Tanium™ Reveal User Guide

Version 1.18.194

August 01, 2022

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 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 and has most recently completed certification against the WCAG 2.1 / VPAT 2.3 standards for all major product modules in summer 2021. In the recent testing the Tanium Console UI achieved supports or partially supports for all applicable WCAG 2.1 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 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 Creating patterns on page 44.

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.

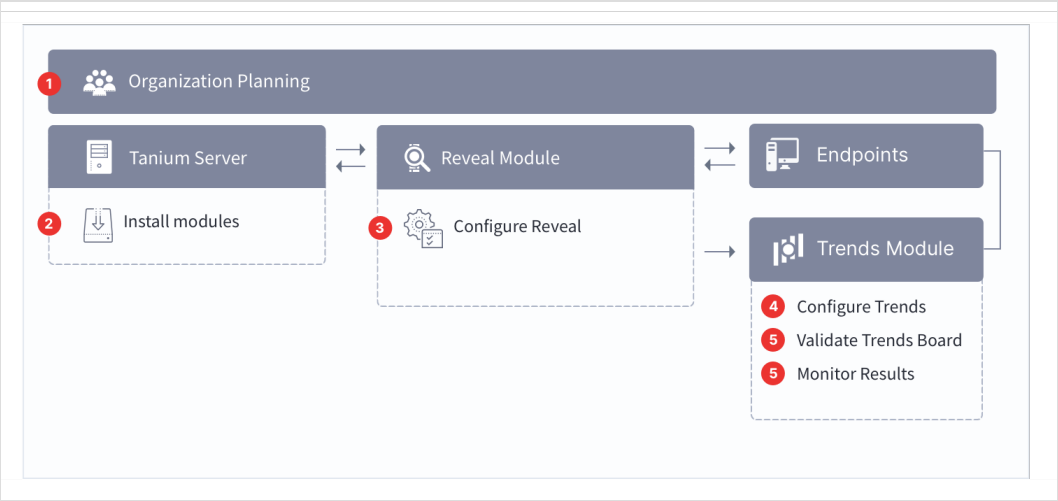
The **Reveal** board features visualizations that show the status of Reveal components on endpoints in an environment and provides visibility into any areas of Reveal that require remediation. Additionally, the **Reveal status** board shows real time and historical statistics concerning rule matches 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 30

☐ 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 Trends

☐ Open Trends and import the Reveal gallery. See Tanium Trends User Guide: Importing the initial gallery. If you installed Trends using the **Tanium Recommended Installation** workflow, the Reveal board is 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 **Tanium Recommended Installation** workflow, 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. See Create a rule set.

☐ Deploy rules. See Deploy rules.

Step 5: Monitor Reveal metrics

☐ From the Trends menu, click **Boards > Reveal**. Review the trending data in the **Reveal Coverage**, **Endpoints with Unconfirmed Sensitive Data**, and **Endpoints with Confirmed Sensitive Data** 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 discovering sensitive data on 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.

