

Tanium™ Reputation User Guide

Autonomous IT. Unstoppable Business.

2025H2 Semiannual Release

Version 6.7

May 26, 2026

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

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

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

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

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

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

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

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

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

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

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

© 2025 Tanium Inc. All Rights Reserved

© 2025 Tanium Inc. All rights reserved.

Table of contents

Reputation overview **8**

Reputation item life cycle 8

Reputation items are added to the reputation database 8

Reputation items are scanned 8

WildFire 8

Recorded Future 8

ReversingLabs A1000 8

ReversingLabs TitaniumCloud 9

VirusTotal 9

Reputation items are rescanned 9

Wildfire 9

Recorded Future 9

ReversingLabs A1000 9

ReversingLabs TitaniumCloud 9

VirusTotal 10

Items are removed from the reputation database 10

Hash List 10

Interoperability with other Tanium products 10

Connect 10

Threat Response 10

Trends 10

Getting started **12**

Step 1: Install and configure Reputation 12

Step 2: Enable reputation hash data in Tanium 12

Step 3: Enable reputation providers 12

Step 4: Manage hashes 12

Step 5: (Optional) Export data 12

© 2025 Tanium Inc. All Rights Reserved

Reputation requirements **13**
Core platform dependencies 13
Solution dependencies 13
Tanium recommended installation 13
Import specific solutions 13
Feature-specific dependencies 13
Tanium™ Module Server 14
Endpoints 14
Third-party software 14
Host and network security requirements 14
Ports 14
Security exclusions 15
Internet URLs 15
User role requirements 15
Installing Reputation **18**
Before you begin 18
Import Reputation with default settings 18
Import Reputation with custom settings 18
Manage solution dependencies 19
Upgrade Reputation 19
Verify Reputation version 19
Configuring Reputation **20**
Configure Reputation 20
Configure Reputation service settings 20
Send data to the reputation service 21
Set up Reputation users 23
Configuring reputation providers **24**
View reputation scan status 24
Configure Palo Alto Networks WildFire reputation provider 24
Prerequisites 25

© 2025 Tanium Inc. All Rights Reserved

Configure settings ... 25
Configure Recorded Future reputation provider ... 27
Prerequisites ... 27
Configure settings ... 27
Configure ReversingLabs A1000 reputation provider ... 29
Prerequisites ... 29
Configure settings ... 29
Configure ReversingLabs TitaniumCloud reputation provider ... 31
Prerequisites ... 31
Configure settings ... 31
Configure VirusTotal reputation provider ... 33
Prerequisites ... 34
Configure settings ... 34
Managing hashes ... 36
View additional hash data ... 36
Add data hashes ... 36
Import hashes ... 37
Export hashes ... 38
Edit notes ... 39
Remove hashes ... 39
Exporting reputation data ... 40
View reputation data ... 40
Send data to Connect destinations ... 40
Send data to Trends boards ... 41
Maintaining Reputation ... 43
Review and remediate Tanium Reputation issues ... 43
Check the Trends metrics for potential issues ... 43
Troubleshooting Reputation ... 44
Collect logs ... 44
Uninstall Reputation ... 44

© 2025 Tanium Inc. All Rights Reserved

Uninstall Reputation so data is restored on reinstall 44
Uninstall Reputation so you start fresh when you reinstall 45
Contact Tanium Support 45

© 2025 Tanium Inc. All Rights Reserved

Reputation overview

With Reputation, you can build a repository of reputation data from various providers, such as Palo Alto Networks WildFire, Recorded Future, ReversingLabs, and VirusTotal. These providers determine threat levels for file hashes. Other Tanium products, such as Tanium™ Threat Response, can use this data to give an indication of potentially malicious files. You can also send reputation data to supported Tanium™ Connect destinations or import reputation data to Tanium™ Trends boards.

The reputation database is a cache that consists of *reputation items*. When configured, reputation items are scanned by a *reputation provider*. A reputation provider is a service that determines whether a reputation item is considered to be malicious, non-malicious, suspicious, or has an unknown status.

Reputation item life cycle

A reputation item remains in the database as long as the Tanium processes are accessing the status of the item. The status of the reputation items is kept up to date based on the settings for the reputation service and provider.

Reputation items are added to the reputation database

As long as the maximum database size is not exceeded, reputation items are added to the reputation database in the following scenarios:

- When a Tanium process, such as Threat Response, identifies a new hash.
- When a saved question connection source sends a list of hashes to Connect.

When the reputation items are first added, it is unknown whether they are malicious. The reputation item state most likely starts out as unknown or pending.

Reputation items are scanned

How long it takes for an initial scan of the items depends on your configured reputation service settings.

If you configure multiple reputation service providers, a reputation item is created for each reputation provider. For example, for a single hash, three separate reputation items are created for WildFire, ReversingLabs, and VirusTotal.

WILDFIRE

All reputation items are sent to WildFire as they are received.

RECORDED FUTURE

The settings for Recorded Future determine how many hashes to send at a time, and the maximum API calls per minute/day. For more information about these settings, see Configure Recorded Future reputation provider on page 27.

REVERSINGLABS A1000

The settings for ReversingLabs A1000 determine how many hashes to send at a time, and the maximum API calls per minute/day. For more information about these settings, see Configure ReversingLabs A1000 reputation provider on page 29.

© 2025 Tanium Inc. All Rights Reserved

REVERSINGLABS TITANIUMCLOUD

The settings for ReversingLabs TitaniumCloud determine how many hashes to send at a time, and the maximum API calls per minute/day. For more information about these settings, see Configure ReversingLabs TitaniumCloud reputation provider on page 31.

VIRUSTOTAL

The settings for VirusTotal determine how many hashes to send at a time, and the maximum API calls per minute/day. For more information about these settings, see Configure VirusTotal reputation provider on page 33.

Reputation items are rescanned

Reputations might change for reputation items over time. When Reputation rescans an item, it is checked against the reputation providers again. For more information on how to configure the rescan properties, see Installing Reputation on page 18.

The **Rescan Item Interval** setting is global for all reputation provider types. The value determines how often Reputation rescans items. For example, if this value is set to 1 day, all of the items in the database get checked every day.

WILDFIRE

Reputation scans Items according to the **Rescan Item Interval** value.

RECORDED FUTURE

You can configure Reputation to rescan items when Recorded Future gets new reputations for hashes.

Reputation compares the **Maximum Age of New Items** setting with the First Seen attribute in Recorded Future. The First Seen attribute is the date when Recorded Future first records any instance of that hash, from any Recorded Future customer. If the item is less than the configured maximum, Reputation considers the item as new and rescans the item. The **Rescan New Item Interval** setting determines how often Reputation rescans the new items.

REVERSINGLABS A1000

You can configure Reputation to rescan items when ReversingLabs A1000 gets new reputations for hashes.

Reputation compares the **Maximum Age of New Items** setting with the First Seen attribute in ReversingLabs A1000. The First Seen attribute is the date when ReversingLabs A1000 first records any instance of that hash. If the item is less than the configured maximum, Reputation considers the item as new and rescans the item. The **Rescan New Item Interval** setting determines how often Reputation rescans the new items.

REVERSINGLABS TITANIUMCLOUD

You can configure Reputation to rescan items when ReversingLabs TitaniumCloud gets new reputations for hashes.

Reputation compares the **Maximum Age of New Items** setting with the First Seen attribute in ReversingLabs TitaniumCloud. The First Seen attribute is the date when ReversingLabs TitaniumCloud first records any instance of that hash, from any ReversingLabs TitaniumCloud customer. If the item is less than the configured maximum, Reputation considers the item as new and rescans the item. The **Rescan New Item Interval** setting determines how often Reputation rescans the new items.

© 2025 Tanium Inc. All Rights Reserved

VIRUSTOTAL

If you have a paid API key for VirusTotal, you can configure Reputation to rescan items when VirusTotal gets new reputations for hashes.

Reputation compares the **Maximum Age of New Items** setting with the First Seen attribute in VirusTotal. The First Seen attribute is the date when VirusTotal first records any instance of that hash, from any VirusTotal customer. If the item is less than the configured maximum, Reputation considers the item as new and rescans the item. The **Rescan New Item Interval** setting determines how often Reputation rescans the new items.

When you configure these settings, be careful to keep the number of API calls within the bounds of your agreement with VirusTotal.

Items are removed from the reputation database

When the number of days in the **Remove Item Interval** value passes, and that item has not been queried by a saved question or other Tanium process to check its status, the item is removed from the database.

A reputation item can be re-added to the database if the hash is found again.

Hash List

The hash list is a list of reputation hashes that are known to be false detections or known to be malicious. Reputation hashes in the hash list are not sent to reputation providers for analysis. You can add or delete specific hashes from the hash list, or you can export and import the entire list.

For more information, see Managing hashes on page 36.

Interoperability with other Tanium products

Reputation works with other Tanium products for additional reporting of related data.

Connect

You can use Tanium Reputation as a connection source or destination in Connect. For more information, see Send data to Connect destinations on page 40 and Exporting reputation data on page 40.

Threat Response

You can configure Tanium Threat Response to search for specific data from Tanium Reputation. For more information, see Tanium Threat Response: Set up the reputation service.

Trends

Reputation features Trends boards that provide data visualization of Reputation concepts.

