



Tanium™ Reputation User Guide

Version 5.2.0

January 21, 2020

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.

© 2020 Tanium Inc. All rights reserved.

Table of contents

- Reputation overview 6**
- Reputation item life cycle 6
- Reputation items are added to the reputation database 6
- Reputation items are scanned 6
- WildFire 6
- Recorded Future 7
- ReversingLabs A1000 7
- ReversingLabs TitaniumCloud 7
- VirusTotal 7
- Reputation items are rescanned 7
- Wildfire 7
- Recorded Future 7
- ReversingLabs A1000 8
- ReversingLabs TitaniumCloud 8
- VirusTotal 8
- Items are removed from the reputation database 8
- Whitelist/Blacklist 9
- Getting started 10**
- Reputation requirements 11**
- Tanium dependencies 11
- Tanium™ Module Server 11
- Third-party software 11
- Host and network security requirements 11

Ports	12
Security exclusions	12
Internet URLs	12
User role requirements	12
Installing Reputation	15
Before you begin	15
Import Reputation	15
Verify installation	15
Set the service account	15
Configure reputation service settings	16
What to do next	16
Configuring connect sources	17
View reputation scan status	17
Configure Palo Alto Networks WildFire reputation source	17
Prerequisites	18
Configure settings	18
Configure Recorded Future reputation source	18
Prerequisites	18
Configure settings	19
Configure ReversingLabs A1000 reputation source	20
Prerequisites	20
Configure settings	20
Configure ReversingLabs TitaniumCloud reputation source	21
Prerequisites	21
Configure settings	21

Configure VirusTotal reputation source	22
Prerequisites	22
Configure settings	23
Managing whitelist or blacklist data	25
Add data hashes	25
Import hashes	25
Export hashes	26
Edit notes	26
Delete hashes	26
Exporting connect data	27
View reputation data	27
Send data to Connect destinations	27
Send data to the reputation service	29
Send data to Trends boards	29
Troubleshooting Reputation	31
Collect logs	31
Uninstall Reputation	31
Uninstall Reputation so data is restored on reinstall	31
Uninstall Reputation so you start fresh when you reinstall	32

Reputation overview

With Reputation, you can build a repository of reputation data from various sources, such as Palo Alto WildFire, Recorded Future, ReversingLabs, and VirusTotal. These sources determine threat levels for file hashes. Other Tanium products, such as Tanium™ Trace, 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 source*. A reputation source 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 get added to the reputation database in the following scenarios:

- When a new hash gets identified by a Tanium process, such as Trace.
- When a list of hashes gets sent to Connect from a saved question connection source.

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 have multiple reputation service providers configured, a reputation item is created for each reputation source. 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 are sent at a time, and how many times the API is called in one minute. For more information about these settings, see [Configure Recorded Future reputation source on page 18](#).

REVERSINGLABS A1000

The settings for ReversingLabs A1000 determine how many hashes are sent at a time, and how many times the API is called in one minute. For more information about these settings, see [Configure ReversingLabs A1000 reputation source on page 20](#).

REVERSINGLABS TITANIUMCLOUD

The settings for ReversingLabs TitaniumCloud determine how many hashes are sent at a time, and how many times the API is called in one minute. For more information about these settings, see [Configure ReversingLabs TitaniumCloud reputation source on page 21](#).

VIRUSTOTAL

The settings for VirusTotal determine how many hashes are sent at a time, and how many times the API is called in one minute. For more information about these settings, see [Configure VirusTotal reputation source on page 22](#).

Reputation items are rescanned

Reputations might change for reputation items over time. When an item is rescanned, it is checked against the reputation sources again. For more information about configuring the rescanning properties, see [Configure reputation service settings on page 16](#).

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

WILDFIRE

Items are only scanned on the **Rescan Item Interval** value.

RECORDED FUTURE

You can configure items to be rescanned as Recorded Future gets new reputations for hashes.

The **Maximum Age of New Items** setting gets compared with the First Seen attribute in Recorded Future. The First Seen attribute is the date at which Recorded Future first recorded any instance of that hash, from any Recorded Future customer. If the item is less

than the configured maximum, the item is rescanned. How often the new items are rescanned is determined by the **Rescan New Item Interval** setting.

REVERSINGLABS A1000

You can configure items to be rescanned as ReversingLabs A1000 gets new reputations for hashes.

The **Maximum Age of New Items** setting gets compared with the First Seen attribute in ReversingLabs A1000. The First Seen attribute is the date at which ReversingLabs A1000 first recorded any instance of that hash. If the item is less than the configured maximum, the item is rescanned. How often the new items are rescanned is determined by the **Rescan New Item Interval** setting.

REVERSINGLABS TITANIUMCLOUD

You can configure items to be rescanned as ReversingLabs TitaniumCloud gets new reputations for hashes.

