Tanium™ Reveal User Guide

Version 1.14.69

April 21, 2021

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://docs.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 to make interaction with Tanium software more intuitive and to accelerate the time to success. To ensure high accessibility standards, Tanium complies with the U.S. Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. We have conducted third-party accessibility assessments over the course of product development for many years, and most recently a comprehensive audit against the WCAG 2.1 / VPAT 2.3 standards for all major product modules was completed in September 2019. 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 best efforts to address any gaps quickly, as is feasible, given the severity of the issue and scope of the changes. These objectives are factored 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, email Tanium Support at support@tanium.com, or email accessibility@tanium.com to make further inquiries.

Table of contents

Reveal overview

With Reveal, you can detect sensitive unstructured data at rest on 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 label 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 add a 'confidential' label to all of the text documents 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.

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 information regarding extending the list, see Contact Tanium Support on page 48.

Integration with other Tanium products

Reveal has built in integration with Tanium™ Trends for additional reporting of related data.

Trends

By default, Reveal features Trends boards that provide data visualization of Reveal concepts.

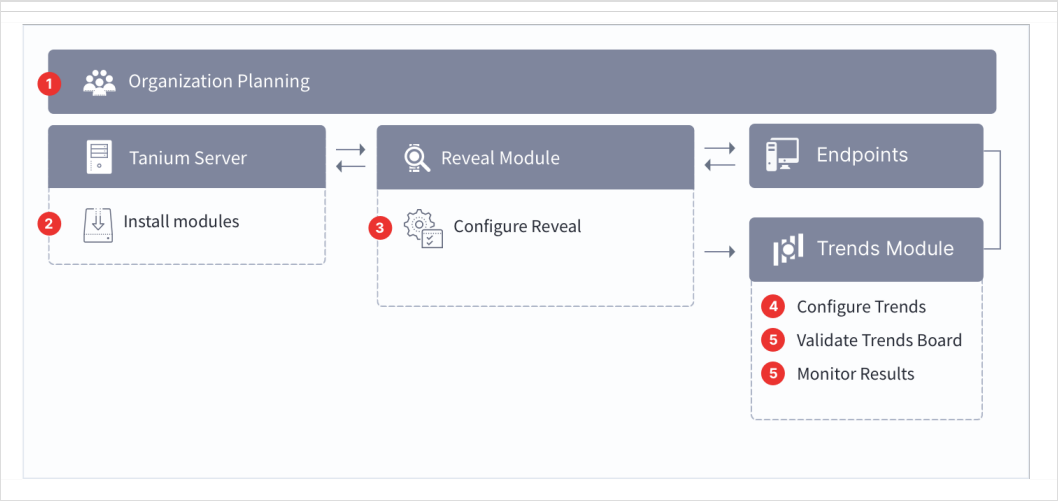
The **Reveal** board features visualizations that show the status of Reveal components on endpoints in an environment and provides visibility into any areas of Reveal that require remediation. Additionally, the **Reveal status** board shows real time and historical statistics concerning rule matches on endpoints. The following panels are in the Reveal board:

- Reveal Coverage
- Endpoints with Confirmed Sensitive Data
- Endpoints with Unconfirmed Sensitive Data
- Unverified Matches
- Label Results
- Endpoint Status
- Data Size
- Scan Failure
- Undersized Reveal Databases
- Reveal Tools Installations
- Applied Rule Sets
- Tools Version

For more information about how to import the Trends boards that are provided by Reveal, see Tanium Trends User Guide: Importing the initial gallery.

Succeeding with Reveal

Follow these best practices to achieve maximum value and success with Reveal. These steps align with the key benchmark metrics: increasing Reveal coverage, monitoring endpoints with confirmed sensitive data, and monitoring endpoints with unconfirmed sensitive data.



Step 1: Gain organizational effectiveness

Complete the key organizational governance steps to maximize Reveal value. For more information about each task, see Gaining organizational effectiveness on page 11.

- ☐ Develop a dedicated Change management process.
- ☐ Define distinct roles and responsibilities in a RACI chart.
- ☐ Validate cross-functional Organizational alignment.
- ☐ Track Operational metrics.

Step 2: Install Tanium modules

- ☐ Install Tanium Reveal. See Installing Reveal on page 29

☐ Install Tanium Trends. See Tanium Trends User Guide: Installing Trends.

☐ Install Tanium Direct Connect. See Tanium Direct Connect User Guide: Installing Direct Connect.

☐ Install Tanium Client Management, which provides Tanium Endpoint Configuration. See Tanium Client Management User Guide: Installing Client Management.

Step 3: Configure Tanium products - Trends and action groups

☐ Open Tanium Trends and import the Reveal gallery. See Tanium Trends User Guide: Importing the initial gallery for more information. If you installed Trends using the Apply Tanium recommended configurations option, the Reveal boards are automatically imported after the Reveal service account is configured.

Step 4: Configure Reveal

☐ Create computer groups for Windows, Linux, and macOS. If you install Reveal using the Apply Tanium recommended configurations option, the computer groups are created automatically.

☐ Add computer groups to Reveal action group.

☐ Create a Rule Set with a name indicating the type of sensitive information you want Reveal to discover.

☐ Deploy rules. See Deploy rules.

Step 5: Configure Trends

☐ From the Trends menu, click **Boards**. Select **Reveal - Executive Metrics**. Click **Validate**. Click **Import**. If you installed Trends using the Apply Tanium recommended configurations option, the Reveal boards are automatically imported after the Reveal service account is configured.

Step 6: Monitor Reveal metrics

☐ From the Trends menu, click **Boards**. Select **Reveal - Executive Metrics**. Review the trending data in the **Reveal - Coverage**, **Reveal - Endpoints with Findings per Rule**, and **Reveal - Validation Needed** panels.

- ☐ Monitor and troubleshoot Reveal coverage.
- ☐ Monitor and troubleshoot endpoints with confirmed sensitive data.
- ☐ Monitor and troubleshoot endpoints with unconfirmed sensitive data.

Gaining organizational effectiveness

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

- Develop a dedicated change management process. See Change management on page 11.
- Define distinct roles and responsibilities. See RACI chart on page 11.
- Track operational maturity. See Operational metrics on page 14.
- Validate cross-functional alignment. See Organizational alignment on page 14.

Change management

Develop a tailored, dedicated change management process for patch management, 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.

