

Tanium™ Reveal User Guide

Autonomous IT. Unstoppable Business.

2026H1 Semiannual Release

Version 2.5

May 27, 2026

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

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

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

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

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

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

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

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

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

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

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

© 2026 Tanium Inc. All Rights Reserved

© 2026 Tanium Inc. All rights reserved.

Table of contents

Reveal overview **8**

Rule sets 8

Rules 8

Patterns 9

Gaining organizational effectiveness with Reveal **10**

Change management 10

RACI chart 10

Organizational alignment 13

Operational metrics 13

Reveal maturity 13

Benchmark metrics 14

Reveal requirements **17**

Core platform dependencies 17

Computer group dependencies 17

Solution dependencies 18

Tanium recommended installation 18

Import specific solutions 18

Required dependencies 18

Client extensions and endpoint tools 18

Tanium Module Server 19

Endpoints 19

Supported operating systems 19

Disk space requirements 20

Host and network security requirements 20

Ports 20

Security exclusions 21

User role requirements 23

© 2026 Tanium Inc. All Rights Reserved

Installing Reveal **28**
Before you begin 28
Import Reveal with default settings 28
Import Reveal with custom settings 29
Manage solution dependencies 29
Upgrade Reveal 29
Remove legacy Index dependencies from endpoints 29
Verify Reveal version 30
Configuring Reveal **31**
Install and configure Tanium Endpoint Configuration 31
Manage solution configurations with Tanium Endpoint Configuration 31
Configure Reveal 32
Configure the Reveal action group 32
Set up Reveal users 32
(Optional) Deploy scans 35
(Optional) Configure Reveal service settings 35
Creating profiles **37**
Profile status 37
Create a profile 37
Prioritize profiles 38
Edit a profile 39
Deploy a profile 39
Delete a profile 39
Creating patterns **40**
Update patterns created by Tanium 40
Update patterns in an air-gapped environment 40
Regex pattern considerations 40
Create a regex pattern 41
Create a keyword list 42
Edit a pattern 42

© 2026 Tanium Inc. All Rights Reserved

Delete a pattern ... 42
Creating rules ... **43**
Criteria for rule evaluation ... 43
Zip file considerations ... 43
Rule conditions ... 44
Create a rule ... 44
Deploy rules ... 47
Creating rule sets ... **48**
Create a rule set ... 48
Add rules to an existing rule set ... 49
Delete a rule set ... 50
Investigating rule matches ... **51**
Investigate by endpoint ... 51
Validating pattern matches ... **53**
Overview ... 53
Create a validation ... 53
Deploy validations ... 54
Audit published validations ... 55
Searching across the enterprise ... **56**
Perform a quick search ... 56
Investigate quick search results ... 56
Maintaining Reveal ... **58**
Review and remediate Tanium Reveal issues ... 58
Monitor and troubleshoot Reveal coverage ... 58
Monitor and troubleshoot endpoints with confirmed sensitive data ... 59
Monitor and troubleshoot endpoints with unconfirmed sensitive data ... 59
Troubleshooting Reveal ... **60**
Collect logs ... 60
Verify endpoint tools ... 60
Identify and resolve issues with Client Extensions ... 60

© 2026 Tanium Inc. All Rights Reserved

Review the Extensions log for an endpoint ... 62
Configure client disk space use ... 62
Modifying client disk space thresholds ... 63
Remove Reveal tools from endpoints ... 63
Uninstall Reveal ... 65
Contact Tanium Support ... 65
Reference: Supported file types for rule evaluation ... 66
Zip file considerations ... 66
File type filters for rules ... 66
Supported MIME types ... 67
Reference: Reveal endpoint tools ... 68
Reference: Reveal endpoint settings ... 69
Tanium Index subscription settings ... 69
Reveal endpoint settings ... 69
Reference: Reveal sensors and packages ... 71
Deprecated Reveal sensors and packages ... 72
Sensor replacements from Reveal 1.x to Reveal 2.x ... 73

© 2026 Tanium Inc. All Rights Reserved

Reveal overview

With Reveal, you can detect sensitive unstructured data at rest on Tanium Client managed endpoints across an entire IT environment. Use Reveal to continuously monitor for artifacts that match patterns. When sensitive content that matches a pattern is discovered, you can categorize the files where the content exists and further analyze or take action on them to address regulatory compliance, information security, or data privacy issues.

Rule sets

Rule sets group related rules that are collectively used for a specific purpose, such as evaluating compliance with a particular standard, and target rules to specific groups of endpoints.

Create and apply rule sets to provide the most relevant Reveal capabilities to specific groups of endpoints. For example, you can create rule sets that apply rules that discover sensitive data specific to financial information or health records.

Reveal features the following rule sets:

PCI

PCI standards help companies that accept, process, store, and transmit credit card information to maintain a secure environment.

HIPAA

HIPAA standards help protect sensitive patient health data.

GDPR

GDPR standards help protect personal data and ensure European Union compliance.

CCPA

CCPA standards help protect personal data and ensure State of California compliance.

Rules

With rules, you can specify patterns to match in specific types of files and perform an action on either the file or the endpoint when Reveal discovers a match. For example, you could categorize all of the text documents as 'confidental' where a social security number pattern matches.

You can create multiple rules to evaluate content on the same files on each endpoint. For example, you can create a rule that detects credit card numbers, a rule that detects social security numbers, and a rule that detects email addresses, and evaluate each rule on specific types of files. The results of each rule indicate which files contain matches for which pattern. Results are categorized by each rule so that you can quickly locate pattern matches.

© 2026 Tanium Inc. All Rights Reserved

TIP

You can view the rules that Reveal provides through Tanium™ Console. From the Main menu, go to **Modules > Reveal > Rules**. Tanium-provided rules appear with the Tanium logo .

Patterns

In Reveal, a pattern is an expression that matches entities that can otherwise be hidden in the context of other information.

For example, a pattern could match an entity such as a credit card number or email address. Such a pattern could be assigned to a rule to match entities in unstructured data such as a word processing document, text file, PDF document, or spreadsheet. Reveal provides patterns for several types of sensitive information, such as credit card numbers, social security numbers, and email addresses. For more information, see Creating patterns on page 40.

TIP

You can view the patterns that Reveal provides through Tanium Console. From the Main menu, go to **Modules > Reveal > Patterns**, and then set the **Author** filter to **Tanium**.

© 2026 Tanium Inc. All Rights Reserved

Gaining organizational effectiveness with Reveal

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

- Develop a dedicated change management process. For more information, see Change management on page 10.
- Define distinct roles and responsibilities. For more information, see RACI chart on page 10.
- Track operational maturity. For more information, see Operational metrics on page 13.
- Validate cross-functional alignment. For more information, see Organizational alignment on page 13.

Change management

Develop a tailored, dedicated change management process for discovering sensitive data on Tanium Client managed endpoints, taking into account the new capabilities provided by Tanium.

- Update SLAs and align activities to key resources for Tanium Reveal activities across IT Security, IT Operations, and IT Risk and Compliance.
- Designate change or maintenance windows for various data identification scenarios; for example, implementing rules for CCPA, GDPR, PCI, PII, custom content, investigating alerts, and validating rules.
- Identify internal and external dependencies to your data identification process; for example, to support eDiscovery, or investigate insider threats and policy violations.
- Create a Tanium Steering Group (TSG) for data identification activities to expedite reviews and approvals of processes that align with SLAs.

RACI chart

A RACI chart identifies the team or resource who is **R**esponsible, **A**ccountable, **C**onsulted, and **I**nformed, and serves as a guideline to describe the key activities across the security, risk/compliance, and operations teams. Every organization has specific business processes and IT organization demands. The following table represents Tanium's point of view for how organizations should align functional resources against discovery of sensitive data. Use the following table as a baseline example.

© 2026 Tanium Inc. All Rights Reserved

RACI chart for Tanium Reveal

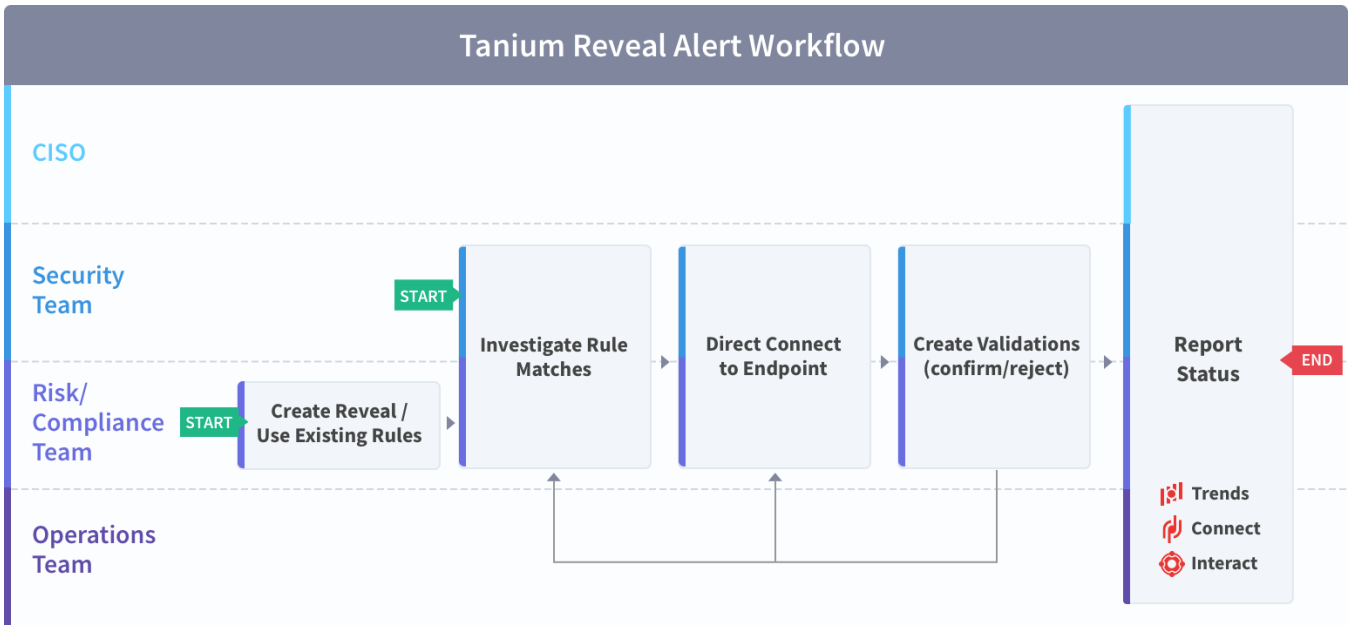
Task	IT Security	IT Operations	IT Risk/Compliance	Executive	Rationale
Determine which default rules to use or which custom rules to create	C	I	R/A	C	When Reveal is originally installed, there are default rules for PCI, HIPAA, GDPR, and CCPA. The Risk/Compliance team might have other items they need to track and will be accountable for defining those rules and categories. The security team will be consulted along with the CIO/CRO/CPO to ensure proper policy coverage.
Investigate rule matches using direct endpoint connections	R/A	I	R/A	-	Both the security and risk/compliance teams will investigate rule matches and are accountable for acting on the alert. The security team is more likely to connect to the endpoint for further investigation.
Validate rule pattern matches	R/A	I	R/A	-	Both the security and risk/compliance teams will validate rule pattern matches to confirm the matches or reject false positives and reduce noise to more accurately represent the alert.
Search for sensitive information that matches a search string in real-time	R/A	R	R/A	-	The security and risk/compliance teams will be accountable to define what data is sensitive; however, operations and the other two teams should have access to search for said data in real time.

