



Tanium™ Reputation User Guide

Version 6.1.27

July 12, 2021

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

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

Please visit <https://docs.tanium.com> for the most current Tanium product documentation.

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

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

Tanium is committed to the highest accessibility standards to make interaction with Tanium software more intuitive and to accelerate the time to success. To ensure high accessibility standards, Tanium complies with the U.S. Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. We have conducted third-party accessibility assessments over the course of product development for many years, and most recently a comprehensive audit against the WCAG 2.1 / VPAT 2.3 standards for all major product modules was completed in September 2019. Tanium can make available any VPAT reports on a module-by-module basis as part of a larger solution planning process for any customer or prospect.

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

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

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.

© 2021 Tanium Inc. All rights reserved.

Table of contents

- Reputation overview** 7
 - Reputation item life cycle 7
 - Reputation items are added to the reputation database 7
 - Reputation items are scanned 7
 - WildFire 7
 - Recorded Future 7
 - ReversingLabs A1000 8
 - ReversingLabs TitaniumCloud 8
 - VirusTotal 8
 - Reputation items are rescanned 8
 - Wildfire 8
 - Recorded Future 8
 - ReversingLabs A1000 8
 - ReversingLabs TitaniumCloud 8
 - VirusTotal 9
 - Items are removed from the reputation database 9
 - Hash List 9
 - Integration with other Tanium products 9
 - Connect 9
 - Threat Response 9
 - Trends 10
- Getting started** 11
 - Step 1: Install and configure Reputation 11
 - Step 2: Enable Reputation sources 11
 - Step 3: Manage hashes 11
 - Step 4: Export data 11
- Reputation requirements** 12

Tanium dependencies	12
Tanium™ Module Server	12
Endpoints	12
Third-party software	13
Host and network security requirements	13
Ports	13
Security exclusions	13
Internet URLs	14
User role requirements	14
Installing Reputation	17
Before you begin	17
Import and configure Reputation with default settings	17
Import and configure Reputation with custom settings	17
Configure service account	18
Configure Reputation service settings	18
Upgrade Reputation	19
Verify Reputation version	19
What to do next	20
Configuring Reputation sources	21
View reputation scan status	21
Configure Palo Alto Networks WildFire reputation source	21
Prerequisites	21
Configure settings	22
Configure Recorded Future reputation source	23
Prerequisites	23
Configure settings	24
Configure ReversingLabs A1000 reputation source	26
Prerequisites	26
Configure settings	27
Configure ReversingLabs TitaniumCloud reputation source	28

Prerequisites	28
Configure settings	29
Configure VirusTotal reputation source	32
Prerequisites	32
Configure settings	32
Managing hashes	34
Add data hashes	34
Import hashes	35
Export hashes	36
Edit notes	36
Remove hashes	36
Exporting Reputation data	37
View reputation data	37
Send data to Connect destinations	37
Send data to the reputation service	38
Send data to Trends boards	40
Troubleshooting Reputation	42
Collect logs	42
Check the Trends metrics for potential problems	42
Uninstall Reputation	42
Uninstall Reputation so data is restored on reinstall	42
Uninstall Reputation so you start fresh when you reinstall	43
Contact Tanium Support	43

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™ 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 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 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 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 to send at a time, and the maximum API calls per minute/day. For more information about these settings, see [Configure Recorded Future reputation source on page 23](#).

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 source on page 26](#).

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 source on page 28](#).

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 source on page 32](#).

Reputation items are rescanned

Reputations might change for reputation items over time. When Reputation rescans an item, it is checked against the reputation sources again. For more information on how to configure the rescan properties, see [Configure Reputation service settings 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.

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. 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 34](#).

Integration with other Tanium products

Reputation has built in integration 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 37](#) and [Send data to the reputation service on page 38](#).

Threat Response

You can use 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.

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 40](#) and [Tanium Trends User Guide: Importing the initial gallery](#).

Getting started

Step 1: Install and configure Reputation

Install and configure Tanium Reputation.

For more information, see [Installing Reputation on page 17](#).

Step 2: Enable Reputation sources

Configure and enable Reputation sources.

For more information, see [Configuring Reputation sources on page 21](#).

