The Process Injection intel document provides a way to alert on incidents that involve techniques such as process injection and credential dumping. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process can allow access to the memory of the process, system and network resources, and possibly elevated privileges. Process injection can also evade detection from security products because the execution is masked under a legitimate process. In the context of process injection, the actor identifies the process or file that performs the process injection. The target identifies the artifact that has been the subject of injection.

Note: Process injection monitoring is not supported on Windows 8.1 and Windows Server 2012 R2 and earlier.

The Tanium Driver can monitor specific Windows API calls by injecting into user processes and kernel callbacks. The Tanium Driver can detect process injection and enable you to configure which process injection techniques result in an alert.

There are several techniques for process injection for which the Tanium Driver can monitor.

Process injection techniques

Technique	Description
Asynchronous Procedure Call	A process injection technique where an asynchronous procedure call executes memory that has potentially been created or modified in a malicious manner.
Asynchronous Procedure Call Write	A process injection technique where an asynchronous procedure call writes to remote memory. For example, an asynchronous procedure call is queued to execute memset.
Atom Bombing	A process injection technique where an asynchronous procedure call is queued to write to memory through GetGlobalAtomName.
Callback Overwrite	A process injection technique that encompasses any method that modifies a function callback pointer in the target to potentially execute malicious code.
Ctrl Inject	A process injection technique where key combination processing (for example, CTRL+C) is used in a possibly malicious manner.

©2026 Tanium Inc. All Rights Reserved

Technique	Description
Exe Header Modification	A process injection technique that includes an executable showing in-memory header modification that could be intended to load a DLL or execute code in a malicious manner.
Image Section Replacement	A process injection technique that involves the removal of a mapped DLL or executable from memory and replaced with new memory in a possibly malicious manner.
Thread	A process injection technique where a new thread has been remotely created in a possibly malicious manner.
Thread Context	A process injection technique where the context of a thread context has been modified to execute in a possibly malicious manner. For example, SetThreadContext.
Unknown Asynchronous Procedure Call	A process injection technique where an asynchronous procedure call that was not detected as queued is about to execute. Such a situation could be indicative of something malicious running in the kernel and injecting into a process or it could be other security products performing their own injection. It could also be caused by the Tanium process monitoring DLL not being injected into the actor process that queued the APC.
Unusual Initial Thread	A process injection technique where the first thread in a process was created in an unusual manner. For example, the operating system did not create the thread, but instead a remote process.
Window	One of any process injection techniques that use various window manipulations to execute code in a possibly malicious manner. For example, SetWindowLongPtr or SetProp.

1. Select **Consume Process Injection Alerts** in a detection configuration to enable Threat Response to consume Process Injection alerts. For more information, see Create detection configurations on page 144.

   Note: By default this option is disabled in new detection configurations.

2. From the Main menu, go to **Modules** > **Threat Response Intel** > **Extended Detections**.
3. Select **Process Injection**. It is not necessary to add the Process Injection intel document to any detection configuration or intel list to consume Process Injection alerts.
4. (Optional) From the **Techniques** tab, Click edit to select the techniques of process injection that you want to monitor. Click **Save**.
5. (Optional) Provide system filters to define the event information to record and add them to a recorder configuration. Ensure the **Consume Process Injection Alerts** setting is enabled in a

©2026 Tanium Inc. All Rights Reserved

deployed detection configuration. Apply system filters to exclude particular processes from having the Tanium Driver inject into them for process injection detection in a deployed recorder configuration. For more information, see Create filters on page 164.

6. (Optional) From the **Suppression Rules** tab, you can view the suppression rules that currently exist for process injection. Suppression rules define the criteria for filtering alerts based on information that you provide. Suppressing alerts for process injection is an effective way to reduce false positive matches and reduce noise in alerts. If you create a suppression rule for process injection it appears in the list displayed on this tab. For more information, see Suppress alerts on page 278.

Result

You can view, investigate, and take action on alerts that are the results of matches to process injection criteria from the Alerts tab of the process injection intel document.

Reputation data

Threat Response integrates with third-party reputation services. Hashes are sent to the reputation service for assessment, then Threat Response enhances intel with the hash ratings. The **Definition** and **Engine Analysis** tabs on the Intel details page provide additional information about how the intel document is structured, which parts are applicable, and the hash rating.

Reputation data provides more insight into which alerts might be good candidates to save for further analysis and action. Through a Tanium™ Connect integration, Threat Response uses the reputation data from third parties, such as VirusTotal. Blocklisted hashes are not included in the results unless the hashes are discovered by the saved question.

Threat Response detects if the reputation service is paused or stopped and in this event does not update reputation data. If after 24 hours the reputation service is disabled or deleted, Threat Response deletes the reputation source and any existing intel documents associated with the source are moved to the Orphaned source. If reputation is added again, the reputation source is created again.

The maximum database size for the reputation database is 10GB by default. You can increase this size as needed in the Reputation settings in the Reputation workbench. If the database exceeds this size, the reputation service is disabled.

Configure reputation data in Tanium Connect

©2026 Tanium Inc. All Rights Reserved

About this task

In Connect, create a connection from a saved question source to the Tanium Reputation destination. This connection initiates a list of hashes to be sent from a saved question in Connect to Reputation. The detect service queries Reputation for all discovered malicious hashes including known bad hashes. Reputation data requires a Connect version from Connect 4.1 to Connect 4.10.5, or Connect 4.11 and Reputation 5.0. For more information about configuring the reputation service settings, see Tanium Reputation User Guide: Reputation overview.

For endpoints that use reputation data, any hashes found by the saved questions are sent to the third-party reputation service for assessment.

> **Note:** Reputation Intel Source improvements (requires Reputation 5.0.0+) including Saved Questions for reputation hashes must now be configured and managed entirely within Tanium Connect. The naming convention of Reputation Intel has changed from Malicious Files $Date:$Time to Reputation Malicious Files $Date:$Time. Additionally, any Reputation intel that has existed before an upgrade is renamed with the date and time of the upgrade appended to the signal name.

1. Select **Consume Reputation Alerts** in a detection configuration to enable Threat Response to consume Reputation alerts. For more information, see Create detection configurations on page 144.

   > **Note:** By default this option is enabled in new detection configurations.

2. To view alerts that are specific to Reputation, from the Main menu, go to **Modules** > **Threat Response Intel** > **Extended Detections**.
3. Select **Reputation Malicious Hashes**.

Add signals

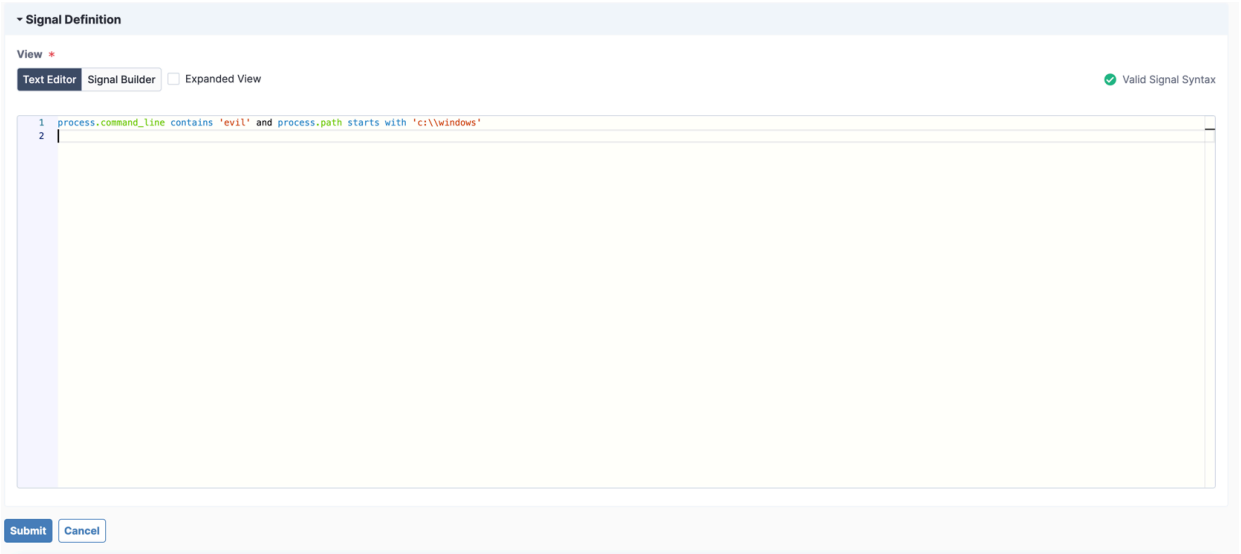
About this task

Signals are monitored by the recorder for live process, file, network, registry, and DNS event matching on the endpoint providing a recorder configuration is enabled in an active profile. If a recorder configuration is not enabled in an active profile, signal matches still initiate alerts, however no specific information regarding the context of the signal match appears in the resulting alert. You can write your own signals. By default, each signal can contain up to 55 terms.

©2026 Tanium Inc. All Rights Reserved

Important: An exhaustive reference to signals syntax - including supported objects, properties, and conditions - is available in the Threat Response Intel Support documentation. To access the Threat Response Intel Support documentation, click ? from the Threat Response overview page and click the Threat Response Intel Support tab.

1. From the Main menu, go to **Modules** > **Threat Response Intel** > **Documents**.
2. Click **Create** > **Signal**.
3. Add a name and description.
4. Select the platforms for the signal to target.
5. (Optional) Select any available reactions to associate with the signal. For more information, see Creating reactions on page 130.
6. (Optional) In the Advanced Settings section, select Set to Active under Intel Safeguards to disable the signal when a high volume of alerts is initiated. For more information. see Intel safeguards on page 90.
7. Select a MITRE Technique ID. Selecting a MITRE Technique ID allows users to align with the MITRE Attack Framework and help map coverage to the different tactics and techniques. You can assign multiple technique IDs to a single signal.
8. Configure the signal.
   For more information, see Reference: Authoring Signals on page 403.



9. (Optional) Add a description.

©2026 Tanium Inc. All Rights Reserved

10. Click **Save**.

Result

Important: If the event is filtered (ignored), it cannot be matched against a signal.

For signals provided by Tanium, see Connect to the Tanium Signals feed on page 93.

You can use the Threat Response Import Signals API to import signals that contain comments in the signal definition. Comments in signals are denoted as // at the beginning of lines or after the signals content.

For example, you can use the Threat Response Import Signals API to import a signal that contains the following syntax:

```
//Description: Generic single line description
//MITRE: T1234
process.command_line contains "foo" and process.path contains "bar"
```

For more information about the Threat Response Import Signals API, click**Help** > **API** and see the API documentation from the Threat Response workbench.

Import and export signals

Import and export signals to move them from one platform to another. For example, you can export signals from a test system and import them to a production system. Signals are imported and exported as JSON files and have a file size limit of 10 MB.

Note: You cannot export OpenIOC, STIX, and YARA intel documents.

Export signals

1. From the Main menu, go to **Modules** > **Threat Response Intel** > **Documents**.
2. Select the signals you want to export and click the ellipsis and select **Export**. Any intel documents that are not signals are omitted from the export.
3. For each signal that you include in an export, select to **Include all Labels** and **Include all Suppressions** if you want to preserve the labels and suppression rules that you have

©2026 Tanium Inc. All Rights Reserved

associated with the signal. Click **OK**. If you do not select to include labels or suppressions, the signal is exported without any associated labels or suppression rules.

> **Note:** When exporting a signal, only signal-specific suppression rules are included in the signal.

4. A JSON file is created for the export. Provide a name for the JSON file and click **Export**.

Import signals

About this task

> **Note:** You can use the Threat Response Import Signals API to import signals that contain comments in the signal definition. Comments in signals are denoted as `//` at the beginning of lines or after the signals content.

> **Important:** Importing a signal bundle that includes suppression rules requires the **Threat Response Suppression Rules** write privilege, in addition to **Threat Response Intel** write. If your account has intel write but not suppression rules write, the import is rejected when the bundle contains suppression rules.

1. From the Main menu, go to **Modules** > **Threat Response Intel** > **Documents**.
2. Click **Upload Signal(s)**.
3. Browse to the JSON files that correspond to the signals you want to import. Click **OK**. Click **Next**.
4. If the signal already exists, or exists with different suppression rules or labels associated with it, select **Action** > **Skip** to not import the signal. Click **Next**.
5. Review the list of the imported signals and click **Finish**.

Result

©2026 Tanium Inc. All Rights Reserved

Note: Exporting signals that include MITRE technique IDs and importing them into an environment where the same signals exist without associated MITRE technique IDs results in a new signal with the same content and the addition of MITRE technique ID information. The result is that two signals exist; one with MITRE technique information, and one without.

Upload intel documents

About this task

You can upload multiple intel documents at the same time, including YARA files. The size limit for uploading intel documents is 10MB for IOCs in XML format, such as STIX version 1.x, and signals in JSON format.

Best Practice: Do not add more than 900 terms per type in a single IOC.

1. From the Main menu, go to **Modules** > **Threat Response Intel** > **Documents**.
2. Click **Import IOC/YARA(s)** or **Import Signal(s)**.
3. Select intel files and click **Upload**.
4. Review the intel validation check. The intel XML schema validation check shows the documents that were successfully uploaded and any documents with errors.
5. Click **Close**.

Create intel documents

About this task

Create an intel document with a set of user-defined rules.

Tip: Quick IOC supports some types of defanged IP address formats that are found in threat intelligence documents, such as 10[.]1[.]1[.]1 or 10 . 1 . 1 . 1.

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Threat Response Intel** > **Documents**.
2. Click **Create** > **Quick IOC**.
3. Type a name for the intel document. For long term usability, use a consistent naming convention.
4. From the **Detect when** drop-down menu, select a type of data.
5. Type the information to match. When you use the matches condition for any supported object, IOC uses regular expressions to evaluate resulting matches. You can include flags in the regular expression string to perform case sensitivity or insensitivity. You can use the (?i) flag around content in the regular expression for case insensivity. To end a section where you want to use case insensitivity, you can use the (?-i) flag.
   For example,(?i)scvhost.exe(?-i) matches include ScVhOsT.eXe, scvhost.exe, and SCVHOST.exe.
6. (Optional) Enable **Exact match required**.
7. In the **Advanced Settings** section, choose whether or not to enable Intel safeguards. Intel safeguards provide the option to set thresholds across the environment for intel and to suppress intel that generates amounts of alerts that exceed the thresholds. For more information about intel safeguards, see Intel safeguards on page 90
8. Select a MITRE Techniques. Selecting MITRE Techniques allows users to align with the MITRE Attack Framework and help map coverage to the different tactics and techniques. You can assign multiple techniques.
9. Select any applicable labels to add labels to the IOC.
10. Click **Create**.

Create IOCs

About this task

Use the IOC editor to create both simple and complex IOCs using AND/OR operators and understand the IOC objects and properties that Threat Response supports. You can edit IOCs that you import to the Threat Response workbench, remove any unsupported objects or properties, and add conditions to fine tune detections. The IOC editor ensures that the syntax is followed and validates that IOCs that you create feature supported terms. Imported IOCs might contain unsupported terms and therefore editing an IOC only enables you to add, modify, or delete terms supported by Threat

©2026 Tanium Inc. All Rights Reserved

Response, and to only delete non-supported terms.

Both the 1.0 and 1.1 versions of OpenIOC are supported.

1. From the Main menu, go to **Modules** > **Threat ResponseIntel** > **Documents**.
2. Click **Create** > **IOC**.
3. Add a name and description.
4. (Optional) Select a reaction to associate with the IOC. Reactions automate one or more actions on an endpoint based on alerts from intel documents (for example, delete one or more files, kill a process, or quarantine an endpoint). For more information about reactions, see Creating reactions on page 130. By default, the reaction is set to Audit Mode. You can disable Audit Mode when you save the IOC.
5. In the **Advanced Settings** section, choose whether or not to enable Intel safeguards. Intel safeguards provide the option to set thresholds across the environment for intel and to suppress intel that generates amounts of alerts that exceed the thresholds. For more information about intel safeguards, see Intel safeguards on page 90
6. Select a MITRE Techniques. Selecting MITRE Techniques allows users to align with the MITRE Attack Framework and help map coverage to the different tactics and techniques. You can assign multiple techniques.
7. Select any applicable labels to add labels to the IOC.
8. Use either the IOC Builder or Text Editor to provide the content of the IOC.
9. (IOC Builder) Select an object, property, condition, and value to use in the IOC. An exhaustive reference to IOC syntax - including supported objects and properties is available in the Threat Response Intel Support documentation. To access the Threat Response Intel Support documentation, click ? from the Threat Response overview page and click the Threat Response Intel Support tab. When you use the matches condition for any supported object, IOC uses regular expressions to evaluate resulting matches. You can include flags in the regular expression string to perform case sensitivity or insensitivity. You can use the (?i) flag around content in the regular expression for case insensivity. To end a section where you want to use case insensitivity, you can use the (?-i) flag. For example,(?i)scvhost.exe(?-i) matches include ScVhOsT.eXe, scvhost.exe, and SCVHOST.exe.
    a. Click **Add Row** to add additional criteria to the IOC. When you have multiple rows, you can select whether the IOC evaluates all of the rows logically as AND or OR.
    b. Click **Save**.

©2026 Tanium Inc. All Rights Reserved

10. (Text Editor) Provide the IOC content using valid syntax. Threat Response validates the content and flags unsupported objects.
    a. Click **Save**.

Result

Important: When you create an OpenIOC that includes a file path condition, use paths native to a single operating system family. Combining Windows-style and non-Windows-style (Linux or macOS) paths in the same IOC causes Index to fall back to a full-table scan instead of an indexed lookup, which can significantly increase endpoint CPU usage during evaluation. To avoid this performance impact, create separate IOCs for Windows paths and non-Windows paths.

Label intel

Use labels to organize intel into sets that are relevant for your environment. For example, you might want to sort intel by priority, incident case, or based on the applicable attack surface.

Create custom labels to control the promotion of intel in a production environment. The names of labels provided by Tanium are subject to change. Signals are generally updated automatically, creating a possibility that label changes could cause unintended consequences in a production environment. A best practice is to adopt a convention for naming custom labels that follows an organization's object naming guidelines. Intel documents that Threat Response provides by default, such as Defender, Deep Instinct, and Process injection do not support labels.

You can apply labels to the Reputation intel document, however if you want to add reputation intel for background scanning, you must add the reputation source in a Detection configuration. You cannot add the reputation intel document to a detection configuration as you would add other intel.

Apply a label

1. From the Main menu, go to **Modules** > **Threat Response Intel** > **Documents**.
2. Select the checkbox next to the intel documents or signals. Click **Labels**.
3. Click **Add Label** and type in a new label or select an existing label.
4. Click **Save Changes**.

Manage existing labels

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Threat Response Intel** > **Documents**.
2. Select the checkbox next to the intel documents or signals. Click **Labels**.
3. Click **Manage Existing Labels** and select or deselect the labels you want to apply to the intel document or signal. In the **Selection Preview** section, review the impact of making changes to intel documents.
4. Click **Save Changes**.

Configure YARA files

About this task

YARA files function like other intel documents, in regards to uploading, streaming from a folder, and labeling. However, Threat Response automatically assigns a scope to limit the evaluation scan; by default, all YARA files are set to scan live files. You can change the evaluation scope for any YARA file.

Note: YARA 4.5 is supported and support for the following default modules is provided: pe, elf, dotnet, hash, cuckoo, math, macho, dex, string, and time.

1. From the Main menu, go to **Modules** > **Threat Response Intel** > **Documents**.
2. Click the intel name, then click the **Search Scope** tab.
3. Select the scope of evaluation scan.
   - **Live Files**: This instructs Threat Response to find the files for any running processes (executable and loaded library files) and then use the YARA rule to scan their file on disk. Limited to the running processes and their executable and library files.
   - **Memory**: Limited to the memory of all running processes.
   - **Paths**: Limited to the configured directory paths. The path search is recursive, up to six directories. When adding paths ensure that no duplicate entries or empty values are added.
4. Click **Save**.

Result

©2026 Tanium Inc. All Rights Reserved

Note: On Mac OS 13.4+, YARA memory scanning is limited to processes without hardened runtimes only.

View orphaned intel documents

About this task

When the source for a piece of intel is removed, the intel moves into an orphaned state.

1. From the Main menu, go to **Modules** > **Threat Response Intel** > **Documents**.
2. Expand the **Filter Results** section and set the **Source** to **Orphaned**.

Assign a reaction to an intel document

To cause the workflows that you define in a reaction to occur when an alert is initiated for an intel document, you need to assign the reaction to an intel document. For more information, see Creating reactions on page 130.

Note: When you duplicate an intel document, any reactions that you have assigned to the document that you are duplicating do not persist in the duplicate intel document.

Testing Intel for deployment

About this task

Best Practice: Test intel in a lab or test environment and deploy intel in a ring-based deployment before deploying to a production environment. Create the new Intel and use on-demand scans to test against endpoints to verify the intel matches on what you expect and that the intel does not match a high number of false positives. Evaluate intel safeguard settings.

When you are ready to promote the intel in a production environment, the following process is advised as a best practice:

©2026 Tanium Inc. All Rights Reserved

1. Import or create the new intel in a production environment.
2. On-demand scan the intel against a computer group that contains a small number of endpoints that you have identified as appropriate for testing purposes. For more information, see Tanium Console User Guide: Create computer groups for more information. On-demand scans send a single piece of intel to the endpoints for immediate matching and alert reporting. You can use signals, OpenIOC, STIX, YARA, or reputation intel in an on-demand scan. For more information, see On-demand scans on page 142. Verify the performance of the intel; for example, ensure it is matching and generating alerts for expected indicators of compromise.
3. On-demand scan the intel against a computer group that contains approximately 10-20% of the total endpoints the intel will ultimately target. Verify the performance of the intel. Modify the intel if necessary.
4. In addition to testing with on-demand scans, deploy intel in a ring-based deployment as a best practice. Modify the intel if necessary.
5. Deploy the intel to the production environment. Continue to verify the performance of intel and refine as necessary.
6. Review the settings you have specified for intel safeguards to evaluate the fidelity of intel documents and disable any intel documents that generate high volumes of alerts. For more information, see Intel safeguards on page 90.

©2026 Tanium Inc. All Rights Reserved

Searching with threat navigator

About this task

Use threat navigator to run hypothesis-based hunts that use signal and IOC syntax and enable you to refine queries and save items of interest for future reference. Threat navigator enables you to search for artifacts on endpoints and test and develop intel across the following sources without creating alerts:

- Historical data captured by recorder
- File index data at rest
- Live data from the recorder for any legitimate signal or IOC intel document

Similar to on-demand scans, threat navigator sends an intel definition in signal or IOC format to endpoints for immediate matching, but unlike on-demand scans matches do not generate alerts. Threat navigator returns search results based on your intel definition.

You can tune intel definitions, iterate on search strategies, and eliminate non-interesting results so that you can focus on more interesting findings. For example, you can locate a single endpoint with a single artifact across a large enterprise and create a workflow that scopes a search to target interesting findings. You can also analyze matches across endpoints and continue to drill down on results.

Test intel documents with threat navigator to evaluate their effectiveness and to better understand the fidelity of intel and to have confidence that the results of findings from intel are complete. You can evaluate search results to understand if a search has exceeded any intel safeguards thresholds and be confident that there are not more intel matches beyond what you can see from alerts. You can test and edit existing signals and IOCs, or create or import custom signals or IOC documents. When you import intel documents it eliminates the need to manually recreate things like IOCs with hundreds of terms in them, or complex signals that you have obtained from a partner, 3rd party, or intel development team. As you iterate on intel definitions that match interesting findings, you can save your work as new intel documents that you can use in detection configurations to generate alerts.

You can use threat navigator to test and refine hypotheses. When a hunt reveals interesting findings,

©2026 Tanium Inc. All Rights Reserved

you can convert the parameters of the hunt into an intel document that generates real-time alerts on an endpoint.

At any time while exploring intel you can export data for all matches to an external CSV file to use for analysis. Threat navigator preserves searches so if you log out of Threat Response, you can resume any work in progress.

Note: Threat navigator requires the **Threat Response Administrator** role, **Threat Response Operator** role, or a custom role that provides permissions required for this feature. The **Threat Response Administrator** role has the **Visibility Bypass** permission. If a user or persona is scoped to a certain computer group, for the purposes of viewing alerts and saved evidence the user or persona can view all of the content. With threat navigator, **Visibility Bypass** does not apply. A **Threat Response Administrator** or other user, role, or persona with **Visibility Bypass** cannot view threat navigator search results data. Such users are limited to the computer groups that they have access to.

Search with intel

About this task

You can search across combinations of artifacts including live data, file index data, and historical recorder data on all Tanium-managed endpoints using supported OpenIOC objects or properties.

Note: Threat Response only supports OpenIOC version 1.1.

For a more process-oriented search, you can search for artifacts in endpoint historical recorder data using signals. Signals are monitored by the recorder for live process, file, network, registry, and DNS event matching on endpoints.

An exhaustive reference to intel syntax - including supported objects and properties for IOCs and signals is available in the Threat Response Intel Support documentation. To access the Threat Response Intel Support documentation, click ? from the Threat Response overview page and click the Threat Response Intel Support tab.

1. From the Main menu, go to **Modules** > **Threat ResponseThreat Navigator**.
2. From the **Run New Search** section, click either **IOC** or **Signal**.

©2026 Tanium Inc. All Rights Reserved

3. (IOC or Signal Builder) Click **Add Row**. Select an object, property, condition, and value to use in the intel definition.
   An exhaustive reference to IOC and signal syntax - including supported objects and properties is available in the Threat Response Intel Support documentation. To access the Threat Response Intel Support documentation, click ? from the Threat Response overview page and click the Threat Response Intel Support tab. When you use the `matches` condition for any supported object, IOC uses regular expressions to evaluate resulting matches. You can include flags in the regular expression string to perform case sensitivity or insensitivity. You can use the (?i) flag around content in the regular expression for case insensitivity. To end a section where you want to use case insensitivity, you can use the (?-i) flag. For example,(?i)scvhost.exe(?-i) matches include ScVhOsT.eXe, scvhost.exe, and SCVHOST.exe. Click **Apply** at the end of the row to add the criteria to your search definition. You cannot search until at least one row is added to a definition.

   a. Click **Add Row** to add additional criteria to the intel definition. For each row, click **Apply** to add the criteria to the definition. When you have multiple rows, you can select whether the intel definition evaluates all of the rows logically as AND or OR.
   b. Click **All Computers** to select computer groups that the search targets.
   c. Click **Run**.
      Step result: The status of the search page shows **Active Search**. Results can take a few minutes to appear in the results grid.

4. (Text Editor) Provide the intel content using valid syntax and click **Search**.
   The status of the search page shows **Active Search**. Threat Response validates the content and flags unsupported objects. Results can take a few minutes to appear in the results grid.

   > **Important:** If you paste a document of the wrong intel type into the IOC or Signal text editor (for example, STIX content into the IOC editor), Threat Navigator shows **Only IOC and signal intel documents are supported.** and disables **Run** with a tooltip describing the syntax problem, instead of accepting the document and failing later.

5. (Optional) You can click **Stop** at any time during an active search to stop the search in progress and leave any results that appear in the results grid.

Quick filters

Quick filters provide an interface to easily filter the results of your search and the ability to apply include or exclude filters to your intel definition using summarized data that appears as results

©2026 Tanium Inc. All Rights Reserved

update. Data in the quick filters view might not show in the results grid if more than 10,000 findings total exist for the search. A loading icon indicates that data collection is in progress. Summarized data is based on up to 100 individual items per endpoint and intends to provide a close representation of the full data set.

The sections show the top five results by count and the bottom five results by count. A loading icon appears next to each section title to indicate that data is not completely loaded. When a section has loaded completely, click **View All** to view all the results for a particular section.

Click **Quick Filters** to filter the data that appears in the results grid using a filter builder. This enables you to gain visibility into filter results and quickly add filters to the filter builder.

From within the Quick Filters results grid, you can select **Include** or **Exclude** to filter the results of the search.

Include filters remove any results that do not match the specified criteria. Only items that match the include filter show in the search results. Exclude filters remove results that match the specified criteria. If a result matches the exclude criteria, it is filtered from the search results.

Selecting these filters adds the corresponding syntax to your search results, updating the results table and showing any active filters in the Filters section. After validating that your filters are taking the desired actions, you can click **Apply to Intel Definition** to add the filter criteria to the intel definition.

Pin artifacts to a search

Pinning artifacts to a search solves a fundamental problem with threat hunting in real-time data. If you find an artifact of interest as part of a hunt, it might not appear in subsequent searches. By pinning the interesting finding and saving it with the search criteria, you can demonstrate what search parameters lead to the discovery of the pinned artifact and keep it as part of a system of record.

Additionally pinning artifacts provides an easy way to keep important information easily accessible for team members. Pinned artifacts:

- Ensure the visibility if important or significant information.
- Help organize discussions by keeping related information together, making it easier to navigate through searches.

©2026 Tanium Inc. All Rights Reserved

- Highlight potential priorities, aiding in quick decision-making.
- Provide a quick entry point to viewing artifacts of interest without the need to study other searches and hypotheses.
- Foster a structured and collaborative environment, enhancing team communication.

Note: The pin action is not available for users who do not have the permission required to create pins.

Pin an artifact to a search

1. From the Main menu, go to **Modules** > **Threat ResponseThreat Navigator**.
2. Click the **Searches** tab.
3. Click the name of an active search.
4. Select one or more items from the **Search Results** and click Pin 📌.
   Artifacts that you pin show in the **Pinned** tab of the **Search Results**. Pinned items are specific to the search iterations you select them in. The information associated with a pinned artifact is limited to the data in the columns for the search results at the time you pinned the artifact. Columns added to the view after you pin an artifact show **No data is available** for that artifact. To capture specific fields (for example, parent path or parent arguments), add those columns to the search results before you pin. If you pin artifacts from different views or with different columns active, the pinned tab might show a mix of populated and unavailable fields across rows. For endpoint result pins, all users with the **Threat Response Threat Navigator Read** permission can view pinned artifacts provided that users have management rights for the computer groups the endpoints on which the pinned artifacts exist. Count result pins show for all users that can see the search. Pinned artifacts persist after data is deleted for a search.

Unpin an artifact

1. From the Main menu, go to **Modules** > **Threat ResponseThreat Navigator**.
2. Click the **Searches** tab.
3. Select the search with which the pinned artifact is associated.

©2026 Tanium Inc. All Rights Reserved

4. Click the **Pinned** tab.
5. Click Pin 📌 in the rows for artifacts you want to unpin.
6. Confirm that you want to unpin the artifact. Click **Unpin**.

Iterate on searches

You can iterate on searches to experiment with different parameters that you apply to intel definitions based on the results of previous searches. Each iteration of a search is saved in a version history so you can revert back to previous searches.

You create a new iteration when you create a new intel definition or change an existing intel definition associated with a search and then run a search.

You must run the search before you can save it. Unsaved iterations are deleted eight hours after completion of the scan.

Iterations form a branch structure that starts with a root search. You can branch from any iteration. To view the **Version History** as a branch view, toggle **Group Data**.

Only five iterations can have data associated with them. When you save a new iteration or refresh an older iteration and save it, the iteration that has the oldest **Last Run At** value is cleared. To remove the root iteration, which is by default Iteration 1, you can delete the search. If you remove an iteration that is the root node in a branch, this also removes all child nodes of that iteration. Additionally, deleting an iteration that features any associated pinned artifacts removes the pins associated with those artifacts.

For any search, view the current iteration at the top of the search page.

To view the branch view of all iterations for a search, click Version History and view the Version History section of the details view. Click any iteration to show options to **Retart the Search** using the parameters that are specific to that iteration, **Show the Seach Critera**, **Edit** the parameters of the intel definition for the iteration, or **Delete** the iteration.

Choose existing intel

About this task

Add an existing IOC or signals intel document from the intel documents page to threat navigator and

©2026 Tanium Inc. All Rights Reserved

edit the parameters of the intel document.

You can add intel documents to threat navigator that you created from the intel page of the Threat Response workbench. For information about importing intel created by other users, see Import intel on page 122.

1. From the Main menu, go to **Modules** > **Threat ResponseThreat Navigator**.
2. From the **Choose Existing Intel** section, click either IOC or Signal.
3. Select an intel document and click **Edit** to edit the intel definition.
   You can filter for intel documents that have the following states of intel safeguards. Intel safeguard status does not effect threat navigator searches. You can run reduced or disabled intel documents with threat navigator.

   Enabled
   : This designation is assigned to any intel documents that are not assigned another state.

   Reduced
   : Indicates intel documents that any single endpoint has disabled. The result of an intel document being assigned this designation is that it no longer provides the complete visibility expected from a high-fidelity intel document. A system notification appears in the audit browser to show which endpoints are in a reduced state.

   Disabled
   : Indicates intel documents that are disabled enterprise-wide. Such intel documents have initiated alerts that have throttled over 250 times. 250 is a default value that you can configure to a more appropriate value for an environment. Intel documents with this designation require tuning and reevaluation to be effective.

   Pending
   : Indicates new or recently modified intel documents that have not been deployed and consequently have no basis for any other designation. If intel is deployed, but the intel document is not applicable to any endpoints, it continues to show as Pending indefinitely. Intel must be included in a Detection configuration to be applied to an endpoint. If an Intel document does not move to a **Reduced** or **Disabled** status, Intel remains in a pending state for up to two hours (by default) after Intel is deployed before moving to an **Enabled** state. This two hour timeframe is based on the Endpoint Safeguard Setting, which is 120 minutes by default.

©2026 Tanium Inc. All Rights Reserved

No Safeguards

Indicates that automatic management of **Enabled**, **Reduced**, or **Disabled** states is turned off for an Intel document. This designation can be only for a specific intel document, or it could be turned off for the entire environment.

4. Click **Search** to start a new active search using the intel document. For more information, see Search with intel on page 116. You can save any changes that you make to the original intel document as a new intel document or overwrite the existing intel document.

Import intel

About this task

Import an IOC or signals intel document that you have obtained from a partner, 3rd party, or intel development team to threat navigator. You can import one intel document at a time to threat navigator.

1. From the Main menu, go to **Modules** > **Threat ResponseThreat Navigator**.
2. From the **Import Intel** section, click either **IOC** or **Signal**.
3. For IOCs, browse to the IOC or XML files that correspond to the IOCs you want to import or drag them from the file system. For signals, browse to the JSON files that correspond to the signals you want to import or drag them from the file system.
4. Click **Import**.
5. Click **Search** to start a new active search using the intel document. For more information, see Search with intel on page 116.

View search activity

View and manage both active and inactive searches. Threat navigator supports 10 active searches at any time. There is no limit to the number of supported inactive searches. An active search indicates that Tanium-managed endpoints are currently the target of the search. You can filter the data that shows in the **Searches** tab by any of the columns.

Active search

Active searches include those that are running and have not completed, and those that have run

©2026 Tanium Inc. All Rights Reserved

and currently have data associated with them. Active searches remain active for seven days starting from the time you last loaded the results or edited filters.

If you select an active search and click **Clear Active Search**, the search becomes an inactive search.

Inactive search

Inactive searches include those that have run to completion. No data is associated with an inactive search. You can load the search definition and perform a new search with this data. In effect, an inactive search is comparable to a command history; it preserves the command, but not the results of the command. The results of performing an inactive search again most likely does not return the exact same results as previous searches because of endpoint activity and the specific endpoints that are online when you search.

You can take action on the searches that appear in the **Search History** section.

For active searches:

Stop Search

Stops a search that is in progress. When you have stopped an active search, **Clear Active Search** is enabled.

Clear Active Search

Sets the results as a inactive search.

Load Search

Shows the search page and search results.

Delete Search

Removes a search from the Search History results.

For inactive searches:

Load Search

Shows the search definition. From the search definition, you can click **Search** to start the search again and show search data.

©2026 Tanium Inc. All Rights Reserved

Delete Search

Removes the search from the **Search History** results.

View search results

Search results appear in the **Searches** tab. Select any active search and click **Load Search** to view search results. The **Search Results** has views for **Counts** and **Endpoints**. The **Counts** tab shows details related to artifacts that matched the search criteria, and a count of matches per unique artifact. The **Endpoint** tab shows the details of each matching artifact alongside the endpoint it was discovered on. This tab also features a column that has a link you can use to direct connect to the endpoint on which the artifact match occurred. For more information about direct connecting to endpoints, see Direct connecting to endpoints and exploring data on page 189.

You can select to show additional columns beyond the default columns in the search results. The number of columns for the count view is limited to ten. Additional columns provide a means for further filtering and tuning the search results.

Threat navigator uses enrichment to add context to process and reputation data in search results. Contextual content appears in the **Counts**, **Endpoints**, and **Pinned** tabs and matches the enrichments shown in the **Alert Details** and **Process Tree Details** panes. Enrichment data populates asynchronously and might not appear immediately when search results first load.

You can add the following enrichment columns to the **Counts**, **Endpoints**, and **Pinned** tabs:

Process Path

The file system path of the process that matched the search criteria.

Process Args

The command-line arguments of the process that matched the search criteria.

Parent Path

The file system path of the parent process.

Parent Args

The command-line arguments of the parent process.

©2026 Tanium Inc. All Rights Reserved

Hash columns include a reputation indicator that identifies potentially malicious files. The reputation indicator matches the appearance and behavior of the reputation indicator in the **Alert Details** pane.

Data that shows in the search results is sampled data. Sampled data is a representation of the type of data you can reasonably expect from endpoints. Data shown is limited to 10,000 items with no more than 100 results reported from each endpoint. This data provides insight into the types and volumes of results to expect from endpoints. Analysis of this data is helpful to tune intel to ensure that the results are useful for your purposes. When a search is seven days old, it becomes an inactive search.

Filters that you apply in the **Quick Filters** section apply to the results in the search results section. Apply quick filters to tune the results in the grid. For more information, see Quick filters on page 117.

You can apply additional filters based on objects, properties, conditions, and values in a filter builder from the results section. For each row in the results, you can **Include** or **Exclude** the artifact from the results. Additionally, you can select a cell in a row and include or exclude that specific value as a filter.

The include method of filtering enables you to replace the default filter to only include the filters you specify to reduce performance impact and enable quick event identification. The exclude method of filtering prevents events that match the criteria you provide from showing.

When you are satisfied with the filters you have applied and the results are useful for your purposes, click **Apply Filters and Run Search** to update the intel definition with the filters you selected. Running the search clears stored filters.



Note: Signals that are overly complicated can have potential negative impacts on endpoints. For more information and best practices for authoring signals, see Reference: Authoring Signals on page 403.

Click **Export** to export the results of the search to a CSV file. The current web browser manages the CSV file download. All exports save to the downloads directory of the web browser that initiated the export.

Create hypotheses

About this task

A hypothesis is a grouping of searches performed by any member of your organization and intel documents. Hypotheses preserve collections or groups of searches as a system of record.

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Threat ResponseThreat Navigator**.
2. Click the Hypothesis tab. Click **Create**.
3. Provide a name and description.
4. Select searches and intel documents to associate with the hypothesis. When you select the Searches tab a list of available searches that have been created by members of your organization show. Select the searches to add them to the hypothesis. Repeat this step for intel documents. You can associate any intel document with a hypothesis; the intel documents you can associate are not limited to intel documents you have imported into threat navigator. As you associate searches and intel documents, the metrics at the top of the **Associated Items** section update to reflect the artifacts that you add to the hypothesis.
5. Click **Create Hypothesis**.

Export a hypothesis

About this task

You can export one or more hypotheses to a MD file.

1. From the Main menu, go to **Modules** > **Threat ResponseThreat Navigator**.
2. Click the Hypothesis tab. Click **Export**
3. The MD file download is managed through the web browser. All exports are exported to the downloads directory of the web browser that initiated the export.

View MITRE techniques

About this task

Threat navigator uses the MITRE ATT&CK framework to help you track threat hunting coverage. Use the **MITRE Techniques** tab to browse the full ATT&CK matrix and see how your searches, intel documents, and hypotheses map to each technique.

Browse MITRE techniques

The **MITRE Techniques** tab displays all MITRE ATT&CK tactics and their associated techniques and sub-techniques. A metric bar at the top of the tab shows the total count of tactics, techniques, and sub-techniques in the framework.

©2026 Tanium Inc. All Rights Reserved

Select a tactic to display its techniques in the grid. The grid includes the following columns:

ID

The MITRE technique ID, for example, T1595. Click the ID to open the technique on the MITRE ATT&CK website.

Technique

The name of the technique or sub-technique.

Tactic

The tactic associated with the technique. This column appears on parent rows only.

Search

The number of searches associated with the technique. Click the count to view the associated searches.

Intel

The number of intel documents associated with the technique. Click the count to view the associated intel documents.

Hypothesis

The number of hypotheses associated with the technique. Click the count to view the associated hypotheses.

Click the expand arrow on a parent row to view its sub-techniques. Sub-techniques have their own ID, technique name, and counts.

1. From the Main menu, go to **Modules** > **Threat Response** > **Threat Navigator**.
2. Click the **MITRE Techniques** tab.
3. Select a tactic from the sidebar to view its techniques.
4. (Optional) Use the **MITRE Technique** or **MITRE Tactics** filters to narrow the techniques displayed.
5. (Optional) Use the search field to find a technique by name or ID across all tactics.
6. Click the expand arrow on a parent row to view sub-techniques.

©2026 Tanium Inc. All Rights Reserved

7. Click an ID link to open the technique on the MITRE ATT&CK website.

Add MITRE techniques to a search

About this task

When you create or edit a search, you can associate MITRE techniques with it in the **MITRE Techniques** section of the search form. The section displays a grid of techniques organized by tactic with expandable sub-technique rows.

1. From the Main menu, go to **Modules** > **Threat Response** > **Threat Navigator**.
2. Create a new search or open an existing search to edit it.
3. In the **MITRE Techniques** section, use the **MITRE Technique** or **MITRE Tactics** filters to find techniques, or enter text in the search field.
4. (Optional) Click the expand arrow on a parent row to view sub-techniques.
5. Select the check box for one or more techniques or sub-techniques.
6. Run or save the search.

Result

The **MITRE Techniques** column on the searches list shows the techniques associated with each search. The **Version History** panel also records the MITRE techniques associated with each iteration of a search.

Manage MITRE techniques for multiple searches

About this task

Use the **Manage MITRE Techniques** modal to add or remove MITRE techniques for one or more searches at the same time.

1. From the Main menu, go to **Modules** > **Threat Response** > **Threat Navigator**.
2. Click the **Searches** tab.
3. Select one or more searches.
4. Click **Manage MITRE Techniques**.

©2026 Tanium Inc. All Rights Reserved

5. In the **All Items** tab, select the check box for each technique or sub-technique to add. Click the **Selected** tab to review or remove currently associated techniques.
6. Review the **Selection Preview** section at the bottom of the modal to confirm what will be added or removed across the selected searches.
7. Click **Save Changes**.

Add MITRE techniques to a hypothesis

About this task

When you create or edit a hypothesis, select MITRE techniques in the **Associated Items** section. The **MITRE Techniques** section uses the same grid as the **MITRE Techniques** tab, with expandable sub-technique rows and filters for technique name and MITRE ID. The metric bar in the **Associated Items** section shows the total count of items associated with the hypothesis, including the count of selected MITRE techniques.

1. From the Main menu, go to **Modules** > **Threat Response** > **Threat Navigator**.
2. Click the **Hypotheses** tab.
3. Click **Create**, or select an existing hypothesis and click **Actions** > **Edit**.
4. Provide a name and description.
5. In the **Associated Items** section, click **MITRE Techniques**.
6. Use the **MITRE Technique** or **MITRE ID** filters to find techniques, or enter text in the search field.
7. (Optional) Click the expand arrow on a parent row to view sub-techniques.
8. Select the check box for one or more techniques or sub-techniques.
9. Click **Create Hypothesis** or **Save**.

©2026 Tanium Inc. All Rights Reserved

Creating reactions

Reactions help to automate actions to disrupt and respond to attacks for both on and off-network endpoints and help reduce the time to remediate issues from hours to seconds. Reactions automate one or more actions on an endpoint based on alerts from intel documents (for example, delete one or more files, kill a process, or quarantine an endpoint). This is different than a response action where a Tanium platform action (Live Response, Quarantine, Download File, Gather Snapshot) runs on a single endpoint after the alert is received by the service and a manual action is run. All reactions occur directly on the endpoint immediately after an intel match occurs. Reactions take place even if the endpoint is not connected to Tanium server.

Reactions reduce the risk of attack by providing a critical advantage in managing security incidents. Reactions help remediate known threats within seconds of identifying them, allowing workflows to be much more efficient and reducing a bad actor's capability of stealing data, causing damage, or intruding further into an organization. Automated workflows such as reactions provide capabilities that have become a regulatory requirement in many countries.

Reactions are defined in the Threat Response workbench and associated with an intel document. You can create a reaction to define a workflow that will occur when an intel match occurs on an endpoint. The intel document defines what to act on, and the reaction defines what action or actions to perform.

Note: Reactions on detections inside ZIP files perform any relevant actions on the ZIP file itself.

Note: If a reaction is scoped to specific profiles and all of those profiles are deleted, the reaction is preserved but does not act on any endpoint. Associate the reaction with an active profile or change its scope to **All Profiles** to reactivate it.

Create a reaction

About this task

©2026 Tanium Inc. All Rights Reserved

Create a reaction in the Threat Response workbench.

> **Note:** Creating reactions in the Threat Response workbench requires the **Threat Response Intel Reaction Write** permission. If a custom role has**Profiles Write** but not **Threat Response Intel Reaction** write access, deleting a profile that removes the last binding on a reaction returns an error, even though the **Delete** action for the profile appears enabled. This occurs because removing the last bound profile requires write access to the reaction in addition to write access to profiles. To delete the profile, either grant the user **Threat Response Intel Reaction** write access, unbind the reaction from the profile first, or have a user with the required permissions perform the deletion. The Administrator and Operator roles include both permissions by default and are not affected.

The **Reactions** page displays a **Scope** column that shows how each reaction applies to profiles: **All Profiles**, a list of specific profile names, or **Selected Profiles** if you don't have read access to the bound profiles.

1. Select **Intel** > **Reactions**. Click **Create Reaction**.
2. In the **Details** section, provide a name and description for the reaction.
3. Select a **Scope** for the reaction: **All Profiles** to apply the reaction wherever the associated intel matches, or **Selected Profiles** to limit it to one or more profiles you have read access to. If you don't select a scope, the reaction applies to **All Profiles**.

   > **Note:** The **Scope** selector isn't available for reactions on built-in intel types that don't support custom reactions, such as Process Injection, Windows Defender, reputation, and Deep Instinct detections. It is also disabled, with the current value visible, when you edit a Tanium Managed (default) reaction — you cannot change the scope of a default reaction.

4. In the **Steps** section, add steps that define the actions to perform when intel matches occur on an endpoint. You can create a step for each type of available action. You cannot create a reaction that contains multiple steps with the same action type. The available actions are:

   Kill Responsible Process

   This action type provides the ability to automatically kill a process when an alert is initiated for an intel match based on custom criteria including hash, name, command line, parent process, and ancestry. In response to an alert, the action takes place immediately on the endpoint to allow the action to take place regardless if it communicating on the Tanium Server. **Kill Responsible Process** actions use the results returned as part of the Advanced Details for an alert to determine what artifact to act on,

©2026 Tanium Inc. All Rights Reserved

for example `processItem` in an IOC intel document.

When you select the **Kill Responsible Process** action, you can select to **Allow Signed Processes to be Killed** for either Windows or macOS endpoints. There are cases where killing a signed process is required. These settings are disabled by default to protect important processes such as `svchost`. **Allow Signed Processes to be Killed** enables you to create one reaction that does not kill OS signed binaries, and another version that you can use to kill OS signed binaries. For example, a **Kill Response Process** action does not kill a powershell.exe process in Windows unless you select this checkbox. Enable this setting for intel documents such as:

```
process.path ends with '\\powershell.exe' AND process.command_line contains '-ExecutionPolicy Bypass'
```

Kill Responsible Process actions act on all process items found in the intel document.

Quarantine Endpoint

This action type provides the ability to automatically quarantine an endpoint when an alert is initiated for an intel match. In response to an alert, the action takes place immediately on the endpoint to allow the action to take place regardless if it is communicating on the Tanium Server.