© 2025 Tanium Inc. All Rights Reserved

The **Reputation** board displays how much data is sent to reputation providers, and usage metrics within Reputation. The following sections and panels are in the **Reputation** board:

- Resource Usage
    - Outbound Items
    - Outbound Processing Queue
    - Outbound API Requests
    - Successful Outbound API Requests
    - Failed Outbound API Requests
    - Reputation Database Size
- Service Usage
    - Inbound Items
    - Total Items
    - Purged Items
    - Hash List
    - Hash List Items in Environment

For more information about how to import the Trends boards that are provided by Reputation, see Send data to Trends boards on page 41 and Tanium Trends User Guide: Importing the initial gallery.

© 2025 Tanium Inc. All Rights Reserved

Getting started

Step 1: Install and configure Reputation

Install and configure Tanium Reputation.

For more information, see Installing Reputation on page 18.

Step 2: Enable reputation hash data in Tanium

Configure Tanium to send hashes to the Reputation service.

For more information, see Send data to the reputation service on page 21.

Step 3: Enable reputation providers

Configure and enable Reputation providers.

For more information, see Configuring reputation providers.

Step 4: Manage hashes

Manage hashes. The **Reputations** section of the Reputation **Overview** page shows any hashes that have been added to the Malicious or Non-Malicious hash lists. You can also search for file hashes and add, import, export, or delete reputation data hashes.

For more information, see Managing hashes on page 36.

Step 5: (Optional) Export data

Export Reputation data.

For more information, see Exporting reputation data on page 40.

© 2025 Tanium Inc. All Rights Reserved

Reputation requirements

Review the requirements before you install and use Reputation.

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium license that includes Reputation. For more information about how to get Reputation, see Tanium Solutions & Bundles.
- **Tanium™ Core Platform servers**: 7.4 or later
- **Tanium™ Client**: No client requirements.

Solution dependencies

Other Tanium solutions are required for specific Reputation 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 Reputation dependencies have their own dependencies, which you can see by clicking the links in the lists of Feature-specific dependencies on page 13. Note that the links open the user guides for the latest version of each solution, not necessarily the minimum version that Reputation requires.

Tanium recommended installation

If you select **Tanium Recommended Installation** when you import Reputation, 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 Reputation to import, you must manually import dependencies. See Tanium Console User Guide: Import, re-import, or update specific solutions.

Feature-specific dependencies

Reputation has the following feature-specific dependencies:

- Tanium Connect
- Tanium Reporting
- Tanium Threat Response

© 2025 Tanium Inc. All Rights Reserved

- Tanium Trends

Tanium™ Module Server

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

> NOTE
>
> The Reputation service is automatically disabled when the disk usage of the Module Server exceeds the value of the **Maximum Disk Capacity** setting. The default value is 85%. For more information on how to configure the Reputation service settings, see Installing Reputation on page 18.

Endpoints

Reputation does not deploy packages to endpoints. For Tanium Client operating system support, see Tanium Client Management User Guide: Client version and host system requirements.

Third-party software

With Reputation, you can integrate with several different kinds of third-party software. If no specific version is listed, there are no version requirements for that software.

- Palo Alto Networks WildFire
- Recorded Future
- ReversingLabs A1000
- ReversingLabs TitaniumCloud
- VirusTotal

Host and network security requirements

Specific ports and processes are needed to run Reputation.

Ports

The following ports are required for Reputation communication.

Ports for Tanium Reputation communication

Source	Destination	Port	Protocol	Purpose
Module Server	Module Server (loopback)	17455	TCP	Internal purposes; not externally accessible

© 2025 Tanium Inc. All Rights Reserved

BEST PRACTICE

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

Security exclusions

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

NOTE

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

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

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\reputation-service\node.exe`

Internet URLs

If security software is deployed in the environment to monitor and block unknown URLs, your security administrator might need to allow URLs on the Tanium Module Server associated with a configured reputation provider. For more information about required URLs to allow, see the reputation provider documentation.

User role requirements

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

- Reputation solution permissions on page 16
- Reputation administration and platform content permissions on page 17: The solution permissions automatically provide some of these permissions.

To review a summary of the predefined roles, see Set up Reputation users on page 23.

© 2025 Tanium Inc. All Rights Reserved

Some Reputation solution permissions provide permissions that are associated with other solutions. Furthermore, all the platform content permissions and some solution permissions apply to content sets that might contain content for other solutions in addition to Reputation. If you create custom roles for Reputation users, be sure to assign all the solution permissions and content set permissions that are required for Reputation functionality. If you are not sure which permissions are required for a custom role, view the permissions of the predefined roles. For more information, see the following sections of the Tanium Console User Guide:

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



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

Reputation solution permissions

Permission	Reputation Administrator[1]	Reputation Operator[1]
Reputation[2,3] READ: Read access to the Reputation shared service WRITE: Write access to the Reputation shared service SHOW: View the Reputation workbench	READ WRITE SHOW	READ WRITE SHOW
Reputation Administrator Administrative access to the Reputation shared service	ADMINISTER	
Reputation Hash List[3] Access to the Reputation hash list data	READ WRITE	READ WRITE
Reputation Provider Access to the provider configurations	READ WRITE	READ WRITE

© 2025 Tanium Inc. All Rights Reserved

Reputation solution permissions (continued)

Permission	Reputation Administrator[1]	Reputation Operator[1]
Reputation Service Account Access to module service accounts to read and write data	✗	✗

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

[2] If you need access to only the **Malicious** tab in the **Reputations** section of the Reputation **Overview** page, you can add the **Reputation** show and **Reputation** read or **Reputation** write permissions to your user.

[3] If you need access to only the **Reputations** section of the Reputation **Overview** page, you can add the **Reputation** show, **Reputation Hash List** read, and either the **Reputation** read or **Reputation** write permissions to your user.

Reputation administration and platform content permissions

Permission	Permission Type	Reputation Administrator	Reputation Operator
Action Group	Administration	✓ READ WRITE	✓ READ WRITE
Plugin	Platform Content	✓ READ EXECUTE	✓ READ EXECUTE
Filter Group	Platform Content	✓ READ WRITE	✓ READ WRITE
Sensor	Platform Content	✓ READ WRITE	✓ READ WRITE

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

© 2025 Tanium Inc. All Rights Reserved

Installing Reputation

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

- **Automatic configuration with default settings**: Reputation is installed with any required dependencies and other selected products. After installation, the Tanium Server automatically configures the recommended default settings. This option is the best practice for most deployments. For more information about the automatic configuration for Reputation, see Import Reputation with default settings on page 18.
- **Manual configuration with custom settings**: After installing Reputation, you must manually configure required settings. Select this option only if Reputation requires settings that differ from the recommended default settings. For more information, see Import Reputation with custom settings on page 18.

Before you begin

- Read the release notes.
- Review the Reputation requirements on page 13.
- If you have Tanium Connect 4.10 or earlier installed, you must first either uninstall Connect or upgrade to Connect 4.11 or later. For more information, see Tanium Connect User Guide: Uninstall Connect or Tanium Connect User Guide: Upgrade Connect.
- Assign the correct roles to users for Reputation. Review the User role requirements on page 15.
    - To import the Reputation solution, you must be assigned the Administrator reserved role.

Import Reputation with default settings

When you import Reputation with automatic configuration, the Reputation 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 Configuring Reputation on page 20.

To import Reputation 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 Reputation version on page 19.

Import Reputation with custom settings

To import Reputation without automatically configuring default settings, be sure to clear the **Apply All Tanium recommended configurations** checkbox while performing the steps in Tanium Console User Guide: Import or update specific solutions. After the import, verify that the correct version is installed: see Verify Reputation version on page 19.

To configure the service account, see Configuring Reputation on page 20.

To configure settings, see Configure Reputation service settings on page 20.

© 2025 Tanium Inc. All Rights Reserved

Manage solution dependencies

When you start the Reputation workbench for the first time, the Tanium Server checks whether all the Tanium modules and shared services (solutions) that are required for Reputation are installed at the required versions. The Reputation workbench cannot load unless all required dependencies are installed. If you selected **Tanium Recommended Installation** when you imported Reputation, the Tanium Server automatically imported all your licensed solutions at the same time. Otherwise, if you manually imported Reputation and did not import all its dependencies, Tanium Console displays a banner that lists the dependencies and the required versions. For more information, see Solution dependencies.

1. Install the dependencies as described in Tanium Console User Guide: Import or update specific solutions.
2. From the Main menu, go to **Shared Services > Reputation** to open the Reputation **Overview** page and verify that the Console no longer displays a banner to list missing dependencies.

Upgrade Reputation

For the steps to upgrade Reputation, see Tanium Console User Guide: Managing Tanium solutions. After the upgrade, verify that the correct version is installed: see Verify Reputation version on page 19.

Verify Reputation version

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

1. Refresh your browser.
2. From the Main menu, go to **Shared Services > Reputation**.
3. To display version information, click Info.

© 2025 Tanium Inc. All Rights Reserved

Configuring Reputation

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

When you import Reputation with automatic configuration, the Reputation 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 Configuring Reputation on page 20.