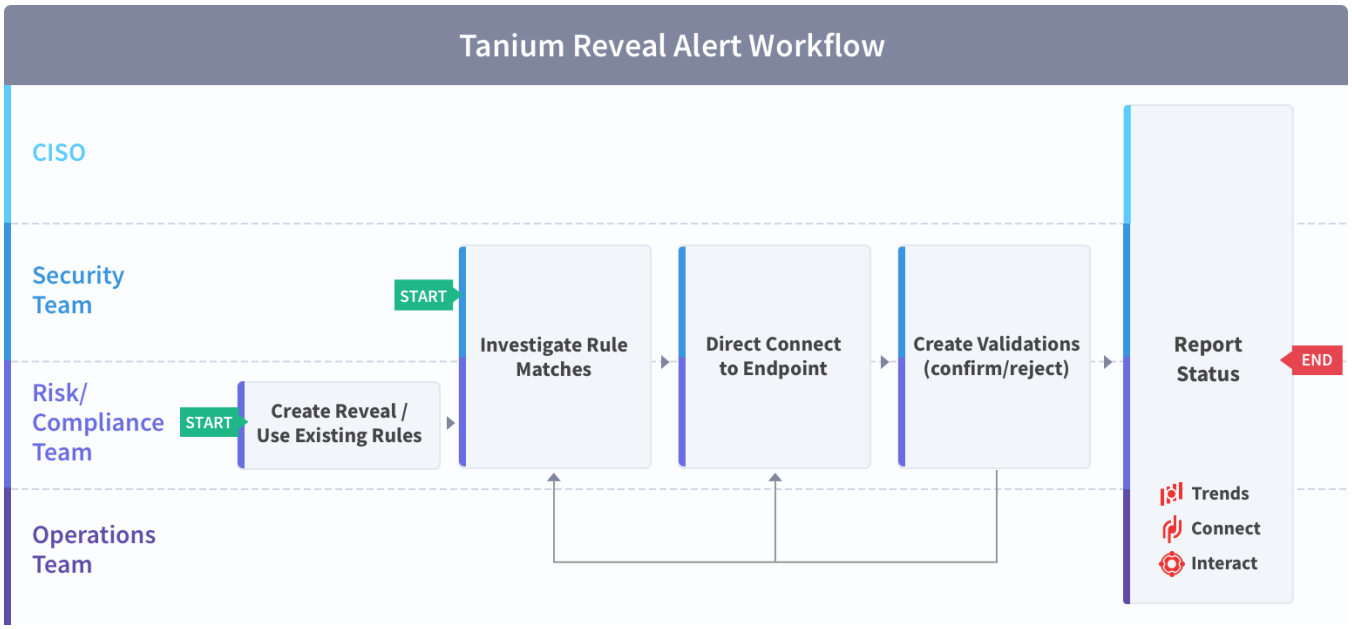
RACI chart

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 patch management. Use the following table as a baseline example.

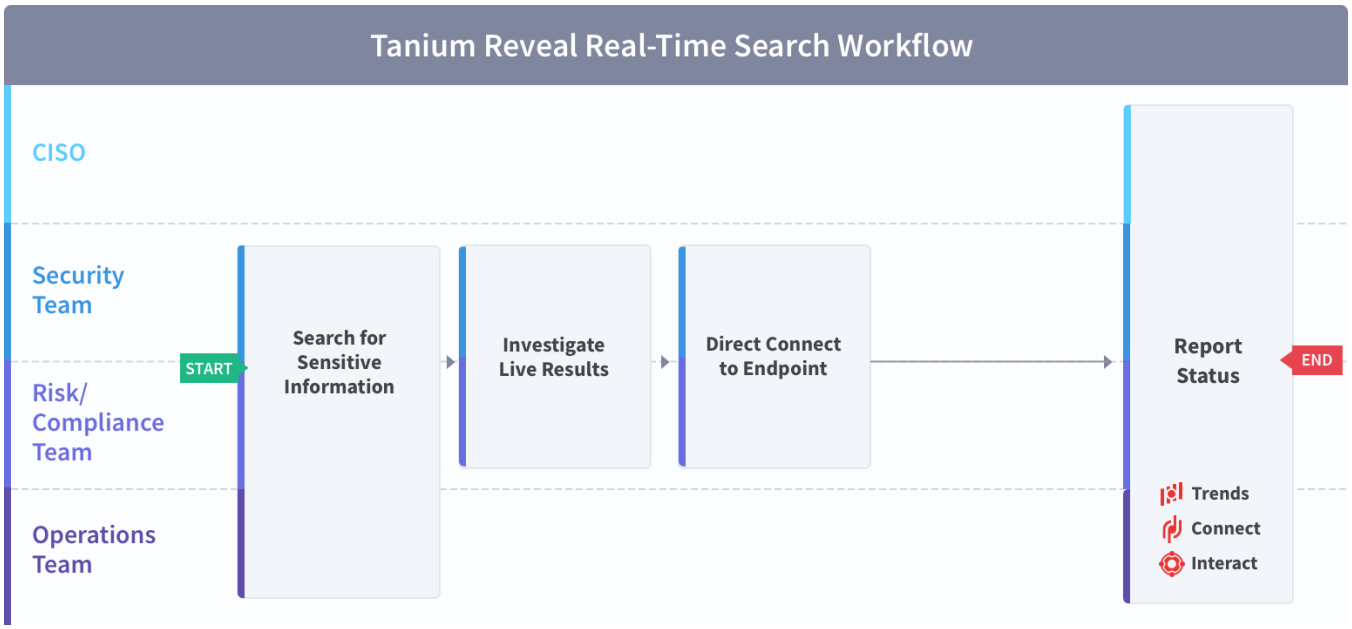
Task	IT Security	IT Operations	IT Risk/Compliance	Executive	Rationale
Determine which default rules to use or which custom rules to create	C	I	R/A	C	When Reveal is originally installed, there are default rules for PCI, HIPAA, GDPR, and CCPA. The Risk/Compliance team might have other items they need to track and will be accountable for defining those rules and labels. The security team will be consulted along with the CIO/CRO/CPO to ensure proper policy coverage.
Investigate rule matches using Live Connect	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.

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



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:

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

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:

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 - confirmed or rejected. 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.

