Tanium™ Reveal User Guide

Version 1.4.2

March 31, 2020

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. To extend the list, contact your TAM for assistance.

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:

- Endpoint Status
- Scan Failure
- Data Size
- Dropped Files
- Unverified Matches
- Label Results

- Module Version
- Tools Version
- Applied Rule Sets

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

Getting started

1. Install and configure Tanium Reveal. For more information, see Installing Reveal on page 24.
2. Create rules. For more information, see Creating rules on page 27.
3. Create rule sets. For more information, see Creating rule sets on page 30.
4. Manage rule matches. For more information, see Investigating rule matches on page 33.
5. Create validations. For more information, see Validating pattern matches on page 35.
6. Search for sensitive information across the enterprise. For more information, see Searching across the enterprise on page 38.

Reveal requirements

Review the requirements before you install and use Reveal.

Tanium dependencies

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

Component	Requirement
Tanium™ Core Platform	7.2.314.2831 or later.
Tanium™ Client	7.2.314.3211 or later. 7.4.1.1955 or later are supported.
Tanium products	If you clicked the **Install with Recommended Configurations** button when you installed Reveal, the Tanium Server automatically installed all your licensed modules at the same time. Otherwise, you must manually install the modules that Reveal requires to function, as described under Tanium Console User Guide: Manage Tanium modules. The following products are required for features of Reveal to function. The given versions are the minimum required: • Tanium Index 2.4.0 or later. • Tanium Direct Connect 1.4.0 or later.
Computer groups	When you first log into the Tanium Console after installing the Tanium Server, the server automatically imports the computer groups that Reveal requires: • `All Computers` • `All Windows` • `All Mac` • `All Linux`

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

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

Tanium Module Server

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

Endpoints

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

Table 1: Supported operating systems

Operating system	OS version
Microsoft Windows Server	• Windows Server 2019 * • Windows Server 2016 * • Windows Server 2012, 2012 R2 • Windows Server 2008 R2 * Nano Server not supported.
Microsoft Windows Workstation	• Windows 10 • Windows 8 • Windows 7
macOS (Intel processor only)	• macOS 10.15 Catalina • macOS 10.14 Mojave • macOS 10.13 High Sierra • macOS 10.12 Sierra • OS X 10.11 El Capitan • OS X 10.10 Yosemite • OS X 10.9 Mavericks • OS X 10.8 Mountain Lion
Linux	Amazon Linux 2 LTS (2017.12)
	Debian 9.x, 8.x
	Oracle Enterprise Linux 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
	Ubuntu 18.04 LTS
	Ubuntu 16.04 LTS

Host and network security requirements

Specific ports and processes are needed to run Reveal.

Ports

The following ports are required for Reveal communication.

Component	Port	Direction	Purpose
Module Server	17475	Inbound	Connecting to the Module Server for direct connections to endpoints.
Zone Server*	17486	Inbound	The binding port that is used by the Zone Server for endpoint connections. The default port number is 17486. If needed, you can specify a different port number when you configure the Zone Proxy.
	17487	Inbound	The binding port that is 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	Inbound	The Direct Connect Zone Proxy installer automatically opens port 17488 on the Zone Server to allow communication between the Zone Server and the Module Server.
*These ports are required only when you use a Zone Server.			

Security exclusions

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

Table 2: Reveal security exclusions

Target Device	Process
Module Server	*<Tanium Module Server>*\services\reveal-service\node.exe

Target Device	Process
Windows endpoints	*<Tanium Client>*\TaniumCX.exe
	<Tanium Client>\Tools\EPI\TaniumExecWrapper.exe
	<Tanium Client>\Tools\EPI\TaniumEndpointIndex.exe
	<Tanium Client>\Tools\Reveal\TaniumReveal.exe
	<Tanium Client>\TaniumClientExtensions.dll
	<Tanium Client>\TaniumClientExtensions.dll.sig
	<Tanium Client>\extensions\RevealCX.dll
	<Tanium Client>\extensions\RevealCX.dll.sig
	<Tanium Client>\extensions\TaniumDEC.dll
	<Tanium Client>\extensions\TaniumDEC.dll.sig
	<Tanium Client>\extensions\core\libTaniumPythonCx.dll
	<Tanium Client> \extensions\core\libTaniumPythonCx.dll.sig
	<Tanium Client>\Python27\TPython.exe(7.2.x clients)
	<Tanium Client>\Python38\TPython.exe(7.4.x clients)
	<Tanium Client>\Python38*.dll(7.2.x clients)