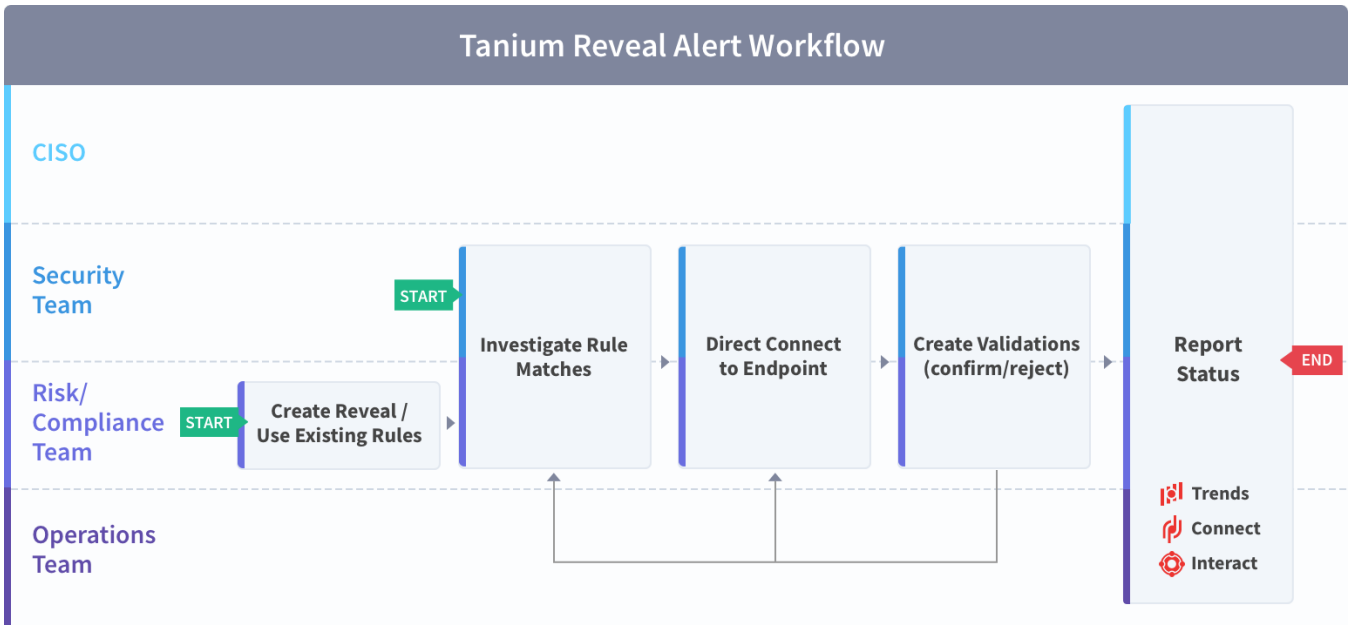
RACI chart

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.

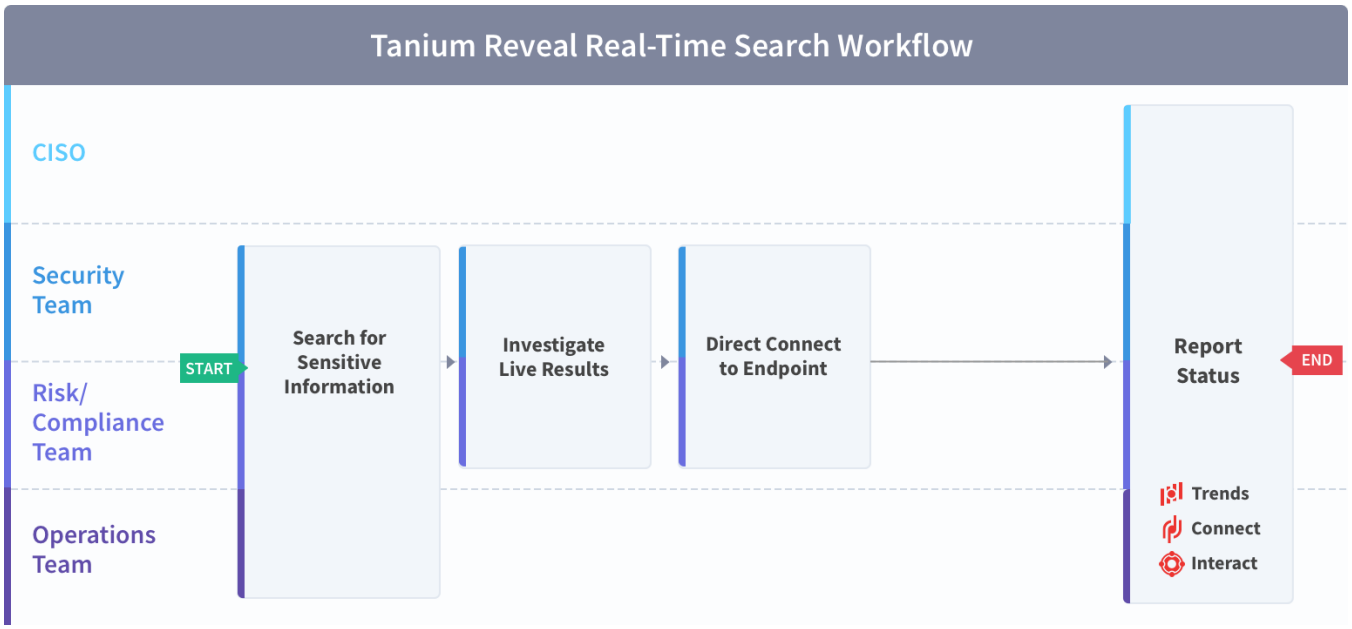
Task	IT Security	IT Operations	IT Risk/Compliance	Executive	Rationale
Determine which default rules to use or which custom rules to create	C	I	R/A	C	When Reveal is originally installed, there are default rules for PCI, HIPAA, GDPR, and CCPA. The Risk/Compliance team might have other items they need to 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 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.

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 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 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 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, Google Chronicle	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; 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.

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium license that includes Reveal
- Tanium™ Core Platform servers: 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.

Computer group dependencies

When you first sign in to the Tanium™ Console after a fresh installation of Tanium Server 7.4.2 or later, 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. See Tanium Console User Guide: Create a computer group.

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 19 and Reveal requirements on page 18. 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. See Tanium Console User Guide: Import all modules and services.

Import specific solutions

If you select only Reveal to import and are using Tanium Core Platform 7.5.2.3531 with Tanium Console 3.0.72 or later, 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.

If you select only Reveal to import and you are using Tanium Core Platform 7.5.2.3503 or earlier with Tanium Console 3.0.64 or earlier, you must manually import or update required dependencies. See Tanium Console User Guide: Import, re-import, or update specific solutions.