The **Maximum Age of New Items** setting gets compared with the First Seen attribute in ReversingLabs TitaniumCloud. The First Seen attribute is the date at which ReversingLabs TitaniumCloud first recorded any instance of that hash, from any ReversingLabs TitaniumCloud customer. If the item is less than the configured maximum, the item is rescanned. How often the new items are rescanned is determined by the **Rescan New Item Interval** setting.

VIRUSTOTAL

If you have a paid API key for VirusTotal, you can configure items to be rescanned as VirusTotal gets new reputations for hashes.

The **Maximum Age of New Items** setting gets compared with the First Seen attribute in VirusTotal. The First Seen attribute is the date at which VirusTotal first recorded any instance of that hash, from any VirusTotal customer. If the item is less than the configured maximum, the item is rescanned. How often the new items are rescanned is determined by the **Rescan New Item Interval** setting.

When you are configuring 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 gets found again.

Whitelist/Blacklist

The Reputation Whitelist/Blacklist is a list of reputation hashes that are known to be false detections or known to be malicious. You can add or delete specific hashes from the Whitelist/Blacklist, or you can export and import the entire list.

For more information, see [Managing whitelist or blacklist data on page 25](#).

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.

Getting started

1. Install Tanium Reputation. See [Installing Reputation on page 15](#).
2. Configure and enable Reputation sources. See [Configuring connect sources on page 17](#).
3. Manage the Reputation Whitelist/Blacklist. See [Managing whitelist or blacklist data on page 25](#).
4. Export Reputation data. See [Exporting connect data on page 27](#).

Reputation requirements

Review the requirements before you install and use Reputation.

Tanium dependencies

Make sure that your environment meets the following requirements.

Component	Requirement
Platform	7.2 or later.
Tanium™ Client	No client requirements.
Tanium Connect	4.11 or later (optional).
Tanium™ Incident Response	For hash data (optional).
Tanium Trace	2.0.5 for reputation data (optional).
Tanium Trends	2.4 or later (optional).

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.

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
- 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.

Component	Port	Direction	Purpose
Module Server	17455	Inbound	Internal purposes; not externally accessible

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 1: Reputation security exclusions

Target Device	Process
Module Server	<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 add the following URLs to the whitelist.

- reversinglabs.com
- virustotal.com
- wildfire.paloaltonetworks.com

User role requirements

Table 2: Reputation user role permissions

Permission	Reputation Administrator	Reputation Service Account
Show Reputation¹ View the Reputation workbench	✓ ²	✗
Reputation Read Read access to the Reputation shared service	✓ ²	✗

Permission	Reputation Administrator	Reputation Service Account
Reputation Write³ Write access to the Reputation shared service	✓ ²	✗
Reputation Administrator Administrative access to the Reputation shared service	✓	✗
Connect Plugin Management Access to manage Connect plugins	✗	✓ ⁴
Reputation Service Account Access to module service accounts to read and write data	✗	✓
Trends Integration Service Account Access for module service accounts to read and write data, and to define sources and boards	✗	✓ ⁵
Trends Api Board Read View boards, sections, and panels for specified content sets	✓ ⁵	✗
Trends Api Board Write Create, edit, delete, and configure boards, sections, and panels for specified content sets	✓ ⁵	✗
Trends Api Source Read View and list sources for specified content sets	✓ ⁵	✗
Trends Api Source Write Create, edit, and delete sources for specified content sets	✓ ⁵	✗

Permission	Reputation Administrator	Reputation Service Account
Trends Data Read Run data queries against sources	✓ ⁵	✗
<p>¹ To install Reputation, you must have the reserved role of Administrator.</p> <p>² Denotes a provided permission.</p> <p>³ If you need access to only the Reputation API, you can add the Reputation Write permission to your user.</p> <p>⁴ Denotes a permission when Connect 4.11 or later is installed.</p> <p>⁵ Denotes a permission when Trends 2.4 or later is installed.</p>		

Table 3: Provided Reputation Advanced user role permissions

Permission	Content Set for Permission	Reputation Administrator	Reputation Service Account
Execute Plugin	Reputation	✓	✓
Execute Plugin	Connect	✗	✓ ¹
Execute Plugin	Trends	✓ ²	✓ ²
<p>¹ Denotes a provided permission when Connect 4.12 or later is installed.</p> <p>² Denotes a provided permission when Trends 3.0 or later is installed.</p>			

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

Installing Reputation

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

Before you begin

- Read the [release notes](#).
- Review the [Reputation requirements on page 11](#).
- 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](#).

Import Reputation

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


1. From the Main menu, click **Tanium Solutions**.
2. In the **Tanium Content** section, select the Reputation row and click **Import Solution**.
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 **Tanium Services > Reputation**. The Reputation **Home** page is displayed.

Verify installation

To verify that Reputation is installed, go to the **Tanium Solutions** page and check the installed version.