Target Device	Process
Linux/macOS endpoints	*<Tanium Client>*/TaniumCX

Target Device	Process
	<Tanium Client>/Tools/EPI/TaniumExecWrapper

Target Device	Process
	<Tanium Client>/Tools/EPI/TaniumEndpointIndex

Target Device	Process
	<Tanium Client>/Tools/Reveal/TaniumReveal

Target Device	Process
	<Tanium Client>/libTaniumClientExtensions.so (Linux)

Target Device	Process
	<Tanium Client>/libTaniumClientExtensions.so.sig(Linux)

Target Device	Process
	<Tanium Client>/extensions/libRevealCX.so(Linux)
	<Tanium Client>/extensions/libRevealCX.so.sig (Linux)
	<Tanium Client>/extensions/libTaniumDEC.so(Linux)
	<Tanium Client>/extensions/libTaniumDEC.so.sig (Linux)
	<Tanium Client>/extensions//core/libTaniumPythonCx.so (Linux)
	<Tanium Client> /extensions/core/libTaniumPythonCx.so.sig(Linux)
	<Tanium Client>/libTaniumClientExtensions.dylib (macOS)
	<Tanium Client>/libTaniumClientExtensions.dylib.sig (macOS)
	<Tanium Client>/extensions/libRevealCX.dylib (macOS)
	<Tanium Client>/extensions/libRevealCX.dylib.sig(macOS)
	<Tanium Client>/extensions/libTaniumDEC.dylib (macOS)
	<Tanium Client>/extensions/libTaniumDEC.dylib.sig (macOS)
	<Tanium Client>/extensions/core/libTaniumPythonCx.dylib (macOS)
	<Tanium Client> /extensions/core/libTaniumPythonCx.dylib.sig (macOS)
	<Tanium Client>/python27/python(7.2.x clients)
	<Tanium Client>/python38/python(7.4.x clients)

User role requirements

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

Table 3: Tanium Reveal User Role Privileges

Permission	Reveal Administrator	Reveal Read Only User	Reveal Service Account	Reveal User
Show Reveal Access to the Reveal workbench	✓	✓	✗	✓
Reveal Affected Files Enables viewing of affected files	✓	✗	✗	✓
Reveal Quick Search Enables viewing of quick search results	✓	✗	✗	✓
Reveal Rules Deploy Enables the deployment of rules to endpoints	✓	✗	✗	✓
Reveal Rules Deploy Status Access to the Reveal workbench	✓[1]	✓	✗	✓[1]
Reveal Rules Read Enables the viewing and listing of rules	✓[1]	✓	✗	✓[1]
Reveal Rules Write Enables the editing of rules	✓	✗	✗	✓

Permission	Reveal Administrator	Reveal Read Only User	Reveal Service Account	Reveal User
Reveal Rule Sets Read Enables the viewing and listing of rule sets	✓[1]	✓	✗	✓[1]
Reveal Rule Sets Write Enables the editing of rule sets	✓	✗	✗	✓
Reveal Service User Enables a user to perform work as the service account user	✗	✗	✓	✗
Reveal Service User Read Allows viewing details of the service account user	✓[1]	✓	✗	✓
Reveal Service User Write Enables modifications to the service user account	✓	✗	✗	✗
Reveal Snippets Enables viewing of snippets of affected files.	✓	✗	✗	✓
Reveal Use API Perform Reveal operations using the API	✓[1]	✓[1]	✓[1]	✓[1]
Reveal Validations Deploy Enables the deployment of validations to endpoints	✓	✗	✗	✓

Permission	Reveal Administrator	Reveal Read Only User	Reveal Service Account	Reveal User
Reveal Validations Deploy Status Enables viewing of the status of validation deployments	✓[1]	✓	✗	✓[1]
Reveal Validations Read Enables viewing and listing of validations	✓[1]	✓	✗	✓[1]
Reveal Validations Write Enables the editing of validations	✓	✗	✗	✓
Reveal Settings Read Enables viewing and listing Reveal settings	✓[1]	✗	✗	✗
Reveal Settings Write Enables the editing of Reveal settings	✓	✗	✗	✗

[1] Denotes a provided permission.