© 2026 Tanium Inc. All Rights Reserved

RACI chart for Tanium Reveal (continued)

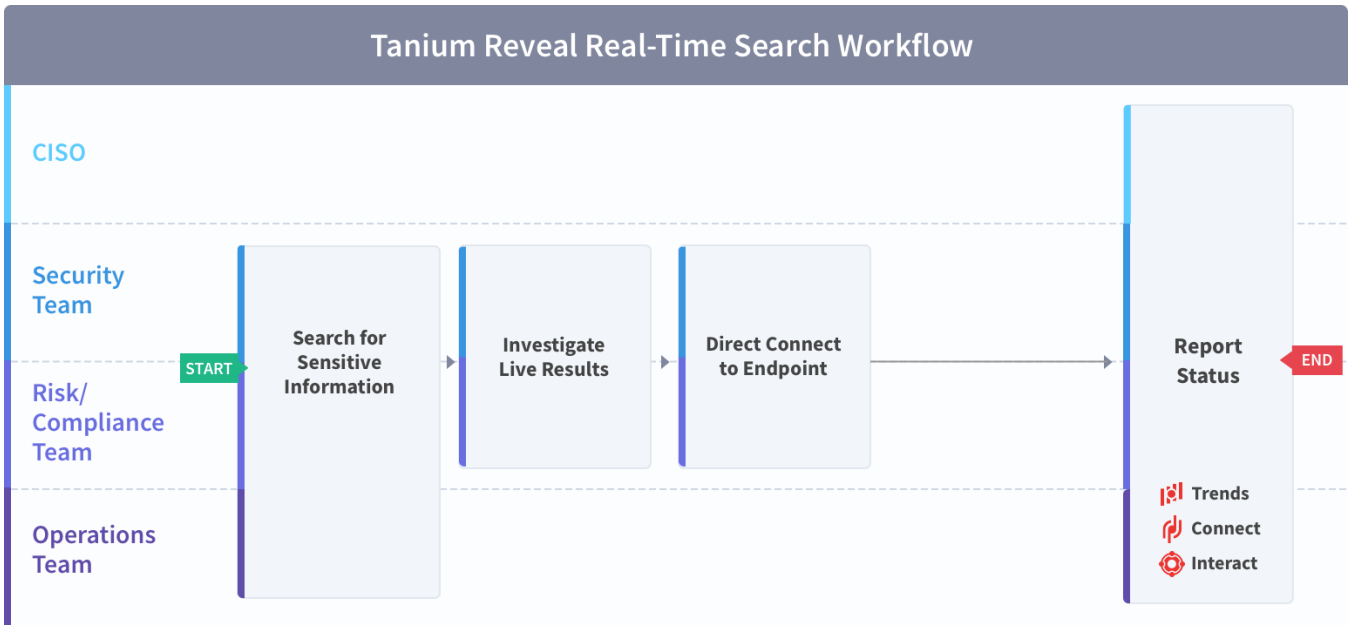
Task	IT Security	IT Operations	IT Risk/Compliance	Executive	Rationale
Reporting through Tanium Trends or external systems; for example, a SIEM.	R/A	I	C/I	C/I	Reporting can be automated via Tanium™ Trends boards and/or integrated with other tools such as a SIEM via Tanium™ Connect for ease to digest, share with executives, or other owners that require action or remediation.

Tanium Reveal alert workflow



© 2026 Tanium Inc. All Rights Reserved

Tanium Reveal real time search workflow



Organizational alignment

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

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

Operational metrics

Reveal maturity

Managing a data identification 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 Reveal program are as follows:

Processes to measure Tanium Reveal maturity

Process	Description
Usage	how and when Reveal is used in your organization
Automation	how automated Reveal is in your environment
Functional Integration	how integrated Reveal is, across IT security, IT operations, and IT risk/compliance teams
Reporting	how automated Reveal is and who the audience of Reveal reporting is

© 2026 Tanium Inc. All Rights Reserved

Benchmark metrics

In addition to the key Reveal processes, the four key benchmark metrics that align to the operational maturity of the Reveal program to achieve maximum value and success are as follows:

Benchmark metrics for Tanium Reveal maturity

Executive Metrics	Reveal Coverage	Endpoints with findings per rule	Validation needed
Description	Percentage of managed endpoints with Reveal installed. Without Reveal , there is no way to know if sensitive or prohibited information is present in files at rest.	Number of endpoints with hits/findings per rule. Rules are based on CCPA, GDPR, HIPAA, PII, PCI, and other custom criteria.	Shows the numbers of unvalidated hits/findings. Over time, as validations are created, this number should trend down.
Instrumentation	Trends panel showing where Reveal is installed.	Trends panel showing matches on endpoints.	Trends panel showing the trend - should trend down.
Why this metric matters	Without Reveal, there is no way to know if sensitive or prohibited information is present in files at rest.	There are many laws and regulations around the world a company must follow to protect personal data. These laws and regulations include CCPA, GDPR, HIPAA, PII, PCI, PHI, and several others. Failure to follow and/or enforce these standards can cost thousands to millions of dollars. There are also similar concerns about PCI, PII, and other sensitive information.	When rule hits are found, they are initially unconfirmed. The Reveal workflow includes an analysts reviewing those hits and creating validations - valid or invalid. Over time, this amount of work should go down as proper validations are created.

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

© 2026 Tanium Inc. All Rights Reserved

Tanium Reveal maturity levels

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
Process	Usage	Reveal module and action group configured, Tanium default rule sets deployed	Target rule sets by Computer Group based on what information is acceptable vs not acceptable on those endpoints	Custom rules created with provided patterns based on governance policies, e.g. customer specific account number. Rule matches investigated and data validated, Include filters and / or pattern / pattern proximity group to reduce false positives	Create rules based on custom patterns. Support for eDiscovery for use in legal proceedings	Taking action based on hits or category results, Identifying and investigating insider threats and policy violations
	Automation	Manual	Manual	Email alert results with Tanium Connect	Email generic alert results with Tanium Connect	Email specific alert results with Tanium Connect tailored to type of data discovered
	Functional integration	Direct Connect for direct endpoint connections	Tanium™ Enforce for device control / removable media, Tanium™ Threat Response	Tanium Connect, Reports on numbers of hits by endpoint or total aggregate to SIEM	Tanium™ Impact, Tanium™ Data Service	ITSM workflow
	Reporting	Manual; via Reveal workbench / dashboard for operators only	Manual; Reveal workbench / dashboard for operators / peer group only	Automated; Reports/Trends Boards tailored to stakeholders ranging from Operator to Executive	Automated; Reports/Trends Boards tailored to stakeholders ranging from Operator to Executive and Legal	Automated; Reports/Trends Boards tailored to stakeholders ranging from Operator to Executive, Legal, and HR

© 2026 Tanium Inc. All Rights Reserved

Tanium Reveal maturity levels (continued)

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
Metrics	Endpoints managed	0-49%	50-65%	65-85%	85-95%	95-100%
	Endpoints with findings	>50%	25-50%	15-24%	10-14%	0-9%
	Validations needed	>= 60%	40-59%	20-39%	10-19%	0-9%

© 2026 Tanium Inc. All Rights Reserved

Reveal requirements

Review the requirements before you install and use Reveal.

NOTE

Reveal 2.0 and later does not run on a Tanium Client managed endpoint as the Reveal Client Extension. All Reveal functionality is provided by the Tanium™ Client Index Extension, and all data is stored in the Index database.

Reveal data in versions 2.0 and later no longer resides in the Tools/Reveal folder on the endpoint. In earlier versions of Reveal, scanned files were first found by Index scans and then parsed by Reveal, and the results stored in the Reveal database.

Reveal versions 2.0 and later still scans endpoint filesystems with Index, and then a parallel Index process detects rule matches.

Core platform dependencies

Make sure that your environment meets the following requirements:

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

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 Reveal requires:

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

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.

© 2026 Tanium Inc. All Rights Reserved

Solution dependencies

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



Some Reveal dependencies have their own dependencies, which you can see by clicking the links in the lists of Required dependencies on page 18 and Reveal requirements on page 17. Note that the links open the user guides for the latest version of each solution, not necessarily the minimum version that Reveal requires.

Tanium recommended installation

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

Import specific solutions

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

Required dependencies

Reveal has the following required dependencies:

- Tanium™ Client Index Extension*
- Tanium™ Direct Connect
- Tanium™ Endpoint Configuration
- Tanium™ Interact
- Tanium™ Data Service (TDS)
- Tanium Trends
- Tanium™ RDB Service

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

Client extensions and endpoint tools

Tanium Endpoint Configuration installs Client Extensions and other tools for Reveal on endpoints. Client extensions perform tasks that are common to certain Tanium solutions. Each Client Extension and tool might have recommended security exclusions to allow them to run without interference. For more information, see Security exclusions. For a list of Reveal tools, see Reference: Reveal endpoint tools on page 68. For a list of all Client Extensions and tools, see Tanium Client Management User Guide: Reference: Client extensions used for Tanium solutions.

© 2026 Tanium Inc. All Rights Reserved

Tanium Module Server

Reveal is installed and runs as a service on the Tanium Module Server. The impact on the Module Server is minimal and depends on usage.

Endpoints

Supported operating systems

Operating system	Version	Notes
Microsoft Windows Server	• Windows Server 2008 R2 SP1 or later	Windows Server 2008 R2 SP1 requires Microsoft KB2758857.
Microsoft Windows Workstation	• Windows 11 • Windows 10 • Windows 8 • Windows 7 SP 1	Windows 7 Service Pack 1 requires Microsoft KB2758857.
macOS	Same as Tanium Client support	Review Tanium™ Client Management for Tanium Client OS support. For more information, see Tanium Client Management User Guide: Client version and operating system requirements

© 2026 Tanium Inc. All Rights Reserved

Operating system	Version	Notes
Linux	• Amazon Linux 2 LTS (2017.12) • Debian 9.x, 8.x, 10x • Oracle Linux 8.x, 7.x, 6.x, 5.x • Red Hat Enterprise Linux (RHEL) 8.x, 7.x, 6.x, 5.x • CentOS 7.x, 6.x, 5.x • AlmaLinux 8.5 • Rocky Linux 8.5 • SUSE Linux Enterprise Server (SLES) 15 • openSUSE 15.x • SUSE Linux Enterprise Server (SLES) 12 • openSUSE 12.x • SUSE Linux Enterprise Server (SLES) 11.3, 11.4 • openSUSE 11.3, 11.4 • Ubuntu 20.04 LTS • Ubuntu 18.04 LTS • Ubuntu 16.04 LTS	

Disk space requirements

The amount of space that Reveal uses varies depending on how much space is used on the local disks that are being indexed. The actual space that is required for the Index database is proportional to the number of files and directories on the local disks and what hashes are configured. Quick search uses additional endpoint disk and CPU resources on endpoints.

Host and network security requirements

Specific ports and processes are needed to run Reveal.

Ports

The following ports are required for Reveal communication.

© 2026 Tanium Inc. All Rights Reserved

Ports for Reveal communication

Source	Destination	Port	Protocol	Purpose
Tanium Client (internal)	Module Server	17475	TCP	Used by the Module Server for endpoint connections to internal clients.
Tanium Client (external)	Zone Server*	17486	TCP	Used by the Zone Server for endpoint connections to external clients. The default port number is 17486. If needed, you can specify a different port number when you configure the Zone Proxy.
Module Server	Module Server (loopback)	17470	TCP	Internal purposes, not externally accessible
Module Server	Zone Server*	17487	TCP	Used by the Zone Server for Module Server connections. The default port number is 17487. If needed, you can specify a different port number when you configure the Zone Proxy.
		17488	TCP	Allows communication between the Zone Server and the Module Server. On TanOS, the Direct Connect Zone Proxy installer automatically opens port 17488 on the Zone Server. This port must be manually opened on Windows.

*These ports are required only when you use a Zone Server.

