Tanium™ Reputation User Guide

Version 6.2.174

March 28, 2023

Table of contents

Reputation overview

With Reputation, you can build a repository of reputation data from various sources, such as Palo Alto Networks 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 26.

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 28.

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 30.

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 Installing Reputation on page 18.

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

WILDFIRE

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

RECORDED FUTURE

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

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

REVERSINGLABS A1000

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

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

REVERSINGLABS TITANIUMCLOUD

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

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

VIRUSTOTAL

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

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

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

Items are removed from the reputation database

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

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

Hash List

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

For more information, see Managing hashes on page 35.

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 39 and Send data to the reputation service on page 40.

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 44 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 18](#).

Step 2: Enable Reputation sources

Configure and enable Reputation sources.

For more information, see [Configuring Reputation sources on page 23](#).

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 35](#).

Step 4: Export data

Export Reputation data.

For more information, see [Exporting Reputation data on page 39](#).

Reputation requirements

Review the requirements before you install and use Reputation.

Core platform dependencies

Make sure that your environment meets the following requirements:

- **Tanium™ Core Platform servers**: 7.4 or later

- **Tanium™ Client**: No client requirements.

Solution dependencies

Other Tanium solutions are required for specific Reputation features to work (feature-specific dependencies). The installation method that you select determines if the Tanium Server automatically imports dependencies or if you must manually import them.

> **NOTE** Some Reputation dependencies have their own dependencies, which you can see by clicking the links in the lists of Feature-specific dependencies on page 12. Note that the links open the user guides for the latest version of each solution, not necessarily the minimum version that Reputation requires.

Tanium recommended installation

If you select **Tanium Recommended Installation** when you import Reputation, the Tanium Server automatically imports all your licensed solutions at the same time. See Tanium Console User Guide: Import all modules and services.

Import specific solutions

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

Feature-specific dependencies

Reputation has the following feature-specific dependencies at the specified minimum versions:

- Tanium Connect 5.2.3 or later

- 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.

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

Endpoints

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

Third-party software

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

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

Host and network security requirements

Specific ports and processes are needed to run Reputation.

Ports

The following ports are required for Reputation communication.

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

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

Security exclusions

If security software is in use in the environment to monitor and block unknown host system processes, Tanium recommends that a security administrator create exclusions to allow the Tanium processes to run without interference. The configuration of these exclusions varies depending on AV software. 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 URLs on the Tanium Module Server associated with a configured reputation source. For more information about required URLs to allow, see the reputation provider documentation.

User role requirements

The following tables list the role permissions required to use Reputation. To review a summary of the predefined roles, see Set up Reputation users on page 21.

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 user role permissions (continued)

Permission	Reputation Administrator[4]	Reputation Operator[4]	Reputation Service Account[3,4]
Reputation Administrator Administrative access to the Reputation shared service	✅ ADMINISTER	❌	❌
Reputation Hash List[2] Access to the Reputation hash list data	✅ READ WRITE	✅ READ WRITE	❌
Reputation Provider Access to the provider configurations	✅ READ WRITE	✅ READ WRITE	❌
Reputation Service Account Access to module service accounts to read and write data	❌	❌	✅ EXECUTE

Reputation user role permissions (continued)

Permission	Reputation Administrator[4]	Reputation Operator[4]	Reputation Service Account[3,4]
Reputation Whitelist Blacklist[2,5] (deprecated) Access to the Reputation hash list data NOTE: In Reputation 6.0.77 and later, use the **Reputation Hash List** permission instead.	❌	❌	❌

[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

Provided Reputation platform content permissions (continued)

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

To view which content set permissions are granted to a role, see Tanium Console User Guide: View effective role permissions.

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 Reputation with default settings on page 18.

- **Manual configuration with custom settings**: After installing Reputation, you must manually configure required settings. Select this option only if Reputation requires settings that differ from the recommended default settings. For more information, see Import Reputation with custom settings on page 18.

Before you begin

- Read the release notes.

- Review the Reputation requirements on page 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 on page 14.

  - To import the Reputation solution, you must be assigned the Administrator reserved role.

Import Reputation with default settings

When you import Reputation with automatic configuration, the Reputation service account is set to the account that you used to import the module.

Configuring a unique service account for each Tanium solution is an extra security measure to consider in consultation with the security team of your organization. See Configure service account on page 20.

To import Reputation and configure default settings, see Tanium Console User Guide: Import all modules and services. After the import, verify that the correct version is installed: see Verify Reputation version on page 19.