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

Installing Reveal

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

- **Automatic configuration with default settings** (Tanium Core Platform 7.4.2 or later only): Reveal is installed with any required dependencies and other selected products. After installation, the Tanium Server automatically configures the recommended default settings. This option is the best practice for most deployments. For details about the automatic configuration for Reveal, see Import and configure Reveal with default settings on page 24.
- **Manual configuration with custom settings**: After installing Reveal, you must manually configure required settings. Select this option only if Reveal requires settings that differ from the recommended default settings. For more information, see Import and configure Reveal with custom settings on page 24.

Before you begin

- Read the Release Notes.
- Review the Reveal requirements on page 10.

Import and configure Reveal with default settings

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

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

To import Reveal and configure default settings, be sure to select the **Apply Tanium recommended configurations** check box while performing the steps under Tanium Console User Guide: Manage Tanium modules. After the import, verify that the correct version is installed: see Verify Reveal version on page 26.

Import and configure Reveal with custom settings

To import Reveal without automatically configuring default settings, be sure to clear the **Apply Tanium recommended configurations** check box while performing the steps under Tanium Console User Guide: Manage Tanium modules. After the import, verify that the correct version is installed: see Verify Reveal version on page 26.

Configure service account

The service account performs the following tasks for Reveal:

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

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

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

- **Tanium Administrator** or **Reveal Service Account** role

For more information about Reveal permissions, see User role requirements on page 21.

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

Configure Reveal action group

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

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

Upgrade the Reveal version

Upgrade Reveal to the latest version from the Solutions page.

1. From the Main menu, click **Tanium Solutions**.
2. Locate Reveal and click **Upgrade to X.X.X.XXXX**.
3. Click **OK**.
   The Import Solution window opens with a list of all the changes and import options.
4. Click **Proceed with Import** and enter your password.
   The installation and configuration process begins.

5. To confirm the upgrade, return to the **Tanium Solutions** page and check the **Installed: X.X.X.XXXX** version for Reveal.

> **Tip:** If the Reveal version does not update, refresh your browser window.

Verify Reveal version

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

1. Refresh your browser.
2. From the Main menu, click **Reveal** to open the Reveal **Home** page.
3. To display version information, click Info .

What to do next

See Getting started on page 9 for more information about using Reveal.

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.

Criteria for rule evaluation

See Reference: Supported file types for rule evaluation on page 43.