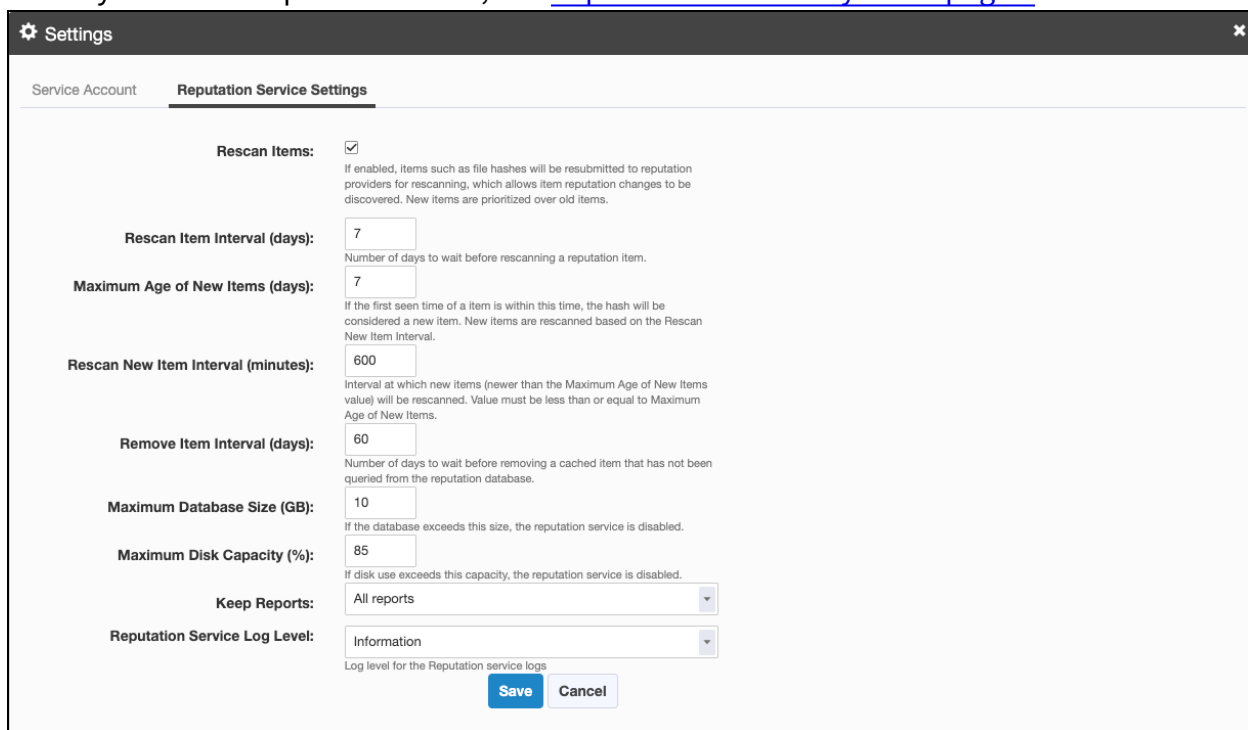
Set the service account

For recurring maintenance activities, specify a Tanium user with the Reputation Service Account role. Specifying these credentials is a one-time configuration. No other credentials need to be added.

1. From the Reputation **Home** page, click Settings .
2. In the **Service Account** tab, enter the Tanium credentials and click **Save**.

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 6](#).



The screenshot shows a 'Settings' window with a 'Reputation Service Settings' tab. The settings are as follows:

Setting	Value	Description
Rescan Items:	<input checked="" type="checkbox"/>	If enabled, items such as file hashes will be resubmitted to reputation providers for rescanning, which allows item reputation changes to be discovered. New items are prioritized over old items.
Rescan Item Interval (days):	7	Number of days to wait before rescanning a reputation item.
Maximum Age of New Items (days):	7	If the first seen time of a item is within this time, the hash will be considered a new item. New items are rescanned based on the Rescan New Item Interval.
Rescan New Item Interval (minutes):	600	Interval at which new items (newer than the Maximum Age of New Items value) will be rescanned. Value must be less than or equal to Maximum Age of New Items.
Remove Item Interval (days):	60	Number of days to wait before removing a cached item that has not been queried from the reputation database.
Maximum Database Size (GB):	10	If the database exceeds this size, the reputation service is disabled.
Maximum Disk Capacity (%):	85	If disk use exceeds this capacity, the reputation service is disabled.
Keep Reports:	All reports	
Reputation Service Log Level:	Information	Log level for the Reputation service logs

Buttons: Save, Cancel

To update these settings, click Settings  and then click **Reputation Service Settings**.

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.

What to do next






See [Getting started on page 10](#) for more information about using Reputation.