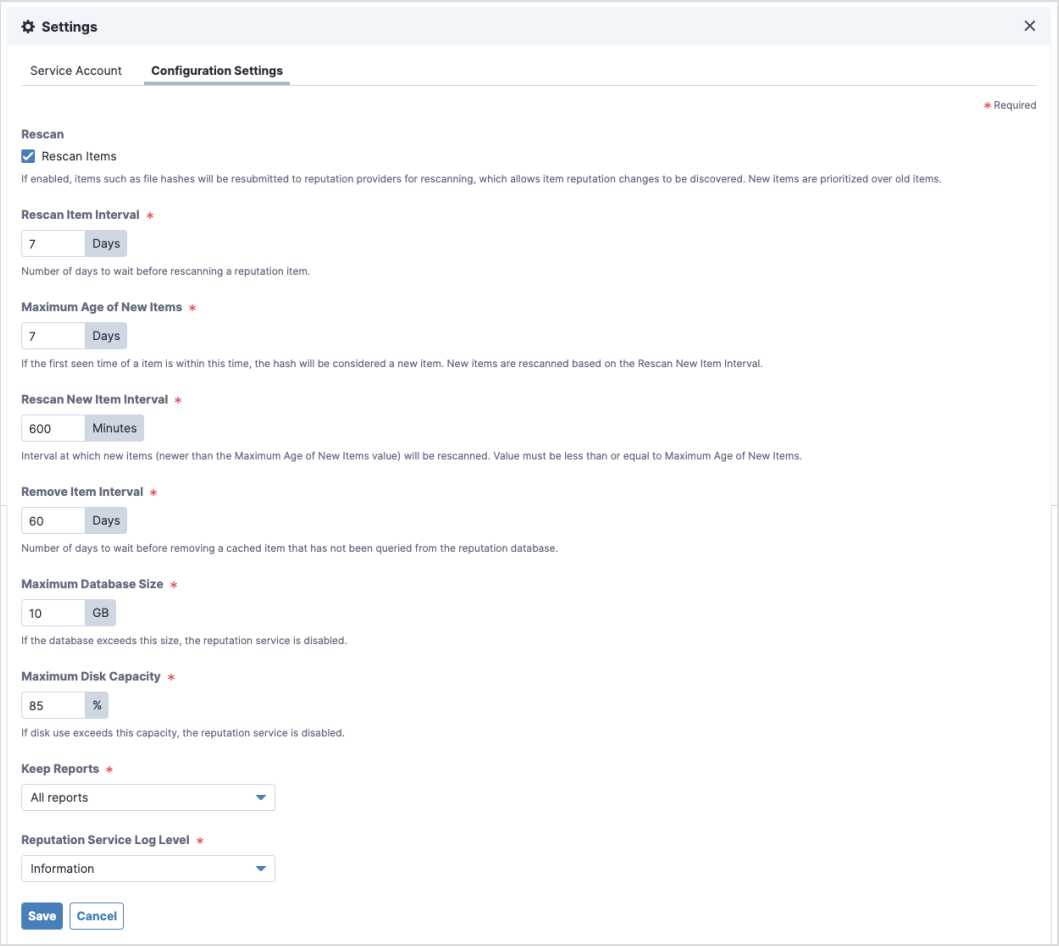
Configure Reputation

Configure Reputation service settings

Reputation service settings determine the contents of the reputation database. These settings determine how often reputation items are scanned in the reputation source, how long to consider items as new, and how long to keep items in the database if their reputation status has not been referenced. For more information about these settings and how they affect the reputation items, see Reputation item life cycle on page 8.

© 2025 Tanium Inc. All Rights Reserved

Reputation service settings



To update these settings, from the Reputation **Overview** page, click Settings, and then click **Configuration Settings**.

The **Maximum Database Size** setting is 10GB by default. You can increase this size as needed. If the database exceeds this size, the reputation service is disabled.

The **Keep Reports** setting determines whether you want the full reports from the reputation source to be kept in the reputation database. You can choose to keep all reports, or only malicious and suspicious reports. Selecting only malicious and suspicious reports saves space in the database. If you are using VirusTotal as a connection source, use the keep all reports option to get the enhanced reporting information.

Send data to the reputation service

If you want to pre-populate reputation data with hashes from your environment, you can send data to the reputation service as a connection destination. When this content is pre-populated, the reputation service can start querying the status of the items from the reputation providers.

© 2025 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules > Threat Response** . Click Settings .
2. Click **Service > Reputation**.
3. Click **Configure Reputation** to generate saved questions and connections.

When you click **Configure Reputation**, the following saved questions are generated:

- Reputation - Driver Details (SHA 256) [Tanium Default]
- Reputation - MS EXE Recently Changed [Tanium Default]
- Reputation - Windows AutoRuns (SHA 256) [Tanium Default]
- Reputation - Running Processes with Hash (SHA256) [Tanium Default]
- Reputation - Mac Autoruns (MD5) [Tanium Default]
- Reputation - Linux Autoruns (MD5) [Tanium Default]
- Reputation - Trace Executed Process Hashes (MD5) [Tanium Default]
- Reputation - Service Module Details (SHA256) [Tanium Default]
- Reputation - Loaded Modules (SHA256) [Tanium Default]
- Reputation - Recently Changed MACHO 32 Bit [Tanium Default]
- Reputation - Recently Changed MACHO 64 Bit [Tanium Default]
- Reputation - Recently Changed ELF [Tanium Default]

When you click **Configure Reputation**, the following Tanium Connect connections are generated to provide reputation intel to Threat Response:

- Reputation - Recently Changed MACHO 64 Bit [Tanium Default]
- Reputation - Recently Changed ELF [Tanium Default]
- Reputation - Recently Changed MACHO 32 Bit [Tanium Default]
- Reputation - Trace Executed Process Hashes (MD5) [Tanium Default]
- Reputation - Loaded Modules (SHA256) [Tanium Default]
- Reputation - Service Module Details (SHA256) [Tanium Default]
- Reputation - Linux Autoruns (MD5) [Tanium Default]
- Reputation - Mac Autoruns (MD5) [Tanium Default]
- Reputation - Running Processes with Hash (SHA256) [Tanium Default]
- Reputation - MS EXE Recently Changed [Tanium Default]
- Reputation - Windows AutoRuns (SHA 256) [Tanium Default]
- Reputation - Driver Details (SHA 256) [Tanium Default]

© 2025 Tanium Inc. All Rights Reserved

Clicking **Configure Reputation** does not recreate any existing connections or saved questions. If any connections or saved questions do not exist in the environment, they are created. Saved questions are recreated when the Threat Response service is restarted.

Set up Reputation users

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

To review specific permissions for each role, see User role requirements on page 15.

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

Reputation Administrator

Assign the **Reputation Administrator** role to users who manage the configuration of Reputation.
This role can perform the following tasks:

- Configure Reputation settings, including the service account, scanning, storage, and logging
- View, create, edit, and delete reputation provider configurations
- View, create, edit, and delete file data hashes

Reputation Operator

Assign the **Reputation Operator** role to users who manage the configuration of Reputation but do not need to manage the service account.
This role can perform the following tasks:

- Configure some Reputation settings, including scanning, storage, and logging
- View, create, edit, and delete reputation provider configurations
- View, create, edit, and delete file data hashes

© 2025 Tanium Inc. All Rights Reserved

Configuring reputation providers

Reputation is a service that queries reputation providers for threat intelligence about given file hashes. You can configure one or more reputation providers to build a repository of reputation data.

View reputation scan status

The **Providers** section of the Reputation **Overview** page shows the total number of reputation items, and the following information about each reputation provider:

Reputation providers



- **Items**: total number of reputation items on this reputation provider
- **New**: reputation items that still need to be scanned on this reputation provider
- **Processed**: reputation items scanned on this reputation provider
- **Rescanning**: reputation items that are rescanning on this reputation provider
- **Malicious Items**: malicious reputation items on this reputation provider
- **Malicious %**: percentage of malicious items out of total reputation items

To sort a column, click the column header.

For configured providers, the **Actions** column contains an **Enable** or **Disable** button, depending on the current state of the provider.

Configure Palo Alto Networks WildFire reputation provider

You can use Palo Alto Networks firewall security policies to capture suspicious files and forward them to the WildFire system for threat analysis. If the file is malware, the status is reported back to the firewall.

After the WildFire analysis is completed, the reputation service can query the results and update the reputation data.