Rule conditions

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

Filter

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

Pattern

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

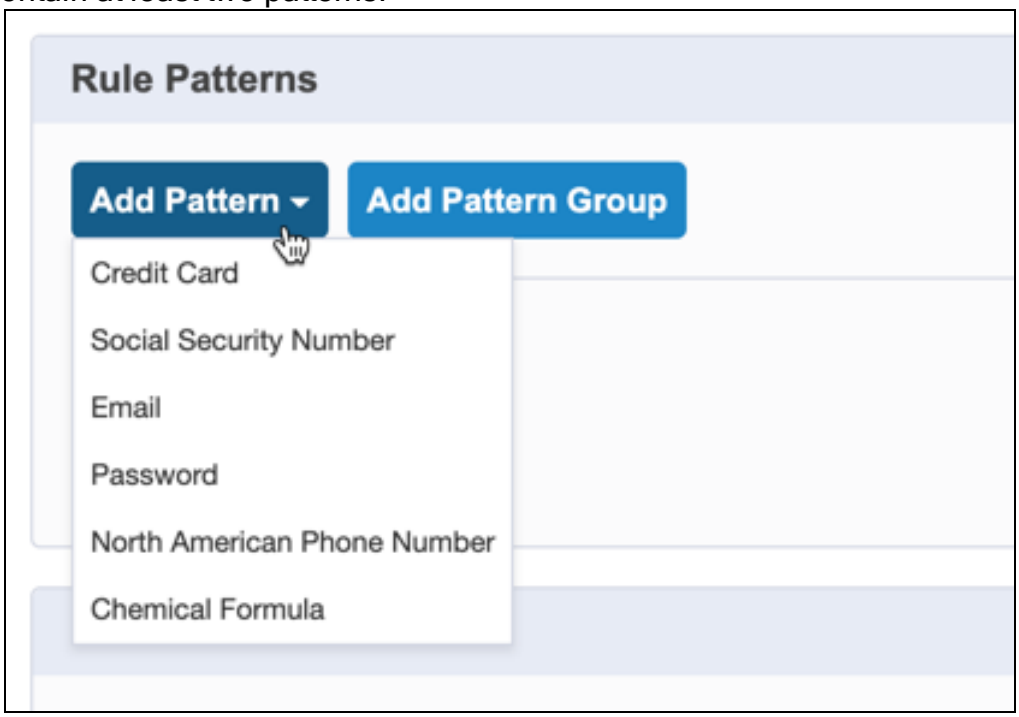
Pattern group

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

Create a rule

1. From the Reveal menu, click **Rules**. Click **Create Rule**.
2. Enter a name and description for the rule.

3. Select one or more rule sets to contain the rule. Click **Add Rule Sets** and select the rule sets you want to associate with the rule. Click **Assign**.
4. [Optional] Add filters to limit the files to target. Under **Rule Filters**, click **Add Filter** and select the criteria that you want the rule to cover. Repeat to add another filter. For a list of file types, see Reference: Supported file types for rule evaluation on page 43.
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. Repeat to add another pattern.
   - To add a proximal pattern match, click **Add Pattern Group**. A rule can contain one pattern group.
     1. For **Proximity**, select the maximum number of characters that the patterns can be from each other.
     2. In the pattern group, click **Add Pattern** and select a pattern to include in the match. Repeat to add a second pattern. A pattern group must contain at least two patterns.



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

"password", Reveal creates five rule matches: four for the email addresses and one for the word "password".

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

Deploy rules

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

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

> **Note:** You can also deploy rules from the **Rule Sets** page and from the **Deploy Rules** configuration step on the Reveal home page.

Customize rule patterns

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

> **IMPORTANT:** Only make customizations to rule patterns under the guidance of your TAM. To be effective, rule patterns must be developed methodically and tested exhaustively.

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

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

Creating rule sets

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

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

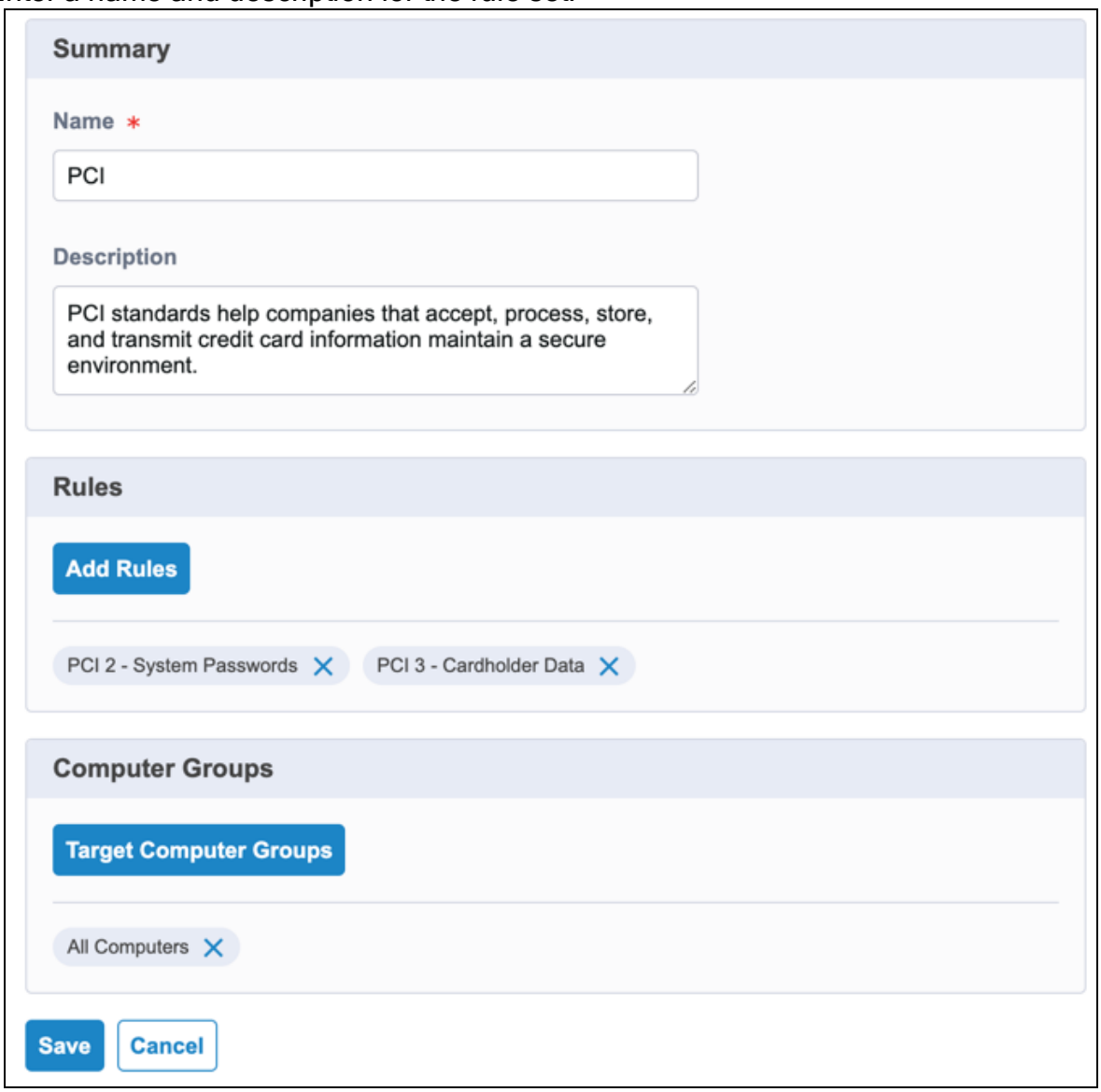
You can view the number of rules that are assigned to each rule set, the computer groups that it targets, and whether there are any pending changes to any of the associated rules.