BEST PRACTICE

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

Security exclusions

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

NOTE

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

© 2026 Tanium Inc. All Rights Reserved

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

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	*<Module Server>*\services\reveal-service\node.exe
		Process	*<Module Server>*\services\endpoint-configuration-service\TaniumEndpointConfigService.exe

Reveal security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Process	*<Tanium Client>*\TaniumCX.exe
		File	*<Tanium Client>*\TaniumClientExtensions.dll
		File	*<Tanium Client>*\TaniumClientExtensions.dll.sig
		File	*<Tanium Client>*\extensions\TaniumDEC.dll
		File	*<Tanium Client>*\extensions\TaniumDEC.dll.sig
		File	*<Tanium Client>*\extensions\TaniumIndex.dll
		File	*<Tanium Client>*\extensions\TaniumIndex.dll.sig
		File	*<Tanium Client>*\extensions\index\index.db
		File	*<Tanium Client>*\extensions\index\index.db-shm
		File	*<Tanium Client>*\extensions\index\index.db-wal

© 2026 Tanium Inc. All Rights Reserved

Reveal security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
Linux		Process	*<Tanium Client>*/TaniumCX
		File	*<Tanium Client>*/libTaniumClientExtensions.so
		File	*<Tanium Client>*/libTaniumClientExtensions.so.sig
		File	*<Tanium Client>*/extensions/libTaniumDEC.so
		File	*<Tanium Client>*/extensions/libTaniumDEC.so.sig
		File	*<Tanium Client>*/extensions/libTaniumIndex.so
		File	*<Tanium Client>*/extensions/libTaniumIndex.so.sig
		File	*<Tanium Client>*/extensions/index/index.db
		File	*<Tanium Client>*/extensions/index/index.db-shm
		File	*<Tanium Client>*/extensions/index/index.db-wal
macOS		Process	*<Tanium Client>*/TaniumCX
		File	*<Tanium Client>*/libTaniumClientExtensions.dylib
		File	*<Tanium Client>*/libTaniumClientExtensions.dylib.sig
		File	*<Tanium Client>*/extensions/libTaniumDEC.dylib
		File	*<Tanium Client>*/extensions/libTaniumDEC.dylib.sig
		File	*<Tanium Client>*/extensions/libTaniumIndex.dylib
		File	*<Tanium Client>*/extensions/libTaniumIndex.dylib.sig
		File	*<Tanium Client>*/extensions/index/index.db
		File	*<Tanium Client>*/extensions/index/index.db-shm
		File	*<Tanium Client>*/extensions/index/index.db-wal

User role requirements

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

- Reveal solution permissions on page 24
- Reveal requirements on page 17: The solution permissions automatically provide some of these permissions.

To review a summary of the predefined roles, see Set up Reveal users on page 32.

© 2026 Tanium Inc. All Rights Reserved

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

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



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

Reveal solution permissions

Permission	Reveal Administrator[1,2]	Reveal Operator[1]	Reveal Read Only User[1]	Reveal User[1]	Reveal Endpoint Configuration Approver[1]
Reveal Provides access to the Reveal workbench and enables viewing of snippets of affected files.	✓ SNIPPETS SHOW	✓ SNIPPETS SHOW	✓ SNIPPETS SHOW	✓ SNIPPETS SHOW	✗
Reveal Admin Perform administrative functions for the Reveal module	✓ ADMINISTRATOR	✗	✗	✗	✗
Reveal Affected Enables viewing of affected files	✓ FILES	✓ FILES	✓ FILES	✓ FILES	✗
Reveal API Perform Reveal operations using the API	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✗

© 2026 Tanium Inc. All Rights Reserved

Reveal solution permissions (continued)

Permission	Reveal Administrator[1,2]	Reveal Operator[1]	Reveal Read Only User[1]	Reveal User[1]	Reveal Endpoint Configuration Approver[1]
Reveal Endpoint Configuration Enables approver privileges in Tanium Endpoint Configuration for Reveal configuration changes.	✗	✗	✗	✗	✓ APPROVE
Reveal Operator Settings Enables viewing, listing, and editing Reveal settings	✓ READ WRITE	✓ READ WRITE	✗	✓ READ	✗
Reveal Patterns Enables viewing and editing patterns	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ WRITE	✗
Reveal Profiles Enables viewing, editing, and deploying profiles	✓ READ WRITE DEPLOY	✓ READ WRITE DEPLOY	✓ READ	✓ READ WRITE DEPLOY	✗
Reveal Quick Enables viewing of quick search results	✓ SEARCH	✓ SEARCH	✓ SEARCH	✓ SEARCH	✗
Reveal Rules Enables the viewing, listing, editing, and deploying of rules	✓ DEPLOY READ WRITE	✓ DEPLOY READ WRITE	✓ READ	✓ DEPLOY READ WRITE	✗
Reveal Rules Deploy Access to the Reveal workbench	✓ STATUS	✓ STATUS	✓ STATUS	✓ STATUS	✗

© 2026 Tanium Inc. All Rights Reserved

Reveal solution permissions (continued)

Permission	Reveal Administrator[1,2]	Reveal Operator[1]	Reveal Read Only User[1]	Reveal User[1]	Reveal Endpoint Configuration Approver[1]
Reveal Rulesets Enables the viewing, listing, and editing of rule sets	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ WRITE	✗
Reveal Settings Enables viewing, editing, and listing Reveal settings	✓ READ WRITE	✓ READ	✗	✓ READ	✗
Reveal Validations Enables viewing, editing, listing, and deploying validations	✓ DEPLOY READ WRITE	✓ DEPLOY READ WRITE	✓ READ	✓ DEPLOY READ WRITE	✗
Reveal Validations Deploy Enables viewing of the status of validation deployments	✓ STATUS	✓ STATUS	✓ STATUS	✓ STATUS	✗

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

[2] You must be assigned the Reveal Administrator role to create and download a support package.

Reveal administration and platform content permissions

Permission	Permission Type	Reveal Administrator[1]	Reveal Operator[1]	Reveal Endpoint Configuration Approver[1]	Reveal User[1]	Reveal Read Only User[1]
Action	Platform Content	✓ READ WRITE	✓ READ WRITE	✗	✓ READ WRITE	✓ READ WRITE
Action Group	Administration	✓ READ	✓ READ	✗	✓ READ	✓ READ
Filter Group	Platform Content	✓ READ	✓ READ	✗	✓ READ	✓ READ

© 2026 Tanium Inc. All Rights Reserved

Reveal administration and platform content permissions (continued)

Permission	Permission Type	Reveal Administrator[1]	Reveal Operator[1]	Reveal Endpoint Configuration Approver[1]	Reveal User[1]	Reveal Read Only User[1]
Own Action	Platform Content	✓ READ	✓ READ	✗	✓ READ	✓ READ
Package	Platform Content	✓ READ WRITE	✓ READ WRITE	✗	✓ READ WRITE	✓ READ
Plugin	Platform Content	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE
Saved Question	Platform Content	✓ READ WRITE	✓ READ WRITE	✗	✓ READ WRITE	✓ READ WRITE
Sensor	Platform Content	✓ READ	✓ READ	✗	✓ READ	✓ READ
User	Administration	✓ READ	✗	✗	✗	✗
Question History	Administrator	✓ READ	✓ READ	✗	✓ READ	✓ READ

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

© 2026 Tanium Inc. All Rights Reserved

Installing Reveal

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

- **Automatic configuration with default settings**: Reveal is installed with any required dependencies and other selected products. After installation, the Tanium Server automatically configures the recommended default settings. This option is the best practice for most deployments. For more information, see Import Reveal with default settings on page 28.
- **Manual configuration with custom settings**: After installing Reveal, you must manually configure required settings. Select this option only if Reveal requires settings that differ from the recommended default settings. For more information, see Import Reveal with custom settings on page 29.

Before you begin

- Read the release notes.
- Review the Reveal requirements on page 17.
- If you are upgrading from a previous version, see Upgrade Reveal on page 29.
- Assign the correct roles to users for Reveal. Review the User role requirements on page 23.
    - To import the Reveal solution, you must be assigned the Administrator reserved role.
    - To configure the Reveal action group, you must be assigned the Administrator reserved role, Content Administrator reserved role, or a role that has the **Action Group write** permission.



For initial installations of Reveal, defining an action group is the event that initiates the distribution of tools to Tanium Client managed endpoints. When you configure an action group, Reveal begins to deploy tools to those endpoints, index file systems, and evaluate rules. When you upgrade Reveal, for example from version 1.14 to 1.15, and an endpoint has no rules or rule sets, Reveal tools are not upgraded and no new tools get deployed until you deploy rules to those endpoints.

Import Reveal with default settings

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

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

© 2026 Tanium Inc. All Rights Reserved

Tanium Reveal default setting

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

To import Reveal and configure default settings, see Tanium Console User Guide: Import all modules and services. After the import, verify that the correct version is installed: see Verify Reveal version on page 30.

Import Reveal with custom settings

To import Reveal without automatically configuring default settings, be sure to clear the **Apply All Tanium recommended configurations** checkbox while performing the steps in Tanium Console User Guide: Import or update specific solutions. After the import, verify that the correct version is installed. For more information, see Verify Reveal version on page 30.

To configure the Reveal action group, see Configure the Reveal action group on page 32.

Manage solution dependencies

Other Tanium solutions are required for Reveal to function (required dependencies) or for specific Reveal features to work (feature-specific dependencies). For more information, see Solution dependencies on page 18.

Upgrade Reveal



Before upgrading the Reveal version, download a troubleshooting package. The troubleshooting package contains a copy of the Reveal database and definitions that you can use in a disaster recovery scenario. For more information on downloading a troubleshooting package, see Collect logs on page 60.

For the steps to upgrade Reveal, see Tanium Console User Guide: Managing Tanium solutions. After the upgrade, verify that the correct version is installed. For more information, see Verify Reveal version on page 30.

If the Reveal version does not update, refresh your browser window.

Remove legacy Index dependencies from endpoints

If you have previously installed Tanium Index as a standalone application, or used the standalone application to upgrade Tanium Index, ensure that all legacy Index assets are uninstalled from endpoints before deploying the latest Reveal tools to endpoints. To ensure complete removal of legacy Index dependencies, deploy the **Index - Remove Legacy Dependent** package to endpoints where legacy versions of Tanium Index dependencies exist.

© 2026 Tanium Inc. All Rights Reserved

1. To target endpoints, issue a question in Interact. Ask the question `Get Tanium File Exists [Tools/EPI/dependents.txt] from all machines`. If the results for an endpoint display `Index` it indicates that the standalone Index content has been used in the past.
2. In the **Question Results** grid, select the rows for the endpoints that require the action, and click **Deploy Action**.
3. From the Deploy Action page, use the Deployment Package search box typeaheads to select packages. Select the **Index - Remove Legacy Dependent [Windows]** or **Index - Remove Legacy Dependent [Non-Windows]** package.
4. Configure a Deployment Schedule and Targeting Criteria. Click **Deploy Action**. For more information, see Deploying actions.

After you have performed these steps, if the results of the **Client Extensions - Status** sensor displays `recorder|has_subscription|index.fileevents` you can use the **Recorder - Clear Subscription [OS]** package to remove a single subscription from recorder.

Verify Reveal version

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

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

© 2026 Tanium Inc. All Rights Reserved

Configuring Reveal

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

Install and configure Tanium Endpoint Configuration

Manage solution configurations with Tanium Endpoint Configuration

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

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

IMPORTANT

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

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

NOTE

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

Optionally, you can use Endpoint Configuration to require approval of configuration changes. When configuration approvals are enabled, Endpoint Configuration does not deploy a configuration change to endpoints until a user with approval permission approves the change. For information about the roles and permissions that are required to approve configuration changes for Reveal, see User role requirements on page 23. For more information about how to enable and use configuration approvals in Endpoint Configuration, see Tanium Endpoint Configuration User Guide: Managing approvals.

© 2026 Tanium Inc. All Rights Reserved

IMPORTANT

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

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

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

- Deploying profiles
- Deleting profiles

Configure Reveal

Configure the Reveal action group

Importing the Reveal module automatically creates an action group to target specific Tanium Client managed endpoints to which the Reveal packages are deployed. If you did not use automatic configuration or you enabled restricted targeting when you imported Reveal, the action group targets **No Computers**. You can set the action group to **All Computers** or any computer groups that you have defined.

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

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

BEST PRACTICE

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

1. From the Main menu, go to **Administration > Actions > Action Groups**.
2. In the list of action groups, click **Tanium Reveal**.
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.

Set up Reveal users

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

For more information about specific permissions for each role, see User role requirements on page 23.