Configuring connect sources

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

View reputation scan status

The Reputation **Home** page displays the total number of reputation items, and the following information about each reputation source:

Enabled Sources	Total Items	Total New	Total Processed	Malicious
5 100% of all	330	0	330 0 rescanning	9.1% 30 items
 Palo Alto Networks WildFire	Items: 63	New: ---	Processed: 63 0 rescanning	Malicious: 6.3% 4 items
 Recorded Future	Items: 63	New: ---	Processed: 63 0 rescanning	Malicious: 7.9% 5 items
 ReversingLabs A1000	Items: 68	New: ---	Processed: 68 0 rescanning	Malicious: 8.8% 6 items
 ReversingLabs TitaniumCloud	Items: 68	New: ---	Processed: 68 0 rescanning	Malicious: 17.6% 12 items
 VirusTotal	Items: 68	New: ---	Processed: 68 0 rescanning	Malicious: 4.4% 3 items

- **Items:** total number of reputation items on this reputation source
- **New:** reputation items that still need to be scanned on this reputation source
- **Processed:** reputation items that have been scanned on this reputation source
- **Malicious:** percentage of items out of total reputation items that are malicious

Configure Palo Alto Networks WildFire reputation source

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.

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

1. From the Reputation **Home** page, click Settings  in the Palo Alto Networks WildFire section.



The screenshot shows the configuration interface for the Palo Alto Networks WildFire reputation service. It includes the following fields and options:

- Host:** (Host name for the Palo Alto Networks WildFire instance.)
- Palo Alto Networks WildFire API Key:**
- Batch Size:** (The number of hashes to process in a batch.)
- Maximum API Calls Per Minute:** (The maximum number of batches processed in a minute.)
- Maximum API Calls Per Day:** (The maximum number of calls per day. (Call count will reset daily. Set to 0 for unlimited calls.)
- Max Hashes Processed Per Day:** 57600
- Use Tanium Module Server Proxy Setting (Use proxy setting defined on your Tanium Module Server.)
- Enabled** (Enable the Reputation Service to use this service provider)

Buttons for **Save** and **Cancel** are located at the bottom right of the form.

2. Specify settings, including the host of your WildFire instance and the API key.
3. Adjust the settings for **Batch Size**, **Maximum Calls Per Minute**, and **Maximum Calls Per Day** according to your agreement with Palo Alto Networks. The **Max Hashes Processed Per Day** value is automatically calculated based on these configured settings.
4. Select **Enabled** to enable the reputation source and click **Save**.

Configure Recorded Future reputation source

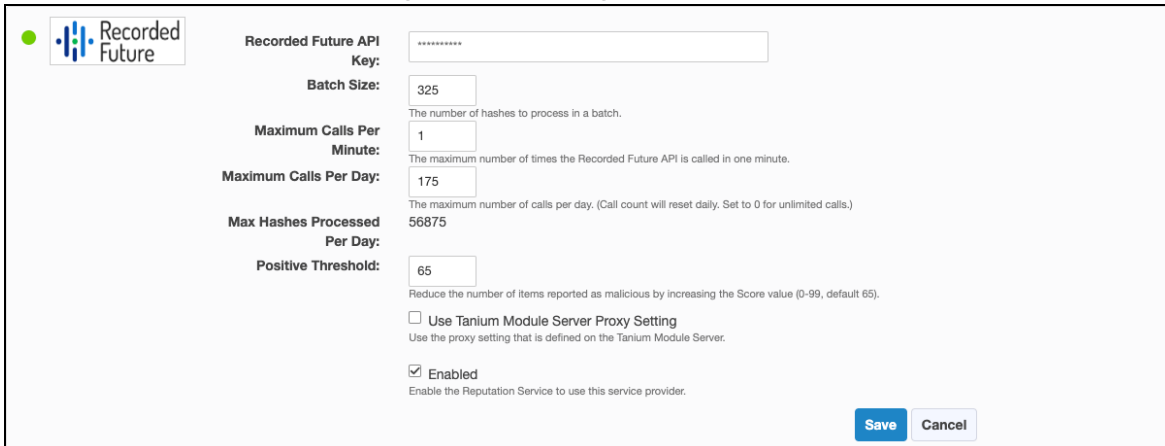
Recorded Future is a cloud-based reputation service provider. The reputation service sends reputation items to the Recorded Future API and returns the results to the reputation database.

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

1. From the Reputation **Home** page, click Settings  in the Recorded Future section.



Recorded Future

Recorded Future API Key: *****

Batch Size: 325
The number of hashes to process in a batch.

Maximum Calls Per Minute: 1
The maximum number of times the Recorded Future API is called in one minute.

Maximum Calls Per Day: 175
The maximum number of calls per day. (Call count will reset daily. Set to 0 for unlimited calls.)

Max Hashes Processed Per Day: 56875

Positive Threshold: 65
Reduce the number of items reported as malicious by increasing the Score value (0-99, default 65).

Use Tanium Module Server Proxy Setting
Use the proxy setting that is defined on the Tanium Module Server.

Enabled
Enable the Reputation Service to use this service provider.

Save Cancel

2. Specify settings for Recorded Future, including the API key.
 - Adjust the settings for **Batch Size**, **Maximum Calls Per Minute**, and **Maximum Calls Per Day** according to your agreement with Recorded Future. The **Max Hashes Processed Per Day** value is automatically calculated based on these configured settings.
 - The **Positive Threshold** is the risk score as determined by Recorded Future. The default value is **65**, which means that any hash that has a Recorded Future risk score of 65 or higher is considered malicious by Reputation.

