# Tanium™ Event Recorder User Guide

Version 1.0.0

March 05, 2019

*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.*

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

# 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 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.

# Getting started

1. Install Tanium Reveal. For more information, see Installing Reveal on page 10.
2. Create rules. For more information, see Creating rules on page 12.
3. Create rule sets. For more information, see Creating rule sets on page 14.
4. Manage rule matches. For more information, see Investigating rule matches on page 16.

# 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 |
|---|---|
| Platform | 7.2.314.2831 or later |
| Tanium Client | 6.0.314.1540 or later recommended |
| Tanium Module | Tanium™ Trace 2.7.7 |

## Tanium Module Server

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

## Endpoints

Reveal supports Windows and macOS endpoints. Up to 2 GB of free disk space is required.

## 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 | 17444 | Inbound | Connecting to the Module Server for live connections to endpoints. |

### 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.

| Target Device | Process |
| --- | --- |
| Module Server | `<Tanium Module Server>\services\ProductName\node.exe` |
| Endpoint computers | `<Tanium Client>\Tools\EPI\TaniumExecWrapper.exe`<br>`<Tanium Client>\Tools\EPI\TaniumEndpointIndex.exe`<br>`<Tanium Client>\Tools\Reveal\win32\TaniumReveal.exe` |

## User role requirements

The **Trace Live Connections Write** permission is required for any user to make direct connections to endpoints to investigate rule matches.

# Installing Reveal

You can install Reveal from the **Tanium Solutions** page.

## Before you begin

- Read the release notes.
- Review the Requirements.

> **Note:** Tanium Trace is required to use Reveal. Make sure that you have installed Trace. For more information see Installing Trace.

## Import Reveal

Import Reveal from the **Tanium Solutions** page.

1. From the Main Menu, click **Tanium Solutions**.
2. Under **Tanium Reveal**, click **Import**.

   > **Note:** Tanium Reveal is a licensed solution. If Tanium Reveal is not on the **Tanium Solutions** page, contact your Technical Account Manager.

3. In the **Content Import Preview** window, you can expand the package to review the Tanium content that is being installed. Click **Proceed with Import**.
4. After the installation process completes, refresh your browser.
5. From the Main Menu, click **Reveal**. The Reveal home page is displayed.

## Verify installation

To verify that Reveal is installed, go to the Tanium Solutions page and check the installed version. To check the installed version on the Reveal home page, click Info .

## Set up Reveal

### Configure service account

The service account is used to create recurring maintenance activities for Reveal.

1. From the Reveal home page, click **Configure Service Account**.
2. Enter a user name and password.
3. Click **Set Credentials**.

**Note:** Configuring the service account installs Reveal tooling on the endpoints and starts the Reveal service. After deploying the tools for the first time, endpoints can take up to four hours to display status.

### 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. Click the **Reveal** action group, then click **Edit**.
3. Select the computer group for the group of endpoints that you want to use for Reveal. 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.XX**.
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.XX** version for Reveal.

**Tip:** If the Reveal version is not updated, refresh your browser window.

## What to do next

See Getting started on page 7 for more information about using Reveal.

# Creating rules

## Overview

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

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

- Be included in an inventory by Tanium Index.
- Be less than 32MB in size. To increase this default size limit, update both config.json for Reveal and config.ini for Tanium Index. For more information on updating config.ini, see Indexing file systems. To reduce this default size limit, it is only necessary to update config.json.
- Be one of the following file types: .doc, .ppt, .log, .rtf, .txt, .csv, .ppt, .xml, .xls, .html, .dev
- Be able to be compressed.

## Create a rule

1. From the Reveal menu, click **Rules**. Click **New Rule**.
2. Enter a name and description for the rule.
3. Select one or more rule sets to contain the rule. Click **Add Rule Set** and select the rule sets you want to associate with the rule. Click **Save**.
4. Add conditions. Conditions include file types and patterns. Click **Add Condition** and select either **File Type** or **Pattern**.
    1. For file type conditions, select the types of files that you want the rule to cover. If you do not select at least one file type, rules do not evaluate.
    2. For Patterns, select the pattern to match.
5. Select the Actions that the rule performs when the conditions have been matched. You can select to apply a label to the files that contain the match.
6. 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 ones. Click **Deploy Rules** to deploy the updated rules immediately.

# Creating rule sets

## Overview

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.

