IBM Security Secret Server
Version 10.5

# *VirusTotal Reputation Connector Guide*

IBM

# Contents



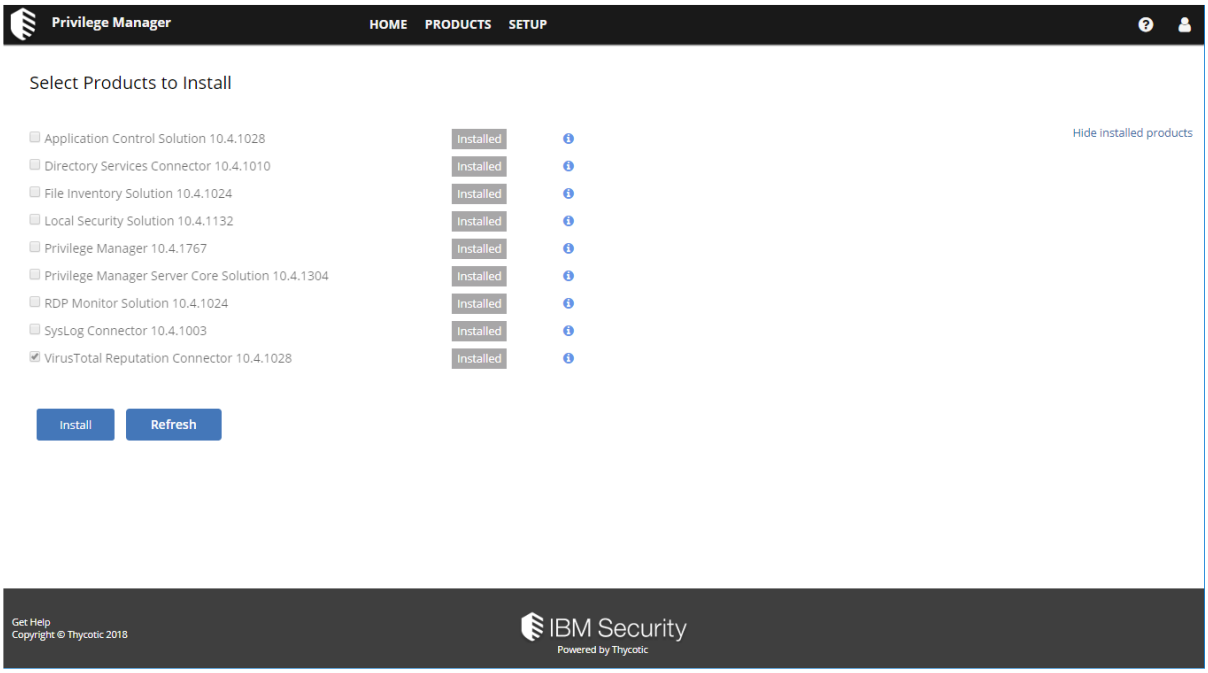
*Last modified: September 20, 2018*

# Getting started

Privilege Manager can perform real-time reputation checks for unknown applications by integrating with analysis tools like VirusTotal. This guide shows you how to integrate Privilege Manager with VirusTotal and create a greylisting policy in Privilege Manager for checking reputations.