Required dependencies

Reveal has the following required dependencies at the specified minimum versions:

- Tanium™ Client Index Extension*
- Tanium™ Direct Connect 1.9.30 or later
- Tanium™ Endpoint Configuration 1.2 or later (installed as part of Tanium™ Client Management 1.5 or later)
- Tanium™ Interact 2.8.105 or later
- Tanium Trends 3.6.343 or later

Tanium™ Threat Response 3.4.346 or later is required if Threat Response exists in the same environment. Threat Response is not a required Reveal dependency.

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

Client extensions

Tanium Endpoint Configuration installs client extensions for Reveal on endpoints. Client Extensions perform tasks that are common to certain Tanium solutions. The Tanium Client uses code signatures to verify the integrity of each client extension prior to loading the extension on the endpoint. Each client extension has recommended security exclusions to allow the Tanium processes to run without interference. See Security exclusions for more information. The following client extensions perform Reveal functions:

- Core CX - Provides a management framework API for all other client extensions and exposes operating system metrics. Tanium Client Management installs this client extension.
- Config CX - Provides installation and configuration of extensions on endpoints. Tanium Client Management installs this client extension.
- DEC CX - Provides a direct connection between endpoint and Module Server. Tanium Direct Connect installs this client extension.

- Index CX - Provides the ability to index the local file systems on endpoints. Tanium Integrity Monitor, Tanium Reveal, or Tanium Threat Response installs this client extension.
- Py CX - Provides a library that enables communication between Python-based client extensions and Core CX. Tanium Integrity Monitor, Tanium Reveal, or Tanium Threat Response installs this client extension.
- Reveal CX - Provides distributed keyword and pattern searching capability against content on disk. Tanium Reveal installs this client extension.

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)

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	For Tanium Client operating system support, see Tanium Client Management User Guide: Client version and host system requirements

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

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

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.

Source	Destination	Port	Protocol	Purpose
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 security software is in use in the environment to monitor and block unknown host system processes, Tanium recommends that a security administrator create exclusions to allow the Tanium processes to run without interference. The configuration of these exclusions varies depending on AV software. For a list of all security exclusions to define across Tanium, see Tanium Core Platform Deployment Reference Guide: Host system security exclusions.

Reveal security exclusions

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 (continued)

Target Device	Notes	Exclusion Type	Exclusion
Windows endpoints		Process	*<Tanium Client>*\TaniumCX.exe
		File	*<Tanium Client>*\TaniumClientExtensions.dll
		File	*<Tanium Client>*\TaniumClientExtensions.dll.sig
		File	*<Tanium Client>*\extensions\TaniumReveal.dll
		File	*<Tanium Client>*\extensions\TaniumReveal.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\core\TaniumPythonCx.dll
		File	*<Tanium Client>*\extensions\core\TaniumPythonCx.dll.sig
	7.2.*x* clients, [1]	Process	*<Tanium Client>*\python27\TPython.exe
	7.2.*x* clients, [1]	Folder	*<Tanium Client>*\python27
	7.4.*x* clients, [1]	Process	*<Tanium Client>*\python38\TPython.exe
	7.4.*x* clients	Folder	*<Tanium Client>*\python38

Reveal security exclusions (continued)

Target Device	Notes	Exclusion Type	Exclusion
Linux endpoints		Process	*<Tanium Client>*/TaniumCX
		File	*<Tanium Client>*/libTaniumClientExtensions.so
		File	*<Tanium Client>*/libTaniumClientExtensions.so.sig
		File	*<Tanium Client>*/extensions/libTaniumReveal.so
		File	*<Tanium Client>*/extensions/libTaniumReveal.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/core/libTaniumPythonCx.so
		File	*<Tanium Client>*/extensions/core/libTaniumPythonCx.so.sig
	7.2.*x* clients	Process	*<Tanium Client>*/python27/python
	7.2.*x* clients	Folder	*<Tanium Client>*/python27
	7.4.*x* clients	Process	*<Tanium Client>*/python38/python
	7.4.*x* clients	Folder	*<Tanium Client>*/python38

Reveal security exclusions (continued)

Target Device	Notes	Exclusion Type	Exclusion
macOS endpoints		Process	*<Tanium Client>*/TaniumCX
		File	*<Tanium Client>*/libTaniumClientExtensions.dylib
		File	*<Tanium Client>*/libTaniumClientExtensions.dylib.sig
		File	*<Tanium Client>*/extensions/libTaniumReveal.dylib
		File	*<Tanium Client>*/extensions/libTaniumReveal.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/core/libTaniumPythonCx.dylib
		File	*<Tanium Client>*/extensions/core/libTaniumPythonCx.dylib.sig
	7.2.*x* clients	Process	*<Tanium Client>*/python27/python
	7.2.*x* clients	Folder	*<Tanium Client>*/python27
	7.4.*x* clients	Process	*<Tanium Client>*/python38/python
	7.4.*x* clients	Folder	*<Tanium Client>*/python38

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

User role requirements

The following tables list the role permissions required to use Reveal. To review a summary of the predefined roles, see Set up Reveal users on page 35.