Recorded Future risk scores are determined as follows:

- Very Malicious: risk score of 90-99
- Malicious: risk score of 65-89
- Suspicious: risk score of 25-64
- Unusual: risk score of 5-24
- No current evidence of risk: risk score of zero

Tip: 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.

3. Select **Enabled** to enable the reputation source and click **Save**.

Configure ReversingLabs A1000 reputation source

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

Prerequisites

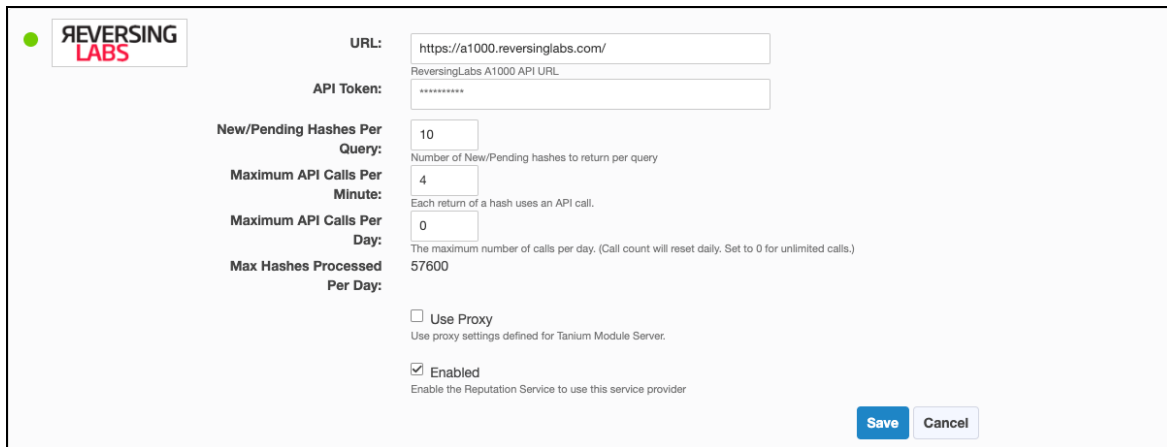
You must already have a ReversingLabs API token. If you have not already registered for ReversingLabs access, contact their sales team at reversinglabs.com.

To get an API key:

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

Configure settings

1. From the Reputation **Home** page, click Settings  in the ReversingLabs A1000 section.



The screenshot shows the configuration interface for the ReversingLabs A1000 reputation source. It includes the following fields and options:

- URL:**
- API Token:**
- New/Pending Hashes Per Query:** (Number of New/Pending hashes to return per query)
- Maximum API Calls Per Minute:** (Each return of a hash uses an API call.)
- Maximum API Calls Per Day:** (The maximum number of calls per day. (Call count will reset daily. Set to 0 for unlimited calls.))
- Max Hashes Processed Per Day:** 57600
- Use Proxy** (Use proxy settings defined for Tanium Module Server.)
- Enabled** (Enable the Reputation Service to use this service provider)

Buttons for **Save** and **Cancel** are located at the bottom right.

2. Add your ReversingLabs A1000 credentials: the **URL** for your API access and your **API Token**.
3. 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 **Max Hashes Processed Per Day** value is automatically calculated based on these configured settings.
4. Select **Enabled** to enable the reputation source and click **Save**.


Configure ReversingLabs TitaniumCloud reputation source

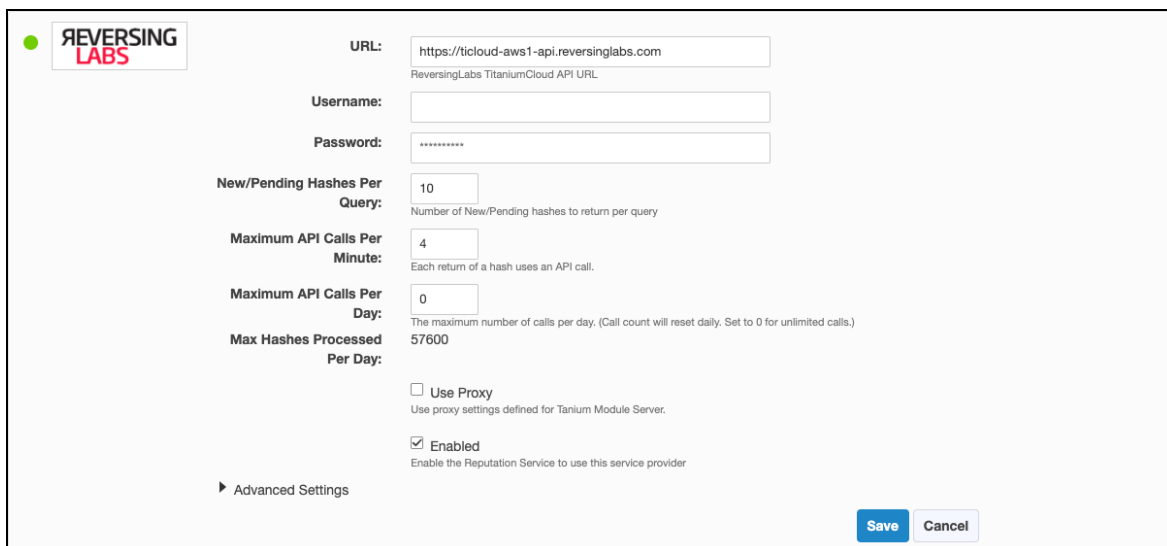
ReversingLabs TitaniumCloud is an online service that analyzes files, hashes, and URLs to identify viruses, worms, trojans, and other kinds of malicious content that is detected by antivirus engines and website scanners. The reputation service sends reputation items to the ReversingLabs API and returns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