Important: Before assigning quarantine actions, ensure that all endpoints that are targets of the intel document that the reaction is associated with meet the Quarantining endpoints on page 317 documented in Quarantining endpoints.

When quarantining an endpoint that has already been quarantined, the quarantine action respects the existing quarantine. In such cases a quarantine is not removed and reapplied.

Select the quarantine profile that you want to use. Changes to the profiles or rules after a quarantine has been applied on an endpoint has no effect on that endpoint unless it is unquarantined and requarantined.



Note: Any alerts that had quarantine reactions associated with them from before the existence of quarantine profiles display as having a deleted quarantine profile.

©2026 Tanium Inc. All Rights Reserved

Delete Files Identified by Intel

This action type provides the ability to automatically delete a file when an alert is initiated for an intel match. In response to an alert, the action takes place immediately on the endpoint to allow the action to take place regardless if it is communicating on the Tanium Server. **Delete Files Identified by Intel** actions use the results returned as part of the Advanced Details for an alert as the artifacts to act on. You can use the **Delete Files Identified by Intel** action type to delete empty folders, but not folders that contain files or other folders, even if the folder or folders it contains are also empty. **Delete Files Identified by Intel** actions act on all file items found in the intel document, including any `fileItem` artifacts that are returned as a child of a `processItem` artifact.



Best Practice: Use caution when you assign a **Delete Files Identified by Intel** action to an intel document that matches on `processItem` artifacts. Because `processItem` alert data contains a secondary `fileItem` artifact that specifies the location of the binary on disk, `processItem` artifacts with a **Delete File Identified by Intel** action match on the secondary `fileItem` and delete the binary from disk.

When you select the **Delete Files Identified by Intel** action, you can select to **Preserve Copy of Files** to save a copy of the file in such a way that endpoint users can no longer execute the file, read the contents of the file, modify, or delete it. Files are preserved in a ZIP file on the endpoint. On the endpoint, the path to preserved files assumes the form of `[Tanium Client]/extensions/threatresponse/data/restricted/[Intel ID][Guid]/reaction-[ID][Step Number].zip`

The file contents of the ZIP file is encrypted. Decrypt files that you download with the password `infected`.



Important: **Delete Files Identified by Intel** actions that are associated with signals intel documents are not supported. If you need to delete specific files, use an OpenIOC or STIX intel document that alerts on a specific file name, or a YARA intel document that alerts on the contents of the file.

Delete Files

You can specify files to delete by pasting in a list of absolute paths that are separated by line breaks that you want to delete when an alert is initiated. You must specify file names

©2026 Tanium Inc. All Rights Reserved

as absolute paths. Quoting or escaping special characters is not required. Do not use quotes in these file paths unless they are actually part of the file name.

When you select the **Delete Files** action, you can select to **Preserve Copy of Files** to save a copy of the file in such a way that endpoint users can no longer execute the file, read the contents of the file, modify, or delete it. Files are preserved in a ZIP file on the endpoint. On the endpoint, the path to preserved files assumes the form of `[Tanium Client]/extensions/threatresponse/data/restricted/[Intel ID][Guid]/reaction-[ID][Step Number].zip`

The file contents of the ZIP file is encrypted. Decrypt files that you download with the password `infected`.

5. Click **Add Step**.
6. For each step that you add, provide a name and description for the step. Select an Action to perform, and select any additional settings that are available for the action.
7. When you have completed the workflow definition by adding steps to perform when an alert is initiated, click **Apply**.
8. Click **Create**.

Assign a reaction to an intel document

About this task

To cause the workflows that you define in a reaction to occur when an alert is initiated for an intel match, you need to assign the reaction to an intel document. Reactions continue to take action on endpoints even when alerts are throttled or intel is put into a reduced state on individual endpoints. The only way to disable a reaction is to delete the intel or remove the associated reaction and re-deploy intel. Alternatively you can disable the intel at an enterprise level by Intel safeguards on page 90.

1. Click **Intel** > **Documents** to locate an intel document that you want to assign a reaction to.
2. Select the intel document that you want to assign a reaction to and click **Edit**.
3. In the **Reaction** dropdown list, select the name of the reaction that you want to assign to the intel document.

©2026 Tanium Inc. All Rights Reserved

4. Select **Set reaction to audit mode** to view the impact of the reaction without any of the actions you assign in a reaction actually occurring. Audit mode enables you to validate that any response actions that are initiated as part of a reaction do not have an unintended impact on an environment. When you create a new intel document and assign a reaction, **Set reaction to audit mode** is enabled by default to provide a safeguard against unintended or untested actions. To perform reactions, this setting must be deselected.

   > **Note:** When you run an on-demand scan for intel that is associated with a reaction that is set to audit mode, you can select **Override Audit Mode for Reaction** in the on demand scan to override audit mode and perform the reaction on endpoints.

   > **Note:** If the reaction associated with the intel is scoped to specific profiles, **Set reaction to audit mode** is locked on for on-demand scans. Point to the locked checkbox for an explanation.

5. Click **Save**.

Result

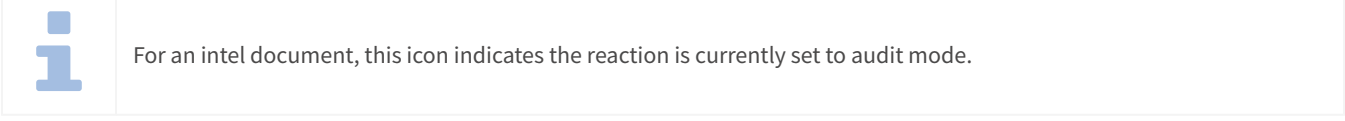
Reactions that you assign to intel documents take effect when the intel is deployed to the endpoint. Intel must be included in a Detection configuration to be applied to an endpoint.

> **Note:** When you duplicate an intel document, any reactions that you have assigned to the document that you are duplicating do not persist in the duplicate intel document.

An indepth overview of supported intel types and the specific intel artifacts that reactions act on, along with examples is available in the Threat Response Intel Support documentation. To access the Threat Response Intel Support documentation, click ? from the Threat Response overview page and click the Threat Response Intel Support tab.

Reaction statuses

The following reaction statuses for reactions are displayed in the Threat Response workbench for either intel documents or in the alerts results:



©2026 Tanium Inc. All Rights Reserved

	For an alert, this icon indicates that the reaction was set to audit mode at the time an alert was initiated.
	For an alert, this icon indicates the reaction completed successfully.
	For an alert, this icon indicates that a reaction has multiple steps and indicates that some steps completed successfully, but at least one step in the reaction failed. For example, if the reaction features a Quarantine Endpoint step, but the endpoints that the reaction targets do not meet the Quarantining endpoints on page 317 , this step would fail. Other steps on the reaction could succeed.
	For an alert, this icon indicates that all steps in the reaction failed to complete successfully.

You can view details regarding any reaction success or failure including the status of each step in a reaction in the alert details of an alert that was initiated by a match on an intel document a reaction is associated with. For more indepth reaction detail data, you can view the endpoint logs. For more information, see Collect troubleshooting information from endpoints on page 353.

Audit reaction data

Audit mode provides a means for the endpoint to report back to the service if a reaction would have been initiated and what actions it would have taken without actually taking those actions. Audit mode enables you to validate that any response actions that are initiated as part of a reaction do not have an unintended impact on an environment.

Note: Audit mode is specified at the intel document level. A reaction can be associated with multiple intel documents. By specifying audit mode at the intel document level, a reaction can be in audit mode for one or more intel documents, but not in audit mode for others.

©2026 Tanium Inc. All Rights Reserved

Analyzing context

Use context analyzer to help determine what normal looks like in your environment. It provides a baseline that you can use to detect anomalies against. Use context analyzer to reduce false positives and benign investigative leads by determining the significance of a particular artifact. If a file or process is a common occurrence, it is likely benign. However, if it represents a rare occurrence, it might be indicative of an issue that requires further investigation. Context analyzer is the first step in helping you gather actionable data quickly and accurately about the normal state of an environment. By understanding the typical patterns in a digital environment, you can better focus on anomalies that might pose a true threat.

Context analyzer provides visibility into the most recent activity for processes, files, IP addresses, and process hashes across all online endpoints. Using file at rest (Index) and historical (Recorder Database) data, context analyzer displays a visual summary of the data followed by a searchable details grid. A sampling of the most recent data from each endpoint is provided, which attempts to prioritize outliers on each endpoint.

Context analyzer queries all files at rest and historical data across every online endpoint, visualizes that data and provides “context” for how an artifact appears in an environment. Such context helps answer questions such as: “Is this artifact normal in my environment?” “Does it exist across just a few or thousands of endpoints?”, “Which users are typically associated with this artifact?", "Does this artifact have the same hash everywhere, or are their many different hashes?", and "Are there any obvious outliers associated with this artifact?".

When you query an artifact, the endpoints that you target return the most recent data available for each artifact. Each endpoint provides responses grouped according to hash, path, operating system, endpoint, and user. Context Analyzer automates the searching for you and returns results received at 95% completion or a maximum of four minutes.

As context analyzer focuses on the most recent activity for an artifact it is important to understand that it works best at identifying the “normality” of an artifact in an environment, and when searching for unique outliers across an enterprise. Context analyzer is not suited for attempting searches such as finding the single outlier in 1000 similar events on a single endpoint. Live Connect and sensors are still often best for that type of analysis or investigation. Context analyzer does not take the place of deployed Intel documents when you need the assurance of artifact existence or non-existence across an entire environment.

©2026 Tanium Inc. All Rights Reserved

Note: Full file path searches are not currently supported.

Example (A): UserA was executing process svcapp-init.exe on this endpoint. Context analyzer can tell you if this process is common across the environment and which users are typically running it.

Example (B): A powershell executable is found in what looks like a non-standard directory. Context analyzer can show you if this path is commonly used anywhere else for this binary, does this binary have a hash in common with other powershell binaries or is this hash unique, is this associated with any particular operating system, if it is being run frequently across the enterprise, and which users are running it.

Example (C): You are creating a new Intel document to help you detect a potential threat. Using context analyzer, you can quickly determine how common a file, hash, process name, or IP address is in the environment and if it would cause an excessive amount of false positive alerts.

Note: Time filters can be very useful in the combined view; however, you might need a very short window due to the quantity of events.

Analyze the context of artifacts

1. Select artifacts to examine from the **Gather Samples** bar on the Threat Response **Context Analyzer** page. Select one of the following values, provide an artifact of interest, select the computer groups to examine and click **Search**.
    - **File Name** - File Name analysis supports any text, Full file path searches are not currently supported.
    - **Hash** - Hash analysis does not support special characters.
    - **IP Address**- IP Address analysis supports valid IPv4 or IPv6 address forms.
    - **Process Name** - Process Name analysis supports any text.

      Note: The search terms that you use are literal terms. Regular expressions and wildcards are not supported.

©2026 Tanium Inc. All Rights Reserved

2. The Sampled Details section provides a list view of the endpoints on which a match has occurred. You can open a direct connection to the endpoint on which the match occurs. After opening a direct connection to an endpoint from a context analyzer result, the workbench displays all events that happened within one minute of the timestamp of the initially selected event.
3. (Optional) In the Sampled Details section, click **Add to an Investigation** in the Actions column to add the match to an investigation in Tanium Investigate. With Tanium Investigate you can identify the root cause of issues that arise on Tanium-managed endpoints and arrive at resolutions to issues more quickly. For more information, see Tanium Investigate User Guide.

Result

Note: Users who are assigned the **Threat Response Read Only User** role must have the **Interact Ask Dynamic Question** permission to use Context Analyzer. To add context analyzer data to an investigation, the **Investigate SHOW** and **Investigate Investigations WRITE** permissions are required.

You can decode encoded text in many places in the Threat Response workbench without having to copy and paste to a third-party tool. For example, you can decode all command line locations in the advanced details for a Threat Response alert.

For the steps to decode encoded text, see Decode encoded text on page 263.

Note: From any location in the Threat Response workbench, press `ALT + \` (Windows and Linux) or `Command + \` (macOS) to display the editor to decode encoded text. On some keyboards it is common for mappings to replace the / key (Scan Code 2B) with other characters, for example, the # character. On such keyboards, use the appropriate key combinations for the locale of the keyboard.

Export Context Analyzer results

1. From the Main menu, go to **Modules** > **Threat Response Context Analyzer**.
2. Select one or more items in the Sampled Details grid to export.
3. Click **Export**.
4. Click **Copy to clipboard** to copy the selected data to the clipboard. Click **Export to CSV** to export the selected data to a CSV file that is saved in the downloads directory of the web

©2026 Tanium Inc. All Rights Reserved

browser.

©2026 Tanium Inc. All Rights Reserved

Scanning endpoints

Threat Response scans each endpoint using the intel documents and Signals that you define. Scanning includes background scans, on-demand scans, and live Signals monitoring through the recorder. Background scans begin shortly after intel is deployed to the endpoint and continue on regular intervals. On-demand scans are initiated on demand, typically when you need to urgently locate all instances of a potential compromise.

A scan can have three possible results:

- **Match**: Identifies potential compromise and generates alerts.
- **No match**: None of the intel matched the data on the endpoints.
- **Inconclusive**: Generally, an indication that the scan did not complete for some reason.

When a scan finds a match, the alert is gathered from the endpoint and reported to Threat Response. From there, you can further investigate the endpoint.

The two available types of scans are background scans and on-demand scans. Background scans and on-demand scans are complementary; background scans are run on a schedule for all intel. On-demand scans are immediate; they are intended for scenarios such as testing or piloting new intel. In this way, you can test the results of specific intel with an on-demand scan and when the intel is revised appropriately to ensure it generates the intended alerts can be scanned on a routine basis through background scans.

Background and on-demand scans, regardless of the intel type, are throttled to ensure they do not overuse endpoint resources. All Tanium Client extensions in total consume no more than 5% of the available CPU resources on each endpoint.

On-demand scans that initiate endpoint throttling cause the endpoint to throttle background scan alerts for the effective period of the throttle, which is one hour by default.

Endpoint throttling does not initiate any system notifications. Server throttling continues to send notifications.

©2026 Tanium Inc. All Rights Reserved

Background scans

Background scans run continuously against intel. Threat Response actively acknowledges alerts when they are received. Alerts are not duplicated for the same artifact on the same endpoint.

To edit a detection configuration, see Creating configurations in Threat Response on page 144.

On-demand scans

About this task

On-demand scans send a single piece of intel to the endpoints for immediate matching and alert reporting. You can use Signals, OpenIOC, STIX, YARA, or reputation intel in an on-demand scan. There is no size limit of the intel document you can use for an on-demand scan, but be aware of the network impacts of sending large amounts of data for scanning.

For Signals, you can use on-demand scans for a seven day historical query on the event recorder database. On-demand scanning on Signals is also useful when you are authoring Signals.

1. From the Main menu, go to **Modules** > **Threat Response Intel**. Click an intel document.
2. From the intel document, click the three dots in the upper right and select **Start On-Demand Scan**.
3. Select **Override scan blockout windows** if you want the on-demand scan to ignore any configured scan blockout windows. Selecting this option forces the on-demand scan to execute on endpoints that are currently online. **Override scan blockout windows** requires the **Threat Response Override Scan** permission.
4. Select the computer groups you want the on-demand scan to target. Click **Start**.
5. When you run an on-demand scan for intel that is associated with a reaction that is set to audit mode, you can select **Override Audit Mode for Reaction** in the on-demand scan to override audit mode and perform the reaction on endpoints. For more information, see Create a reaction on page 130.
6. Click **Run**.
7. A new on-demand scan is initiated in the **On-Demand Scans** section of the intel document page. For each active on-demand scan you can view the number of alerts for the intel you are scanning for and the total number of online endpoints and the number of endpoints on

©2026 Tanium Inc. All Rights Reserved

which that the scan has completed. A completed scan indicates that the scan has been deployed to targeted endpoints and no additional endpoints will receive the scan. After a scan has completed, endpoints that the scan targets that might have been offline could come back online and report alerts. Each on-demand scan has an associated scan ID which is a six digit number. You can filter by scan ID on the **Alerts** tab of the intel document page to view alerts that are associated with the on-demand scan.

> **Note:** Results are limited to endpoints that are online, have an active Threat Response profile deployed, and are present in one or more of the computer groups you have targeted for the on-demand scan.

8. When an on-demand scan is complete, the results of the scan are available on the **On-Demand Scan History** tab of the intel document page. You can view historical on-demand scans and their results and preserve this data for auditing purposes.

Result

> **Note:** On-demand scans are action-based and require an approver if action approval is enabled. You can add the Threat Response content set to action approval bypass to allow action bypass for on-demand scans.

> **CAUTION:** On-demand scans of intel documents can generate a new alert for a condition or event that alerted in the past. This is expected behavior; each on-demand scan is a unique search activity. An example where this can occur is with Tanium Signals; if a signal is matched and alerts in real time, and the same signal document is later on-demand scanned, a second alert could be generated for the same event if the event falls within the seven day look-back period.

©2026 Tanium Inc. All Rights Reserved

Creating configurations in Threat Response

Overview

Configurations are groups of settings that control the behavior of Threat Response components. You can create different configurations for each Threat Response component to control how it performs on specific groups of endpoints.

For example, you might want to apply and scan for specific intel on one group of endpoints, but not other groups. Or, you might want to apply a subset of Threat Response capabilities to a group of endpoints. Use configurations to customize which intel to apply, how and when to evaluate intel, how to index file systems, which events to record on all the endpoints in an enterprise, and what event data to stream to an external destination.

You can orchestrate configurations for detection, the recorder, index, and stream in a profile that is assigned to one or more computer groups. You can import and export configurations to make them easy to apply to target groups of computers. Threat Response provides example configurations that feature the most common configuration settings for specific operating systems.

Create detection configurations

About this task

Detection configurations provide directions for scanning endpoints for intel matches. To avoid scanning important endpoints or to limit when detection is active, you can include blockout periods to prevent scans during those times.

1. From the Main menu, go to **Modules** > **Threat Response Management** > **Configurations**. Click **Create** > **Detection**.
2. In the **General Settings** section, provide a name and description for the detection configuration.
3. (Optional) In the **Engine Options** section, select **Use UTC instead of the local time on the**

©2026 Tanium Inc. All Rights Reserved

endpoint when calculating Scan Blockout.

4. In the **Engine Options** section, select the hours and days for the **Scan Blockout** period to stop scanning against available intel during the times you select.

5. Configure the **Settings**.
    a. (Optional) Select **Consume Deep Instinct Alerts** to enable Threat Response to consume Deep Instinct alerts and display alerts from Deep Instinct detection. Selecting **Consume Deep Instinct Alerts** requires the Deep Instinct agent to be running on the endpoint. By default this option is disabled.

    > **Note:** For the integration to work correctly, you must configure additional flags for the Deep Instinct Agent (D-Client) using the Deep Instinct CLI. For more information, see the Deep Instinct documentation or contact Deep Instinct support.

    b. (Optional) Select **Consume Deep Instinct Alerts** to enable Threat Response to consume Deep Instinct alerts and display alerts from Deep Instinct on endpoints. By default this option is disabled.
    c. (Optional) Select **Generate Deep Instinct Reactions** to have Threat Response treat Deep Instinct detections as reactions instead of standalone findings. By default, this setting is disabled.
    d. (Optional) Select **Consume Defender Alerts** to enable Threat Response to consume Defender alerts and display alerts from Defender on Windows endpoints. By default this option is disabled.
    e. (Optional) Select **Generate Defender Reactions** to have Threat Response treat Microsoft Defender detections as reactions instead of standalone findings. By default, this setting is disabled.

    > **Note:** Enabling **Generate Defender Reactions** for a profile overrides the global `processActionsAsPrimaryFindings` setting for that profile: a single Defender malware-action event produces either an alert or a reaction, not both.

    f. (Optional) Select **Consume Process Injection Alerts** to enable Threat Response to consume Process Injection alerts. Selecting **Consume Process Injection Alerts** requires configuring the Process Injection intel document. For more information, see Configure process injection on page 100. By default this option is disabled.
    g. (Optional) Select **Consume Reputation Alerts** to enable Threat Response to consume Reputation alerts.
    h. Specify a value (in days) for **Initial Lookback**. The initial lookback value that you

©2026 Tanium Inc. All Rights Reserved

provide defines the number of days in the past to look in the Recorder database for matching.

6. (Optional) In the **Advanced Settings** section, specify a value for the **YARA File Size** or accept the default. This corresponds to the maximum size of file YARA can scan. (Default: 32 MB). YARA File Size and YARA Process Size do not apply to On-demand Scans. The values you provide in these fields are used by detection configurations for continuous data scanning.
7. (Optional) In the **Advanced Settings** section, specify a value for the **YARA Process Size** or accept the default. This corresponds to the maximum size of the process YARA can scan. (Default: 256 MB). YARA File Size and YARA Process Size do not apply to On-demand Scans. The values you provide in these fields are used by detection configurations for continuous data scanning.
8. In the **Intel** section, click **Add Intel**. Select the intel you want to add. Click **Add**.
9. Select Intel that you have added to Threat Response. Click **OK**. Click **Save**.

Result

Important: Changes you make to the intel that is included in a detection configuration do not take effect until the next intel deployment.

After you have deployed detection configurations to endpoints, you can view and manage findings that result from intel matches. For more information, see Managing Threat Response alerts on page 262.

Create index configurations

About this task

Use an index configuration to detect and report threat indicators for files at rest. Index creates an index of local file systems, computes file hashes, and gathers file attributes and magic numbers in an SQLite database on the endpoint. Index returns the files that are contained in zip archives. For more information about Index configuration settings, see Client Index Extension User Guide.

©2026 Tanium Inc. All Rights Reserved

Note: To accommodate architectural changes made to Index, when upgrading to the latest version of Threat Response, existing Index exclusions and **Hash Types to Calculate** are migrated from each legacy Index configuration into a new Index configuration with a matching name. If legacy Index configurations were attached to a Threat Response profile, the corresponding new Index configurations are added to that profile.

Index configurations determine how file indexing and hashing occur on the local file systems of endpoints. Index is optimized to minimize endpoint resource use and work with journaled file systems, when available.

Note: Legacy Index versions must be removed from endpoints before you deploy new Index configurations. For more information about removing legacy Index versions, see Upgrade the Threat Response version on page 66.

1. From the Main menu, go to **Modules** > **Threat Response Management** > **Configurations**. Click **Create** > **Index**. Provide a name and description for the index configuration.
2. Select the **Hashes To Calculate**. Index can record any combination of four different hash types: MD5, SHA1, SHA256, or SHA512. Do not select any hash type to disable calculation of hashes. You can select the following data to record to the index database:
    - **Magic Number** - The magic number is the first 4 bytes of the file. You can use the magic number to identify many types of files. Magic Number shows as selected if you select any hash type. If you select any hash type, you cannot deselect Magic Number.
    - **File Version Info** - File version information writes information such as product name and version, the file version, company name, a description, language, and orignal filename (if available) to the index database.
    - **Signature Data** - Signature data writes information such as timestamp, status, the issuer of a signature and subject to the index database.

    Note: If legacy index configurations included the **Include Malicious Hash List** setting, you must add the new Reputation intel document to intel configurations. When you upgrade to Threat Response 3.4 or later, any malicious hashes that exist in the reputation database are added to the Reputation Intel document. All malicious hashes identified after upgrade are added to this same intel document moving forward. Open each detection configuration and ensure that the Reputation source is added anywhere you want endpoints to match against the malicious hashes.

©2026 Tanium Inc. All Rights Reserved

3. (Optional) In the **Advanced Settings** section, change the default values for the following settings:

   High Priority Path Scan Fail-Safe Frequency

   Use high priority path scan fail-safe frequency to receive more frequent updates for files in certain regions of the disk. In addition to the baseline disk scan, you can specify high priority paths that use recorder events to update data. (Default: 24 hours). High Priority Paths are indexed more frequently. Performance impacts on the endpoint increase with the frequency of indexing and the size of the path. Using the root directory as a High Priority Path is discouraged as this can quickly consume resources.

   Index Scan Frequency

   Threat Response uses Index to scan the entire disk on an endpoint at regular intervals that typically occur between once a day and once a week. Index does not use recorder events to update file data across the entire disk. Enter a value for how often the Index scan runs. (Default: 7 days).

   Index First Scan Distribute Over Time

   The delay time after Index starts before starting the initial index scan. (Default: 24 hours).

   File Filters by Regular Expression

   File names to skip when calculating hashes, written in regular expression format. A filtered file may still be hashed if another subscription requests it. For example: ".*\.docx" matches any file with a .docx extension. Place each regular expression on a new line.

   Directory Filters by Regular Expression

   Paths to skip when scanning, written in regular expression format. Files under a filtered directory may still be indexed if another subscription requests them. For example: "C:\\Program Files \(x86\)\\Tanium\\Tanium Client" matches the Tanium Client install directory on Windows. Place each regular expression on a new line.

4. In the **High Priority List** section, select filters that you want to designate as high-priority paths. See Create filters on page 164 for more information. Click **Manage Priority List** to select existing filters. Select any or all of the available filters. Only filters that have already been created are available to select. When you have selected the filters that you want to add to the configuration, click **Apply**. See Create filters on page 164 for more information about filter methods. Click **Save**. You cannot add more than 24 filter definitions.

5. Click **Save**.

6. Click **Create**.

©2026 Tanium Inc. All Rights Reserved

Result

After you have deployed index configurations to endpoints, you can use sensors to query indexed files. See Reference: Sensors on page 408

Create indexing exclusions

About this task

Important: * = Starting in Tanium Client Management version 1.12.132, you add Index exclusions that apply globally to all Tanium solutions that use Tanium Index. Exclusions that you add in Tanium Client Management are not visible in the list of exclusions that you set in Tanium modules; it is important to view the exclusions in both locations to understand the total exclusions that are applied to the Tanium environment. For more information, see Create and deploy an Index configuration.

Create recorder configurations

About this task

The recorder saves forensic evidence for each endpoint in a local database. With recorder configuration settings, you can restrict database volume by size and days of storage.

Adjust the settings for each endpoint database to suit a specific environment. Systems with different roles can generate a higher volume of certain types of events. For example, domain controllers typically generate more security events and network traffic than an average end-user workstation. You can build custom configurations that maximize event retention across an environment, while excluding unwanted activity. Starting in Threat Response 3.5, recorder configurations that target Windows endpoints require the Tanium Driver to be installed and enabled to record process and command line events. The Tanium Driver is installed as part of Threat Response and is upgraded when Threat Response upgrades are applied.

1. From the Main menu, go to **Modules** > **Threat Response Management** > **Configurations**. Click **Create** > **Recorder**. Provide a name and description for the recorder configuration.
2. In the **Database Configuration** section, configure settings for the recorder database. The recorder database contains configuration data, signal match data, and configured event data. The events of a signal match are always written to the database, and override any filters that

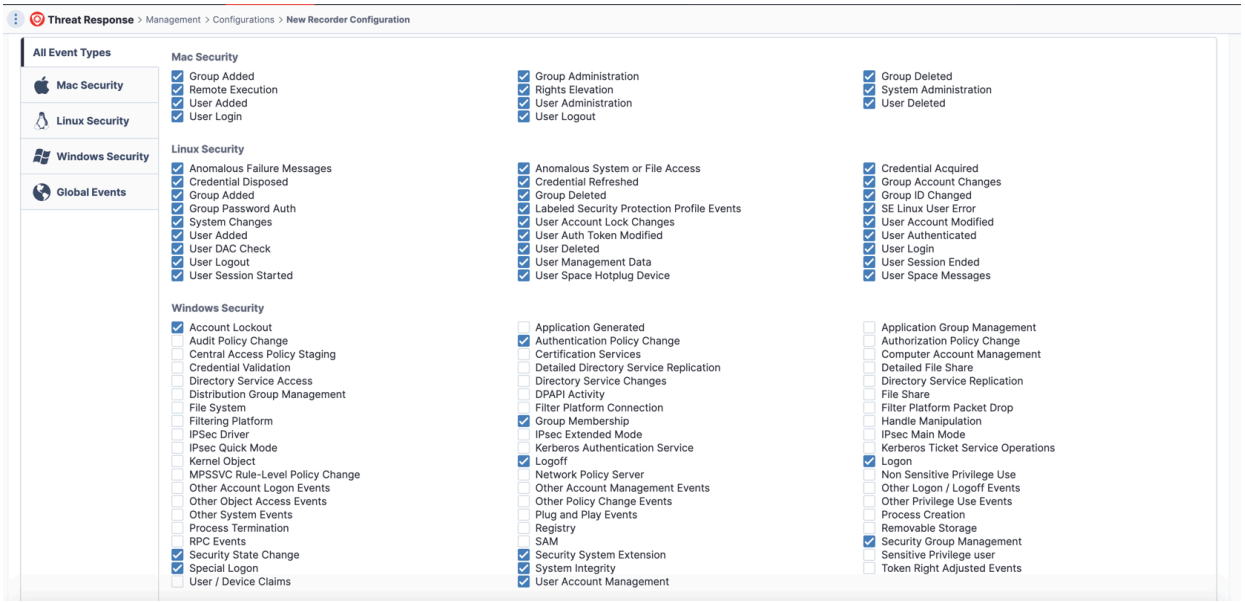
©2026 Tanium Inc. All Rights Reserved

are included in a recorder configuration.

a. Provide a **Maximum Database Size**. The endpoint purges events if the maximum database size is reached. If this database is larger than 2.5 GB, you cannot reimport the database if it is exported.
b. Provide the **Maximum Days to Retain Events** to specify the number of days that events are retained. Older events are purged from the endpoint database. Entering 0 prevents events from being purged based on age.
c. Select whether or not to **Record Tanium Client Processes**. Selecting this option includes all Tanium Client processes, and all child process of Tanium Client in recorded events.
d. Select whether or not to **Encrypt Database**. By default, the recorder database (recorder.db) is encrypted using AES 128 bit encryption. Deselect the database encryption setting if you do not want this data to be encrypted. Deselecting this setting does not revert any encrypted databases to a decrypted state. If changing an endpoint to a decrypted state, change the configuration, deploy the updated profile, and then deploy an action to the endpoints with `Recorder - Reset Database`. After the reset action is complete, the recorder.db exists in a decrypted state.

> **Note:** If encryption is enabled, a recorder database cannot be decrypted offline.

3. In the **Recorded Events** section, select the types of events to record for the current configuration.



©2026 Tanium Inc. All Rights Reserved

Security Events

Security events include events such as authentication, privilege escalation, and more. This event type includes logon events, even if operating system logs have rolled. For Linux security events, see https://github.com/linux-audit/audit-userspace/blob/master/lib/libaudit.h for more information about specific event IDs. For Windows security events, see https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-auditing-faq for more information about specific event IDs. More information about event IDs is available in the Recorder Security Event Details documentation. To access the Recorder Security Event Details documentation, click ? from the Threat Response overview page and click the Recorder Security Event Details tab.

Global Events

Event types under global events do not apply the same across operating systems. When a global event is disabled, events are not recorded unless they are associated with an applied signal. To preserve all intel alert context, even partial match events related to an intel document are recorded.

Database event filters do not apply for event types that are globally disabled. To filter recorded events associated with intel alerts, that event type must be enabled in the Threat Response Database configuration. For example, to prevent image load events from being recorded, you must enable image load events, and filter them appropriately.

Global events contain the following:

- **Registry**

  [Windows only] Changes to the registry, such as the creation or alteration of registry keys and values. Includes the associated process and user context.

- **Network**

  Network connection events, such as an HTTP request to an internet location, including the associated process and user context. Events are recorded for all inbound and outbound TCP connections.

- **Process**

  Process events, such as path, hash, command line, user information, ancestry, and the signed status of a process.

©2026 Tanium Inc. All Rights Reserved

- File

  File system events, such as files written to directory locations on the endpoint. The associated process and user context are included. Examples: A malware file copied to a location that Windows Update uses, or content changes made to a file.

- DNS

  [Windows 8.1 or later and Linux endpoints where eBPF is enabled] Request information, including the process path, user, query, response, and the type of operation. On Windows and Linux endpoints where eBPF is enabled, DNS events are only recorded when you use the system DNS client. DNS events for applications that use their own DNS client are not recorded (for example, nslookup and Google Chrome). On Linux endpoints eBPF-based DNS recording generates one event per resolved address. A single DNS resolution that returns multiple addresses produces multiple DNS events.

- Image Loads

  [Windows only] Returns historical data from each endpoint regarding image loads; for example, the full path and hash, the entity that signed an image, or a designation of "Unsigned" if the image is not signed. A possible example is the loading of an unsigned DLL. If you do not select Image Loads, any signal that uses the image event type results in an Unmatched Events warning in the Alert Details. Selecting Image Loads filters for image and process.path is not 'system'. Selecting Image Loads does not apply filters for Linux or Mac endpoints.

  Note: Note: The driver load view in recorder is categorized as an image load ending in .sys and originating from PID 4 (SYSTEM). Driver load events display in the image load event view and therefore image load events might be displayed on Linux and Mac endpoints. While there is no support for image loads on Linux and Mac endpoints, driver load events such as these are presented as image loads.

- Driver Loads

  Returns historical data from each endpoint regarding driver loads; for example, the full path and hash of a driver. By default, Driver Load events

©2026 Tanium Inc. All Rights Reserved

are not selected. Selecting Driver Loads on Windows filters for `image` and `process.path is 'system'`. Selecting Driver Loads on Linux or macOS filters for `image`.

- HTTP headers

  [Windows only] Returns HTTP header information from connections on endpoints including the time connections occurred, the connection ID of the connection, the remote (destination) address, and the header name and value.

  Important: When using HTTP headers as recorded events, be aware that CPU usage on endpoints is impacted; especially on servers. When capturing HTTP headers as recorded events, ensure that you are monitoring the performance impacts on the endpoints from which they are captured and tune their collection appropriately.

4. In the **Filters** section, click **Manage File Filters** to select existing filters. Select any or all of the available filters. Only filters that have already been created are available to select. See Create filters on page 164 for more information about filter creation. When you have selected the filters that you want to add to the configuration, click **Apply**. In the **Filters** section, designate the method you want to apply for each set of filters. Select either **Include** or **Exclude**. See Create filters on page 164 for more information about filter methods.
5. (Linux only) In the **Custom Audit Rules (Linux Only)** section, add **Custom Audit Rules**. Provide custom audit rules for use on Linux endpoints. Audit rules are provided to the auditd service and are in the following format: `-a exit,always -S adjtimex -S settimeofday -k time_change` . You can provide up to 500 custom audit rules.

   Note: By default eBPF is enabled on supported endpoints. When eBPF is enabled, any custom auditd rules that you have added to a Recorder configuration are not used. To disable eBPF, use the CX.recorder.BPFEnableBPF configuration setting and set the value to "0". For more information, see the Client Recorder Extension User Guide.
6. Click **Save**.

Result

©2026 Tanium Inc. All Rights Reserved

After you have deployed recorder configurations, you can view events that occur on the endpoints where you have applied the configuration. For more information, see Direct connecting to endpoints and exploring data on page 189.

Create stream configurations

About this task

Stream provides the ability to send rich endpoint data from the recorder to an external destination. This raw data includes process, network, file, driver events that you can use to investigate incidents, enrich other workflows, or perform custom analytics. Stream configurations enable you to specify and filter recorder events for the endpoints in an environment, and provide instructions for exporting - or streaming - these events directly to an SIEM for analysis in JSON format. For example, you can specify that all network events with one or more filters be streamed to Chronicle, Microsoft Sentinel, Splunk, Elastic, or Syslog. Tanium customers use this data to solve critical data gaps and Tanium Partners leverage this data to build their own security programs.

1. From the Main menu, go to **Modules** > **Threat Response Management** > **Configurations**. Click **Create** > **Stream**. Provide a name and description for the stream configuration.
2. Select a **Management Method**. You can manually provide configuration parameters, or upload a JSON file with configuration parameters for a stream configuration. Select either **Manual** or **File Upload**. If you select **File Upload**, click **Browse for File** and select a JSON file to upload. The JSON file contains the configuration parameters for the stream configuration. If you select **Manual**, complete the following tasks.
3. In the **Configuration** section, select a **Destination Type**. The **Destination Type** you select determines the additional required configuration settings that you are prompted to provide. When you select a destination type and provide configuration information for that specific destination type, you cannot change the destination type.
   Chronicle
   - Namespace - A namespace consists of a label part and a UUID. If a namespace label does not exist, then using it will create a new namespace with that label and a random UUID.
   - Chronicle Configuration URL - The URL to configure Chronicle. The provided URL must be complete and begin with `HTTPS://`
   - API Key - The API key that is used to authenticate calls.

©2026 Tanium Inc. All Rights Reserved

- Customer ID - The Chronicle customer ID for your environment.

ELK

- URL - The URL for Logstash HTTP input.
- Enable Transport Layer Security (TLS)

  (Optional) - Select Enable Transport Layer Security (TLS) to use a secure connection to transmit data to the destination. This ensures that the data is encrypted and authenticated between the sender and the receiver. If you select Enable Transport Layer Security (TLS) you must provide the following details:

  - Server Verification - Specify the type of authentication to use with the destination for TLS. Select one of the following:

    - Use Internal Certificate Authority (CA) Certificates

      - Verifies server identity using a built-in set of CA certificates that Stream maintains, based on the Mozilla root CA trust store. Use this option when the server presents a certificate issued by a publicly trusted CA.

    - Disable Certificate Verification

      - Turns off all server identity checks, which can expose connections to security vulnerabilities. Use this option only in lab or development environments where certificates are not yet configured.

    - Upload PEM-formatted Certificate Authority (CA) Certificate

      - Verifies server identity using a specific CA certificate that you provide. Use this option when the server uses a certificate that Stream cannot verify using its built-in CA list.

  - Client Verification

    - Specify the type of authentication to use for the client.

      - None - Select this option to not require client verification.

©2026 Tanium Inc. All Rights Reserved

- Upload Certificate and Key

  - Select this option to specify a certificate and key that are used to verify the identity of the client. If you select this option, browse to a certificate and a PEM file to upload to the destination and provide a passphrase that corresponds to the certificate.

HTTP/HTTPS

- URL - The URL for the HTTP or HTTPS endpoint.
- Enable Transport Layer Security (TLS)

  (Optional) - Select Enable Transport Layer Security (TLS) to use a secure connection to transmit data to the destination. This ensures that the data is encrypted and authenticated between the sender and the receiver. If you select Enable Transport Layer Security (TLS) you must provide the following details:

  - Server Verification - Specify the type of authentication to use with the destination for TLS. Select one of the following:

    - Use Internal Certificate Authority (CA) Certificates

      - Verifies server identity using a built-in set of CA certificates that Stream maintains, based on the Mozilla root CA trust store. Use this option when the server presents a certificate issued by a publicly trusted CA.

    - Disable Certificate Verification

      - Turns off all server identity checks, which can expose connections to security vulnerabilities. Use this option only in lab or development environments where certificates are not yet configured.

    - Upload PEM-formatted Certificate Authority (CA) Certificate

      - Verifies server identity using a specific CA certificate that you provide. Use this option when the server uses a certificate that Stream cannot verify using its built-in CA list.

©2026 Tanium Inc. All Rights Reserved

- Client Verification

  - Specify the type of authentication to use for the client.

    - None - Select this option to not require client verification.

    - Upload Certificate and Key

      - Select this option to specify a certificate and key that are used to verify the identity of the client. If you select this option, browse to a certificate and a PEM file to upload to the destination and provide a passphrase that corresponds to the certificate.

- (Advanced setting) HTTP Payload Encoding - Select the encoding format for streamed data. Select **Plain** to send uncompressed data, or select **Gzip** to send compressed data.

- (Advanced setting) HTTP Headers - Add custom HTTP headers as key/value pairs to include with each request. After you save the configuration, header names remain visible but values are hidden. To change a value, enter a new one. To remove a header, delete its row before saving the update. The **Content-Type: application/json** header is included by default. Headers with empty keys are not included in requests.

Microsoft Sentinel CEF

- Host/IP - The hostname of IP address of the AMA log forwarder.

- Port Number - The numeric value for the syslog port which must be less than or equal to 65535. Only numeric values are allowed.

- Enable Transport Layer Security (TLS)

  (Optional) - Select Enable Transport Layer Security (TLS) to use a secure connection to transmit data using Syslog over TLS (Transport Layer Security) to the destination. This ensures that the data is encrypted and authenticated between the sender and the receiver. If you select Enable Transport Layer Security (TLS) you must provide the following details:

  - Server Verification - Specify the type of authentication to use with the

©2026 Tanium Inc. All Rights Reserved

destination for TLS. Select one of the following:

- Use Internal Certificate Authority (CA) Certificates

  - Verifies server identity using a built-in set of CA certificates that Stream maintains, based on the Mozilla root CA trust store. Use this option when the server presents a certificate issued by a publicly trusted CA.

- Disable Certificate Verification

  - Turns off all server identity checks, which can expose connections to security vulnerabilities. Use this option only in lab or development environments where certificates are not yet configured.

- Upload PEM-formatted Certificate Authority (CA) Certificate

  - Verifies server identity using a specific CA certificate that you provide. Use this option when the server uses a certificate that Stream cannot verify using its built-in CA list.

- Client Verification

  - Specify the type of authentication to use for the client.

  - None - Select this option to not require client verification.

  - Upload Certificate and Key

    - Select this option to specify a certificate and key that are used to verify the identity of the client. If you select this option, browse to a certificate and a PEM file to upload to the destination and provide a passphrase that corresponds to the certificate.

- Message Severity

  - Select the logging severity that Stream uses for output data. You must configure the Microsoft Sentinel data collection rule to have a minimum logging severity level that is lower or the same as the value you specify.

©2026 Tanium Inc. All Rights Reserved

- Message Facility

  - Select the logging facility that Stream uses for output data. You must configure the Microsoft Sentinel data collection rule to observe this facility.

> **Note:** For more information about message facilities, message severities, and data collection rules, see https://learn.microsoft.com/en-us/azure/sentinel/connect-cef-syslog-ama?tabs=portal#select-facilities-and-severities.

Splunk HEC

- URL - The URL to access the Splunk REST API.
- Authorization Token - The authorization token to access your Splunk environment. Do not include the `Splunk` prefix in this token.
- Disable Certificate Validation (Less Secure) - Select to disable the validation of the certificate presented by the destination. By default certificate validation is performed.
- Enable Transport Layer Security (TLS)

  (Optional) - Select Enable Transport Layer Security (TLS) to use a secure connection to transmit data to the destination. This ensures that the data is encrypted and authenticated between the sender and the receiver. If you select Enable Transport Layer Security (TLS) you must provide the following details:

  - Server Verification - Specify the type of authentication to use with the destination for TLS. Select one of the following:

    - Use Internal Certificate Authority (CA) Certificates

      - Verifies server identity using a built-in set of CA certificates that Stream maintains, based on the Mozilla root CA trust store. Use this option when the server presents a certificate issued by a publicly trusted CA.

    - Disable Certificate Verification

©2026 Tanium Inc. All Rights Reserved

- Turns off all server identity checks, which can expose connections to security vulnerabilities. Use this option only in lab or development environments where certificates are not yet configured.

- Upload PEM-formatted Certificate Authority (CA) Certificate

  - Verifies server identity using a specific CA certificate that you provide. Use this option when the server uses a certificate that Stream cannot verify using its built-in CA list.

- Client Verification

  - Specify the type of authentication to use for the client.

    - None - Select this option to not require client verification.

    - Upload Certificate and Key

      - Select this option to specify a certificate and key that are used to verify the identity of the client. If you select this option, browse to a certificate and a PEM file to upload to the destination and provide a passphrase that corresponds to the certificate.

Splunk TCP

- Host - The fully-qualified Splunk host domain name or IP address.

- Port - The port for the stream communication to the host.

Syslog

- Host - Provide the fully-qualified host domain name or IP address.

- Port - Provide the port for stream communication to the host.

- Enable Transport Layer Security (TLS) (Optional) - Select Enable Transport Layer Security (TLS) to use a secure connection to transmit data using Syslog over TLS (Transport Layer Security) to the destination. This ensures that the data is encrypted and authenticated between the sender and the receiver. If you select Enable Transport Layer Security (TLS) you must provide the following details:

©2026 Tanium Inc. All Rights Reserved

- Server Verification - Specify the type of authentication to use with the destination for TLS. Select one of the following:
    - Use Internal Certificate Authority (CA) Certificates

      - Verifies server identity using a built-in set of CA certificates that Stream maintains, based on the Mozilla root CA trust store. Use this option when the server presents a certificate issued by a publicly trusted CA.

    - Disable Certificate Verification

      - Turns off all server identity checks, which can expose connections to security vulnerabilities. Use this option only in lab or development environments where certificates are not yet configured.

    - Upload PEM-formatted Certificate Authority (CA) Certificate

      - Verifies server identity using a specific CA certificate that you provide. Use this option when the server uses a certificate that Stream cannot verify using its built-in CA list.

- Client Verification - Specify the type of authentication to use for the client.
    - None - Select this option to not require client verification.

    - Upload Certificate and Key - Select this option to specify a certificate and key that are used to verify the identity of the client. If you select this option, browse to a certificate and a PEM file to upload to the destination and provide a passphrase that corresponds to the certificate.

- (Advanced setting) Format - Select either Common Event Format or JSON.

- (Advanced setting) Message Severity - Select the logging severity that Stream uses for output data.

- (Advanced setting) Message Facility - Select the logging facility that Stream uses for output data.

©2026 Tanium Inc. All Rights Reserved

- (Advanced setting) Message Format - Provide a custom syslog message format. If you leave this value empty, messages use the default format. The default format is: <{PRI}>{VERSION} TIMESTAMP {HOSTNAME} {APP-NAME} {PROCID} {MSGID} MESSAGE

JSON over TCP

- Host - The fully-qualified host domain name or IP address.
- Port - The port for the stream communication to the host.
- Enable Transport Layer Security (TLS) (Optional) - Select Enable Transport Layer Security (TLS) to use a secure connection to transmit data to the destination. This ensures that the data is encrypted and authenticated between the sender and the receiver. If you select Enable Transport Layer Security (TLS) you must provide the following details:
    - Server Verification - Specify the type of authentication to use with the destination for TLS. Select one of the following:
        - Use Internal Certificate Authority (CA) Certificates

          - Verifies server identity using a built-in set of CA certificates that Stream maintains, based on the Mozilla root CA trust store. Use this option when the server presents a certificate issued by a publicly trusted CA.

        - Disable Certificate Verification

          - Turns off all server identity checks, which can expose connections to security vulnerabilities. Use this option only in lab or development environments where certificates are not yet configured.

        - Upload PEM-formatted Certificate Authority (CA) Certificate

          - Verifies server identity using a specific CA certificate that you provide. Use this option when the server uses a certificate that Stream cannot verify using its built-in CA list.

    - Client Verification - Specify the type of authentication to use for the

©2026 Tanium Inc. All Rights Reserved

client.

- None - Select this option to not require client verification.
- Upload Certificate and Key - Select this option to specify a certificate and key that are used to verify the identity of the client. If you select this option, browse to a certificate and a PEM file to upload to the destination and provide a passphrase that corresponds to the certificate.

Local File

- Directory - Enter an absolute path for the output directory on the endpoint.
- File Name - Provide a base file name for the files that contain streamed data. For example if you provide test.csv, the file is renamed test0.csv when the file size reaches the Max Size value. The file rotates to use higher-and-higher numbers until the number of files reaches the Max Number of Files value.
- Max Size - The maximum size in MB of the file before it rotates.
- Max Number of Files - The maximum number of files to keep.

4. Select **Dry Run** if you want to collect statistics about the data that would be streamed to the destination, but not actually send data.

   Best Practice: By default, **Dry Run** is enabled when you create a stream configuration. Analyze the amount of event data that would be streamed to a destination before you deselect **Dry Run**. While this setting is enabled, no data is streamed to a destination; it must be disabled for data streaming to occur.

   You can use the Threat Response - Daily Stream Stats sensor to gain an understanding of the amount of data that would be sent.

5. Select **Filter Tanium Processes** to filter all Tanium Client processes, and all child processes of Tanium Client in the recorded events. For example, if Tanium Client starts Python to run a sensor, this is filtered from the recorded events.
6. (Optional) If you want to use a proxy to provide a gateway, provide the host, port, and a username and password for the proxy. This setting is not available for all destination types.
7. In the **Event Types** subsection, select the event types that you want to stream. For more

©2026 Tanium Inc. All Rights Reserved

information about event types, see Create recorder configurations on page 149. At least one event type is required.