© 2025 Tanium Inc. All Rights Reserved

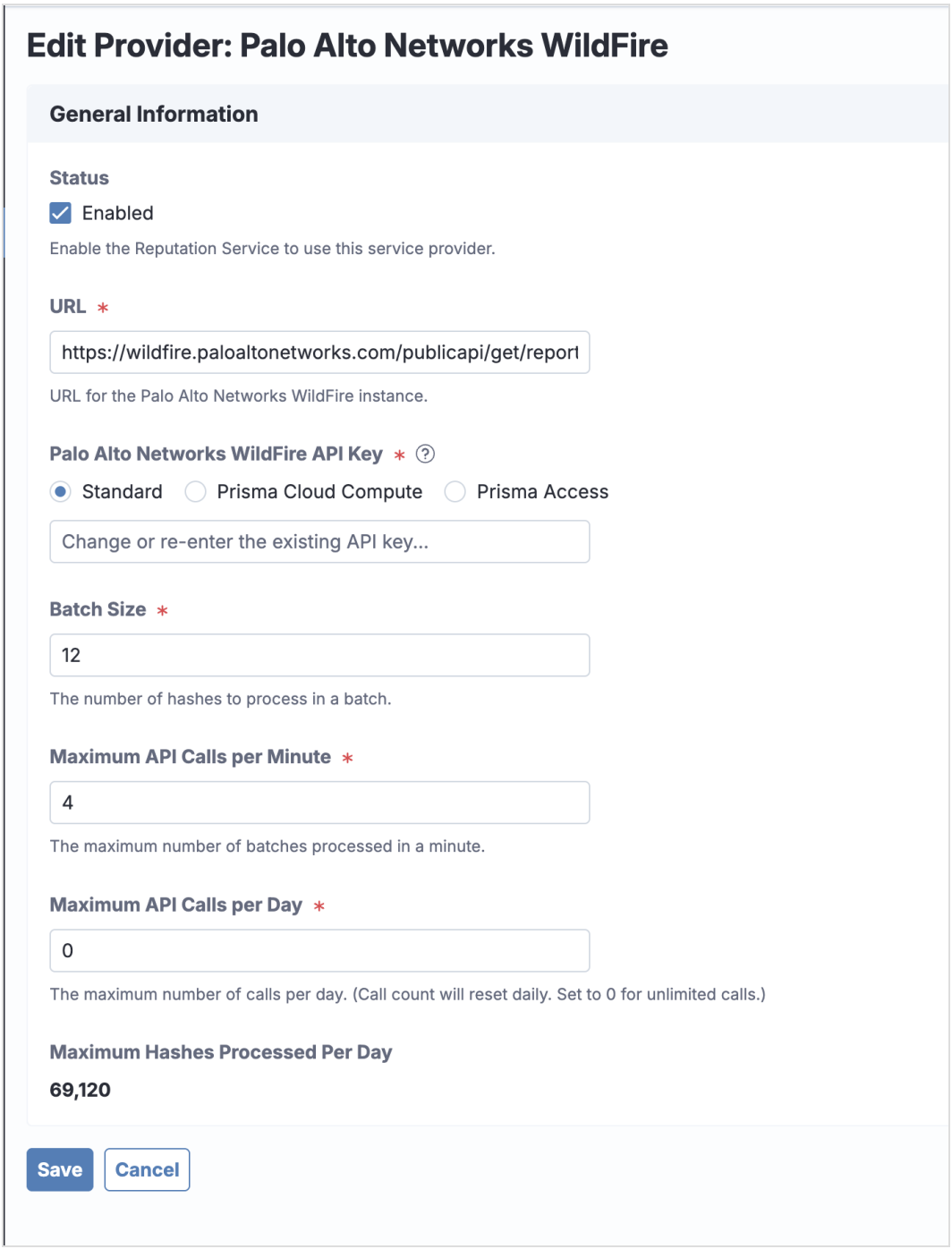
Prerequisites

- A subscription to Cloud WildFire (wildfire.paloaltonetworks.com) or a configured WF-500 WildFire appliance.
- Palo Alto Networks Firewall with or without Panorama.

Configure settings

© 2025 Tanium Inc. All Rights Reserved

1. In the **Providers** section, click Configure Provider in the Palo Alto Networks WildFire row.
2. Select **Enabled** to enable the reputation provider.



3. Specify the settings for Palo Alto Networks WildFire, including the URL for your WildFire instance and the API key. Select the type of Wildfire subscription you have purchased. Your WildFire API key is assigned when you purchase your WildFire (either firewall-attached or as a standalone WildFire API subscription), Prisma Cloud Compute, or Prisma Access

© 2025 Tanium Inc. All Rights Reserved

subscription and expires when the expiration date is reached. If you have multiple firewalls with WildFire subscriptions, the API key is tied to the subscription that expires last. You cannot delete a WildFire public cloud API key; it only expires. If you need a WildFire public cloud API key removed for security reasons, you must open a support case.

4. Adjust the settings for **Batch Size**, **Maximum API Calls Per Minute**, and **Maximum API Calls Per Day** according to your agreement with Palo Alto Networks. The **Maximum Hashes Processed Per Day** value is automatically calculated based on these configured settings.
5. Select **Use Tanium Module Server Proxy Setting** to use the proxy setting defined on the Tanium Module Server.
6. Click **Save**.

Configure Recorded Future reputation provider

Recorded Future is a cloud-based reputation service provider. The reputation service sends reputation items to the Recorded Future API and returns the results to the reputation database.

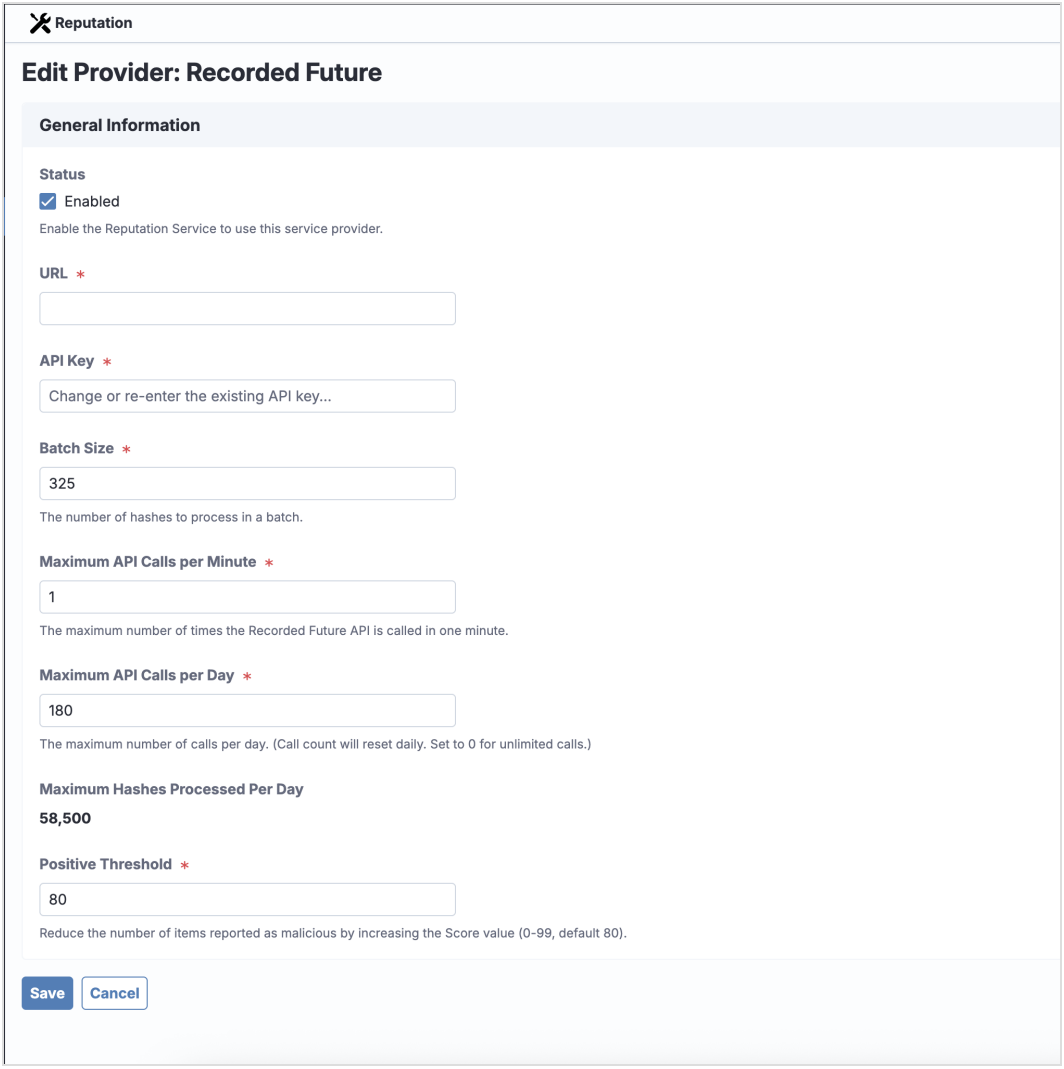
Prerequisites

You must already have a Recorded Future API token. If you have not already registered for Recorded Future access, contact their sales team at recordedfuture.com.

Configure settings

© 2025 Tanium Inc. All Rights Reserved

1. In the **Providers** section, click Configure Provider in the Recorded Future row.
2. Select **Enabled** to enable the reputation provider.



3. Specify the settings for Recorded Future, including the URL and API key.
4. Adjust the settings for **Batch Size**, **Maximum API Calls Per Minute**, and **Maximum API Calls Per Day** according to your agreement with Recorded Future. The **Maximum Hashes Processed Per Day** value is automatically calculated based on these configured settings.

© 2025 Tanium Inc. All Rights Reserved

5. Adjust the **Positive Threshold**, which is the risk score as determined by Recorded Future. The default value is `80`, which means that any hash with a Recorded Future risk score of 80 or higher is considered malicious by Reputation.

   Risk scores are banded into four severity levels of indicators on any given risk list (indicators with no current evidence of risk are assigned a risk score of 0):

   - Very Malicious: risk score of 90-99
   - Malicious: risk score of 80-89
   - Suspicious: risk score of 25-79
   - Unusual: risk score of 5-24
   - No current evidence of risk: risk score of zero

   For more information, see the Recorded Futures support portal.

   Setting **Positive Threshold** to `0` results in the maximum number of reports for malicious items. Setting **Threat Level** to `99` results in the fewest number of reports for malicious items.

6. Select **Use Tanium Module Server Proxy Setting** to use the proxy setting that is defined on the Tanium Module Server.
7. Click **Save**.

Configure ReversingLabs A1000 reputation provider

ReversingLabs is an application that companies can install locally to analyze files and provide reputation results through API requests or a web interface.

Prerequisites

You must already have a ReversingLabs API token. If you have not already registered for ReversingLabs access, contact their sales team at reversinglabs.com.