		Level 1 (Needs improvement)	Level 2 (Below average)	Level 3 (Average)	Level 4 (Above average)	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 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 label results, Identifying and investigating insider threats and policy violations

		Level 1 (Needs improvement)	Level 2 (Below average)	Level 3 (Average)	Level 4 (Above average)	Level 5 (Optimized)
	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 Live Connect	Tanium Enforce for device control / removable media, Tanium Threat Response	Tanium Connect, Reports on numbers of hits by endpoint or total aggregate to SIEM, Google Chronicle	Tanium Impact, Tanium Data Services	ITSM workflow
	Reporting	Manual; via Reveal workbench / dashboard for operators only	Manual; Reveal workbench / dashboard for operators / peer group only	Automated; Trends Boards tailored to stakeholders ranging from Operator to Executive	Automated; Trends Boards tailored to stakeholders ranging from Operator to Executive and Legal	Automated; Trends Boards tailored to stakeholders ranging from Operator to Executive, Legal, and HR
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%

Reveal requirements

Review the requirements before you install and use Reveal.

Tanium dependencies

In addition to a license for the Reveal product module, make sure that your environment also meets the following requirements.

Component	Requirement
Tanium™ Core Platform	7.3.314.4250 or later.
Tanium™ Client	Any supported version of Tanium Client. For the Tanium Client versions supported for each OS, 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.
Tanium products	If you clicked the **Install with Recommended Configurations** button when you installed Reveal, the Tanium Server automatically installed all your licensed modules at the same time. Otherwise, you must manually install the modules that Reveal requires to function, as described under Tanium Console User Guide: Manage Tanium modules. The following products are required for features of Reveal to function. The given versions are the minimum required: • Tanium Index 2.5.2 or later. • Tanium Trends 3.6.331 or later. • Tanium Interact 2.5.146 or later. • Tanium Direct Connect 1.4.0 or later. • Tanium Endpoint Configuration 1.2 or later. NOTE Endpoint Configuration is installed as part of Tanium Client Management 1.5 or later.

Component	Requirement
Computer groups	When you first log into the Tanium Console after installing the Tanium Server, the server automatically imports the computer groups that Reveal requires: • `All Computers` • `All Windows` • `All Mac` • `All Linux`

Reveal deploys the Tanium Index 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)

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

Up to 2 GB of free disk space is required on each endpoint.

Supported operating systems

Operating system	OS version
Microsoft Windows Server	• Windows Server 2008 R2 SP1 or later
Microsoft Windows Workstation	• Windows 10 • Windows 8 • Windows 7 SP1 NOTE Windows 7 Service Pack 1 requires Microsoft KB2758857.

Supported operating systems (continued)

Operating system	OS version
macOS (Intel processor only)	• macOS 11.0 Big Sur • macOS 10.15 Catalina • macOS 10.14 Mojave • macOS 10.13 High Sierra • macOS 10.12 Sierra • OS X 10.11.6 El Capitan
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 8x, 7.x, 6.x, 5.x
	Ubuntu 20.04 LTS
	Ubuntu 18.04 LTS
	Ubuntu 16.04 LTS

Host and network security requirements

Specific ports and processes are needed to run Reveal.

Ports

The following ports are required 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.

Source	Destination	Port	Protocol	Purpose
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.				

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 security software is in use in the environment to monitor and block unknown host system processes, your security administrator must create exclusions to allow the Tanium processes to run without interference.

Reveal security exclusions

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

Reveal security exclusions (continued)

Target Device	Notes	Process
Windows endpoints		*<Tanium Client>*\TaniumCX.exe
		<Tanium Client>\Tools\EPI\TaniumExecWrapper.exe
		<Tanium Client>\Tools\EPI\TaniumEndpointIndex.exe
		<Tanium Client>\TaniumClientExtensions.dll
		<Tanium Client>\TaniumClientExtensions.dll.sig
		<Tanium Client>\extensions\RevealCX.dll
		<Tanium Client>\extensions\RevealCX.dll.sig
		<Tanium Client>\extensions\TaniumDEC.dll
		<Tanium Client>\extensions\TaniumDEC.dll.sig
		<Tanium Client>\extensions\core\libTaniumPythonCx.dll
		<Tanium Client>\extensions\core\libTaniumPythonCx.dll.sig
	7.2.*x* clients, [1]	*<Tanium Client>*\Python27\TPython.exe
	7.4.*x* clients, [1]	*<Tanium Client>*\Python38\TPython.exe
	7.2.*x* clients	*<Tanium Client>*\Python38*.dll

Reveal security exclusions (continued)

Target Device	Notes	Process
Linux endpoints		*<Tanium Client>*/TaniumCX
		<Tanium Client>/Tools/EPI/TaniumExecWrapper
		<Tanium Client>/Tools/EPI/TaniumEndpointIndex
		<Tanium Client>/libTaniumClientExtensions.so
		<Tanium Client>/libTaniumClientExtensions.so.sig
		<Tanium Client>/extensions/libRevealCX.so
		<Tanium Client>/extensions/libRevealCX.so.sig
		<Tanium Client>/extensions/libTaniumDEC.so
		<Tanium Client>/extensions/libTaniumDEC.so.sig
		<Tanium Client>/extensions/core/libTaniumPythonCx.so
		<Tanium Client>/extensions/core/libTaniumPythonCx.so.sig
	7.2.*x* clients	*<Tanium Client>*/python27/python
	7.4.*x* clients	*<Tanium Client>*/python38/python

Reveal security exclusions (continued)

Target Device	Notes	Process
macOS endpoints		*<Tanium Client>*/TaniumCX
		<Tanium Client>/Tools/EPI/TaniumExecWrapper
		<Tanium Client>/Tools/EPI/TaniumEndpointIndex
		<Tanium Client>/libTaniumClientExtensions.dylib
		<Tanium Client>/libTaniumClientExtensions.dylib.sig
		<Tanium Client>/extensions/libRevealCX.dylib
		<Tanium Client>/extensions/libRevealCX.dylib.sig
		<Tanium Client>/extensions/libTaniumDEC.dylib
		<Tanium Client>/extensions/libTaniumDEC.dylib.sig
		<Tanium Client>/extensions/core/libTaniumPythonCx.dylib
		<Tanium Client>/extensions/core/libTaniumPythonCx.dylib.sig
	7.2.*x* clients	*<Tanium Client>*/python27/python
	7.4.*x* clients	*<Tanium Client>*/python38/python

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

User role requirements

Use role-based access control (RBAC) permissions to restrict access to Reveal functions.