For more information about role permissions and associated content sets, see Tanium Console User Guide: Managing RBAC.

Reveal user role permissions

Permission	Reveal Administrator[4]	Reveal Operator	Reveal Read Only User	Reveal Service Account[3]	Reveal User[1]	Reveal Endpoint Configuration Approver[2]
Reveal Provides access to the Reveal workbench and enables viewing of snippets of affected files.	✓ SNIPPETS SHOW	✓ SNIPPETS SHOW	✓ SHOW	✗	✓ SNIPPETS SHOW	✓ SHOW
Reveal Affected Enables viewing of affected files	✓ FILES	✓ FILES	✗	✗	✓ FILES	✗
Reveal API Perform Reveal operations using the API	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✗
Reveal Operator Settings Enables viewing, listing, and editing Reveal settings	✓ READ WRITE	✓ READ WRITE	✗	✗	✗	✗
Reveal Profiles Enables viewing, editing, and deploying profiles	✓ READ WRITE DEPLOY	✓ READ WRITE DEPLOY	✓ READ	✗	✓ READ WRITE DEPLOY	✗
Reveal Patterns Enables viewing and editing patterns	✓ READ WRITE	✓ READ WRITE	✓ READ	✗	✓ READ WRITE	✗

Reveal user role permissions (continued)

Permission	Reveal Administrator[4]	Reveal Operator	Reveal Read Only User	Reveal Service Account[3]	Reveal User[1]	Reveal Endpoint Configuration Approver[2]
Reveal Quick Enables viewing of quick search results	✓ SEARCH	✓ SEARCH	✗	✗	✓ SEARCH	✗
Reveal Rules Enables the viewing, listing, editing, and deploying of rules	✓ DEPLOY READ WRITE	✓ DEPLOY READ WRITE	✓ READ	✗	✓ DEPLOY READ WRITE	✓ READ
Reveal Rules Deploy Access to the Reveal workbench	✓ STATUS	✓ STATUS	✓ STATUS	✗	✓ STATUS	✗
Reveal Rule Sets Enables the viewing, listing, and editing of rule sets	✓ READ WRITE	✓ READ WRITE	✓ READ	✗	✓ READ WRITE	✓ READ
Reveal Service Enables a user to perform work as the service account user	✓ READ WRITE	✗	✓ READ	✓ USER	✗	✗
Reveal Validations Enables viewing, editing, listing, and deploying validations	✓ DEPLOY READ WRITE	✓ DEPLOY READ WRITE	✓ READ	✗	✓ DEPLOY READ WRITE	✓ READ
Reveal Validations Deploy Enables viewing of the status of validation deployments	✓ STATUS	✓ STATUS	✓ STATUS	✗	✓ STATUS	✗

Reveal user role permissions (continued)

Permission	Reveal Administrator[4]	Reveal Operator	Reveal Read Only User	Reveal Service Account[3]	Reveal User[1]	Reveal Endpoint Configuration Approver[2]
Reveal Settings Enables viewing, editing, and listing Reveal settings	✓ READ WRITE	✗	✗	✗	✗	✓ READ
Reveal Admin Perform administrative functions for the Reveal module	✓ ADMINISTRATOR	✗	✗	✗	✗	✗
Reveal Endpoint Configuration Enables approver privileges in Tanium Endpoint Configuration for Reveal configuration changes.	✗	✗	✗	✗	✗	✓ APPROVE

[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 enabled configuration approvals in Endpoint Configuration, then 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 the **Reveal Service Account** role and adding the relevant content sets. For more information, see Tanium Endpoint Configuration User Guide: User role requirements and Tanium Endpoint Configuration User Guide: Managing approvals.

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

Provided Reveal administration and platform content permissions

Permission	Permission Type	Reveal Administrator [1,2]	Reveal Operator	Reveal Endpoint Configuration Approver	Reveal User	Reveal Read Only User	Reveal Service Account
Action Group	Administration	✓ READ	✓ READ	✗	✓ READ	✓ READ	✓ READ
User	Administration	✓ READ	✗	✗	✗	✗	✗
Action	Platform Content	✓ READ WRITE	✓ READ WRITE	✗	✓ READ WRITE	✗	✓ READ WRITE
Filter Group	Platform Content	✓ READ	✓ READ	✗	✓ READ	✓ READ	✓ READ
Own Action	Platform Content	✓ READ	✓ READ	✗	✓ READ	✓ READ	✓ READ
Package	Platform Content	✓ READ WRITE	✓ READ WRITE	✗	✓ READ WRITE	✗	✓ READ WRITE
Plugin	Platform Content	✓ READ EXECUTE	✓ READ EXECUTE	✗	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE
Saved Question	Platform Content	✓ READ WRITE	✓ READ WRITE	✗	✓ READ WRITE	✓ READ	✓ READ
Sensor	Platform Content	✓ READ	✓ READ	✗	✓ READ	✓ READ	✓ READ

You can view which content sets are granted to any role in the Tanium Console.