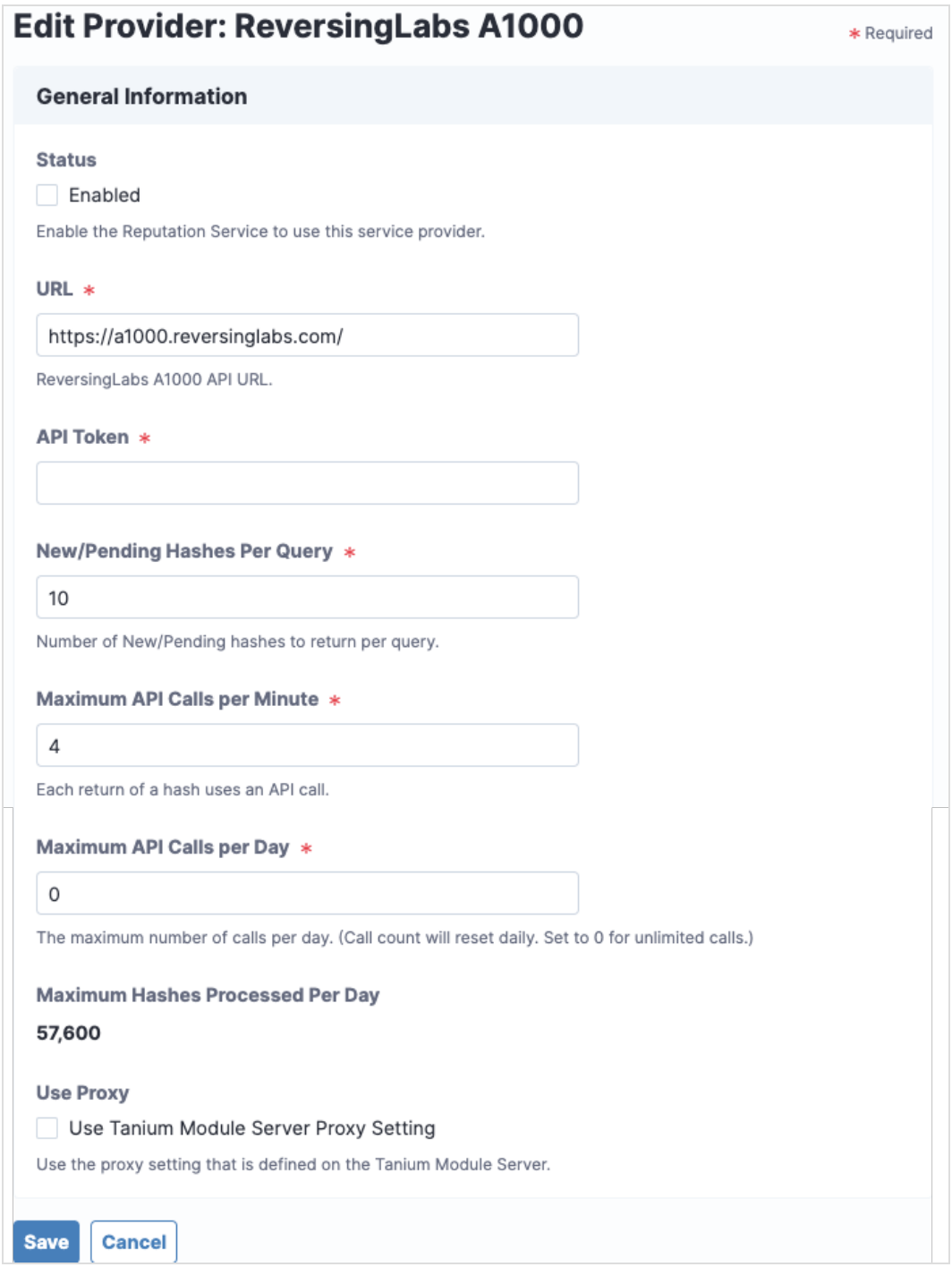
To get an API key:

1. Sign in to ReversingLabs.
2. Click the User Profile icon.
3. Select **Administration**.
4. Click **Tokens**.

Configure settings

© 2025 Tanium Inc. All Rights Reserved

1. In the **Providers** section, click Configure Provider in the ReversingLabs A1000 row.
2. Select **Enabled** to enable the reputation provider.



3. Specify the settings for ReversingLabs A1000, including the **URL** for your API access and your **API Token**.

© 2025 Tanium Inc. All Rights Reserved

4. Adjust the settings for **New/Pending Hashes Per Query**, **Maximum API Calls Per Minute**, and **Maximum API Calls Per Day** according to your API agreement with ReversingLabs and your network requirements. The **Maximum Hashes Processed Per Day** value is automatically calculated based on these configured settings.
5. Select **Use Tanium Module Server Proxy Setting** to use the proxy setting defined on the Tanium Module Server.
6. Click **Save**.

Configure ReversingLabs TitaniumCloud reputation provider

ReversingLabs TitaniumCloud is an online service that analyzes files, hashes, and URLs to identify viruses, worms, trojans, and other kinds of malicious content that is detected by anti-virus software and website scanners. The reputation service sends reputation items to the ReversingLabs API and returns the results to the reputation database.

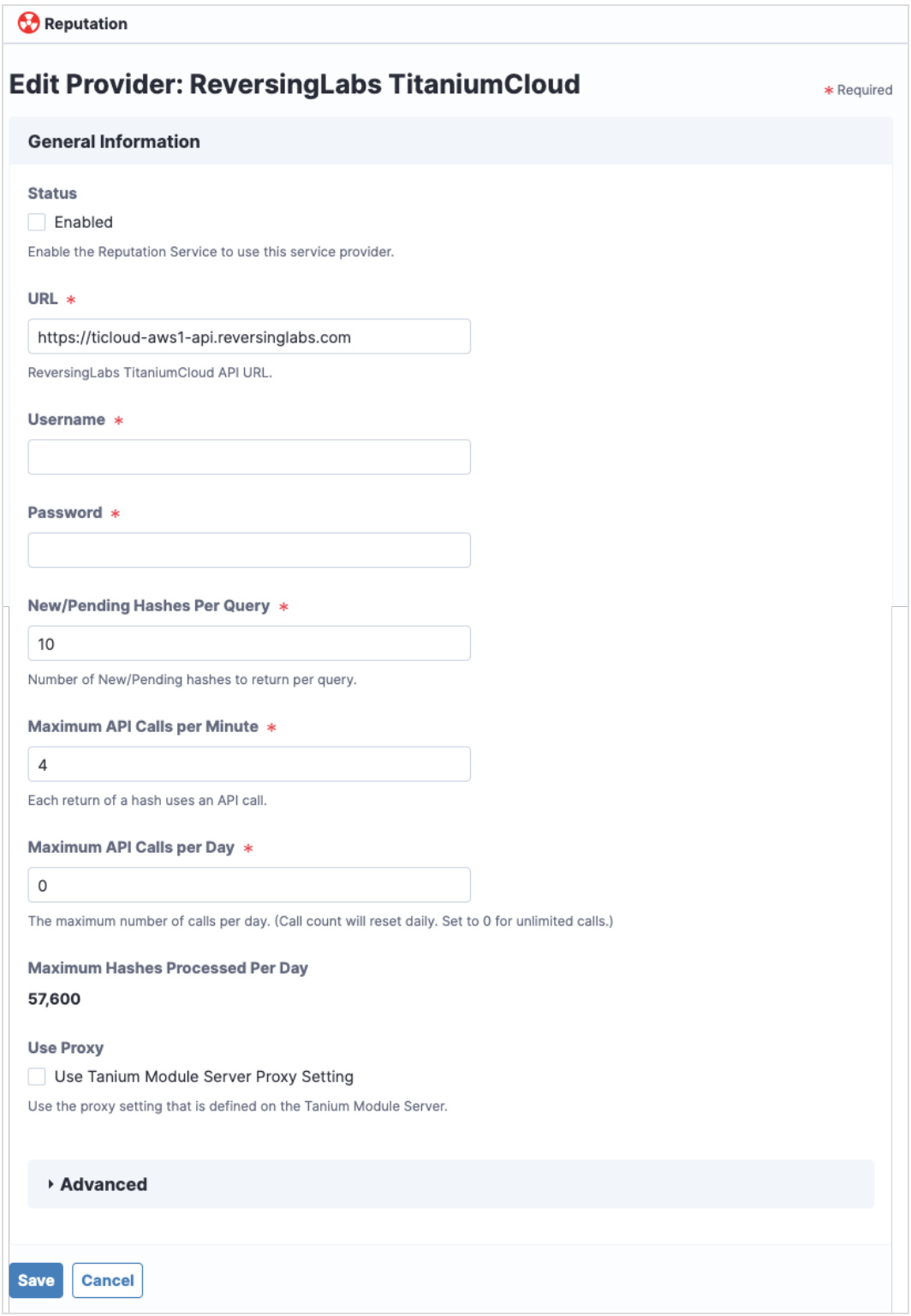
Prerequisites

You must already have a ReversingLabs TitaniumCloud account. If you have not already registered for ReversingLabs TitaniumCloud access, contact their sales team at reversinglabs.com.