Tanium Reveal User Role Privileges

Permission	Reveal Administrator	Reveal Operator	Reveal Read Only User	Reveal Service Account[3]	Reveal User[1]	Reveal Endpoint Configuration Approver[2]
Show Reveal Access to the Reveal workbench	✓	✓	✓	✗	✓	✓
Reveal Affected Files Enables viewing of affected files	✓	✓	✗	✗	✓	✗

Tanium Reveal User Role Privileges (continued)

Permission	Reveal Administrator	Reveal Operator	Reveal Read Only User	Reveal Service Account[3]	Reveal User[1]	Reveal Endpoint Configuration Approver[2]
Reveal Quick Search Enables viewing of quick search results	✓	✓	✗	✗	✓	✗
Reveal Rules Deploy Enables the deployment of rules to endpoints	✓	✓	✗	✗	✓	✗
Reveal Rules Deploy Status Access to the Reveal workbench	✓	✓	✓	✗	✓	✗
Reveal Rules Read Enables the viewing and listing of rules	✓	✓	✓	✗	✓	✓
Reveal Rules Write Enables the editing of rules	✓	✓	✗	✗	✓	✗
Reveal Rule Sets Read Enables the viewing and listing of rule sets	✓	✓	✓	✗	✓	✓
Reveal Rule Sets Write Enables the editing of rule sets	✓	✓	✗	✗	✓	✗
Reveal Service User Enables a user to perform work as the service account user	✗	✗	✗	✓	✗	✗

Tanium Reveal User Role Privileges (continued)

Permission	Reveal Administrator	Reveal Operator	Reveal Read Only User	Reveal Service Account[3]	Reveal User[1]	Reveal Endpoint Configuration Approver[2]
Reveal Service User Read Allows viewing details of the service account user	✓	✗	✓	✗	✗	✗
Reveal Service User Write Enables modifications to the service user account	✓	✗	✗	✗	✗	✗
Reveal Snippets Enables viewing of snippets of affected files.	✓	✓	✗	✗	✓	✗
Reveal Use API Perform Reveal operations using the API	✓	✓	✓	✓	✓	✗
Reveal Validations Deploy Enables the deployment of validations to endpoints	✓	✓	✗	✗	✓	✗
Reveal Validations Deploy Status Enables viewing of the status of validation deployments	✓	✓	✓	✗	✓	✗
Reveal Validations Read Enables viewing and listing of validations	✓	✓	✓	✗	✓	✓
Reveal Validations Write Enables the editing of validations	✓	✓	✗	✗	✓	✗

Tanium Reveal User Role Privileges (continued)

Permission	Reveal Administrator	Reveal Operator	Reveal Read Only User	Reveal Service Account[3]	Reveal User[1]	Reveal Endpoint Configuration Approver[2]
Reveal Settings Read Enables viewing and listing Reveal settings	✓	✗	✗	✗	✗	✓
Reveal Settings Write Enables the editing of Reveal settings	✓	✗	✗	✗	✗	✗
Reveal Operator Settings Read Enables viewing and listing Reveal settings	✓	✓	✗	✗	✗	✗
Reveal Operator Settings Write Enables the editing of Reveal settings	✓	✓	✗	✗	✗	✗
Reveal Admin Perform administrative functions for the Reveal module	✓	✗	✗	✗	✗	✗
Trends Integration Service Account Provides access for module service accounts to read and write data, and to define sources and boards.	✗	✗	✗	✗	✓	✗

Tanium Reveal User Role Privileges (continued)

Permission	Reveal Administrator	Reveal Operator	Reveal Read Only User	Reveal Service Account[3]	Reveal User[1]	Reveal Endpoint Configuration Approver[2]
Reveal Endpoint Configuration Approve Enables approver privileges in Tanium Endpoint Configuration for Reveal configuration changes.	✗	✗	✗	✗	✗	✓

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

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

[3]If you installed Tanium Client Management, Endpoint Configuration is installed, and by default, configuration changes initiated by the module service account (such as tool deployment) require approval. You can bypass approval for module-generated configuration changes by applying the **Endpoint Configuration Bypass Approval** permission to this role and adding the relevant content sets. For more information, see Tanium Endpoint Configuration User Guide: User role requirements.

For more information and descriptions of content sets and permissions, see the Tanium Core Platform User Guide: Users and user groups.

Installing Reveal

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

- **Automatic configuration with default settings** (Tanium Core Platform 7.4.2 or later only): 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 details about the automatic configuration for Reveal, see Import and configure Reveal with default settings on page 29.
- **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 and configure Reveal with custom settings on page 29.

Before you begin

- Read the Release Notes.
- Review the Reveal requirements on page 18.

Import and configure Reveal with default settings

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

- The Reveal service account is set to the account that you used to import the module.
- The Reveal action group is set to the computer group `All Computers`.

To import Reveal and configure default settings, be sure to select the **Apply Tanium recommended configurations** check box while performing the steps under Tanium Console User Guide: Manage Tanium modules. After the import, verify that the correct version is installed: see Verify Reveal version on page 31.

Import and configure Reveal with custom settings

To import Reveal without automatically configuring default settings, be sure to clear the **Apply Tanium recommended configurations** check box while performing the steps under Tanium Console User Guide: Manage Tanium modules. After the import, verify that the correct version is installed: see Verify Reveal version on page 31.

Configure service account

The service account performs the following tasks for Reveal:

- Create scheduled actions for automatic tools deployment and indexing
- Schedule automatic rules deployment
- Gather stats and results

After deploying the tools for the first time, endpoints can take some time to display status, depending on throttling

configuration.

The service account is a user that runs several background processes for Reveal. This user requires the following roles and access:

- **Tanium Administrator** or **Reveal Service Account** role.
- If you installed Tanium Client Management, Endpoint Configuration is installed, and by default, configuration changes initiated by the module service account (such as tool deployment) require approval. You can bypass approval for module-generated configuration changes by applying the **Endpoint Configuration Bypass Approval** permission to this role and adding the relevant content sets. For more information, see Tanium Endpoint Configuration User Guide: User role requirements.

For more information about Reveal permissions, see User role requirements on page 24.

1. From the Main menu, go to **Modules > Reveal** to open the **Reveal Overview** page.
2. Click Settings and open the **Service Account** tab.
3. Update the service account settings and click **Save**.

Configure Reveal action group

The action group defines the set of endpoints to which you are deploying the Reveal packages. By default, the **Computer Group Targets** setting for the Reveal action group is set to **No Computers**. You can set the action group to **All Computers** or any computer groups that you have defined.

1. From the Main menu, go to **Administration > Actions > Action Groups**.
2. In the list of action groups, click **Tanium Reveal** .
3. Click **Edit**, select computer groups to include in the action group, and click **Save**.