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

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.

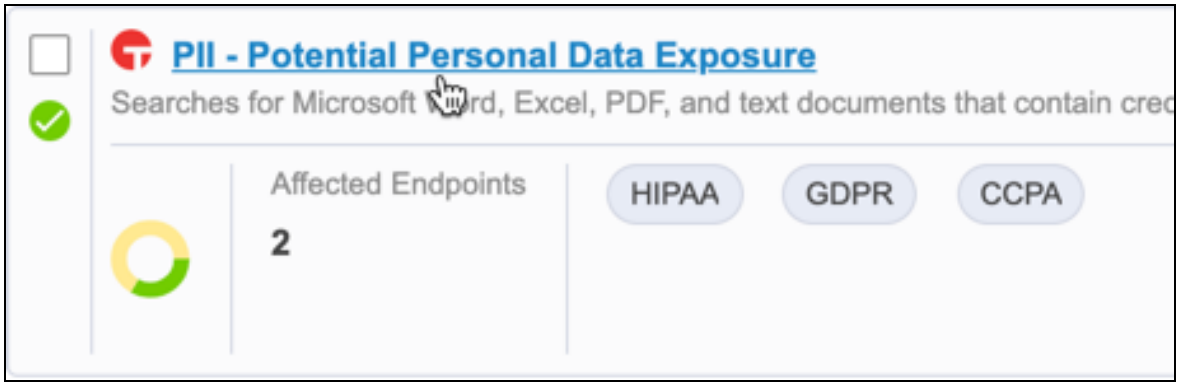
Investigating rule matches

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 an endpoint and click **Connect**. A live connection is opened to the endpoint. When the endpoint connection state displays as **Active**, click the endpoint name to view files that contain matches.

5. For files where matches have occurred, the file name, number of hits, and path are displayed.
6. Click an affected file to view snippets that show pattern matches in context.

Take action on files where rule matches occur

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

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

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

Validating pattern matches

Create validations to improve the accuracy of rule performance and to reduce the number of false positive results on the data that rules target. Validate rules to ensure that pattern matches are accurate and consistent in the targeted data. By validating rules, you can focus any analysis of data on results that have been confirmed or rejected as relevant pattern matches.

Validations apply to pattern matches in the context of a rule where the text appears exactly as it does in the validation. New validations display in a pending state, and are only visible to the user who created them. Pending validations automatically apply to snippet results, but do not affect rule hit counts until they are published.