Step 3: Manage hashes

Manage hashes. The **Reputations** section of the Reputation **Overview** page shows a list of hashes that are malicious or non-malicious. You can also search for file hashes and add, import, export, or delete reputation data hashes.

For more information, see [Managing hashes on page 34](#).

Step 4: Export data

Export Reputation data.

For more information, see [Exporting Reputation data on page 37](#).

Reputation requirements

Review the requirements before you install and use Reputation.

Tanium dependencies

Make sure that your environment meets the following requirements.

Component	Requirement
Tanium™ Core Platform	7.3.314.4250 or later
Tanium™ Client	No client requirements.
Tanium products	<p>If you selected Tanium Recommended Installation when you installed Reputation, the Tanium Server automatically installed all your licensed modules at the same time. Otherwise, you must manually install the modules that Reputation requires to function, as described under Tanium Console User Guide: Manage Tanium modules.</p> <p>The following modules are optional, but Reputation requires the specified minimum versions to work with them:</p> <ul style="list-style-type: none">• Tanium Connect 5.2.3 or later• Tanium™ Incident Response for hash data• Tanium Threat Response 1.4 or later• Tanium Trends 3.6.323 or later

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.



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 [Configure Reputation service settings 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.

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



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

Security exclusions

If security software is in use in the environment to monitor and block unknown host system processes, your security administrator must create exclusions to allow the Tanium processes to run without interference. For a list of all security exclusions to define across Tanium, see [Tanium Core Platform Deployment Reference Guide: Host system security exclusions](#).

Reputation security exclusions

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 the following URLs.

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


User role requirements

The following tables list the role permissions required to use Reputation. For more information about role permissions and associated content sets, see [Tanium Core Platform User Guide: Managing RBAC](#).

Reputation user role permissions

Permission	Reputation Administrator ⁴	Reputation Operator ⁴	Reputation Service Account ^{3,4}
Reputation^{1,2} 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 List² Access to the Reputation hash list data	 READ WRITE	 READ WRITE	
Reputation Provider Access to the provider configurations	 READ WRITE	 READ WRITE	

Reputation user role permissions (continued)

Permission	Reputation Administrator ⁴	Reputation Operator ⁴	Reputation Service Account ^{3,4}
<p>Reputation Service Account</p> <p>Access to module service accounts to read and write data</p>	✘	✘	<p>✔</p> <p>EXECUTE</p>
<p>Reputation Whitelist Blacklist^{2, 5} (deprecated)</p> <p>Access to the Reputation hash list data</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> In Reputation 6.0.77 and later, use the Reputation Hash List permission instead.</p> </div>	✘	✘	✘

¹ 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.










² 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.

³ This role provides module permissions for Tanium Connect. You can view which Connect permissions are granted to this role in the Tanium Console. For more information, see [Tanium Connect User Guide: User role requirements](#).

⁴ This role provides module permissions for Tanium Trends. You can view which Trends permissions are granted to this role in the Tanium Console. For more information, see [Tanium Trends User Guide: User role requirements](#).

⁵ The **Reputation Whitelist Blacklist** read and write permissions are deprecated. When you upgrade to Version 6.0.77 or later, default roles (Reputation Administrator and Reputation Operator) automatically update to use the **Reputation Hash List** read and write permissions. You must manually update any custom roles that use the deprecated permissions.

Provided Reputation platform content permissions

	Content Set for Permission	Reputation Administrator	Reputation Operator	Reputation Service Account
Plugin	Reputation	 READ EXECUTE	 READ EXECUTE	 READ EXECUTE
Connect Plugin	Connect			 MANAGEMENT
Plugin	Trends	 READ EXECUTE	 READ EXECUTE	 READ EXECUTE

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

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

Installing Reputation

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

- **Automatic configuration with default settings** (Tanium Core Platform 7.4.2 or later only): 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 and configure Reputation with default settings on page 17](#).
- **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 and configure Reputation with custom settings on page 17](#).

Before you begin

- Read the [release notes](#).
- Review the [Reputation requirements on page 12](#).
- 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](#).
 - To import the Reputation solution, you must be assigned the Administrator reserved role or a role that has the **Import Signed Content** permission.

Import and configure 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.