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

[2] This role provides content set permissions for Tanium Direct Connect. You can view which Direct Connect content sets are granted to this role in the Tanium Console. For more information, see Tanium Direct Connect User Guide: User role requirements.

Installing Reveal

Use the Tanium Console **Solutions** page to install Reveal and choose either 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 Reveal with default settings on page 30.
- **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 31.

Before you begin

- Read the release notes.
- Review the Reveal requirements on page 18.
- If you are upgrading from a previous version, see Upgrade Reveal.
- Assign the correct roles to users for Reveal. Review the User role requirements on page 25.
    - 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 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

(Tanium Core Platform 7.4.5 or later only) 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: Dependencies, default settings, and tools deployment.

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

Setting	Default value
Action group	• Restricted targeting disabled (default): `All Computers` computer group • Restricted targeting enabled: `No Computers` computer group
Service account	The service account is set to the account that you used to import the module. Configuring a unique service account for each Tanium solution is an extra security measure to consider in consultation with the security team of your organization. See Configure service account on page 34.

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 32.

Import Reveal with custom settings

To import Reveal without automatically configuring default settings, be sure to clear the **Apply All Tanium recommended configurations** check box while performing the steps in Tanium Console User Guide: Import, re-import, or update specific solutions. After the import, verify that the correct version is installed: see Verify Reveal version on page 32.

To configure the service account, see Configure service account on page 34.

To configure the Reveal action group, see Configure the Reveal action group on page 34.

Manage solution dependencies

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

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 Troubleshooting Reveal: Collect logs.

For the steps to upgrade Reveal, see Tanium Console User Guide: Import, re-import, or update specific solutions. After the upgrade, verify that the correct version is installed: see Verify Reveal version on page 32.

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.

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 display version information, click Info  .

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 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 25.

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.

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 service account

The service account is a user that performs the following tasks for Reveal:

- Creates scheduled actions for automatic tools deployment and indexing
- Schedules automatic rules deployment
- Gathers stats and results

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

This user requires the following roles and access:

- **Tanium Administrator** or **Reveal Service Account** role.
- If you enabled configuration approvals in Endpoint Configuration, then 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 the **Reveal Service Account** role and adding the relevant content sets. For more information, see Tanium Endpoint Configuration User Guide: User role requirements and Tanium Endpoint Configuration User Guide: Managing approvals.

For more information about Reveal permissions, see User role requirements on page 25.

If you imported Reveal with default settings, the service account is set to the account that you used to perform the import. Configuring a unique service account for each Tanium solution is an extra security measure to consider in consultation with the security team of your organization.

1. On the Reveal **Overview** page, click Settings and then click **Service Account** if needed.
2. Provide a user name and password, and then click **Save**.

Configure the Reveal action group

Importing the Reveal module automatically creates an action group to target specific 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.

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.

To review specific permissions for each role, see User role requirements on page 25.

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

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
- 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

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.

Reveal Service Account

Assign the **Reveal Service Account** role to the account that configures system settings for Reveal.
This role can perform several background processes for Reveal.

(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 on these settings, 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 click **Deploy Scans**.
2. Select an operating system in the **Scan Specific Path (Reveal)** section to deploy the `Reveal - Index Path package` 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 on the parameters on this page, see Tanium Console User Guide: Deploying actions.

   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 on the parameters on this page, see Tanium Console User Guide: Deploying actions.

(Optional) Configure Reveal service settings

Configure settings to tune the Reveal service for your environment.

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

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

Setting	Default value	Description
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.
Rule Results Scan Interval	600 seconds	The frequency to gather rule results metrics from endpoints.
Status Scan Interval	600 seconds	The frequency to query the Reveal status from endpoints.
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 Files	1000 files	The maximum number of files retrieved from an endpoint.
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.
Package File Cache Timeout	300 seconds	The total 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 packages to download before timing out.
Time Sync Frequency	60 minutes	The frequency to send out a time sync package.
Time Sync Distribute Over Time	600 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.

Setting	Default value	Description
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.

3. Click **Save**.

Creating profiles

Create a profile to specify the Reveal endpoint configuration settings for groups of 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.

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.

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

Create a profile

1. From the Reveal menu, click **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 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.

   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 about Index subscriptions, 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 about these settings, see Tanium Client Index Extension User Guide: Overview and Tanium Client Index Extension User Guide: Customize Index endpoint settings.

6. In the **Reveal Settings** section, specify the endpoint settings as needed.
7. Click **Create**.

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

Prioritize profiles

If you have more than one profile, prioritize profiles to determine which profile applies to endpoints targeted by more than one profile. Zero (0) is the highest priority.

1. From the Reveal menu, click **Profiles**. 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 on deploying profiles to endpoints, see Deploy a profile.