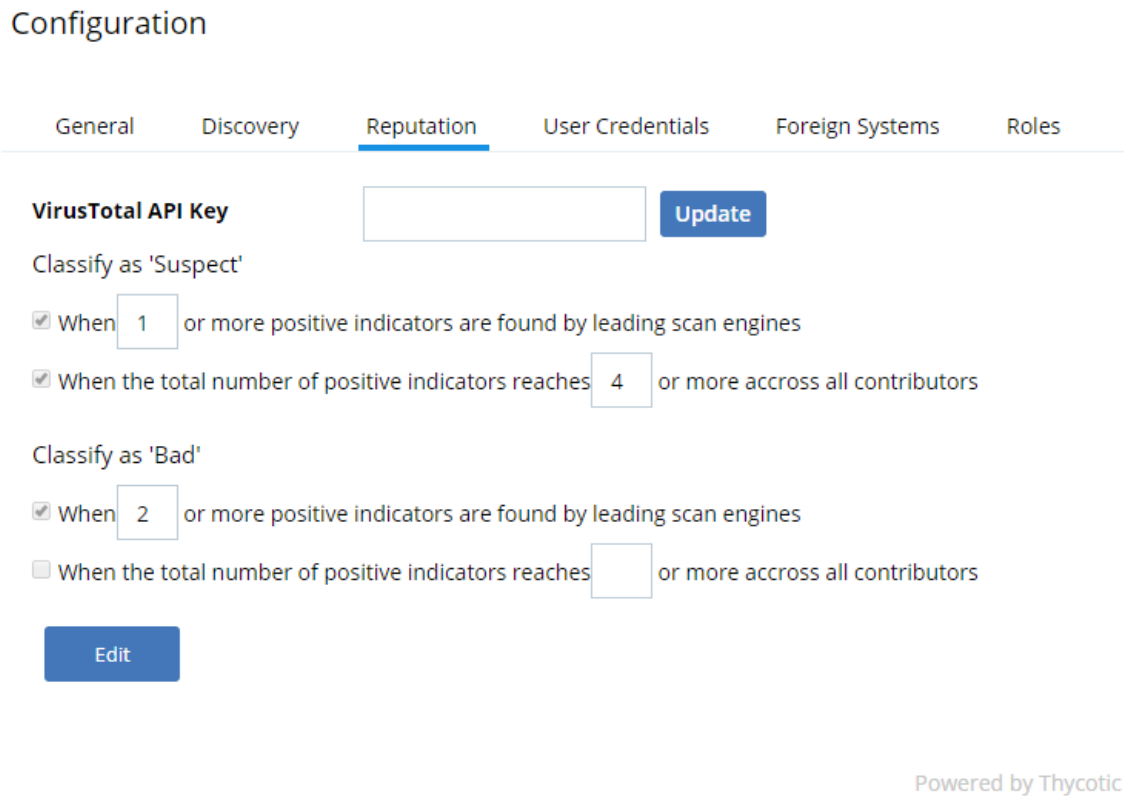
# Installing and configuring the VirusTotal Reputation connector

1. Configure VirusTotal Ratings Provider.
    a. Sign up for a free VirusTotal account at https://www.virustotal.com/.
    b. Sign in to the VirusTotal web site and find your API key under your **Username | Settings | API Key**.
2. Install VirusTotal in Privilege Manager. Note that you will need outbound access on your server to install:
    a. Open a browser on your Privilege Manager web server, and browse to ***Error! Hyperlink reference not valid.***.
    b. On the Currently Installed Products screen, choose **Install/Upgrade Products**.
3. Select the VirusTotal Reputation Connector and click **Install**.