8. In the **Filters** section, click **Manage Filters** to add filters to use in the stream configuration. Only filters that have already been created are available to select. See Create filters on page 164 for more information about filter creation. When you have selected the filters that you want to add to the configuration, click **Apply**. In the **Filters** section, designate the method you want to apply for each set of filters. Select either **Include** or **Exclude**. See Create filters on page 164 for more information about filter methods.
9. Click **Save**.

Create filters

About this task

Filters provide a way to define the event information to record to reduce performance impacts and enable quick event identification. Filters are applied in high priority paths, recorder configurations, stream configurations and are created for specific types of recorder events. Threat Response provides a default set of filters for each type of recorder event that you can use in configurations. You can also create your own filters. You can either include or exclude filters. The **Include** method of filtering enables you to replace the default filter to only include the filters you specify to reduce performance impact and enable quick event identification. The **Exclude** method of filtering prevents events that match the criteria you provide from recording.

Filters are constructed in signals syntax. You cannot have more than 55 unique terms in a signal.

If a configuration enables process, file and network event types but an include filter only includes process events. No file or network events are recorded. When using an include filter for network events, the associated process events are automatically included.

1. From the Main menu, go to **Modules** > **Threat Response Management** > **Filters**. Click **Create**.
2. Select a **Filter Type**.
   File
   File filters define criteria for files to record when path or operation values match.

   High Priority Path
   Threat Response uses Index to scan the entire disk on an endpoint at regular intervals

©2026 Tanium Inc. All Rights Reserved

that typically occur between once a day and once a week. Index does not use recorder events to update file data across the entire disk. It is common to want more frequent updates for files in certain regions of the disk. To provide this visibility, in addition to the baseline disk scan, Threat Response enables you to specify high priority paths that use recorder events to update data and also scans every 24 hours by default. To change the default setting:

a. From the Main menu, click **Modules** > **Threat Response** to open the **Threat Response Overview** page.

b. Click Settings and open the **Service** tab.

c. In the Misc section provide a value (in hours) for the **High Priority Path Scanning for Index Configurations (Hours)** setting.

d. Click **Save**.

A high priority path must include a file.path starts with clause in Tanium signal syntax. Escape backslash characters in paths. For example, use C:\\Users\\Administrator to make C:\Users\Administrator a high profile path.

- Supported: file.path starts with 'C:\\Users\\Administrator'
- Unsupported: file.path starts with 'C:\'

A high priority path, in addition to the file.path starts with clause, can additionally specify one or more file.path ends with clauses to narrow the file types to inspect.

- Supported: file.path starts with 'C:\\Users\\Administrator' and file.path ends with '.dat'
- Supported: file.path starts with 'C:\\Windows\\System32' and file.path ends with '.dll' and file.path ends with '.exe'
- Unsupported: file.path ends with '.dat'

Image

Image filters define criteria for image events to record when path, hash, or signature values match.

©2026 Tanium Inc. All Rights Reserved

Network

Network filters define criteria for network events to record when a match is made for a defined IP address, port, or DNS query.

Process

Process filters exclude events based on criteria such as the process path, hash, user name, user group, or command-line to filter out a process. Process filters do not exclude child processes from being recorded. Use an ancestry filter statement to exclude child processes.

> **Note:** If you have a process-based filter, but that process spawns child processes, it is expected that the process that matches the process filter will still be recorded to ensure complete process trees. However, events for the process (for example, file events) that match the process filter are not recorded. Additionally, a process matching a process filter can also be recorded to ensure completeness of data, if there is a Signal match that contained the filtered process.

Registry

Registry filters define criteria for Windows registry events to record when specific key-value pairs match.

System (Windows and Linux only)

System filters provide paths of files to match or filter from the Linux audit daemon (auditd) logging. On Windows endpoints, system filters exclude particular processes from having the Tanium Driver inject into them for API monitoring and process injection monitoring. On Linux endpoints, system filters completely blind the recorder from any activity from the defined path, for example, process launches. When eBPF is enabled, any system filters that you have added to a recorder configuration are not used. To disable eBPF, use the CX.recorder.BPFEnableBPF configuration setting and set the value to "0". For more information, see the Client Recorder Extension User Guide. Because system filters filter content from auditd, other auditd consumers will also be blind to this path, not just the recorder.

3. Select an **Operating System**. Provide a name and description for the filter.
4. In the **Filter Definition** section, click **Filter Builder**.
5. Click **Row** or **Grouping** to add a filter definition using the filter builder. Select a type, a property, and condition. The available properties and conditions differ for each filter type.

©2026 Tanium Inc. All Rights Reserved

You can use properties and conditions to create logical patterns for matching specific events. You can add multiple statements to each filter. For each statement that you add, specify a logical and or a logical or to define the relationship of the statements in a filter. The following table provides a reference for properties and conditions for each filter type.

Properties and conditions for filters

Type	Property	Supported Conditions	Comments
File	operation	is is not	One of create , write , `open_write` , rename , permissions , or delete . **Note:** `open_write` is only relevant on endpoints that rely on auditd. **Note:** The `rename` operation corresponds to the `move` operation in the recorder events view.
	path	is is not contains contains not starts with starts with not ends with ends with not matches matches not	The full path to the file.
Process	path	is is not contains	The full path to the process executable. Process filters do not exclude child processes from being recorded. Use an ancestry filter statement to exclude child processes.

©2026 Tanium Inc. All Rights Reserved

Type	Property	Supported Conditions	Comments
		contains contains not starts with starts with not ends with ends with not matches matches not	**Note:** If you have a process-based filter, but that process spawns child processes, it is expected that the process that matches the process filter will still be recorded to ensure complete process trees. However, events for the process (for example, file events) that match the process filter are not recorded. Additionally, a process matching a process filter can also be recorded, to ensure completeness of data, if there is a Signal match that contained the filtered process.
	hash	is is not	The MD5 hash of the process executable file.
	command line	is is not contains contains not starts with starts with not ends with ends with not matches matches not	The full command line of the process.
	user name	is is not	The user name executing the process.

©2026 Tanium Inc. All Rights Reserved

Type	Property	Supported Conditions	Comments
		contains contains not starts with starts with not ends with ends with not matches matches not	
	user group	is is not contains contains not starts with starts with not ends with ends with not matches matches not	The user group or domain of the user executing the process.
	parent path	is is not contains contains	The full path to the parent process file.

©2026 Tanium Inc. All Rights Reserved

Type	Property	Supported Conditions	Comments
		not starts with starts with not ends with ends with not matches matches not	
	parent command line	is is not contains contains not starts with starts with not ends with ends with not matches matches not	The full command line of the parent process.
	ancestry path	is is not contains contains not starts with	The full path to any of the parent processes.

©2026 Tanium Inc. All Rights Reserved

Type	Property	Supported Conditions	Comments
		starts with not ends with ends with not matches matches not	
	ancestry hash	is is not	The MD5 hash of any of the parent processes.
	ancestry command line	is is not contains contains not starts with starts with not ends with ends with not matches matches not	The full command line of any of the parent processes.
	ancestry user name	is is not contains contains not	The user name executing any of the parent processes.

©2026 Tanium Inc. All Rights Reserved

Type	Property	Supported Conditions	Comments
		starts with starts with not ends with ends with not matches matches not	
	ancestry user group	is is not contains contains not starts with starts with not ends with ends with not matches matches not	The user group or domain of the user executing any of the parent processes.
	signature status	is is not	One of verified , unverified , or no_signature
	signature issuer	is is not contains contains	The signature issuer of the process.

©2026 Tanium Inc. All Rights Reserved

Type	Property	Supported Conditions	Comments
		not starts with starts with not ends with ends with not matches matches not	
	signature subject	is is not contains contains not starts with starts with not ends with ends with not matches matches not	The signature subject of the process.
Network	address	is is not contains contains not starts with	The IPv4 remote address.

Type	Property	Supported Conditions	Comments
		starts with not ends with ends with not matches matches not	
	port	is is not contains contains not starts with starts with not ends with ends with not matches matches not	A direction-specific non-ephemeral port. Local on incoming, remote on outgoing.
	dns query	is is not contains contains not starts with starts with not	The hostname requested for DNS resolution. **Note:** This filter syntax will be replaced with DNS Query.Query

©2026 Tanium Inc. All Rights Reserved

Type	Property	Supported Conditions	Comments
		ends with ends with not matches matches not	
	operation	is is not	Network operations that include connect and accept.
Registry	key path	is is not contains contains not starts with starts with not ends with ends with not matches matches not	The full path to the registry key, including the full hive name.
	operation	is is not	Registry operations that include create, set_value, delete, and rename.
	value name	is is not contains contains not starts with	The registry value name.

©2026 Tanium Inc. All Rights Reserved

Type	Property	Supported Conditions	Comments
		starts with not ends with ends with not matches matches not	
Image	path	is is not contains contains not starts with starts with not ends with ends with not matches matches not	The full path to the file.
	hash	is is not	The MD5 hash.
	signature status	is is not	One of verified , unverified , or no_signature
	signature issuer	is is not contains	The signature issuer of the process.

©2026 Tanium Inc. All Rights Reserved

Type	Property	Supported Conditions	Comments
		contains contains not starts with starts with not ends with ends with not matches matches not	
	signature subject	is is not contains contains not starts with starts with not ends with ends with not matches matches not	The signature subject of the process.
System	path (Linux)	starts with starts with not	The full path to the file.
	actor path (Windows)	is is not	The full path to the process or file that performs the process injection.

©2026 Tanium Inc. All Rights Reserved

Type	Property	Supported Conditions	Comments
		starts with starts with not	**Note:** When using is or is not filter construction, the filter must match a file and not a folder. For example, process_injection.actor_path is C:\\exclude\\ is invalid construction.
DNS Query	Query	is is not contains contains not starts with starts with not ends with ends with not	The hostname requested for DNS resolution. **Note:** This filter syntax will replace Network.DNS Query

Property values can be an integer, a simple alphanumeric string, or they can be more complex and include other characters, such as spaces, backslashes, and hex-encoded values. Property values do not support wildcards. For properties that offer the matches and matches not conditions, the value is a regular expression written in RE2 syntax. Regular expressions are case-sensitive. To ignore case, add the (?i) flag at the start of the expression; for example, process.command_line matches '(?i)evil'. On Windows platforms, case is not sensitive for other provided property values; for example, TaniumClient or taniumclient has the same effect. To create patterns for properties that start with, contain, or end with, use conditions and add additional statements to filters. For searches with non-alphanumeric values or spaces, enclose the value in single quotes. To escape special characters within the single quotes, including in regular expressions, the following sequences are supported:

- `\r` For carriage return
- `\n` For newline
- `\t` For tab
- `\\` For the backslash itself
- `\'` For a single quote within the quotes

©2026 Tanium Inc. All Rights Reserved

- `\x` To allow a single-byte hex-encoded sequence. For example \x20 would translate to a single space.

> **Note:** The hex-encoding is required to handle UTF-8 characters outside of the single-byte character set. Any UTF-8 character can be added via the hex-encoding, if needed

The following sample expressions demonstrate combined expressions, precedence, and escaped special characters:

- `process.command_line contains 'evil' AND process.path starts with 'c:\\windows'`
- `(file.path starts with 'c:\\temp' OR file.path ends with '.evil.tmp') AND process.path contains cmd.exe`

6. (Optional) Click **Group**. Using a group indicates that you intend to match all conditions in the group against a single event. For example, to ensure that matches happen against the same file event, you should group those events. You can then include multiple groups to achieve matches against different events in time. You can use logical AND and logical OR to further refine group behavior.
7. Click **Save**.
8. In the **Filters** section of a Recorder or Stream configuration, click **Include** or **Exclude** next to any filter that you have added to designate the method you want to apply for each set of filters. The **Include** method of filters enables you to replace the default filter to only include the filters you specify to reduce performance impact and enable quick event identification. For example, for registry events, if you provide one or more registry filters as include, those replace the default include filter of 'registry'. The **Exclude** method enables you to effectively prevent events from recording. If a set of filters that you designate to **Include** contains a specific filter that has been designated to a set of filters to **Exclude**, a warning displays in the workbench.

Import and export configurations and filters

About this task

Import and export configurations and filters to apply them in a different Threat Response environment. For example, you can export configurations or filters that you have tested from a lab environment and import them into a production environment. With the exception of index

©2026 Tanium Inc. All Rights Reserved

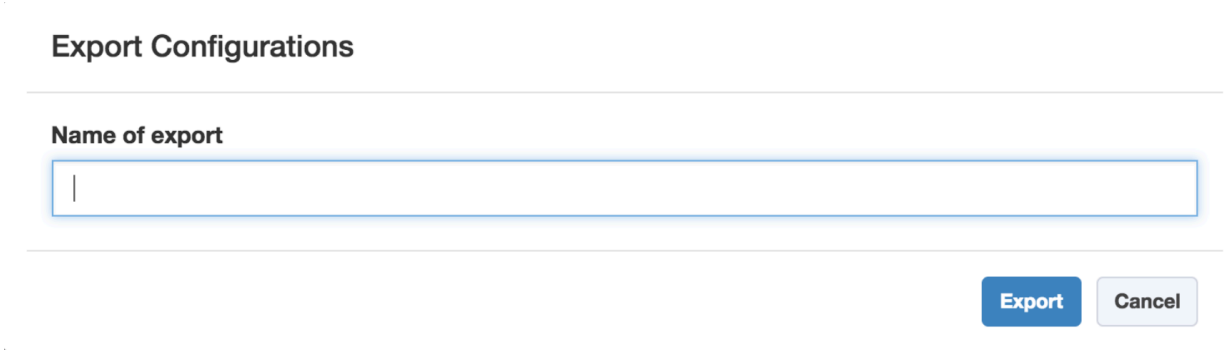
configurations, both configurations and filters are imported and exported exclusively as JSON files.

Export configurations

1. From the Main menu, go to **Modules** > **Threat Response Management** > **Configurations**.
2. Select one or more configurations to export. Click **Actions** > **Export** to export the selected configurations. To export all configurations, click **Export All**.
3. On the export page, provide a name and click **Export**. All of the configurations in the Threat Response environment are exported.

Export filters

1. From the Main menu, go to **Modules** > **Threat Response Management** > **Filters**.
2. Click **Export All**.
3. On the export page, provide a name and click **Export**.
   All of the filters in the Threat Response environment are exported.



Import configurations

About this task

©2026 Tanium Inc. All Rights Reserved

Important: When you import a detection configuration into a different Threat Response environment, intel sources and labels are resolved by name, not by ID. The workbench shows the mapping results during import.

- If a source with the same name exists in the destination, the configuration uses it. If no matching source exists, its source-label mapping is removed from the imported configuration. To preserve the mapping, create a source with the same name in the destination before importing.
- If a label with the same name exists, the configuration uses it. If no matching label exists, the workbench creates the label with no intel documents assigned. Assign intel documents to the new label to activate the mapping.
- Computer groups assigned to profiles are not included in import or export. Reassign computer groups to the profile in the destination after import.

1. From the Main menu, go to **Modules** > **Threat Response Management** > **Configurations**.
2. Click **Import/Export**. Select **Import JSON** and browse to a JSON file.
3. Click **Import**.

Import filters

1. From the Main menu, go to **Modules** > **Threat Response Management** > **Filters**.
2. Click **Import**. Browse to a JSON file.
3. Click **Import**.

©2026 Tanium Inc. All Rights Reserved

Creating profiles in Threat Response

Overview

Profiles combine configurations and apply them to one or more computer groups. Create and apply profiles to provide the most relevant Threat Response capabilities to specific groups of endpoints. For example, you can create profiles that apply configurations for such groups as:

- Endpoint type, such as servers or employee workstations
- Endpoint location, such as by country or time zone
- Endpoint priority, such as business-critical endpoints
- Endpoint configuration needs, such as VDI endpoints

The Profiles page displays all the profiles that are available to use with Threat Response. Threat Response provides default profiles that feature commonly used configurations as examples. For each profile, you can view a description and the computer groups that have the profile assigned. Profiles display as Deployed, New, Updated, or Deploying.

Threat Response profiles support multiple Stream configurations in each profile. This enables endpoints to stream endpoint telemetry to multiple different Stream destinations.

Suppression rules can target specific profiles. When you delete a profile, review any suppression rules that targeted it to avoid leaving orphaned rules in **Suppression Rules**.

Deployed

: Indicates that the profile is currently in use on one or more computer groups and that no changes have been made to the profile settings.

New

: Indicates that the profile has never been deployed to endpoints.

©2026 Tanium Inc. All Rights Reserved

Updated

Indicates that the profile is in use but there are pending changes that cannot take effect until the profile is deployed again.

Pending

Indicates that the profile is in the process of being deployed to endpoints.

Warning - Deleted Computer Groups

Indicates that profile targets computer groups that have been deleted. Ensure that the intel documents contained in the profile all target valid computer groups.

Note: Deleting a profile also orphans any profile-specific suppression rules that targeted it. Go to **Intel** > **Suppression Rules** to review and remove rules that target the deleted profile. Deleting a profile also makes inert any profile-scoped reactions that targeted it. Go to **Intel** > **Reactions** to re-bind or rescope affected reactions.

When you duplicate a profile, you can select **Copy suppression rule associations** to bind the new profile to the same profile-scoped suppression rules as the source profile.

Tanium Managed profiles

Tanium Managed profiles are provided that contain updated configurations. These profiles are the result of Tanium data and experience and have been designed to use settings that are considered safer and to provide more real-time visibility with index and recorder data. You can not delete Tanium Managed profiles. Tanium Managed profiles are intended to be a starting point that you can build off of or expand and are initial starting points that are based off of Tanium best practices. No existing profiles are changed when you install a version of Threat Response that provides Tanium Managed profiles. This is a new point of departure to accelerate the time for configuring the operation of Threat Response as quickly as possible without having extensive Tanium experience or subject matter expert guidance.

[Tanium Managed] Low Resource Assets

The **[Tanium Managed] Low Resource Assets** profile is intended for endpoints with limited CPU and memory resources. Includes less than 8 GB of memory and 4 logical processors/cores.

©2026 Tanium Inc. All Rights Reserved

This profile is supported for Linux, MacOS and Windows endpoints.

[Tanium Managed] Windows Domain Controllers

The **[Tanium Managed] Windows Domain Controllers** profile is intended for Windows domain controllers with specific recorder filters assigned to optimize the retention of recorder data.

[Tanium Managed] Servers

The **[Tanium Managed] Servers** profile is intended as a set of best practices based on Tanium data for Servers.

This profile uses a two day **Index Scan Frequency**, and a **High Priority Path Scanning** interval of 12 hours.

The `All Linux` and `All Windows Servers` computer groups are intended targets for this profile.

[Tanium Managed] Workstations

The **[Tanium Managed] Workstations** profile is intended as a set of best practices based on Tanium data for Workstations.

The profile uses a one day **Index Scan Frequency**, and a **High Priority Path Scanning** interval of 12 hours.

The `All Windows Workstations` and `All Mac` computer groups are intended targets for this profile.

Create a profile

About this task

Create a profile to manage configurations for deployment to one or more computer groups.

1. From the Main menu, go to **Modules** > **Threat Response Management** > **Profiles**. Click **Create Profile**. Provide a name and description for the profile.
2. Select to **Enable** or **Disable** the profile. When you **Disable** a profile, the targeting for that profile is made such that it is not applicable to any endpoints. The targeted Computer Groups that you have assigned that profile are not changed, however it is not deployed to endpoints

©2026 Tanium Inc. All Rights Reserved

that are included in those Computer Groups. For example, `Profile A` targets the `All Windows` Computer Group. If you disable `Profile A`, it still appears to target the `All Windows` Computer Group, but it is not deployed to those endpoints. Any endpoints that are targets of a disabled profile move to their next applicable enabled profile based on priority. Any configurations deployed by the profile before it was disabled are removed if no profile is currently applicable. If you switch a deployed profile from enabled to disabled you are prompted to deploy the profile so the change can take effect.

3. In the **Computer Groups** section, click **Select Computer Groups** to add the computer groups to which you want to deploy the Threat Response configurations. Computer groups that you have associated with custom tags provides advantages over common Computer Groups, such as `All Computers`, or `All Windows`. By using Custom Tags, you can take advantage of the profile prioritization in Threat Response without needing to make any changes to the profiles themselves, for example, needing to re-deploy the profiles after changes are made.

   > **Note:** Manual computer groups are not supported.

4. In the **Detection**, **Index**, **Recorder DB**, and **Stream** sections, select an available configuration. Stream configurations are the only configuration type that you can add multiple configurations of to a profile. A summary of the configuration is available to preview. If you need to make changes to the configuration, click **Edit**.

   > **Note:** When a detection configuration is not enabled, you can still perform on-demand scans. To fully disable detection from running on endpoints, create and enable a detection profile and configure a complete blockout window.

   If any component of an active profile is not configured, the implications are as follows:

Implications of unconfigured components of an active profile

Configuration	Implication
Detection	If the Intel component of an active Threat Response profile is not configured, intel documents are still updated on endpoints. However, intel is not used by Threat Response to generate alerts. On-demand scans are evaluated if the endpoint is part of a targeted group and is not within a blackout window. A detection configuration should be specified with a 24/7 blockout scan window to prevent on-demand scans from evaluating.

©2026 Tanium Inc. All Rights Reserved

Configuration	Implication
Recorder	If the recorder component of an active Threat Response profile is not configured, the TaniumClient process continues running. However, the recorder does not record activity on endpoints in the action group. On Linux endpoints, the auditd and audispd processes restart when a configuration is added or changed. Ensure the Track Changes setting is not enabled in an Index Configuration or the recorder could become enabled.
Index	If the index component of an active Threat Response profile is removed, Index continues to be deployed to endpoints, however Threat Response does not perform Index tasks.
Stream	No data is streamed to a destination outside of Tanium.

5. (Optional) Specify a **TPA Scan Frequency** for Windows endpoints to configure how often the Tanium Persistence Analyzer runs on endpoints. Changing this setting affects the data that Threat Response sensors return.
6. Click **Save**.

Prioritize profiles

About this task

A computer group can have one assigned profile. However, an endpoint can be a member of multiple computer groups. If an endpoint is a member of multiple computer groups, the profile with the highest priority is applied to that endpoint. If another user updates profiles before the prioritization of profiles can complete, the prioritization is reset.

1. From the Main menu, go to **Modules** > **Threat Response Management** > **Profiles**.
2. Click **Prioritize**.
3. Order the profiles in the order of their priority. The profile with the priority number of one (1) has the highest priority.
4. Click **Save**.

Deploy a profile

©2026 Tanium Inc. All Rights Reserved

About this task

Deploy a profile to enable the functionality of Threat Response on all of the endpoints in the computer groups that the profile targets. When a user deploys a profile, Threat Response deploys it using the Tanium System User Service (SUS) account rather than that user's personal account. When deploying profiles using the system user service, a user must have either unrestricted management rights, or rights to All Computers to deploy profiles. For more information, see Tanium Console User Guide: Controlling endpoint management rights through computer groups.

> **Note:** Confirm that all packages are cached before you deploy a profile. A ribbon appears on the profiles page if you attempt to deploy a profile prior to all packages being cached. Click the ribbon to view details about the state of package caching.

1. From the Main menu, go to **Modules** > **Threat Response Management** > **Profiles**.
2. Select one or more profiles to deploy and click **Profile Actions** > **Deploy**.

   > **Important:** Profile deployment is not part of a scheduled action. You need to deploy a profile in order for Threat Response capabilities to function on endpoints.

3. Enter your password to confirm the deployment. Click **OK**.

   > **Important:** When a user deploys a profile, Threat Response deploys it using the Tanium System User Service (SUS) account rather than that user's personal account. The **Deploy as Service Account** setting is always enabled and cannot be changed. The setting remains visible in **Settings** > **Service** > **Misc** as a checked, disabled checkbox with a tooltip that explains why it cannot be changed. A user can deploy a profile to any computer group they have management rights to, without needing unrestricted management rights or rights to All Computers. If a deployment is denied because of insufficient management rights, the error message identifies the specific computer groups involved. After you upgrade, profiles that were previously deployed under a user account are marked as needing deployment. Redeploy these profiles to complete the transition to this behavior. Profiles that you have not redeployed retain the previous behavior until you redeploy them.

Deploy intel

About this task

©2026 Tanium Inc. All Rights Reserved

Before you deploy intel, ensure that you have thoroughly tested intel to verify that:

- The intel matches on what you expect
- The intel does not match a high number of false positives

See Testing Intel for deployment on page 113 for more information.

Configure the intel deployment setting

1. From the Threat Response overview page, click Settings.
2. On the **Service** tab, click **Intel**. Make intel package selections:
   - **Intel Package Publication Interval**: Specifies how frequently the intel documents and labels are pushed to the endpoints (Default: 24 hours).
3. Click **Save**.

Immediately deploy intel to endpoints

About this task

Intel is automatically published to the endpoints on a regular interval. If a situation requires it, you can manually push the intel documents and Signals to the endpoints.

1. Click **Management** > **Profiles**.
2. Click **Deploy Intel**.

Result

Note: Assign the **Threat Response Intel Deploy Approval Bypass** permission to roles that deploy intel to bypass approvals for intel.

©2026 Tanium Inc. All Rights Reserved

Direct connecting to endpoints and exploring data

You can review endpoint data with a direct connection or from an endpoint snapshot.

- Direct connection

  With direct connections, you can conduct analysis within seconds, without time-consuming data transfers or parsing. You can take multiple snapshots of the endpoint data, browse the file system, export events, and save evidence for remediation.

- Endpoint snapshot

  Snapshots capture the endpoint data for asynchronous investigation offline, preserving the recorder database for storage and collaborative analysis on the Tanium Module Server. With snapshots, you can export events, and save evidence for long-term analysis.

Threat Response supports direct connections using Tanium Direct Connect. Direct Connect provides a communication channel for other Tanium modules and a central location for configuring and administering direct endpoint connections across modules. Direct Connect replaces the mechanism for live endpoint connections that was used in previous versions of Threat Response to provide better performance and a consistent experience across Tanium modules. To install Direct Connect, see Tanium Direct Connect User Guide.

For new installations beginning with Threat Response 2.4, Direct Connect is enabled by default.

Direct connect to an endpoint

About this task

You can connect to endpoints that are registered with Tanium and are a member of a computer group that is accessible to you. You must have the IP address or computer name of the endpoint. If you do not have management rights to an endpoint, it appears offline.

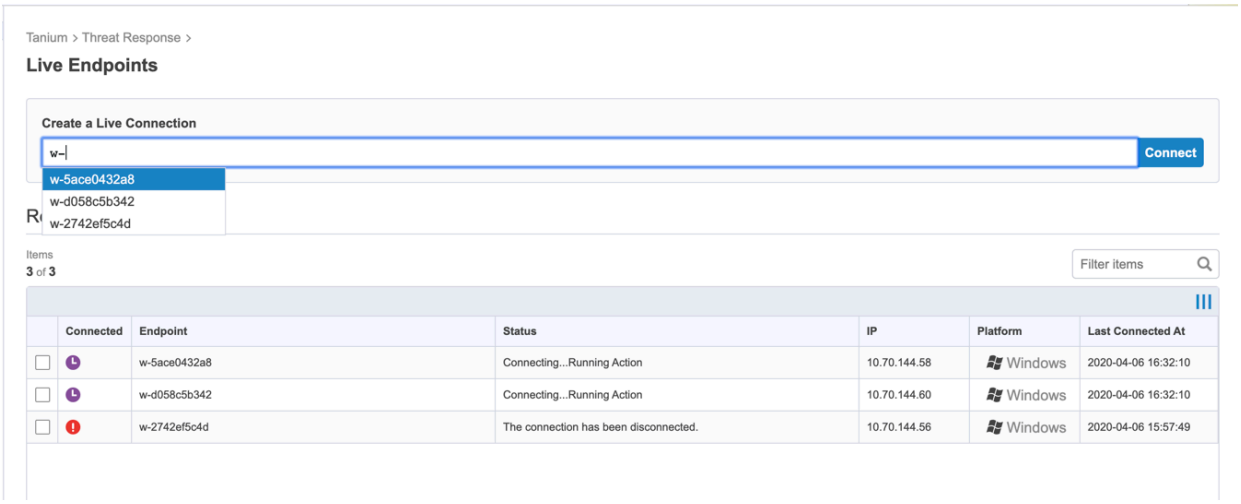
You can make a direct connection to one or more endpoints.

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Threat Response Direct Connect**.
2. Type the IP address or computer name of an endpoint that you want to add. Matching endpoints appear as you type.

   Note: If the endpoint you want to add is not in the list, verify that the endpoint is a member of a computer group that you can access. An indicator next to the text field shows whether an endpoint is currently online.

3. Select one or more endpoints to add.
   Click **Connect**.



Result

The live endpoint list displays endpoint connections that have been attempted, are connected, have failed, or where the connection has been closed. The history of connected endpoints is sorted by the last date on which endpoints were connected. Additionally, the date and a link to the last must gather package for the endpoint is provided. To download the most recent must gather package for an endpoint, click the link in the Last Must Gather column for the endpoint. If you do not see the Last Must Gather column, click the additional details icon at the top right of the grid and make sure to select Last Must Gather column to display this data. Live endpoint connection status appears next to the endpoint with the connection information. An endpoint remains on the Direct Connect list until the connection is manually closed, regardless of the connection status. The connection times out after ten minutes of inactivity.

Add to investigation

©2026 Tanium Inc. All Rights Reserved

In the events grid on a live connection, click **Add to an Investigation** in the Actions column to add the event to an investigation in Tanium Investigate. With Tanium Investigate you can identify the root cause of issues that arise on Tanium-managed endpoints and arrive at resolutions to issues more quickly. For more information, see Tanium Investigate User Guide.

Capture a snapshot

About this task

You can capture a snapshot of an endpoint database for offline analysis and detailed forensics.

> **Note:** When you use Direct Connect to manage live endpoint connections, you cannot view snapshots of Recorder 1.x databases (monitor.db). This does not apply to Recorder 2.x databases (recorder.db).

1. From the Main menu, go to **Modules** > **Threat Response Direct Connect**.
2. Click the computer name to go to the events grid. Click **Capture**.
3. Go to **Saved Evidence**.
4. View the snapshot progress by expanding the computer name.

Result

To view endpoint name and the number of captures, go to the **Snapshots** menu. The snapshot name is the endpoint host name with a timestamp in a YYYY_MM_DDTHH.MM.SS.mmmZ format.

Close the connection

You can manually close a connection to one or more endpoints. Select the endpoints you want to disconnect on the **Direct Connect** page. Click **Delete**.

Browse the file system on connected endpoints

About this task

You can browse the file system on connected endpoints and download files that you want to keep as saved evidence. You can delete files on an endpoint if you have the Threat Response Administrator

©2026 Tanium Inc. All Rights Reserved

role.

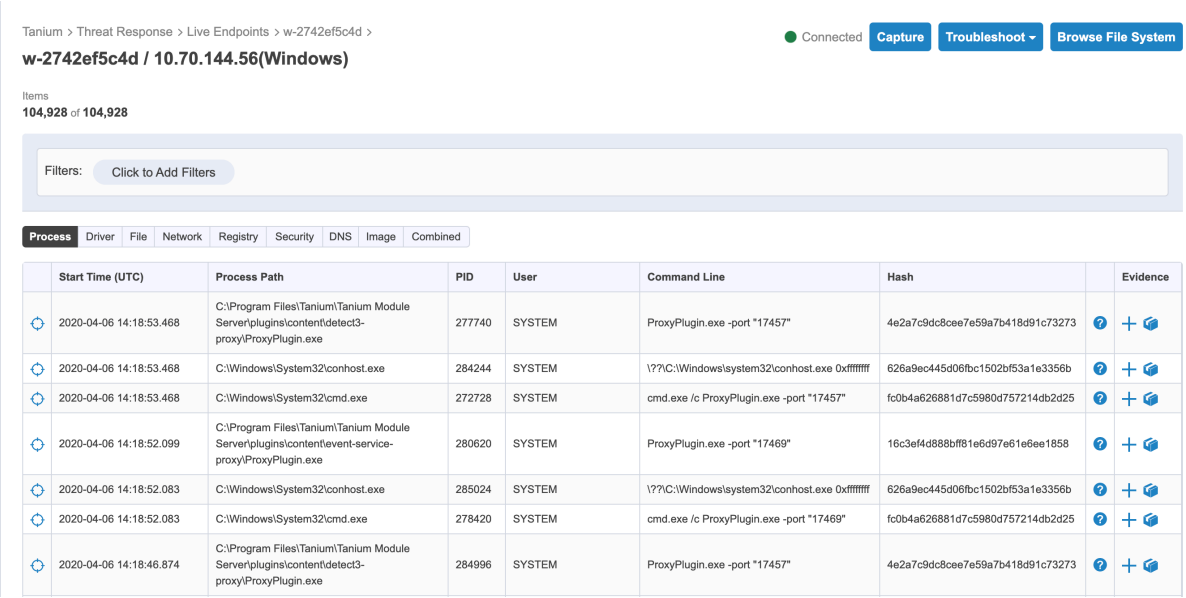
1. Click an endpoint from the live endpoint list.
2. Click **Browse File System** to open a file browser at the root directory. On Windows endpoints the default location is c:\. On macOS and Linux endpoints the default location is /. Click a row in the results grid and click the folder icon in the process path column to open the file system to the directory that contains the file.
3. Navigate the file system by typing a path, or by clicking directories in the file browser of the breadcrumbs of the path. For each file in a directory you can view the size, creation date, modification date, and the permissions for the file. Symbolic links are visible while file browsing in a live connection.
4. Click one or more files to download as saved evidence. From the Main menu, go to **Modules** > **Threat Response Saved Evidence** > **Files** to access the files that you download.
5. You can delete files and folders on an endpoint if you have the Threat Response Administrator role. To delete a file, ensure that you have the Threat Response Administrator role and click the delete icon at the end of the row. Click **Delete**. Deleting symbolic links requires Tanium Direct Connect 2.4 or higher.

Search for events

About this task

You can inspect and investigate endpoint data after you make a live connection or capture a snapshot. Search endpoint data for events using various parameters and operators. The search section displays all times in the UTC time standard.

©2026 Tanium Inc. All Rights Reserved



1. Open the events grid on a live connection or snapshot.
2. Click an exploration button to search for events.
   Each exploration button is associated with a specific event type. The filter criteria for each event type changes based on the event type you select. For example, you can filter on such criteria as process path, IP address, operation, event type, hash, signature, key value, and more. For example, for file events you can sort on the following operations:

   Create
   An event that corresponds with the creation of a file

   Write
   An event that corresponds with writing to a file

   Delete
   An event that corresponds with the deletion of a file

   Move
   An event that corresponds with the moving of a file to a different location in the file system

   Permissions Changed
   An event that corresponds with changing the permission on a file

   Open
   An event that corresponds with the opening of a file by another process

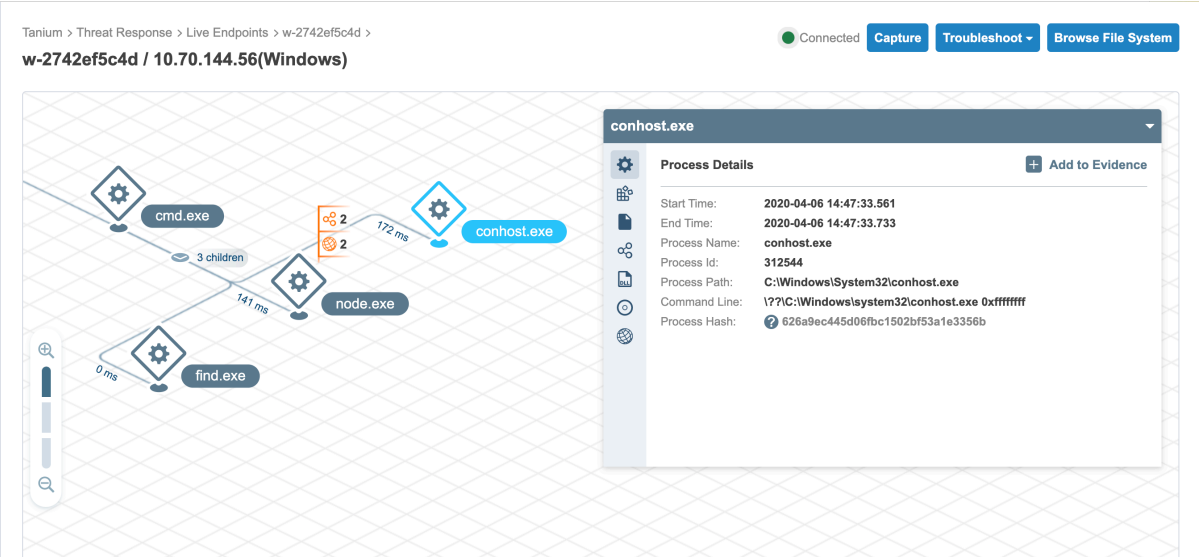
©2026 Tanium Inc. All Rights Reserved

3. Filter the search results to locate specific events that match criteria you provide.
   You can enter multiple sets of criteria based on various attributes of the event type. Less than three sets of filter criteria are treated as a logical `AND`. If you add more than two sets of filter criteria you can select to apply any or all of the criteria you have provided as a filter. The results are shown below the filters that you specify.

4. For most event types, the event grid features a column with a pivot ? icon. Click the icon to display questions that you can ask in Tanium Interact to gain further insight into the event.

View process details and hash ratings

Click a process to view additional details. The **Process Tree** visualization appears with focus on the process you selected. If a process is currently running, it displays the refresh icon. Drag the visualization in any direction to view peer or ancestor processes.



Processes in the **Process Tree** view include a **Pivot** button. Click **Pivot** to open the Tanium Ask workflow for the selected process.

The **Process Tree** view displays all of the file, network, registry, and child process activity that was initiated by the current process. This page also provides the full process image path and arguments, user context, hash, and parent command line. A tree view of network processes display, including the current process, parent, children, and peer nodes. You can zoom in and out, click and drag, and click events to change the view. You can isolate one of the processes in the tree view and quickly focus on an artifact for analysis.

Hash information for each process is available from the events grid or from the **Process Tree** view for any specific process.

©2026 Tanium Inc. All Rights Reserved

A hash can have one of the following ratings:

- Non-Malicious (Green)
- Malicious (Red)
- Unknown (Grey)
- Pending

You can decode encoded text in many places in the Threat Response workbench without having to copy and paste to a third-party tool. For example, you can decode all command line locations in the advanced details for a Threat Response alert.

For the steps to decode encoded text, see Decode encoded text on page 263.



Note: From any location in the Threat Response workbench, press `ALT + \` (Windows and Linux) or `Command + \` (macOS) to display the editor to decode encoded text. On some keyboards it is common for mappings to replace the / key (Scan Code 2B) with other characters, for example, the # character. On such keyboards, use the appropriate key combinations for the locale of the keyboard.

Explore artifact and event details with Tanium Autonomous IT

Use Tanium Autonomous IT to generate artifact and event enrichment to streamline the incident response process.

You can view contextual content in the Threat Response workbench to minimize the need to conduct external research. This content can help you understand the implications or potential impacts of artifacts.

Artifact enrichment enables you to:

- Understand the known common malicious uses for artifacts.
- Click any artifact or event that displays the enrich button to view a detailed description, expected uses, functionality, and if there are known malicious uses.
- Click **Explore in Tanium Ask** to conduct more research in Tanium Ask and prompt follow-on

©2026 Tanium Inc. All Rights Reserved

questions to guide potential actions to take.

Manage snapshots

Snapshots show all the data from an endpoint. The database file contains historical event activity going back to the first moment of recording or to the configured limits. Snapshots are stored on the Tanium Module Server.

Export a snapshot from an endpoint

About this task

You can retrieve the endpoint database manually if an offline endpoint or a direct connection fails.

1. Log on to the endpoint with administrator credentials.
2. Stop the endpoint recorder by deploying a profile that does not contain a recorder configuration.
3. Copy the recorder.db file to a location accessible to the Tanium Console from the <Tanium Client>/extensions/recorder directory.

   Note: Change the file name to include the host name and a timestamp in the format: hostname_YYYY_MM_DDTHH.MM.SS.mmmZ.db. The file name appears in Threat Response.
4. Start the endpoint recorder by deploying a profile with a recorder configuration.

Download a snapshot

About this task

You can download snapshots an endpoint databases for offline analysis and detailed forensics outside of Threat Response.

1. Go to **Threat Response** > **Saved Evidence**. Click **Snapshots**.
2. Select the snapshots that you want to download and click **Download**.
3. The snapshot downloads are managed through the web browser. Note the location to which the browser downloads the file. Multiple snapshots are added to a zipped file.

©2026 Tanium Inc. All Rights Reserved

Result

> **Note:** You can view uploaded snapshots from users who are using the same active persona as the active persona that uploaded the snapshot. Additionally you can view uploaded snapshots if the current user is the same as the user that uploaded the snapshot. The Threat Response Administrator role has access to view all uploaded snapshots. To provide other roles visibility into all uploaded snapshots, assign the **Threat Response Visibility Bypass** permission to those roles.

Upload a snapshot

1. (Optional) Install upload authentication certificates.
2. In the Tanium Console, go to **Threat Response** > **Saved Evidence** and click **Upload Snapshot**.
3. Browse to the saved snapshot.
4. Click **Upload & Connect**.

Result

If you are having difficulty uploading a snapshot, see Troubleshooting Threat Response on page 351.

Save files and events

About this task

While reviewing the event data from a direct connection, you can save files - including locked files - and events directly from the events grid as you investigate. You can save files of any type.

> **Note:** You must have a direct connection to the endpoint to save file evidence. Saving evidence files from the endpoint is limited by available hard disk space on the Tanium Module Server. When viewing snapshots, you cannot save file evidence from snapshots.

1. Open the events grid.
2. Double-click an event row to open the **Process Details** page.
3. Select **Save Process Evidence**.

©2026 Tanium Inc. All Rights Reserved

Result

The file is saved under **Saved Evidence**.

> **Note:**
>
> You can view evidence saved from endpoints that belong to computer groups for which you have permissions to access. For example, you can view evidence from endpoints for which the active persona belongs to at least one management rights group to which the endpoint belongs. If the current user belongs to at least one management rights group to which the endpoint is a member of, saved evidence for that endpoint is visible. The Threat Response Administrator role has access to view all saved evidence. To provide other roles visibility into all saved evidence, assign the **Threat Response Visibility Bypass** permission to those roles.
>
> To toggle the visibility of one or more types of saved evidence for a user, add or remove the following permissions that correspond to the type of saved evidence for the user role:
>
> Download: Threat Response Downloads READ
>
> Export: Threat Response Exports READ
>
> Event: Threat Response Saved Evidence READ
>
> Snapshot: Threat Response Snapshot READ
>
> If you remove the **Threat Response Downloads Read/Write** permissions for a user, the files tab is not available under saved evidence, however selecting **All** still displays files in the results.
>
> If an endpoint is offline for longer than the configured value of the **Max Endpoint Age (Days)** setting in Tanium Interact, only the users with the **Threat Response Visibility Bypass** permission can view alerts and saved evidence for the endpoint. If such an endpoint comes back online, alerts and saved evidence become visible to users with the correct permissions.

Download a file

Suspicious files might require more analysis or reporting to threat intelligence. After you save files from a direct connection as evidence, you can also download them from the **Saved Evidence** page in Threat Response. The file contents are in an encrypted ZIP format that is downloaded to the

©2026 Tanium Inc. All Rights Reserved

endpoint that is hosting the browser. Decrypt files that you download with the password `infected`. If you need to inspect the file without opening it, the ZIP headers are not encrypted. The file evidence encryption method is based on the file size. Files that are greater than or equal to 2^32 bytes are encrypted with aes256 encryption. Files that are less than 2^32 bytes are encrypted with ZIP 2.0 encryption. Some ZIP utilities that support ZIP 2.0 decryption may not support aes256 decryption.

You can select multiple items of saved evidence to download at one time. When you download multiple items of saved evidence each item is downloaded as a ZIP file that is nested in a container ZIP file. Each ZIP file in this container is encrypted with the password `infected`. You can download a single file of any size. When downloading multiple files the total size of the downloaded files cannot exceed a total size of 1GB. To download files that exceed 1 GB in total size, download them individually.

Select one or more files from the **Saved Evidence** page. Click **Download**. The files are saved in a ZIP file in the downloads directory for the Web browser.

Create Enforce rules

About this task

You can pivot from evidence on a single endpoint to create Enforce policies for multiple computer groups that contain Windows endpoints. You can add policies to existing process rule policies or create new ones from Threat Response, where you seamlessly complete the policy configuration in Enforce.

1. From the Main menu, go to **Modules** > **Threat Response Saved Evidence**.
2. Click one or more saved events.
3. Click **Create Protection Policy**.
4. Confirm the evidence to use and click **Create**.
5. On the **Policy Selector** page, create a new policy or add the evidence to an existing policy.
6. Complete the information on the **Edit Policy** page.
7. Click **Create** or **Update** as appropriate.
8. Review the **Policy Summary** and add enforcements as needed.

©2026 Tanium Inc. All Rights Reserved

Export events

You can export some or all of the events from an endpoint as a ZIP file that contains a CSV file. If you are exporting a large event database, take a snapshot and export the events from the snapshot to reduce the load on the endpoint.

> **Note:** Large exports might take a while to become available.

Select the rows in the events grid that you want to export, and click Export .

Manage IOCs

Indicators of Compromise (IOCs) are artifacts observed on an endpoint that indicate a breach of security. IOCs help you detect data breaches, malware infections, or other threat activities. IOCs include the following:

- Hash values of suspicious files
- IP addresses that are known to be malicious
- Domain names associated with malicious activities
- URLs that are used for phishing attacks
- Email addresses used to send spam or malware
- File paths of malicious software
- Registry keys modified by malware

As you examine the endpoint event data during an investigation, you might confirm that an event is malicious. You can save such events and files as evidence.

Generate an IOC

1. From the Main menu, go to **Modules** > **Threat Response Intel**.

©2026 Tanium Inc. All Rights Reserved

2. Select **Add** > **Evidence Based IOCs**.
3. In the IOC Normalized Tree drop-down menu, select **Item from saved evidence**. Add one or more items.
4. Select an indicator type and value from the drop-down menus. Threat Response populates the list information from the details of saved evidence.
5. Click **Generate**.

©2026 Tanium Inc. All Rights Reserved

Searching across the enterprise

Use event data to locate suspicious activity on other endpoints. Evaluate the extent of an intrusion and take informed action at scale.

Hunt across the enterprise

You can use the Threat Response sensors to search for suspicious events on multiple endpoints across the network.

Queries for simple events, such as a process, registry key, or file, yield immediate results. You can search for “known-bad” events, and recognize and evaluate the “known-good” events. You might be encountering a set of evidence that seems suspicious, at first, but might actually be normal system activity.

1. From the Main menu, go to **Modules** > **Threat Response Enterprise Hunting**.
2. (Optional) Narrow the list of sensors by clicking filters or typing in search terms. This limits the visible sensors and highlights the applicable Common Uses.
3. To review the sensor summary, click the caret to expand.
4. Click the sensor name to open the parameters configuration page and complete the fields as needed.

   > **Note:** If a sensor has no configurable parameters, the Interact results grid opens immediately.

   If you select **Common Uses** the parameter fields are automatically populated. Click **Ask Question**. The results are available in an Interact grid where you can also create a saved question. You must close the grid to select a different sensor. For more information, see the Tanium Interact User Guide: Results.
5. Select the results that need further investigation.

©2026 Tanium Inc. All Rights Reserved

6. Open a live connection or take a snapshot of the endpoints and verify that the events are actually malicious.
7. (Optional) Quarantine or remediate the compromised endpoints.
8. Create an IOC to scan for this type of activity in the future.

To search for files on disk, see Tanium Client Index Extension User Guide: Reference: Index sensors.

To search historical activity, use the following sensors.

- Trace DNS Queries

  > **Note:** If this sensor returns `No Events`, ensure that DNS events are configured and the recorder is using eBPF.

- Trace Executed Process Hashes
- Trace Loaded Drivers
- Trace Executed Processes
- Trace Logon Events
- Trace Executed Process Trees
- Trace Network Connections
- Trace File Operations
- Trace Image Loads
- Trace Registry Keys or Values

Enterprise hunting questions

You can sort the enterprise hunting questions to display them for which attack phase they are relevant.