Import Reputation with custom settings

To import Reputation without automatically configuring default settings, be sure to 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.

To configure the service account, see Configure service account on page 20.

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

Manage solution dependencies

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

1. Install the dependencies as described in Tanium Console User Guide: Import, re-import, or update specific solutions.

2. From the Main menu, go to **Administration > Shared Services > Reputation** to open the Reputation **Overview** page and verify that the Console no longer displays a banner to list missing dependencies.

Upgrade Reputation

For the steps to upgrade Reputation, see Tanium Console User Guide: 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 .

Configuring Reputation

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

When you import Reputation with automatic configuration, the Reputation service account is set to the account that you used to import the module.

Configuring a unique service account for each Tanium solution is an extra security measure to consider in consultation with the security team of your organization. See .

Configure Reputation

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 .

> **NOTE**
> If you imported Reputation with default settings, the service account is set to the account that you used to perform the import. Configuring a unique service account for each Tanium solution is an extra security measure to consider in consultation with the security team of your organization.

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](#).

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.

Set up Reputation users

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

To review specific permissions for each role, see [User role requirements on page 14](#).

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

Reputation Administrator

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

- Configure Reputation settings, including the service account, scanning, storage, and logging

- View, create, edit, and delete reputation provider configurations

- View, create, edit, and delete file data hashes

Reputation Operator

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

- Configure some Reputation settings, including scanning, storage, and logging

- View, create, edit, and delete reputation provider configurations

- View, create, edit, and delete file data hashes

Reputation Service Account

Assign the **Reputation Service Account** role to the account that configures system settings for Reputation.
This role can perform several background processes for Reputation. For more information, see Installing Reputation on page 18.

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

To sort a column, click the column header.

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

Configure Palo Alto Networks WildFire reputation 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.

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 ✱

https://api.recordedfuture.com/v2/soar/enrichment

API Key ✱

Batch Size ✱

325

The number of hashes to process in a batch.

Maximum API Calls per Minute ✱

1

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

Maximum API Calls per Day ✱

175

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 ✱

65

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.

[Save] [Cancel]

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:

   - 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.

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.

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 ✱

```
https://ticloud-aws1-api.reversinglabs.com
```

ReversingLabs TitaniumCloud API URL.

Username ✱

Password ✱

New/Pending Hashes Per Query ✱

```
10
```

Number of New/Pending hashes to return per query.

Maximum API Calls per Minute ✱

```
4
```

Each return of a hash uses an API call.

Maximum API Calls per Day ✱

```
0
```

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**

Save   **Cancel**

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**.

> 💡 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. 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.

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.

> 💡 **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

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 view additional context for each hash, and for certain sources you can also view additional information on the source's website. You can also search for file hashes and add, import, export, or delete reputation data hashes.

> **NOTE** Hashes that you add to the hash list are not sent to reputation sources for analysis.

View additional hash data

1. In the **Reputations** section, click the **Malicious** tab.

2. To sort a column, click the column header.

3. Click ▶ to expand the **Hash** line-item to view reputation data for a hash.

Add data hashes

1. In the **Reputations** section, click the **Hash List** tab.

2. To sort a column, click the column header.

3. Click **Add**.

4. To add hashes that are known to be malicious, select **Malicious**, enter the **Hashes** and any **Notes** to associate with each hash, and click **Save**.

5. To add hashes that are known to be false detections, select **Non-Malicious**, enter the **Hashes** and any **Notes** to associate with each hash, and click **Save**.

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

Import hashes

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

Header field	Required	Description
`hash`	Required if `md5`, `sha1`, and `sha256` are not included, Optional if `md5`, `sha1`, and `sha256` are included	An MD5, SHA-1, or SHA-256 file hash value.

Header field	Required	Description
`list`	Required	Whether the file hash value is `malicious` or `non-malicious`.
`md5`	Required if `sha1` and `sha256` are included, Optional if `hash` is included	An MD5 file hash value.
`notes`	Optional	A string describing the file hash value.
`sha1`	Required if `md5` and `sha1` are included, Optional if `hash` is included	A SHA-1 file hash value.
`sha256`	Required if `md5` and `sha1` are included, Optional if `hash` is included	A SHA-256 file hash value.
`uploadedAt`	Optional	The timestamp at which this file hash value is uploaded. If undefined, this defaults to the current time.
`uploadedBy`	Optional	The user that uploaded this file hash value. If undefined, this defaults to your user.
`uploadedHash`	Optional	The uploaded file hash value.

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

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]

4. Select a **Method** for the import:

   - To replace the current hashes, select **Replace existing list**.