Create a validation

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

   Note: Excluded snippets are unverified snippets that do not match patterns exactly. This includes matches to pattern groups outside the proximity range. You can confirm or reject an excluded snippet.
6. For each snippet, highlight the relevant text. Validations are tracked relative to the beginning of the match. Unicode and ASCII control characters - with the exception of tab, carriage return (CR) and line feed (LF) - are not supported in validation text. This includes Unicode characters U+0000 through U+0008, U+000B through U+000C, U+000E, and U+000F. If you select validation text that contains unsupported control characters, an error displays in the **Create Validation** page.
7. Select **Confirm** or **Reject**. Rejected snippets are filtered from future results.

   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. Reveal displays a preview of the text you have validated 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** at the top of the page to create validations in the next file on the endpoint where patterns have been matched.

When validations have been confirmed or rejected, values in the affected files view for any rule where patterns have been matched and validated display in orange in the **Unconfirmed hits** and **Confirmed hits** columns. Orange indicates that the data is "stale"; meaning that new validation data exists. If a file is designated as stale, it is prioritized for rescanning. When no new validation data exists, the values display in black.

Deploy validations

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

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

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

Audit published validations

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

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

5. Click a file to view snippets that match the validation.

Searching across the enterprise

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

Reveal converts search strings to lowercase, removes punctuation, and removes common stop words, such as articles. Reveal then searches for the exact sequence of tokens across the environment. For example, if a search query is `process is started`, this is tokenized as `["process","started"]`. These tokens match `the malicious process has started` , but not `started the process` because the tokens are not in the same order as the query.

Perform a quick search

1. From the Reveal menu, click **Quick Search**.
2. In the search field, provide a literal search string. 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**.

Investigate quick search results

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

> **Tip:** 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.

> **Note:** Both the quick search query and the searchable data are encrypted with a one way hash. Hashing occurs before the query is distributed to endpoints, and unencrypted queries and results are not persisted. The query is retained in the browser during the search workflow only. When results snippets are requested, the file is read on demand on the endpoint, and results are returned directly to Reveal.

Reveal does not write any unencrypted file content to disk, and no unencrypted query or result is ever sent as Tanium content.

Troubleshooting Reveal

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

Remediating "Needs Attention" messages from Reveal Status

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

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

Possible reason	Steps for remediation
Files have been dropped from the Reveal database	It is possible that the maximum size allowed for the Reveal database has been exceeded, and as a result, files have been dropped. The <*Tanium Client*>/Tools/Reveal/results/drop_latest.json file contains detailed information. If this is the cause, you can increase the Maximum Database Size setting. See Endpoint configuration settings for more information.
A previous Reveal indexing pass might have ended with a failure	The <*Tanium Client*>/Tools/Reveal/results/status.failed.json file contains detailed information that is useful for troubleshooting. Additionally, the <*Tanium Client*>/Tools/Reveal/log/reveal.index.log and <*Tanium Client*>/Tools/Reveal/log/reveal.log contain useful information. You can provide these files to your TAM for help determining the need for attention.
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.

Possible reason	Steps for remediation
The latest data is stale	If there are Reveal results available, but they have not been updated in two hours, it indicates the Reveal process is not running even though it is installed. Verify that the endpoint is receiving the **Deploy Start Indexing** action. The Reveal Status value displays as **OK** when Reveal runs on the endpoint and results have been returned.

If you are unable to remediate a Reveal Status of **Needs Attention**, contact your TAM.

Collect logs

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

1. From the Reveal **Home** 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 send it to your TAM.

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

Uninstall Reveal

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

1. From the Tanium Console, click **Solutions**.
   The **Solutions** page opens.
2. Locate Reveal, and then click **Uninstall**.
   The Uninstall window opens, showing the list of contents to be removed.
3. Click **Proceed with Uninstall**.
4. Enter your password to start the uninstall process.
   A progress bar displays as the installation package is removed.
5. Click **Close**.
6. To confirm, return to the **Solutions** page and check that the **Import** button is available.

Tip: If the Reveal module has not updated in the console, refresh your browser.