Edit a profile

1. From the Reveal menu, click **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 on deploying profiles to endpoints, see Deploy a profile.

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 Reveal menu, click **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 Reveal menu, click **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.

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 keywords or regular expressions (regex).

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.

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 endpoints, based on the time configured in the **Rule Publication On Modify** setting. To immediately deploy updated rules, from the Main menu, click **Rules**, click **Deploy All Rule Sets**, enter your credentials, and click **OK**. For more information, see Deploy rules.

- To adjust the automatic update schedule, go to the **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/reveal-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, set the **Content Feed Update Interval Hours** to **0**. An **Upload Content** tab appears.
5. Click the **Upload Content** tab and drag and drop the content archive to the tab to upload it.

Create a regex pattern

Before you begin

- Use an online tutorial, such as RegEx101: RegEx101 Regex Quiz, to learn the Perl Compatible Regular Expressions (PCRE) syntax and style. For more information about PCRE, see PCRE: pcre2pattern
- Define the use case 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.

1. From the Reveal menu, go to **Patterns > Create Pattern > Regex Pattern**.
2. Specify a name for the pattern using only letters, numbers, spaces, dashes and underscores.
3. (Optional) Update the **Pattern ID**.
   The **Pattern ID** is automatically set to the same value as the **Name**. If you modify the pattern ID, use only lowercase letters [a-z], numbers, and underscores. IDs must be between 5-50 characters.
4. Provide a description for the pattern.
5. Specify a regular expression (PCRE syntax) to define the pattern for the data that you want to find in files.
6. (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.

   BEST PRACTICE 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.
7. Click **Create**.

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 Reveal menu, go to **Patterns > Create Pattern > Keyword Pattern**.
2. Enter a name for the pattern.
3. (Optional) Update the Pattern ID.
   The **Pattern ID** is automatically set to the same value as the **Name**. If you modify the pattern ID, use only lowercase letters [a-z], numbers, and underscores. IDs must be between 5-50 characters.
4. (Optional) Provide a description for the pattern.
5. 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 50 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.
6. Click **Create**.

Edit a pattern

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

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.

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

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, create and deploy a custom profile to update the **Maximum Size Non-Streamable File Formats** setting. Note that text files do not have a size limit. For more information, see Creating profiles.
- 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.