©2026 Tanium Inc. All Rights Reserved

Data Theft

An attacker has obtained or is attempting to obtain account credentials or other sensitive information within your environment. Data exfiltration or some form of system impact might occur soon. Attackers might attempt to interrupt, manipulate, steal, or destroy critical assets. It is not uncommon for bad actors to use encrypted channels or stagger the transfers to avoid detection.

Initial Compromise

An attacker has gained access or is attempting to gain access to your environment. If successful, attackers might attempt to move to the next attack phase.

Lateral Movement

An attacker is expanding or attempting to expand the attack scope within your environment. Data exfiltration or some form of system impact can occur shortly after this happens. Attackers can interrupt, manipulate, steal, or destroy your assets.

Persistence

An attacker is attempting to maintain or increase access to your environment. If successful, attackers might attempt to load malicious payloads onto your environment, such as bots and malware, which might remain dormant in your environment even if the attacker stops.

The following list provides a reference for enterprise hunting questions:

- Account Lockouts Security Event Log Search on page 208
- AutoRun Files on page 208
- AutoRun Program Details on page 209
- Autoruns by Category on page 209
- Certificate Search on page 210
- Cleared Windows Security Event Log Search on page 211
- Command Line of Process on page 211
- Command Line with Hash Match on page 212

©2026 Tanium Inc. All Rights Reserved

- DLL Load Order Hijacking Search on page 212
- Driver Details with Hash on page 213
- Environment Variables on page 213
- Established Connections with Hash on page 214
- Explicit Logon Security Event Log Search on page 214
- File Certificate Details on page 215
- File Handle Details on page 216
- File Handles Of Process on page 216
- Generic Event Log Search on page 217
- Has Incident Response ID Files on page 218
- Has Scheduled Task on page 218
- Hash Of File on page 218
- Hosted Services Name Audit on page 219
- iCloud Settings on page 219
- Injected Threads on page 220
- Is File Digitally Signed on page 221
- Linux AutoRuns on page 222
- Listen Ports with Hash on page 222
- Loaded Modules Not Matching Whitelist on page 223
- Loaded Modules Of Process on page 223
- Loaded Modules with Hash on page 224
- Logon Security Event Log Search on page 224

©2026 Tanium Inc. All Rights Reserved

- Mac AutoRuns on page 225
- Mac Downloaded Files on page 226
- Mac Firewall Settings on page 226
- Mac Gatekeeper Settings on page 227
- Mac Kext Details on page 227
- MD5 Hash Of File on page 228
- MD5 Hash Match Files Executing on page 228
- MD5 Hash Single File Match on page 229
- Mutex Details on page 230
- Mutex Handles Of Process on page 230
- Network Details on page 231
- Non-Approved Established Connections with Hash on page 231
- Original Filename on page 232
- PowerForensics File Record on page 232
- PowerForensics Master Boot Record on page 233
- PowerForensics Prefetch on page 233
- PowerForensics Recently Opened Office Files by User on page 234
- PowerForensics Shim Cache on page 235
- Processes Using Module on page 236
- RDP Client History on page 237
- Remote Desktop Event Log Search on page 237
- Run Command History on page 238

©2026 Tanium Inc. All Rights Reserved

- Running Processes With Filename Mismatch on page 238
- Running Processes with Hash on page 239
- Running Processes with MD5 Hash on page 239
- Scheduled Tasks on page 239
- Semaphore Details on page 240
- Service Module Details on page 240
- Service Module Details with Hash on page 241
- Service Process Details on page 241
- Service Status with Hash on page 242
- Service System Event Log Search on page 242
- SHA1 Hash Match Files Executing on page 243
- SHA1 Hash Single File Match on page 244
- SHA1 Hash Of File on page 244
- Shell History on page 245
- SIP Settings on page 245
- SSH Known Hosts on page 246
- Trace DNS Queries on page 246
- Trace Executed Process Hashes on page 247
- Trace Executed Process Trees on page 248
- Trace Executed Processes on page 250
- Trace File Operations on page 252
- Trace Image Loads on page 253

©2026 Tanium Inc. All Rights Reserved

- Trace Loaded Drivers on page 255
- Trace Logon Events on page 256
- Trace Network Connections on page 257
- Trace Registry Keys or Values on page 258
- Windows Audit Policy on page 260
- Windows Credential Security Settings on page 260
- WMI Event Consumers on page 261

Account Lockouts Security Event Log Search

Retrieves lockout events from the Windows Security Event log in a specified time period. Also retrieves attempts to authenticate with a locked-out account. Using this sensor requires enabling account lockout auditing.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Retrieve	Select either **Account Lockouts** or **Logon Attempts with Locked out Accounts** .
Look Back Hours (Max 168)	Enter the number of hours to look back.

This sensor returns data that provides the time of the lockout, the hostname, account name, account domain, logon type, status, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

AutoRun Files

Returns a subset of the AutoRuns data, specifically the name of each AutoRun file and the cryptographic hash of the file in MD5, SHA1, SHA256, or IMP format. This sensor uses cached data;

©2026 Tanium Inc. All Rights Reserved

you can use the **Incident Response - Generate Autorun Cache [Windows]** package to regenerate this data.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Hash Type	Select the hashing algorithm to display in the results for each file. You can select MD5, SHA1, SHA256, or IMP.
Include Microsoft Entries	Select this option to include Microsoft entries in the results. Do not select this option if you want to exclude Microsoft entries from the results.

This sensor returns data that provides the filename, hash, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

AutoRun Program Details

Retrieves information about the Autorun applications found in the Windows Registry. This sensor uses cached data; you can use the **Incident Response - Generate Autorun Cache [Windows]** package to regenerate this data.

This sensor is available for Windows endpoints.

There are no parameters that you can edit for this sensor. This sensor returns data that provides information about the Autorun applications found in the Windows Registry is displayed in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

Autoruns by Category

Retrieves Autorun data for the enabled auto-start extension points (ASEPs). Use parameters to specify the category and hash for each ASEP. Note: This sensor uses cached data; this cached data can be regenerated with the **Incident Response - Generate Autorun Cache [Windows]** package.

This sensor is available for Windows endpoints.

©2026 Tanium Inc. All Rights Reserved

Sensor parameters

Parameter	Description
Hash Algorithm	Select the hashing algorithm to use to display each autorun application in the results. You can select MD5, SHA1, SHA256, PESHA1. PSHA265, or IMP.
Autoruns Category	Select the category of the autoruns applications in the results. You can select Logon and Authentication, Application, or System.
Include Binaries with Microsoft as Publisher	You can select this parameter to include binaries that identify Microsoft as the publisher. Be aware that it is possible for this designation to not be genuine.

This sensor returns data that provides information about the Autorun applications found based on the provided criteria in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

Certificate Search

Enables searching for installed certificates. You can search by SHA1 hash. The default is to return all installed certificates.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
SHA1 Hash	Enter the SHA1 hash that corresponds with the certificate you are searching for.
Certificate Name	Enter the name that corresponds with the certificate you are searching for.

This sensor returns data that provides information about the certificates found based on the provided criteria in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

©2026 Tanium Inc. All Rights Reserved

Cleared Windows Security Event Log Search

Retrieves events generated when the Windows Security Event Log has been cleared.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Number of Days to Look Back	Select the number of days to look back. The maximum is seven days.
Include Domain Controllers in Event Search	Select to include domain controllers in the results of endpoints on which the Windows Security Event Log has been cleared in the specified time.

This sensor returns data that provides information about the endpoints on which the Windows Security Event Log has been cleared based on the provided criteria in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

Command Line of Process

Returns the command line of any process by process name.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Process Name (Regular Expression)	A regular expression that matches the process name.

This sensor returns data that provides information about command lines of processes that match the provided regular expression in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

©2026 Tanium Inc. All Rights Reserved

Command Line with Hash Match

Returns the following information for any running process matching the specified hash: process, command line arguments of the process, and the module used by the process.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Hash Type	Select the hashing algorithm to use to display each autorun application in the results. You can select MD5, SHA1, or SHA256.
Hash to Match	Enter the hash that corresponds to the value you selected in the **Hash Type** parameter.

This sensor returns data that provides information about the running process matching the specified hash including the process, command line arguments of the process, and the module used by the process in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

DLL Load Order Hijacking Search

Searches for instances where DLL search order hijacking might have occurred in currently running processes. False positives are possible, so you must manually verify the results.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Exclude Signed Libraries	Select this option to return only unsigned potentially hijacked DLLs. Be aware that it is possible for this designation to not be genuine; for example, the signature of a library is not validated to confirm any authenticity.

This sensor returns data that provides information about the process name, DLL path, DLL MD5 hash, whether or not the DLL is signed, the reason for determining that the DLL is hijacked, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export

©2026 Tanium Inc. All Rights Reserved

the data to a CSV file.

Driver Details with Hash

Retrieves information about loaded device drivers, including a hash of each driver file.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Hash Type	Select the hashing algorithm to use to display each autorun application in the results. You can select MD5, SHA1, or SHA256.

This sensor returns data that provides information about the display name, state, path, version, hash, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Environment Variables

Retrieves environment variables.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Variable	The environment variable to search for; for example, HOME or PATH.

This sensor returns data that provides information about the corresponding value for the provided variable in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

©2026 Tanium Inc. All Rights Reserved

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Established Connections with Hash

Retrieves information about established connections with the hash value of the connected processes.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Hash Type	Select the hashing algorithm to use to display each autorun application in the results. You can select MD5, SHA1, or SHA256.

This sensor returns data that provides information about the process, hash, name, and target IP in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Explicit Logon Security Event Log Search

Searches the Windows Security Event Log for explicit logon events.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Subject User Name	This value represents the username of the account that performed the action logged by the event.
Subject Domain Name	This value represents the domain to which the subject is associated.

©2026 Tanium Inc. All Rights Reserved

Parameter	Description
Target User Name	This value represents the user account or resource being acted upon. It represents the recipient or object of a specific system action. For example, in an access attempt or permission modification, the target username indicates which account or resource is being affected.
Target Domain Name	This value represents the domain being acted upon.
Target Server Name	This value represents the server being acted upon.
Include Logons to Localhost?	Select this value to include logons to localhost in the results.
Enable Output from Domain Controllers?	Select this value to enable details from domain controllers to be reported in the results grid.
Look Back Hours	Enter the number of hours in the past that you want to include in the results grid.

This sensor returns data that provides information about the subjects and targets in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

File Certificate Details

Provides details about embedded certificates in Unix PE and COFF format image files.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
PE/COFF Executable File to Examine for Certificates	The full path to the image file for which you want to view certificates.

This sensor returns data that provides information about the filename of the executable for which you want to find certificates, the subject of an associated certificate, the serial number of the associated certificate, valid dates for the associated certificate, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

©2026 Tanium Inc. All Rights Reserved

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

File Handle Details

Retrieves information about the specified file handle that matches the input string. When a file is opened by a process, a file handle is associated with it until either the process terminates or the handle is closed. The file handle is used to identify the file in many function calls.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
File Handle String to Match (Regular Expression)	Enter a PCRE regular expression that matches the file handle that you want to find.

This sensor returns data that provides information about the process that created the file handle, the PID of the file handle, the user associated with creating the file handle, the handle ID, and a path to the handle in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

File Handles Of Process

Finds the file handles that are currently open in the specified process. The parameter is a regular expression of the process name. When a file is opened by a process, a file handle is associated with it until either the process terminates or the handle is closed. The file handle is used to identify the file in many function calls.

This sensor is available for Windows endpoints.

©2026 Tanium Inc. All Rights Reserved

Sensor parameters

Parameter	Description
Process Name to Match (Regular Expression)	Enter a PCRE regular expression that matches the process for which you want to find associated file handles.

This sensor returns data that provides information about the file handles created by the process in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Generic Event Log Search

Searches Windows event logs for entries that match a specified event ID and search term within a lookback period.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
EID	Enter the numeric event ID that you want to search for.
Search Term	Enter a string to search for within matching event log entries.
Lookback Period	Enter how many days back you want the sensor to search the event log.
Event Log Source	Specify the event log to search: enter the path to an EVTX file, enter a system-relevant event log name (for example, `System` or `Application`), or select from a list of available EVTX files.

This sensor returns data that provides the event ID, search term match, event log source, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

©2026 Tanium Inc. All Rights Reserved

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Has Incident Response ID Files

Identifies the Incident Response ID files that exist on a machine. For example, "irsearch1234".

This sensor is available for Windows endpoints.

Legacy versions of Tanium Incident Response provided files that were deployed to endpoints that were used to search and gather artifacts.

This sensor returns data that provides information about the Incident Response ID files in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

Has Scheduled Task

Returns whether the specified scheduled task exists.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Scheduled Task Name	Enter the name of a scheduled task.

This sensor returns data that provides a boolean value that indicates whether or not a scheduled task exists and the number of findings for each returned scheduled task in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Hash Of File

Returns the hash digest in the chosen algorithm of a specified file path.

©2026 Tanium Inc. All Rights Reserved

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Hash Type	Select the hashing algorithm to use to display each matching file in the results. You can select MD5, SHA1, or SHA256.
File to Hash	Enter the full path of the file you want to hash. For example, c:\windows\notepad.exe .

This sensor returns data that provides a hash value for each matching file in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Hosted Services Name Audit

Returns the Windows Service Group Name and a sorted list of service names in each group.

This sensor is available for Linux, macOS, and Windows endpoints.

This sensor returns data that provides the service group to which the hosted service is associated, the list of hosted service names, and count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

iCloud Settings

Displays all iCloud settings for all users by default. You can search by user, iCloud setting, or both.

This sensor is available for macOS endpoints.

©2026 Tanium Inc. All Rights Reserved

Sensor parameters

Parameter	Description
User Name	The name of the user associated with the iCloud setting.
Setting	The name of the iCloud setting to search for. For more information about iCloud settings, see https://support.apple.com/

This sensor returns data that provides the user associated with the setting, the setting name, a boolean value that indicates if the setting has been set, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Injected Threads

Returns threads executing possibly injected code. This is determined by finding thread start function addresses not mapped to a file on disk.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Show PID/TID	By default is unchecked and will display [omitted] for both PID and TID. Check this box for both process and thread IDs to be displayed.
Show Omitted Results	By default believe false positives will be omitted from results. Select this setting to see all possible false positive results.

This sensor returns data that provides:

- The full path of the process. This shows mismatches found between process and kernel paths.
- The PID provided that the Process ID when Show PID/TID is selected.

©2026 Tanium Inc. All Rights Reserved

- The TID provided the Thread ID when Show PID/TID is selected.
- The header which corresponds to the first 2 bytes of allocated memory region in hex.
- The mapped file which corresponds to the file mapped to this memory region or No Mapped File. The memory type which corresponds to the type of the pages in the memory region such as `MEM_MAPPED` or `MEM_PRIVATE`.
- Allocated Protection which corresponds to the protection of the memory region when allocated such as `PAGE_EXECUTE_READWRITE` or `PAGE_EXECUTE_WRITECOPY`.
- Page Protection which indicates if protection of the page in the memory region such as `PAGE_EXECUTE_READWRITE` or `PAGE_EXECUTE_WRITECOPY`.
- Start Address which indicates the Win32 thread function start address.
- Region size which indicates the total size of the allocated memory region the Win32 thread function start address is in. When no suspicious threads are found, "No injected threads found" is returned.

All data appears in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Is File Digitally Signed

Checks whether or not the specified file is digitally signed. Uses the Windows WinVerifyTrust API to verify the signature embedded in the file.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Full Path of File to Check	Enter the full path of the file you want to check. For example, c:\windows\notepad.exe

©2026 Tanium Inc. All Rights Reserved

This sensor returns data that provides boolean value that indicates if the file has been digitally signed, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Linux AutoRuns

Linux AutoRuns and their types, from known categories such as Systemd.

This sensor is available for Linux endpoints.

Sensor parameters

Parameter	Description
Hash Algorithm	Select the hashing algorithm to use to display each matching file in the results. You can select MD5, SHA1, SHA224, SHA256, SHA384, or SHA512.

This sensor returns data that provides the path, name, executable, category, command line, hash and a number of findings of the autorun file in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Listen Ports with Hash

Identifies listening TCP ports, including the process listening to the port, the hash of the process, the display name of the process (if available), and the listening IP Address and port.

This sensor is available for Linux, macOS, and Windows endpoints.

©2026 Tanium Inc. All Rights Reserved

Sensor parameters

Parameter	Description
Hash Type	Select the hashing algorithm to use to display each matching file in the results. You can select MD5, SHA1, or SHA256.

This sensor returns data that provides the process listening to the port, the hash of the process, the display name of the process (if available), and the listening IP address and port in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Loaded Modules Not Matching Whitelist

Lists the MD5 hash and fully-qualified path of any loaded modules that are not on the current MD5 whitelist.

This sensor is available for Linux, macOS, and Windows endpoints.

This sensor returns data that provides the path of the loaded module that does not match the whitelist, the MD5 hash of the module, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Loaded Modules Of Process

Lists the modules loaded by the specified process. The parameter is a regular expression of the process or module name.

This sensor is available for Linux, macOS, and Windows endpoints.

©2026 Tanium Inc. All Rights Reserved

Sensor parameters

Parameter	Description
Process or Module Name (Regular Expression)	Enter a regular expression that matches the process or module name.

This sensor returns data that provides the loaded modules of a process that matches the regular expression you provided and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Loaded Modules with Hash

Displays the fully-qualified path and hash of each loaded module.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Hash Type	Select the hashing algorithm to use to display each matching file in the results. You can select MD5, SHA1, or SHA256.

This sensor returns data that provides the path and hash of the loaded module and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Logon Security Event Log Search

Searches Windows Security Event log and equivalent logging sources on macOS for logon events.

This sensor is available for macOS and Windows endpoints.

©2026 Tanium Inc. All Rights Reserved

Sensor parameters

Parameter	Description
User Name	The user name that is associated with the events you want to search.
Domain	The domain you want to search.
Hours to Look Back (Max 168)	Select the number of hours to look back. The maximum is 168 hours.
Logon Type	Select the logon type to search for.
Include Domain Controllers in Event Search	Select to include domain controllers in the results of endpoints on which the Windows Security Event Log has been cleared in the specified time.

This sensor returns data that provides the date of the logon security event, the user associated with the logon, the domain that was logged into, the type of logon, and an a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Mac AutoRuns

Mac AutoRuns and their types, from known categories such as launch agents, launch daemons, startup items, user login items, and kernel extensions.

This sensor is available for macOS endpoints.

Sensor parameters

Parameter	Description
Hash Algorithm	Select the hashing algorithm to use to display each matching file in the results. You can select MD5, SHA1, SHA224, SHA256, SHA384, or SHA512.
Include Apple Signed Items	Select this setting to include autoruns that are signed by Apple in the results.

This sensor returns data that provides the path to the autorun file, the name of the autorun file, the executable, category, command line, hash, and a count of findings in a results grid. You can

©2026 Tanium Inc. All Rights Reserved

customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Mac Downloaded Files

Queries the ~/Library/Preferences/com.apple.LaunchServices.QuarantineEvent* file for downloaded files.

This sensor is available for macOS endpoints.

Sensor parameters

Parameter	Description
User Name	Enter the user name of the user for which you want to search for download activity.
File Name	Enter a comma separated list that includes the file names that you want to search for to see if a user has downloaded them.

This sensor returns data that provides the user, file GUID, time stamp, identifier, app, URL, sender name, sender address, download type, origin title, origin URL, origin alias and count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Mac Firewall Settings

Enumerate the firewall settings on macOS.

This sensor is available for macOS endpoints.

©2026 Tanium Inc. All Rights Reserved

Sensor parameters

Parameter	Description
Setting	Enter the macOS firewall setting that you want to search for. For more information about macOS firewall settings, see https://support.apple.com/ .

This sensor returns data that provides the setting name, the status of the setting, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Mac Gatekeeper Settings

Enumerate the Gatekeeper settings on macOS.

This sensor is available for macOS endpoints.

Sensor parameters

Parameter	Description
Setting	Enter the macOS Gatekeeper setting that you want to search for. For more information about macOS Gatekeepr settings, see https://support.apple.com/ .

This sensor returns data that provides the setting name, any notes about the setting, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Mac Kext Details

Allows you to find allowed kernel extensions on a macOS endpoint.

©2026 Tanium Inc. All Rights Reserved

This sensor is available for macOS endpoints.

Sensor parameters

Parameter	Description
Team ID	The team ID that corresponds with the team for which you want to search Kext details.
Bundle ID	The bundle ID that corresponds with the bundle for which you want to search Kext details.

This sensor returns data that provides the path, team ID, bundle ID, boot UUID, create time, last seen time, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

MD5 Hash Of File

Returns the MD5 hash for a file at a specified path.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Full Path of File	Enter the full path of the file for which you want to see the hash.

This sensor returns data that provides the hash of the provided file in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

MD5 Hash Match Files Executing

Retrieves a fully-qualified path of an executable file for a running process that matches the specified

©2026 Tanium Inc. All Rights Reserved

MD5 hash. Results also indicate if the file is executing.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
MD5 Hash to Match	Enter an MD5 hash to match a process.

This sensor returns data that provides the process that matches the provided hash and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

MD5 Hash Single File Match

Indicates whether the file at the specified path matches the specified MD5 hash.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Full Path of File	The full path of the file you want to seach for.
MD5	The MD5 hash of the file you want to match to the file you are searching for.

This sensor returns data that provides a boolean value that indicates if the file and hash match and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

©2026 Tanium Inc. All Rights Reserved

Mutex Details

Returns details about a specified mutex object, including process, PID, user, handle ID, and mutex name.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Mutex String to Match (Regular Expression)	Enter a PCRE regular expression that matches a process, PID, user, handle ID, or mutex name that matches a specific mutex you want to find.

This sensor returns data that provides the process, PID, user, handle ID, mutex and a count of findings of matches to the regular expression you provided in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Mutex Handles Of Process

Returns the open handles to file mutex objects for a specified process. The parameter is a regular expression for a process name.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Process Name to Match (Regular Expression)	Enter a PCRE regular expression that matches a process that matches a specific mutex you want to find.

This sensor returns data that provides the mutex handle and a count of findings of matches to the regular expression you provided in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

©2026 Tanium Inc. All Rights Reserved

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Network Details

Enumerates verbose network connection details.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Hostname or IP	The hostname or IP address of the network for which you want to view details.
Hashing Algorithm	Select the hashing algorithm to use to display each matching file in the results. You can select MD5, SHA1, or SHA256.

This sensor returns data that provides the process name and ID, the parent process, the path to the process, the hash of the process, the protocol, local IP address and port, remote IP address and port, and the state in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Non-Approved Established Connections with Hash

Lists information about established connections that were opened by a prohibited process or to a prohibited destination. Returns the process responsible for the connection, the hash of the process, the display name of the process (if available), and the target IP Address and port. Processes and IP ranges can be excluded in the sensor definition.

This sensor is available for Linux, macOS, and Windows endpoints.

©2026 Tanium Inc. All Rights Reserved

Sensor parameters

Parameter	Description
Hash Type	Select the hashing algorithm to use to display each matching file in the results. You can select MD5, SHA1, or SHA256.

This sensor returns data that provides the process, the hash of the process, the name of the process, and the target IP in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Original Filename

Gathers the original filename for that binary on disk. This is a potential indicator that someone has renamed a legitimate binary. For example, copying and renaming the cmd.exe binary to a different location in an attempt to avoid detection.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
File Path	Enter a full path to the file you want to investigate. For example, c:\windows\notepad.exe .

This sensor returns data that provides the file path, the original filename, the internal filename, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

PowerForensics File Record

Retrieves the Master File Table (MFT) modified, accessed, changed, and born times for a specified file

©2026 Tanium Inc. All Rights Reserved

name. Returns file name, STANDARD_INFORMATION (SI) time stamps, and FILE_NAME (FN) time stamps. All time stamps are returned in UTC format.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Specify the Path to a Folder or File	Enter the full path to a file of a folder. For example, c:\windows or c:\windows\notepad.exe .

This sensor returns data that provides the file name, SI modified time, SI accessed time, SI changed time, SI born time, FN modified time, FN accessed time, FN changed time, and FN born time in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

PowerForensics Master Boot Record

Retrieves the operating system name, enumerated through WMI, and the MD5 hash of the master boot record (MBR) code section.

This sensor is available for Windows endpoints.

This sensor returns data that provides the operating system of managed endpoints and the MD5 hash of the master boot record in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

PowerForensics Prefetch

Searches prefetch entries for previously executed applications with a provided file path.

©2026 Tanium Inc. All Rights Reserved

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Path	Enter a relative path to an executed application that you want to search for.
Volume Name	Enter the volume name you want to search. If a value is not entered the volume defaults to %SystemRoot% .

This sensor returns data that provides the name of the executed application and the path to the executed application in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

PowerForensics Recently Opened Office Files by User

Returns the path of any recently opened Office files by a user. Requires PowerShell 2.0 or later.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Username	Enter the username of the user associated any recently opened office files you want to seach for.

This sensor returns data that provides the name of any recently opened office files and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

©2026 Tanium Inc. All Rights Reserved

PowerForensics Shim Cache

Retrieves executables that might have been run from entries in the Microsoft Application Compatibility section of the registry. If an Explorer window is opened to a location for a given executable, a shim cache entry might be created even if the executable was never run.

Example output: C:\Windows\System32\cmd.exe^N/A Verbose

Example output: C:\Windows\System32\cmd.exe^2016-04-11 14:28.

A common use case for this sensor is to search for shim cache AppData entries.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Path to Match	Enter a path to search for.
Verbose Timestamp	Select this setting to display the timestamps in the results grid in a verbose format.
Include Tanium Client Entries	Select this setting to include entries that are associated with Tanium Client.

This sensor returns data that provides the path to executables that might have been run from entries in the Microsoft Application Compatibility section of the registry and their last modified time in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Process Details

Returns verbose details about running processes.

This sensor is available for Linux, macOS, and Windows endpoints.

©2026 Tanium Inc. All Rights Reserved

Sensor parameters

Parameter	Description
Hashing Algorithm	Select the hashing algorithm to use to display each matching file in the results. You can select MD5, SHA1, or SHA256.
Hostname or IP	Enter a hostname or IP address for the endpoint on which you want to find details about running processes.

This sensor returns data that provides the process name and path, the user associated with the process, the process ID, parent process ID, hash, and command line of the process in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Processes Using Module

Lists processes that use a specified module.

A common use case for this sensor is to search for processes that are loading PowerShell automation DLL.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Module to Search For	Enter a module to search for to view a list of processes that use it in a results grid.

This sensor returns data that provides the process and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

©2026 Tanium Inc. All Rights Reserved

RDP Client History

Returns local profile, RDP target name or IP, and remote logon name for a remote desktop client. If an attacker starts the RDP client with the /Public option, this information is not recorded in the user profile registry hive.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Account Searching String	Enter the account you want to search.
Host Search String	Enter the host you want to search.
Max Returned per Host	Select the maximum number of results to return per host.

This sensor returns data that provides the local profile, the RDP target name or IP address, the remote logon account, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Remote Desktop Event Log Search

Retrieves the most recent RDP events from the Terminal Services Event Log.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Look Back Hours (Maximum 168)	Enter the number of hours to look back.
Include Domain Controllers in Event Search	Select to include domain controllers in the results.

©2026 Tanium Inc. All Rights Reserved

This sensor returns data that provides the time, target hostname, account name, account domain, source IP address, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Run Command History

Lists the commands that were run from the Windows command prompt field on the Start menu.

This sensor is available for Windows endpoints.

This sensor returns data that provides the name of the user who ran a command, and the command that they ran in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Running Processes With Filename Mismatch

Gathers running processes and inspects the original filename for that binary on disk. If the running process and the binary original filename are different, results return. This is a potential indicator that someone has renamed a legitimate binary. For example, copying and renaming the cmd.exe binary to a different location in an attempt to avoid detection.

This sensor is available for Windows endpoints.

This sensor returns data that provides the name of the process, the original filename, internal filename, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

©2026 Tanium Inc. All Rights Reserved

Running Processes with Hash

Lists the fully-qualified path and hash of each running executable.

This sensor is available for Linux, macOS, and Windows endpoints.

Parameter	Description
Hash Type	Select the hashing algorithm to use to display each matching file in the results. You can select MD5, SHA1, or SHA256. This sensor returns data that provides the path of the process, the hash, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Running Processes with MD5 Hash

Lists the fully-qualified path and MD5 hash of each running executable file.

This sensor is available for Linux, macOS, and Windows endpoints.

This sensor returns data that provides the path of the process, the hash, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Scheduled Tasks

Returns scheduled tasks on a system, created either with "at" or "schtasks". Time and frequency information is omitted to limit unique strings.

This sensor is available for Windows endpoints.

This sensor returns data that provides the task name, the command, and a count of findings in a

©2026 Tanium Inc. All Rights Reserved

results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Semaphore Details

Returns details about a specified semaphore.

Example: symphony.exe|2400|WIN764\Administrator|2B4|\BaseNamedObjects\daemon242861781sem.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Semaphore String to Match (Regular Expression)	Enter a PCRE regular expression that matches a semaphore that you are searching for. For more information about semaphores, see https://learn.microsoft.com/en-us/windows/win32/sync/semaphore-objects

This sensor returns data that provides the process, PID, user associated with the semaphore, handle ID, and semaphore in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Service Module Details

Lists services that are running at the time the Question is asked. The details include the path to the service executable (if it is a stand-alone service), the module (DLL) path (if it is a hosted service), and the loaded modules if the service implements a COM application.

This sensor is available for Windows endpoints.

©2026 Tanium Inc. All Rights Reserved

This sensor returns data that provides the service name, service caption, image path, module path, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Service Module Details with Hash

Collects a comprehensive list of stand-alone services, hosted services, COM+ application components, and the selected hash (MD5, SHA1, and SHA256) of the binary.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Hash Type	Select the hashing algorithm to use to display in the results. You can select MD5, SHA1, or SHA256.

This sensor returns data that provides the name, caption, image path, binary path, hash of the binary in the selected algorithm, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Service Process Details

Returns verbose details about running processes for services.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Hostname or IP	Enter the host name or IP address of the endpoint that you want to search for service process details.

©2026 Tanium Inc. All Rights Reserved

This sensor returns data that provides the name of the process, the display name, the process ID, the process path, the start type, the service type, the user associated with the process, the status of the process, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Service Status with Hash

Provides information about each of the Microsoft Windows Services that are installed on the endpoint, including the hash and whether the service is running.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Hash Type	Select the hashing algorithm to use to display in the results. You can select MD5, SHA1, or SHA256.

This sensor returns data that provides the short name of the service, the long name of the service, the service status, the account associated with the service, the command line, hash, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Service System Event Log Search

Searches and stacks Windows service start, stop, or install entries in the System event log that occurred within a specified time period.

Common use cases for this sensor are searching to find if credential theft services or the PsExec service has been installed recently.

This sensor is available for Windows endpoints.

©2026 Tanium Inc. All Rights Reserved

Sensor parameters

Parameter	Description
Service Name	Enter one or more | seperated services to search for. For example, (wce|pwdump|cachedump|gsecdump|fgdump) .
Service State	Select a service status; Service Installed, Service Started, or Service Stopped.
Lookback Hours	Enter the number of hours in the past to look back.

This sensor returns data that provides the date of the service state, the service name, service information, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

SHA1 Hash Match Files Executing

Matches a specified SHA1 hash against files that are currently executing. Returns the paths to matching executing files, and "Yes", or "No" if no executing files match.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
SHA1 Hash to Match	Enter a SHA1 hash to search for.

This sensor returns data that provides the matches for the provided SHA1 hash, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

©2026 Tanium Inc. All Rights Reserved

SHA1 Hash Single File Match

Compares the file at a specified path to a provided SHA1 hash. Returns "Yes" if the file at the specified path matches the hash.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Full Path of File to Check	Enter the full path of the file to check. For example, c:\windows\notepad.exe .
SHA1	Enter the SHA1 hash of the file to check.

This sensor returns data that provides a boolean value that indicates whether or not the file exists with the matching hash in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

SHA1 Hash Of File

Returns the SHA1 hash of a specified file path.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
File to Hash	Enter the full path of the file to hash.

This sensor returns data that provides the matches for the provided file, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

©2026 Tanium Inc. All Rights Reserved

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Shell History

Returns the requested command(s) from the shell history files of all users (if found), or only one user if specified.

This sensor is available for Linux and macOS endpoints.

Sensor parameters

Parameter	Description
User	Enter a user that you want to search the shell history of.
Command	Enter a command that you want to search the shell history of.

This sensor returns data that provides the user, commands, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

SIP Settings

Returns the SIP settings on macOS endpoints. If all components are enabled, you see only one line "System Integrity Protection status: enabled." Otherwise, each component appears with a status.

This sensor is available for macOS endpoints.

This sensor returns data that provides the component, setting, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

©2026 Tanium Inc. All Rights Reserved

SSH Known Hosts

Retrieves entries from the .ssh/known_hosts file for a user.

This sensor is available for Linux and macOS endpoints.

Sensor parameters

Parameter	Description
User	Enter the user for which you want to see the entries of the known_hosts file.
Hostname	Enter the hostname of the endpoint on which you want to see the known_hosts file.

This sensor returns data that provides the user, host, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Trace DNS Queries

Returns historical data from each endpoint regarding DNS queries.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Time Range	Returns historical results within the selected relative time range for each endpoint, by default from one hour ago until now, or uses the range set in the Absolute Time Range option only if that option is specified.
Absolute Time Range	Returns historical results within the selected Absolute Time Range for each endpoint, only if values are provided.
All Times UTC	Select this option to display all times in UTC format.

©2026 Tanium Inc. All Rights Reserved

Parameter	Description
Treat Inputs as Regular Expressions	Select this option to use regular expressions in input fields.
Output only Yes or No	Select this option to have Yes and No returned for all matches to search parameters.
Max Results Per Host	Enter the maximum number of results to return from each host.
Remove Endpoint Name, Username, and Timestamps to Stack Results	Select this setting to omit columns that are likely to be unique per host.
Process Path	The path of the process to be found. For example, jane.smith\software.exe .
Username	The username that executed the process.
Query	Enter the DNS query to search for.
Response	Enter the DNS response to search for.
Operation	Enter the DNS operation to search for.

This sensor returns data that provides the process name, the query, the response, the operation and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Trace Executed Process Hashes

Returns the MD5 hashes of process executed within a specified time range.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Time Range	Returns historical results within the selected relative time range for each endpoint, by default from one hour ago until now, or uses the range set in the Absolute Time Range option only if that option is specified.

©2026 Tanium Inc. All Rights Reserved

Parameter	Description
Absolute Time Range	Returns historical results within the selected Absolute Time Range for each endpoint, only if values are provided.
All Times UTC	Select this option to display all times in UTC format.
Max Results Per Host	Enter the maximum number of results to return from each host.

This sensor returns data that provides the MD5 hash for executed processes in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Trace Executed Process Trees

Generates process trees from a process name (regex). With "As Parent" the specified process name appears at the top of the tree. With "As Child" it appears at the bottom.

Common use cases for this sensor are to search for:

- Adobe Reader as parent process - Search to discover if acrord32.exe is being used as the parent process responsible for initiating any child processes.
- Command Shell as child process - Search to discover if cmd.exe is the child process of any suspicious parent processes.
- Command Shell as parent process - Search to discover if cmd.exe has initiated any suspicious child processes.
- Net Command as child process - Search to discover if net.exe is the child process of any suspicious parent processes.
- Office application as parent process - Search to discover if any Microsoft Office applications (outlook.exe|winword.exe|excel.exe) has initiated any suspicious child processes.
- PowerShell as child process - Search to discover if powershell.exe is the child process of any suspicious parent processes.

©2026 Tanium Inc. All Rights Reserved

- PowerShell as parent process - Search to discover if powershell.exe has initiated any suspicious child processes.
- PsExec Service as parent process - Search to discover if psexesvc.exe has initiated any suspicious child processes.
- Web Browser as parent process Search to discover if a web browser (firefox.exe|chrome.exe|iexplore.exe) has initiated any suspicious child processes.
- WMI Service as parent process = Search to discover if wmiprvse.exe has initiated any suspicious child processes.

This sensor is available for Linux and Windows endpoints.

Sensor parameters

Parameter	Description
Process Name	Specifies the process name.
Treat Inputs as Regular Expressions	Treat input strings as regular expressions. By default, this option is cleared, and input is treated as a simple case-insensitive substring match.
Use Full File Paths	Select this option to use full file paths in the results grid.
Output only Yes or No	Select this option to have Yes and No returned for all matches to search parameters.
Process Context	Select one of the following values to specify where the process appears in the tree: "As Child" or "As Parent". By default, this value is set to "As Child".
Number of Events to Search	Specifies the number of events to search.
Time Range	Returns historical results within the selected relative time range for each endpoint, by default from one hour ago until now, or uses the range set in the Absolute Time Range option only if that option is specified.
All Times UTC	Select this option to display all times in UTC format.

This sensor returns data that provides the executed processes and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

©2026 Tanium Inc. All Rights Reserved

Trace Executed Processes

Returns historical data from each endpoint regarding process executions.

Common usse cases for this sensor are to search for:

- Adding user account with NET
- launching a Command shell by an unusual parent
- Decoding with Certutil
- Domain reconnaissance with NET
- JavaScript ran via rundll32 or MSHTA
- MacOS security_trampoline privilege escalation
- NET use to mount remote root share
- PowerShell spawned by script interpreter
- PowerShell suspicious command line arguements
- PowerShell version downgrade attack
- ProcDump dumping LSASS memory for credential stealing
- PsExec child processes
- Remote task creation with at
- Volume shadow copy deletion
- WinRAR encrypted archive creation
- WMI remote command execution

This sensor is available for Linux, macOS, and Windows endpoints.

©2026 Tanium Inc. All Rights Reserved

Sensor parameters

Parameter	Description
Time Range	Returns historical results within the selected relative time range for each endpoint, by default from one hour ago until now, or uses the range set in the Absolute Time Range option only if that option is specified.
Absolute Time Range	Returns historical results within the selected Absolute Time Range for each endpoint, only if values are provided.
All Times UTC	Select this option to display all times in UTC format.
Treat Inputs as Regular Expressions	Select this option to use regular expressions in input fields.
Output only Yes or No	Select this option to have Yes and No returned for all matches to search parameters.
Max Results Per Host	Enter the maximum number of results to return from each host.
Remove Endpoint Name, Username, and Timestamps to Stack Results	Select this setting to omit columns that are likely to be unique per host.
Process Path	The directory and file name of the executed process.
Parent Process Path	The directory and file name of the parent process.
Command Line	Arguments supplied to the executed process; might or might not include full path, depending on how the process was launched.
MD5 Hash	The hash of the process executable file.
Domain	The domain or system context for the user that executed the process, for example CORP.
Username	The username that executed the process, for example joe.smith .

This sensor returns data that provides the parent process path, the process path, command line, MD5 hash and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

©2026 Tanium Inc. All Rights Reserved

Trace File Operations

Returns historical data from each endpoint regarding filesystem activity.

Common use cases for this sensor are to search for:

- *nix persistence with SSH authorized_keys
- Creation or modification of user startup files
- Delete shell history
- Executable created by Java
- Executable created by PDF readers
- Files in recycle bin boot
- PowerShell profile modified or created
- Processes in AppData changing document files
- RAR file creation
- Script creation in web accessible folders

This sensor is available for Linux and Windows endpoints.

Sensor parameters

Parameter	Description
Time Range	Returns historical results within the selected relative time range for each endpoint, by default from one hour ago until now, or uses the range set in the Absolute Time Range option only if that option is specified.
Absolute Time Range	Returns historical results within the selected Absolute Time Range for each endpoint, only if values are provided.
All Times UTC	Select this option to display all times in UTC format.

©2026 Tanium Inc. All Rights Reserved

Parameter	Description
Treat Inputs as Regular Expressions	Select this option to use regular expressions in input fields.
Output only Yes or No	Select this option to have Yes and No returned for all matches to search parameters.
Max Results Per Host	Enter the maximum number of results to return from each host.
Remove Endpoint Name, Username, and Timestamps to Stack Results	Select this setting to omit columns that are likely to be unique per host.
File Path	The full path to the file you want to search for.
File Operation	The operation on the file, for example CreateNewFile, Write, DeletePath, or RenamePath.
Process Path	The path of the process executing the operation, for example system32\cmd.exe .
Domain	The domain or system context for the user that executed the process responsible for the file operation, for example CORP .
Username	The username that executed the process responsible for the file operation, for example joe.smith .

This sensor returns data that provides the file path, the process path, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Trace Image Loads

Returns historical data from each endpoint regarding Image Loads.

This sensor is available for Windows endpoints.

©2026 Tanium Inc. All Rights Reserved

Sensor parameters

Parameter	Description
Time Range	Returns historical results within the selected relative time range for each endpoint, by default from one hour ago until now, or uses the range set in the Absolute Time Range option only if that option is specified.
Absolute Time Range	Returns historical results within the selected Absolute Time Range for each endpoint, only if values are provided.
All Times UTC	Select this option to display all times in UTC format.
Treat Inputs as Regular Expressions	Select this option to use regular expressions in input fields.
Output only Yes or No	Select this option to have Yes and No returned for all matches to search parameters.
Max Results Per Host	Enter the maximum number of results to return from each host.
Remove Endpoint Name, Username, and Timestamps to Stack Results	Select this setting to omit columns that are likely to be unique per host.
Process Path	The directory and file name of the executed process.
Image Path	The directory and file name of the image.
Image Hash	The MD5 hash of the image.
Image Signed	Indicates whether or not the image is signed.
Signing Entity	Indicates the signer of the image.

This sensor returns data that provides the process name, the image path, the image hash, and the signing entity in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

©2026 Tanium Inc. All Rights Reserved

Trace Loaded Drivers

Returns historical data from each endpoint regarding loaded drivers.

This sensor is available for Linux and Windows endpoints.

Sensor parameters

Parameter	Description
Time Range	Returns historical results within the selected relative time range for each endpoint, by default from one hour ago until now, or uses the range set in the Absolute Time Range option only if that option is specified.
Absolute Time Range	Returns historical results within the selected Absolute Time Range for each endpoint, only if values are provided.
All Times UTC	Select this option to display all times in UTC format.
Treat Inputs as Regular Expressions	Select this option to use regular expressions in input fields.
Output only Yes or No	Select this option to have Yes and No returned for all matches to search parameters.
Max Results Per Host	Enter the maximum number of results to return from each host.
Remove Endpoint Name, Username, and Timestamps to Stack Results	Select this setting to omit columns that are likely to be unique per host.
Driver Path	The Windows path and device driver filename, for example windows\system32\driver.sys .
Driver Hash	The hash of the specified driver file.
Driver Signed	Select one of the following values to specify whether the device driver is signed: "Yes", "No", or "Either". By default, this value is set to "Yes."
Signing Entity	The name of the vendor that signed the file.

This sensor returns data that provides the driver path, the driver hash, the signature of the driver, the signing entity and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

©2026 Tanium Inc. All Rights Reserved

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Trace Logon Events

Returns historical data from each endpoint regarding logon events.

This sensor is available for Linux and Windows endpoints.

Sensor parameters

Parameter	Description
Time Range	Returns historical results within the selected relative time range for each endpoint, by default from one hour ago until now, or uses the range set in the Absolute Time Range option only if that option is specified.
Absolute Time Range	Returns historical results within the selected Absolute Time Range for each endpoint, only if values are provided.
All Times UTC	Select this option to display all times in UTC format.
Treat Inputs as Regular Expressions	Select this option to use regular expressions in input fields.
Output only Yes or No	Select this option to have Yes and No returned for all matches to search parameters.
Max Results Per Host	Enter the maximum number of results to return from each host.
Remove Endpoint Name, Username, and Timestamps to Stack Results	Select this setting to omit columns that are likely to be unique per host.
Max Database Rows	Indicates the maximum number of rows to process when the sensor runs.
Domain	The domain to be searched for the process, for example CORP .
Username	The Active Directory username associated with the user account.
Source Host	The host name or IP address of one endpoint that is the target for sensor execution.
Logon Process	The file name of the executable that launched the logon process.

©2026 Tanium Inc. All Rights Reserved

Parameter	Description
Logon Type Number	A number indicating the logon type. This must be one of the following options: 2: Interactive 3: Network 7: Unlock 10: Remote Interactive.
Logon Provider	The process associated with the logon event.

This sensor returns data that provides the source user, the source domain, the target user, the target domain, the login result, the logon type, the logon provider, the proces, the source host, the source IP address and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Trace Network Connections

Returns historical data from each endpoint regarding network connections made by processes.

A common use case for this sensor is searching for PowerShell HTTPS connections.

This sensor is available for Linux and Windows endpoints.

Sensor parameters

Parameter	Description
Time Range	Returns historical results within the selected relative time range for each endpoint, by default from one hour ago until now, or uses the range set in the Absolute Time Range option only if that option is specified.
Absolute Time Range	Returns historical results within the selected Absolute Time Range for each endpoint, only if values are provided.
All Times UTC	Select this option to display all times in UTC format.
Treat Inputs as Regular Expressions	Select this option to use regular expressions in input fields.
Output only Yes or No	Select this option to have Yes and No returned for all matches to search parameters.

©2026 Tanium Inc. All Rights Reserved

Parameter	Description
Max Results Per Host	Enter the maximum number of results to return from each host.
Remove Endpoint Name, Username, and Timestamps to Stack Results	Select this setting to omit columns that are likely to be unique per host.
Include 127.0.0.1 Traffic	Select to include network connections from the localhost. This option assumes that the localhost is the device running Tanium Console. By default, traffic from the localhost is included.
Local IP Address	If the sensor is targeted to a single host, the IPv4 address of the device.
Local Port	The port number from which the connection was made on the targeted host.
Remote IP Address	The IPv4 address of the destination.
Remote Port	The number of the port to which the connection was made.
Process Path	Use this option to specify the process path of the process to be found.
Domain	The domain to be searched for the process, for example CORP .
Username	The Active Directory username associated with the user account.

This sensor returns data that provides the process image path, the operation, the remote IP address, the remote port, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Trace Registry Keys or Values

Returns historical data from each endpoint regarding registry activity.

Common use cases for this sensor are searching for:

- Image file execution debugger value

©2026 Tanium Inc. All Rights Reserved

- RDP tunnel configuration
- Run key changes
- Sdclt.exe UAC bypass
- Service dll changes
- Service imagepath changes
- UAC notification manipulation

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Time Range	Returns historical results within the selected relative time range for each endpoint, by default from one hour ago until now, or uses the range set in the Absolute Time Range option only if that option is specified.
Absolute Time Range	Returns historical results within the selected Absolute Time Range for each endpoint, only if values are provided.
All Times UTC	Select this option to display all times in UTC format.
Treat Inputs as Regular Expressions	Select this option to use regular expressions in input fields.
Output only Yes or No	Select this option to have Yes and No returned for all matches to search parameters.
Max Results Per Host	Enter the maximum number of results to return from each host.
Remove Endpoint Name, Username, and Timestamps to Stack Results	Select this setting to omit columns that are likely to be unique per host.
Registry Key Path	The registry key path to search the target computer group for, for example HKLM\Software\VendorName\ .
Registry Value Name	The key value to search the target computer group for, for example "Setting name" in HKEY_CURRENT_USER\Software\Vendor's name\Application's name\Version\Setting name.
Operation	The type of registry event, for example SetValueKey, DeleteKey, or DeleteValueKey.

©2026 Tanium Inc. All Rights Reserved

Parameter	Description
Process Path	The path of the process to be found.
Domain	The domain to be searched for the process, for example CORP .
Username	The Active Directory username associated with the user account.

This sensor returns data that provides the registry key, the key value, the operation, the process path, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Windows Audit Policy

Retrieves the Windows Audit Policy; Trace records the operating system audit data typically seen in the Windows Security Event Log. This policy can be altered. However, if Group Policy is set, it might overwrite the log.

This sensor is available for Windows endpoints.

This sensor returns data that provides the category, subcategory, activity rating, audit status, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Windows Credential Security Settings

Returns the results of 10 Windows configuration settings that affect security.

This sensor is available for Windows endpoints.