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 and configure Reputation with custom settings


To import Reputation without automatically configuring default settings, be sure to deselect the **Apply All Tanium recommended configurations** check box while performing the steps in [Tanium Console User Guide: Import, re-import, or update specific solutions](#). After the import, verify that the correct version is installed: see [Verify Reputation version on page 19](#).

Configure service account

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

- **Reputation Service Account** role
- (Optional) **Connect User** role to send Reputation data to Tanium Connect

For more information about Reputation permissions, see [User role requirements on page 14](#).

1. From the Main menu, go to **Administration > Shared Services > Reputation** to open the Reputation **Overview** page.
2. Click Settings  and open the **Service Account** tab.
3. Update the service account settings 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 7](#).

Settings [X]

Service Account **Configuration Settings** * Required

Rescan

Rescan Items
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 *

7 Days
Number of days to wait before rescanning a reputation item.

Maximum Age of New Items *

7 Days
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 *

600 Minutes
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 *

60 Days
Number of days to wait before removing a cached item that has not been queried from the reputation database.

Maximum Database Size *

10 GB
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

Save Cancel

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

Upgrade Reputation

For the steps to upgrade Reputation, see [Tanium Console User Guide: Import, re-import, or update specific 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 **Administration > Shared Services > Reputation** to open the Reputation **Overview** page.
3. To display version information, click Info .

What to do next

See [Getting started on page 11](#) for more information about using Reputation.

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

Status	Name	Items	New	Processed	Rescanning	Malicious Items	Malicious %	Actions
⊖	Palo Alto Networks WildFire	0	0	0	0	0	-	Enable ⚙️
⊕	Recorded Future	28,763	28,719	44	44	26	0.1%	Disable ⚙️
⊖	ReversingLabs A1000	0	0	0	0	0	-	⚙️
⊕	ReversingLabs TitaniumCloud	23,960	0	23,960	0	9	0%	Disable ⚙️
⊕	VirusTotal	79,578	0	79,578	0	15	0%	Disable ⚙️
⊕	Hash List: Non-Malicious	1,145	-	-	-	0	0%	
⊕	Hash List: Malicious	200,659	-	-	-	200,659	100%	

- **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 scanned on this reputation source
- **Rescanning:** reputation items that are rescanning on this reputation source
- **Malicious Items:** malicious reputation items on this reputation source
- **Malicious %:** percentage of malicious items out of total reputation items

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

Edit Provider: Palo Alto Networks WildFire * Required

General Information

Status

Enabled

Enable the Reputation Service to use this service provider.

URL *

URL 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.)

Maximum Hashes Processed Per Day

57,600

Use Proxy

Use Tanium Module Server Proxy Setting

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

3. Specify the settings for Palo Alto Networks WildFire, including the URL for your WildFire instance and 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 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 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. In the **Providers** section, click Configure Provider  in the Recorded Future row.
2. Select **Enabled** to enable the reputation source.

Edit Provider: Recorded Future * Required

General Information

Status

Enabled

Enable the Reputation Service to use this service provider.

URL *

API Key *

Batch Size *

The number of hashes to process in a batch.

Maximum API Calls per Minute *

The maximum number of times the Recorded Future API is called in one minute.

Maximum API Calls per Day *

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

Maximum Hashes Processed Per Day

56,875

Positive Threshold *

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

Use Proxy

Use Tanium Module Server Proxy Setting

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

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.
5. Adjust the **Positive Threshold**, which is the risk score as determined by Recorded Future. The default value is 65, which means that any hash with a Recorded Future risk score of 65 or higher is considered malicious by Reputation.

Recorded Future risk scores are determined as follows:

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



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

Configure settings

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

Edit Provider: ReversingLabs A1000 * Required

General Information

Status

Enabled

Enable the Reputation Service to use this service provider.

URL *

ReversingLabs A1000 API 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.)

Maximum Hashes Processed Per Day

57,600

Use Proxy

Use Tanium Module Server Proxy Setting

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

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

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 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 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

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

 Reputation

Edit Provider: ReversingLabs TitaniumCloud * Required

General Information

Status

Enabled

Enable the Reputation Service to use this service provider.

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.)

