Tanium™ Reputation User Guide

Version 5.0.1

July 11, 2019

Table of contents

Reputation overview

With Reputation, you can build a repository of reputation data from various sources, such as Palo Alto WildFire, 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.

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.

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 17.

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 17.

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 19.

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 14.

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.

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.

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 .

Getting started

1. Install Tanium Reputation. See .
2. Configure and enable Reputation sources. See .
3. Manage the Reputation Whitelist/Blacklist. See .
4. Export Reputation data. See .

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	Version 4.11 or later (optional).
Tanium™ Trace	Version 2.0.5 for reputation data (optional).
Tanium™ Incident Response	For hash data (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	`<Tanium 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
Show Reputation[1] View the Reputation workbench	✅[2]
Reputation Read Read access to the Reputation shared service	✅[2]

Permission	Reputation Administrator
Reputation Write[3] Write access to the Reputation shared service	✅[2]
Reputation Administrator Administrative access to the Reputation shared service	✅

[1] To install Reputation, you must have the reserved role of Administrator.

[2] Denotes a provided permission.

[3] If you need access to only the Reputation API, you can add the **Reputation Write** permission to your user.

 Table 3:   Provided Reputation Advanced user role permissions for Tanium 7.1.314.3071 or later

Permission	Content Set for Permission	Reputation Administrator
Execute Plugin	Reputation	✅

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.

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.

To update these settings, click 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 data

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.

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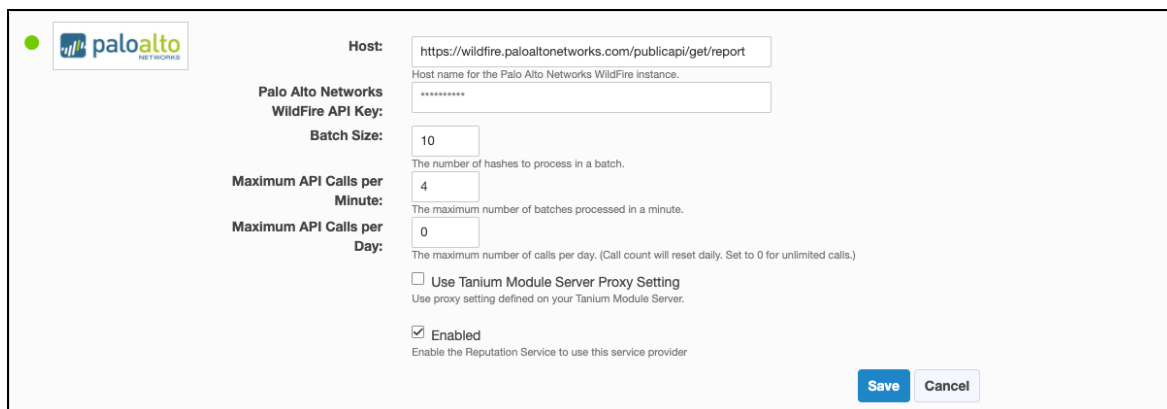
After the WildFire analysis is completed, the reputation service can query the results and update the reputation data.

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.

2. Specify settings, including the host of your WildFire instance and the API key.
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.
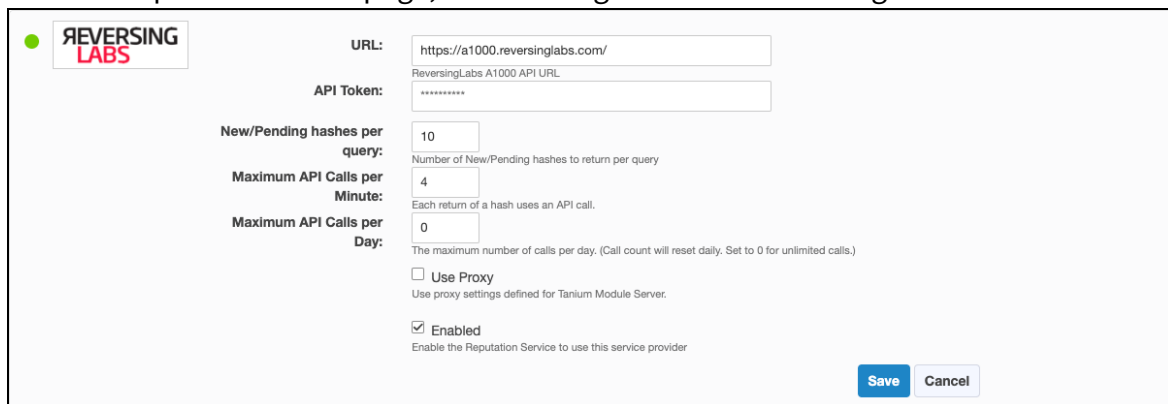
Prerequisites

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.