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 proximity group

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

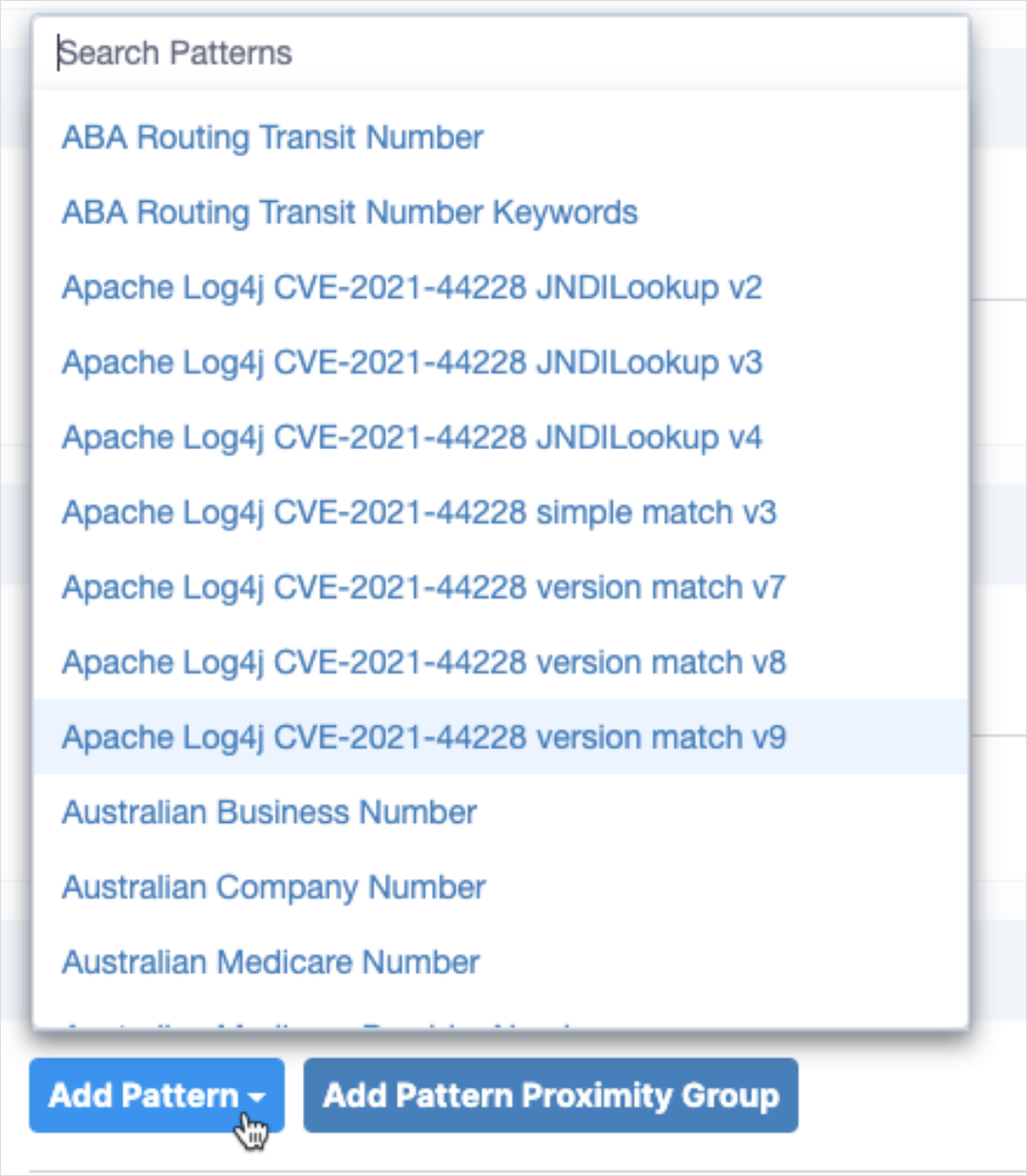
IMPORTANT

Patterns in a pattern proximity group are joined with an AND operator.

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 67.
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.



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 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, 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 .

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.

BEST PRACTICE

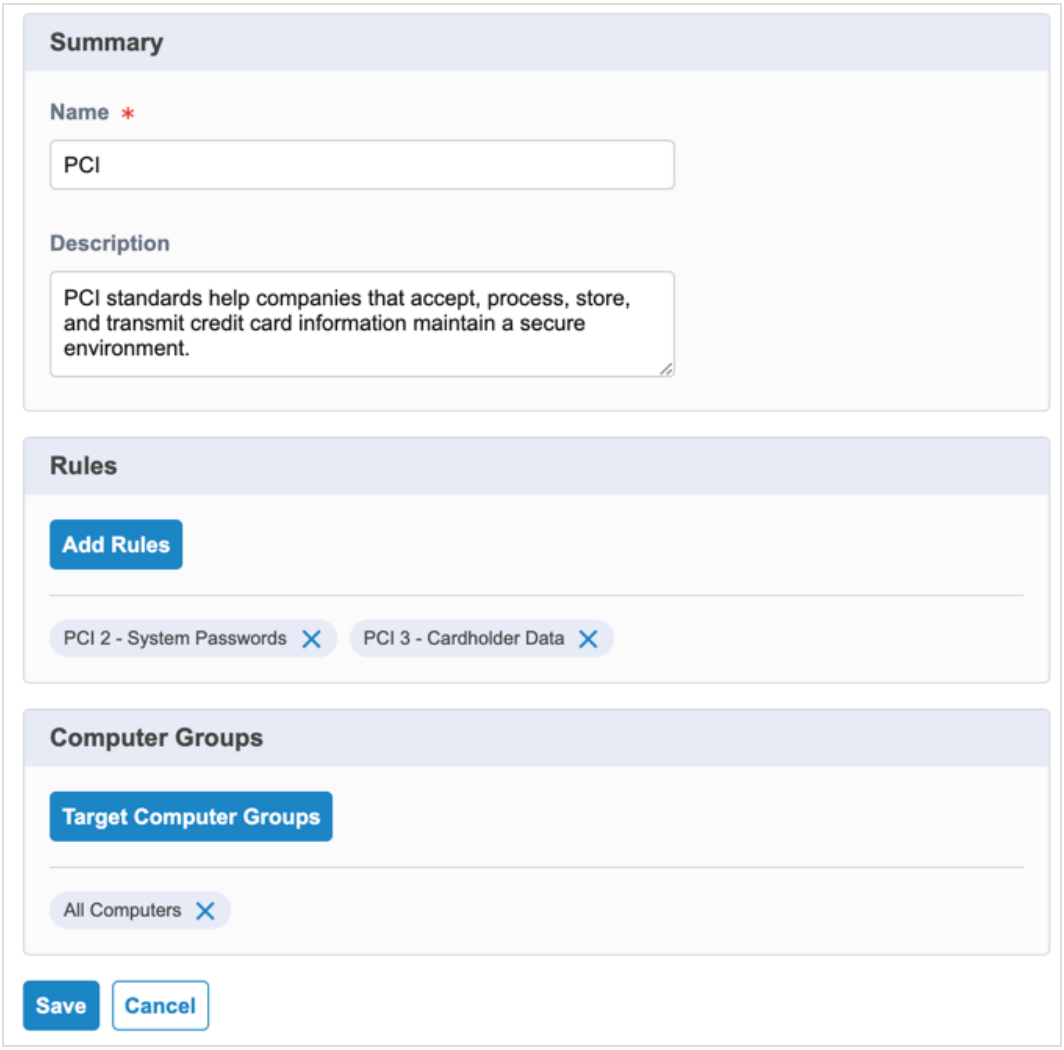
Test and verify rules before adding to rule sets.