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.

NOTE Endpoint Configuration is installed as a part of Tanium Client Management. For more information, see the Tanium Client Management User Guide: Installing Client Management.

Additionally you can use Endpoint Configuration to manage configuration approval. For example, configuration changes are not deployed to endpoints until a user with approval permission approves the configuration changes in Endpoint Configuration. For more information about the roles and permissions that are required to approve configuration changes for Reveal, see User role requirements on page 24.

To use Endpoint Configuration to manage approvals, you must enable configuration approvals.

1. From the Main menu, go to **Administration > Shared Services > Endpoint Configuration** to open the Endpoint Configuration **Overview** page.
2. Click Settings and click the **Global** tab.
3. Select **Enable configuration approvals**, and click **Save**.

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

Manage dependencies for Tanium solutions

When you start the Reveal workbench for the first time, the Tanium console ensures that all of the required dependencies for Reveal are installed at the required version. You must install all required Tanium dependencies before the Reveal workbench can load. A banner appears if one or more Tanium dependencies are not installed in the environment. The Tanium Console lists the required Tanium dependencies and the required versions.

1. From the Main menu, go to **Administration > Configuration > Solutions**.
2. Select the required solutions, click **Import Selected**, and then click **Begin Import**. When the import is complete, you are returned to the **Tanium Solutions** page.
3. From the Main menu, go to **Modules > Reveal** to open the Reveal **Overview** page after you import all of the required Tanium dependencies.

Upgrade the Reveal version

Upgrade Reveal to the latest version.

BEST PRACTICE 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 Troubleshooting Reveal: Collect logs.

For the steps to upgrade the Reveal solution, see Tanium Console User Guide: Manage Tanium modules. To verify the version, see Verify Reveal version on page 31.

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

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 display version information, click Info  .

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 label 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.

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. 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.

Criteria for rule evaluation

See Reference: Supported file types for rule evaluation on page 49.

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 endpoints from the computer groups specified in the rule set.

Pattern

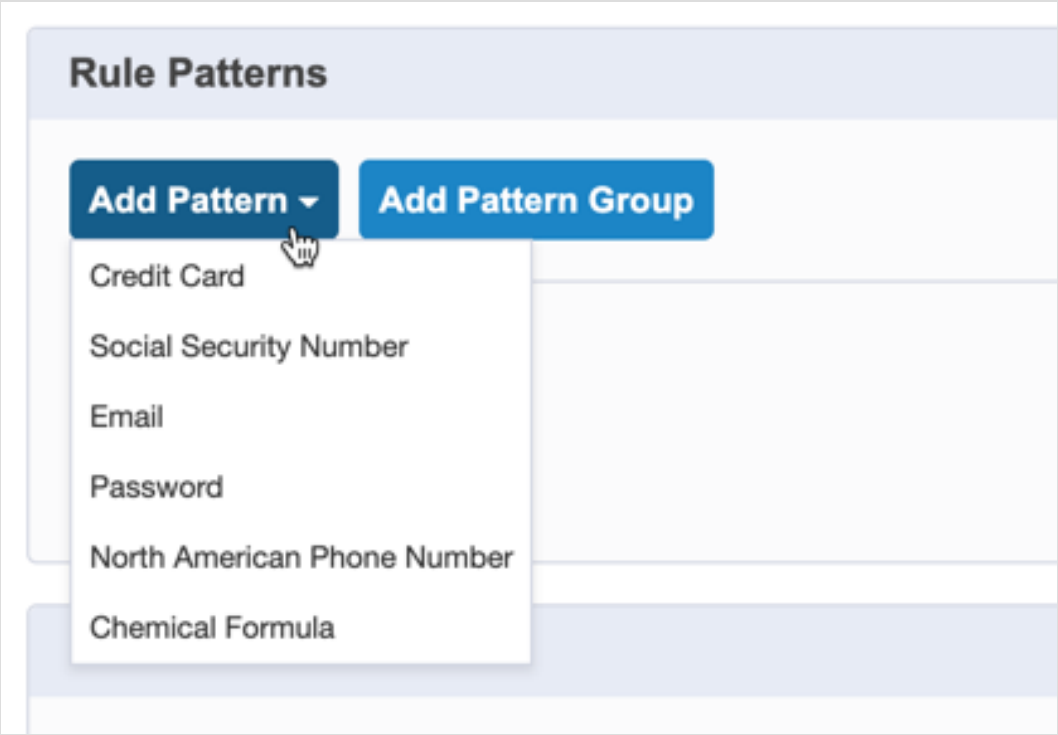
Use patterns to find sensitive data in files that match the filters. Patterns include credit cards, social security numbers, email addresses, passwords, and phone numbers.

Pattern group

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

Create a rule

1. From the Reveal menu, click **Rules**. 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 a list of file types, see Reference: Supported file types for rule evaluation on page 49.
5. Under **Rule Patterns**, add one or more rule patterns. Rules must contain at least one condition.
    1. 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.
    2. To add a proximal pattern match, click **Add Pattern Group**. A rule can contain one pattern group.
        a. For **Proximity**, select the maximum number of characters that the patterns can be from each other.
        b. In the pattern group, click **Add Pattern** and select a pattern to include in the match. Repeat to add a second pattern. A pattern group must contain at least two patterns.



Each instance that matches the pattern group results in a rule match. For example, you can create a pattern 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 five rule matches: four for the email addresses and one for the word "password".

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

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, navigate to the **Rules** page, click **Deploy Rules**, enter your credentials, and click **OK**.

Test and verify rules before deploying to endpoints.

You can also deploy rules from the **Rule Sets** page and from the **Deploy Rules** configuration step on the Reveal overview page.

Customize rule patterns

You can download a copy of rule patterns and file types to customize, and upload any customizations that you make to refine the scope of rules.

To be effective, rule patterns must be developed methodically and tested exhaustively.

1. From the Main menu, click **Reveal**. The Reveal Overview page appears.
2. Click Settings and open the **Pattern Definitions** tab.
3. To download pattern definitions, click **Download**.
4. Edit the downloaded file and either drag the file into the upload dialog, or click **Select a file** to browse top the file you want to upload.

You cannot upload a file that is not valid. Make sure that any file you attempt to upload is structurally valid.

Creating rule sets

Rule sets group rules together and assign them to specific groups of 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.