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** and **New/Pending queries per minute** according to your API agreement with ReversingLabs and your network requirements.
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
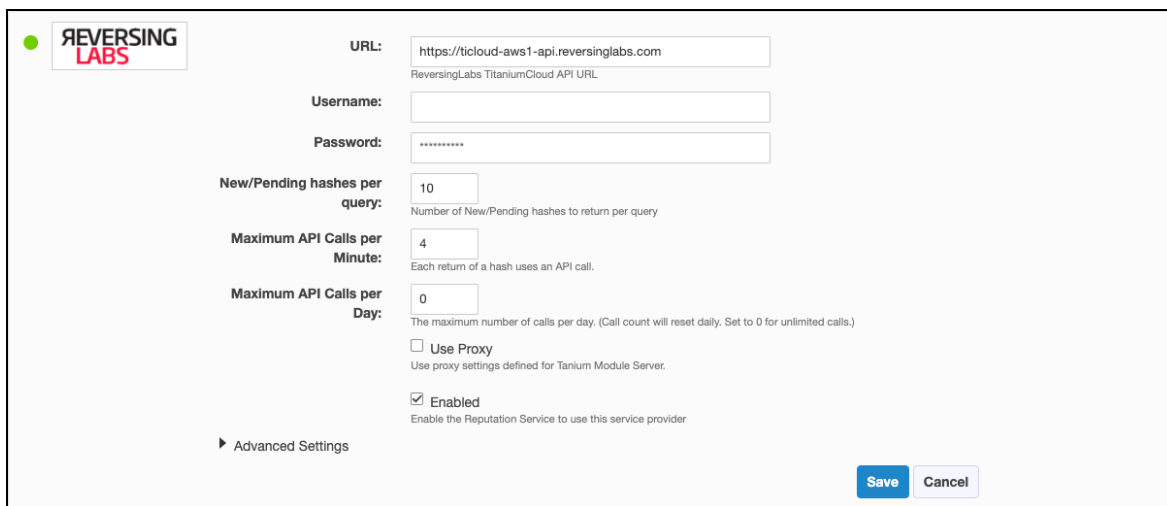
antivirus engines and website scanners. The reputation service sends reputation items to the ReversingLabs API and returns the results to the reputation database.

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.

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** and **New/Pending queries per minute** according to your API agreement with ReversingLabs and your network requirements.

4. To reduce the number of items reported as malicious, expand **Advanced Settings** and adjust the settings for **Threat Level** and **Trust Factor**.

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

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.
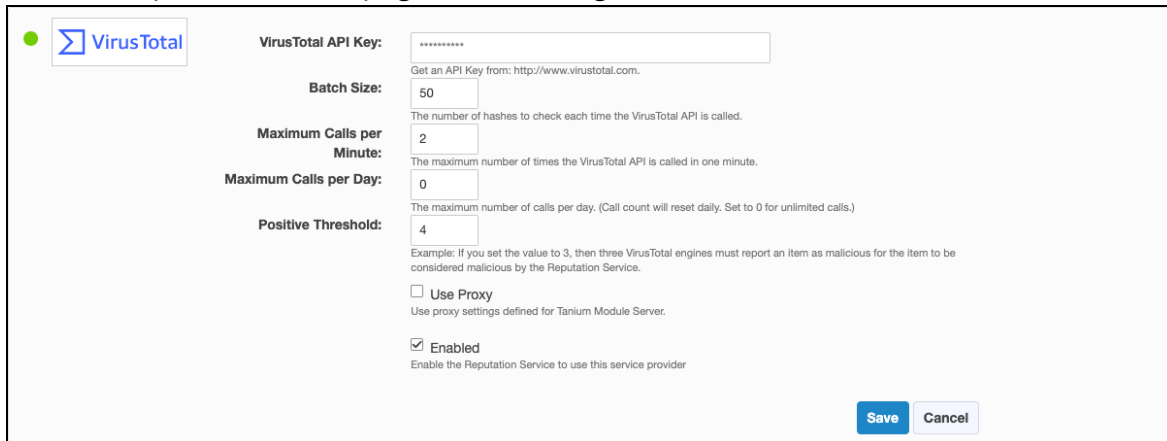
Prerequisites

Register for a VirusTotal API key at virustotal.com. 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.

2. Specify settings for VirusTotal, including the API key.
   - Adjust the settings for **Batch Size** and **Maximum Calls per Minute** according to your agreement with VirusTotal.
   - 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.
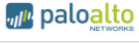
     Example: If you set the value to 3, then three VirusTotal engines must report an item as malicious for the item to be sent to Connect.
     Setting the value to 0 disables the threshold. If any VirusTotal engine reports that item as malicious, the item is sent to Connect.

     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**.

View reputation scan status

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

- **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

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**.

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**.

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.

Malicious Reputations			
Items: 3 — Download All			Show file hash contain
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
⏮ ◀ 1 ▾ ▶ ⏭ 100 ▾ items per page			1 - 3 of 3 items

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 reputation 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**.

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.

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**.

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.

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 ProductName 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 `\Program Files\Tanium\Tanium 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 Reputationso you start fresh when you reinstall

1. .
2. Manually delete the `\Program Files\Tanium\Tanium 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.