Maximum Hashes Processed Per Day

57,600

Use Proxy

Use Tanium Module Server Proxy Setting

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

▶ Advanced

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**.

▼ **Advanced**

Threat Level *

0: No Threat ▼

Threat Level measures how malicious a malware sample is perceived.

Trust Factor *

0: Maximum Trust ▼

Trust Factor depends on the software vendor.



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

Edit Provider: VirusTotal * Required

General Information

Status
 Enabled
Enable the Reputation Service to use this service provider.

API Key *

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

Batch Size *

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

Maximum API Calls per Minute *

The maximum number of times the VirusTotal API is called in one minute.

Maximum API Calls per Day *

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

Maximum Hashes Processed Per Day
144,000

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

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.
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 , then three VirusTotal engines must report an item as malicious for the item to be sent to Connect.

Setting the value to 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:

1. Malicious: if the number of positives is greater than the threshold
 2. Suspicious: if the number of positives is greater than zero, but less than the threshold
 3. Non-malicious: if the number of positives is zero
 4. 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**.

Managing hashes

The **Reputations** section of the Reputation **Overview** page shows a list of hashes that are malicious or non-malicious. You can also search for file hashes and add, import, export, or delete reputation data hashes.

Add data hashes

1. In the **Reputations** section, click the **Hash List** tab.
2. Click **Add**.
3. To add hashes that are known to be malicious, select **Malicious**, enter the hashes, and click **Save**.
4. To add hashes that are known to be false detections, select **Non-Malicious**, enter the hashes, and click **Save**.



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

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

Add Hashes * Required

Hash Information

```
hash,list
fadb1154b2a36dc45264a8f74b919105,malicious
356b5b978323b83b1182d8c914bc3b51,non-malicious
```

The uploaded file must be a CSV file with the "hash" and "list" header fields. Hashes can be of type: md5, sha1, or sha256.

File *

Browse

Import a CSV file or a previously exported Hash List file.

Method

Replace existing list

Add to existing list

Save **Cancel**

The uploaded file must be a CSV file with `hash` and `list` header fields. Hashes can be MD5, SHA1, or SHA256.


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



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

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**.

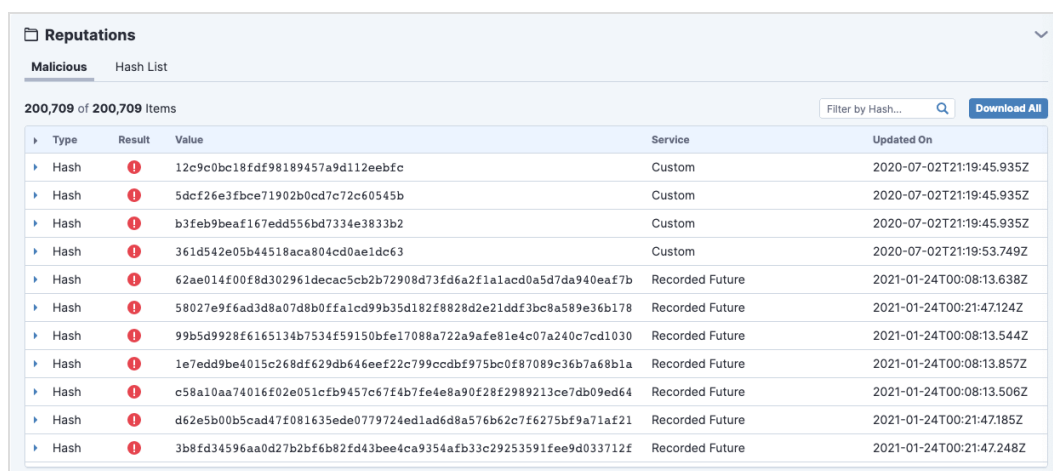
Remove hashes

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 .

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.



The screenshot shows the 'Reputations' section with the 'Malicious' tab selected. It displays a 'Hash List' containing 200,709 items. The table lists various hashes with their results (all marked as malicious with a red 'i' icon), their values, the services they were identified by, and the dates they were updated.