Configure settings

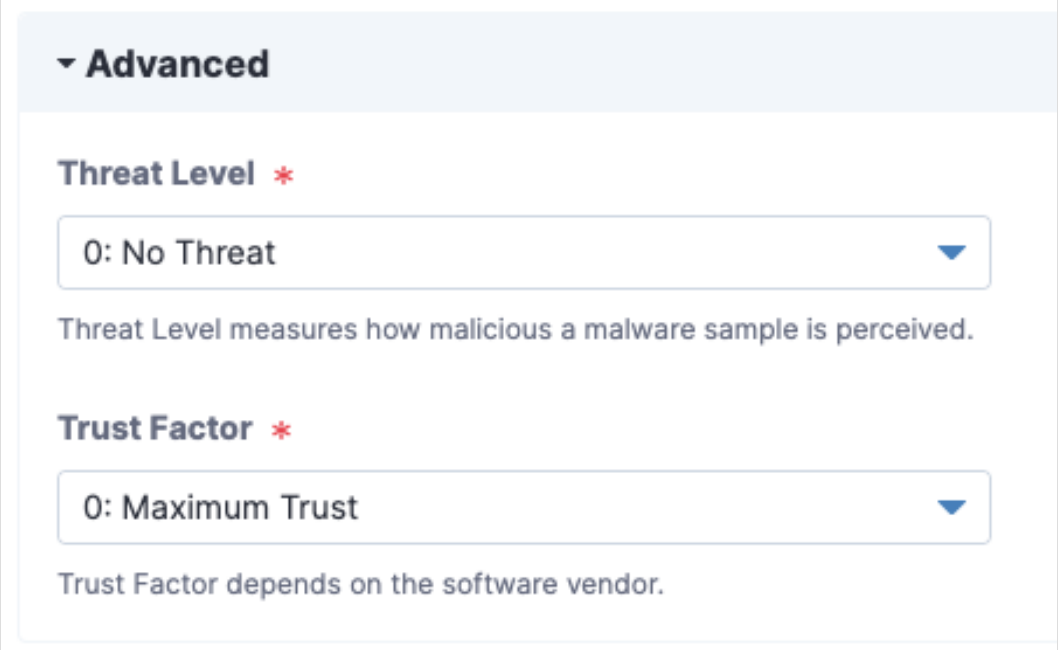
© 2025 Tanium Inc. All Rights Reserved

1. In the **Providers** section, click Configure Provider in the ReversingLabs TitaniumCloud row.
2. Select **Enabled** to enable the reputation provider.



© 2025 Tanium Inc. All Rights Reserved

3. Add your ReversingLabs TitaniumCloud credentials: the **URL** for your API access, your **Username**, and your **Password**.
4. Adjust the settings for **New/Pending Hashes Per Query**, **Maximum API Calls Per Minute**, and **Maximum API Calls Per Day** according to your API agreement with ReversingLabs and your network requirements. The **Maximum Hashes Processed Per Day** value is automatically calculated based on these configured settings.
5. Select **Use Tanium Module Server Proxy Setting** to use the proxy setting defined on the Tanium Module Server.
6. To reduce the number of items reported as malicious, expand **Advanced** and adjust the settings for **Threat Level** and **Trust Factor**.



TIP

Setting **Threat Level** to `0` and **Trust Factor** to `0` results in the maximum number of reports for malicious items. Setting **Threat Level** to `5` and **Trust Factor** to `5` results in the fewest number of reports for malicious items.

7. Click **Save**.

Configure VirusTotal reputation provider

VirusTotal is an online service that analyzes files, hashes, and URLs to identify viruses, worms, trojans, and other kinds of malicious content that is detected by antivirus engines and website scanners. The reputation service sends reputation items to the VirusTotal API and returns the results to the reputation database.

© 2025 Tanium Inc. All Rights Reserved

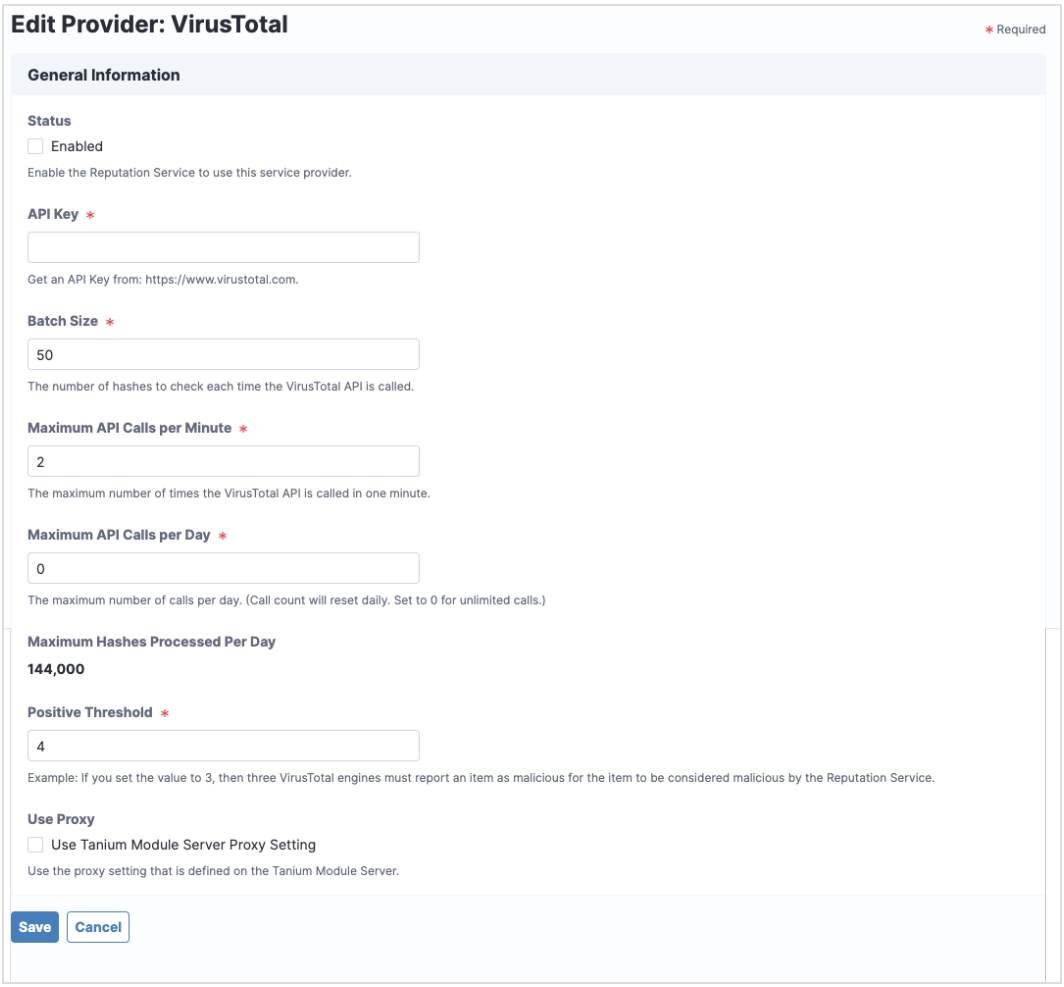
Prerequisites

Register for a VirusTotal API key at virustotal.com. VirusTotal makes their catalog available for query with an API key. Refer to the VirusTotal API use policy to determine which type of API key is appropriate.

To get the API key on the VirusTotal website, sign in and click ***your_user_image*** **> Settings > API Key**.

Configure settings

1. In the **Providers** section, click Configure Provider in the VirusTotal row.
2. Select **Enabled** to enable the reputation provider.



3. Specify settings for VirusTotal, including the API key.
4. Adjust the settings for **Batch Size**, **Maximum API Calls Per Minute**, and **Maximum API Calls Per Day** according to your agreement with VirusTotal. The **Maximum Hashes Processed Per Day** value is automatically calculated based on these configured settings.

© 2025 Tanium Inc. All Rights Reserved

5. Adjust the **Positive Threshold**, which is a number of positive reports that must be on the hash to be considered a potential threat or malware.

   The likelihood that VirusTotal reports might include false positive indicators is higher when the value is set lower.

   Example: If you set the value to `3`, then three VirusTotal engines must report an item as malicious for the item to be sent to Connect.

   Setting the value to `0` disables the threshold. If any VirusTotal engine reports that item as malicious, the item is sent to Reputation.

   Reputation results for VirusTotal are determined as follows:

   - Malicious: if the number of positives is greater than the threshold
   - Suspicious: if the number of positives is greater than zero, but less than the threshold
   - Non-malicious: if the number of positives is zero
   - Unknown: if there is no data

6. Select **Use Tanium Module Server Proxy Setting** to use the proxy setting defined on the Tanium Module Server.
7. Click **Save**.

© 2025 Tanium Inc. All Rights Reserved

Managing hashes

The **Reputations** section of the Reputation **Overview** page shows a list of hashes that are malicious or non-malicious. You can view additional context for each hash, and for certain providers you can also view additional information on the provider's website. You can also search for file hashes and add, import, export, or delete reputation data hashes.



Hashes that you add to the hash list are not sent to reputation providers for analysis.

When a hash is manually added as malicious or non-malicious in Reputation, it is not sent to any of the reputation providers.

When Intel deployment occurs, Threat Response queries the Reputation malicious hash list for an updated list of malicious hashes to include with the Reputation intel document

At a regular frequency (default: 24 hours) the Threat Response service makes a new intel database and sends it to endpoints. This includes the hashes that were received from the reputation service since the last sync between Threat Response and Reputation.

When this intel database is received by the endpoint, a background scan begins within a few minutes. During the background scan all intel sources, apart from Signals, are evaluated by looking at the Recorder and Index databases. Since Reputation hashes are in its own intel source, the background scan includes searching for all the hashes that were found/manually entered in Reputation. If a hash corresponded to an executable, and that executable was run, the match of the hash is seen in the Recorder database. If the file is not an executable, or was not run a match is found in the intel database. In either case, an alert for that hash match is returned.

View additional hash data

1. In the **Reputations** section, click the **Malicious** tab.
2. To sort a column, click the column header.
3. Click ▶ to expand the **Hash** line-item to view reputation data for a hash.

Add data hashes

1. In the **Reputations** section, click the **Hash List** tab.
2. To sort a column, click the column header.
3. Click **Add**.
4. To add hashes that are known to be malicious, select **Malicious**, enter the **Hashes** and any **Notes** to associate with each hash, and click **Save**.
5. To add hashes that are known to be false detections, select **Non-Malicious**, enter the **Hashes** and any **Notes** to associate with each hash, and click **Save**.