   - To append to the current hashes, select **Add to existing list**.

5. Click **Save**.

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

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

Export hashes

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.
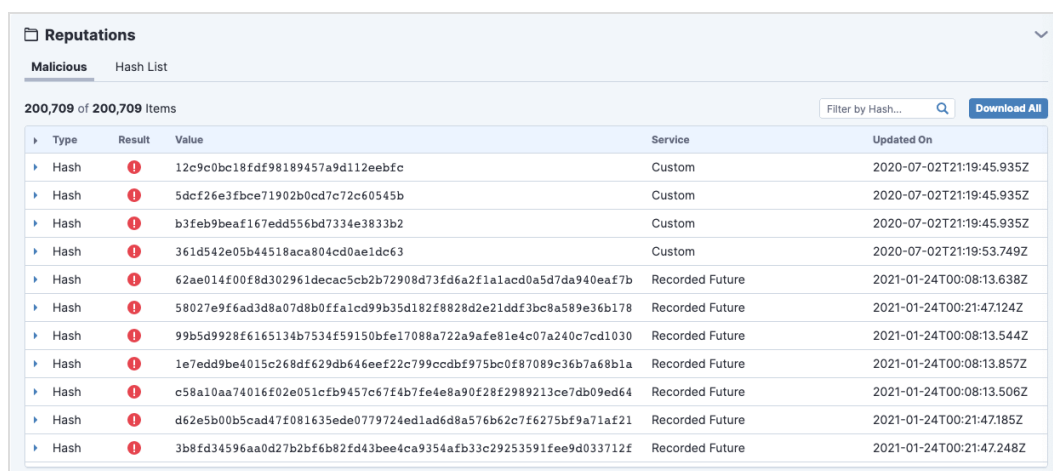
2. To delete specific hashes, select one or more hashes and click Remove from Hash List ⊗.

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.

Type	Result	Value	Service	Updated On
▸ Hash	❗	12c9c0bc18fdf98189457a9d112eebfc	Custom	2020-07-02T21:19:45.935Z
▸ Hash	❗	5dcf26e3fbce71902b0cd7c72c60545b	Custom	2020-07-02T21:19:45.935Z
▸ Hash	❗	b3feb9beaf167edd556bd7334e3833b2	Custom	2020-07-02T21:19:45.935Z
▸ Hash	❗	361d542e05b44518aca804cd0ae1dc63	Custom	2020-07-02T21:19:53.749Z
▸ Hash	❗	62ae014f00f8d302961decac5cb2b72908d73fd6a2f1a1acd0a5d7da940eaf7b	Recorded Future	2021-01-24T00:08:13.638Z
▸ Hash	❗	58027e9f6ad3d8a07d8b0ffa1cd99b35d182f8828d2e21ddf3bc8a589e36b178	Recorded Future	2021-01-24T00:21:47.124Z
▸ Hash	❗	99b5d9928f6165134b7534f59150bfe17088a722a9afe81e4c07a240c7cd1030	Recorded Future	2021-01-24T00:08:13.544Z
▸ Hash	❗	1e7edd9be4015c268df629db646eef22c799ccdbf975bc0f87089c36b7a68b1a	Recorded Future	2021-01-24T00:08:13.857Z
▸ Hash	❗	c58a10aa74016f02e051cfb9457c67f4b7fe4e8a90f28f2989213ce7db09ed64	Recorded Future	2021-01-24T00:08:13.506Z
▸ Hash	❗	d62e5b00b5cad47f081635ede0779724ed1ad6d8a576b62c7f6275bf9a71af21	Recorded Future	2021-01-24T00:21:47.185Z
▸ Hash	❗	3b8fd34596aa0d27b2bf6b82fd43bee4ca9354afb33c29253591fee9d033712f	Recorded Future	2021-01-24T00:21:47.248Z
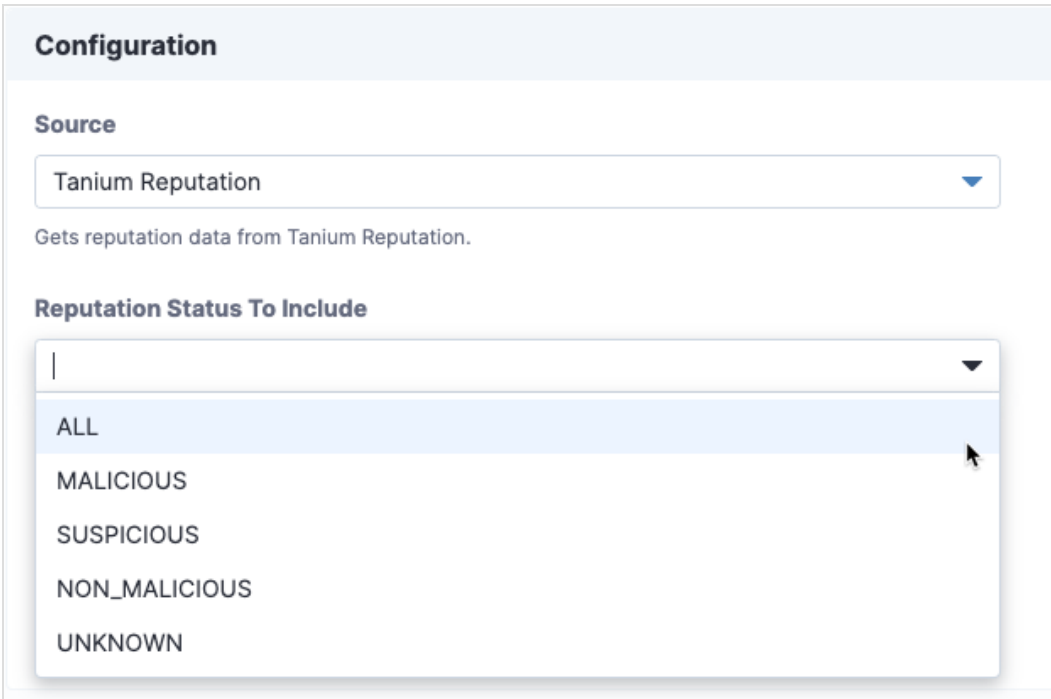
Only hashes with a malicious or pending status are listed.