Reference: Supported file types for rule evaluation

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

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

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

Category	Format	File types
Configuration	Text	CFG, CONF, INI, YAML
Microsoft Excel	Binary	ODS, XLAM, XLSM, XLSX, XLTM, XLTX
Microsoft PowerPoint	Binary	ODP, POTM, POTX, PPA, PPSM, PPSX, PPTM, PPTX
Microsoft Word	Binary	DOCM, DOCX, DOTM, DOTX, ODT
PDF	Binary	FDF, PDF
Structured text	Text	CSV, JSON, PRN, XML
Text	Text	TXT
Zip[1]	Binary	EAR, JAR, WAR, ZIP
Everything Else	Binary / Text	Any files with a MIME type that are not already contained in another category.

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

Reveal can read files in any of the supported file types, regardless of the file extension. If you do not specify a file type filter for a rule, the rule attempts to read all files that are

hashed by Tanium Index. When you assign a file type to a rule, the rule only attempts to read files with the listed file extensions.

Reference: Reveal settings

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

> **IMPORTANT:** Consult with your Technical Account Manager (TAM) before you edit any settings in Reveal.

Reveal service settings

Setting	Default value	Description
Log Level	info	The log level for the Reveal service.
Enable Sensitive Data Logging	false	Include search details and file paths in audit logs.
Rule Publication Interval	12 hours	The time interval to automatically deploy rule and rule sets assignments to endpoints.
Validation Publication Interval	30 minutes	The time interval to automatically deploy pending validations.
Rule Results Scan Interval	1800 seconds	The frequency to gather rule results metrics from endpoints.
Tools Deployment Distribute Over Time	1200 seconds	The time period to distribute tools to target endpoints.
Tools Deployment Reissue Interval	3600 seconds	The frequency to run the action to deploy tools.
Process Endpoint Distribute Over Time	1200 seconds	The time period to distribute indexing packages to target endpoints.
Process Endpoint Reissue Interval	3600 seconds	The frequency to run the action to index endpoints.
Live Connection Max Files	1000 files	Any files with a MIME type that are not already contained in another category.
Live Connection Max Snippets	1000 snippets	The maximum number of snippets retrieved from a file from an endpoint.
Live Connection Page Expiration	60 minutes	The security setting to expire URLs after the specific period.

Setting	Default value	Description
Live Connection URL Scope	session	The security setting to share connection urls across users, scope them to the user, or to the users current session.
Rule Set Profile Distribute Over Time	1200 seconds	The time period to distribute rule set profiles to target endpoints.
Rule Set Profile Reissue Interval	3600 seconds	The frequency to run the action to deploy rule set profiles.
Rules Distribute Over Time	1200 seconds	The time period to distribute rules to target endpoints.
Rules Profile Reissue Interval	3600 seconds	The frequency to run the action to deploy rules.
Validations Deployment Distribute Over Time	1200 seconds	The time period to distribute validations to target endpoints.
Validations Reissue Interval	3600 seconds	The frequency to run the action to deploy validations.
Package File Cache Timeout	300 seconds	The amount of time to wait for the Tanium Server to cache files for packages. Package and action creation fail if this timeout is exceeded.
Package Download Timeout	1800 seconds	The amount of time to allow for Reveal package to download before timing out.

Endpoint configuration settings

Setting	Default value	Description
Log Level	info	The log level for Reveal endpoint tools.
Path Filter Exclusions	none	Paths to exclude from parsing, in regular expressions.
Path Stem Exclusions	none	Path stems to exclude from parsing.
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 CPU	3%	The maximum percentage of CPU to use.
Maximum Document Per DB Shard	10000 files	The maximum number of documents per database shard.

Setting	Default value	Description
Maximum Database Size	1024 MB	The maximum size of the Reveal database.
Maximum Size Non-Streamable File Formats	32768 KB	The maximum size of non-streamable file formats to index.
Minimum Available Disk Space	2048 MB	The minimum amount of available disk space required to start an indexing operation.
Context Characters	100 characters	The number of characters to include on either side of a pattern hit.
Tanium Index Max Query Files	1000 files	The maximum number of files to request from Tanium Index at a time.
Max Files on Prune	10000 files	The maximum number of files to process per prune operation.
Minimum Document Frequency	5 documents	The minimum number of documents required to include a term in the global vocabulary.
(Internal) Vocabulary Sampling Exponent	-10	The vocabulary sampling rate.
(Internal) Vocabulary Builder Decimation Coefficient	.5	The decimation coefficient used by the vocabulary builder.

Index configuration settings

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