NOTE

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.

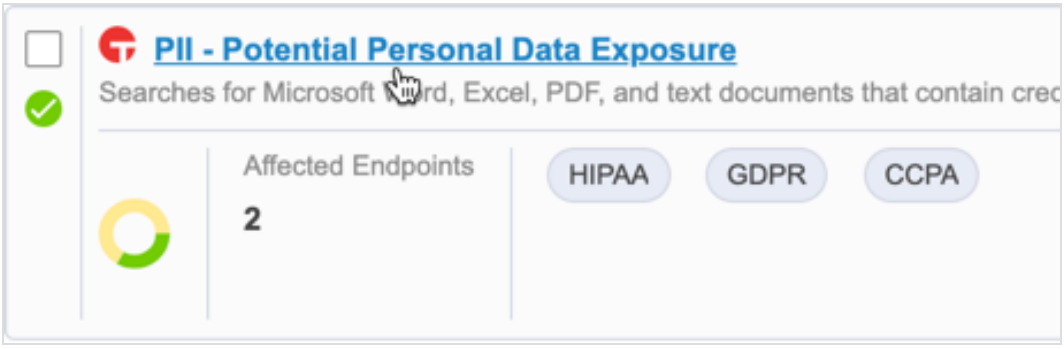
Investigating rule matches

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.

When validations have been confirmed or rejected, values in the **Unconfirmed hits** and **Confirmed hits** columns on the **Affected Files - <Computer Name>** page for any rule where patterns have been matched and validated display 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 display in black.

For more information about validations, see Validating pattern matches.

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 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 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.

If a matched rule uses a pattern proximity group, the pattern match is automatically validated. For more information about pattern proximity groups, see Creating rules.

Create a validation

1. From the Reveal menu, click **Rules**.
2. Click the rule name for 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 **Connect** .
4. After the connection establishes, click the computer name.
5. Click the **Filename** for the file that contains one or more pattern matches.
6. Review the snippets that show where a pattern matches. Confirmed and unverified snippets are shown by default. The text in the file that matches the pattern is highlighted. To limit which results display, click **Filter Results** to view or hide unverified, confirmed, rejected, and excluded snippets.

   NOTE

   Excluded snippets are unverified snippets 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 **Confirm** or **Reject**. 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 (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.

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 confirmed or rejected.
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 confirmed or rejected, values in the **Unconfirmed hits** and **Confirmed hits** columns on the **Affected Files - *<Computer Name>*** page for any rule where patterns have been matched and validated display 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 display in black.

Deploy validations

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

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

Collect logs

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

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.

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. To change this setting from the default value, create and deploy a custom profile. For more information, see Creating profiles.
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 66.

Possible reason	Steps for remediation
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.

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.

Contributing factor	Corrective action
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.
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.

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.

To review the client extensions that Reveal installs and uses, see Client extensions.

1. 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.

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

2. Target one or more endpoints with errors, and uninstall tools that report errors without blocking reinstallation: 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.

3. 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:

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. • 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: 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.
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.
Manually Blocked:`blocked`	The tool was previously blocked, either manually or during a previous uninstallation. Unblock the tool: see Endpoint Configuration User Guide: Block or unblock tools from installing on an endpoint.

4. Review the Extensions logs on the endpoint. Take note of entries that include `fail` or `error`: see Review the Extensions log for an endpoint on page 64.

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 **Administration > 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.

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`
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: 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 **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.

   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**.

   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.

   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**.

If you have enabled Endpoint Configuration approval, 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, create and deploy a custom profile to update the **Maximum Size Non-Streamable File Formats** setting. Note that text files do not have a size limit. For more information, see Creating profiles.
- 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.

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, 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 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:

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 endpoint settings

You can modify these Reveal endpoint settings by creating and deploying a profile. For more information, see Creating profiles. To update settings for the Reveal service, see Configure Reveal service settings.

Tanium Index subscription settings

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.

Reveal endpoint settings

Setting	Default value	Description

Reveal Parse Exclusions by Regular Expression	`.*\\Windows\\servicing\\.*`
	`.*\\Windows\\WinSxS\\.*`
	`.*\\Windows\\CSC\\.*`
	`.*\\Windows\\SoftwareDistribution\\Download\\.*`
	`.*\\ProgramData\\Microsoft\\Windows Defender\\Scans\\History\\.*`
	`.*\\Tanium\\Tanium Client\\.*`
		Paths to exclude from parsing in regular expression format. For example: `.*\.docx` filters any files that end with the .docx file extension.

Reveal Parse Exclusions by File Path	`/opt/Tanium/TaniumClient`
	`/Library/Tanium/TaniumClient`
	`/System/Volumes/Data/Library/Tanium/TaniumClient`
		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.

Setting	Default value	Description
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	150 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	100000 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.