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

Send data to Connect destinations

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

1. From the Connect **Overview** page, click **Create Connection**.

2. Specify a name and description.

3. For the source, select **Tanium Reputation**.

   You can also select the reputation status to include.

4. Configure the destination settings for the connection.

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

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

Send data to the reputation service

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

1. Create a saved question for each of the following questions to collect hash data from your environment:

Question syntax	Saved Question Name
`Get AutoRun Files[SHA256,1] from all machines with is Windows contains true`	Reputation - Windows AutoRuns (SHA 256)
`Get Linux AutoRuns[MD5,1] from all machines with Is Linux contains true`	Reputation - Linux Autoruns (MD5)
`Get Mac AutoRuns[MD5,1] from all machines with Is Mac contains true`	Reputation - macOS Autoruns (MD5)
`Get Index - File Hash Recently Changed [100,*,*,*,4D5A*,*,*,*,*,0,3,1] from all machines`	Reputation - Microsoft EXE Recently Changed
`Get Index - File Hash Recently Changed [100,*,*,*,FEEDFACE*,*,*,*,*,0,3,1] from all machines`	Reputation - Recently Changed macOS MACH-O 32 Bit
`Get Index - File Hash Recently Changed [100,*,*,*,FEEDFACF*,*,*,*,*,0,3,1] from all machines`	Reputation - Recently Changed macOS MACH-O 64 Bit
`Get Index - File Hash Recently Changed [100,*,*,*,7F454C46*,*,*,*,*,0,3,1] from all machines`	Reputation - Recently Changed macOS ELF
`Get "Driver Details with Hash"[SHA256] from all machines`	Reputation - Driver Details (SHA 256)
`Get "Loaded Modules with Hash"[SHA256] from all machines`	Reputation - Loaded Modules (SHA256)
`Get "Running Processes with Hash"[SHA256] from all machines`	Reputation - Running Processes with Hash (SHA256)
`Get "Service Module Details with Hash"[sha256] from all machines`	Reputation - Service Module Details (SHA256)
`Get Trace Executed Process Hashes[3 hours,1571257836726|1571261435726,500] from all machines`	Reputation - Trace Executed Process Hashes (MD5)

Question syntax	Saved Question Name

> **NOTE** The saved questions in this table are examples that can return hash data from endpoints. Implement saved questions and use hash types that are appropriate for your environment. If you use Index sensors to populate the reputation service, the Index configuration must have the appropriate hash type enabled. For more information, see Tanium Threat Response User Guide: Index configurations.

For more information on creating saved questions, see Tanium Console User Guide: Create a saved question.