1. From the Reputation **Home** page, click Settings  in the ReversingLabs TitaniumCloud section.



The screenshot shows the configuration interface for the ReversingLabs TitaniumCloud reputation source. It includes the following fields and options:

- URL:** (ReversingLabs TitaniumCloud API URL)
- Username:**
- Password:**
- New/Pending Hashes Per Query:** (Number of New/Pending hashes to return per query)
- Maximum API Calls Per Minute:** (Each return of a hash uses an API call.)
- Maximum API Calls Per Day:** (The maximum number of calls per day. (Call count will reset daily. Set to 0 for unlimited calls.)
- Max Hashes Processed Per Day:** 57600
- Use Proxy** (Use proxy settings defined for Tanium Module Server.)
- Enabled** (Enable the Reputation Service to use this service provider)

At the bottom left, there is a link for **Advanced Settings**. At the bottom right, there are **Save** and **Cancel** buttons.

2. Add your ReversingLabs TitaniumCloud credentials: the **URL** for your API access, your **Username**, and your **Password**.
3. 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 **Max Hashes Processed Per Day** value is automatically calculated based on these configured settings.
4. To reduce the number of items reported as malicious, expand **Advanced Settings** and adjust the settings for **Threat Level** and **Trust Factor**.

▼ Advanced Settings

Reduce the number of items reported as malicious by increasing the Threat Level and/or Trust Factor values.

Threat Level: 0 1 2 3 4 5

0: No Threat

Threat Level measures how malicious a malware sample is perceived.

Trust Factor: 0 1 2 3 4 5

0: Maximum Trust

Trust Factor depends on the software vendor.

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.

5. Select **Enabled** to enable the reputation source and click **Save**.

Configure VirusTotal reputation source

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.

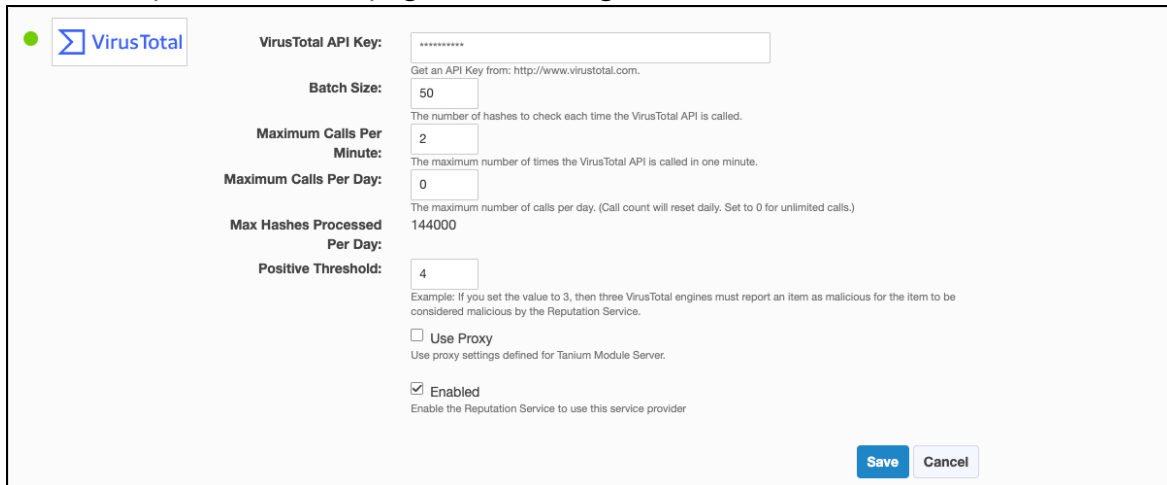
Prerequisites

Register for a VirusTotal API key at [virustotal.com](https://www.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. From the Reputation **Home** page, click Settings  in the VirusTotal section.



VirusTotal

VirusTotal API Key:

Get an API Key from: <http://www.virustotal.com>.

Batch Size:
The number of hashes to check each time the VirusTotal API is called.

Maximum Calls Per Minute:
The maximum number of times the VirusTotal API is called in one minute.

Maximum Calls Per Day:
The maximum number of calls per day. (Call count will reset daily. Set to 0 for unlimited calls.)