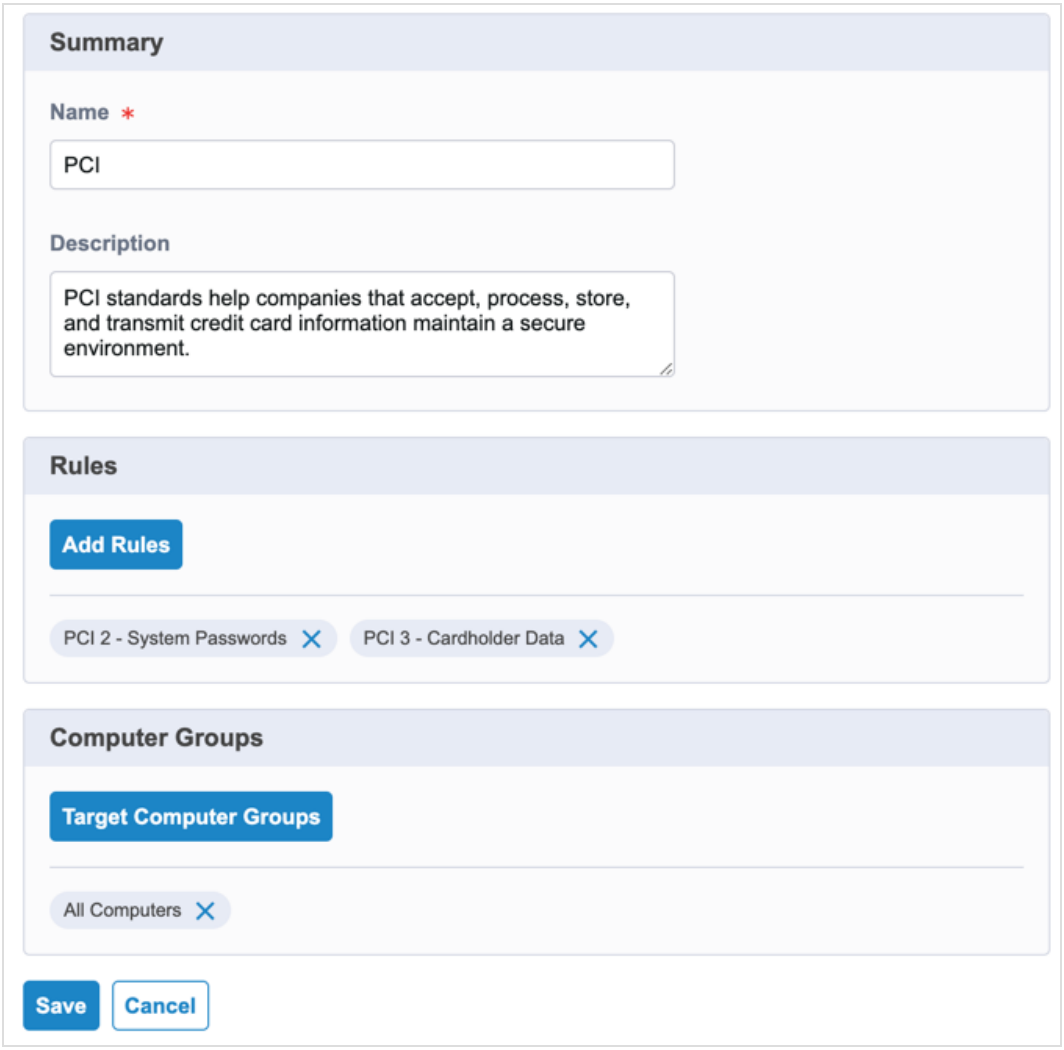
A rule set has no effect unless it contains at least one rule. The default rule sets contain at least one rule. The default rules cannot be edited, but you can delete them, or make a duplicate of a rule and customize it for your specific needs.

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. 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

1. From the Reveal menu, click **Rule Sets**. Click **New Rule Set**.
2. Enter a name and description for the rule set.



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

1. From the Reveal menu, click **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. Click **Save**.

Delete a rule set

1. From the Reveal menu, click **Rule Sets**.
2. Select the check box 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.

Deleting a rule set does not remove any historical matches from any metrics.

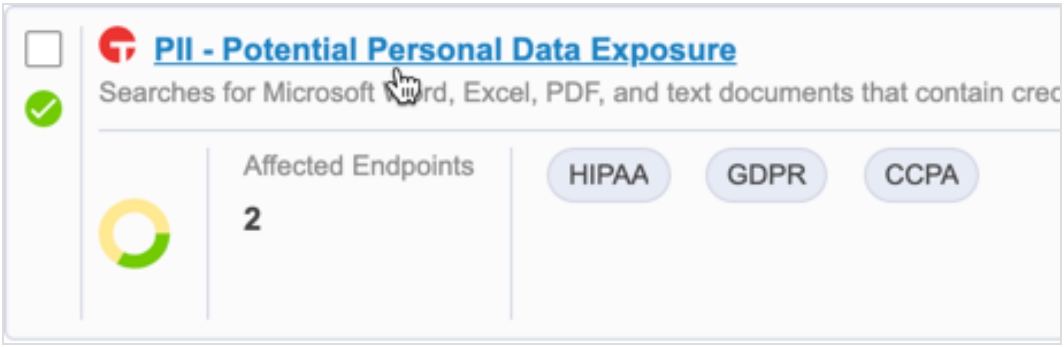
Investigating rule matches

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 endpoint. You can further investigate the details of the match. Each rule displays 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.

From the Rules page, you can investigate the affected endpoints, and files where matches are detected when a rule match occurs.

Investigate by endpoint

1. From the Reveal menu, click **Rules**.
2. Click a rule that has matches that you want to investigate.



3. Under **Results**, Reveal displays 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 displays 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 are displayed.
6. Click an affected file to view snippets that show pattern matches in context.

Take action on files where rule matches occur

When a rule applies a label to files that contain a rule match, you can use Tanium questions to take action on affected files.

1. From the Main menu, click Interact.
2. Ask the question **Get Reveal - Label Results from all machines**. The results grid displays the labels that have been applied to files, and the number of files that are labeled.
3. Select the rows for the labels that require the action, and then click **Deploy Action**. Interact displays the Deploy Action workflow page.

For more information, see Tanium Interact User Guide: Questions.

Validating pattern matches

Create validations to improve the accuracy of rule performance and to reduce the number of false positive results on the data that rules target. 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.

Validations apply to pattern matches in the context of a rule where the text appears exactly as it does in the validation. 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.