Type	Result	Value	Service	Updated On
Hash	i	12c9c0bc18fdf98189457a9d112eebfc	Custom	2020-07-02T21:19:45.935Z
Hash	i	5dcf26e3fbce71902b0cd7c72c60545b	Custom	2020-07-02T21:19:45.935Z
Hash	i	b3feb9beaf167edd556bd7334e3833b2	Custom	2020-07-02T21:19:45.935Z
Hash	i	361d542e05b44518aca804cd0ae1dc63	Custom	2020-07-02T21:19:53.749Z
Hash	i	62ae014f00f8d302961decac5cb2b72908d73fd6a2f1a1acd0a5d7da940eaf7b	Recorded Future	2021-01-24T00:08:13.638Z
Hash	i	58027e9f6ad3d8a07d8b0ffa1cd99b35d182f8828d2e21ddf3bc8a589e36b178	Recorded Future	2021-01-24T00:21:47.124Z
Hash	i	99b5d9928f6165134b7534f59150bfe17088a722a9afe81e4c07a240c7cd1030	Recorded Future	2021-01-24T00:08:13.544Z
Hash	i	1e7edd9be4015c268df629db646eeef22c799ccdbf975bc0f87089c36b7a68b1a	Recorded Future	2021-01-24T00:08:13.857Z
Hash	i	c58a10aa74016f02e051cEb9457c67f4b7fe4e8a90f28f2989213ce7db09ed64	Recorded Future	2021-01-24T00:08:13.506Z
Hash	i	d62e5b00b5cad47f081635ede0779724ed1ad6d8a576b62c7f6275bf9a71af21	Recorded Future	2021-01-24T00:21:47.185Z
Hash	i	3b8fd34596aa0d27b2bf6b82fd43bee4ca9354afb33c29253591fee9d033712f	Recorded Future	2021-01-24T00:21:47.248Z

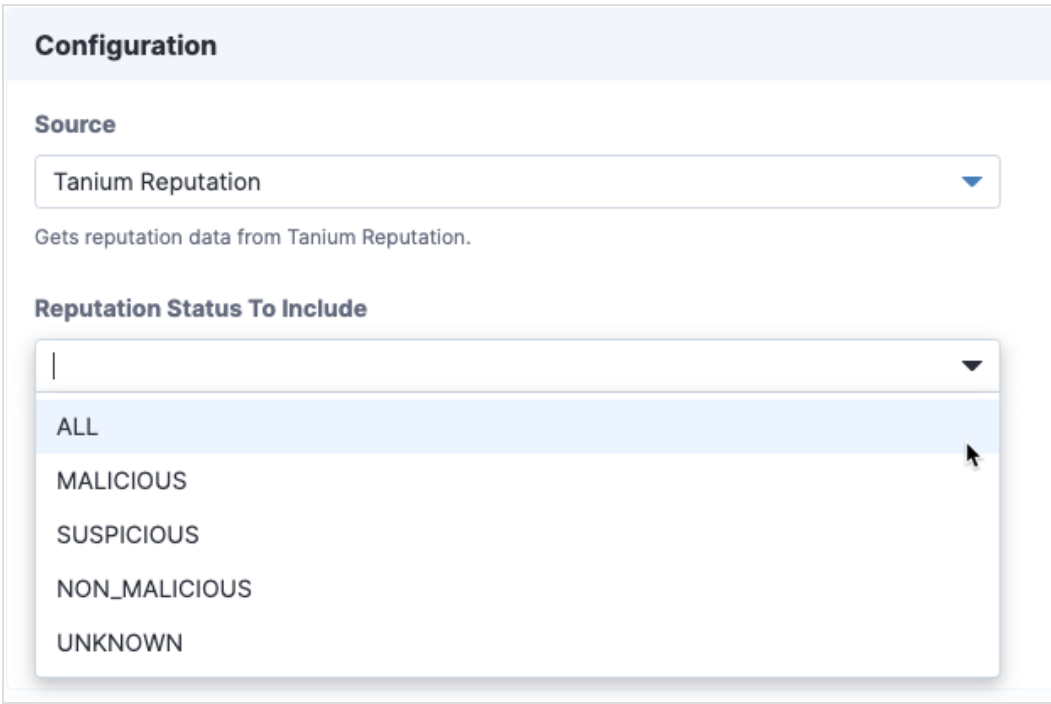
Only hashes with a malicious or pending status are listed.