Max Hashes Processed Per Day: 144000

Positive Threshold:
Example: If you set the value to 3, then three VirusTotal engines must report an item as malicious for the item to be considered malicious by the Reputation Service.

Use Proxy
Use proxy settings defined for Tanium Module Server.

Enabled
Enable the Reputation Service to use this service provider

2. Specify settings for VirusTotal, including the API key.
 - Adjust the settings for **Batch Size**, **Maximum Calls Per Minute**, and **Maximum Calls Per Day** according to your agreement with VirusTotal. The **Max Hashes Processed Per Day** value is automatically calculated based on these configured settings.
 - The **Positive Threshold** is a number of positive reports that must be on the hash to be considered a potential threat or malware.

Tip: 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

3. Select **Enabled** to enable the reputation source and click **Save**.

Managing whitelist or blacklist data

To view a list of hashes that have been whitelisted or blacklisted, click **Whitelist/Blacklist** from the Reputation **Home** page. You can also search for file hashes and add, import, export, or delete reputation data hashes.

Add data hashes

1. From the Reputation **Home** page, click **Whitelist/Blacklist** and then click **Add Hashes**.
2. To add hashes that are known to be malicious to the blacklist, enter a hash, select **blacklist**, and click **Save to Blacklist**.
3. To add hashes that are known to be false detections to the whitelist, enter a hash, select **whitelist**, and click **Save to Whitelist**.

Import hashes

1. From the Reputation **Home** page, click **Whitelist/Blacklist** and then click **Import Hashes**.

Import Hashes

The uploaded file must be a CSV file with the "hash" and "list" header fields.

```
hash,list
fadb1154b2a36dc45264a8f74b919105,whitelist
356b5b978323b83b1182d8c914bc3b51,blacklist
```

You can also upload the same CSV format as the Whitelist/Blacklist export file.


Replace Current Hashes **Append** Cancel

2. To replace the current hashes, click **Replace Current Hashes** and select your file in CSV format or a previously exported Whitelist/Blacklist file.
3. To append to the current hashes, click **Append** and select your file in CSV format or a previously exported Whitelist/Blacklist file.

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 Whitelist/Blacklist file, edit the file to add hashes in the appropriate columns for a specific row, and then import the updated file using the **Replace Current Hashes** option.


Export hashes

1. From the Reputation **Home** page, click **Whitelist/Blacklist**.
2. To export specific hashes, select one or more hashes and click Export .
3. To export all hashes, click **Download All**.

Edit notes

1. From the Reputation **Home** page, click **Whitelist/Blacklist**.
2. Select a hash and click **Edit Note**.

Delete hashes

1. From the Reputation **Home** page, click **Whitelist/Blacklist**.
2. To delete specific hashes, select one or more hashes and click Delete .
3. To delete all hashes, click **Delete All**.

Exporting connect data

View reputation data

To view a list of the malicious hashes that Reputation has pulled from the reputation services, click **Malicious Reputations** from the Reputation menu.

Type	Value	Service	Updated On
hash	c33a4765676df4b1ba7e8cb0db4ce26633576d8807749002b136b5e37f580da7	WILDFIRE	2019-05-21 21:33:06.480
hash	5dcf26e3fbce71902b0cd7c72c60545b	CUSTOM	2019-05-21 21:33:06.480
hash	b3feb9beaf167edd556bd7334e3833b2	CUSTOM	2019-05-21 21:33:06.480

Only hashes with a malicious or pending status are listed.

In Trace, you can view the ratings on hashes for Live Endpoints or Snapshots. For more information, see [Tanium Trace User Guide: How reputation data works with Trace](#).

Send data to Connect destinations


You can use Connect 4.11 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.

1. From the Connect menu, click **Connections**.
2. Click **Create Connection > Create** to create a new connection.

3. When you select a source for the connection, select **Tanium Reputation**.

Source and Destination

Source: Where is the data coming from?



Tanium Reputation

Reputation Status To Include:

Advanced

Timeout:

ALL
Include all reputation responses.

MALICIOUS
List reputation responses that were reported as a threat or malware.

NON_MALICIOUS
List reputation responses that do not include evidence of threat or malware.

SUSPICIOUS
List reputation responses that were reported as a possible threat or malware.

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 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 about the status of the items from the reputation sources.

1. From the Connect menu, click **Connections**.
2. Click **Create Connection > Create** to create a new connection.
3. For the source, choose a saved question that returns a hash, such as **Running Processes with MD5 Hash**.
4. For the destination, choose **Tanium Reputation** and select the appropriate hash type for the **Hash Field**.

The screenshot shows a configuration window titled "Source and Destination" with two main sections: "Source" and "Destination".