This sensor returns data that provides the setting name, the setting value, and the OS version in a

©2026 Tanium Inc. All Rights Reserved

results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

WMI Event Consumers

Lists Windows Management Instrumentation (WMI) event consumers. Returns script path for ActiveScriptEventConsumers and command for CommandLineEventConsumers.

This sensor is available for Windows endpoints.

This sensor returns data that provides the name, class, command line template, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

©2026 Tanium Inc. All Rights Reserved

Managing Threat Response alerts

When Threat Response detects a match to intel that you have deployed to a computer group, the endpoint reports an alert. You can view alerts in the Alerts page or in individual intel documents.

> **Note:**
>
> You can view alerts from endpoints that belong to computer groups for which you have permissions to access. For example, you can view alerts on endpoints for which the active persona belongs to at least one management rights group to which the endpoint belongs. If the current user belongs to at least one management rights group to which the endpoint is a member of, alerts for that endpoint are visible. The Threat Response Administrator role has access to view all alerts. To provide other roles visibility into all alerts, assign the **Threat Response Visibility Bypass** permission to those roles.
>
> If an endpoint is offline for longer than the configured value of the **Max Endpoint Age (Days)** setting in Tanium Interact, only the users with the **Threat Response Visibility Bypass** permission can view alerts and saved evidence for the endpoint. If such an endpoint comes back online, alerts and saved evidence become visible to users with the correct permissions.

Background and On-demand scans, regardless of the intel type, are throttled to ensure they do not overuse endpoint resources. All Tanium Client extensions in total consume no more than 5% of the available CPU resources on each endpoint.

On-demand scans that cause endpoint throttling also suppress background scan alerts for the throttle period (one hour by default).

To ensure the performance and health of the database, Threat Response prunes the alerts table in the Threat Response database every five minutes. Pruning occurs when the alert.pruning.shouldPrune setting in the API is set. By default, this setting is disabled in on-premises environments. Tanium Cloud does not support disabling alert pruning. To toggle pruning on-premise, use a PATCH method request to /plugin/products/threat-response/api/v1/settings/alert.pruning.shouldPrune with the value set to `true` to enable.

Pruning removes all alerts except for the latest 100,000 alerts that are not assigned the status of **In**

©2026 Tanium Inc. All Rights Reserved

Progress or **Resolved**. Alerts that are assigned the status of **In Progress** or **Resolved** are never pruned. Threat Response then determines if there are any alerts that are not assigned the status of **In Progress** or **Resolved** that are older than 60 days, and prunes them from the database. Finally, Threat Response checks for any intel that has created the vast majority of alerts and deletes 90% of the oldest alerts for that intel and keeps only the newest 10%.

View alerts

From the Main menu, go to **Modules** > **Threat Response Alerts**. At the top of the page all of the alerts across the endpoints in an environment display ranked by endpoint with most alerts, event type, the intel document that initiated the alert, the path to the file or process that initiated the alert, the status of the alert, and a range of dates where the alert was detected. Click any of the fields in the rankings to create filters that display alerts that match the criteria you selected.

Specify any additional criteria to filter Alerts. For example, create filters to display alerts based on endpoint, event type, path, intel name, label, or MITRE technique. Click Advanced Details to view more information about the endpoint on which the alert occurred, the process that caused the alert, and the intel document that matched the alert.

Decode encoded text

About this task

You can decode encoded text in many places in the Threat Response workbench without having to copy and paste to a third-party tool. For example, you can decode all command line locations in the advanced details for a Threat Response alert.

1. For any encoded text item, click the **Decode** icon.
2. Select the **Encoding Schema** of the encoded text.
3. Select the character encoding standard for output of the decoded text.
   You can select either UTF-8 or UTF-16LE. This option is not available for all encoding schemas.
4. Click **Decode**.
   Step result: The decoded results appear in the **Output** section of the page. You can copy the results to the clipboard.

Result

©2026 Tanium Inc. All Rights Reserved

Note: From any location in the Threat Response workbench, press `ALT + \` (Windows and Linux) or `Command + \` (macOS) to display the editor to decode encoded text. On some keyboards it is common for mappings to replace the / key (Scan Code 2B) with other characters, for example, the # character. On such keyboards, use the appropriate key combinations for the locale of the keyboard.

An alert that results from a Signal that matches signature status can display the following signature status values:

- Unverified - The signature could not be verified.
- Verified - The signature was verified and passed policy requirements.
- No Signature - The file had no signature.
- Error - There was an error processing the signature. For example, an antivirus solution could be preventing access.
- Disallowed - The signature was explicitly disallowed by the operating system.
- Not Trusted - The signature was not from a trusted source.
- Not Trusted Policy - The signature was disallowed based on policy settings.
- File Does Not Exist - The file did not exist at the time the check occurred.
- Checking Disabled - Recorder was configured not to check signature for this file type.
- Timed Out - The request to check the signature timed out before it could complete.

Explore alert details with Tanium Autonomous IT

Use Tanium Autonomous IT to analyze alerts and provide enrichment to streamline the incident response process.

The alert details list shows the **Alert ID** as its first row, so you can reference the alert when following up in chat.

Alert enrichment

©2026 Tanium Inc. All Rights Reserved

You can view contextual content in the Threat Response workbench to minimize the need to conduct external research to gather information about artifacts that are indicated by alerts and their implications or potential impacts. For a given alert and processes in the ancestry for the alert, process path and name, process command line, DLL name, and registry path are fields that can display data enrichment.

Alert enrichment enables you to:

- Understand the known common malicious uses for artifacts.
- Click the send-to-chat icon next to any artifact used by a process to ask Tanium Autonomous IT about it directly in the chat panel — a detailed description, expected uses, functionality, and any known malicious uses.
- Click **Explore in Tanium Ask** to conduct more research in Tanium Ask and prompt follow-on questions to guide potential actions to take.

Alert analysis

From the alerts details view of an alert, click **Analyze** to initiate Tanium Ask. From Tanium Ask, you can view an alert overview, a description of the artifacts that have been analyzed, the context of any investigation of an alert, and a list of potential next steps you can take. You can continue the conversation with Tanium Ask to guide and inform decisions to decide on next steps for working with the alert. For more information, see Working with Tanium Ask.

Assign a status to an alert

Assigning status to an alert enables incident response efforts to identify alerts that are being investigated or remediated. For example if you encounter a suspicious alert and you begin to take investigative actions, you can change the status of an alert to **In Progress**. Similarly when you have completed the remediation of an alert, you can assign the **Resolved** status to the alert. The Available statuses for alerts are:

- **Dismissed**
- **In Progress**
- **Resolved**

©2026 Tanium Inc. All Rights Reserved

- **Unresolved**

> **Best Practice:** The more quickly you can evaluate the risk associated with a given activity, the more quickly you can begin resolving a threat. Develop a plan for investigating and resolving alerts and be diligent about assigning alert statuses. Alert status dispositions are used to calculate the mean time to investigation and mean time to resolution; both key success metrics for Threat Response.

Additionally when an alert is suppressed by a suppression rule, the status of an alert is **Suppressed**. This status is removed from a suppressed alert when the suppression rule is removed.

View alerts by intel document

From the Main menu, go to **Modules** > **Threat Response Intel**. To open a single piece of intel, click the name of the item. From the individual page, you can review alerts that are associated with the intel, the activity over the last 30 days, the MITRE technique ID, and you can edit the definition.

Each Signal can have one or more associated MITRE technique IDs. Technique IDs can categorize Signals to better align with the MITRE Attack Framework and help map coverage to the different tactics and techniques. You can filter alerts by technique ID.

You can also initiate on demand scans for intel documents from the intel page.

Microsoft Defender alerts

Microsoft Defender is an anti-malware component of Microsoft Windows. Use Windows Defender alerts to gain visibility into common areas of Windows for changes which might have been caused by spyware, malware, and general security events. Windows Defender integration requires enabling the **Consume Defender Alerts** setting in a detection configuration for a deployed profile. By default, this setting is enabled for new configurations. For existing configurations, this setting needs to be enabled.

To subscribe to Defender process actions, such as Event ID 1007, go to Settings and click **Service** > **Misc**. Select **Microsoft Defender Process Action**.

When Defender generates an alert on a Windows endpoint, an alert is generated in Threat Response that you can view in the alerts page. You can filter the alerts page for Defender alerts.

©2026 Tanium Inc. All Rights Reserved

Enabling the **Generate Defender Reactions** setting in a detection configuration has Threat Response treat Defender detections as reactions instead of standalone findings for that profile. Enabling this setting overrides the global `processActionsAsPrimaryFindings` setting for that profile: a single Defender malware-action event produces either an alert or a reaction, not both.

Deep Instinct alerts

Deep Instinct is a solution that applies deep learning to cybersecurity and adds next-generation AV capabilities to Threat Response by integrating the investigative abilities of Threat Response to Deep Instinct alerts. For example, you can use the quarantine, collection, investigation, and remediation capabilities from Deep Instinct Alerts in Threat Response. Deep Instinct alerts that are saved on the Deep Instinct cloud can leverage Tanium roles and permissions to control access to alert data, enabling customers to access Deep Instinct alert data in a GDPR compliant setting.

Deep Instinct integration is available on Windows and macOS endpoints. Deep Instinct integration requires enabling the Generate Deep Instinct Alerts setting in a detection configuration for a deployed profile. By default, this setting is disabled for new configurations. For alerts to be returned from endpoints, the Deep Instinct agent must be running on the endpoint. Deep Instinct alerts are throttled as to not cause performance issues on an endpoint.

When Deep Instinct generates an alert on an endpoint, an alert is generated in Threat Response that you can view in the alerts page. You can filter the alerts page for Deep Instinct alerts. Deep Instinct Alert details contain a **Deep Instinct** section that shows Event Type, Event Action, File Path, File Type, file Hash, and Signature where applicable.

Deep Instinct alert details also include the Advanced Details JSON in the alert Details Drawer, matching the behavior of other alert types.



Note: For the integration to work correctly, you must configure additional flags for the Deep Instinct Agent (D-Client) using the Deep Instinct CLI. For more information, see the Deep Instinct documentation or contact Deep Instinct support.

Deep Instinct alerts feature a Deep Instinct section in the alerts details section of each Deep Instinct alert. Each alert shows one of the following event types from Deep Instinct:

- Deep Static Analysis – Detection

©2026 Tanium Inc. All Rights Reserved

- Ransomware Behavior
- Arbitrary Shellcode
- Malicious PowerShell Command Execution
- Malicious JavaScript Command Execution
- Remote Code Injection
- Credential Dumping
- Suspicious Script Execution
- Reflective DLL Injection
- .Net Reflection
- AMSI Bypass
- Known Payload Execution



Note: Threat Response does not generate alerts for Deep Instinct “Suspicious Events” events.

In addition to showing the Event Action that Deep Instinct took in response to the alert, You can view the file path and type of the artifact that caused the alert and the probability percentage that the detection was of several types of malware as calculated by Deep Instinct.

Investigate reputation data

About this task

Investigating reputation data requires the reputation service to be configured. See Reputation data on page 103 for more information.

For endpoints that use reputation intel, hashes found by the saved questions are sent to the reputation service for assessment. If this intel generates an alert, the hashes display with red or yellow status. Any known malicious matches automatically initiate an on-demand scan on targeted computer groups and generate an IOC for ongoing background scans. Each reputation IOC can

©2026 Tanium Inc. All Rights Reserved

contain up to 20 hashes. These IOCs are listed with **Reputation** as their source.

When the reputation for a hash changes, the intel is updated. For example, if a hash is no longer considered malicious according to reputation data, the associated intel document is updated so no further alerts are generated. If no malicious hashes exist in an intel document, the document is deleted.

1. To view more details about a hash, open the side panel. A hash can have one of the following ratings:
    - Non-Malicious (Green)
    - Malicious (Red)
    - Suspicious (Yellow)
    - Unknown (Gray)
    - Pending
2. Click a hash to view more details. For reputation data that comes from VirusTotal, you can expand the details and see a color-coded list of intelligence providers that have assessed the hash.

Result

The Threat Response icon pulses while the on-demand scan is running. After the on-demand scan completes, you can use the Interact icon to view the detailed results of the scan. Alerts are generated and gathered asynchronously from the scan. Alerts might be displayed on the Alerts page before the scan completes.

Investigate alerts

About this task

If you have a suspicious alert, you can open a live connection to investigate further.

1. From the Main menu, go to **Modules** > **Threat Response Alerts**. Select the alert that you want to investigate. You can investigate one alert at a time.
2. From the alerts results, click the name of the endpoint to which you want to open a live connection.
3. Click **Start live connection**.

Result

©2026 Tanium Inc. All Rights Reserved

The live endpoint page opens, with appropriate filtering for the type of alert you are investigating. Take a snapshot of suspicious endpoints for saved evidence.

Distinguish between malicious and false positive alerts

When Threat Response begins to return alerts, the next common question is "How do I know if this alert is legitimately bad?" This can be easy or very complicated to verify. Use a systematic approach to assess results and help determine if an alert shows malicious activity, for example, are other alerts encountered in the same environment from antivirus or a network device. The following approach is useful when assessing alerts:

1. Review the complete results in the alert to determine if it appears to be a suspicious process (appdata\local\temp\svchost.exe) or come from suspicious ancestry (outlook.exe > 2r4fe34.exe > excel.exe > cmd.exe) or anything else that looks unusual based on the alert details.

2. Search all alerts to see if the associated activity only occurs on one endpoint, several endpoints, or a very large number of endpoints.

3. Ask about software installed on endpoints to verify if the alert is normal enterprise software.

4. Pivot to a live connection to review the recorded telemetry of the processes. For more information, see Direct connecting to endpoints and exploring data.

    a. Look for any suspicious network connections by this process or around the same time on the endpoint. For more information, see Search for events.

    b. Look at the file activity in this process on the endpoint during this time for unusual activity. File system events include files written to directory locations on the endpoint. The associated process and user context are included. Examples: A malware file copied to a location that Windows Update uses, or content changes made to a file.

    c. Look at the registry activity under this process and on this endpoint around this time. For example, changes to the registry, such as the creation or alteration of registry keys and values. Registry data in an alert contains the associated process and user context.

    d. Look for unusual images being loaded into this process. For example, the full path

©2026 Tanium Inc. All Rights Reserved

and hash, the entity that signed an image, or a designation of "Unsigned" if the image is not signed. A possible example is the loading of an unsigned DLL.

5. Search for the hash reputation of the process to see if this is a known file or unknown. For more information, see Tanium Reputation User Guide.

6. Collect evidence for offline analysis with Live Response, including a memory capture if necessary. For more information, see Collecting data from endpoints with Live Response.

Note: For guidance in assessing signal alerts, contact Tanium Support. For more information, see Contact Tanium Support on page 373.

Filter false positives

If you have false positives, you need to filter them from future alerts. Whenever possible, suppression should be the default method of filtering false positives and tuning alerts. Look for alerts that are common to large sets of false positives and create a suppression to filter them from the environment.

There are a few occasions when a suppression is not possible, and a signal should be duplicated and edited, with the duplicate being deployed instead of the Signal Feed signal as a last resort.

If there is a signal that is alerting for a process that is run continuously on large numbers of endpoints and initiates numerous alerts that suppression impact an endpoint, you might need to make a duplicate signal and edit and deploy that instead. This is an unlikely scenario, but can occur especially in cases related to new signals. It is important to test signals on a small subset, and in phases, to solve false positives before they are run at scale. For more information, see Testing intel for deployment.

When suppressing alerts, you need to find something unique about the alerting process or process ancestry for the suppression to work as expected. This typically is the process or process ancestry path, command line argument, or user that is always present in the false positive alerts. This unique data can consist of a hash, if the hash does not change (for example, binaries and objects that are not expected to update or patch).

If there is no obvious way to eliminate false positives using process data, contact Tanium Support. For more information, see Contact Tanium Support on page 373.

©2026 Tanium Inc. All Rights Reserved

Add alerts to an investigation in Tanium Investigate

Add to an Investigation in the Actions column to add the alert to an investigation in Tanium Investigate. With Tanium Investigate you can identify the root cause of issues that arise on Tanium-managed endpoints and arrive at resolutions to issues more quickly. For more information, see Tanium Investigate User Guide.

Deploy an action to an endpoint

About this task

If you have a suspicious alert, you can deploy an action to a single affected endpoint directly from the alert.

1. From the Main menu, go to **Modules** > **Threat Response Alerts**. Select the alert for which you want to deploy an action to remediate or perform other action.
2. Click **Actions** > **Deploy Action**.
3. The **Deploy Action** page appears and the targeted endpoint is identified.
4. Select the package that you want to deploy. Depending on the package that you select, you are prompted to provide parameters for the package. If you select a package for Live Response, you can specify the collection configuration and destination configuration you want to use for Live Response file collection.
5. Provide a unique name and description for the action.
6. If you do not want to deploy the action immediately, specify a start to create a scheduled action. The time refers to the system clock on the Tanium Server, not on the endpoint. For example, if you specify the action to deploy at 1:00 am, it deploys when the Tanium Server system clock time is 1:00 am.
7. Optionally specify an end time. This is important If you configure reissue intervals for the action, unless you are sure it is the type of action that you want to reissue indefinitely. If you are not sure, configuring the schedule to end in six months is better than running indefinitely.
8. You can schedule the action to repeat at intervals. Specifying to reissue an action creates a scheduled action. Specifying a reissue interval is appropriate when:
    - Action approval is enabled and you are not certain it will be approved before the action expires.

©2026 Tanium Inc. All Rights Reserved

- You want to be sure software or configuration updates are made not only to the clients currently online but also to those currently offline that will be predictably online within a window that the reissue interval defines.
- The action is a continual hygiene practice. For example, you want to check periodically that a client service is running or a client configuration has a particular value.

9. Click **Deploy**. Confirm that you want to deploy the action.

Initiate a Response Action from an alert

About this task

If you have a suspicious alert, you can initiate a response action to a single affected endpoint directly from the alert. Initiating Live Response, Quarantine, or Gather Snapshot deploys a *response action*. A response action, unlike a scheduled action, runs once during a provided time range and ensures that if an endpoint is not online when you deploy the action, it runs when the endpoint comes online. Once deployed, from the Main menu, go to **Modules** > **Threat Response Response Activity** to view the status or stop a response action.

1. From the Main menu, go to **Modules** > **Threat Response Alerts**. Select the alert for which you want to deploy an action.
2. Click **Response Actions** > **Live Response**, **Response Actions** > **Quarantine**, **Response Actions** > **Gather Snapshot**, **Response Actions** > **Download File**, or **Response Actions** > **Unquarantine**.

   Note: When you download a file as a response action, the file is saved as saved evidence. From the Main menu, go to **Modules** > **Threat Response Saved Evidence** > **Files** to access the files that you download.

3. Provide parameters for the response action. For example, if you select the response action for Live Response, you can specify the collection configuration and destination configuration you want to use for Live Response file collection. For Quarantine response actions you must select the quarantine profile to use. Changes to the profiles or rules after a quarantine has been applied on an endpoint has no effect on that endpoint unless it is unquarantined and requarantined.
4. Click **Run**. Confirm that you want to deploy the response action.

©2026 Tanium Inc. All Rights Reserved

Result

You can select up to 100 alerts to assign quarantine and unquarantine response actions to at a time.

Remediate alerts in Tanium Enforce

About this task

You can create a remediation policy in Tanium Enforce, and specify conditions to enforce that policy from an alert. For example, a remediation policy defines specific actions to perform for an alert, and an enforcement defines the endpoints and schedule for performing the actions defined in the policy. Policies such as deleting files, killing a process, and performing registry tasks are available to perform when an alert is generated. By default, the remediation only targets the endpoint that generated the alert. To create remediation policies from an alert, Tanium Enforce must be installed . Additionally, to create remediation policies in Tanium Enforce, the **Enforce Create Enforcement** permission must be granted.

1. From the Main menu, go to **Modules** > **Threat Response Alerts**. Select the alert that you want to remediate in Tanium Enforce.
2. Select **Actions** > **Remediate in Enforce**.

   Note: If an instance Tanium Enforce is not installed, this option is not available from the Actions menu.
3. In the Policy Details section, provide a name and description for the policy.
4. In the Tasks section, click **Add Tasks** to perform as part of the remediation. You can select multiple tasks to add. Each task that you add to the remediation policy requires additional data that is by default populated with the data from the alert. Available tasks are:

   Delete file

   Provide a path to a single file to delete. By default, this path is populated with the data from the alert. Select to continue or exit if an error occurs.

   Kill process

   Select to use the Name, Path, or Hash of the process. Paths support wildcard syntax such as *, !, and ?. Group syntax is also supported. Hashes support an optional maximum file size. Provide any additional command line arguments for a process. Command line arguments support regular expression syntax such as C:\^Win$\.* .

©2026 Tanium Inc. All Rights Reserved

Provide a timeout value in seconds. If the number of seconds you specify is exceeded without killing the specified process, the kill process task fails. You can additionally provide a number of attempts for the task before the task fails.

Select to continue or exit if an error occurs.

Edit Registry Data

Select a hive in which to edit the registry data: HKEY_CLASSES_ROOT HKEY_LOCAL_MACHINE HKEY_CURRENT_CONFIG HKEY_USERS

Additionally provide the path relative to the hive you select. For example, System\CurrentControlSet\Hardware Profiles\Current

Select the type of the data to edit and provide new data to use to replace the value of the existing data.

Select if you want to create the value using the data you provided if no value matching the alert is detected. Select to continue or exit if an error occurs.

Update Registry Value

Select a hive in which to update the registry data: HKEY_CLASSES_ROOT HKEY_LOCAL_MACHINE HKEY_CURRENT_CONFIG HKEY_USERS

Additionally provide the path relative to the hive you select. For example, System\CurrentControlSet\Hardware Profiles\Current

Select to edit the value with data that you provide, or to delete the current value. Select to continue or exit if an error occurs.

Delete Registry Key

Select a hive in which to delete the registry key: HKEY_CLASSES_ROOT HKEY_LOCAL_MACHINE HKEY_CURRENT_CONFIG HKEY_USERS

Additionally provide the path relative to the hive you select. For example, System\CurrentControlSet\Hardware Profiles\Current

Select to continue or exit if an error occurs.

Run Service Action

Use to control the state of a service on the affected endpoint. For example, if malware has installed itself as a Windows service, stopping the service prevents further execution.

©2026 Tanium Inc. All Rights Reserved

Provide the name of the service to target. Select the action to perform. The available actions depend on the platform of the affected endpoint:

- Windows: **Start**, **Stop**, **Pause**, or **Resume**
- Linux: **Start**, **Stop**, **Restart**, **Enable**, or **Disable**
- Mac: **Load**, **Unload**, **Enable**, or **Disable**

> **Important:** For the **Service Name** field, enter the Service Name, not the Service Display Name.

Select to continue or exit if an error occurs.

Run Service Configuration

[Windows only] Use to change the startup type of a Windows service. For example, after stopping a malicious service, setting the startup type to Disabled prevents it from restarting after a reboot. Provide the name of the service to target. Select the startup type: Auto, Delayed, Manual, or Disabled.

> **Important:** For the **Service Name** field, enter the Service Name, not the Service Display Name.

Select to continue or exit if an error occurs.

5. In the Enforcements section, click **Add Enforcement**. Select **Computer Group** to target the remediation to an entire computer group. Select **Individual Computers** to provide one or more endpoints for the remediation to target. Add the fully qualified host name of each endpoint you want the remediation to target. Comma delimit multiple endpoints. Provide a start and end time for when you want to perform the remediation. Select to distribute over time to balance resource use over a time duration that you specify. The duration of the Distribute over time setting must be at least 10 minutes shorter than the Issue time setting. Select if you want to repeat the action and how often.
6. Click **Remediate**. The remediation is available in Tanium Enforce. From the Main menu, click **Modules > Enforce > Policies > Remediations** to view and edit the remediation in Tanium Enforce.

©2026 Tanium Inc. All Rights Reserved

Export alerts

About this task

Export alerts to a CSV file.

1. From the Main menu, go to **Modules** > **Threat ResponseAlerts**. Select the alerts that you want to export.

   > **Note:** Note: You can export up to 10,000 alerts.

2. Click **Actions** > **Export to CSV**.
3. Alert data is exported to a CSV file with the following data (if available) for each alert:

Result

- Date
- Endpoint
- Event Type
- Hash
- Hash Type
- Intel Name
- Intel Source
- MITRE Technique(s)
- Outbound Impact
- On-Demand Scan ID
- OS
- Path
- Platform

©2026 Tanium Inc. All Rights Reserved

- Status

The CSV file download is managed through the web browser. All exports are exported to the downloads directory of the web browser that initiated the export.

Delete alerts

You can delete alerts any time. If an alert is matched again later, the alert is generated again.

Suppress alerts

About this task

Create suppression rules to prevent the creation of a Signal-based alert when an intel match occurs. Use suppression rules to reduce false positives for Signals that you cannot edit, such as those from the Tanium Signal Feed. You can also add suppression rules for custom Tanium Detection types, like Process Injection. Suppression rules are not intended for use as a substitution for properly crafted Signals; if you are suppressing alerts consistently due to a Signal not matching as intended, it is a good indication that the Signal should be revised to more accurately match. By thoughtfully analyzing alerts you can tune the Signals that generate them optimally. See Reference: Authoring Signals on page 403 for more information.

Suppressed alerts are removed from the database after seven days by default. You can edit the number of days to wait after an alert is suppressed before removing it from the database in **Settings** from the Threat Response overview page.

You can apply rules that suppress alerts that match Process Path, Process Command Line, Parent Command Line, Process Hash, Parent Process Path, Ancestry Path, Ancestry Command Line, and User.

> **Note:** All of the selected suppression fields are required to match before the alert is suppressed.

The **Suppression Rules** page displays a **Scope** column that shows how each rule applies to profiles:

- **All Profiles**: the rule applies to every profile that uses the matched intel.

©2026 Tanium Inc. All Rights Reserved

- A list of profile names: the rule applies only to the profiles shown. If more profiles are bound than fit in the column, the column shows the first few names and a **+N** indicator. Point to the indicator to view the remaining profile names.

- **Orphaned**: the rule targeted profiles that have all been deleted. The rule remains in the list but does not apply to any active profile.

- **Selected Profiles**: the rule targets specific profiles that you do not have read access to. Contact your Threat Response administrator to request profile-read access if you need to see which profiles are bound.

Filter the **Suppression Rules** list by scope, by orphaned state, or by profile binding. Expand the advanced filters and select values to narrow the list. When you select multiple profile bindings, the list shows rules bound to any of the selected profiles.

1. From the Main menu, go to **Modules** > **Threat Response Intel** > **Suppression Rules** and click **Add Rule**.

2. Select the type of suppression rule to create. **All Signals** rules apply to all Signals where a match occurs. An intel-specific rule only applies to matches to a specific intel document that you specify. Select **All Signals** or **Intel-Specific**. If you select **Intel-Specific**, select an available intel type.

3. Provide a name and description for the suppression rule.

4. Select the fields that you want to use for suppression rules. For process injection suppression rules, specify artifacts that are both the actor and target process of process injection in the corresponding fields. The fields are identical for both the actor and target processes.
    a. **Process Path**: The path in the file system to a specific process. For example, c:\windows\notepad.exe.
    b. **Process Command Line**: Additional parameters that were provided for a process. For example, if a process is wevtutil.exe, a possible process command line is: wevtutil cl Application.
    c. **Parent Command Line**: The full command line of the parent process.
    d. **Parent Process Path**: The path in the file system to a parent process. For example, c:\windows\system32\cmd.exe.
    e. **Ancestry Command Line**: Additional parameters that were provided for a parent process.
    f. **Ancestry Path**: The path in the file system to a process more remote than a parent process.

©2026 Tanium Inc. All Rights Reserved

g. **Process MD5/SHA1/SHA256**: A specific MD5, SHA1, or SHA256 hash value that corresponds to a process.
h. **User**: A specific user on the system that is associated with a process.

> **Note:** If a Signal has generated an alert, you can click the **Suppress Alert** link from an alert page to preview the expected values for each of the fields.

5. Specify how you want to compare the field to the alert. You can choose to suppress an alert if a field is a direct match, contains a value, or matches a pattern specified by a regular expression.
   a. Select **Is** to suppress an alert when a direct match occurs. For example, a specific hash value or user name matches.
   b. Select **Contains** to suppress an alert when a subset of the alert criteria matches. For example, a path that contains "Windows".
   c. Select **Matches** to suppress an alert when a pattern matches the criteria. A regular expression needs to match the whole string. If you want to match Win and Windows, the regular expression needs to be .*Win.*. By default, regular expressions in suppression rules are case insensitive. Use of ^ and $ and flags are not supported.
6. Select **Retroactive** to run the suppression rule against all existing alerts that have not been resolved. If unselected, the rule does not apply to existing unresolved alerts, but applies to future Signal matches.
7. Click **Preview** to view a list of existing unresolved alerts that match the criteria you specify in the suppression rule. Threat Response evaluates 1000 alerts at a time until all applicable alerts have been evaluated, or until 10,000 alerts have been evaluated. Click **Save**.

Suppress an alert

You can create a suppression rule directly from an alert. From the Main menu, go to **Modules** > **Threat Response Alerts**. Select an alert and click **Actions** > **Suppress**. The suppression rule page appears and features all of the values that are required to suppress the alert. Provide a name and description for the suppression rule and select **Retroactive** if you want to apply the suppression rule against all existing alerts that have not been resolved. Click **Save**.

Edit and delete suppression rules

You can edit or delete existing suppression rules. From the Main menu, go to **Modules** > **Threat Response Intel** > **Suppression Rules**. Select a suppression rule that you want to edit. Click **Actions** >

©2026 Tanium Inc. All Rights Reserved

Edit.

To delete a suppression rule, select the suppression rules that you want to delete. Click **Actions** > **Delete**.

When you edit a suppression rule that has no explicit profile scope, the editor shows an inline hint that the rule remains scoped to **All Profiles** until you select **Selected Profiles**.

Suppression rules and deleted profiles

If you delete a profile that a suppression rule targets, the suppression rule remains in **Suppression Rules** but no longer applies to any active profile. Review suppression rules after deleting profiles to remove or reassign any rules that targeted the deleted profile.

Orphaned rules appear in the **Suppression Rules** list with an **Orphaned** badge in the **Scope** column. On an orphaned rule, **Actions** > **Edit** is relabeled to **Actions** > **Re-scope**; select it to open the editor and bind the rule to one or more active profiles, or scope it to **All Profiles**. To remove an orphaned rule instead, select it and click **Actions** > **Delete**.

Note: If a custom role has **Profiles Write** but not **Threat Response Suppression Rules** write access, deleting a profile that a **Selected Profiles** suppression rule is bound to returns an error, even though the **Delete** action for the profile appears enabled. This occurs because removing the profile would narrow or orphan the bound suppression rule, which requires write access to suppression rules in addition to write access to profiles. To delete the profile, either grant the user **Threat Response Suppression Rules** write access, unbind the suppression rule from the profile first, or have a user with the required permissions perform the deletion. The Administrator and Operator roles include both permissions by default and are not affected.

Note: If deleting a profile would orphan one or more suppression rules, the delete confirmation dialog lists the specific rules that will be affected. This list only appears if you have the **Threat Response Suppression Rules** read privilege; without it, the dialog does not mention affected suppression rules.

View the status of a retroactive task

If you edit a suppression rule and select **Retroactive** to run the suppression rule against all existing alerts that have not been resolved, you can view the status of how that rule is retroactively applied.

©2026 Tanium Inc. All Rights Reserved

From the Main menu, go to **Modules** > **Threat ResponseIntel** > **Suppression Rules**. Click **Retroactive Tasks**. View the status column to see if the retroactive task is Not Started, Incomplete, Completed, or has resulted in an error.

Import and export suppression rules

Import and export suppression rules to move them from one platform to another. For example, you can export All Signals suppression rules from a test system and import them to a production system. All Signals type suppression rules are imported and exported as CSV or JSON files.

Export specific suppression rules

About this task

Note: The suppression rules table in the Export dialog includes a **Scope** column, shown after **Intel Name**.

1. From the Main menu, go to **Modules** > **Threat Response Intel** > **Suppression Rules**.
2. Select the suppression rules that you want to export. Click **Actions** > **Export**.
3. Provide a name for the exported suppression rules.
4. Select to export the suppression rules in CSV or JSON format. If you select JSON, intel-specific suppression rules are omitted from the export.
5. Click **Export**.

Export all suppression rules

1. From the Main menu, go to **Modules** > **Threat Response Intel** > **Suppression Rules**. Click **Export All**.
2. Select to export the suppression rules in CSV or JSON format.
3. Click **Export**.

Import suppression rules

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Threat Response Intel** > **Suppression Rules**. Click **Import** and browse to a JSON file that you want to import. Click **OK**. Suppression rules are imported as JSON files and have a file size limit of 1 MB.
2. Review the suppression rules to be imported. Click **OK**. You can **Skip** a suppression that is conflicting with one that already has the same name or **Import and Rename** to apply a suffix of `Duplicate <time stamp>` to the suppression. For example, if a suppression is named `test` and you select **Import and Rename**, the resulting imported rule would be named `test Duplicate <time stamp>`.
3. From the summary window that displays the suppression rules that have been imported, click **Finish**.
4. Refresh the list of suppression rules to view the suppression rules that have been imported.

Manage the impact of lateral movement with Tanium Impact

If you installed Tanium Impact, and are assigned the Impact Asset Items Read and Impact Asset Details Read permissions, an **Outbound Impact** column appears in the alerts results grid. The value in the **Outbound Impact** column quantifies the number of user accounts and endpoints that can be reached from the corresponding Windows endpoint. Click the alert to view the alert details. In the **Impact Details** section of the alert details you can view data to better understand the lateral impact the endpoint has in an environment should it become compromised to help prioritize alert remediation.

Click **Explore in Impact** to view more detailed information about how the Windows endpoint fits into a larger topology. For more information, see Contact Tanium Support on page 373.

Set up Tanium Connect forwarding

About this task

Threat Response sends event information to Tanium Connect by default. To save this event information, you must configure Connect for the events to be passed to a destination. If you do not configure a destination, the events are dropped.

You can configure a Connect forwarding connection at any time. If you configure the connection during the installation process, all history is captured.

©2026 Tanium Inc. All Rights Reserved

1. From Connect, create a new connection with **Event** as the source and **Tanium Threat Response Alerts** as the event group.
2. Select the Threat Response events that you want preserved.
    - **Match Alerts Raw** sends alert details in JSON format. Match alerts are generated when intel deployed in a profile matches an event on an endpoint.
    - **Match Alerts** sends alert details as strings. Strings can be encoded in Base64 if the **Base64 encode events sent to Connect** setting is enabled. Match alerts are generated when intel deployed in a profile matches an event on an endpoint.
    - **All Events** includes scan matches. When you select **All Events**, audit events and deleted alerts are not sent to the destination as part of the **All Events** information. Audit events and deleted alerts are included in the Tanium **Audit Report**. For more information, see Tanium Connect on page 342.

      > **Note:** In Threat Response 4.0, **All Events** is effectively the same as **Match Events**; it does not send messages and notifications. Messages and notifications have been converted to audit messages in Threat Response 4.0 and are sent with the Audit source. If you have configured **All Events** enable the **Audit Report** type in Connect to continue receiving the same messages you expect.

      When forwarding events to Tanium Connect using **Match Alerts** or **Match Alerts Raw**, an intel source field has been added that corresponds to the intel document that the generated alert is associated with.

If you want to Base64 encode event details that are sent to Connect, from the Threat Response overview page, click Settings , click **Service** > **Misc**, and enable **Base64 encode events sent to Connect**. For **Match Alerts** and **All Events**, enabling this setting encodes the details field of the sent data. The following table details the type of data for the details field of event details when this setting is enabled or disabled.

Base64 encode events sent to Connect implications

Setting state on Threat Response version	Match Alerts Raw	Match Alerts	All Events
Enabled on Threat Response version 3.10	JSON	B64	B64
Disabled on Threat Response version 3.10	JSON	STRING	STRING

©2026 Tanium Inc. All Rights Reserved

Setting state on Threat Response version	Match Alerts Raw	Match Alerts	All Events
Enabled on Threat Response version 4.0 and later	JSON	B64	B64
Disabled on Threat Response version 4.0 and later	JSON	STRING	STRING

3. Configure the destination; such as a SIEM service or Write to File.
   All data that is sent features a link to all alerts in the Threat Response workbench, which enables quick access to the alert in Threat Response for context.

Result

When configuring reputation intel for Threat Response, you do not need to configure Tanium Connect as Threat Response inserts data into the reputation database.

For more information see the Tanium Connect User Guide.

©2026 Tanium Inc. All Rights Reserved

Managing response activity

From the Main menu, go to **Modules** > **Threat Response Response Activity** to view the status, create or stop a response action. A response action, unlike a scheduled action, runs once during a provided time range and ensures that if an endpoint is not online when you deploy the action, it runs when the endpoint comes online. Initiate a response action to a single affected endpoint. You can initiate Live Response, Quarantine, download a file, or gather a snapshot from a targeted endpoint.

The response actions that you can view are restricted to the actions that the user created. Users that have the bypass privilege can view additional response actions. A user that has multiple personas can view their response actions across personas, providing the personas have the ability to view response actions.

You can initiate response actions from an alert. For more information, see Initiate a Response Action from an alert on page 273.

Create a response action for an endpoint

1. From the Main menu, go to **Modules** > **Threat Response** > **Response Activity**.
2. Click **Create** > **Download File**, **Create** > **Gather Snapshot**, **Create** > **Live Response**, **Create** > **Quarantine**, or **Create** > **Unquarantine**.
3. Select an endpoint that is the target of the response action.

   Note: When you download a file as a response action, the file is saved as saved evidence. From the Main menu, go to **Modules** > **Threat ResponseSaved Evidence** > **Files** to access the files that you download.

4. Provide parameters for the response action. For example, if you select the response action for Live Response, you can specify the package you want to use for Live Response file collection.
5. Click **Run**. Confirm that you want to deploy the response action.

Response Action: Download File

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Threat Response** > **Response Activity**.
2. Click **Create** > **Download File**.
3. Select an endpoint that is the target of the response action.
   When you download a file as a response action, the file is saved as saved evidence. From the Main menu, go to **Modules** > **Threat ResponseSaved Evidence** > **Files** to access the files that you download.
4. Provide the full path of the file you want to download to saved evidence.
5. Provide an expiration time and date that corresponds to the expiration of the response action.
   The response action runs every four hours until a status is reported from the endpoint, or until the expiration time on the response action occurs.
6. Click **Run Response Action**. Confirm that you want to deploy the response action.

Response Action: Gather Snapshot

1. From the Main menu, go to **Modules** > **Threat Response** > **Response Activity**.
2. Click **Create** > **Gather Snapshot**.
3. Select an endpoint that is the target of the response action.
   When you gather a snapshot as a response action, the snapshot is saved as saved evidence. From the Main menu, go to **Modules** > **Threat ResponseSaved Evidence** > **Snapshots** to access the snapshot that you gathered.
4. Provide an expiration time and date that corresponds to the expiration of the response action.
   The response action runs every four hours until a status is reported from the endpoint, or until the expiration time on the response action occurs.
5. Click **Run**. Confirm that you want to deploy the response action.

Response Action: Live Response

1. From the Main menu, go to **Modules** > **Threat Response** > **Response Activity**.
2. Click **Create** > **Live Response**.

©2026 Tanium Inc. All Rights Reserved

3. Select an endpoint that is the target of the response action.

4. Select the **Live Response Package** to use.
   You can select **Threat Response - Live Response [Linux]**, **Threat Response - Live Response [Mac]**, or **Threat Response - Live Response [Windows]** depending on the operating system of the endpoint from which you want to collect data.

5. Select one or more **Collections** to use.
   A collection defines the data to collect from an endpoint. Default collections are provided, or you can create custom collections. For more information about collections and a procedure for creating a collection, see Collections on page 299.

6. Select a **Destination**. You can select either **Defined Destination** or **Dynamic AWS S3 Configuration**.
   A destination is a location to save forensic data. The server that receives information from Live Response can be Azure, an Amazon S3 Bucket, or a server that communicates over SFTP, SCP, or SMB (Windows only - SMB destinations are not included in Live Response packages for macOS and Linux.) protocols. For more information about destinations and a procedure for creating a destination, see Destinations on page 292.

   A defined destination is a preconfigured definition - including authentication data - that you can use to receive data from the targeted endpoint. A dynamic AWS S3 configuration enables you to enter dynamic credentials that are used to authenticate with a specific destination you can use in the context of the response action.

7. If you select **Defined Destination**, provide the following information:
   a. Select one or more preconfigured destinations.
   b. Provide a **Base Directory** that corresponds to a directory name where files are placed as they are collected.
      This directory is created under the **Remote Path** value that you provide in the destination you are using for the Live Response package. For example, if you provide a **Base Directory** of `MyCollection` where the **Remote Path** is `FileCollection`, the result would be FileCollection/MyCollection. Review the **Remote Path** setting that is specified in the preconfigured destination to understand where collected files are located.

   c. (Optional) Select **Flatten Output Files** if you want all collected files placed in one directory where the filename includes the original path, but does not retain the folder structure.

©2026 Tanium Inc. All Rights Reserved

8. If you select **Dynamic AWS S3 Configuration**, provide the following information:
    a. Provide a **Bucket** that corresponds to the name of the S3 Bucket.
    When using an S3 bucket as a destination make sure that clients are synchronized with a time server. Transfers fail if the client time differs from the server time by more than 15 minutes.

    b. Provide an **Access Key** that corresponds with a secret access key. For example, `AKIAIOSFODNN7EXAMPLE`.
    c. Provide a **Secret Access Key** that corresponds with an access key ID. For example, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`.
    Manage your access keys as securely as you do your user name and password. When you create access keys, you create the access key ID and secret access key as a set. During access key creation, AWS gives you one opportunity to view and download the secret access key part of the access key. If you do not download the key or if you lose the key, you can delete the access key and then create a new one.

    d. Provide a **Session Token** that is a valid STS token if you are not using permanent keys.
    e. Provide a **Region** that corresponds to an explicitly defined S3 region.
    f. Provide a **Host** that corresponds to the fully qualified domain name of the host.
    g. Provide a **Port** that corresponds to the port to use for the connection for the destination. The default is 443.
    h. (Optional) Select **Use SSL** to enable SSL encryption.
    i. Select **Force Path Style Types** to force API calls to use path-style URLs where the bucket name is part of the URL path for accessing buckets.
    j. Select **Connection Timeout** to specify the amount of time to attempt to establish a connection.
    k. Provide a **Remote Path** that corresponds to a path on the destination where data is collected.
    l. Provide a **Base Directory** that corresponds to a directory name where files are placed as they are collected.
    This directory is created under the **Remote Path** value that you provide in the destination you are using for the Live Response package. For example, if you provide a **Base Directory** of `MyCollection` where the **Remote Path** is `FileCollection`, the result would be FileCollection/MyCollection.

    m. (Optional) Select **Flatten Output Files** if you want all collected files placed in one directory where the filename includes the original path, but does not retain the

©2026 Tanium Inc. All Rights Reserved

folder structure.

9. Provide an expiration time and date that corresponds to the expiration of the response action.
   The response action runs every four hours until a status is reported from the endpoint, or until the expiration time on the response action occurs.

10. Click **Run**. Confirm that you want to deploy the response action.

Response Action: Quarantine

1. From the Main menu, go to **Modules** > **Threat Response** > **Response Activity**.
2. Click **Create** > **Quarantine**.
3. Select an endpoint that is the target of the response action.
4. Select the Quarantine Package to use.
   You can select **Threat Response - Quarantine Endpoint [Linux]**, **Threat Response - Quarantine Endpoint [Mac]**, or **Threat Response - Quarantine Endpoint [Windows]** depending on the operating system of the endpoint you want to quarantine.
5. Select the Quarantine Profile to use.
   A profile enables you to make a package that contains configuration information and rules that you can deploy to targeted endpoints. For more information about the Tanium Default Quarantine Profile, see Quarantining endpoints on page 317.
6. Provide an expiration time and date that corresponds to the expiration of the response action.
   The response action runs every four hours until a status is reported from the endpoint, or until the expiration time on the response action occurs.
7. Click **Run**. Confirm that you want to deploy the response action.

Response Action: Unquarantine

1. From the Main menu, go to **Modules** > **Threat Response** > **Response Activity**.
2. Click **Create** > **Unquarantine**.
3. Select an endpoint that is the target of the response action.

©2026 Tanium Inc. All Rights Reserved

4. Provide an expiration time and date that corresponds to the expiration of the response action.
   The response action runs every four hours until a status is reported from the endpoint, or until the expiration time on the response action occurs.

5. Click **Run**. Confirm that you want to deploy the response action.

Stop a response action

1. From the Main menu, go to **Modules** > **Threat Response** > **Response Activity**.
2. Select the response action that you want to stop from the list of response actions.
3. Click **Actions** > **Stop**.

©2026 Tanium Inc. All Rights Reserved

Collecting data from endpoints with Live Response

A critical step in the incident response process is the collection of data from compromised endpoints for further forensic analysis. Threat Response provides a feature called Live Response that you can use to collect specific information from endpoints to use for forensic analysis, data correlation, and to investigate potentially compromised systems with a customizable and extensible framework.

Live Response collects forensic information from endpoints, and transfers the results to a network location that you specify in a package. The Live Response package contains configuration files that identify the data to collect, and where to copy the data. Specify the data that you want to collect from endpoints, and the network destination to save the collected files.

Destinations

About this task

A destination is a location to save forensic data. The server that receives information from Live Response can be Azure, an Amazon S3 Bucket, or a server that communicates over SFTP, SCP, or SMB (Windows only - SMB destinations are not included in Live Response packages for macOS and Linux.) protocols.

For SSH (SFTP/SCP) destinations, a user with write access to the share on the destination is required. Consider modifying the /etc/ssh/sshd_config file on the server to allow only SFTP or SCP access. A best practice is to use Linux SFTP/SCP destinations for SCP/SFTP transfers.



Note: SSH server destinations are only supported on Linux and macOS.

The key exchange algorithms supported by Live Response for SSH destinations include:

- curve25510-sha256@libssh.org
- ecdh-sha2-nistp256

©2026 Tanium Inc. All Rights Reserved

- ecdh-sha2-nistp384
- ecdh-sha2-nistp521
- diffie-hellman-group14-sha1
- diffie-hellman-group1-sha1
- diffie-hellman-group-exchange-sha256

Note: At least one of these algorithms must be supported by the server for SSH (SFTP/SCP) destinations.

For an SMB copy location, the system account is used. SMB shares work with domain joined endpoints. Either the specific endpoint must have write access, or the domain computers group must have write access. Required advanced permissions:

- Create files / write data
- Create folders / append data
- Write attributes

For Amazon S3 Bucket copy locations, ensure that clients are synchronized with a time server. Transfers fail if the client time differs from the server time by more than 15 minutes.

To access SMB destinations when a system has been quarantined, you must also allow access via Kerberos to the Domain Controller. For more information, see the example in Reference: Custom rules examples on page 337.

1. From the Main menu, go to **Modules** > **Threat Response Management** > **Live Response**. Click **Create** > **Destination**.
2. In the General Information section, provide a name and description for the destination.
3. Select a destination type. Available destination types are Azure, S3, SSH, and SMB. The destination type that you select determines the types of required setting information. For more information, see destination types.
4. Click **Save**.

©2026 Tanium Inc. All Rights Reserved

Result

Tip: Be aware that keys you use to authenticate destinations should be considered public. Do not use keys that provide access to sensitive information, and ensure the keys are limited in scope. Do not allow keys to read, overwrite, or delete data.

Destination types

Different types of destinations require different settings.

Note: There is no option for disabling hostkey verification for SSH destinations in Live Response for Threat Response.

AZURE DESTINATIONS

For Azure destinations, the following settings are required:

Setting	Description
Storage Account	Provide the name of the storage account that contains Azure Storage data objects. The storage account provides a unique namespace for Azure Storage data that you can access from HTTP or HTTPS. Storage account names must be 3-24 characters long and can contain only lowercase letters and numbers.
Container	Provide the name of the Azure Container Instance where Live Response data is saved. Container names must be 3-63 characters long and can contain only lowercase letters, numbers, and hyphens. The name must start and end with a letter or number, and consecutive hyphens are not allowed.
Key File	Provide the storage account access key to construct a connection string to access Azure Storage. The values in the connection string are used to construct the Authorization header that is passed to Azure Storage.
SAS Token	A shared access signature (SAS) is a token that permits delegated access to resources in your storage account. The SAS token encapsulates all of the information needed to authorize a request to Azure Storage on the URL.
Host	Optionally, provide a custom host for Azure Storage. Use this setting for Azure Government cloud instances, which use a different Azure Blob host than commercial Azure instances. If you leave this field blank, Live Response uses the default Azure Storage host.