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

© 2026 Tanium Inc. All Rights Reserved

Reveal Administrator

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

- Administrative functions for Reveal, including viewing, editing, and listing Reveal settings
- Configure the service account user
- Perform Reveal operations using the API
- View snippets of affected files
- View affected files
- View, edit, and deploy profiles
- View and edit patterns
- Perform a quick search
- View, list, edit, and deploy rules
- View, list, and edit rule sets
- View, list, edit, and deploy validations
- View the status of validation deployments
- View the status of rules deployments

Reveal Operator

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

- View, edit, and list Reveal settings
- Perform Reveal operations using the API
- View snippets of affected files
- View affected files
- View, edit, and deploy profiles
- View and edit patterns
- Perform a quick search
- View, list, edit, and deploy rules
- View, list, and edit rule sets

© 2026 Tanium Inc. All Rights Reserved

- View, list, edit, and deploy validations
- View the status of validation deployments
- View the status of rules deployments

Reveal User

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

- Perform Reveal operations using the API
- View snippets of affected files
- View affected files
- View, edit, and deploy profiles
- View and edit patterns
- Perform a quick search
- View, list, edit, and deploy rules
- View, list, and edit rule sets
- View, list, edit, and deploy validations
- View the status of validation deployments
- View the status of rules deployments

Reveal Read Only User

Assign the **Reveal Read Only User** role to users who need visibility into Reveal configurations but do not need rights to update them.
This role can perform the following tasks:

- Perform Reveal operations using the API
- View rules and rule sets
- View profiles
- View patterns
- View the status of validation deployments
- View the status of rules deployments

© 2026 Tanium Inc. All Rights Reserved

Reveal Endpoint Configuration Approver

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

(Optional) Deploy scans

Reveal scans files that are indexed by Tanium Client Index Extension. The Index endpoint settings determine the frequency of the index scans. For more information, see Tanium Client Index Extension User Guide: Indexing file systems.

If you have an urgent need to scan endpoints or a specific directory on endpoints outside of the distributed scan time periods, you can deploy a package to force a scan.

1. On the Reveal **Overview** page, click Settings, and then go to the **Deploy Scans** tab.
2. Select an operating system in the **Scan Specific Path (Reveal)** section to deploy the `Index - Request Immediate One-Time Scan` to force Reveal to scan a specific path for the selected operating system, and then click **Deploy**.
   The Action Deployment page opens. Specify the required parameters and click **Deploy Action**. For more information, see Tanium Console User Guide: Deploying actions in Console and Interact.

   CAUTION

   CAUTION: This operation is resource intensive, especially if you specify NFS mounts or broad directories, such as `/mnt` or `/home`. Do not deploy this action unless you completely understand its scope, impact on individual endpoints, and impact on the environment given the number of targeted endpoints.
3. Select an operating system in the **Scan Full Disk (Index)** section to deploy the `Index - Force Start Scans` package to force start all Client Index Extension scans for the selected operating system, and then click **Deploy**.
   The Action Deployment page opens. Specify the required parameters and click **Deploy Action**. For more information, see Tanium Console User Guide: Deploying actions in Console and Interact.

(Optional) Configure Reveal service settings

Configure settings to tune the Reveal service for your environment.

NOTE

Use profiles to configure Tanium Index subscription and Reveal settings for endpoints. For more information, see Creating profiles on page 37.

© 2026 Tanium Inc. All Rights Reserved

1. On the Reveal **Overview** page, click Settings and then click **Settings**.
2. Update the settings as needed:

Reveal settings

Setting	Default value	Description
Log Level	info	The log level for Reveal.
Enable Sensitive Data Logging	false	Include search details and file paths in audit logs.
Enable Rule Sets and Tools Automatic Deployment	selected	Select to automatically deploy rule sets and upgrade Reveal tools to the latest available versions when Reveal is installed or upgraded.
Rule Publication Interval	12 hours	The time interval to automatically deploy rule and rule sets assignments to endpoints.
Rule Publication On Modify	30 minutes	The time to automatically deploy rule and rule sets assignments to endpoints after a rule or rule set has been modified.
Validation Publication Interval	30 minutes	The time interval to automatically deploy pending validations.
Content Feed Update Interval Hours	24 hours	The frequency to poll and automatically update the Reveal content feed. Set the value to 0 to manually upload content.
Live Connection Max Snippets	500 snippets	The maximum number of snippets retrieved from a file from an endpoint.
Live Connection Page Expiration	60 minutes	The security setting to expire URLs after the specified period.
Live Connection URL Scope	session	The security setting to share connection URLs across users, scope them to the user, or to the user's current session.

3. Click **Save**.

© 2026 Tanium Inc. All Rights Reserved

Creating profiles

Create a profile to specify the Reveal endpoint configuration settings for groups of Tanium Client managed endpoints. For example, some endpoint types might require a different Reveal database size. Endpoints that are not targeted by a custom profile receive the default profile, which sets all Reveal endpoint settings to the default values.



If you upgrade Reveal from a version earlier than 1.18 to version 1.18 or later, any settings that were configured on the **Endpoint Configuration** tab in the Reveal settings are carried forward to the default profile.

Profile status

The **Profiles** page includes a banner with a summary of the status for all profiles:

New

A user created and saved the profile but did not deploy it to targeted endpoints.

Updated

A user edited the profile but did not deploy the updated profile to targeted endpoints.

Pending Approval

A user deployed the profile in Reveal, but the profile requires approval in Endpoint Configuration to push out to or delete from targeted endpoints.

Deployed

A user deployed the profile in Reveal, and the profile deployed to targeted endpoints via Endpoint Configuration.

Deleted

A user deleted the profile in Reveal.

The **Status** column in the grid on the **Profiles** page shows the status for each profile.

Create a profile

Create a profile to specify configuration settings for endpoints in a computer group.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules > Reveal > Profiles**.
2. Create a profile based on the default settings or an existing profile:
    - To create a profile based on the default settings, click **Create Profile**.
    - To create a profile based on an existing profile, select the checkbox for the profile and click **Duplicate**.
3. In the **General Information** section, specify the **Profile Name** and optional **Profile Description**.
4. In the **Target** section, click **Select Computer Groups** and select one or more computer groups to configure with this profile.
5. In the **Tanium Index Subscription Settings** section, specify the **Tanium Index Scan Frequency** and **Tanium Index First Scan Distribute Over Time** settings. To exclude files from indexing in Reveal versions before 1.18, use the **Path Stem Exclusions** or **Path Filter Exclusions** settings (from the Reveal **Overview** page, click **Settings > Endpoint Configuration**). To exclude files from indexing in Reveal versions 1.18 and later, use the **File Name Exclusions** or **Path Exclusions** settings in a Reveal profile.

    NOTE

    - These settings apply only to the Reveal subscription to Tanium Client Index Extension (Index). Index settings for other modules that use Index are not affected. For more information, see Tanium Client Index Extension User Guide: Indexing file systems.
    - Changing these settings from the default values can cause performance impacts on endpoints. For more information, see Tanium Client Index Extension User Guide: Overview and Tanium Client Index Extension User Guide: Customize Index endpoint settings.
6. (Optional) Enable or disable **Quick Search** functionality (Default: disabled). Quick search uses additional endpoint disk and CPU resources on endpoints. For more information, see Troubleshooting Reveal: Configure client disk space use.
7. (Optional) Enable or disable **Quick Search High-Frequency Word Threshold** (Default: enabled). When enabled, high-frequency words - for example, articles - are not searched. By not searching for such strings, endpoint resources are reserved. Enter a value to identify the number of files in which a string occurs before it is considered a high-frequency word. For example, if more than this number of files contain a word, the word is not saved in the database for the file. This reduces database size and therefore disk use.
8. In the **Reveal Settings** section, specify the endpoint settings as needed.
9. Click **Create**.

The profile status is New until you deploy it. For information on deploying profiles to endpoints, see Deploy a profile on page 39.

Prioritize profiles

Prioritize profiles to determine which profile applies to endpoints targeted by more than one profile. Zero (0) is the highest priority.

NOTE

You must have more than one profile to assign priorities.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules > Reveal > Profiles**, and then click **Prioritize**.
2. Drag and drop profiles in the list to change the priority. The first profile in the list has the highest priority (0).
3. Click **Prioritize**.

Existing profiles that were previously deployed automatically redeploy as needed to reflect the new priorities. You must deploy new profiles that were not previously deployed. For information, see Deploy a profile on page 39.

Edit a profile

1. From the Main menu, go to **Modules > Reveal > Profiles**.
2. Click the profile name. Click Edit Profile .
3. Make the necessary changes. Click **Save**.

The profile status is Updated until you deploy it. For information, see Deploy a profile on page 39.

Deploy a profile

Deploy a profile to push the settings out to targeted endpoints. You can deploy all profiles or a single profile.

1. From the Main menu, go to **Modules > Reveal > Profiles**.
    - To deploy all profiles, click **Deploy All Profiles**.
    - To deploy a single profile, select the checkbox for that profile. Click **Deploy**.

If you enabled configuration approvals in Endpoint Configuration, you must approve the deployment in Endpoint Configuration. The profile status is Pending Approval  until a designated approver approves the deployment in Endpoint Configuration. For more information, see Endpoint Configuration User Guide: Managing approvals.

Delete a profile

When you delete a profile, endpoints targeted by the deleted profile receive the next highest priority profile that targets the endpoints. If an endpoint is not targeted by another custom profile, it receives the default profile.

1. From the Main menu, go to **Modules > Reveal > Profiles**.
2. Select the checkbox for the profile. Click **Delete**.

If you enabled configuration approvals in Endpoint Configuration, you must approve the deletion in Endpoint Configuration. The profile status is Pending Approval  until a designated approver approves the deletion in Endpoint Configuration. For more information, see Endpoint Configuration User Guide: Managing approvals.

© 2026 Tanium Inc. All Rights Reserved

Creating patterns

In Reveal, a pattern is an expression that matches entities that can otherwise be hidden in the context of other information. You can create patterns based on regular expressions (regex) or keywords.

For example, a pattern could match an entity such as a credit card number or email address. Assign a pattern to a rule to match entities in unstructured data such as a word processing document, text file, PDF document, or spreadsheet. Reveal provides patterns for several types of sensitive information, such as credit card numbers, social security numbers, and email addresses.

You can view the patterns that Reveal provides through Tanium Console. From the Main menu, go to **Modules > Reveal > Patterns**, and then set the **Author** filter to **Tanium**.

Update patterns created by Tanium

Patterns created by Tanium update automatically through a content feed that is checked once every 24 hours by default. If a deployed rule uses an updated pattern, the update automatically deploys to Tanium Client managed endpoints, based on the time configured in the **Rule Publication On Modify** setting. To immediately deploy updated rules, from the Main menu, go to **Modules > Reveal > Rules**, click **Deploy All Rule Sets**, enter your credentials, and click **OK**. For more information, see Deploy rules on page 47.

- To adjust the automatic update schedule, go to the Reveal **Overview** page and click Settings. On the **Settings** tab, update the **Content Feed Update Interval Hours** setting.
- To manually check for updates, click Refresh in the **Last Modified by Tanium** section of the **Patterns** page.

Update patterns in an air-gapped environment

If you want to manually update content or your Tanium Server is in an air-gapped environment, you can upload the content archive from the Reveal settings.

1. Download the latest content archive from a computer that can access the internet: https://content.tanium.com/files/published/reveal/reveal-content/stable/reveal2-content-stable.zip
2. Transfer the file to a computer in the air-gapped environment.
3. Go to the Reveal **Overview** page and click Settings.
4. On the **Settings** tab, clear the value in the **Content Feed Update Interval Hours**. Click **Save**. An **Upload Content** tab appears
5. Click the **Upload Content** tab. Drag and drop the content archive to the tab to upload it.

Regex pattern considerations

Consider the following items before creating a regex pattern.

© 2026 Tanium Inc. All Rights Reserved

- Use the RE2 syntax and style. For more information, see https://github.com/google/re2/wiki/Syntax
- Define the goal for your pattern:
    - Who is the intended user for this pattern?
    - What data does that user need to discover?
    - Why does that user need to discover that data?
- Research and understand the format of the data that you want to match. For example, you might want to look for a particular ID that has 4-10 alphanumeric characters that are not case sensitive.
- Define example matches, both expected matches and some examples that are close, but that you do not want to match.
- Develop, test, and validate your regex using a regex editor, such as https://regex101.com.
- Optimize your regex:
    - Minimize the use of open-ended terms (such as `*`) and lookaheads.
    - Use a regex editor that displays the number of steps the engine took to match your test data. Try to minimize the number of steps required for a match.
    - Avoid using ^ or $ anchors in regex patterns.
    - To add a comment, use the pound sign (#). To use # as a literal character, escape it with a backslash (\), for example, `\#`.