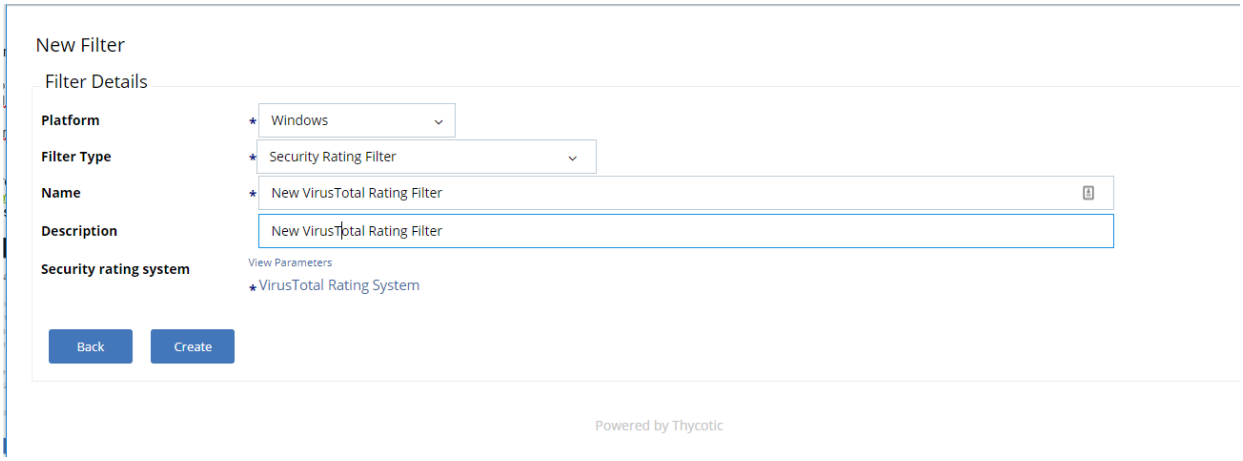



4. Click the **Home** button.
5. Navigate to **Products > Privilege Manager > Configuration > Reputation**.

6. Add your VirusTotal API Key and click **Update**.

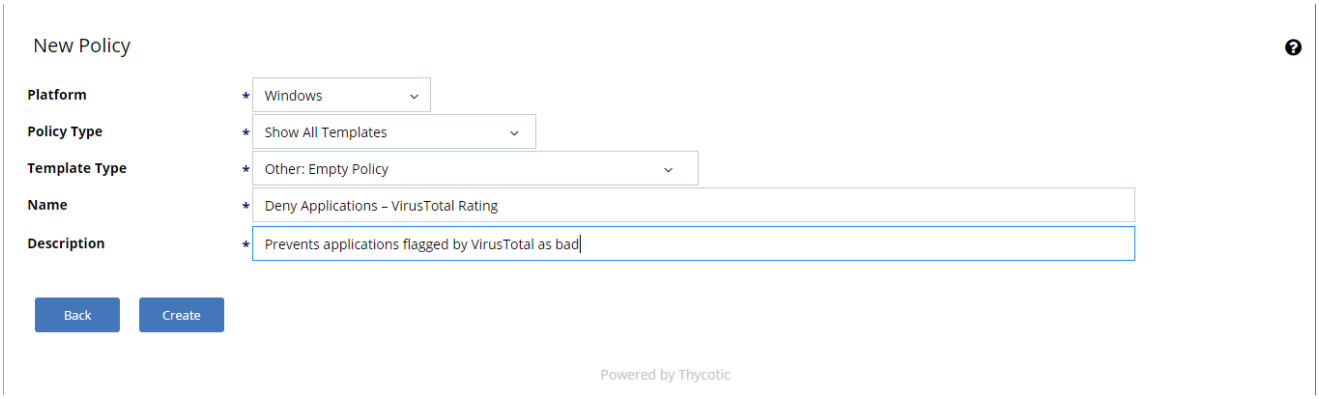



7. Create a Security Rating Filter for VirusTotal.
    a. Browse to **Home > Filters**, then click **Add Filter**.
    b. Select a platform, then as a **Filter Type**, select **Security Rating Filter**. Name the filter and add a description.
    c. Under **Security Rating System**, select **View Parameters** and then select **VirusTotal** as a **Resource**.
    d. Click **Create**.



# Creating a policy for VirusTotal

1. After your filter is created, browse to **Home > Policies**, and click **Add New Policy**.
    a. Select **Windows** as a **Platform**.
    b. For **Policy Type**, select **Show All Policies**.
    c. For **Template Type**, select **Other: Empty Policy**.
2. Name the policy. For example: `Deny Applications – VirusTotal Rating`.
3. Add a description. For example: `Prevents applications flagged by VirusTotal as bad.`
4. Click **Create**.




5. Click **Edit** and select **Enabled**. Select the **Conditions**. Select **Add Application Target**. Search for the filter created in the previous steps (VirusTotal). Select that filter and click **Add**.
6. Next, select the **Actions** tab.
7. Select **Add Action**.
8. In the search field, type `Application Denied`, and locate the **Application Denied Message Action**.
9. Select this action and click **Add**.
   This policy sends any executable the user executes to VirusTotal for analysis. To minimize unnecessary calls, it is suggested that you place the VirusTotal policy at the bottom of your execution order. You do this step so that it will only fire if no other policies have already identified the file as permitted. You might also choose to add an inclusion filter to the policy to limit the checks to files executed from the user's downloads or temp directories.