Create a validation

1. From the Reveal menu, click **Rules**.
2. Select a specific rule to view a list of results and associated endpoints.
3. Select the check box next to an endpoint that has one or more files that match patterns. Click **Live Connect** .
4. After the connection establishes, click the computer name.
5. Select a file that contains one or more pattern matches.
6. View the snippets that show where a pattern matches. Confirmed and unverified snippets are shown by default. To limit which results display, click **Filter Results** to view or hide unverified, confirmed, rejected, and excluded snippets.

   Excluded snippets are unverified snippets that do not match patterns exactly. This includes matches to pattern groups outside the proximity range. You can confirm or reject an excluded snippet.
7. For each snippet, highlight the relevant text. 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.
8. Select **Confirm** or **Reject**. Rejected snippets are filtered from future results.

   Keyboard shortcuts include (c) for Confirm and (r) for Reject. If you do not want to add a name and description for the validation, press (cc) for Confirm and Save, or (rr) for Reject and Save; these two shortcuts skip the next two steps.

9. 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 confirmed or rejected.
10. 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** 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 confirmed or rejected, values in the affected files view for any rule where patterns have been matched and validated display in orange in the **Unconfirmed hits** and **Confirmed hits** columns. 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 display in black.

Deploy validations

Deploying validations creates new **Reveal - Validations** packages, and recreates the **Reveal - Deploy Validations** saved actions.

Published validations apply to all hits of the corresponding rule. Rejected hits are ignored.

1. From the Reveal menu, click **Rule Validations**.
2. Click **Deploy Validations**.

Audit published validations

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

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

Searching across the enterprise

Use Reveal to search for specific items of sensitive information across an entire 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 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 exact sequence of tokens across the environment. For example, if a search query is `process is started`, this is tokenized as `["process","started"]`. These tokens match `the malicious process has started`, but not `started the process` because the tokens are not in the same order as the query.

Perform a quick search

1. From the Reveal menu, click **Quick Search**.
2. In the search field, provide a literal search string or a token from a previous or saved search. For example, 123-45-6789 to find an exact match.
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 ad preserved as a token that corresponds to the original search terms. By obfuscating the original search terms, potentially sensitive data is not displayed 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 displays as **Active**, click the endpoint name to investigate the files where matches occur.

Click the check box next to a file name and click **Find Similar Files** to see other computers in your enterprise that have the same file or similar files.

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.

Troubleshooting Reveal

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

Remediating "Needs Attention" messages from Reveal Status

Use the Reveal - Status sensor to query the status of Reveal on endpoints in an environment. From Tanium Interact, ask the question `Get Reveal - Status[*] from all machines`. The results grid provides detailed information regarding the status of Reveal, and tools that Reveal uses to discover sensitive data.

If the value of Reveal Status in the results grid displays as **Needs Attention** there are troubleshooting steps you can take to determine the cause, and to correct any issues that Reveal encounters. The following table describes situations that cause the value of the Reveal Status row in the results grid to display **Needs Attention** and corresponding corrective measures to take to resolve.

Possible reason	Steps for remediation
Files have been dropped from the Reveal database	It is possible that the maximum size allowed for the Reveal database has been exceeded, and as a result, files have been dropped. The `<Tanium Client>/Tools/Reveal/results/drop_latest.json` file contains detailed information. If this is the cause, you can increase the Maximum Database Size setting. See Endpoint configuration settings for more information.
A previous Reveal indexing pass might have ended with a failure	The `<Tanium Client>/Tools/Reveal/results/status.failed.json` file contains detailed information that is useful for troubleshooting. Additionally, `<Tanium Client>/Logs/extensions0.txt` contains useful information. For more information, see Contact Tanium Support on page 48.
There is no data from a previous Reveal indexing pass	It is possible that Reveal has not yet run on the endpoint. The Reveal Status value displays as **OK** when Reveal runs on the endpoint and results have been returned.
The latest data is stale	If there are Reveal results available, but they have not been updated in two hours, it indicates the Reveal process is not running even though it is installed. Verify that the endpoint is receiving the **Deploy Start Indexing** action. The Reveal Status value displays as **OK** when Reveal runs on the endpoint and results have been returned.

If you are unable to remediate a Reveal Status of **Needs Attention**, see Contact Tanium Support.

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 factor	Corrective action
Tools Not Deployed	Verify Tanium Clients are current and supported. For more information see Requirements: Tanium dependencies. 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. Use the **Index Resolved Config** sensor to see how Index combined any Index configuration files from all modules using Index.

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 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.
Recently updated rule not on desired endpoint(s) or the rule(s) or Reveal may not yet have had time to be processed.	After deploying a rule, it might take several hours to begin to see results. You might need to allow Reveal a couple more hours. If longer than a few hours has passed, you can ask the Tanium question “`Get Reveal - Background Scan Results[*] from all machines`”. In the results, look for the name of the rule you are troubleshooting. Use the Filter Text box to filter to just that rule. Select columns to display and add “Rule Revision”. Use Tanium to drill down to find out about any hosts with outdated rule.
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.

Contributing factor	Corrective action
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 - confirmed or rejected - of the rule. All similar snippets on all endpoints then show confirmed results. Rejected snippets no longer display 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 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.

Collect logs

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

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 `reveal-troubleshooting.zip` file downloads to the local download directory.
4. Attach the ZIP file to your Tanium Support case form or Contact Tanium Support.

Tanium Reveal maintains logging information in the `reveal.log` and `reveal-audit.log` files in the *<Module Server>*`\services\reveal-files\logs` directory.

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 computers 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 <OS> equals True`, for example:
   `Get Endpoint Configuration - Tools Status from all machines with Is Windows equals True`
2. In the results, select the row for **Reveal**, drill down as necessary, and select the targets from which you want to remove Reveal tools. For more information, see Tanium Interact User Guide: Managing question results.
3. Click **Deploy Action**.
4. On the **Deploy Action** page, enter `Endpoint Configuration - Uninstall` in the **Enter package name here** box, and 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 **Reveal**.
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 on an endpoint, you must deploy the **Endpoint Configuration - Unblock Tool [Windows]** or **Endpoint Configuration - Unblock Tool [Non-Windows]** package (depending on the targeted endpoints) before the tools can be reinstalled.
7. (Optional) To remove all Reveal databases and logs from the endpoints, clear the selection for **Soft uninstall**.
8. (Optional) To also remove any tools that were dependencies of the Reveal tools that are not dependencies for tools from other modules, select **Remove unreferenced dependencies**.
9. Click **Show preview to continue**.
10. A results grid displays 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, tool removal must be approved in Endpoint Configuration before tools are removed from endpoints.