©2026 Tanium Inc. All Rights Reserved

Setting	Description
Maximum Attempts	Specifies the maximum number of attempts an operation will be tried before producing an error.
Simultaneous Uploads	Specifies the number of concurrent uploads that can occur.
Connection Timeout	The amount of time to attempt to establish a connection.

S3 DESTINATIONS

For S3 destinations, the following settings are required:

Setting	Description
Bucket	The name of the S3 Bucket. When using an S3 bucket as a destination make sure that clients are synchronized with a time server. Transfers fail if the client time differs from the server time by more than 15 minutes.
Access Key ID	An ID that corresponds with a secret access key. For example, `AKIAIOSFODNN7EXAMPLE`
Secret Access Key	A secret key that corresponds with an access key ID. For example, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY` . Manage your access keys as securely as you do your user name and password. When you create access keys, you create the access key ID and secret access key as a set. During access key creation, AWS gives you one opportunity to view and download the secret access key part of the access key. If you do not download the key or if you lose the key, you can delete the access key and then create a new one.
Session Token	A valid AWS Security Token Service (STS) token. Provide a Session Token when authenticating with temporary credentials issued by AWS STS or assumed through an IAM role. Leave this setting empty when authenticating with permanent access keys.
Region	An explicitly defined S3 region.
Host	The fully qualified domain name of the host.
Port	The port to use for the connection for the destination. The default is 443.

©2026 Tanium Inc. All Rights Reserved

Setting	Description
Use SSL	SSL encryption is enabled.
Force Path Style Types	Forces API calls to use path-style URLs where the bucket name is part of the URL path for accessing buckets.
Connection Timeout	The amount of time to attempt to establish a connection.
Remote Path	A path on the destination where data is collected.

SSH DESTINATIONS

For SSH destinations, the following settings are required:

Setting	Description
Protocol	Select SFTP or SCP as the protocol to transfer collected files to the destination.
Authentication Type	Private Key or Password. The type of protocol that you select determines whether you are prompted to provide a private key or a password to authenticate with the destination.
Host	The fully qualified domain name of the host.
Port	The port to use for the SSH connection for the destination. The default is 22.
Username	The user name for the connection to the destination.
Password or Private Key	The password for the user name, or a private key to authenticate the connection to the destination. An RSA key must be base64 encoded before you enter it into the private key field.  **Note:** You cannot password protect private keys used for live response destinations. In PowerShell you can convert to base64 encoding using the following command: `[Convert]::Tobase64String([System.IO.File]::ReadAllBytes('<filepath>')) | clip`

©2026 Tanium Inc. All Rights Reserved

Setting	Description

	Adding | clip to the end of the command sends the base64 output directly to the clipboard for pasting. If you try to copy and paste from the command line output, it is possible to introduce carriage returns which break the input and produce the error " invalid character " in the Tanium data entry console.
	On Linux you can convert to base64 encoding using the following command:
	`cat <filepath> | base64 -w 0`
	On macOS you can convert to base64 encoding using the following command:
	`cat <filepath> | base64 -b 0`
	Note: Although the normal openSSH format is assumed to be base64, encode the entire key again before uploading.

Known Hosts	The content of an SSH known hosts file. See Generate known_hosts and test connections on page 297
Connection Timeout	The amount of time to attempt to establish a connection.
Remote Path	A path on the destination where data is collected. This path is relative to the home directory of the present user. Absolute paths are not supported.

SMB DESTINATIONS

Note: The SMB transfer protocol is only supported on Windows operating systems. SMB destinations are not included in Live Response packages for macOS and Linux.

For SMB destinations, the following settings are required:

Setting	Description
Universal Naming Convention	The UNC path of the destination. For example, `\\server\folder`

Generate known_hosts and test connections

About this task

©2026 Tanium Inc. All Rights Reserved

The **Threat Response - Live Response [Windows]** package contains taniumfiletransfer_32.exe and taniumfiletransfer_64.exe. When the package is deployed, the file that is appropriate for endpoint is copied to the endpoint and renamed to taniumfiletransfer.exe. Download taniumfiletransfer_32.exe or taniumfiletransfer_64.exe from the **Threat Response - Live Response [Windows]** package.

To see a list of supported protocols, run one of the following commands depending on the architecture you are using:

`taniumfiletransfer_64 protocol`

`taniumfiletransfer_32 protocol`

To see details about a specific protocol, including options for the protocol connection string, run: `taniumfiletransfer_64 protocol <protocol>`

To generate a known_hosts file for use with SFTP or SCP:

1. Connect to the host you want to get a capture from.
2. Get the target IP you want to transfer the file to.
3. Run the following command: `C:\> taniumfiletransfer_64.exe ssh-keyscan <host> > known_hosts` on Windows endpoints or `ssh-keyscan <host> > known_hosts` on Linux and macOS endpoints.

Result

To update the known_hosts file in the live response package paste the contents of the file that you generated to the known_hosts field in the destination. The ssh-keyscan command produces a file with all SSH fingerprints commented with a # character. Edit the file that is created by using this command and remove the # before the fingerprints that should be accepted. A description of the fingerprints is provided with two ## characters and these should be left as comments. If you use a non-standard port, the output in the known_hosts file needs to be edited to reference that port. Lines starting with a double-hash ## need to be edited. For example, if you are using port 222, update the line:

Host: 192.168.0.113:22 (192.168.0.113:22)...

to:

Host: 192.168.0.113:222 (192.168.0.113:222)...

©2026 Tanium Inc. All Rights Reserved

If the known_hosts file is not edited to reference the correct port, Live Response encounters a failure. The known_hosts file must be ASCII encoded.

Alternatively you can perform the following steps:

1. Generate the destination package. For more information, see Collect data from endpoints on page 312.
2. Delete the known_hosts file in the **Threat Response - Live Response [OS]** package.
3. Add the file you generated with no changes. A Linux package cannot be updated from a Windows endpoint due to the changes Windows makes to the file format.
4. Save the package.

To test sending a file via an SFTP string enter the following command:

```
C:\> taniumfiletransfer_64.exe send test_file -d
sftp://<user>:<password>@<host>:/<dir>#knownHostsFile=known_hosts
```

Collections

About this task

A collection defines the data to collect from an endpoint. The following configurations are provided with Live Response:

- **Standard Collection**: Use for default data. The standard collection contains file collectors to collect specific files from endpoints. See File Collector Sets for a reference of the file collectors that are contained in each type of collection. The following data is captured by default, and is configurable in the standard collection:
    - Enumerate Running Processes
    - Enumerate Process Modules
    - Enumerate System Drivers
    - Analyze Windows Prefetch
    - Analyze Windows Amcache

©2026 Tanium Inc. All Rights Reserved

    - Analyze Windows Shimcache
    - Analyze Windows Filesystem .LNK Files
    - Analyze Windows Scheduled Jobs
    - Analyze Windows Recent Files Cache
    - Analyze Windows User Assist Recent Applications
    - Analyze Network Connection Details
    - Analyze Process and File Handle Details
    - Analyze System Startup
- **Extended Collection**: Use to collect the same data as the standard collection, plus more file based artifacts, such as the kernel, the Master File Table, USN Journal, event logs, registry hive files, and so on. The extended collection contains file collectors to collect specific files from endpoints. See File Collector Sets for a reference of the file collectors that are contained in each type of collection. The following data is configurable in the extended collection:
    - Enumerate Running Processes
    - Enumerate Process Modules
    - Enumerate System Drivers
    - Analyze Windows Prefetch
    - Analyze Windows Amcache
    - Analyze Windows Shimcache
    - Analyze Windows Filesystem .LNK Files
    - Analyze Windows Scheduled Jobs
    - Analyze Windows Scheduled Tasks Via Schtasks
    - Analyze Windows Recent Files Cache

©2026 Tanium Inc. All Rights Reserved

- Analyze Windows User Assist Recent Applications
- Collect Parsed UsnJrnl Entries
- Analyze Network Connection Details
- Analyze Process and File Handle Details
- Analyze System Startup Applications
- Collect Recorder Database Snapshot

The option to **Collect Recorder Database Snapshot** enables you to collect a snapshot of either recorder.db or monitor.db from endpoints. **Collect Recorder Database Snapshot** creates a snapshot of a recorder database - whether or not it is encrypted - and adds the snapshot to the collection. The snapshot that this module creates is removed from the endpoint when the collection has completed. By default, recorder database snapshots are saved in a folder named RecorderSnapshot on a path that corresponds with the name of the endpoint. For example, <base_directory>\<endpoint_name>\collector\RecorderSnapshot\<database_name>.db.

- **Memory Collection**: Use for memory acquisition. The memory collection contains file collectors to collect specific files from endpoints. See File Collector sets on page 302 for a reference of the file collectors that are contained in each type of collection. Memory data is configurable in the memory collection.

You can create a custom configuration to collect specific data from endpoints.

1. From the Main menu, go to **Modules** > **Threat Response Management** > **Live Response**. Click **Create** > **Collection**.
2. In the General Information section, provide a name and description for the collection.
3. Select the modules that you want to include in the data collection.
   A module is a functional area of forensic investigation. For example, the Network Connections module collects data that is helpful to understanding network connections that the endpoint has been involved in. The operating system icons next to each module show the operating systems to which the modules apply.

   
   Note: The Dump System Memory module is not supported on macOS versions after Big Sur 11.X.

©2026 Tanium Inc. All Rights Reserved

4. Select the File Collector sets that you want to include in the collection. See File Collector sets on page 302 for more information.
5. Under Script Sets, select the script sets that you want to include in the collection. See Script sets on page 312 for more information.
6. Click **Save**.

File Collector sets

About this task

File collector sets to define the types of files that you want to collect from endpoints. For example, you can select all files of a specific type, or files that reside on a specific path. Live Response on Windows collects alternate data streams. The name of the alternate data stream is appended to the regular data stream preceded by an underscore. For example, if an alternate data stream named hidden_datastream exists for a file named hosts, this alternate data stream would be collected as <path>\hosts_hidden_datastream.



Note: When setting a maximum recursive depth, enter `-1` to represent unlimited.

File collector set details

File Collector set	File Collector	Featured in Collection	Operating System	Path	File Pattern
Hosts File	Windows Hosts File	Standard, Extended	Windows	%systemdrive%\ windows\ system32\ drivers\etc	(^hosts$)
	Non-Windows Hosts File	Standard, Extended	Linux, Mac	/etc	(^hosts$)
Etc Folder Tree	Etc	Standard, Extended	Linux, Mac	/etc	.*
Shell History Files	PowerShell	Standard,	Windows	%userprofile%\ AppData\ Roaming\ Microsoft\Windows\ PowerShell\PSReadline\	^ConsoleHost_history.txt$

©2026 Tanium Inc. All Rights Reserved

File Collector set	File Collector	Featured in Collection	Operating System	Path	File Pattern
	History	Extended			
	Bourne Again (bash) Shell History	Standard, Extended	Linux, Mac	$HOME	^\.bash_history$
	Bourne (sh) Shell History	Standard, Extended	Linux, Mac	$HOME	^\.sh_history$
	Bourne Again (bash) Sessions	Standard, Extended	Mac	$HOME/.bash_sessions	.*history.*
Secure Shell (SSH) Files	User's Known Hosts	Standard, Extended	Linux, Mac	$HOME/.ssh	^known_hosts$
	User's Authorized Keys	Standard, Extended	Linux, Mac	$HOME/.ssh	^authorized_keys$
	Current SSH Users	Standard, Extended	Linux, Mac	/var/run	^utmp.*
	SSH Logon Logoff	Standard, Extended	Linux	/var/log	^wtmp.*
	Failed SSH Logon	Standard, Extended	Linux	/var/log	^btmp.*
	SSH Last Logged On Users	Standard, Extended	Linux	/var/log	^lastlog$
	SSH Daemon	Standard,	Linux, Mac	/etc/ssh	^sshd_config$

©2026 Tanium Inc. All Rights Reserved

File Collector set	File Collector	Featured in Collection	Operating System	Path	File Pattern
	Configuration	Extended			
	SSH Client Configuration	Standard, Extended	Linux, Mac	/etc/ssh	^ssh_config$
Systemd Folder Tree	Systemd	Standard, Exended	Linux	/etc/systemd/system	.*
Kext Details	Kext Details	Standard, Extended	Mac	/var/db/ SystemConfiguration	^KextPolicy$
	Kext Details (v11+)	Standard, Extended	Mac	/var/db/ SystemPolicyConfiguration	^KextPolicy$
Master File Table	Windows Master File Table	Extended	Windows	%systemdrive%	(\MFT)
UsnJrnl	UsnJrnl	Extended	Windows	%systemdrive%\$Extend	(%.UsnJrnl$)
Kernel	Windows Kernel	Exended, Memory	Windows	%systemdrive%\windows\ system32\	ntoskrnl\.exe
System Registry Hives	Windows System Registry Hives	Extended	Windows	%systemdrive%\windows\ system32\config\	((^system$)\|(^security$)| (^software$)\|(^sam$))
User Registry Hives	Windows User Registry Hives	Extended	Windows	%userprofile%\	(^ntuser\.dat$)
Windows Event Logs	Windows Event Logs	Extended	Windows	%systemdrive%\windows\ system32\winevt\logs\	.*\.evtx
Windows Prefetch Files	Windows Prefetch Files	Extended	Windows	%systemroot%\prefetch\	(.*\.pf)|(layout\.ini)|(.*\.db)|(pfsvperfstats\.bin

©2026 Tanium Inc. All Rights Reserved

File Collector set	File Collector	Featured in Collection	Operating System	Path	File Pattern
Chrome User Data	Windows Chrome User Data - Cache	Extended	Windows	%LOCALAPPDATA%\Google\Chrome\User Data\ Default\Cache\	.*
	Windows Chrome User Data - Local Storage	Extended	Windows	%LOCALAPPDATA%\Google\Chrome\User Data\ Default\Local Storage\	.*
	Windows Chrome User Data - Profile	Extended	Windows	%LOCALAPPDATA%\Google\Chrome\User Data\ Default\	.*
	MacOS Chrome Data	Extended	Mac	$HOME/Library/Application Support/Google/Chrome	.*
	Linux Chrome Data	Extended	Linux	$HOME/.config/google-chrome	.*
Shell Configuration Files	Bourne Again (bash) Settings	Extended	Linux, Mac	$HOME	^\.bash(rc|_profile| _aliases)$
	C Shell (csh and tcsh) Settings	Extended	Linux, Mac	$HOME	^\.(tcshrc| cshrc)$
Available Shells	Available Shells	Extended	Linux, Mac	/etc	^shells$
Passwd and Group Files	Passwd and Group Files	Extended	Linux,Mac	/etc	^(passwd|group)$
Shadow Files	Shadow Files	Extended	Linux, Mac	/etc	^(shadow|gshadow| master\.shadow)$

©2026 Tanium Inc. All Rights Reserved

File Collector set	File Collector	Featured in Collection	Operating System	Path	File Pattern
Sudoers Configuration	Sudoers File	Extended	Linux, Mac	/etc	^sudoers$
	Sudoers.d Folder Contents	Extended	Linux, Mac	/etc/sudoers.d	.*
Mount Points	Mount Points	Extended	Linux	/etc	^fstab$
	NFS Mount Points	Extended	Linux	/etc	^exports.*
Preload Shared Libraries	LD Preload Shared Libraries	Extended	Linux	/etc	ld\.so.*
	LD Preload Shared Libraries Configuration Directory	Extended	Linux	/etc/ld.so.conf.d	.*
Auditd Configuration and Rules	LD Preload Shared Libraries	Extended	Linux	/etc/audit	.*
RPM GPG Keys	RPM GPG Keys	Extended	Linux	/etc/pki/rpm-gpg	.*
SSL/TLS Certificates and PKI	SSL/TLS Certificates Directory	Extended	Linux	/etc/pki/tls	.*
	SSL/TLS Certificate Authority	Extended	Linux	/etc/pki/CA	.*

©2026 Tanium Inc. All Rights Reserved

File Collector set	File Collector	Featured in Collection	Operating System	Path	File Pattern
	Directory				
User Recently Used/Deleted Files	Recently Used GTK Files	Extended	Linux	$HOME/.local/share	recently-used\ .xbel
	Recently Deleted Info	Extended	Linux	$HOME/.local/share/ Trash/ info	.*
	Recently Deleted Files	Extended	Linux	$HOME/.local/share/ Trash/ files	.*
User Vim Configuration	Vim Info	Extended	Linux, Mac	$HOME	^\.viminfo$
	Non-Windows Vim Configuration	Extended	Linux, Mac	$HOME	^\.vimrc$
	Windows Vim Configuration	Extended	Windows	%homepath%\	^_vimrc$
User Less History	Less History	Extended	Linux, Mac	$HOME	^\.lesshst$
User Database History	Database History	Extended	Linux, Mac	$HOME	^\.(psql|mysql| sqlite)_history$
Cron Settings	Cron Files	Extended	Linux, Mac	/etc/	cron.*
	Cron Logs	Extended	Linux, Mac	/var/log	cron.*
Spotlight Information	Spotlight Disk Database	Extended	Mac	/.Spotlight-V100/ Store-V2	. *store\\.db
	User Spotlight Shortcuts	Extended	Mac	$HOME/Library/ Preferences/	^com\\.apple\ \.spotlight\\.plist$

©2026 Tanium Inc. All Rights Reserved

File Collector set	File Collector	Featured in Collection	Operating System	Path	File Pattern
	User Spotlight Shortcuts	Extended	Mac	$HOME/Library/ Application Support/	^com\\.apple\ \.spotlight\\.Shortcuts$
User and Application Analytics	MacOS User and Analytics Information	Extended	Mac	/var/db/CoreDuet/Knowledge	^knowledgeC\\.db$
	MacOS Per-User and Analytics Information	Extended	Mac	$HOME/Library/Application Support/Knowledge/	^knowledgeC\\.db$
Program Execution Reports	Program Execution Reports	Extended	Mac	/Library/Logs/ DiagnosticReports	.*\\.core_analytics
	Program Execution Aggregate Analytics	Extended	Mac	/private/var/db/ analyticsd/ aggregates	.*
Domain User Information	Domain User Information	Extended	Mac	/private/var/db/ ConfigurationProfiles/Store/	ConfigProfiles\ \.binary
User Mail Data	User Mail Data	Extended	Mac	$HOME/Library/Mail/	.*
Microsoft Office	MacOS Microsoft Office Artifacts	Extended	Mac	$HOME/Library/Group Containers/	^MicrosoftRegistrationDB\ \.reg$
Deleted Users	MacOS Deleted Users	Extended	Mac	/Library/Preferences/	^com\\.apple\\.preferences\ \.accounts\\.plist$
Notifications	MacOS	Extended	Mac	/var/folders/	^db(-wal|-shm)*$

©2026 Tanium Inc. All Rights Reserved

File Collector set	File Collector	Featured in Collection	Operating System	Path	File Pattern
	Notifications Database Files				
Event Monitor	MacOS Event Monitor	Extended	Mac	/System/Library/LaunchDaemons/	^com\\.apple\\.emond\\.plist$
DHCP Leases	MacOS DHCP Leases	Extended	Mac	/private/var/db/dhcpclient/leases/	.*
Edge (Chromium) Internet Explorer Data Collection (Mac)	MacOS Edge (Chromium) Data	Extended	Mac	$HOME/Library/Application Support/Microsoft Edge	.*
Edge (Chromium) Internet Explorer Data Collection (Windows)	Windows Edge (Chromium) Data - Cache	Extended	Windows	%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Cache\	.*
	Windows Edge (Chromium) Data - Local Storage	Extended	Windows	%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Local Storage\	.*
	Windows Edge (Chromium) Data - Profile	Extended	Windows	%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\	.*
MacOS Finder Information	MacOS Finder MRU	Extended	Mac	$HOME/Library/Preferences/	^com\\.apple\\.finder\ \.plist$
	MacOS Recently Opened Items	Extended	Mac	$HOME/Library/Preferences	^com\\.apple\\.recentitems\ \.plist$
	MacOS	Extended	Mac	$HOME/Library/Application Support/	.*

©2026 Tanium Inc. All Rights Reserved

File Collector set	File Collector	Featured in Collection	Operating System	Path	File Pattern
	Recently Opened Items 11+			com.apple.sharedfilelist	
Network Services, Settings, and Logs	MacOS Network Services and Settings	Extended	Mac	/Library/Preferences/SystemConfiguration/	^preferences\\.plist$
	VPN Log	Extended	Mac	/var/log	^ppp\\.out$
	Daily Network Log	Extended	Mac	/var/log	^daily\\.out$
	Network Usage	Extended	Mac	/var/networkd	^netusage\\.sqlite$
	MacOS Remembered Networks	Extended	Mac	/Library/Preferences/SystemConfigurations/	^com\\.apple\\.airport\ \.preferences\\.plist$
Update and Backup Information	MacOS Last Update	Extended	Mac	/Library/Preferences/	^com\\.apple\\.SoftwareUpdate\ \.plist$
	MacOS Last Time Machine Backup	Extended	Mac	/Library/Preferences/	^com\\.apple\\.TimeMachine\ \.plist$
Scripting Additions	MacOS Scripting Additions	Extended	Mac	/System/Library/ScriptingAdditions/	.*
System Administrators	MacOS System Administrators	Extended	Mac	/var/db/dslocal/nodes/Default/groups/	^admin\\.plist$

©2026 Tanium Inc. All Rights Reserved

File Collector set	File Collector	Featured in Collection	Operating System	Path	File Pattern
Authorization Database	MacOS Authorization Database	Extended	Mac	/var/db	^auth\\.db$
Safari User Data	MacOS Safari User Data	Extended	Mac	$HOME/Library/Safari/	^(History\\.db|Downloads\ \.plist|TopSites\\.plist| RecentlyClosedTabs\ \.plist|Bookmarks\ \.plist| CloudTabs\\.db)$
Firefox User Data	MacOS Firefox User Data	Extended	Mac	$HOME/Library/Application Support/Firefox/Profiles/	^(places\\.sqlite|addons\ \.json|extensions\\.sqlite| extensions\\.json |search\\.sqlite)$

You can create custom file collector sets.

1. From the Main menu, go to **Modules** > **Threat Response Management** > **Live Response**. Click **Create** > **File Collector Set**.
2. In the General Information section, provide a name and description for the file collection set.
3. Click **Create File Collector**.
4. Provide a name for the file collector.
5. Provide a path for files to collect. Paths support environment variables and regular expressions. For more information, see Regular expressions and environment variables on page 314.
6. Provide a file pattern for the files to collect. File patterns support regular expressions. For more information, see Regular expressions and environment variables on page 314.
7. Specify the maximum depth of directories to recurse from the path you provided.
8. Specify the maximum number of files to collect.
9. (Optional) Select **Raw** to preserve the format of the files that are collected. When using **Raw**, the following file systems are supported: NTFS, ExFat, Ext, Fat, and HFS Plus.
10. Select the operating systems from which you want the file collector to collect files.
11. Click the check mark in the top right to save the file collector.

©2026 Tanium Inc. All Rights Reserved

12. Click **Save**.

Script sets

About this task

You can configure scripts to run on endpoints when you deploy the collection. PowerShell scripts run on Windows endpoints only. Python scripts run on Linux and macOS endpoints only.

1. From the Main menu, go to **Modules** > **Threat Response Management** > **Live Response**. Click **Create** > **Script Set**.
2. In the General Information section, provide a name and description for the script set.
3. Under **Scripts** click **Add a Script**.
4. Provide a filename for the script.
5. Select **Python** (Linux and macOS) or **PowerShell** (Windows only) as the type of script.
6. Provide any script arguments to use as part of running the script.
7. Add the script source.
8. Click **Save**.

Result

Script output is saved in a file that has the same as the script, and has -results appended to the file extension. For example, a script named test.ps1 creates output in test.ps1-results. All standard output is directed to the collector directory.

Collect data from endpoints

About this task

To collect data from endpoints, deploy a Live Response package.

Important: To prevent resource overload on endpoints, only issue this action manually. Do not create a scheduled action.

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Threat Response Response Activity** > **Create** > **Live Response**.
2. Target endpoints for data collection. Use an operating system-based question, for example: `Get Computer Name from machines with Is Windows containing "True"` .
3. Select the endpoints from which you want to collect data and click **Deploy Action**.
4. In the **Deployment Package** field, type `Live Response`.
5. Select the package that matches the collection and destination settings that you want to deploy.
6. In the **Base Directory** field, provide a directory name where files are placed as they are collected. This directory is created under the **Remote Path** value that you provide in the destination you are using for the Live Response package. For example, if you provide a Base Directory of MyCollection for an SSH destination where the **Remote Path** is FileCollection, the result would be /home/username/FileCollection/MyCollection because the remote path provided in SSH destinations is relative to the home directory of the present user. Depending on the type of destination, the location of the **Remote Path** can vary. For example, in SMB destinations it is explicit; whereas in SSH destinations it is relative to the home directory of the present user.
7. Optionally select **Flatten Output Files** if you want all collected files placed in one directory where the filename includes the original path, but does not retain the folder structure.
8. Click **Show Preview to Continue**.
9. After you preview the list of endpoints to which the action is being deployed, click **Deploy Action**.

Result

Threat Response tests the connection by writing a LRConnectionTestfile to the destination. If the write fails, the action tries the other destinations in the transfer configuration in the order they are listed in the configuration file. If all the connection tests fail, the action does not proceed.

Tanium shows the package as complete almost immediately after the package is downloaded on the endpoints. This completion is not accurate because Live Response runs in detached mode. File transfers continue after the action completes.

©2026 Tanium Inc. All Rights Reserved

The actual time to complete the transfer depends on the endpoint activity and connection speed between the endpoint and the destination system.

For macOS and Linux endpoints, memory data that is transferred to a destination is packaged in a ZIP file. For example, if you selected memory details as an included module, Live Response creates a ZIP file that contains a raw memory dump and additional system files. You can analyze this data with a tool such as Winpmem or Volexity Surge. For Windows endpoints, memory data is collected as one or more raw files.

Collect logs

In addition to the standard action logs on the endpoint (Tanium_Client_Location\Tools\IR\data\Action_xxxxx\Action_####.log), a log file of activities resides in the same directory. This file follows the naming convention: YYYYMMDDhhmm_LR.log.

When collection completes, the YYYYMMDDhhmm_LR.log is copied to the destination. The action log is not copied to the destination.

Use both the action log and the Live Response log to troubleshoot problems. The action log captures messages written to standard error (stderr).

Regular expressions and environment variables

File patterns support regular expression syntax.

The following table provides some example patterns to show how Live Response uses both regular expressions and environment variables on Windows, Linux, and macOS endpoints.

File patterns regular expression syntax

Example Live Response task	Operating system	Path	File pattern	Explanation
Collect host file	Windows	%systemdrive%\windows\system32\drivers\etc	^hosts$	Collects a single file called 'hosts' from an appropriate directory using the `%systemdrive%` environment variable to avoid

©2026 Tanium Inc. All Rights Reserved

Example Live Response task	Operating system	Path	File pattern	Explanation
				assuming the system drive is C: .
	Linux/ macOS	/etc	^hosts$	In this example, hosts matches.
Collect Bash History of every user	Windows	Not Applicable	Not Applicable	Not Applicable
	Linux/ macOS	$HOME	/.bash_history$	A file name that matches .bash_history . The forward slash in the file pattern /.bash_history$ is necessary because the path uses an environment variable ($HOME) and the environment variable does not include a trailing forward slash.
Collect a file named findme.txt from platform root	Windows	C:\	^findme.txt$	The filename starts with findme.txt
	Linux/ macOS	/	^findme.txt$	The filename starts with findme.txt

Any environment variables that you use resolve as described in the following table. Paths containing environment variables apply to all user profiles on the endpoint.

Environment variable support

Environment variable	Supported operating system	Corresponding value
%appdata%	Windows	C:\Users\username\appdata\roaming
%homepath%	Windows	\Users\username
%localappdata%	Windows	C:\Users\username\appdata\local

©2026 Tanium Inc. All Rights Reserved

Environment variable	Supported operating system	Corresponding value
%psmodulepath%	Windows	C:\Users\username\documents\windowspowershell\modules
%temp%	Windows	C:\Users\username\appdata\local\temp
`%tmp%`	Windows	C:\Users\username\appdata\local\temp
%userprofile%	Windows	C:\Users\username
%taniumdir%	Windows	Tanium Client directory. Defaults are: \Program Files\Tanium\Tanium Client\ (32-bit OS) \Program Files (x86)\Tanium\Tanium Client\ (64-bit OS)
$TANIUMDIR	Linux, Mac	Tanium Client directory. Defaults are: /Library/Tanium/TaniumClient/ (macOS) /opt/Tanium/TaniumClient/ (Linux)
$HOME	Linux, Mac	All user home directories that do not have a home directory set to blocklisted shells, and match shells that are listed in /etc/shells file. If there is no /etc/shells file, all shells are allowed.
Environment variables that are local to the endpoint are supported. For example, if %SYSTEMROOT% is set on an endpoint to expand to C:\WINDOWS , you can use such a variable on a path.		

©2026 Tanium Inc. All Rights Reserved

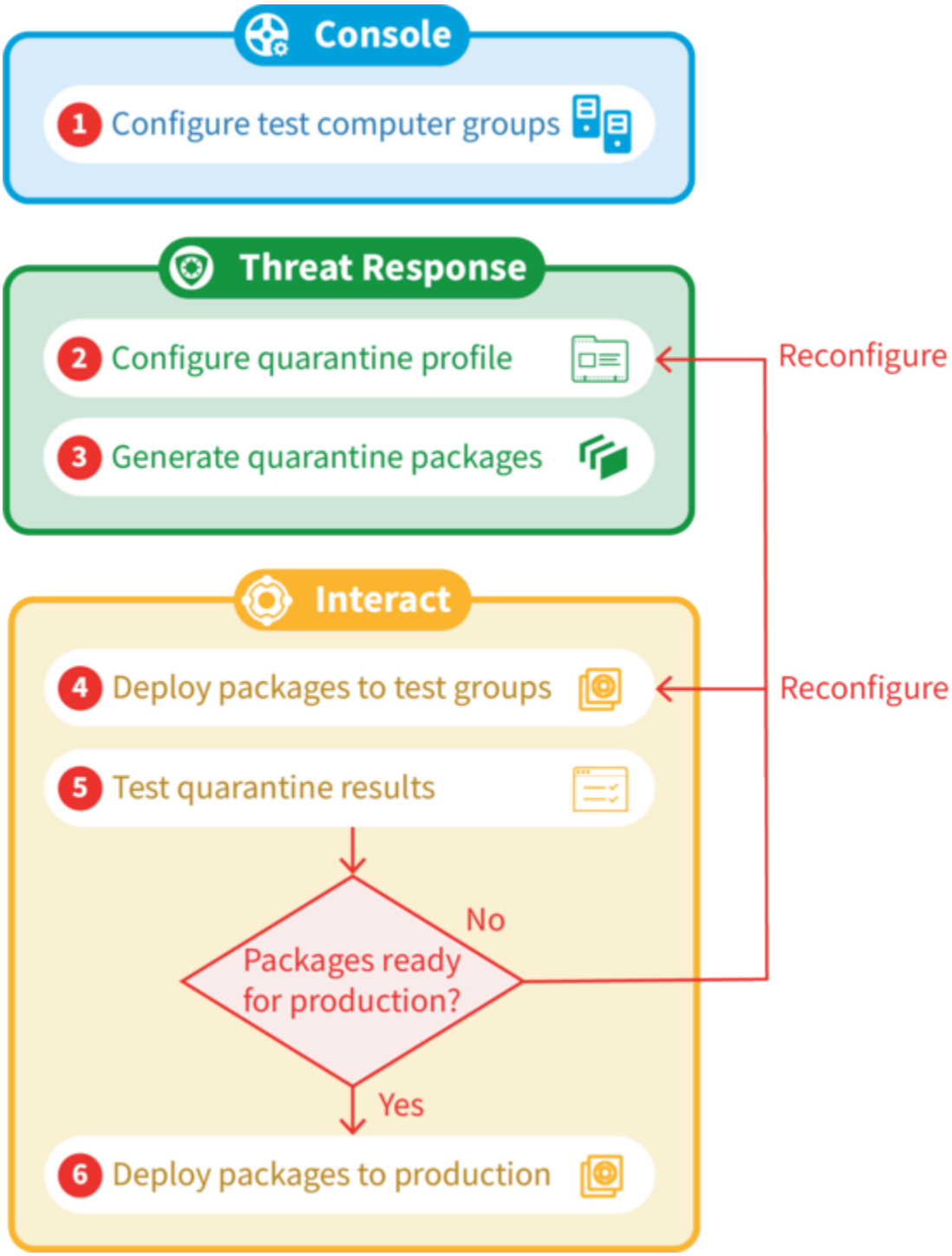
Quarantining endpoints

Quarantine a Windows, Linux, or macOS endpoint that shows evidence of compromise or other suspicious activity. Use Threat Response to apply, remove, and test for quarantine.

Quarantine enables you to create custom profiles that contain rules that define the parameters to use for quarantining endpoints. After you create a profile, you can generate packages that you can deploy to targeted endpoints to quarantine them. The following diagram illustrates the basic workflow for deploying quarantine profiles:

Figure 3. Example quarantine workflow

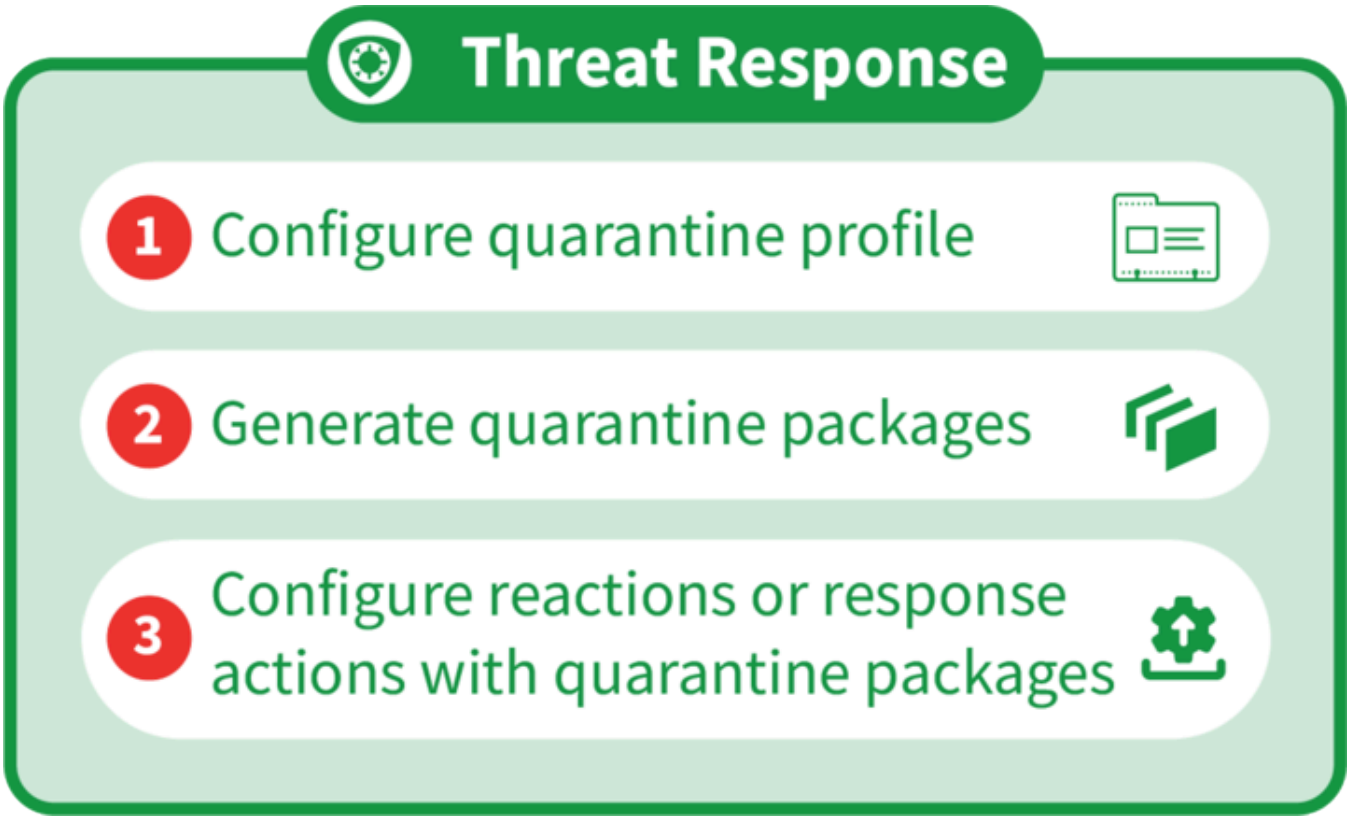
©2026 Tanium Inc. All Rights Reserved



You can also use quarantine profiles to use as part of a response action or reaction. In this case, you can generate quarantine packages that are used when reactions match on an endpoint or as a response action that you initiate as a response to an alert.

Figure 4. Example quarantine workflow

©2026 Tanium Inc. All Rights Reserved



When an endpoint is quarantined, by default the only approved traffic allowed on the quarantined endpoint includes:

- Between Tanium Client on the quarantined endpoint and Tanium Server over port 17472.
- Between the quarantined endpoint and DHCP or DNS servers to obtain and resolve IP addresses.
- Direct Connect connections to the endpoint.
- Live Response destinations.

Threat Response includes a safety feature that automatically reverses a quarantine policy. After a quarantine policy is applied, the effect of the policy is logged. If the endpoint is able to communicate with Tanium Server, Threat Response logs the successful application of the policy. If a policy prevents the endpoint from communicating with Tanium Server, Threat Response backs out the policy and saves logs in the action folder.

©2026 Tanium Inc. All Rights Reserved

Tip: Tanium Automate implements quarantine and quarantine removal in playbook steps. You can configure reusable playbooks with various steps and run a playbook multiple times to streamline and simplify your business processes. For more information on building a playbook, see Tanium Automate User Guide: Building playbooks. For more information on the available playbook steps, see Tanium Automate User Guide: Reference: Steps.

Before you begin

Important: Test quarantine policies before deploying the profile. Do not apply a profile until its behavior is known and predictable. Incorrectly configured profiles can block access to Tanium Server.

- You must have a Content Administrator account for Tanium Console. For more information, see Tanium Core Platform User Guide: Managing Roles.
- Identify the traffic that is required when an endpoint is under quarantine.
- You must have a lab endpoint on the target operating system (Windows, Linux, or Mac) you can use to test the quarantine policies. You must be able to physically access the machine or to access it using RDP (Windows) or SSH (Linux, Mac).
- You must have access to the endpoint that you want to quarantine through a sensor or saved question in the Tanium Console.
- Beginning with Threat Response 4.6, the Quarantine packages are included with Threat Response. Do not install the IRQuarantine solution on environments where releases of Threat Response 4.6 or later is installed.
- By default an attempt to quarantine an endpoint with a response action times out after seven days. If you are using quarantine as a response action, you can set the **Action Expiration Time** to a custom value when the response action is created. If you deploy quarantine packages to endpoints using Tanium Interact or the Tanium Console, the action uses the value of the package timeout.

©2026 Tanium Inc. All Rights Reserved

Note: Quarantine operates as a layer 3 network firewall and functions at the IP and port level without awareness of higher-layer protocols or application-specific traffic. Quarantine does not recognize any proxies or solutions that operate above layer 3 such as those at layer 4 (Transport) or layer 7 (Application). For these proxies or higher-layer solutions to interact with or be permitted by the quarantine solution, their details must be explicitly defined as `IP:Port` pairs in the quarantine configuration. If Tanium Client is connected through a proxy during the quarantine action and **All Tanium Servers** is selected, a rule for CurrentProxy is added to allow for Tanium Client communications.

Endpoint operating system requirements

Supported Windows versions

- Windows 7 (SP1)
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11
- Windows Server 2003
- Windows Server 2008
- Windows Server 2012
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025
- Windows Server 2012R2 or later
- Windows Server 2008R2 (SP1)

©2026 Tanium Inc. All Rights Reserved

Supported Linux OS versions

- AlmaLinux 8.x
- AlmaLinux 9.x
- AlmaLinux 10.x
- RedHat/CentOS 5 IPTables on SYSV
- RedHat/CentOS 6 IPTables on SYSV
- RedHat/CentOS 7 Firewalld on Systemd (Note: A reboot is required on RedHat/CentOS 7.1 endpoints after removing quarantine.)
- RedHat/CentOS 8
- RedHat/CentOS 9
- RedHat/CentOS 10
- Rocky Linux 8.x
- Rocky Linux 9.x
- Rocky Linux 10.x
- Ubuntu 12, 14 UFW on Upstart
- Ubuntu 15, 16, 18, 20, 22, 24, and 26 UFW on Upstart/Systemd

CentOS Stream 8 and 9 variants of CentOS are not currently supported.

Supported macOS versions

- OS X 10.9 Mavericks
- OS X 10.10 Yosemite
- OS X 10.11 El Capitan
- macOS 10.12 Sierra

©2026 Tanium Inc. All Rights Reserved

- macOS 10.13 High Sierra
- macOS 10.14 Mojave
- macOS 10.15 Catalina
- macOS 11.0 Big Sur
- macOS 12 Monterey
- macOS 13 Ventura
- macOS 14 Sonoma
- macOS 15 Sequoia
- macOS 26 Tahoe

OSX 10.8 - Mountain Lion and earlier releases are based on ipfirewall (IPFW) and are not supported.

Create quarantine rules

About this task

Quarantine rules are the building blocks of profiles. Each profile that you create contains one or more rules. Quarantine rules define allowed traffic direction, allowed IP addresses, ports, and protocols. All other traffic is blocked. These rules are in the same format for Windows, Linux and macOS. If you do not define any quarantine rules, the default values are used, which gives the quarantined endpoint access only to the Tanium Server and permits DNS/DHCP traffic. If you previously provided a Windows IPsec policy file, the IPsec policy overrides the custom quarantine rules.

1. From the Main menu, go to **Modules** > **Threat Response Management** > **Quarantine**. Click the **Rules** tab.
2. Click **Create**. Provide a name and description for the rule.
3. Select the **Direction** for the rule. You can select either **In** or **Out**. The value you select specifies whether incoming or outgoing traffic is allowed.
4. Select the **Protocol** for the traffic. You can select **ICMP**, **TCP**, or **UDP**. If you specify ICMP, the ICMP protocol is allowed to communicate to and from the specified addresses. This limitation is because IPSec does not filter ICMP Type/Codes. The filtering is done by

©2026 Tanium Inc. All Rights Reserved

advfirewall. When using quarantine rules to block the ICMP protocol, the MTU negotiation packages can become blocked when the size of the MTU package on the endpoint is larger than the router allowed MTU size. Normally the router will see a packet that is too large and send an ICMP packet to the endpoint to identify that the packet is too large and advises lowering the permissible MTU size. If the negotiation packet is not able to reach the destination due to quarantine, the endpoint can become unresponsive. The endpoint is still is quarantined but loses communication with the Tanium Server. Disabling ICMP traffic while quarantined should only be done after proper testing.

5. Enter an **IP Address** for the rule. Enter any IPv4 address or you can use ANY for all.
6. Enter a **CIDR**. Valid values are 0-32 or, if ANY is used in IP Address, undefined. This is the subnet mask that represents the number of bits available to the IP address. Undefined is the same as 32 and uses the IP address.
7. (TCP or UDP protocols only) Enter a **Port**. Valid values are 0-65535. Ranges are not currently supported, only individual ports or all ports can be defined. Setting the number as 0 allows all ports.

Create a quarantine profile

About this task

A profile enables you to make a package that contains configuration information and rules that you can deploy to targeted endpoints. When you create a profile you can define the criteria for the scope of a quarantine within the Threat Response workbench. You can import existing taniumquarantine.dat files into a profile. If you import an existing taniumquarantine.dat file into a profile, ensure that all configurations are specified in the correct syntax.

Quarantine uses the legacy `taniumquarantine.dat` file if the quarantine package is called directly. This file is ignored by quarantine actions that are issued by the Threat Response workbench and Threat Response API (for example in a reaction or response action). All quarantine actions issued from the Threat Response workbench or THR API (for example in a reaction or response action) ignore the taniumquarantine.dat file and use the appropriate `quarantineprofileconfig_#.dat file`. If no profile is specified in these cases, quarantine uses the default profile that is specified in the Threat Response Quarantine Workbench.

A syntax example is provided for each setting in the following steps.

©2026 Tanium Inc. All Rights Reserved

Note: With the introduction of profiles and rules for quarantine, you can change the details contained in profiles and rules after an endpoint has been quarantined. Changes to the profiles or rules after a quarantine has been applied on an endpoint has no effect on that endpoint unless it is unquarantined and requarantined.

1. From the Main menu, go to **Modules** > **Threat Response Management** > **Quarantine**. Click **Create**. Provide a name and description for the profile.
2. In the **Rules** section, add or remove rules to the profile. Quarantine rules and options define allowed traffic direction, allowed IP addresses, ports, and protocols. All other traffic is blocked. These rules are in the same format for Windows, Linux and macOS. If you do not define any quarantine rules, the default values are used, which gives the quarantined endpoint access only to the Tanium Server and permits DNS/DHCP traffic. If you previously provided a Windows IPsec policy file, the IPsec policy overrides the custom quarantine rules. Test the quarantine profile before deploying the profile. Do not apply a profile until its behavior is known and predictable. Incorrectly configured profiles can block access to the Tanium Server. For more information about rules, see Create quarantine rules on page 323.
3. In the **Servers** section, configure server details for the profile. You can configure server settings, alternate Tanium servers, VPN servers, and configure a message to notify the user that the system is being quarantined.
    a. In the **Configuration** section, configure server settings to use with the profile. You can select the following allowances:

    ### Server settings

Allowance Name	Option Name (configuration file)	Description
All DHCP	AllDHCP	Allows DHCP traffic to any destination. When updating taniumquarantine.dat files manually *, use the following format: Set to `true` to allow traffic Default: `true`
DNS	AllDNS	Allows DNS traffic to any destination. When updating taniumquarantine.dat files manually *, use the following format:

©2026 Tanium Inc. All Rights Reserved

Allowance Name	Option Name (configuration file)	Description
		Set to `true` to allow traffic Default: `true`
	CurrentDNS	Allows DNS traffic only to the DNS servers currently configured on the endpoint being quarantined. When updating taniumquarantine.dat files manually *, use the following format: Set to `true` to allow traffic Default: `false`
All Tanium Servers	TaniumServers	Allows Tanium traffic to the Tanium Servers that are defined in the ServerList or Servers configuration on Tanium Client. When updating taniumquarantine.dat files manually *, use the following format: Set to `true` to allow traffic Default: `true` **Note:** This option only applies to Tanium Servers and Zone Servers on TCP/17472. It does not include the module server, and it does not include TCP/17475 and TCP/17486 required for Direct Connect/ Live Endpoint connections. Additional rules are required.
Direct Connect	See Reference: Custom rules examples on page 337	Allows Direct Connect to access quarantined endpoints.
Live Response	See Reference: Custom rules examples on page 337	Allows Live Response to collect data from quarantined endpoints.

* = To specify configuration settings in taniumquarantine.dat, use the following format:

©2026 Tanium Inc. All Rights Reserved

Allowance Name	Option Name (configuration file)	Description
`OPTION:OptionName:OptionValue`		

b. In the **Advanced Settings** section, select whether or not to **Validate Availability** of the Tanium Server.

Advanced settings

Setting Name	Option Name (configuration file)	Description
Validate Tanium Server Availability	CheckTS	Validate that the Tanium Server can be reached on the Tanium port. If this validation fails, the quarantined status of the endpoint is revoked. When updating taniumquarantine.dat files manually *, use the following format: Set to `true` to validate that the Tanium Server can be reached on the Tanium port Default: `true`
* = To specify configuration settings in taniumquarantine.dat, use the following format: `OPTION:OptionName:OptionValue`		

c. In the **Alternate Tanium Servers** section, specify alternate Tanium Servers to use with this profile.