© 2025 Tanium Inc. All Rights Reserved

NOTE

The **Hashes** field is limited to 1,000 hashes. To add more than 1,000 hashes at one time, use a file import. For more information, see Import hashes.

Import hashes

Import a CSV file containing one or more MD5, SHA-1, or SHA-256 file hashes. You can include the following header fields in the CSV file:

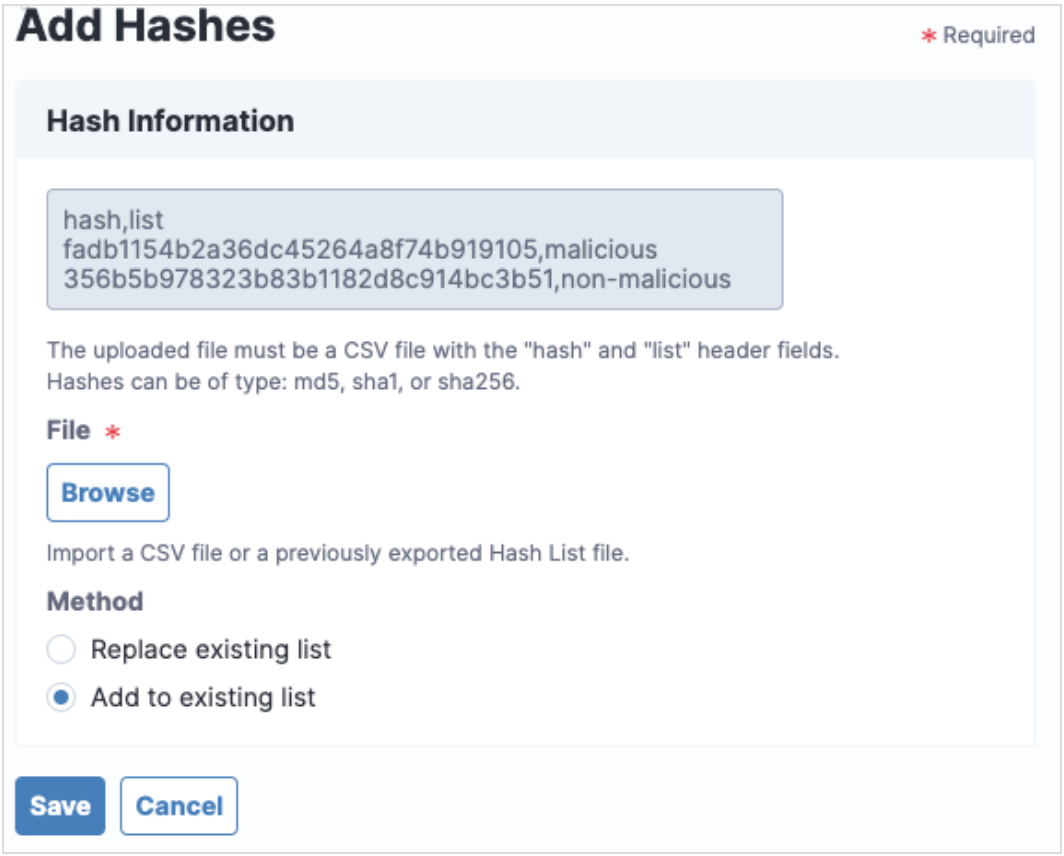
Header fields in a CSV file for import

Header field	Required	Description
`hash`	Required if `md5`, `sha1`, and `sha256` are not included, Optional if `md5`, `sha1`, and `sha256` are included	An MD5, SHA-1, or SHA-256 file hash value.
`list`	Required	Whether the file hash value is `malicious` or `non-malicious`.
`md5`	Required if `sha1` and `sha256` are included, Optional if `hash` is included	An MD5 file hash value.
`notes`	Optional	A string describing the file hash value.
`sha1`	Required if `md5` and `sha1` are included, Optional if `hash` is included	A SHA-1 file hash value.
`sha256`	Required if `md5` and `sha1` are included, Optional if `hash` is included	A SHA-256 file hash value.
`uploadedAt`	Optional	The timestamp at which this file hash value is uploaded. If undefined, this defaults to the current time.
`uploadedBy`	Optional	The user that uploaded this file hash value. If undefined, this defaults to your user.
`uploadedHash`	Optional	The uploaded file hash value.

At a minimum, a CSV file requires the `hash` and `list` header fields, with one file hash per row. You can also upload a CSV file with the `md5`, `sha1`, `sha256`, and `list` header fields, with at least one file hash per row.

© 2025 Tanium Inc. All Rights Reserved

1. In the **Reputations** section, click the **Hash List** tab.
2. Click **Import**.
3. Click **Browse** and select the file to import.



4. Select a **Method** for the import:
   - To replace the current hashes, select **Replace existing list**.
   - To append to the current hashes, select **Add to existing list**.
5. Click **Save**.

> NOTE
> Reputation automatically handles consolidating duplicate records by learning from service providers when different types of hashes represent the same file.

If you want to manually consolidate hashes, you can export the existing hash list, edit the file to add hashes in the appropriate columns for a specific row, and then import the updated file using the **Replace existing list** option.

Export hashes

© 2025 Tanium Inc. All Rights Reserved

1. In the **Reputations** section, click the **Hash List** tab.
2. To export specific hashes, select one or more hashes and click Export .
3. To export all malicious hashes, click the **Malicious** tab, and then click **Download All**.

Edit notes

1. In the **Reputations** section, click the **Hash List** tab.
2. Select a hash and click **Edit Notes**.
3. Update the notes for the hash and click **Save**.

Remove hashes

1. In the **Reputations** section, click the **Hash List** tab.
2. To delete specific hashes, select one or more hashes and click Remove from Hash List .

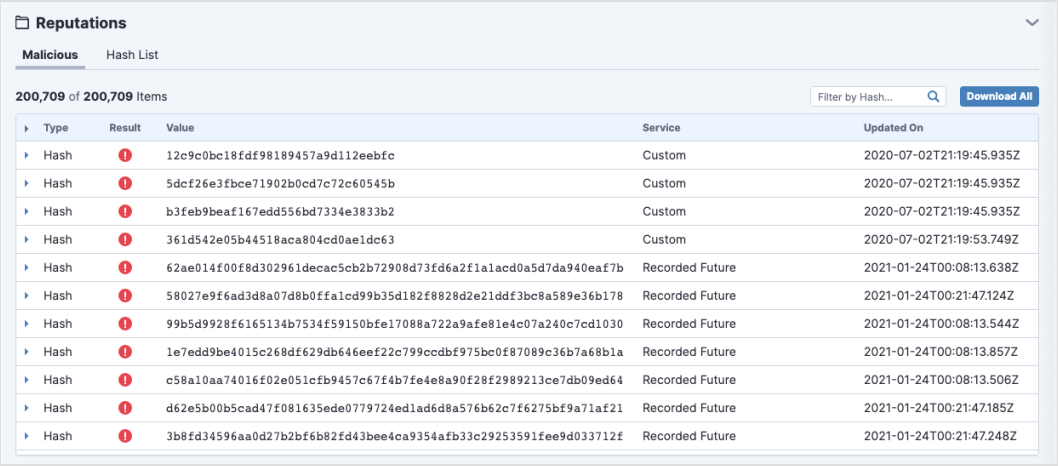
© 2025 Tanium Inc. All Rights Reserved

Exporting reputation data

View reputation data

To view a list of the malicious hashes that Reputation has pulled from the reputation services, open the **Malicious** tab in the **Reputations** section of the **Overview** page.

Malicious reputations



Type	Result	Value	Service	Updated On
Hash	!	12c9c0bc18fdf98189457a9d112eebfc	Custom	2020-07-02T21:19:45.935Z
Hash	!	5dcf26e3fbce71902b0cd7c72c60545b	Custom	2020-07-02T21:19:45.935Z
Hash	!	b3feb9beaf167edd556bd7334e3833b2	Custom	2020-07-02T21:19:45.935Z
Hash	!	361d542e05b44518aca804cd0ae1dc63	Custom	2020-07-02T21:19:53.749Z
Hash	!	62ae014f00f8d302961decac5cb2b72908d73fd6a2f1a1acd0a5d7da940eaf7b	Recorded Future	2021-01-24T00:08:13.638Z
Hash	!	58027e9f6ad3d8a07d8b0ffa1cd99b35d182f8828d2e21ddf3bc8a589e36b178	Recorded Future	2021-01-24T00:21:47.124Z
Hash	!	99b5d9928f6165134b7534f59150bfe17088a722a9afe81e4c07a240c7cd1030	Recorded Future	2021-01-24T00:08:13.544Z
Hash	!	1e7edd9be4015c268df629db646eef22c799ccdbf975bc0f87089c36b7a68b1a	Recorded Future	2021-01-24T00:08:13.857Z
Hash	!	c58a10aa74016f02e051cfb9457c67f4b7fe4e8a90f28f2989213ce7db09ed64	Recorded Future	2021-01-24T00:08:13.506Z
Hash	!	d62e5b00b5cad47f081635ede0779724ed1ad6d8a576b62c7f6275bf9a71af21	Recorded Future	2021-01-24T00:21:47.185Z
Hash	!	3b8fd34596aa0d27b2bf6b82fd43bee4ca9354afb33c29253591fee9d033712f	Recorded Future	2021-01-24T00:21:47.248Z

Only hashes with a malicious or pending status are listed.