Create a regex pattern

Create a regex pattern to specify a pattern for the data that you want to find in files. You can use the pattern in a rule to search for that data.

Before creating the pattern, review Regex pattern considerations on page 40.

1. From the Main menu, go to **Modules > Reveal > Patterns**, click **Create Pattern**, and then select **Regex Pattern**.
2. Specify a name for the pattern using only letters, numbers, spaces, dashes and underscores.
3. Provide a description for the pattern.
4. Specify a regular expression (RE2 syntax) to define the pattern for the data that you want to find in files.
5. (Optional) If you used an online regular expression debugger, such as https://regex101.com, to build your expression, provide the shared URL in the **Regex Test URL** field for quick reference.

   Test and validate regular expressions in a regular expression debugger before you use them in a pattern. Test all patterns in a lab environment before using them in a production environment.
6. Click **Create**.

© 2026 Tanium Inc. All Rights Reserved

Create a keyword list

Create a keyword list to specify keywords for the data that you want to find in files. This keyword list is included as a pattern that you can use in a rule to search for that data.

1. From the Main menu, go to **Modules > Reveal > Patterns**, click **Create Pattern**, and then select **Keyword Pattern**.
2. Enter a name for the pattern.
3. (Optional) Provide a description for the pattern.
4. Specify the keywords for the data that you want to find in files, using one of the following methods:
   a. Add keywords to the **Keyword List**. Enter one keyword per line, with a maximum of 500 keywords.
   b. Upload keywords from a CSV file. Click **Browse** and import a single-column CSV file.

   > NOTE
   > This option replaces any existing keywords in your keyword list for this pattern.

5. Click **Create**.

Edit a pattern

1. From the Main menu, go to **Modules > Reveal > Patterns**.
2. Click View Details next to the pattern name for the pattern that you want to edit.

   > NOTE
   > You cannot edit patterns created by Tanium.

3. Click Edit Pattern.
4. Make the necessary changes and click **Save**.

Delete a pattern

You can delete only patterns that are not Reserved patterns or used in a rule.

1. From the Main menu, go to **Modules > Reveal > Patterns**.
2. Click View Details next to the pattern name for the pattern that you want to delete.

   > NOTE
   > You cannot delete patterns created by Tanium.

3. Click Delete Pattern.

© 2026 Tanium Inc. All Rights Reserved

Creating rules

A rule is a combination of conditions that you define and an action to perform when the conditions are met. Rules are evaluated every hour on all files that have been hashed by Tanium™ Index. When all of the conditions of a rule are matched, an action is triggered. For example, you can categorize files that contain matches to social security number patterns as confidential. You can apply multiple rules to target the same files so you can discover many types of sensitive information in the same file set.

Reveal provides default rules that feature commonly used configurations as examples. While you cannot edit default rules, you can duplicate them and create a version that you can customize.

NOTE

Depending on the role and permissions you have been assigned, you can view rules or create and edit rules. For more information, see User role requirements on page 23. For example, if you have write permissions for rules, you can edit the content of rules. Conversely, if you do not have write permissions for rules, you can view the rule information but not make edits and save changes. Regardless of permissions, you cannot edit or save rules that are designated as Tanium Managed.

TIP

You can view the rules that Reveal provides through Tanium Console. From the Main menu, go to **Modules > Reveal > Rules**. Tanium-provided rules appear with the Tanium logo .

Criteria for rule evaluation

For rules to evaluate on a file, the file must match the following criteria:

- The file must be hashed by Tanium Index using hash type MIME.
- The file must be in a format that Tanium Reveal can read. For more information, see Reference: Supported file types for rule evaluation on page 66.
- Binary files must be less than 32 MB. To increase the default size limit, edit the setting `CX.index.ExtractorMaxSourceMB`.
- The file must not be filtered by the **Reveal Parse Exclusions by Regular Expression** or **Reveal Parse Exclusions by File Path** settings, which you can configure using a profile. For more information, see Creating profiles on page 37.

Zip file considerations

The contents of Zip archives are extracted into memory and Reveal evaluates rules against such contents if the compressed zip file size is within the specified overall maximum configured file size. By default this setting is 32 MB, and you can customize this default value using the `CX.index.MaxZipSizeMB` setting. If the uncompressed size is larger than the `MaxZipSizeMB` setting size, the archive is not extracted into memory and indexed.

For example, if you use the default setting value (32MB):

© 2026 Tanium Inc. All Rights Reserved

- A zip file that is 1MB (compressed) and 20MB (uncompressed) would have its contents indexed.
- A zip file that is 5MB (compressed) and 40MB (uncompressed) would not have its contents indexed.

A zip archive is determined by magic number 504b0304. Many file types are actually zip archives with a magic number of 504b0304. For example: ZIP, JAR, WAR, EAR, XLSX, PPTX, XLSX. Use the CX.index.ZipRecursionLimit (default 10) setting to configure the recursion limit for how deep to extract and index within zip files. For more information, see Tanium Client Index Extension User Guide: Indexing file systems.

Rule conditions

Rule conditions are criteria that determine if a file matches the rule. The following are the types of conditions that you can apply to a rule:

Filter

Use filters to limit the rule to files that match. Filters include file type, file location, file modification date, and file size. If you do not specify any filters, the rule applies to all eligible files on the Tanium Client managed endpoints from the computer groups specified in the rule set.

Pattern

Use patterns to find sensitive data in files that match the filters. Patterns include credit cards, social security numbers, email addresses, passwords, and phone numbers.

Pattern proximity group

Use pattern proximity groups to find combinations of patterns that are in close proximity to each other within a file.



Multiple patterns and patterns in a pattern proximity group are joined with an AND operator.

Create a rule

Create a rule to define conditions and an action to perform when the conditions are met.

1. From the Main menu, go to **Modules > Reveal > Rules**, and then click **Create Rule**.
2. Enter a name and description for the rule.
3. Select one or more rule sets to contain the rule. Click **Add Rule Sets** and select the rule sets you want to associate with the rule. Click **Assign**.
4. [Optional] Add filters to limit the files to target. Under **Rule Filters**, click **Add Filter** and select the criteria that you want the rule to cover. Repeat to add another filter. For more information, see Reference: Supported file types for rule evaluation on page 66.

© 2026 Tanium Inc. All Rights Reserved

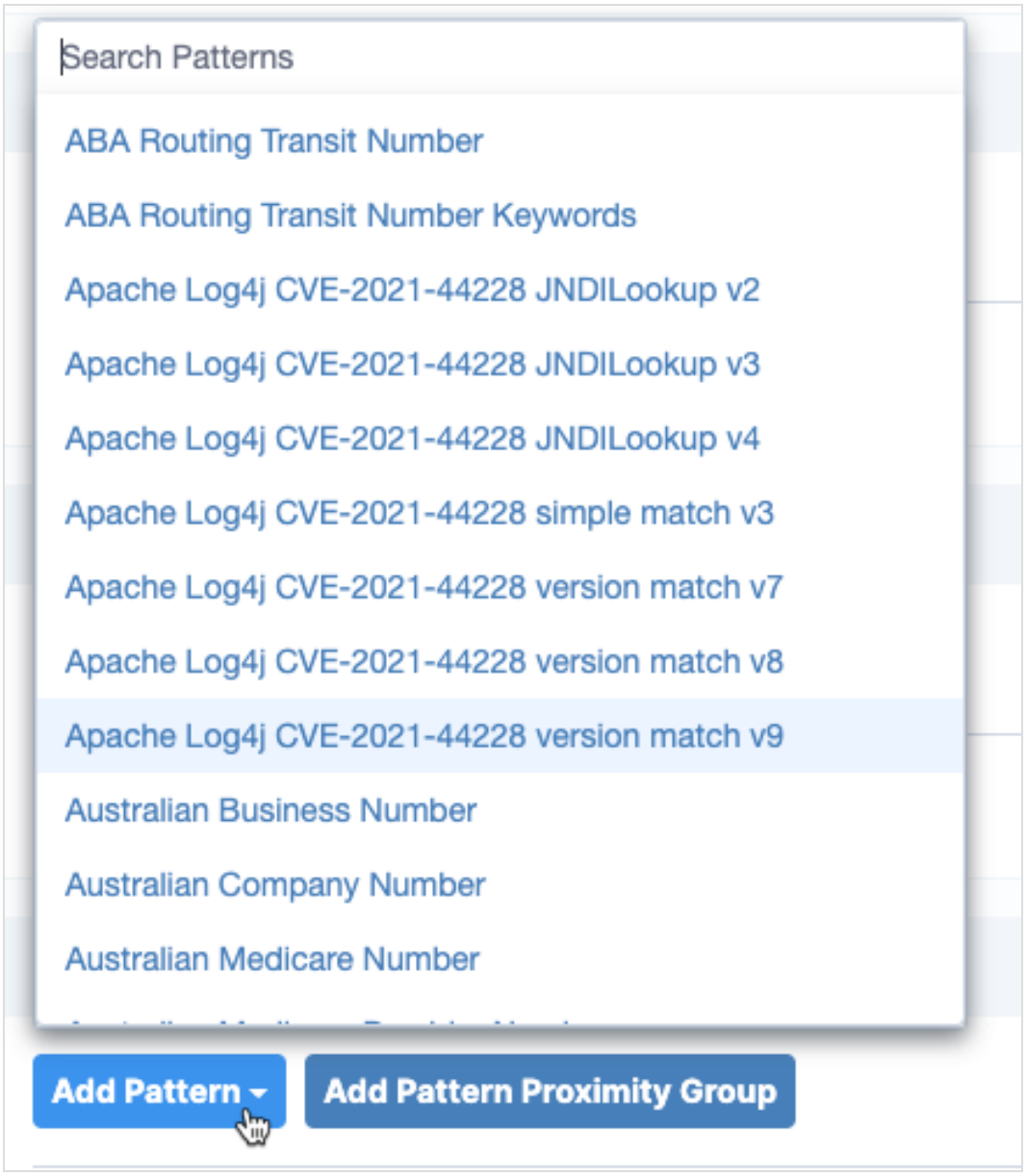
5. Under **Rule Patterns**, add one or more rule patterns. Rules must contain at least one condition.

    - To match a pattern, click **Add Pattern** and select the pattern to match. Enter the minimum number of matches to the pattern that must occur for the rule to match. Repeat to add another pattern.
    - To add a proximal pattern match, click **Add Pattern Proximity Group**. A rule can contain one pattern proximity group.

        a. For **Proximity**, select the maximum number of characters that the patterns can be from each other.

        b. In the pattern proximity group, click **Add Pattern** and select a pattern to include in the match. Repeat to add a second pattern. A pattern proximity group must contain at least two patterns. Patterns are joined with an AND operator.
        Rule Patterns options

© 2026 Tanium Inc. All Rights Reserved



Each instance that matches the pattern proximity group results in a rule match. For example, you can create a pattern proximity group that searches for email addresses and password text that appear within 100 characters of each other. If there are four email addresses that appear within 100 characters of the word "password", Reveal creates a rule match that includes all the matching search criteria.

6. Under **Rule Actions**, click **Add** to select the action to perform when all the conditions match. To add a category to files that match the conditions of the rule, select **Tag the affected files**, and select one or more categories.
7. Click **Save**.

© 2026 Tanium Inc. All Rights Reserved

Deploy rules

Reveal deploys rules to endpoints through a rules package. Rules packages also contain information that maps rules to rule sets and determines how endpoints in specific computer groups monitor for rules. Multiple rule sets can apply to an endpoint; and all rules in all of the applicable rule sets are evaluated.

Rules are automatically included in the next scheduled deployment when you update existing rules or create new rules. To immediately deploy updated rules, go to the **Rules** page, click **Deploy All Rule Sets**, enter your credentials, and click **OK**.



Test and verify rules before deploying to endpoints.



You can also deploy rules from the **Rule Sets** page.

© 2026 Tanium Inc. All Rights Reserved

Creating rule sets

Rule sets group rules together and assign them to specific groups of Tanium Client managed endpoints. You can group rules into rule sets that address specific categories of sensitive information, or that monitor specific types of files.