Alternate Tanium servers

Setting Name	Option Name (configuration file)	Description
Alternate Tanium Servers	ALTTS	Specify IP addresses. For example, use this option when you want to avoid using DNS during Quarantine. When removed from quarantine, the original Tanium Server is restored. Separate with a comma or leave empty for no alternates.

©2026 Tanium Inc. All Rights Reserved

Setting Name	Option Name (configuration file)	Description
* = To specify configuration settings in taniumquarantine.dat , use the following format: `OPTION:OptionName:OptionValue`		

d. In the **VPN Servers** section, specify any VPN servers to use with the profile. Paste one or more IP addresses in a line-delimited list.

VPN servers

Setting Name	Option Name (configuration file)	Description
VPN Servers	VPNSERVERS	Specify the VPN servers to automatically create rules for with a comma-delimited list. When updating taniumquarantine.dat files manually *, use the following format: IP:50/51,UDP:500,4500,TCP/UDP:443 Default: `NO VPNServers`
* = To specify configuration settings in taniumquarantine.dat , use the following format: `OPTION:OptionName:OptionValue`		

4. (Windows and macOS only) In the **Notification** section, specify a message that displays to the user upon quarantine of the endpoint.

Notification settings

Setting Name	Option Name (configuration file)	Description
Notification Message	Notify	Specify a string message to notify the user that the system is being quarantined. The message limit is 255 characters. Certain characters are not allowed, such as ($), (!), (`), (‘),(*) and some characters require escapes, such as (\"). Test any special characters before using in production.

©2026 Tanium Inc. All Rights Reserved

Setting Name	Option Name (configuration file)	Description
		Note: The Notification Message option is not supported on Windows 10 and 11 Home edition or Linux endpoints. Notification messages in languages other than English might require a different character code. For example, in the case of Japanese messages, apply the following character codes: For Windows: Shift-JIS, and for macOS: UTF-8. Character codes are applied when the notification message is defined in the taniumquarantine.dat file. Default: `No notification`
* = To specify configuration settings in taniumquarantine.dat , use the following format: `OPTION:OptionName:OptionValue`		

5. Click **Save**.

Delete a profile

To delete a profile, from the Main menu, go to **Modules** > **Threat Response Management** > **Quarantine** and select a profile. Click Delete. When a quarantine profile is deleted, the reactions that use that profile revert to using the default quarantine profile on the next intel deployment, regardless of whether the quarantine packages are generated after the deletion or not. If the quarantine packages are generated, but intel is not deployed, the reactions or response actions will fail. For this reason, deploy intel before generating the packages.

Duplicate a profile

You can duplicate a profile to create a version of the profile that is tailored to a specific scenario. The name of the duplicated profile has the time stamp that the original profile was duplicated to the profile name. To duplicate a profile, from the Main menu, go to **Modules** > **Threat Response Management** > **Quarantine** and select a profile. Click Duplicate.

©2026 Tanium Inc. All Rights Reserved

Edit a profile

To edit a profile, from the Main menu, go to **Modules** > **Threat Response Management** > **Quarantine** and select a profile. Click Edit.

Export a profile

To export a profile, from the Main menu, go to **Modules** > **Threat Response Management** > **Quarantine** and select a profile. Click Export. The profile is exported to the downloads directory of the web browser in JSON format.

Export all profiles

To export all profiles, from the Main menu, go to **Modules** > **Threat Response Management** > **Quarantine**. Select the profiles that you want to export and click **Export All**. The profiles are exported to the downloads directory of the web browser in JSON format.

Import a profile

To import a profile, from the Main menu, go to **Modules** > **Threat Response Management** > **Quarantine**. Click **Import**. Drag and drop the profile that you want to import in either JSON or DAT format. Alternatively, you can browse to the profile. Click **Import**.

Generate Quarantine Packages

About this task

When you have created a profile and assigned rules to the profile, you can **Generate Packages** to create quarantine packages that you deploy to targeted endpoints.

Best Practice: Deploy intel before generating quarantine packages. Deleting a Quarantine rule or profile also displays the unapplied-changes banner: There are unapplied quarantine changes. Click Generate Packages to incorporate your changes. Click Generate Packages so the deployed packages reflect the deletion.

©2026 Tanium Inc. All Rights Reserved

Quarantine package descriptions

Package Name	Description
`Threat Response - Quarantine Endpoint [Windows]`	The `Threat Response - Quarantine Endpoint [Windows]` package uses Windows IPsec policies to quarantine the endpoint. You can also add custom rules and options. See Reference: Create custom quarantine rules on page 334 for more information. **Note:** You cannot use Windows IPsec Quarantine on networks where a domain IPsec policy is already enforced. Check that the IPsec Policy Agent service is running on the endpoints Optionally, you can verify that the IPsec Policy Agent is listed as a running service in Windows. 1. In Interact, ask the question: `Get Service Details containing "PolicyAgent" from all machines with Service Details containing "PolicyAgent"` 2. In the table that gets returned, check the results in the following columns. • **Service Status**: Running or Stopped • **Service Startup Mode**: Manual or Automatic 3. If necessary, drill down into the results to determine which endpoints do not have the IPsec Policy Agent running.
`Threat Response - Quarantine Endpoint [Linux]`	The `Threat Response - Quarantine Endpoint [Linux]` package quarantines endpoints that are running Linux-based operating systems that support the use of the iptables module. **Important:** You cannot use `Threat Response - Quarantine Endpoint [Linux]` on endpoints where SELinux is enforcing without first adding a policy for Tanium Quarantine. Deploy the **Apply Linux Quarantine SELinux Policy** package to endpoints that are enforcing SELinux policies to add a policy for Tanium Quarantine. When the policy for Tanium Quarantine is added to an endpoint that is enforcing SELinux, you can quarantine the endpoint using the **Apply Linux IPTables Quarantine** package. Verify that endpoints are not using Network Manager `Threat Response - Quarantine Endpoint [Linux]` checks to ensure that the iptables module is installed and disables the use of the Network Manager module on endpoints that are targeted for quarantine. You can check for Linux-based endpoints that are running Network Manager by using the **Linux Network Manager** sensor to determine if Network Manager is enabled. In Interact, type `network manager` to find the sensor. This sensor has no parameters.

©2026 Tanium Inc. All Rights Reserved

Package Name	Description
`Threat Response - Quarantine Endpoint [Mac]`	The `Threat Response - Quarantine Endpoint [Mac]` package quarantines endpoints that are running Mac OS X operating systems that support the use of Packet Filter (PF) rules. This package creates packet filter rules that isolate endpoints by eliminating communication with network resources. PF software must be installed on endpoints that are targeted for quarantine.

1. From the Main menu, go to **Modules** > **Threat Response Management** > **Quarantine**. Click **Generate Packages**.
2. You can view the status of the package creation from **Management** > **Audit** > **Tasks.** Each time you generate quarantine packages a task is listed that is named **Generate Quarantine Packages**.
3. When you have generated packages that contain the quarantine parameters that you have defined in the profile that you used to generate the package, you can deploy the packages to endpoints. Follow the steps in Test quarantine on endpoints on page 332 to deploy the packages to endpoints.

Test quarantine on endpoints

About this task

By default, the quarantine on the endpoint blocks all communication except with the Tanium Server.



Important: Do not deploy quarantine packages to production endpoints without testing first.

1. Target computers for quarantine. The questions provided assume that the endpoints have been assigned a name that matches a convention for identifying them as test endpoints.
    a. Click **Create a Question**, and ask one of the following questions to target an appropriate group of endpoints.
        i. `computer name contains testendpointname and is windows equals true`

        ii. `computer name contains testendpointname and is linux`

©2026 Tanium Inc. All Rights Reserved

`equals true`

iii. `computer name contains testendpointname and is mac contains true`

b. Select the row from the drill-down question results, and click **Deploy Action**.

2. In the **Deployment Package** field, type the name of the quarantine package that you want to deploy:
   - `Threat Response - Quarantine Endpoint [Windows]`
   - `Threat Response - Quarantine Endpoint [Linux]`
   - `Threat Response - Quarantine Endpoint [Mac]`

3. (Optional) Define quarantine rules and options. For more information about quarantine rules, see Reference: Create custom quarantine rules on page 334.
   - If you already attached a taniumquarantine.dat file to the package you are deploying, you do not need to make any other configurations.
   - Otherwise, select **Override Config** to apply custom rules to the action.
   - If you are using the options and rules in this package deployment, select any options that you want to enable and enter your custom quarantine rules into the **Custom Quarantine Rules** field.

4. Click **Show Preview to Continue** to preview the targeting criteria for the action. Click Deploy Action.

5. Verify quarantine of the targeted endpoint. Confirm that the computer has no available means of communication to resources other than Tanium Server and any endpoints that you configured in custom quarantine rules. You can use RDP (Windows), SSH (Linux/macOS), the Ping network utility, or a similar means to confirm that communication is blocked. By default, the only traffic that the quarantine allows is between Tanium Client on the quarantined computer and Tanium Server over port 17472. If the computer is a server that must allow connections to name servers, verify that those connections are allowed to pass through.

6. Verify the visibility of the quarantined computer to Tanium Server.
   a. Target the endpoint with a question or sensor.
   b. Check the sensor results for the visibility of the quarantined endpoint.
   c. On the Quarantine dashboard, click **Isolated Machines**. A single computer is listed with a `Yes` on the **Quarantine: Isolated Machines** page.

Result

©2026 Tanium Inc. All Rights Reserved

Action folders are located under the Tanium Client installation folder on the endpoint, usually Downloads\Action_XXXX.log.

View quarantined endpoints

You can easily and immediately see what endpoints are quarantined from the **Overview** page of the Threat Response workbench. You can remove endpoints from quarantine from the **Overview** page of the Threat Response workbench. For more information about removing endpoints from quarantine, see Remove endpoints from quarantine on page 334.

Remove endpoints from quarantine

You can remove endpoints from quarantine from the **Overview** page of the Threat Response workbench. In the Quarantined Endpoints section of the **Overview** page of the Threat Response workbench, view the endpoints that are currently quarantined. Select one or more endpoints to remove from quarantine and click **Remove from Quarantine**.

Alternatively, you can deploy the `Threat Response - Unquarantine Endpoint [Windows]`, `Threat Response - Unquarantine Endpoint [Linux]`, or `Threat Response - Unquarantine Endpoint [Mac]` package to the endpoint to remove the quarantine from the computer. Use RDP (Windows), SSH (Mac/Linux), the Ping utility, or another method to confirm the removal of the quarantine and the normal communication of the test computer.



Note: Removing endpoints from quarantine from the workbench uses a response action, which enables targeting of offline endpoints. The packages only target online endpoints.

Reference: Create custom quarantine rules

You can define quarantine rules and options by either attaching a configuration file to the package, or by selecting options in Tanium Console when you deploy a quarantine action. Using this technique only impacts standard platform actions. For most quarantine operations, use the Threat Response workbench or response actions.

©2026 Tanium Inc. All Rights Reserved

Attach configuration file to package

You can attach a taniumquarantine.dat configuration file that defines quarantine rules and options to either a new package or the existing Quarantine packages. Then push that package out to the endpoints. For an example taniumquarantine.dat file, see Reference: Custom rules examples on page 337.

1. From the Main menu, go to **Administration** > **Content** > **Packages**.
2. You can either create a new package, or edit one of the existing Quarantine packages:
   - `Threat Response - Quarantine Endpoint [Windows]`
   - `Threat Response - Quarantine Endpoint [Linux]`
   - `Threat Response - Quarantine Endpoint [Mac]`
3. Update the taniumquarantine.dat file.
   a. To download the current file, click **Download**.
   b. Remove the file that is currently in the package.
   c. Click **Add** to upload the updated taniumquarantine.dat file.
4. Click **Save** to save the updates to the package.

   Add custom quarantine rules that allow connectivity for Direct Connect and Live Response to the quarantine package to avoid issues collecting artifacts during an investigation.

Select options in user interface when you deploy Quarantine actions

When you deploy the `Threat Response - Quarantine Endpoint [Windows]`, `Threat Response - Quarantine Endpoint [Linux]`, or `Threat Response - Quarantine Endpoint [Mac]` actions, you can define the quarantine rules and options as a part of that action. For more information, see Test quarantine on endpoints on page 332.

Reference: Custom rules and options

©2026 Tanium Inc. All Rights Reserved

Custom rules format

The format for custom rules is not case sensitive. Put each rule on a new line. Trailing white spaces are not supported. This format is used for both the configuration file and in the user interface.

```
Direction:Protocol:IPAddress:CIDR:Port
#Comment
```

Direction

Valid values: `IN` or `OUT` Specifies whether incoming or outgoing traffic is allowed.

Protocol

Valid values: `ICMP`, `TCP`, `UDP` If you specify ICMP, the ICMP protocol is allowed to communicate to and from the specified addresses. This limitation is because IPSec does not filter ICMP Type/Codes. The filtering is done by advfirewall.

When using quarantine rules to block the ICMP protocol, the MTU negotiation packages can become blocked when the size of the MTU package on the endpoint is larger than the router allowed MTU size. Normally the router will see a packet that is too large and send an ICMP packet to the endpoint to identify that the packet is too large and advises lowering the permissible MTU size. If the negotiation packet is not able to reach the destination due to quarantine, the endpoint can become unresponsive. The endpoint is still is quarantined but loses communication with the Tanium Server. Disabling ICMP traffic while quarantined should only be done after proper testing.

IPAddress

Specifies any IPv4 address or you can use `ANY` for all.

CIDR

Valid values: `0-32` or, if `ANY` is used in IPAddress, undefined. Subnet masks in dotted decimal format are not permitted in the input file. Undefined (blank) is same as /32 and uses the IPAddress only.

Port

Valid values: `0-65535` or undefined Leave undefined (blank) to permit all ports. Ranges are not currently supported, only individual ports or all ports can be defined.

©2026 Tanium Inc. All Rights Reserved

> **Note:** When using the Custom Quarantine Rules parameter in the package, the total characters should be 1100 or less. If you need more characters, you can use a custom DAT file.

Reference: Custom rules examples

Example for Custom Quarantine Rules field

```
IN:UDP:10.0.0.21:32:161
OUT:UDP:10.0.0.21:32:162
```

This example defines two rules:

- Allow SNMP queries (UDP Port 161) from another device at 10.0.0.21.
- Allow SNMP traps (UDP Port 162) to be sent to a device at 10.0.0.21.

> **Note:** This example demonstrates the use of parameter options in the package and not a taniumquarantine.dat file.

taniumquarantine.dat sample file

For DAT files, each entry must be on one line; you cannot use pipe (|) characters to combine lines. Trailing white spaces are not supported.

```
#Allow ICMP out to a specific IP Address

OUT:ICMP:192.168.10.15:32:0

#Allow ICMP in from a specific IP Address

IN:ICMP:192.168.20.10:32:0
#Allow ICMP out to any IP Address
OUT:ICMP:ANY::0
#Allow ICMP in from any IP Address
IN:ICMP:ANY::0

#Allow Kerberos to DC (10.10.1.10) - to allow SMB access
OUT:TCP:10.10.1.10::88
#Allow TCP port 80 in from a specific /24 subnet

IN:TCP:192.168.1.0:24:80

#Allow UDP port 161 in from a specific IP Address
IN:UDP:10.0.0.21:32:161
#Allow HTTPS (tcp 443) out to a specific /16 subnet
OUT:TCP:192.168.0.0:16:443
```

©2026 Tanium Inc. All Rights Reserved

```
OPTION:ALLDNS:TRUE

OPTION:CURRENTDNS:FALSE

OPTION:ALLDHCP:TRUE

OPTION:TANIUMSERVERS:TRUE

OPTION:CHECKTS:TRUE

OPTION:NOTIFY:This Device has been Quarantined

#Allow Live Endpoint/Direct Connect from LAN to Tanium Module Server (192.168.10.9)

OUT:TCP:192.168.10.9:32:17475

#Allow Live Endpoint/Direct Connect from remote endpoint to Zone Server (172.16.31.31)

OUT:TCP:172.16.31.31:32:17486
#Allow Live Response from LAN to NAS (\\192.168.10.135\Tanium\THR-Live-Response)
OUT:TCP:192.168.10.135:32:22
#Allow Live Response from LAN to NAS (\\192.168.10.135\Tanium\THR-Live-Response)
OUT:TCP:192.168.10.135:32:443
#Allow Live Response from LAN to NAS (\\192.168.10.135\Tanium\THR-Live-Response)
OUT:TCP:192.168.10.135:32:445
```

©2026 Tanium Inc. All Rights Reserved

Exporting audit data

You can review actions taken from the Threat Response workbench to audit for malicious internal actions or to validate remediation steps. For more information about viewing notifications and task status, and viewing and exporting action log data, see Troubleshooting Threat Response on page 351.

Events and alerts generated by Threat Response are sent to Connect. By configuring a Connect destination, this information is actionable outside of Tanium. Export data from Threat Response to Tanium Connect destinations, such as Email, File, HTTP, Socket Receiver, Splunk, and SQL Server, to gain visibility into Threat Response actions that users have performed during a specific time range.

Note: Audit log and system notification pruning runs every 24 hours and the default retention for audit logs and system notifications is 90 days. You can use the Threat Response API to change the number of days to a maximum of 365. If you need to retain audit logs or system notifications for longer periods, send the data to Tanium Connect. Tasks are not pruned.

You can send the following events to Connect:

Events to send to Tanium Connect

Detection events	Action type
Group configurations	• Creating • Deleting • Modifying
On-demand scans	• Initiating • Deleting
Service settings	• Resetting • Modifying
System user	• Modifying
Labels	• Modifying

©2026 Tanium Inc. All Rights Reserved

Detection events	Action type
	• Deleting
Intel	• Creating • Deleting • Modifying • Modifying labels of intel
Alerts	• Deleting • Modifying • Deleted batches of alerts • Modifying batches of alerts
Profiles	• Creating • Editing • Importing • Deleting • Reordering profiles • Deploying a profile • Duplicating
Configurations	• Creating • Editing • Importing • Deleting • Duplicating
Filters	• Creating • Editing • Importing • Deleting • Duplicating
Intel Deployment	• Migrating

©2026 Tanium Inc. All Rights Reserved

Detection events	Action type
Service Account	• Setting • Deleting
Threat Response Settings (With the exception of detection or recorder specific settings)	• Creating • Editing • Deleting
Recorder Settings	• Uploading Zone Server certifications • Adding, deleting, or deploying Zone server settings to endpoints • Saving values for default module server address, service URL for snapshot uploads, and the maximum number of rows to export from live connections
Live Endpoint Connections	• Creating and deleting live endpoint connections • Viewing directories from live endpoint connections • Downloading and deleting files from live endpoint connections • Creating and deleting exports from live endpoint connections • Creating, uploading, and deleting snapshots from live endpoint connections • Creating and deleting events from live endpoint connections
Live Response Collections	• Creating • Editing • Duplicating • Deleting
Live Response Destinations	• Creating • Editing • Duplicating • Deleting
Live Response File Collectors	• Creating • Editing • Duplicating • Deleting

©2026 Tanium Inc. All Rights Reserved

Detection events	Action type
Live Response Script Sets	• Creating • Editing • Duplicating • Deleting
Live Response Packages	• Generating
Notifications	• Creating (Including notifications for intel safeguards) • Deleting

Tanium Connect

To export data from Threat Response to Connect destinations such as Email, File, HTTP, Socket Receiver, Splunk, and SQL Server, create a connection.

Before you begin

- You must have access to Connect with Connect User role.
- You must have Connect 4.10.5 or later.

Create a connection

1. From the Connect menu, click **Connections** and then click **Create Connection** .
2. Under General Information, provide a name and description for the connection. Select a Log Level.
3. Under Source, Select **Tanium Threat Response Audit Source**.
4. In the type field, select **Audit Report**.
5. In the **Batch Size** field, enter the number of rows of Threat Response data to return at a time. The default is 1000.
6. In the **Minutes to Collect** field, enter the number of minutes prior to the start time to collect data. For an exhaustive log, leave this field blank.

©2026 Tanium Inc. All Rights Reserved

7. Select **Send the Audit State Column to Tanium Connect as JSON** to send the data in JSON format. If selected, data is sent as a string object.
8. Under Destination, select where you want Connect to send the audit data. Provide any additional configuration for the type of destination you select.
9. Provide any filters you want to apply to the data. You can use filters to modify the data that you are getting from your connection source before it is sent to the destination.
10. Expand **Columns** to review the format of the output data. Make changes as appropriate and add any custom columns that are relevant.
11. Click **Save Changes**.

Test a connection and review audit data

1. From the Connect **Overview** page, click **Connections**.
2. Click the connection that you created for Threat Response audit data.
3. Click **Run Now**. Confirm that you want to run the connection.
4. View the summary of the run.
5. View the audit report in the destination that you configured for the connection.

Schedule the connection

For more information about how to run connections on a schedule, see Tanium Connect User Guide: Schedule connections.

©2026 Tanium Inc. All Rights Reserved

Maintaining Threat Response

Perform monthly maintenance tasks to ensure that Threat Response successfully performs scheduled activities on all the targeted endpoints and does not overuse endpoint or network resources. If Threat Response is not performing as expected, you might need to troubleshoot issues or change settings. See Troubleshooting Threat Response on page 351 for related procedures.

Threat Response monthly maintenance

1. From the Main menu, go to **Administration** > **Shared Services** > **Client Management**.
2. From the Client Management menu, select **Client Health** and click the **Deployment** tab.
3. Review the **Health Failures** panel for issues that relate to Tanium™ Threat Response domains:
    - `dec` (Direct Connect)
    - `index` (Tanium Index)
    - `recorder` (Tanium Recorder)
    - `stream` (Tanium™ Stream)
    - `threatresponse` (Tanium™ Threat Response Client Extension)
4. Investigate health failures and review the status and configurations of endpoint tools for Threat Response, including:
    - Non-default configuration settings on clients
    - Tools versions
    - Client extension versions
    - (Windows only) Tanium™ Driver status and version
    - Berkeley Packet Filter (BPF) support

    For the specific steps, see Tanium Threat Response User Guide: Get Threat Response endpoint tools status and configurations.
5. From the Main menu, go to **Modules** > **Threat Response** > **Overview**.

©2026 Tanium Inc. All Rights Reserved

6. Go to the **Metrics** panel and check the Threat Response **Coverage**.
7. If the **Coverage** is lower than expected, investigate and remediate coverage as described under Tanium Threat Response User Guide: Monitor and troubleshoot Threat Response coverage. If coverage issues might result from missing or misconfigured Threat Response profiles, click the **Coverage** value to open the **Profiles** page and review profile configurations. For more information about profile issues, see Tanium Threat Response User Guide: My device has no profile or the wrong profile.
8. To investigate and remediate other Threat Response issues, see the following sections in the Tanium Threat Response User Guide:
    - Troubleshooting Threat Response
    - Reference: Common health check issues

Get Threat Response endpoint tools status and configurations

Ask the question: `Get Client Extensions - Status from all machines`.

This retrieves the status of Client Extensions (such as Threat Response, Index, Recorder), Threat Response profile status, and any client extensions health issues.

The following domains are Threat Response related:

- dec
- index
- recorder
- stream
- threatresponse

Threat Response related domains

Domain	Key	Value	Explanation
[Any]	health_check	[Any value]	For more information, see Tanium Client Management User Guide: Monitor the client health overview in Client Management and take corrective actions to ensure Threat Response is healthy in your

©2026 Tanium Inc. All Rights Reserved

Domain	Key	Value	Explanation
			environment.
recorder	has_event_source	[Multiple]	This displays which event sources the Tanium Recorder is using.
recorder	has_subscription	[Multiple]	This displays which Tanium components are consuming events from the Tanium Recorder process.
recorder	is_using_tanium_driver	True | False	(Windows Only) This displays if the Tanium Recorder Process is consuming events from the Tanium Driver.
recorder	min_requirements_met	True | False	This displays if the system meets the minimum CPU requirements for the Tanium Recorder to run. Two or more CPU cores are required.
threatresponse	applied_intel_revision	[Any]	This value identifies the version of Threat Response intel currently installed on the endpoint.
threatresponse	applied_profile applied_profile_id applied_profile_revision	[Multiple]	These keys return information about which Threat Response profile name, profile unique ID, and profile revision is currently in use on the endpoint.

Ask the question: `Get Client Health - Client Settings from all machines`.

This question returns any non-default configuration settings that are set explicitly on the clients. If settings are not explicitly set, no results are displayed for that setting. It is useful to review these settings for any non-default settings which you can set on Threat Response or Tanium Client components and causing unexpected behavior.

The following domains are Threat Response related:

- dec
- index
- recorder
- stream
- threatresponse

©2026 Tanium Inc. All Rights Reserved

Ask the question: `Get Endpoint Configuration - Tools Status from all machines`.

This returns the Threat Response tools versions targeted and installed to verify the correct endpoint tools are installed. Current tools versions can be referenced in the Threat Response release notes: https://kb.tanium.com/Category:Tanium_Threat_Response

The following Tool Names are Threat Response related:

- Threat Response
- Threat-response-cx
- Threat Response Stream
- cx-stream
- Incident Response
- index-cx
- Direct Connect
- dec-cx
- Driver
- Recorder
- Recorder BPF Support

Ask the question: `Get Client Extensions - Installed Extensions from all machines`.

This returns the installed Threat Response client extension binary versions. Current client extension binary versions can be referenced in the Threat Response release notes: https://kb.tanium.com/Category:Tanium_Threat_Response

The following Domains are Threat Response related:

- index

©2026 Tanium Inc. All Rights Reserved

- recorder
- stream
- threatresponse

Ask the question: `Get Tanium Driver Status from all machines with Is Windows matches true`.

This returns the installed Tanium Driver Status from all Windows machines (Tanium Driver is supported on Windows only). The following tables include some common Tanium Driver Status results:

Tanium Driver successful installation results

Successful installation	
Tanium Driver Status Results that indicate it is properly installed and running	Service Status: SERVICE_RUNNING Driver install path: \SystemRoot\System32\drivers\TaniumRecorderDrv.sys

Tanium Driver installation errors

Errors to look for	
Tanium Driver	Install Recommended
Tanium Driver Service is not installed	Service Installation: Not installed
Tanium Driver Service is present but not running	Service Status: Not started Service Status: SERVICE_STOPPED
Tanium Driver is not installed	Driver Location: Not installed Driver Version N/A Driver Controller Version N/A

Ask the question: `Get Tanium Driver Version from all machines with Is Windows matches true`.

This returns the installed Tanium Driver Version of the binary on disk from all Windows endpoints (Tanium Driver is supported on Windows only). This can be useful to verify that the correct version of

©2026 Tanium Inc. All Rights Reserved

the Tanium Driver is installed.

Tanium Driver Versions by Threat Response release: https://kb.tanium.com/Category:Tanium_Threat_Response

Use the following sensors to help troubleshoot and determine if eBPF is supported and available for use by Tanium Recorder on Linux systems.

Sensors to evaluate eBPF support

Sensor	Results
Recorder - Is BPF BCC Supported	Returns True if BPF BCC is supported on the endpoint.
Recorder - Is BPF CO-RE Supported	Returns True if BPF CO-RE (Compile Once Run Everywhere) is supported on the endpoint.
Recorder - Is BPF Supported Details	Returns details about whether or not BPF is supported on the endpoint.

For more information, see Tanium Interact User Guide: Asking questions.

Monitor and troubleshoot Threat Response coverage

The following table lists contributing factors into why the Threat Response coverage metric might be lower than expected, and corrective actions you can make.

Contributing factors and corrective actions for Tanium Threat Response

Contributing factor	Corrective action
Tools not deployed	Ensure the Threat Response Action Group is set to All Computers . Ensure that all endpoints belong to a computer group that is defined in a Threat Response profile.
Tools in an unhealthy state	Review the client health features in Client Management. For more information, see Tanium Client Management User Guide: Monitor the client health overview in Client Management and take corrective actions to ensure Threat Response is healthy in your environment.

Monitor and troubleshoot mean time to investigate threats

©2026 Tanium Inc. All Rights Reserved

The following table lists contributing factors into why the mean time to investigate threats metric might be higher than expected, and corrective actions you can make.

Contributing factors and corrective actions for Tanium Threat Response

Contributing factor	Corrective action
Alert status not being properly updated in the Threat Response workbench	Ensure analysts are accurately updating alerts from New to In Progress and then from In Progress to Resolved . If alerts are sent to a SIEM or another location, ensure that your workflow uses the Tanium Threat Response API to appropriately set alert state in Tanium to be able to track this metric correctly.

Monitor and troubleshoot mean time to remediate threats

The following table lists contributing factors into why the mean time to investigate threats metric might be higher than expected, and corrective actions you can make.

Contributing factors and corrective actions for Tanium Threat Response

Contributing factor	Corrective action
Alert status not being properly updated in the Threat Response workbench	Ensure analysts are accurately updating alerts from New to In Progress and then from In Progress to Resolved . If alerts are sent to a SIEM or another location, ensure that your workflow uses the Tanium Threat Response API to appropriately set alert state in Tanium to be able to track this metric correctly.

©2026 Tanium Inc. All Rights Reserved

Troubleshooting Threat Response

If Threat Response is not performing as expected, you might need to troubleshoot issues or change settings. For more information, see Contact Tanium Support on page 373.

General troubleshooting

- Collect logs
    - Collect troubleshooting information from the Threat Response service on page 353
    - Collect troubleshooting information from endpoints on page 353

Managing the Threat Response workbench

- View notifications on page 354
- View task status on page 355
- View and export log data on page 356

Endpoint troubleshooting

- View and export log data on page 356

Threat Response component troubleshooting

- Profiles and configurations
    - My device has no profile or the wrong profile on page 360
- Detection and Intel
    - No alerts are generated on page 362
    - Too many alerts are generated on page 363
- Index

©2026 Tanium Inc. All Rights Reserved

    - Configure client disk space use on page 368
    - Files are not being hashed or indexed on page 367
- Recorder
    - The lifetime of recorder events is too short on page 364
    - Start or stop the recorder on page 366
    - File, network, or security events are not displayed on Oracle Linux server on page 365
    - Identify Linux endpoints that are missing auditd on page 366
    - Start or stop the recorder on page 366
- Live connections
    - Cannot establish a live connection on page 368
- Live Response
    - Test Live Response connections manually on page 368
- Stream
    - Stream is not sending data on page 369
    - Stream is sending too much data on page 370
- Live Response
    - Configuration not available or not updated to the latest settings when deploying package on page 371
    - Action not running on endpoint on page 371
    - Artifacts not being copied to destination on page 371
- Quarantine
    - Custom configurations are missing on page 372

©2026 Tanium Inc. All Rights Reserved

- Live Connections are not working while quarantined on page 372
- Live Response is not working to copy files to the destination while quarantined on page 372

- Verify endpoint tools on page 373
- Contact Tanium Support on page 373
- Uninstall Threat Response on page 373

Collect logs

Collect troubleshooting information from the Threat Response service

About this task

Use Threat Response to compile a collection of logs relevant for troubleshooting. You can collect logs and other artifacts from the Threat Response service located on the server to help troubleshoot service side issues. The ZIP file is also known as a support bundle.

1. From the Threat Response overview page, click Help ?, then click the **Troubleshooting** tab.
2. Click **Create Package**. Normally creating the troubleshooting package takes a few minutes, but can take longer for large packages.
3. When the status of the package creation is complete, click **Download Package**.

Result

The log zip file might take a few moments to appear in the download folder.

Collect troubleshooting information from endpoints

About this task

You can collect logs and other artifacts from individual endpoints to help resolve issues. Collecting logs from endpoints requires a live connection to the endpoint from which you want to gather troubleshooting information.

1. From the Main menu, click **Administration** > **Client Management** to open the **Client**

©2026 Tanium Inc. All Rights Reserved

Management Overview page.

2. From the Client Management menu, click **Client Health**.
3. In the Direct Connect section, create a live connection to the endpoint from which you want to collect troubleshooting information. For more information about creating a live connection, see Direct connecting to endpoints and exploring data on page 189.
4. Click the Gather tab. In the domain section select Threat Response.
5. Click **Gather from Endpoint**.
6. A package is gathered from the endpoint. The name of the link is the time stamp of the troubleshooting package. Select the Must Gather that you want to download and click **Download** to download a ZIP file that contains troubleshooting information.

Result

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

> **Note:** The legacy **Troubleshooting** button has been removed from direct connections to endpoints and the **Must Gather** column from the grid for connected endpoints has been removed. Any previous Threat Response troubleshooting bundles are removed on upgrade to a newer version of Threat Response.

View notifications

> **Note:** Viewing notifications requires the **Threat Response Audit** permission.

From the Main menu, go to **Modules** > **Threat Response Management** > **Audit** > **System Notifications**. These notifications show various Threat Response service related events and notifications. You can expand these notifications to view additional information.

- Alert Pruning: Notifies when alerts have been pruned from the Threat Response alerts database.

©2026 Tanium Inc. All Rights Reserved

- Automatic Intel Deployment Error: Threat Response has failed to deploy the Intel database.
- Intel Deployment Excluded Intel: Possible corrupted Intel database.
- Endpoint Throttle: Alerts were throttled at the endpoint level for an Intel document. An endpoint throttles alerts that match five times in five minutes for the same intel document. When this occurs, alerts are not sent to the service until the cool off time of one hour occurs. After one hour, alerts are sent to the service again.
- Service Throttle Start: Alerts were throttled at the service level for an Intel document. You can customize the values for service level throttling from the Alert Throttling section of the Service Settings in the Threat Response workbench. Intel documents that initiate alerts at a rate that exceeds the settings you provide are disabled. If additional alerts match during the cool off period, the extension factor calculated time is added to the cool off time.
- Service Throttle Update: Alerts were throttled again after the original throttle start at the service level for an Intel document.
- Threat Navigator Decompression Size Error: A Threat Navigator search or scan on an endpoint produced a payload that could not be decompressed within the configured size limit, so the response was dropped. Expand the notification to see the affected endpoint name, scan ID, search ID, iteration, run number, gather type, question ID, max bytes, and payload hash.
- Tanium Signal Stream Update: Threat Response updated to a new version of Tanium Signals.

To delete a notification, select the row and click **Delete**.

View task status



Note: Viewing task status requires the **Threat Response Audit** permission.

You can view the status of and review other historic data for Threat Response tasks.

From the Main menu, go to **Modules** > **Threat Response Management** > **Audit** > **Tasks**.

When troubleshooting, it is useful to identify tasks which have not been completed successfully. You can filter by task status:

©2026 Tanium Inc. All Rights Reserved

- Error
- Incomplete
- Not Started
- Started

Some examples of Threat Response tasks include (but are not limited to):

- Deploy Profile
- Deploy Intel
- Deploy Tools
- Generate Live Response packages
- Response Action
- Start Index
- Suppress Alerts

In the event of an error, you can locate a specific task and expand the cell to view results and metadata from log files. The data that appears in the advanced details view provides information that is useful for troubleshooting and saves the time of trying to locate debugging information in lengthy log files or in formats that are not intended to be human readable.

View and export log data

About this task



Note: Viewing and exporting log data requires the **Threat Response Audit** permission.

You can view and export data for actions in tables of the Threat Response database for Threat Response tasks. You can view and export audit data from the following tables of the Threat Response database:

©2026 Tanium Inc. All Rights Reserved

- Alert
- Audit
- Collection Config
- Config
- Cron Task
- Endpoint Must Gather
- Event Evidence
- Export
- File Collector Set
- File Evidence
- File Management
- Filter
- Intel DB
- Intel Document
- Intel Document Label
- Label
- Live Connection
- Live Response Package
- Migration
- On Demand Scan
- Plugin Schedule Subscription
- Profile

©2026 Tanium Inc. All Rights Reserved

- Response Action
- Script Set
- Service Account
- Settings
- Snapshot
- Source
- Suppression Rule
- Task
- Transfer Destination
- Yara Scope

1. From the Main menu, go to **Modules** > **Threat Response Management** > **Audit** > **Logs**.
2. Expand any row to view JSON to show the details of the action.
3. (Optional) Select one or more actions and click **Export Selected Logs** to export data for the actions to the local downloads folder as a JSON file. Click **Export All** to export all the logs to the local downloads folder as a JSON file.
4. (Optional) Filter the table of actions to display a more focused list of actions. You can filter by specific tables in the Threat Response database, specific action types, specific personas, users, or a time range.

Remove Threat Response tools from endpoints

About this task

You can deploy an action to remove Threat Response 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`

©2026 Tanium Inc. All Rights Reserved

2. In the results, select the row for Threat Response, drill down as necessary, and select the targets from which you want to remove Threat Response 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 Threat Response.
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 Threat Response to reinstall tools, deploy the **Endpoint Configuration - Unblock Tool [Windows]** or **Endpoint Configuration - Unblock Tool [Non-Windows]** package (depending on the targeted endpoints).
   - If you reinstall tools manually, select **Unblock Tool** when you deploy the **Endpoint Configuration - Reinstall Tool [Windows]** or **Endpoint Configuration - Reinstall Tool [Non-Windows]** package.

7. (Optional) To remove all Threat Response 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 Threat Response tools that are not dependencies for tools from other solutions, select **Remove unreferenced dependencies**.

©2026 Tanium Inc. All Rights Reserved

9. (Optional) In the **Deployment Schedule** section, configure a schedule for the action.

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

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

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

My device has no profile or the wrong profile

The profile deployment process is the process of generating, saving, and deploying a profile from the server to the endpoint. If an endpoint, or client, does not have a profile or the incorrect profile, then the profile deployment action could have failed on the server.

Common reasons for failure include the following:

- The profile is disabled.
  - From the Main menu, go to **Modules** > **Threat Response Management** > **Profiles**. Ensure that the intended profile is **Enabled**. Any endpoints that are targets of a disabled profile receive the next applicable enabled profile based on priority. Any configurations deployed by the profile before it was disabled are removed if no profile is currently applicable.
- The profile was not deployed.
  - From the Main menu, go to **Modules** > **Threat Response Management** > **Profiles** and make sure a profile has successfully deployed. A profile has successfully deployed if it has a green check under the status column.
  - Verify the last deployment time.
  - Verify the Profile Targeting (Computer Groups).

©2026 Tanium Inc. All Rights Reserved

    - Verify the Profile Priority.
    - Verify the Profile ID on the Profiles page and compare to the output of **Client Extensions - Status**.
    - Verify the Profile Revision on the Profiles page and compare to the output of **Client Extensions - Status**.
    - From the **Threat Response** > **Tasks** page, verify that the profile was deployed successfully.
- The profile was deployed, but it did not reach the client.
    - Verify in Endpoint Configuration that the Threat Response Profile configuration was updated.
    - Verify the Endpoint Configuration – Manifest was updated on the endpoints.
    - Verify there are no pending Endpoint Configuration Approvals.
    - Verify there are no pending Action Approvals for Endpoint Configuration.
- The profile was deployed and received, but the client was unable to apply the correct configuration.
    - Verify the currently installed Threat Response Profile ID and revision matches the Threat Response deployed profile using the **Client Extensions – Status** sensor.
    - Review the <Tanium Client>\Logs\extensions0.txt log to identify issues applying the profile.
    - If endpoints are not applying configurations as expected, try creating a simple change to the profile (for example, change the description) and save the profile to increment the revision number. Then deploy the profile again. The updated revision forces the client to re-apply the entire profile.
    - Review the output of the Client Extensions – Status sensor for any health_check results.

Should none of these actions resolve the issue then a server-side troubleshooting bundle is required. For more information, see Collect troubleshooting information from endpoints on page 353. Return

©2026 Tanium Inc. All Rights Reserved

the collected information and a detailed description of the issue seen and the steps taken to Tanium for analysis.

No alerts are generated

Outside of specific testing scenarios, alert generation is rare. Under normal circumstances, a system does not generate alerts based on deployed intel — no alerts or very low alert counts indicate normal operation. The alert generation and collection process involve interaction between the client and the service of Threat Response and so validation of both of these is required to validate that the process is working as expected.

The following steps are targeted at troubleshooting a testing scenario where alert generation is expected because of user interaction on an endpoint to validate the detection and alerting process.

To validate that the service side parts of the process have been applied correctly:

- Ensure that profile and intel have been deployed as expected and that the system shows the correct profile ID and revision and intel revision from the **Client Extensions - Status** sensor. If this output shows issues then the following steps would be recommended as initial remedial actions:
    - Redeploy all relevant profiles and intel from the Threat Response profiles page validate any actions do not require approval and are waiting in the queue.
    - Ensure that the Threat Response System Notifications page does not show throttle messages for the intel document in question.

If none of these actions resolve the issue, or if profiles have not deployed or questions have not been issued, collect a server-side troubleshooting bundle. For more information, see Collect troubleshooting information from endpoints on page 353. Return the collected information and a detailed description of the issue seen as well as the steps taken to Tanium for analysis.

If the above checks show the expected results then endpoint investigation is required. To validate that the endpoint is working as expected (these actions assume access to the endpoint is available) perform the following steps:

- Validate that the **Endpoint Configuration - Tools** Status sensor shows all relevant tools installed.

©2026 Tanium Inc. All Rights Reserved

- Ensure that any actions being taken to trigger alerts are starting from a new process each time they are attempted (such as, if a user is trying to trigger a signal from a command prompt then open a new command prompt for each attempt).
- Ensure that the **Threat Response System Notifications** page does not show throttle messages for the intel document in question.

If one of the above actions show unexpected output, then take the following steps to try and resolve the issue:

- Redeploy any tools that have not deployed as expected by using the **Endpoint Configuration - Reinstall Tool** action targeting the tool in question.
- Wait for throttles to clear for a given intel document or attempt firing a different intel document from the endpoint.
- Ensure commands to trigger alerts are executed in a new instance for each attempt.

If none of the above steps show an issue or provide a resolution then a client-side troubleshooting bundle is required. For more information, see Collect troubleshooting information from endpoints on page 353. Return the collected information and a detailed description of the issue seen and the steps taken to Tanium via a support case for analysis.

Too many alerts are generated

The following steps are directed at validating the source of the high number of alerts and to ensure that remedial actions are targeted correctly:

- Validate the intel document names and ID's associated with the number of alerts using the home page graphics or the **Alerts** page.
- Investigate if the alerts matches are intended or unintended based on the syntax of the indicator and the alert details provided.

Depending on the findings from the above actions there can be several courses of action that you can perform to reduce the alert load:

- Remove the intel document from the profile associated with affected endpoints and then redeploy the profile and intel database.

©2026 Tanium Inc. All Rights Reserved

- Modify the intel document to ensure it is matching the correct artifacts or endpoint behavior and redeploy the intel document.
- For Tanium Signal-based alerts create a suppression rule for the intel document to prevent specific circumstances from generating alerts. Deploy the suppression rule using the Intel deployment action to apply it to endpoints and the service.
- Configure or tune endpoint or service throttling to prevent higher than expected numbers alerts from being sent for a given intel document.

Note: An alert backlog can grow on the endpoints and in the service, which could mean that the above remedial actions prevents new alerts on the endpoints, and might not resolve the situation with a very large backlog.

Should alerts continue to arrive in the user interface and cause performance issues, it is advised to create a support case with Tanium with a detailed description of the issue seen and the steps taken.

The lifetime of recorder events is too short

The lifetime of the recorder is controlled by the settings for the database from the Threat Response recorder configuration. The default values are 1 gigabyte (GB) for size and 90 days for length.

The volume of data sent to the recorder is regulated by the filters associated with its configuration. These filters are used to include or exclude specific elements of telemetry in the recorder database.

There are two possible reasons why the database does not hold events for a sufficient retention period:

- The size of the DB is not sufficient to store all of the required data.
- The length of time the DB holds events is too short.

There are multiple options available to ensure the required data is recorded in the database:

- Modify the maximum size of the recorder database.
- Modify the maximum retention period for the recorder database.

©2026 Tanium Inc. All Rights Reserved

- Modify the filters for the configuration to reduce the recorded events in the DB.

Important: The settings for maximum size and retention period take effect in the order that they are received by the endpoint. If the maximum database size is reached before the maximum lifetime of the database then the recorder will start pruning events from the database to ensure that it remains at the maximum size. Alternatively, if the maximum retention period is reached before the maximum size is reached then the recorder starts pruning events.

You might need to change both configurations at the same time to achieve the required outcome. Because of the uncertainty of the impact of changing the database size or the retention period these options are less optimal when trying to regulate the retention period.

If it is impossible to change the maximum size (this is the most common situation), or more control of the content of the database is required, then the alternative, and preferred, option is to use filters to remove unnecessary recorded telemetry from the database. This exercise requires some investigation of the database content and validate the unnecessary content and create filters for it.

Note: When deploying filters, any process filters that are applied filters all activity from that process (there is no file, registry, etc data recorded) as such these are the broadest filters and can reduce the amount recorded telemetry quickly. Deploying other filters for the other event types (file, network, registry, security, and image events) are more specific and can be used to remove very specific events from the recorded telemetry. For additional information about filters, see Create filters on page 164.

On Linux endpoints, a System filter enables you to specify a path that is excluded from audit configuration. When providing this type of filter, be sure to provide the full path to the file.

Should there continue to be issues with the volume of data recorded then a client-side troubleshooting bundle and an export of the Recorder configuration are required. Return the collected information and a detailed description of the issue seen and the steps taken to Tanium via a support case for analysis.

File, network, or security events are not displayed on Oracle Linux server

If you are not seeing file, network, or security events in the recorder results, you can disable SELinux.

©2026 Tanium Inc. All Rights Reserved

When SELinux is enabled and the auditd fallback is disabled on Oracle Linux, only process information is returned. Alternatively, ensure that the Client Recorder Extension configuration parameters are set as follows:

- **CX.recorder.AuditdStopAuditdService** is set to 0.
- **CX.recorder.AuditdEnableAudispdFallback** is set to 1.

For more information, see Client Recorder Extension User Guide: Configuring recorded events .

Identify Linux endpoints that are missing auditd

About this task

If Linux endpoint events are not being recorded, they might be missing the audit daemon and audispd services. Ideally, the audit daemon is installed and configured before installing the Threat Response module, but it is possible for endpoints to come online at a later time.

1. (Optional) Create the auditd package.
   You can either create a general installation package and put the logic in the scripts or you can have a simple script and put the logic in the Tanium query. For more information, see Tanium Core Platform User Guide: Creating and managing packages.
2. Ask the question: `Get Installed Application Exists[audit] from all machines with Is Linux containing "true"`.
3. Deploy the appropriate auditd package to the identified endpoints.

   Important: If you need to distribute the package to a large number of endpoints, spread the changes out over time to avoid a negative impact on the network.

Start or stop the recorder

About this task

You might need to manually start or stop the recorder.

Resolve the underlying issue and restart the recorder. Or, if you find that the recorder is using more system resources than expected, you can stop the recorder and troubleshoot the issue.

©2026 Tanium Inc. All Rights Reserved

1. Identify the computer groups that contain endpoints on which you want to stop the recorder.
2. Deploy a profile that does not contain a recorder configuration to the computer groups you want to target.
3. You can optionally create a live endpoint connection to specific endpoints to troubleshoot any issues.

Result

To start the recorder, deploy a profile that has a recorder configuration to the targeted computer groups.

Files are not being hashed or indexed

Index is optimized to minimize endpoint resource utilization. The solution indexes local file systems, computes file hashes, and gathers file attributes and magic numbers. This information is recorded in an SQLite database for detection and reporting of threat indicators for files at rest.

Index creates and maintains an inventory of the file system on an individual endpoint with the following operations:

- Detect file changes
- Compute file hashes
- Calculate magic number

For more information about indexing in Threat Response, see Client Index Extension User Guide.

If the configuration does not exclude the file or location then it is possible that Index is not running on the system for some reason.

To validate that this is the case, perform the following steps:

- Use the **Client Extensions - Status** sensor to validate that Index is running and configured.
- Confirm that Index is enabled in the Threat Response profile applied to the endpoint, and that the profile has deployed successfully.

©2026 Tanium Inc. All Rights Reserved

Configure client disk space use

For information about the disk space warning and critical thresholds, the Client Extensions that use them, and how to change the values, see Client Index Extension User Guide: Manage client disk space thresholds.