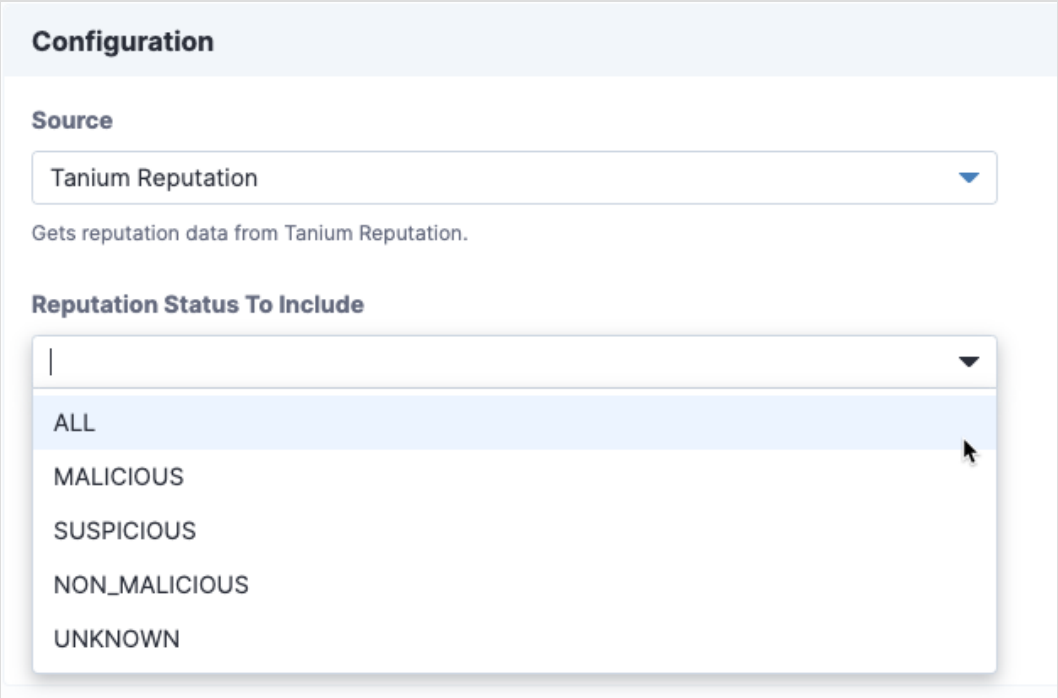
In Threat Response, you can view the ratings on hashes for live endpoints or snapshots. For more information, see Tanium Threat Response User Guide: Connecting to live endpoints and exploring data.

Send data to Connect destinations

Use Connect 5.2.3 or later to create a connection to send the data that is in the reputation database to any Connect destination. For example, you might configure a connection to create an email notification when a malicious item is found.

© 2025 Tanium Inc. All Rights Reserved

1. From the Connect **Overview** page, click **Create Connection**.
2. Specify a name and description.
3. For the source, select **Tanium Reputation**.



   You can also select the reputation status to include.
4. Configure the destination settings for the connection.

> **NOTE** The first run of a connection that uses **Tanium Reputation** as a source retrieves all available reputation items. Subsequent runs of that connection retrieve only the reputation changes since the last time the connection ran.

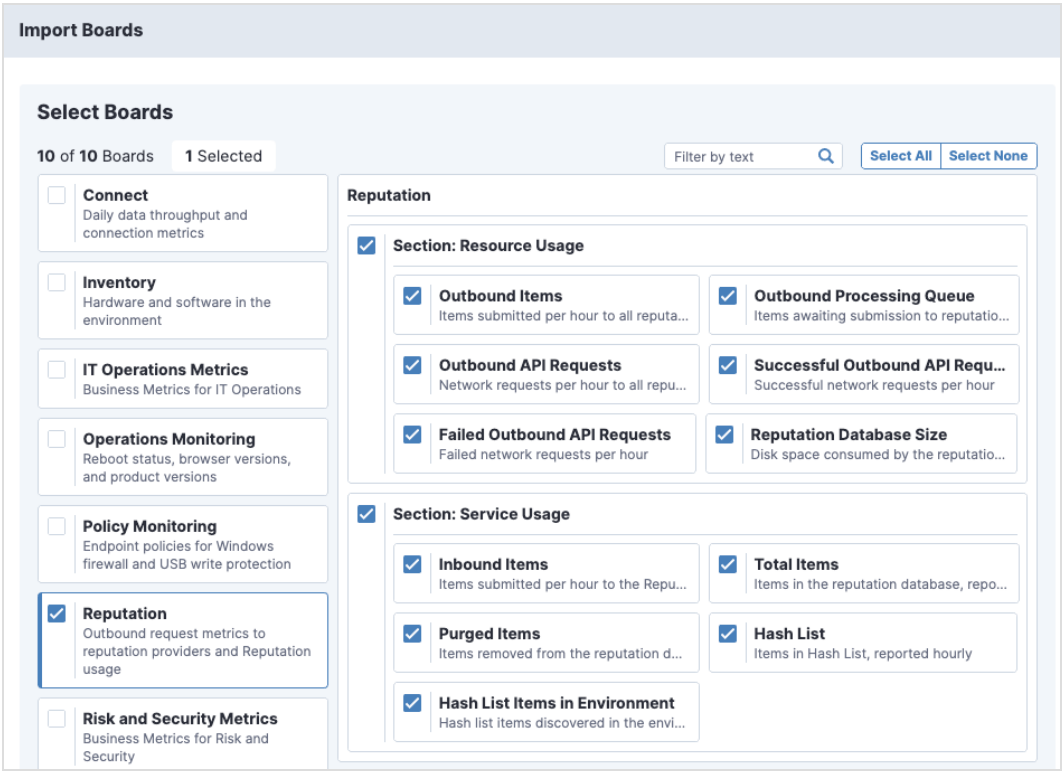
For more information, see Tanium Connect User Guide: Managing connections.

Send data to Trends boards

Use Trends 3.6.323 or later to import a board that contains different panels of reputation metrics. By default, the Reputation **Overview** page shows the metrics from the Service Usage section of the Reputation board.

© 2025 Tanium Inc. All Rights Reserved

1. From the Trends menu, click **Boards** and then click **Import > Gallery**.
2. Select **Reputation** and then select which sections or panels you want to import.



   By default, everything is selected.
3. Click **Validate**.

   > NOTE
   >
   > If you see a warning about missing content sets, select **Reputation**.

4. Click **Import**.

For more information, see Tanium Trends User Guide: Importing the initial gallery.

© 2025 Tanium Inc. All Rights Reserved

Maintaining Reputation

Perform monthly maintenance tasks to ensure that Reputation successfully performs scheduled activities on all the targeted endpoints and does not overuse endpoint or network resources. If Reputation is not performing as expected, you might need to troubleshoot issues or change settings. See Troubleshooting Reputation on page 44 for related procedures.

Review and remediate Tanium Reputation issues

1. From the Main menu, go to **Modules > Trends > Boards**.
2. Click the **Reputation** board and review the panels for issues that need attention.
3. If the **Failed Outbound API Requests** panel displays failures, verify that the reputation providers are configured correctly. See .
4. If data shows up faster in the **Inbound Items** panel than in the **Outbound Items** panel and the **Outbound Processing Queue** panel is consistently high, configure the reputation providers to send fewer hashes by lowering the **Maximum Hashes Processed Per Day** value.
5. To troubleshoot other Reputation issues or collect logs for a support package, see .

Check the Trends metrics for potential issues

1. From the Trends menu, click **Boards** and then click **Reputation**.
2. If the **Failed Outbound API Requests** panel displays failures, verify that your reputation providers are configured correctly.
3. If data shows up faster in the **Inbound Items** panel than it does in the **Outbound Items** panel and the **Outbound Processing Queue** panel is consistently high, configure your reputation providers to send fewer hashes.

© 2025 Tanium Inc. All Rights Reserved

Troubleshooting Reputation

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

Collect logs

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

1. From the Reputation **Overview** page, click Help, then the **Troubleshooting** tab.
2. Click **Create Package**.
   A `reputation-support.[timestamp].zip` file downloads to the local download directory.
3. Contact Tanium Support to determine the best option to send the ZIP file. For more information, see Contact Tanium Support on page 45.

Tanium Reputation maintains logging information in the `reputation-service.log` file in the `<Module Server>\services\reputation-service` directory.

Uninstall Reputation

The basic Reputation shared service uninstallation is designed so that the data you have collected is restored if you later decide to reinstall Reputation. In some cases, you might want to start "clean" and not restore the data. To do this, you must manually remove some files.

IMPORTANT

Consult with Tanium Support before you uninstall or reinstall Reputation.

Uninstall Reputation so data is restored on reinstall

1. Sign in to the Tanium Console as a user with the Administrator role.
2. From the Main menu, go to **Administration > Configuration > Solutions**.
3. In the **Content** section, select the **Reputation** row and click **Uninstall**.
4. Review the summary and click **Yes** to proceed with the uninstallation.
5. When prompted to confirm, enter your password.

If you later import the Reputation shared service, the previous data is restored.

© 2025 Tanium Inc. All Rights Reserved

Uninstall Reputation so you start fresh when you reinstall

1. Uninstall Reputation so data is restored on reinstall on page 44.
2. Manually delete the `<Module Server>\services\reputation-files\` directory.

Deleting the `reputation-files` directory removes all existing Reputation data. All logs, output, the Reputation database, and any other Reputation data is deleted. If you later import the Reputation shared service, the previous data is not restored.

Contact Tanium Support

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

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

© 2025 Tanium Inc. All Rights Reserved