2. From the Connect **Overview** page, click **Create Connection**.

3. Choose **Saved Question** from the **Source** drop-down, select one of the saved questions that you created in step 1 from the **Saved Question Name** drop-down, and select **All Computers** from the **Computer Group** drop-down.
   You can use the following settings for saved questions:

Setting	Description
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. 💡 **TIP** For the best results, set this to **10** minutes.
Batchsize	Number of rows that are returned for the saved question results at one time. This setting might vary depending on your destination.

4. Specify a name that matches the saved question name and enter a connection description.

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

> 👉 **IMPORTANT** Each reputation service connection destination can only be configured for 1 hash column name. If a saved question returns multiple hash types (such as MD5 and SHA256) and you want to send both hashes to Reputation, you must create 2 connections, one for each hash type in the **Hash Field**.

6. In the Schedule section, select **Enable Schedule** to update and stagger the schedule and prevent these connections from running simultaneously.

7. Select **Advanced - Define as a Cron Expression** and enter one of the following Cron expressions in the **Advanced** field:

Saved Question Name	Cron expression	Frequency
Reputation - Windows AutoRuns (SHA 256)	`0 */3 * * *`	0 minute every third hour
Reputation - Linux Autoruns (MD5)	`48 */3 * * *`	48th minute every third hour
Reputation - macOS Autoruns (MD5)	`56 */3 * * *`	56th minute every third hour
Reputation - Microsoft EXE Recently Changed	`8 */3 * * *`	8th minute every third hour
Reputation - Recently Changed macOS MACH-O 32 Bit	`16 */3 * * *`	16th minute every third hour
Reputation - Recently Changed macOS MACH-O 64 Bit	`24 */3 * * *`	24th minute every third hour

Saved Question Name	Cron expression	Frequency
Reputation - Recently Changed macOS ELF	`32 */3 * * *`	32th minute every third hour
Reputation - Driver Details (SHA 256)	`10 */1 * * *`	10th minute every hour
Reputation - Loaded Modules (SHA256)	`20 */1 * * *`	20th minute every hour
Reputation - Running Processes with Hash (SHA256)	`30 */1 * * *`	30th minute every hour
Reputation - Service Module Details (SHA256)	`40 */1 * * *`	40th minute every hour
Reputation - Trace Executed Process Hashes (MD5)	`50 */1 * * *`	50th minute every hour

> **NOTE**
> The cron expressions provided in this table are examples demonstrating a staggered schedule. Implement a connection schedule that is appropriate for your environment. Running all of the aforementioned saved questions/connection jobs can quickly consume an API quota for a given reputation provider, such as VirusTotal. Configure the "Maximum Hashes Processed Per Day" setting if the provider allows it. Fewer saved questions/connection jobs may be required to avoid consuming the API quota.

> **IMPORTANT**
> Understand the potential resource usage of sensors on endpoints and implement according to your environment. Use discretion when implementing saved questions that run on a frequent basis. Environments with resource constraints may be impacted. For example, "Loaded Modules with Hash [SHA256]" takes time to run and returns stringy results. Increasing the connection frequency, staggering the connection job schedules, modifying the hash type or excluding low resource endpoints from targeting may be necessary. Contact Tanium Support for assistance in understanding the reputation workflow and defining the saved questions and connection schedule suitable for your environment.

8. **Save** the connection.

9. Repeat steps 2-8 for the remaining saved questions.

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.

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.

Maintaining Reputation

Perform monthly maintenance tasks to ensure that Reputation successfully performs scheduled activities on all the targeted endpoints and does not overuse endpoint or network resources. If Reputation is not performing as expected, you might need to troubleshoot issues or change settings. See Troubleshooting Reputation on page 47 for related procedures.

Review and remediate Tanium Reputation issues

1. From the Main menu, go to **Modules > Trends > Boards**.

2. Click the **Reputation** board and review the panels for issues that need attention.

3. If the **Failed Outbound API Requests** panel displays failures, verify that the reputation sources are configured correctly. See Configuring Reputation sources on page 23.

4. If data shows up faster in the **Inbound Items** panel than in the **Outbound Items** panel and the **Outbound Processing Queue** panel is consistently high, configure the reputation sources to send fewer hashes by lowering the **Maximum Hashes Processed Per Day** value.

5. To troubleshoot other Reputation issues or collect logs for a support package, see Troubleshooting Reputation on page 47.

Check the Trends metrics for potential issues

1. From the Trends menu, click **Boards** and then click **Reputation**.

2. If the **Failed Outbound API Requests** panel displays failures, verify that your reputation 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.

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 48](#).

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.

> 👉 Consult with Tanium Support before you uninstall or reinstall Reputation.
>
> **IMPORTANT**

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 47](#).

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.