Cannot establish a live connection

Live connections are established using the shared service component Direct Connect. Elements of the Direct Connect services are included in the Threat Response user interface to enable users to search for devices and make connections and the capabilities for downloading files or navigating the Recorder database are provided on top of this connection via Threat Response.

To ensure that Direct Connect is working as expected, perform the following steps:

- Review the outputs of the **Get Client Extensions - Status** sensor to validate that the endpoints in question have the required endpoint tools deployed and are working as expected.
- Review the outputs of the **Direct Connect - Connection Configuration** sensor to validate that the endpoints in question have the correct configuration.
- Review the outputs of the saved question **Direct Connect - Endpoint Info** and ensure the endpoint in question is showing in the results (this can also serve to refresh the data that shows in the live response search bar).

Should the outputs of these commands show an issue then it might be required to force the distribution of the Direct Connect tools to the endpoint in question to ensure that it is ready to accept connections, issuing the action **Endpoint Configuration - Reinstall Tool** for the relevant operating system, and selecting the option for Direct Connect in the Tool Name dropdown list to reinstall the tools on the endpoint.

Should there continue to be issues connecting to the endpoint then a client-side troubleshooting bundle should be collected for Direct Connect. Return the collected information and a detailed description of the issue seen and the steps taken to Tanium via a support case for analysis.

Test Live Response connections manually

©2026 Tanium Inc. All Rights Reserved

To test Live Response connections manually, see Generate known_hosts and test connections on page 297.

Stream is not sending data

Stream provides the capability to send telemetry from the recorder directly to destinations outside of the Tanium infrastructure such as SIEM. The stream capability relies on the correct configuration from the service as well as access to the configured destination to be able to perform its function. It is important to first validate that the receiving side for the telemetry is configured and running as expected testing this from target endpoints is the only way to ensure that connectivity is working as expected. As with most components, there is a service and an endpoint component to troubleshooting problems.

To validate the service side components of Stream:

- Validate that Stream and Recorder tools are deployed and reporting as expected using the **Get Client Extensions - Status** sensor.
- Ensure the Stream configuration is pointing to the correct destination or URL and that any credentials are included to ensure that the endpoints have access to the destination.
- Validate that **Dry Run** is not enabled in the configuration. By default, **Dry Run** is enabled when you create a stream configuration.
- Ensure that any filters applied to the Stream configuration send the required telemetry from the endpoint to the destination system.
- When deploying a custom configuration, validate that the JSON syntax is correct and that the client is able to parse and deploy the given configuration.
- On Linux systems, confirm that no system file filters are blocking the Recorder from gathering the required telemetry.

If the service configuration appears correct, the issue might be on the endpoint. The following steps require access to the endpoint:

- Ensure enough time has passed for Stream to reach the threshold of sending data, this can take some time depending on the configuration and the amount of telemetry being generated by the endpoint.

©2026 Tanium Inc. All Rights Reserved

- Ensure that the endpoint can resolve and contact the destination server for receipt of telemetry (there are many options for this but commands such as ping, host, nslookup, telnet, etc.).
- Validate that the endpoint has recorded the events expected to be sent to the destination utilizing the live connection capability.

If no telemetry is received after verifying the receiving side, service, and endpoint, collect a client-side troubleshooting bundle and export the Stream configuration. Return the collected information and a detailed description of the issue seen and the steps taken to Tanium via a support case for analysis.

Stream is sending too much data

The volume of data sent from any given client to the Stream destination is determined by the activity on the endpoint and the configuration that has been applied to Stream. While data volume is not an error, high volumes might cause issues on specific endpoints or the receiving side.

There are two mechanisms available to reduce the volume of data being sent by Stream depends on the configuration and the requirements for the data being sent from each endpoint. The two options available are:

- Disable specific event types from being sent.
- Use filters to reduce the numbers of specific events sent.

Depending on the requirements for the use of the telemetry being sent from Stream, you can use one or both of these mechanisms to reduce the total amount of data being sent from the endpoints:

- Removing an entire event type from the configuration removes all of the events of this type from the data being sent from the endpoint to the receiving side. Unlike Recorder filters, when disabling process events the other event types for the given process are sent (although the references to process in these events are no longer resolvable).
- Using filters to remove events provides a more specific reduction in data volume. The filters available are the same as those available for the Recorder configuration and can be reused.

©2026 Tanium Inc. All Rights Reserved

Note: Although Stream uses Recorder data, Stream is a separate subscription to that data, and options including the Stream configuration do not impact the data being sent to the Recorder database, or vice versa.

If data volume issues persist, collect a client-side troubleshooting bundle and export the Stream configuration. Return the collected information and a detailed description of the issue seen and the steps taken to Tanium via a support case for analysis.

Configuration not available or not updated to the latest settings when deploying package

If a configuration is not available or has not updated to the latest settings when you deploy a Live Response package to endpoints, from the Main menu, go to **Modules** > **Threat Response Management** > **Live Response**, and click **Generate Packages**. You must update all Live Response packages that you deploy to endpoints to reflect updated configurations.

Action not running on endpoint

If an action is not running on an endpoint, ensure that the connection to the endpoint is working by testing the Live Response connections manually. For more information, see testing connections manually.

If the connections to remote endpoints work correctly, but actions are not running, confirm that action approval is not stopping the action from running. Action approval means that actions a user initiates cannot deploy until another user approves those actions. Approvers can be users with the Administrator reserved role or a role that grants Approve Action and Sensor read permissions. If your organization allows exceptions to approval requirements, you can configure a role that grants Bypass Action Approval permission. For more inforrmation, see Tanium Console User Guide: Managing Action Approval.

Artifacts not being copied to destination

If artifacts are not being copied to the destination, review the Live Response log in the folder that corresponds to the action ID.

In addition to the standard action logs on the endpoint (Tanium_Client_Location\Downloads\

©2026 Tanium Inc. All Rights Reserved

Action_###\Action_####.log), a log file of activities resides in the same directory. This file follows the naming convention: YYYYMMDDhhmm_LR.log.

When collection completes, the YYYYMMDDhhmm_LR.log is copied to the destination. The action log is not copied to the destination.

Use both the action log and the Live Response log to troubleshoot problems. The action log captures messages written to standard error (stderr).

Custom configurations are missing

The content of taniumqarantine.dat is restored to the default values every time quarantine content is updated. For example, if you upgrade Threat Response or install a newer version of the Tanium Quarantine solution, any custom configurations that you have added to the quarantine packages either by using the Live Response workbench or by editing the packages manually are overwritten with the default versions of the packages.



Best Practice: Keep a backup copy of any Live Response packages that contain custom configurations so that you can restore your customized packages after a tools upgrade.

Live Connections are not working while quarantined

If you are unable to make live connections to endpoints that you have quarantined, make sure that the ports that Tanium Direct Connect uses to communicate with remote endpoints are not blocked on the target endpoint, and that the IP addresses for the Tanium Module Server (or Zone Server, if applicable) are not blocked. For a list of the ports that must be enabled for remote endpoint communication, see Tanium Direct Connect User Guide: Requirements.

Live Response is not working to copy files to the destination while quarantined

If Live Response is not copying files to the destination while quarantined, make sure that all destination IP addresses and ports for the protocols you are using are defined in the quarantine configuration. For more information, see Isolating Endpoints: Reference: Custom rules and options.

©2026 Tanium Inc. All Rights Reserved

Verify endpoint tools

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

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

Uninstall Threat Response

About this task

You might need to remove Threat Response from the Tanium Module Server for troubleshooting purposes.

1. From the Main menu, go to **Administration** > **Configuration** > **Solutions**.
2. Under Threat Response, click **Uninstall**. Click **Proceed with Uninstall** to complete the process.

Contact Tanium Support

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

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

©2026 Tanium Inc. All Rights Reserved

Reference: Common health check issues

Review common Threat Response health check issues and possible solutions. For more information about general issues in Threat Response, see Troubleshooting Threat Response on page 351.

Fatal error loading subscriptions: auditd raw logging is enabled. Not loading rules.

Cause

This health check appears when auditd.conf is configured to log messages.

Solution

Consider using RAW logging only in instances where disabling would cause a data point of interest to be dropped. For example, use RAW logging if an endpoint has excess resources to handle the CPU and IO load, and an application such as Splunk is analyzing data. To disable RAW logging, deploy the **Recorder - Disable Raw Logging [Linux]** package. The package edits the auditd.conf file with the appropriate setting to disable raw logging for the version of auditd on the endpoint. Deploy the **Recorder - Auditd [Linux]** package to restart auditd after disabled raw logging.

Scan completion took longer than configured scan interval. Maybe under spec or subscription misconfigured?

Cause

This health check appears when an Index scan exceeds the configured scan interval.

Solution

Ensure that all endpoints meet the system requirements for the Client Index Extension and that the subscription is configured properly. Change the scan interval in the Index configuration.

©2026 Tanium Inc. All Rights Reserved

Subscription has dropped events: <subscription name>

Cause

This health check appears when the number of pending journal files has reached or exceeded the maximum number of pending files. A single dropped event causes this health check to display; however, no count of dropped events is provided.

Solution

No action is required with the recorder to address this error. Ensure that systems meet the minimum requirements. Action to mitigate this health check might be required on the consumer end if, for example, a Signal returns many matches that result in alerts.

System minimum requirements not met to enable features: Single CPU detected. Not loading rules.

Cause

This health check appears when an endpoint with a single CPU is detected.

Solution

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 and macOS) ./TaniumClient config set CX.recorder.EnableSingleCpuRequirement 0

©2026 Tanium Inc. All Rights Reserved

All configured audit rules did not load. Check rules for correctness. Recorder may not be seeing all events.

Cause

This health check appears when there is a problem with the existing ruleset. Auditd is encountering an invalid rule and is aborting rule loading. Recorder determines this by returning a nonzero exit code for auditctl -R /etc/audit/audit.rules.

Solution

Ensure that no rules are invalid in /etc/audit/rules.d/audit.rules.

TaniumAuditPipe not running.

Cause

This health check appears when the TaniumAuditPipe is installed, but not currently running. This health check commonly occurs. when running SELinux with a policy that was incorrectly applied.

Solution

Ensure that the directories for Tanium client and above are not symlinks. Ensure that all policies for SELinux have been installed correctly. Review the var/log messages and ensure the pipe is starting.

Failed to configure Tanium Driver provider. Check extensions log. Recorder may not be seeing all events.

Cause

This health check appears when a connection to the Tanium Driver cannot be established.

Solution

Use the **Tanium Driver Status** and **Tanium Driver Version** sensors to ensure that the Tanium Driver is installed properly and running. Look for error messages in these sensors. You can use

©2026 Tanium Inc. All Rights Reserved

Tanium Endpoint Configuration to reinstall the Tanium Driver and/or Tanium Recorder.

Fatal error loading subscriptions: waiting for TaniumAuditPipe to be available. Not getting events.

Cause

This health check appears when audispd is not running, or if it is crashing. The audit pipe is a child process of audispd.

Solution

Ensure that the directories for Tanium Client and above are not symlinks. Ensure that all policies for SELinux have been installed correctly. Review the var/log messages and ensure the pipe is starting.

Profile and/or Intel not fully resolved.

Cause

This health check displays when profiles or intel are not up to date or are incomplete on endpoints.

Solution

Ensure that intel and profiles are deployed to endpoints and that all endpoints meet the minimum requirements. Use the **Client Extensions – Status** sensor to verify that the profile and intel versions are the expected versions.

©2026 Tanium Inc. All Rights Reserved

Reference: Alert data

The Threat Response Client Extension (THR-CX) manages detections and all endpoint resource throttling related to detection and alerting. Alerts are actively acknowledged when they are received and are not duplicated for the same artifact on the same endpoint.

THR-CX returns a finding when intel matches occur. Findings are made available to the Threat Response service. If conditions are met, the Threat Response service uses the content in the finding to generate an alert. A finding consists of the objects it describes. Through the whats object in a finding, a list of ArtifactActivity types is provided. In the ArtifactActivity, an acting_artifact (an Artifact) and/or some relevant_actions can be returned. Those relevant_actions are ArtifactAction, which each can have an Artifact and a verb that describes relevant data points.

A finding from a Signal features an acting_artifact that holds a process. Depending on the Signal definition, it can contain zero or more relevant_actions. For example, if the Signal was checking to see if a file was deleted, there would be a relevant_action that has a FileArtifact as the target with a verb of “delete”.

A sample alert


```
{
  "Alert Id": "00000000-0000-0000-21c5-3019f0ac0143",
  "Timestamp": "2022-06-10T23:19:38.000Z",
  "Computer Name": "mediatoo",
  "Computer IP": "172.16.8.70",
  "Intel Id": 365,
  "Intel Type": "tanium-signal",
  "Intel Name": "Unsigned Process Creating a Binary",
  "Intel Labels": "Beta,Execution,Windows",
  "Match Details": {
    "finding": {
      "whats": [
        {
          "intel_intra_ids": [
            {
              "id": 1204114022
            },
            {
              "id": 1670888670
            },
            {
              "id": 2753281896
            },
            {
              "id": 3854795733
            }
          ],
```


©2026 Tanium Inc. All Rights Reserved

```
          "source_name": "recorder",
          "artifact_activity": {
            "relevant_actions": [
              {

              },
              {
                "verb": 6,
                "target": {
                  "file": {
                    "path": "C:\\Users\\Bob\\AppData\\Local\\Temp\\gfw-install-CZejgRlL.exe",
                    "hash": {
                      "md5": "d41d8cd98f00b204e9800998ecf8427e",
                      "sha1": "da39a3ee5e6b4b0d3255bfef95601890afd80709",
                      "sha256":
"e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"
                    },
                    "size_bytes": {

                    },
                    "modification_time": "2022-06-10T23:19:37.000Z",
                    "instance_hash_salt": "132993767777627641"
                  },
                  "instance_hash": "86390933698657764 59",
                  "artifact_hash": "15425104092171844481"
                },
                "timestamp": "2022-06-10T23:19:37.000Z",
                "tanium_recorder_event_table_id": "4611686018468280136"
              },
              {
                "verb": 6,
                "target": {
                  "file": {
                    "path": "C:\\Users\\Bob\\AppData\\Local\\Temp\\gfw-install-CZejgRlL.exe",
                    "hash": {
                      "md5": "d41d8cd98f00b204e9800998ecf8427e",
                      "sha1": "da39a3ee5e6b4b0d3255bfef95601890afd80709",
                      "sha256":
"e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"
                    },
                    "size_bytes": {

                    },
                    "modification_time": "2022-06-10T23:19:37.000Z",
                    "instance_hash_salt": "132993767777627641"
                  },
                  "instance_hash": "86390933698657764 59",
                  "artifact_hash": "15425104092171844481"
                },
                "timestamp": "2022-06-10T23:19:37.000Z",
                "tanium_recorder_event_table_id": "4611686018468280136"
              }
            ],
            "acting_artifact": {
              "process": {
                "handles": [

                ],
                "pid": 8372,
                "arguments": "\"C:\\Program Files\\Git\\usr\\bin\\mktemp.exe\" -t gfw-
install-XXXXXXXX.exe",
                "file": {
                  "file": {
                    "path": "C:\\Program Files\\Git\\usr\\bin\\mktemp.exe",
```


©2026 Tanium Inc. All Rights Reserved

```
                    "hash": {
                      "md5": "2204459dcbf34aed8906daac26db6f56"
                    }
                  },
                  "instance_hash": "7306911300040087486",
                  "artifact_hash": "7306911300040087486"
                },
                "user": {
                  "user": {
                    "name": "Bob",
                    "domain": "MEDIATOO"
                  }
                },
                "parent": {
                  "process": {
                    "handles": [

                    ],
                    "pid": 7528,
                    "arguments": "sh \"C:\\\\Program Files\\\\Git\\\\mingw64\\\\bin\\\\git-
update-git-for-windows\" --quiet --gui",
                    "file": {
                      "file": {
                        "path": "C:\\Program Files\\Git\\usr\\bin\\sh.exe",
                        "hash": {
                          "md5": "0d46559e826c8a7b5d432d0a91954ba2"
                        }
                      },
                      "instance_hash": "4573824187960625975",
                      "artifact_hash": "4573824187960625975"
                    },
                    "user": {
                      "user": {
                        "name": "Bob",
                        "domain": "MEDIATOO"
                      }
                    }"start_time": "2022-06-10T23:19:37.000Z",
                    "tanium_unique_id": "8426546338933681227"
                  },
                  "instance_hash": "2725601412602158353",
                  "artifact_hash": "6063500060437154276"
                },
                "start_time": "2022-06-10T23:19:37.000Z",
                "tanium_unique_id": "3601155573093657773"
              },
              "instance_hash": "17370642301569032073",
              "artifact_hash": "16343609532904785305",
              "is_intel_target": true
            }
          }
        }
      ],
      "domain": "threatresponse",
      "intel_id": "365:2:761d796b-b362-455f-98ae-6d0472ecf640",
      "hunt_id": "1",
      "threat_id": "1204114022,1670888670,2753281896,3854795733",
      "source_name": "recorder",
      "system_info": {
        "os": "Microsoft Windows 11 Pro",
        "bits": 64,
        "platform": "Windows",
        "build_number": "22000",
        "patch_level": "10.0.22000.0.0"
      },
```


©2026 Tanium Inc. All Rights Reserved

```
      "first_seen": "2022-06-10T23:19:38.000Z",
      "last_seen": "2022-06-10T23:19:38.000Z",
      "finding_id": "2433404061633741123",
      "reporting_id": "reporting-id-placeholder"
    },
    "match": {
      "version": 1,
      "type": "process",
      "source": "recorder",
      "hash": "16343609532904785305",
      "properties": {
        "pid": 8372,
        "args": "\"C:\\Program Files\\Git\\usr\\bin\\mktemp.exe\" -t gfw-install-
XXXXXXXX.exe",
        "recorder_unique_id": "3601155573093657773",
        "start_time": "2022-06-10T23:19:37.000Z",
        "ppid": 7528,
        "user": "MEDIATOO\\Bob",
        "file": {
          "md5": "2204459dcbf34aed8906daac26db6f56",
          "fullpath": "C:\\Program Files\\Git\\usr\\bin\\mktemp.exe"
        },
        "parent": {
          "pid": 7528,
          "args": "sh \"C:\\\\Program Files\\\\Git\\\\mingw64\\\\bin\\\\git-update-git-for-
windows\" --quiet --gui",
          "recorder_unique_id": "84265463389336812227",
          "start_time": "2022-06-10T23:19:37.000Z",
          "ppid": 10396,
          "user": "MEDIATOO\\Bob",
          "file": {
            "md5": "0d46559e826c8a7b5d432d0a91954ba2",
            "fullpath": "C:\\Program Files\\Git\\usr\\bin\\sh.exe"
          }
        }
      }
    }
  },
  "MITRE Techniques": "[\"T1036\",\"T1036.001\"]",
  "Impact Score": ""
}
```


The following fields in the parent JSON provide information that is globally relevant to all alerts and provides information to identify the alert and details about where the alert originated. Not all fields are included in every alert, and sometimes values can be omitted. For example, if Tanium Impact is not present in the environment, you can expect an empty value for Impact score.

Parent JSON fields and descriptions

Field	Field type	Description
Alert ID	string	A unique ID that is assigned to an alert.
Timestamp	timestamp	The timestamp for when the alert was generated on the endpoint.

©2026 Tanium Inc. All Rights Reserved

Field	Field type	Description
Computer Name	string	The name of the endpoint on which the alert was generated.
Computer IP	IP address	The IPv4 address of the endpoint on which the alert was generated.
Intel ID	number	The ID of the intel document that matched an event to generate the alert.
Intel Type	string	The type of intel that matched an event to generate the alert.
Intel Name	string	The name of the intel document that matched an event to generate the alert.
Intel Labels	string	Any labels that have been assigned to the intel document that matched an event to generate the alert.
MITRE Techniques	array	Any MITRE techniques that are relevant to the intel document that matched an event to generate the alert. For more information about MITRE, see MITRE Attack Framwork .
Impact Score	number	The score assigned to the endpoint by Tanium Impact. For more information about Tanium Impact, see Tanium Impact User Guide .

The following tables provide a reference to the objects in the alert, and descriptions of the fields each object supports.

- Artifact on page 387
- ArtifactAction (relevant_actions) on page 387
- ArtifactActivity on page 385
- ArtifactHash on page 395
- AutomationEngine on page 395
- DNSRequestArtifact on page 393
- DriverArtifact on page 395
- ExternalSecurityEvent on page 386
- FileArtifact on page 390

©2026 Tanium Inc. All Rights Reserved

- Finding on page 384
- Finding.Whats on page 385
- IntraIdContext on page 386
- LocalSystemInfo on page 388
- MicrosoftDefenderEventArtifact on page 398
- NetworkPortArtifact on page 394
- ProcessArtifact on page 389
- ProcessArtifact.Handle on page 389
- ReactionStatusDetails on page 396
- ServiceArtifact on page 393
- SignatureData on page 397
- Step on page 396
- StepResult on page 396
- UserArtifact on page 390
- WindowsPEInfo on page 398
- WindowsPEInfo.Exports on page 399
- WindowsPEInfo.Section on page 398
- WindowsPEInfo.Import on page 399
- WindowsPEInfo.Symbol on page 399
- RegistryArtifact on page 391
- RegistryArtifact.MultiSZ on page 392
- RegistryArtifact.Value on page 391

©2026 Tanium Inc. All Rights Reserved

Finding

Finding fields and descriptions

Field	Field type	Description
intel_id	string	An ID that represents the intel document.
hunt_id	string	An ID that represents a hunt. A hunt is a grouping of the currently active intel.
threat_id	string	An ID that provies a way to differentiate findings within a single intel document, this field offers a way to separate.
source_name	string	Informational name of where Threat Response found the finding. Valid values are live, tanium-index, tanium-recorder, netstat, and at-rest.
system_info	LocalSystemInfo on page 388	The information about the system on which the finding happened.
artifact	Artifact on page 387	Deprecated.
first_seen	timestamp	The timestamp of the first finding of the instance.
last_seen	timestamp	The timestamp of the last finding of the instance.
whats[]	Finding.Whats on page 385	A short description of the finding. This is specific to the intel type and the finding itself. Some examples might be the rule name for YARA, the hash for a bad hash, or the technique for process injection.
description	string	A text description of the finding.
finding_id		Internal use only.
legacy_detect_alert_payload		Deprecated.
reporting_id	string	Information that you can use to identify whether the alert was triggered by an On-Demand scan. This data includes the Scan ID when an alert is the result of an On-Demand Scan.
domain	string	For all findings, the domain is threatresponse .
reason	string	Information from a third-party source, for example, Deep Instinct. If available, this field can contain the cause for the finding.

©2026 Tanium Inc. All Rights Reserved

Finding.Whats

Finding.Whats fields and descriptions

Field	Field type	Description
source_name	string	Informational name of where Threat Response found the finding. Valid values are live, tanium-index, tanium-recorder, netstat, and at-rest.
artifact_activity	ArtifactActivity on page 385	The state change that is responsible for the current state.
intel_intra_ids[]	IntraIdContext on page 386	Internal use only. The intel id that generated this What instance. When that intel specifies intra_id's, those may be populated here to give indication of what conditions were met to yield to the match.
security_event	ExternalSecurityEvent on page 386	An external entity was used to locate a finding. It is possible to learn information from the external event and even enrich it. In as much, this is supplemental to the `what` but not part of it.
additional_fields	protobuf "Struct"	Free-form extra data for findings; populated for Defender, Deep Instinct, and Process Injection

ArtifactActivity

ArtifactActivity fields and descriptions

Field	Field type	Description
acting_artifact	Artifact on page 387	Corresponds to the ProcessArtifact on page 389 object.
relevant_actions[]	ArtifactAction (relevant_actions) on page 387	Corresponds to the ArtifactAction (relevant_actions) on page 387 object.
bystander	Artifact on page 387	Corresponds to the ProcessArtifact on page 389 object. In some cases, when a detection is made, it is due to an inline inspector such as Microsoft defender or Deep Instinct inspecting an object because a handle to it has been opened. In many cases, this ends up being Tanium or the EPP solution.

©2026 Tanium Inc. All Rights Reserved

IntraIdContext

IntraIdContext fields and descriptions

Field	Field type	Description
id	deprecated; internal use	Internal use only. Deprecated.
token	string	Internal use only.
id_v2	internal use	Internal use only.
Note: A data structure for internal use that helps identify the components within an intel document that matched.		

ExternalSecurityEvent

ExternalSecurityEvent fields and descriptions

Field	Field type	Description
timestamp	timestamp	The timestamp of the external security event.
type_identifier	string	A representation of the type or non-unique id of the event in string format.
unique_identifier	string	A unique identifier to the event source if one is available.
external_action	enum	a value that corresponds to the type of external action. Value values are (0)unspecified, (1)clean, (2)quarantine, (3)remove, and (4)block.

©2026 Tanium Inc. All Rights Reserved

ArtifactAction (relevant_actions)

ArtifactAction fields and descriptions

Field	Field type	Description
verb	enum	The type of action. Valid values are (0)unknown, (1)connect (including reconnect), (2)accept, (3)disconnect, (4)delete, (5)open, (6)create, (7)move (including rename), (8)write, (9)query, (10)load, (11)inject, (12)execute, and (13)set permissions.
target	Artifact on page 387	The entity acted-upon. For file move or rename, this is the destination. In most cases this holds the entity, which can be various artifact objects.
origin	Artifact on page 387	Used for things like move/rename of file. Most times this is not used.
timestamp	timestamp	The timestamp of the action.
tanium_recorder_event_table_id	number	For cases where the target of this action can be found in the Tanium Recorder, this id allows for deeper inspection.
tanium_recorder_context	MatchItem	Deprecated.

Artifact

Artifact fields and descriptions

Field	Field type	Description
instance_hash	hash	Uniquely identifes an artifact instance across time on a single endpoint.
artifact_hash	hash	Correlates related items across time on a single endpoint or even across endpoints.
is_intel_target	bool	Indicates that this was the artifact originally scoped and found by the intel.
process	ProcessArtifact on page 389	Corresponds to the ProcessArtifact on page 389 object.

©2026 Tanium Inc. All Rights Reserved

Field	Field type	Description
user	UserArtifact on page 390	Corresponds to the UserArtifact on page 390 object.
file	FileArtifact on page 390	Corresponds to the FileArtifact on page 390 object.
windows_registry	RegistryArtifact on page 391	Corresponds to the RegistryArtifact on page 391 object.
windows_event_log	WindowsEventLogArtifact on page 392	Corresponds to the WindowsEventLogArtifact on page 392 object.
service	ServiceArtifact on page 393	Corresponds to the ServiceArtifact on page 393 object.
dns	DNSRequestArtifact on page 393	Corresponds to the DNSRequestArtifact on page 393 object.
port	NetworkPortArtifact on page 394	Corresponds to the NetworkPortArtifact on page 394 object.
driver	DriverArtifact on page 395	Corresponds to the DriverArtifact on page 395 object.
windows_defender_event	MicrosoftDefenderEventArtifact on page 398	Corresponds to the MicrosoftDefenderEventArtifact on page 398 object.

LocalSystemInfo

LocalSystemInfo fields and descriptions

Field	Field type	Description
os	string	The operating system of the endpoint on which the finding occurs.
build_number	string	If available, the build level of the operating system of the endpoint.
patch_level	string	If available, the patch level of the operating system of the endpoint.
bits	number	Valid values are 32 or 64.
platform	enum	The platform of the endpoint. Valid values are: (0)Unknown, (1)Windows, (2)Mac, (3)Linux, (4)AIX, and (5)Solaris.

©2026 Tanium Inc. All Rights Reserved

ProcessArtifact

ProcessArtifact fields and descriptions

Field	Field type	Description
pid	number	The process ID of the ProcessArtifact.
name	string	The name of the ProcessArtifact.
working_directory	string	The working directory of the ProcessArtifact.
arguments	string	The command line of the ProcessArtifact including any arguments.
start_time	timestamp	The start time of the ProcessArtifact.
end_time	timestamp	The end time of the ProcessArtifact.
file	Artifact on page 387	Corresponds to the FileArtifact on page 390 object.
user	UserArtifact on page 390	Corresponds to the UserArtifact on page 390 object.
parent	Artifact on page 387	Corresponds to the ProcessArtifact type that represents an ancestory of the ProcessArtifact.
tanium_unique_id		A unique ID assigned to the ProcessArtifact.
handles[]	ProcessArtifact.Handle on page 389	Corresponds to the ProcessArtifact.Handle on page 389 object.
tanium_recorder_table_id		An ID that corresponds to a table in the Recorder database.

ProcessArtifact.Handle

ProcessArtifact.Handle fields and descriptions

Field	Field type	Description
name	string	A possible name of the ProcessArtifact on page 389 .
type	string	A possible type of the ProcessArtifact on page 389 .

©2026 Tanium Inc. All Rights Reserved

UserArtifact

UserArtifact fields and descriptions

Field	Field type	Description
name	string	The user who initiated the artifact.
domain	string	The domain (or group on macOS/Linux) under which the artifact was initiated.
user_id	string	The user ID of the user who initiated the artifact.
group_id	string	The group ID of the user who initiated the artifact.

FileArtifact

FileArtifact fields and descriptions

Field	Field type	Description
path	string	The full path in the file system for the FileArtifact.
hash	ArtifactHash on page 395	Corresponds to the Artifact Hash type. The algorithm and hash of the file artifact.
size_bytes	number	The file size of the FileArtifact.
modification_time	timestamp	The timestamp of the most recent file modification for the FileArtifact.
instance_hash_salt	hash	Internal use only.
magic_number	number	Deprecated.
magic_number_hex	string	The hex value of the magic number for the FileArtifact.
windows_pe_info	WindowsPEInfo on page 398	Information about Windows PE endpoints.
signature_data	SignatureData on page 397	Corresponds to the SignatureData on page 397 object.
container	Artifact	Corresponds to the FileArtifact object.

©2026 Tanium Inc. All Rights Reserved

RegistryArtifact

RegistryArtifact fields and descriptions

Field	Field type	Description
hive	string	The hive (a logical group of keys, subkeys, and values) in the registry.
key_path	string	The path to the key in the registry.
modification_time	timestamp	The timestamp of the most recent modification for the RegistryArtifact.
num_subkeys	number	The number of subkeys of the RegistryArtifact.
num_values	number	The number of values of the RegistryArtifact.
values[]	RegistryArtifact.Value on page 391	Corresponds to the RegistryArtifact.Value on page 391 object.

RegistryArtifact.Value

RegistryArtifact.Value fields and descriptions

Field	Field type	Description
name	string	The name of the registry value.
reg_dword	number	The data type of the registry value. Only one of these fields are supported for each object instance.
reg_qword	number	
reg_sz	string	
reg_expand_sz	string	
reg_multi_sz	RegistryArtifact.MultiSZ on page 392	
reg_binary	bytes	

©2026 Tanium Inc. All Rights Reserved

RegistryArtifact.MultiSZ

RegistryArtifact.MultiSZ fields and descriptions

Field	Field type	Description
reg_sz[]	string	A sequence of null-terminated strings, terminated by an empty string (\0). The following is an example: String1\0String2\0String3\0LastString\0\0. The first \0 terminates the first string, the second-from-last \0 terminates the last string, and the final \0 terminates the sequence.

WindowsEventLogArtifact

WindowsEventLogArtifact fields and descriptions

Field	Field type	Description
eid	number	A unique ID that corresponds to a specific endpoint.
log_name	string	Name of the event log to which events from different logging components are written. Events are commonly logged for system, security, and applications.
source_name	string	Name of the program or software causing the event log.
message	string	The content of the log that matched to generate the alert.
computer	string	Name of the computer logging the event.
category	string	Identifies the type of recorded event log. Application developers can also define task categories to serve as extra information about the event.
gen_time	timestamp	Includes the date and time when the event occurred.
write_time	timestamp	Includes the date and time when the event was logged.
category_number	number	A numeric representation of the category.

©2026 Tanium Inc. All Rights Reserved

ServiceArtifact

ServiceArtifact fields and descriptions

Field	Field type	Description
name	string	A string that corresponds to the name of an artifact that comes from a Windows service value.
descriptive_name	string	A string that corresponds to the descriptive name of an artifact that comes from a Windows service value.
description	string	A string that corresponds to the description of an artifact that comes from a Windows service value.
started_as	string	A string that corresponds to the started at time of an artifact that comes from a Windows service value.
mode	string	A string that corresponds to a Windows service value.
status	string	A string that corresponds to a Windows service value.
type	string	A string that corresponds to a Windows service value.
exe	FileArtifact on page 390	Corresponds to the FileArtifact on page 390 object.
dll	FileArtifact on page 390	Corresponds to the FileArtifact on page 390 object.
process	ProcessArtifact on page 389	Corresponds to the ProcessArtifact on page 389 object.
arguments	string	The command line of the ServiceArtifact on page 393 including any arguments.

DNSRequestArtifact

DNSRequestArtifact fields and descriptions

Field	Field type	Description
host	string	The service that runs Domain Name System (DNS)

©2026 Tanium Inc. All Rights Reserved

Field	Field type	Description
record_name	string	The name of the record that directs a hostname to an IP address.
ttl	number	The duration of time to cache a query before requesting a new one.
ipv4	string	The IPv4 address of the endpoint.
cname	string	A record that functions as an alias for domain names that share a single IP address.
observed_time	timestamp	Correlates to when the request was seen in a cache or in an actual request if that was available.
text_request	string	A text version of the record request.
text_response	string	A text version of the response to the record request.

NetworkPortArtifact

NetworkPortArtifact fields and descriptions

Field	Field type	Description
protocol	string	The protocol that was used in the network event. For example, HTTP.
local_ip	string	The IP address of the local endpoint.
remote_ip	string	The IP address of the remote endpoint.
local_port	number	The port used on the local endpoint.
remote_port	number	The port used on the remote endpoint.
state	string	The state of the remote network port. For example, forwarding.
process	ProcessArtifact on page 389	Corresponds to the ProcessArtifact on page 389 object.
connection_time	timestamp	The timestamp of the network connection.

©2026 Tanium Inc. All Rights Reserved

DriverArtifact

Driver artifact fields and descriptions

Field	Field type	Description
name	string	The name of the DriverArtifact on page 395 .
file	Artifact	Corresponds to the FileArtifact on page 390 object.

ArtifactHash

Artifact hash fields and descriptions

Field	Field type	Description
md5	string	The hash of the artifact using the MD5 hashing algorithm.
sha1	string	The hash of the artifact using the SHA1 hashing algorithm.
sha256	string	The hash of the artifact using the SHA256 hashing algorithm.

AutomationEngine

AutomationEngine fields and descriptions

Field	Field type	Description
`friendly_name`	string	The name given to a reaction by the user.
`dry_run`	boolean	Whether or not a reaction was run in audit mode.
`step`	Step on page 396	Repeated field of step results from an automation.

©2026 Tanium Inc. All Rights Reserved

ReactionStatusDetails

ReactionStatusDetails fields and descriptions

Field	Field type	Description
at	timestamp	Timestamp at which the reaction was completed.
`automation_engine`	AutomationEngine on page 395	Collected details from an internal run of a reaction.

Step

Step fields and descriptions

Field	Field type	Description
friendly_name	string	The name of the reaction step given by the user.
`reaction_step_idx`	integer	An index of the step that was run. Zero based index.
result	StepResult on page 396	The result information for this step.
artifact	Artifact on page 387	A repeated artifact field of the artifacts that were acted on by the step.
step_type	string	A system specified string of a generalization of what the step was (Remove File, Kill Process, Quarantine, etc.)

StepResult

StepResult fields and descriptions

Field	Field type	Description
`step_name`	string	Name of the step. Matches friendly_name from Step.
`step_number`	integer	An index of the step that was run. Zero based index.

©2026 Tanium Inc. All Rights Reserved

Field	Field type	Description
`step_description`	string	Description of what the step was doing.
`step_message`	string	Result message from the step. Empty if no errors.
`result_code`	enum	An enumeration of the result of a step. Valid values are (0)Step has not yet been run, (1)Step completed successfully with no errors, (2)Step completed with non-critical errors. Automation will continue, (3)Step failed with critical error. Automation will exit, (4)Step timed out
`start`	timestamp	Timestamp of when the step started.
`end`	timestamp	Timestamp of when the step completed.

SignatureData

SignatureData fields and descriptions

Field	Field type	Description
status	enum	The status of the signature data. Valid values are (0)Unverified, (1)Verified, (2)NoSignature, (3)Error, (4)Disallowed, (5)NotTrusted, (6)NotTrustedPolicy, (7)FileNotExists, (8)NotChecked, (9)Pending, (10)CheckingDisabled, and (11)TimedOut.
issuer	string	The entity who issued the signature.
subject	string	The subject of the signature.

©2026 Tanium Inc. All Rights Reserved

MicrosoftDefenderEventArtifact

MicrosoftDefenderEventArtifact fields and descriptions

Field	Field type	Description
timestamp_ms	number	The timestamp of the Microsoft Defender event.
event	ETWDefenderEvent	The event ID of the Microsoft Defender event. For more information about Microsoft Defender events, see https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/troubleshoot-microsoft-defender-antivirus .

WindowsPEInfo

WindowsPEInfo fields and descriptions

Field	Field type	Description
type	string	The type of object.
timestamp	timestamp	The timestamp of the object.
sections[]	WindowsPEInfo.Section on page 398	Corresponds to the WindowsPEInfo.Section on page 398 object.
exports	WindowsPEInfo.Exports on page 399	Corresponds to the WindowsPEInfo.Exports on page 399 object.
imports[]	WindowsPEInfo.Import on page 399	Corresponds to the WindowsPEInfo.Import on page 399 object.

WindowsPEInfo.Section

WindowsPEInfo.Section fields and descriptions

Field	Field type	Description
name	string	The name of the section.
size_bytes	number	The size (in bytes) of the section.

©2026 Tanium Inc. All Rights Reserved

WindowsPEInfo.Exports

WindowsPEInfo.Exports fields and descriptions

Field	Field type	Description
name	string	The name of the export.
symbols[]	WindowsPEInfo.Symbol on page 399	Corresponds to the WindowsPEInfo.Symbol on page 399 object.

WindowsPEInfo.Import

WindowsPEInfo.Import fields and descriptions

Field	Field type	Description
name	string	The name of the import.
symbols[]	WindowsPEInfo.Symbol on page 399	Corresponds to the WindowsPEInfo.Symbol on page 399 object.

WindowsPEInfo.Symbol

WindowsPEInfo.Symbol fields and descriptions

Field	Field type	Description
name	string	The name of the symbol.

©2026 Tanium Inc. All Rights Reserved

Reference: Set up the zone proxy service

In Threat Response, the options for the Zone Proxy setup is contained in Tanium Direct Connect. To use Direct Connect to manage zone proxy connections, you must install and enable Direct Connect. For more information, see Tanium Direct Connect User Guide: Installing.

In earlier versions of Threat Response there was a requirement to make a configuration from Threat Response and import on the zone server. In the current version, the configurations for zone proxy are all contained in Direct Connect. When Direct Connect is configured and running there are no required actions for Threat Response. When the Direct Connect service is enabled when making a live connection the Threat Response service issues the **Deploy Direct Connect - Open Session** action.

To install Direct Connect and configure the Direct Connect Zone Proxy:

1. Install Direct Connect. See Tanium Direct Connect User Guide: Installing for more information.

2. Install and configure the Direct Connect Zone Proxy. See Tanium Direct Connect User Guide: Configure Zone Proxies for more information.

In an upgrade scenario, to get the zone proxy to run on the same ports are you have been using you need to stop and remove the current zone proxy infrastructure prior to installing the Direct Connect proxy and ensure that the ports are available for the new service. From Threat Response, click Settings and click the current zone server configuration. To move from this configuration to the Direct Connect configuration, use the same port in the Direct Connect configuration.

©2026 Tanium Inc. All Rights Reserved

Reference: Gateway examples for Threat Response

Tanium Gateway provides a GraphQL API integration point for Tanium solutions, including Threat Reponse. Threat Response includes a mutation to assign the **Resolved** status to a Threat Response alert.

For additional Gateway example syntax, see Tanium Gateway User Guide: Reference: Filter syntax and Tanium Gateway User Guide: Reference: Gateway examples.

Assign Resolved status to an alert

About this task

`mutation.threatResponseAlertResolve`

Assign Resolved status to alert

(mutation.threatResponseAlertResolve)

About this task

The following request assigns the **Resolved** status to the Threat Response alert matching the GUID.

```
mutation exampleResolveTHRAlert($guid: ID) {
  threatResponseAlertResolve(ref: {guid: $guid}) {
    resolved
    guid
    error
  }
}
```

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

```
{
  "guid": "12345678-90ab-cdef-1234-567890abcdef"
}
```

Example response:

```
{
```

©2026 Tanium Inc. All Rights Reserved

```
  "data": {
    "threatResponseAlertResolve": {
      "resolved": true,
      "guid": "12345678-90ab-cdef-1234-567890abcdef",
      "error": null
    }
  }
}
```

©2026 Tanium Inc. All Rights Reserved

Reference: Authoring Signals

You can use Signals for the continuous, real-time evaluation of process, network, registry (Windows only), and file events on endpoints. Signals are available as a feed from Tanium, or you can author your own Signals that are specific to your environment.

With Signals you can detect suspicious or interesting process behavior by combining multiple search expressions. A narrow search scope helps you minimize false-positive alerts.

How Signals work

Signals use a specific language syntax to build search expressions for process-related events on the endpoint.

Like other intel, Signals get validated when they are added to the Threat Response service to ensure proper structure. The Signals are compiled, then sent and applied to the appropriate computer groups.

Unlike other types of intel, the recorder continuously inspects each process creation event in real time and Threat Response reports a finding when a match occurs, rather than performing periodic scans. Each event gets evaluated against any Signal definitions. Whenever a Signal condition is matched, a finding is generated. Threat Response regularly polls the endpoints with a saved question to gather alerts that are written to the Alerts page.

Signal syntax

Important: An exhaustive reference to Signals syntax - including supported objects, properties, and conditions - is available in the Threat Response Intel Support documentation. To access the Threat Response Intel Support documentation, click ? from the Threat Response overview page and click the Threat Response Intel Support tab.

The syntax of Signals are built from the supported *objects*, *properties*, *conditions*, and the search

©2026 Tanium Inc. All Rights Reserved

values into search expressions. One or more expressions make up the Signal *definition*. The objects reference process-related events. For example, a file object is an operation on a file by a process. A Signal can have multiple expressions in a single definition, connected with AND or OR operators. Use parentheses to dictate precedence.

Write Signal expression in one of the following formats:

- object.property condition value
- object.property condition 'value with spaces'

Each object is a type of process event and has one or more properties that narrow the scope of the event. The condition specifies how the object and property relate to the value provided. Not all conditions are supported with all object properties.



Note: You cannot have more than 55 unique terms in a Signal.

Property values can be an integer, a simple alphanumeric string, or they can be more complex and include other characters, such as spaces, backslashes, and hex-encoded values. For searches with non-alphanumeric values or spaces, enclose the value in single quotes. To escape special characters within the single quotes, the following sequences are supported:

- `\r` For carriage return
- `\n` For newline
- `\t` For tab
- `\\` For the backslash itself
- `\'` For a single quote within the quotes
- `\x` To allow a single-byte hex-encoded sequence. For example \x20 would translate to a single space. The Signal builder does not support the \x escape character.

©2026 Tanium Inc. All Rights Reserved

Note: The hex-encoding is required to handle UTF-8 characters outside of the single-byte character set. Any UTF-8 character can be added via the hex-encoding, if needed.

The following sample expressions demonstrate combined expressions, precedence, and escaped special characters:

- Windows: `process.command_line contains 'evil' AND process.path starts with 'c:\\windows'`
- Linux: `process.command_line contains 'evil' AND process.path starts with '/usr/sbin/'`
- Windows: `(file.path starts with 'c:\\temp' OR file.path ends with '.evil.tmp') AND process.path contains cmd.exe`
- Linux: `(file.path starts with '/var/tmp/' OR file.path ends with 'evil.gz') AND process.path ends with 'sh'`

You can use modifiers in parenthetical groupings to change the behavior of all items within that grouping. A modifier is an identifier that precedes an open parenthesis. One example is for event grouping:

```
group(file.operation is 'create' and file.path contains 'foo')
```

Without the group this would appear as a boolean grouping prioritized in operation by the ()'s and could be satisfied with two different events, however in this case the group modifier is applied thus changing the matching behavior so that both conditions must match a single event.

Note: Event groups do not support terms that contain process events.

An event group modifier is a modifier with the name group and indicates that you intend to match all conditions in the group against a single event. For example, to ensure that matches happen against the same file event, you should group those events. You can then include multiple groups to achieve matches against different events in time. One example would be:

```
group(file.operation is 'create' and file.path contains 'foo') and
group(file.operation is 'delete' and file.path contains 'bar')
```

©2026 Tanium Inc. All Rights Reserved

This signal would only match if at some point a process creates a file containing foo and at a different time deletes a file with name containing bar, but will not match if the created file contained bar and the deleted file contained foo.

An event group modifier can only apply to objects of the same type. So, you may not mix file and registry events in the same group, though you may mix groups containing those into the same expression as:

```
group(registry.key_path contains 'alpha' and registry.value_name contains 'a') and group(file.path.contains 'beta' and file.path ends with '.b')
```

Note: Signals are not case-sensitive.

Note: For file operations, the `rename` operation corresponds to the `move` operation in the recorder events view.

Signal use cases

Signals are designed to identify suspicious or malicious process activity in real time, and therefore are not intended to alert on large lists of file properties, such as hashes or file names. These use cases are better solved with background intel scanning or reputation alerting. For example, alerting on excel.exe is not very useful and creates a lot of unnecessary activity with little value.

However, a security operations center might want an alert if excel.exe launches PowerShell.exe. and the parent process is 'excel.exe'. For example, `process.path ends with 'powershell.exe' AND process.parent_path ends with 'excel.exe'`.

A comparable example for Linux could be: `process.path ends with 'sshd' AND process.parent_path ends with 'systemd'`.

Use Signals to detect activity that, while not malicious, is unwanted within a specific group of computers. For example, the use of dsquery.exe or dsget.exe to administer Active Directory could be an unwanted activity. If your normal process is to use custom PowerShell scripts, use of these other

©2026 Tanium Inc. All Rights Reserved

processes might signify that an intruder is trying to make modifications. If firewall settings are inherited through GPO settings, the use of netsh.exe on an endpoint might need to be understood.

Use Signals to ensure that some activity has happened. For example, receiving alerts from servers when a critical application has launched following a reboot might be a Signal to consider. Alerting that the w3wp.exe process has launched after an IIS server has rebooted might be something a Web Content team would want to see.

Signals must have a narrow scope, specific targets, and a clear intended use.

©2026 Tanium Inc. All Rights Reserved

Reference: Sensors

Use sensors for scoping incidents and rapidly responding to them. Threat Response provides sensors that are executed on all endpoints and diagnostic sensors to monitor the Threat Response service. Where appropriate, these sensor results include a timestamp in the `YYYY-MM-DD HH:MM:SS.mmm+00:00` format.



Note: Threat Response sensors permit the use of regular expressions. If the **Treat input as regular expression** option is enabled, special characters and literals require character escapes.

About deploying parameterized sensors as actions

Sensors that require extensive computational resources across the security enterprise are deployed as actions. An example of a computational sensor is one that hashes files and performs binary searches. Deploying parameterized sensors as actions increases the speed of larger tasks, including:

- Searching across directories for binary data
- Matching the hash values of files across many directories
- Hashing and matching executables and their loaded modules

Actions are not processed one at a time. Short actions run at the same time as longer actions. Because actions are not strictly queued, shorter actions are not delayed by the execution of more extensive actions.

Actions do not time out. Because the processing time of an action depends on the nature of the task, an action is considered complete when the job begins. The results, however, might not be immediately available.

©2026 Tanium Inc. All Rights Reserved

Deploy a parameterized sensor as an action

1. Identify the endpoints that you want to target.
    a. Ask a question to return a set of endpoints.
    b. Select the endpoints and click **Deploy Action**.
2. Specify the parameterized sensor.
    a. Type the name of the parameterized sensor in the **Deployment Package** field.
    b. Specify parameters for the sensor.
    c. Click **Show Preview to Continue** and review the results.
    d. Complete deployment of the action. Click **Deploy Action**.
3. Get the results of the parameterized sensor action.

©2026 Tanium Inc. All Rights Reserved