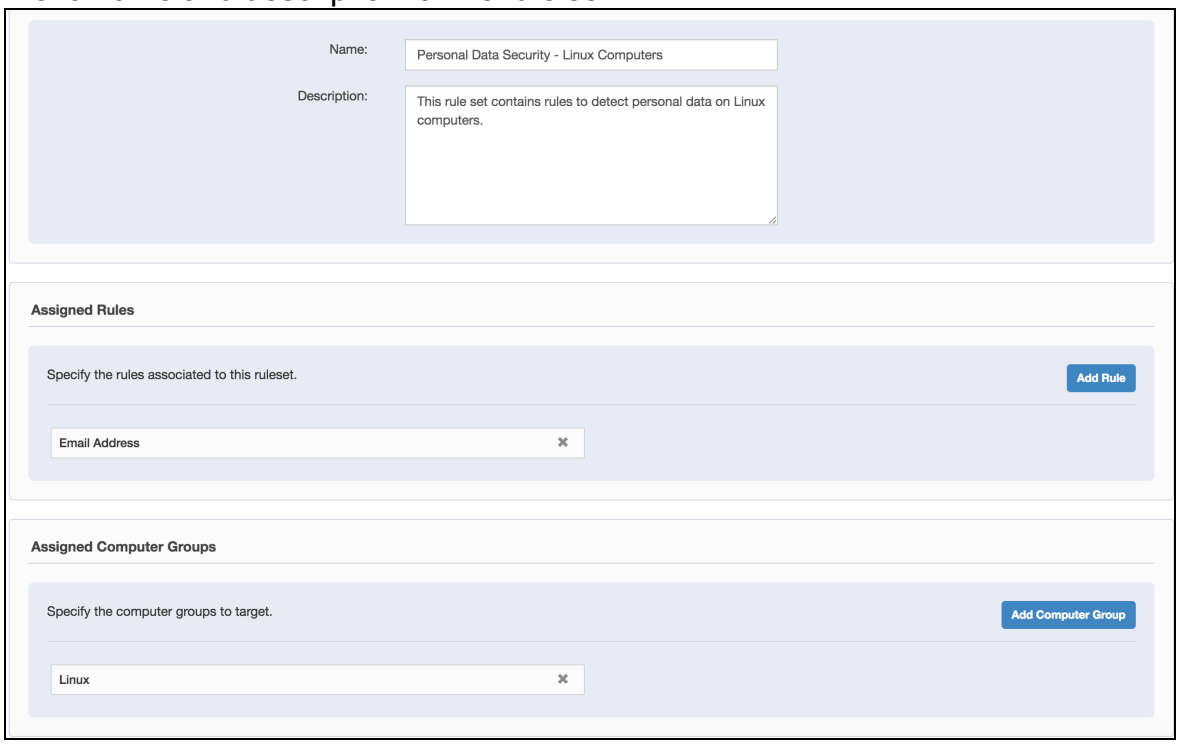
For example, you might want to apply and monitor for specific rules on one group of endpoints, but not other groups. Or, you might want to apply a subset of the available rules to a group of endpoints.

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.

By default, each rule set has one rule assigned to it. The default rule cannot be edited, but you can delete it, or make a duplicate of the 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 Rule** and select the rules you want to associate with the rule set. Click **Save**.
4. 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.
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 **Add Rule** and select the rules you want to associate with the rule set. Click **Save**.

## Delete a rule set

1. From the Reveal menu, click **Rule sets**.
2. Select the rule set that you want to delete.
3. Click **Action > Delete**. Confirm that you want to delete the rule set.

# Investigating rule matches

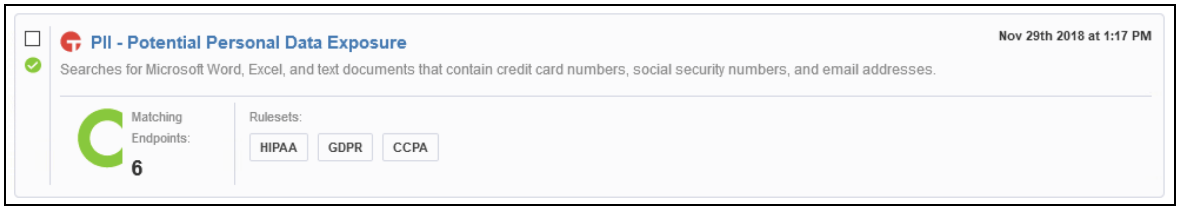
## Overview

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 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 Trace live connection to the endpoint and drill down to perform further analysis. You can investigate the number of matches across the endpoints over time, and filter the matches by computer group or keywords.

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. Reveal displays the endpoints where matches have occurred.
4. Select an endpoint and click **Create Connection**. A live connection is opened to the endpoint. When the endpoint connection displays as **Active**, click the endpoint name to view files that contain matches.
5. Click an endpoint to view files that contain rules matches. For files where matches have occurred, the file name, Rule ID, Number of hits, date modified, size, and path

are displayed.