For example, you might want to apply and monitor for specific rules on one group of endpoints, but not other groups. Or, you might want to apply a subset of the available rules to a group of endpoints.

You can view the number of rules that are assigned to each rule set, the computer groups that it targets, and whether there are any pending changes to any of the associated rules.

A rule set has no effect unless it contains at least one rule. The default rule sets contain at least one rule. The default rules cannot be edited, but you can delete them, or make a duplicate of a rule and customize it for your specific needs.



Test and verify rules before adding to rule sets.



Depending on the role and permissions you have been assigned, you can view rule sets or create and edit rule sets. For more information, see User role requirements on page 23. For example, if you have write permissions for rule sets, you can edit the content of rule sets. Conversely, if you do not have write permissions for rule sets, you can view the rule set information but not make edits and save changes.

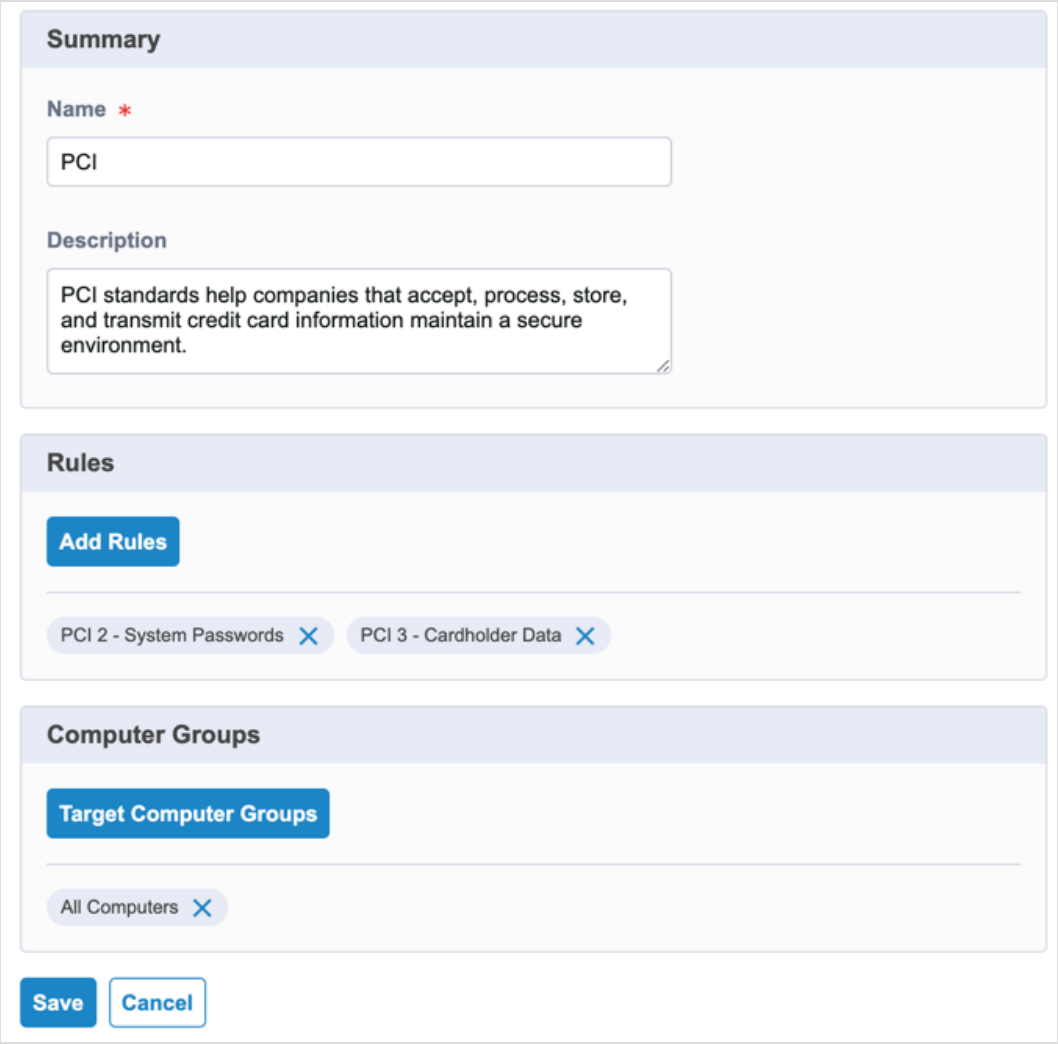
Create a rule set

Create a rule set to identify one or more rules to assign to endpoints in the computer group.

1. From the Main menu, go to **Modules > Reveal > Rule Sets**, and then click **New Rule Set**.

© 2026 Tanium Inc. All Rights Reserved

2. Enter a name and description for the rule set.
Rule Sets options



3. Select one or more rules to associate with the rule set. Click **Add Rules** and select the rules you want to associate with the rule set. Click **Assign**.
4. Under **Computer Groups**, click **Target Computer Groups** to add computer groups that you want the rule set to target. The rules that are associated with the rule set are applied to the endpoints in the computer groups you specify. Click **Assign**.
5. Click **Save**.

Add rules to an existing rule set

You can add additional rules to an existing rule set. For example, you might add a new rule with a new pattern to an existing rule set.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules > Reveal > Rule Sets**.
2. Click the title of the rule set to which you want to add one or more rules.
3. Click **Edit Rule Set**.
4. Click **Add Rules** and select the rules you want to associate with the rule set. Click **Assign**.
5. Under **Computer Groups**, click **Target Computer Groups** to add computer groups that you want the rule set to target. The rules that are associated with the rule set are applied to the endpoints in the computer groups you specify. Click **Assign**.
6. Click **Save**.

Delete a rule set

Delete a rule set that you no longer need. Deleting a rule set does not remove any historical matches from any metrics.

1. From the Main menu, go to **Modules > Reveal > Rule Sets**.
2. Select the checkbox next to the rule set that you want to delete.
3. Click **Actions > Delete**. Enter your credentials to confirm that you want to delete the rule set.

© 2026 Tanium Inc. All Rights Reserved

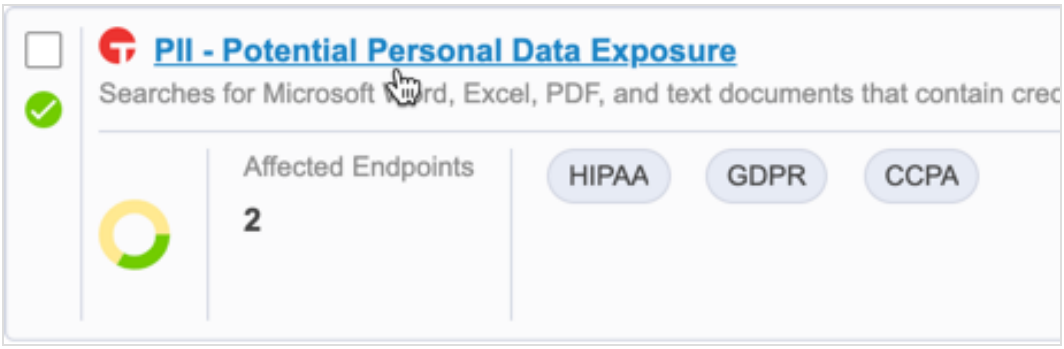
Investigating rule matches

When Reveal finds a match to a rule, the **Rules** and **Rule Sets** pages update to show a breakdown of all endpoints affected by the rule according to how many matches occur on that Tanium Client managed endpoint. You can further investigate the details of the match. Each rule contains information about the number of endpoints on which matches have been detected. You can create a live connection to the endpoint and drill down to perform further analysis. You can investigate the number of matches across the endpoints over time.

Investigate by endpoint

Investigate the affected endpoints and files where matches are detected when a rule match occurs.

1. From the Main menu, go to **Modules > Reveal > Validations**.
2. Click a rule that has matches that you want to investigate.



3. Under **Results**, Reveal shows the endpoints where matches have occurred.



4. Select up to five endpoints and click **Connect**. A live connection is opened to the selected endpoints. When an endpoint connection state shows as **Active**, click the endpoint name to view files that contain matches.
5. For files where matches have occurred, the file name, number of hits, and path appear.
6. Click an affected file to view snippets that show pattern matches in context.

© 2026 Tanium Inc. All Rights Reserved

When validations have been validated or invalidated, values in the **No validation hits** and **Valid hits** columns on the **Affected Files - <Computer Name>** page for any rule where patterns have been matched and validated appear in orange. Orange indicates that the data is "stale"; meaning that new validation data exists. If a file is designated as stale, it is prioritized for rescanning. When no new validation data exists, the values appear in black.

For more information, see Validating pattern matches on page 53.

© 2026 Tanium Inc. All Rights Reserved

Validating pattern matches

Validate rules to ensure that pattern matches are accurate and consistent in the targeted data. By validating rules, you can focus any analysis of data on results that have been confirmed or rejected as relevant pattern matches.

Overview

Validations apply to pattern matches in the context of a rule where the text selected for the validation is in specific proximity to the matched pattern. A successful validation is comprised of three parts:

- The selected (highlighted) validation characters
- The number of characters, including spaces, between the validation selection and the start of the pattern match
- The pattern match itself

New validations display in a pending state and are only visible to the user who created them. Pending validations automatically apply to snippet results, but do not affect rule hit counts until they are published.



For more information about pattern proximity groups, see Creating rules on page 43.

Validations always take precedence over invalidations. This is to reduce the number of false positives that are returned for rule matches. Additionally, the most recent validations take precedence over older validations.

Tanium Reveal does not move, copy, touch, or store text file data. The data Reveal uses is tokenized; it can never be read without the private key to decode it. When you connect to an endpoint to investigate findings, you view one or more snippets. If you see a snippet when connected to an endpoint, the file is physically present on the endpoint. If you click a file and nothing is displayed, the file has been moved or removed between the time Tanium Reveal found it and when you clicked the file.

Create a validation

Create a validation to improve the accuracy of rule performance and to reduce the number of false positive results on the data that a rule targets.

1. From the Main menu, go to **Modules > Reveal > Rules**.
2. Click the rule name for a specific rule to view a list of results and associated Tanium Client managed endpoints.
3. Select the checkbox next to an endpoint that has one or more files that match patterns. Click **Connect**.
4. After the connection establishes, click the computer name.
5. Click the **Filename** for the file that contains one or more pattern matches.

© 2026 Tanium Inc. All Rights Reserved

6. Review the snippets that show where a pattern matches. Valid and No Validation snippets appear by default. The text in the file that matches the pattern is highlighted. To limit which results appear, click **Filter Results** to view or hide no validation, valid, invalid, and excluded snippets.

   > NOTE
   >
   > Excluded snippets are snippets with no validation that do not match patterns exactly. This includes matches to pattern proximity groups outside the proximity range. You can confirm or reject an excluded snippet.

7. For each snippet, select the highlighted text that matches either a confirmation or rejection, and then click **Validate** or **Invalidate**. Rejected snippets are filtered from future results.

   Validations are tracked relative to the beginning of the match. Unicode and ASCII control characters - with the exception of tab, carriage return (CR) and line feed (LF) - are not supported in validation text. This includes Unicode characters U+0000 through U+0008, U+000B through U+000C, U+000E, and U+000F. If you select validation text that contains unsupported control characters, an error appears in the **Create Validation** page.

   Validations for snippets are applied to the entire document by default unless the document is in table format. If a document is in table format, the validation applies to the individual cell, column, or row that is actively selected when you create the validation.

   > TIP
   >
   > Keyboard shortcuts include (v) for Validate and (i) for Invalidate. If you do not want to add a name and description for the validation, press (vv) for Validate and Save, or (ii) for Invalidate and Save; these two shortcuts skip the next two steps.

8. Provide a name and description for the validation. A preview of the text you have validated appears and reports the number of pattern matches that the validation affects in the current file, the rule that the validation affects, and whether matching patterns should be validated or invalidated.

9. Click **Save**. Snippets that contain validations are displayed as pending; meaning that validations have been authored recently and have not been distributed to endpoints. Validations deploy to endpoints within 30 minutes of authoring.

When you have completed validating pattern matches in a file, click **Next File** at the top of the page to create validations in the next file on the endpoint where patterns have been matched.