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 https://support.tanium.com.

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.
- Binary files must be less than 32 MB. To increase the default size limit, update the **Maximum Size Non-Streamable File Formats** setting (from the Reveal **Overview** page, go to Settings and click **Endpoint Configuration**). Note that text files do not have a size limit.
- The file must not be filtered by the **Path Stem Exclusions** or **Path Filter Exclusions** settings (from the Reveal **Overview** page, click **Settings > Endpoint Configuration**).

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:

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
Microsoft Word	Binary	DOCM, DOCX, DOTM, DOTX, ODT
PDF	Binary	FDF, PDF
Structured text	Text	CSV, TSV, JSON, PRN, XML, DB (SQLite Databases)
Text	Text	TXT
Zip[1]	Binary	EAR, JAR, WAR, ZIP
Everything Else	Binary / Text	Any files with a MIME type that are not already contained in another category.

[1] If a rule only targets files in the Zip category, the rule matches all supported file types inside the supported archived files. If a rule does not target files in the Zip category, all files in archives are ignored.

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 Index. 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:

zip:

- application/zip
- application/vnd.openxmlformats-officedocument
- application/vnd.oasis.opendocument
- application/java-archive

xml:

- text/xml
- text/html
- application/vnd.oasis.opendocument

text:

- text*

sqlite:

- application/x-sqlite3

pdf:

- application/pdf
- application/x-pdf

csv:

- text/plain (also must match a file extension for “tabular” in definitions.json)

Reference: Reveal settings

To access Reveal settings from the Reveal **Overview** page, go to Settings and click **Settings**.

Reveal service settings

Setting	Default value	Description
Enable Sensitive Data Logging	false	Include search details and file paths in audit logs.
Rule Publication Interval	12 hours	The time interval to automatically deploy rule and rule sets assignments to endpoints.
Validation Publication Interval	30 minutes	The time interval to automatically deploy pending validations.
Rule Results Scan Interval	1800 seconds	The frequency to gather rule results metrics from endpoints.
Tools Deployment Distribute Over Time	1200 seconds	The time period to distribute tools to target endpoints.
Tools Deployment Reissue Interval	3600 seconds	The frequency to run the action to deploy tools.
Process Endpoint Distribute Over Time	1200 seconds	The time period to distribute indexing packages to target endpoints.
Process Endpoint Reissue Interval	3600 seconds	The frequency to run the action to index endpoints.
Live Connection Max Files	1000 files	Any files with a MIME type that are not already contained in another category.
Live Connection Max Snippets	1000 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 specific period.
Live Connection URL Scope	session	The security setting to share connection urls across users, scope them to the user, or to the users current session.
Rule Set Profile Distribute Over Time	1200 seconds	The time period to distribute rule set profiles to target endpoints.
Rule Set Profile Reissue Interval	3600 seconds	The frequency to run the action to deploy rule set profiles.
Rules Distribute Over Time	1200 seconds	The time period to distribute rules to target endpoints.

Setting	Default value	Description
Rules Profile Reissue Interval	3600 seconds	The frequency to run the action to deploy rules.
Validations Deployment Distribute Over Time	1200 seconds	The time period to distribute validations to target endpoints.
Validations Reissue Interval	3600 seconds	The frequency to run the action to deploy validations.
Package File Cache Timeout	300 seconds	The amount of time to wait for the Tanium Server to cache files for packages. Package and action creation fail if this timeout is exceeded.
Package Download Timeout	1800 seconds	The amount of time to allow for Reveal package to download before timing out.
Time Sync Frequency	10 minutes	How frequently to send out a time sync package.
Time Sync Distribute Over Time	1200 seconds	The time period to distribute the time sync to target endpoints.
Vocabulary Sampling Interval	600 seconds	The time period between when vocabulary sampling questions are sent out.
Decimation Schedule Automatic Deployment Interval	48 hours	How frequently the decimation schedule gets recreated.
Decimation Schedule Expiration Period	7 days	How long a decimation schedule is valid.
Global Vocabulary Decimation Threshold	50 percent	Global completion percentage to reach before decimating the global vocabulary.
Decimation Scheduler Horizon	21 days	How far into the future the decimation scheduler will attempt to predict.
Decimation Scheduler Growth Factor Gain	1 percent	Determines how much effect each sampling status has on the growth factor.
Decimation Scheduler Deploy Frequency	24 hours	The maximum amount of time allowed to pass before a new decimation schedule is deployed.
Decimation Scheduler Distribute Over Time	1200 seconds	The time period to distribute decimation scheduler to endpoints.
Decimation Schedule Reissue Interval	3600 seconds	How frequently the action to deploy the decimation schedule runs.

Endpoint configuration settings

Setting	Default value	Description
Path Filter Exclusions	none	Paths to exclude from parsing in regular expression format. For example: `.*\.docx` filters any files that end with the .docx file extension.
Path Stem Exclusions	none	Path stems represent absolute paths to exclude from parsing. For example: `C:\Program Files (x86)\Tanium\Tanium Client\` filters all content under `Tanium Client`.
Maximum File Batch Size	100000 files	The maximum files to process per index operation.
Maximum Text Content	1024 KB	The maximum amount of text content to extract per file.
Maximum Document Per DB Shard	10000 files	The maximum number of documents per database shard.
Maximum Database Size	1024 MB	The maximum size of the Reveal database.
Maximum Size Non-Streamable File Formats	32768 KB	The maximum size of non-streamable file formats to index.
Minimum Available Disk Space	2048 MB	The minimum amount of available disk space required to start an indexing operation.
Context Characters	100 characters	The number of characters to include on either side of a pattern hit.
Tanium Index Max Query Files	1000 files	The maximum number of files to request from Tanium Index at a time.
Max Files on Prune	10000 files	The maximum number of files to process per prune operation.
Minimum Document Frequency	5 documents	The minimum number of documents required to include a term in the global vocabulary.
(Internal) Vocabulary Sampling Exponent	-10	The vocabulary sampling rate.
(Internal) Vocabulary Builder Decimation Coefficient	.5	The decimation coefficient used by the vocabulary builder.

Index configuration settings

Setting	Default value	Description
Maximum CPU	3%	The maximum percentage of CPU that Tanium Index can use.
Rescan Interval	3600 seconds	The frequency that Tanium Index scans.
Exclude from Hashing	none	Regex paths to exclude from hashing.