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.

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



The screenshot shows a configuration window titled "Configuration". Under the "Source" section, a dropdown menu is set to "Tanium Reputation" with a description below it: "Gets reputation data from Tanium Reputation." Under the "Reputation Status To Include" section, a dropdown menu is open, showing a list of options: "ALL", "MALICIOUS", "SUSPICIOUS", "NON_MALICIOUS", and "UNKNOWN". The "ALL" option is currently selected and highlighted in blue.

You can also select the reputation status to include.

4. Configure the destination settings for the connection.



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 **Overview** page, click **Create Connection**.
2. Specify a name and description.
3. For the source, choose a saved question that returns a hash, such as **Running Processes with MD5 Hash**.
You can use the following settings for saved questions:

Setting	Description
Flatten Results	You might want to enable the Flatten Results setting to process results as individual records. For example, you might want to get notified when you see a new MD5 hash on a machine. Without the Flatten Results setting enabled, the entire data set that is retrieved by the saved question from a machine, such as all MD5 hashes, is considered to be a single record. Any change that is made to this data set shows up in the destination. By enabling the Flatten Results setting, Connect processes the new hashes on an individual basis (one MD5 hash from one machine) instead of all hashes from a machine as a single record.
Hide Errors	If the saved question returns an error, you can use the Hide Errors setting to prevent the error results from getting sent to the destination.
Hide No Results	If the saved question returns [No results], you can use the Hide No Results setting to prevent this result from being sent to the destination.
Include Recent Results	If you want to include results from machines that are offline, select Include Recent Results , which returns the most recent answer to the saved question for the offline endpoint.
Answer Complete Percent	Results are returned when the saved question returns the configured complete percent value. Any results that come in after the configured percent value has passed are not sent to the destination. If you are finding that the data returned from the saved question is incomplete in your destination, you can disable this setting by setting it to 0. If disabled, all data is returned after the timeout passes.
Timeout	Minutes to wait for clients to reply before returning processed results when Answer Complete Percent is set to 0. If the Answer Complete Percent value is not met at the end of the time limit, then the connection run is marked as a failure.
Batchsize	Number of rows that are returned for the saved question results at one time. This setting might vary depending on your destination.

4. For the destination, choose **Tanium Reputation** and select the appropriate hash type for the **Hash Field**.

Source Saved Question Returns the result of a Saved Question that reports data from Tanium.	Destination Tanium Reputation
Saved Question Name Running Processes with MD5 Hash Get Running Processes with MD5 Hash from all machines	Hash Field ⓘ MD5 Hash
Computer Group All Computers Salicompeters()	▶ Advanced
<input checked="" type="checkbox"/> Flatten Results When enabled, results that contain multiple values per row for a column are broken out into individual rows.	
<input checked="" type="checkbox"/> Hide Errors Answers with errors are not sent to the connection destination.	
<input type="checkbox"/> Hide No Results Answers with "No Results" are not sent to the connection destination.	
<input type="checkbox"/> Include Recent Answers Include answers from machines that are not currently turned on.	



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


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.

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.

The screenshot shows the 'Import Boards' interface. On the left, under 'Select Boards', there are seven board options: Connect, Inventory, IT Operations Metrics, Operations Monitoring, Policy Monitoring, Reputation (selected), and Risk and Security Metrics. The 'Reputation' board is highlighted with a blue border and a checkmark. On the right, the 'Reputation' board is expanded, showing two sections: 'Section: Resource Usage' and 'Section: Service Usage'. Each section contains several panels, all of which are checked. The 'Resource Usage' section includes Outbound Items, Outbound API Requests, Failed Outbound API Requests, Outbound Processing Queue, Successful Outbound API Requests, and Reputation Database Size. The 'Service Usage' section includes Inbound Items, Purged Items, Hash List Items in Environment, Total Items, and Hash List.

By default, everything is selected.

3. Click **Validate**.



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 **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 43](#).

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

Check the Trends metrics for potential problems

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 sources 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 sources to send fewer hashes.

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.



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.

Uninstall Reputation so you start fresh when you reinstall

1. [Uninstall Reputation so data is restored on reinstall on page 42.](#)
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 <https://support.tanium.com>.