When validations have been validated or invalidated, values in the **No validation hits** and **Valid hits** columns on the **Affected Files - <*Computer Name*>** page for any rule where patterns have been matched and validated appear in orange. Orange indicates that the data is "stale"; meaning that new validation data exists. If a file is designated as stale, it is prioritized for rescanning. When no new validation data exists, the values appear in black.

Deploy validations

Published validations apply to all hits of the corresponding rule. By default, Reveal checks at a regular interval for changes to rules and reprocesses files that have existing rule matches. Validation changes only cause files that match a rule to be reprocessed. Validations are automatically deployed every 30 minutes as long as there are changes that have not been deployed.

You can manually deploy validations.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules > Reveal > Validations**.
2. Click **Deploy Validations**.

Audit published validations

Audit validations to view snippets where pattern matches affected by a validation apply.

1. From the Main menu, go to **Modules > Reveal > Validations**.
2. Click a published validation to view endpoints that contain pattern matches to which the validation has been applied.
3. Select the checkbox next to an endpoint that has one or more files that match patterns. Click **Connect**.
4. View files affected by the validation.
5. Click a file to view snippets that match the validation.

© 2026 Tanium Inc. All Rights Reserved

Searching across the enterprise

You can search for sensitive information that matches a search string in real-time and not wait for an alert from a rule match. Quick search targets all of the Tanium Client managed endpoints in the Reveal action group. Use a literal search string and parameters that you want the search to target. Reveal returns a list of results that match the search criteria you provide.

Reveal converts search strings to lowercase, removes punctuation, and removes common stop words, such as articles. Reveal then searches for the tokens across the environment. For example, if a search query is `process is started`, this is tokenized as `["process","started"]`.



When you create or edit a profile, you can enable or disable quick search in the **Tanium Index Subscription Settings** section. By default, quick search is disabled. Be aware that quick search uses additional disk and CPU resources on endpoints. For information, see Creating profiles on page 37.

Perform a quick search

Use Reveal to search for specific items of sensitive information across an entire enterprise.

1. From the Main menu, go to **Modules > Reveal > Quick Search**.
2. In the search field, provide a literal search string or a token from a previous or saved search. For example, `123456789` to find an exact match. When you perform a quick search, the space character is a delimiter in addition to the `"=+!@#%^&*()_-` characters. The quick search matches on the group of characters before and after the delimiter. For example, if you search for `John@Doe`, the quick search returns any result that includes **john** and **doe**.
3. (Optional) Expand **Search Parameters** to add filters to limit the files that you want to target.
4. Click **Search**.

Recent quick searches are saved to enable you to perform the same search multiple times. However, the search terms used in the search are obfuscated and preserved as a token that corresponds to the original search terms. By obfuscating the original search terms, potentially sensitive data does not appear in the Reveal workbench.

Investigate quick search results

Quick search results appear as Reveal discovers matches to the search criteria. Select up to five endpoints and click **Connect**. A live connection is opened to the endpoints. When the endpoint connection state appears as **Active**, click the endpoint name to investigate the files where matches occur.

© 2026 Tanium Inc. All Rights Reserved

NOTE

Both the quick search query and the searchable data are encrypted with a one way hash. Hashing occurs before the query is distributed to endpoints, and unencrypted queries and results are not persisted. The query is retained in the browser during the search workflow only. When results snippets are requested, the file is read on demand on the endpoint, and results are returned directly to Reveal. Reveal does not write any unencrypted file content to disk, and no unencrypted query or result is ever sent as Tanium content.

© 2026 Tanium Inc. All Rights Reserved

Maintaining Reveal

Perform monthly maintenance tasks to ensure that Reveal successfully performs scheduled activities on all the targeted Tanium Client managed endpoints and does not overuse endpoint or network resources. If Reveal is not performing as expected, you might need to troubleshoot issues or change settings. For more information, see Troubleshooting Reveal on page 60.

Review and remediate Tanium Reveal issues

Review the health of Reveal tools on endpoints to remediate issues.

1. From the Main menu, go to **Modules > Reveal > Overview**.
2. Go to the **Health** dashboard to review:
    - **Reveal Coverage**: To investigate endpoints that do not have Reveal tools installed, click the number above **Needs Attention**. The Tanium Server issues a question that returns the computer name, operating system, IP address, and Reveal coverage (installation) status for the affected endpoints. For more information, see Troubleshooting Reveal on page 60.
    - **Endpoint Status**: To investigate endpoints that have issues related to Reveal operations, click **Attention Needed**. The Tanium Server issues a question that returns the computer name, operating system, IP address, and Reveal tools status for the affected endpoints. For more information, see Troubleshooting Reveal on page 60.

Monitor and troubleshoot Reveal coverage

The following table lists contributing factors into why the Reveal coverage metric might be lower than expected and corrective actions you can make.

Contributing factors of a low veal coverage metric

Contributing factor	Corrective action
Tools Not Deployed	Verify Tanium Clients are current and supported. For more information, see Core platform dependencies on page 17. Ensure the Reveal action group is set to `All Computers`. Ensure the Trends action group is set to `All Computers`. Ensure the intended Reveal targets are in the appropriate computer groups. Ensure the computer groups are included in the appropriate rule set in Reveal.
Index Health and Configuration	Ensure Index is properly configured and operating as expected on the endpoints. Ensure you are not excluding the files you want Reveal to scan from indexing or hashing. This could be by an ExcludeFrom(Hashing|Indexing) setting or if the file exceeds the setting of MaxFileSizeToHashMB, 32MB by default.

© 2026 Tanium Inc. All Rights Reserved

Monitor and troubleshoot endpoints with confirmed sensitive data

The following table lists contributing factors into why the endpoints with confirmed sensitive data metric might be higher than expected and corrective actions you can make.

Contributing factors of a high confirmed sensitive data metric

Contributing factor	Corrective action
See “Tools Not Deployed” and “Index Health and Configuration” above.	See the Corrective Actions for “Tools Not Deployed” and “Index Health and Configuration” in the preceding table.
Reveal rules not targeted as desired or required	To assign Reveal rules, they must be assigned to a rule set and the rule set must target the desired computer groups. First, review the specific rule and make sure it’s assigned to a rule set. Next, review the rule set and confirm it targets the appropriate computer group. Examine the computer group and ensure that it properly targets the desired computers.
Reveal findings are not yet confirmed	Reveal finds matches to rules, but the findings are only confirmed once an analyst confirms or rejects the findings. Click the results of the desired rule, then select and connect to an endpoint with findings. Select a file to see the snippets, then highlight an appropriate selection of text and click **Confirm** to create a validation - valid or invalid - of the rule. All similar snippets on all endpoints then show confirmed results. Invalid snippets no longer appear in the results.

Monitor and troubleshoot endpoints with unconfirmed sensitive data

The following table lists contributing factors into why the endpoints with unconfirmed sensitive data metric might be higher than expected and corrective actions you can make.

Contributing factors of a high unconfirmed sensitive data metric

Contributing factor	Corrective action
Reveal not fully deployed or operational	See the corrective actions detailed in the previous two tables to ensure Reveal tools and rules are properly targeted and deployed.
Reveal findings are not yet confirmed	Reveal finds matches to rules, but the findings are only confirmed once an analyst confirms or rejects the findings. Click the results of the desired rule, then select and connect to an endpoint with findings. Select a file to see the snippets, then highlight an appropriate selection of text and click **Confirm** to create a confirmed match of the rule. All similar snippets on all endpoints then show confirmed results.

© 2026 Tanium Inc. All Rights Reserved

Troubleshooting Reveal

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

Collect logs

The information is saved as a ZIP file that you can download with your browser. The zip file is also known as a support bundle. You must be assigned the Reveal Administrator role to create and download a support bundle.

1. From the Reveal **Overview** page, click Help, then the **Troubleshooting** tab.
2. Click **Create Package**. When the status shows that the package is complete, click **Download Package**.
3. A `tanium-reveal-support-[timestamp].zip` file downloads to the local download directory.
4. Attach the ZIP file to your Tanium Support case form or Contact Tanium Support on page 65.

Verify endpoint tools

If you are experiencing issues such as a feature not working on an endpoint or seeing incorrect data in the workbench, confirm that your endpoints have the latest toolset version. For more information, see Tanium Endpoint Configuration User Guide: Identify and resolve issues with endpoint tools or Client Extensions. For more information about Reveal tools, see Reference: Reveal endpoint tools on page 68.

Identify and resolve issues with Client Extensions

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

> TIP For more information about the Client Extensions that Reveal installs and uses, see Client Extensions.

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

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

© 2026 Tanium Inc. All Rights Reserved

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

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

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

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

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

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

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

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

© 2026 Tanium Inc. All Rights Reserved

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

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

5. Review the Extensions logs on the endpoint. Take note of entries that include `fail` or `error`. For more information, see Review the Extensions log for an endpoint on page 62.

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

Review the Extensions log for an endpoint

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

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

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

Configure client disk space use

You can use two configurable client settings for disk space use:

CX.core.DiskSpaceWarningPercent

CX.core.DiskSpaceCriticalPercent

© 2026 Tanium Inc. All Rights Reserved

Use these client settings to surface warnings about the amount of disk space left on the disk that the Tanium Client is installed on. By default, these settings are 5% and 1% respectively. CX-core checks the available disk space on the endpoint once every five minutes.

When the DiskSpaceCriticalPercent threshold is reached, IndexCX pauses indexing until the free disk space is increased above the critical threshold. Endpoints that have reached either the Warning or Critical thresholds will display a health check in the Client Extensions – Status sensor. Use the following question to list all endpoints with a disk space health check:

`Get Computer Name and Client Extensions - Status contains disk space from all machines with Client Extensions - Status contains disk space`

Modifying client disk space thresholds

The free disk space thresholds can be set via the command line or using a Tanium Action. For more information, see Tanium Client Management User Guide: Managing client settings and Index configurations.

Command line example:

Set the warning threshold to 10 percent and the critical threshold to 5 percent:

```
./TaniumClient config set CX.core.DiskSpaceWarningPercent 10
```

```
./TaniumClient config set CX.core.DiskSpaceCriticalPercent 5
```

Tanium action example

Windows	Non-Windows
Package: Modify Tanium Client Setting	Package: Modify Tanium Client Setting [Non-Windows]
RegType: REG_DWORD	Type: Numeric
ValueName: CX.core.DiskSpaceWarningPercent	ValueName: CX.core.DiskSpaceWarningPercent
ValueData: 10	ValueData: 10

You can check non-default disk space settings with the question:

`Get Tanium Client Explicit Setting[CX.core.DiskSpaceWarningPercent] and Tanium Client Explicit Setting[CX.core.DiskSpaceCriticalPercent] from all machines`

A result of “Key/Value not found” indicates that the setting is the default value (5% for Disk Space Warning and 1% for Disk Space Critical).

Remove Reveal tools from endpoints

You can deploy an action to remove Reveal 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 , drill down as necessary, and select the targets from which you want to remove Reveal tools. For more information, see Tanium Interact User Guide: Drill Down.
3. Click **Deploy Action**.
4. For the **Deployment Package**, select **Endpoint Configuration - Uninstall Tool [Windows]** or **Endpoint Configuration - Uninstall Tool [Non-Windows]**, depending on the endpoints you are targeting.
5. For **Tool Name**, select .
6. (Optional) By default, after the tools are removed they cannot be reinstalled. To allow tools to be automatically reinstalled, clear the selection for **Block reinstallation**. Re-installation occurs almost immediately.

   NOTE

   If reinstallation is blocked, you must unblock it manually:

   - To allow Reveal 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 Reveal 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 Reveal tools that are not dependencies for tools from other solutions, select **Remove unreferenced dependencies**.
9. (Optional) In the **Deployment Schedule** section, configure a schedule for the action.

   BEST PRACTICE

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

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

NOTE

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

© 2026 Tanium Inc. All Rights Reserved

Uninstall Reveal

You might need to remove Reveal from the Tanium Module Server for troubleshooting purposes.

1. From the Main menu, go to **Administration > Configuration > Solutions**. Under Reveal, click **Uninstall**. Click **Proceed with Uninstall** to complete the process.
2. Enter your password to start the uninstall process.
   A progress bar displays as the installation package is removed.
3. Click **Close**.
4. If the Reveal module has not updated in the console, refresh your browser.