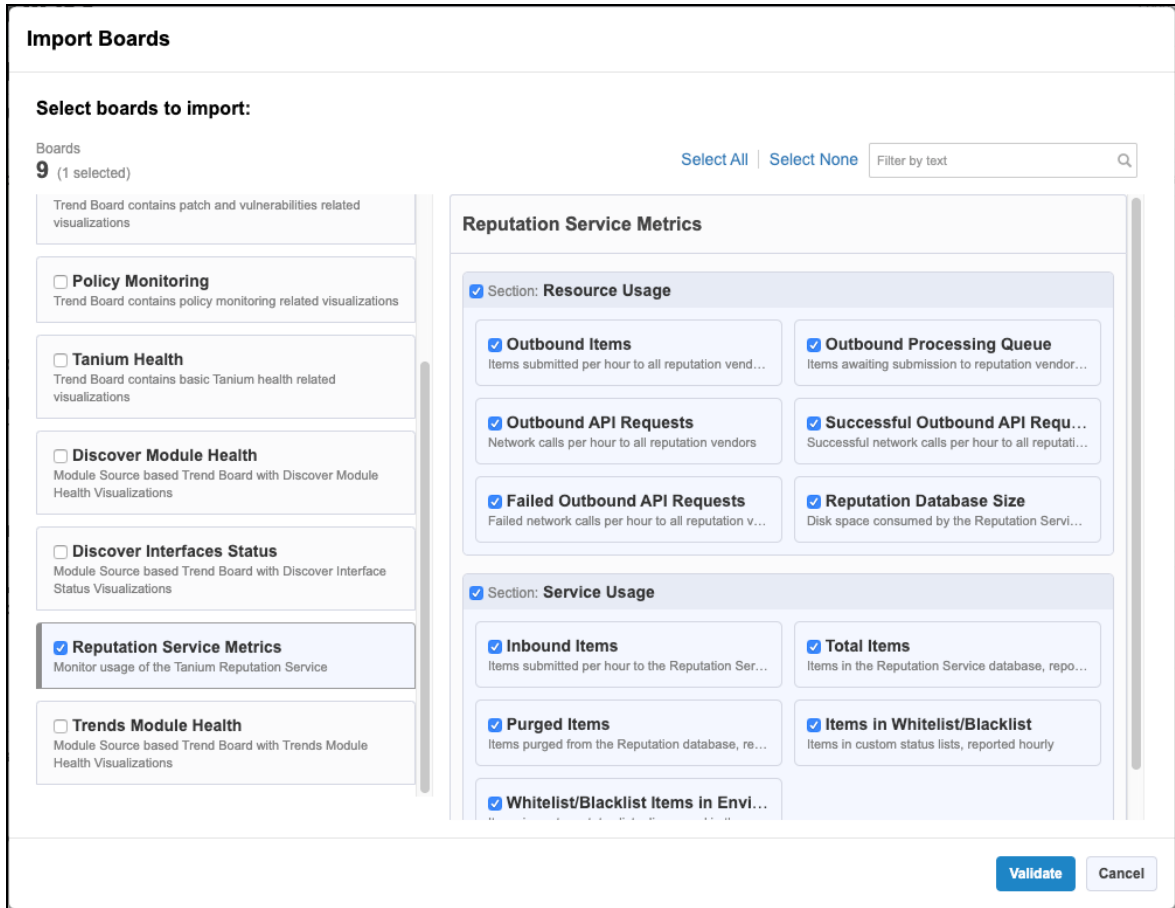
- Source:** "Where is the data coming from?"
 - Source: TANIUM
 - Saved Question: Running Processes with MD5 hash
 - Saved Question Name: Running Processes with MD5 hash
 - Computer Group: All Computers
 - Advanced: (collapsed)
- Destination:** "Where is the data going?"
 - Destination: TANIUM
 - Destination: Tanium Reputation
 - Hash Field: MD5 Hash
 - Hash Field Description: The column name in the results of the saved question that contains the hash (MD5, SHA1, SHA256) of the file to be checked.
 - Advanced Settings: (collapsed)

IMPORTANT: Each reputation service connection destination is configured for a specific hash column name. You must use a separate destination for each hash type that you are populating. For example, if you are populating both MD5 and SHA1 hashes from different saved questions, create two connection destinations with different values for the **Hash Field** field.

Send data to Trends boards

You can use Trends 2.4 or later to import a board that contains different panels of reputation metrics.

1. From the Trends menu, click **Boards** and then click **Import > Gallery**.
2. Select **Reputation Service Metrics** 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](#).

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.

1. From the Reputation **Home** page, click Help , then the **Troubleshooting** tab.
2. Click **Collect**.
A `reputation-support.[timestamp].zip` file downloads to the local download directory.
3. Attach the ZIP file to your Tanium Support case form or send it to your TAM.

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 your TAM before you uninstall or reinstall Reputation.

Uninstall Reputation so data is restored on reinstall

1. Sign into the Tanium Console as a user with the Administrator role.
2. From the Main menu, click **Tanium Solutions**.
3. In the **Tanium Solutions** section, select the **Reputation** row and click **Uninstall Solution**.
4. Review the summary and click **Proceed with Uninstall**.
5. When prompted to confirm, enter your password.

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

Uninstall Reputation so you start fresh when you reinstall

1. [Uninstall Reputation so data is restored on reinstall on page 31.](#)
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.