Contact Tanium Support

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

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

© 2026 Tanium Inc. All Rights Reserved

Reference: Supported file types for rule evaluation

For rules to evaluate on a file, the file must match the following criteria:

- The file must be hashed by Tanium Index using hash type MIME.
- The file must be in a format that Tanium Reveal can read. For more information, see Reference: Supported file types for rule evaluation on page 66.
- Binary files must be less than 32 MB. To increase the default size limit, edit the setting `CX.index.ExtractorMaxSourceMB`.
- The file must not be filtered by the **Reveal Parse Exclusions by Regular Expression** or **Reveal Parse Exclusions by File Path** settings, which you can configure using a profile. For more information, see Creating profiles on page 37.

Zip file considerations

The contents of Zip archives are extracted into memory and Reveal evaluates rules against such contents if the compressed zip file size is within the specified overall maximum configured file size. By default this setting is 32 MB, and you can customize this default value using the `CX.index.MaxZipSizeMB` setting. If the uncompressed size is larger than the `MaxZipSizeMB` setting size, the archive is not extracted into memory and indexed.

For example, if you use the default setting value (32MB):

- A zip file that is 1MB (compressed) and 20MB (uncompressed) would have its contents indexed.
- A zip file that is 5MB (compressed) and 40MB (uncompressed) would not have its contents indexed.

A zip archive is determined by magic number 504b0304. Many file types are actually zip archives with a magic number of 504b0304. For example: ZIP, JAR, WAR, EAR, XLSX, PPTX, XLSX. Use the CX.index.ZipRecursionLimit (default 10) setting to configure the recursion limit for how deep to extract and index within zip files. For more information, see Tanium Client Index Extension User Guide: Indexing file systems.

File type filters for rules

When you create or edit a rule, you can add a filter to target file types in one or more categories. The following options are available:

File type options for rule filters

Category	Format	File types
Configuration	Text	CFG, CONF, INI, YAML
Microsoft Excel	Binary	ODS, XLAM, XLSM, XLSX, XLTM, XLTX
Microsoft PowerPoint	Binary	ODP, POTM, POTX, PPA, PPSM, PPSX, PPTM, PPTX

© 2026 Tanium Inc. All Rights Reserved

File type options for rule filters (continued)

Category	Format	File types
Microsoft Word	Binary	DOCM, DOCX, DOTM, DOTX, ODT
PDF	Binary	FDF, PDF
Structured text	Text	CSV, TSV, PSV, JSON, XML
Text	Text	TXT

Reveal can read files in any of the supported file types, regardless of the file extension. If you do not specify a file type filter for a rule, the rule attempts to read all files that are hashed by Tanium Client Index Extension. When you assign a file type to a rule, the rule only attempts to read files with the listed file extensions.

Supported MIME types

Reveal supports the following MIME types:

xml:

- text/xml
- text/html

text:

- text*

pdf:

- application/pdf

csv:

- .csv
- .tsv
- .psv

zip:

- A zip archive is determined by magic number 504b0304.

© 2026 Tanium Inc. All Rights Reserved

Reference: Reveal endpoint tools



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

Endpoint tools for Tanium Reveal

Tool	Description
core-cx	Provides a management framework API for all other Client Extensions and exposes operating system metrics
cx-config	Provides installation and configuration of extensions on an endpoint
extras-cx	Provides a helper library that contains re-usable functions for various client extensions to use
index-cx	Provides the ability to index the local file systems on an endpoint

Reveal deploys the Tanium Client Index Extension tools, if necessary, and starts the indexing process. Additionally, Reveal deploys a default Index configuration. Ensure that any file types or directories that you expect Reveal to scan are not excluded from hashing. By default, the following directories are excluded from hashing:

- `^/Library/Tanium/TaniumClient/` (macOS)
- `^/opt/Tanium/TaniumClient/` (Linux)
- `\\Tanium\\Tanium Client\\` (Windows)

© 2026 Tanium Inc. All Rights Reserved

Reference: Reveal endpoint settings

You can modify these Reveal Tanium Client managed endpoint settings by creating and deploying a profile. For more information, see Creating profiles on page 37. For more information about updating settings for the Reveal service, see (Optional) Configure Reveal service settings on page 35.

Tanium Index subscription settings

A Reveal profile contains the following default Tanium Index subscription settings. You can modify these settings. For more information, see Create a profile on page 37.

Setting	Default value	Description
Tanium Index Scan Frequency	10080 minutes	Controls how often the Tanium Index scan runs.
Tanium Index First Scan Distribute Over Time	1440 minutes	Sets the time for the initial Tanium Index scan.
Quick Search	Disabled	Enables or disables quick search functionality. Quick search uses additional disk and CPU resources on endpoints.
Quick Search High-Frequency Word Threshold	Enabled	Enable or disable quick search high-frequency word filtering (Default: enabled). When enabled, high-frequency words - for example, articles - are not searched. By not searching for such strings, endpoint resources are reserved.
Quick Search High-Frequency Word Threshold Value	500	The number of files in which a string occurs before it is considered a high-frequency word. For example, if more than this number of files contain a word, the word is not saved in the database for the file. This reduces database size and therefore disk use.

Reveal endpoint settings

To exclude files from indexing in Reveal versions before 1.18, use the **Path Stem Exclusions** or **Path Filter Exclusions** settings (from the Reveal **Overview** page, click **Settings > Endpoint Configuration**). To exclude files from indexing in Reveal versions 1.18 and later, use the **Reveal Parse Exclusions by Regular Expression** or **Reveal Parse Exclusions by File Path** settings in a Reveal profile.

© 2026 Tanium Inc. All Rights Reserved

Setting	Default value	Description

File Name Exclusions	`.*\\Windows\\servicing\\.*`
	`.*\\Windows\\WinSxS\\.*`
	`.*\\Windows\\CSC\\.* .*\\Windows\\SoftwareDistribution\\Download\\.*`
	`.*\\ProgramData\\Microsoft\\Windows Defender\\Scans\\History\\.*`
	`.*\\Tanium\\Tanium Client\\.*`
	`.*Resources\/.*lproj.*`
	`.*olk15Message`
	`.*olk15MsgAttachment`
	`.*olk15Event`
	`.*\.png`
	`.*\/Microsoft\/Teams\/Cache\/.*_0`
	`.*\/Cache_Data\/.*_0`
	`.*Service Worker\/CacheStorage.*`
	`.*\/Code Cache\/js\/.*_0`
	`\/System\/Library\/Assistant\/FlowDelegatePlugins.*bin`
		Paths to exclude* from parsing in regular expression format. For example: `.*\.docx` filters any files that end with the .docx file extension.

Path Exclusions	`/opt/Tanium/TaniumClient`
	`/Library/Tanium/TaniumClient`
	`/System/Volumes/Data/Library/Tanium/TaniumClient`
	`/System/Library/Frameworks`
	`/System/Library/PrivateFrameworks`
	`/System/iOSSupport`
		Paths to exclude* from parsing. For example: `C:\Program Files (x86)\Tanium\Tanium Client\` filters all content under `Tanium Client`.

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.

© 2026 Tanium Inc. All Rights Reserved

Reference: Reveal sensors and packages

Use the Index sensors to get details about Reveal functionality on Tanium Client managed endpoints.

Reveal Index sensors

Sensor	Description
Reveal - Index File Details	Returns details of index files that match one or more supplied inputs.
Reveal - Index File Count	Returns count of index files that match one or more supplied inputs.
Reveal - Index File Exists	Returns Yes or No, using Index to determine whether the specified file exists based on the supplied input.
Reveal - Index File Hash Recently Changed	Returns details of index files that match one or more supplied inputs.
Reveal - Index Has Category Hit	Returns Yes/No for endpoints with files that match a category.
Reveal - Index Has No Validation Rule Hit	Returns Yes/No for endpoints with files that match a rule with no validation hits.
Reveal - Index Has Rule Hit	Returns Yes/No for endpoints with files that match a rule.
Reveal - Index Has Valid Rule Hit	Returns Yes/No for endpoints with files that match a rule with at least one valid validation hit.
Reveal - Index Installed Rules	Returns Rule IDs installed on the endpoint.
Reveal - Index Is Path Indexed	Evaluates an index configuration to see if a path will be indexed.
Reveal - Index List Discovered Volumes	Returns list of filesystem volumes discovered by index.
Reveal - Index No Validation Rule Hit Files	Returns files that match rules with no validation hits.
Reveal - Index Quick Search	Search for a hashed token on an endpoint.
Reveal - Index Rule Hit Files	Returns files that match rules.
Reveal - Index Rule Hit Files by Validation	Returns files that match rules with validation hits.
Reveal - Index Rule Hit Summary	Returns a summary of rule hits.
Reveal - Index Tuning - Get Top Extensions	Returns the top ten file extensions with highest file counts for tuning Index.
Reveal - Index Tuning - Get Top Paths	Returns the top ten paths with highest file counts for tuning Index. The paths that are returned are non-recursive.

© 2026 Tanium Inc. All Rights Reserved

Reveal Index sensors (continued)

Sensor	Description
Reveal - Index Valid Rule Hit Files	Returns files that match rules with valid validation hits.

The following packages are provided with Reveal. Open a package in the console to edit package parameters and deploy the package to appropriate endpoints.

Package	Description
Index - Request Immediate One-Time Scan	This package starts an index of a targeted endpoint.

Deprecated Reveal sensors and packages

The following Reveal sensors have been deprecated:

- Reveal - Background Scan Results
- Reveal - Background Scan Summary
- Reveal - Confirmed Files
- Reveal - Coverage Status
- Reveal - Endpoint Rule Result
- Reveal - Endpoints with Confirmed Sensitive Data
- Reveal - Endpoints with Unconfirmed Sensitive Data
- Reveal - File Details
- Reveal - Installed Rule Sets
- Reveal - Installed Rule Sets by Name
- Reveal - Label Results
- Reveal - Status
- Reveal - Validation Results
- Reveal - Tools Version

The following packages have been deprecated:

- Reveal - Delete Indexing Data [Linux]
- Reveal - Delete Indexing Data [Mac]
- Reveal - Delete Indexing Data [Windows]
- Reveal - Index Path [Linux]

© 2026 Tanium Inc. All Rights Reserved

- Reveal - Index Path [Mac]
- Reveal - Index Path [Windows]
- Reveal - Rebuild Indexing Data [Linux]
- Reveal - Rebuild Indexing Data [Mac]
- Reveal - Rebuild Indexing Data [Windows]
- Reveal - Set Time Offset [Linux]
- Reveal - Set Time Offset [Mac]
- Reveal - Set Time Offset [Windows]
- Reveal - Start Indexing [Linux]
- Reveal - Start Indexing [Mac]
- Reveal - Start Indexing [Windows]

Sensor replacements from Reveal 1.x to Reveal 2.x

The following sensors have been replaced from Reveal 1.x to Reveal 2.x.

Reveal 1.x	Reveal 2.x
Reveal - Background Scan Results	Reveal - Index Rule Hit Summary
Reveal - Background Scan Summary	Reveal - Index Rule Hit Summary
Reveal - Confirmed Files	Reveal - Index Valid Rule Hit Files
Reveal - Coverage Status	Client Extensions - Status Endpoint Configuration - Tools Status
Reveal - Endpoint Rule Result	--
Reveal - Endpoints with Confirmed Sensitive Data	Reveal - Index Has Valid Rule Hit
Reveal - Endpoints with Unconfirmed Sensitive Data	Reveal - Index Has No Validation Rule Hit
Reveal - File Details	--
Reveal - Installed Rule Sets	Reveal - Index Installed Rules
Reveal - Installed Rule Sets by Name	Reveal - Index Installed Rules
Reveal - Label Results	--

© 2026 Tanium Inc. All Rights Reserved

Reveal 1.x	Reveal 2.x
Reveal - Status	Client Extensions - Status
Reveal - Validation Results	--
Reveal - Tools Version	Endpoint Configuration - Tools Status
--	Reveal - Index Has Category Hit
--	Reveal - Index Has Rule Hit
--	Reveal - Index Quick Search
--	Reveal - Index No Validation Rule Hit Files

© 2026 Tanium Inc. All Rights Reserved