IBM Security Verify Privilege On-Premises
Version 10.9

Syslog Connector Guide

IBM

Contents

Last modified: September 21, 2020

Getting started

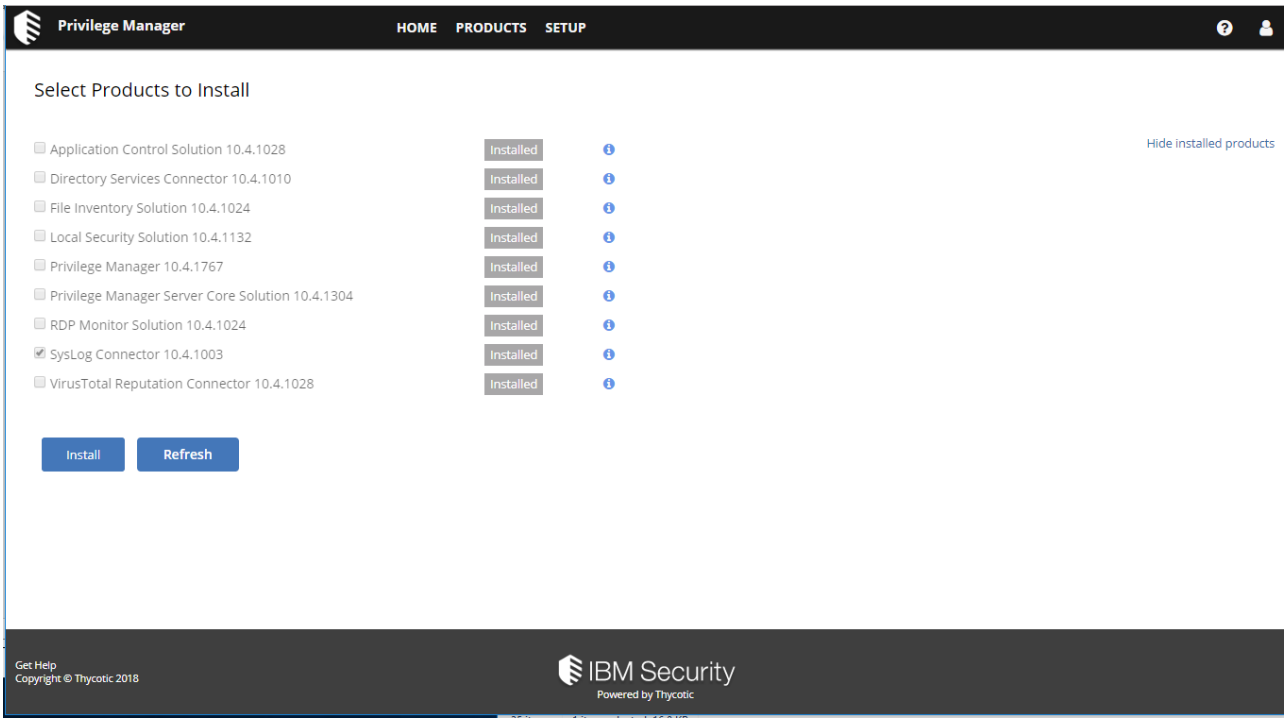
Privilege Manager can push Syslog formatted messages on a set schedule. This action does not happen immediately when events occur. The following steps describe how to configure the syslog connection and schedule the frequency of sending Discovery Event logs to a Syslog server.

Configuring the Syslog connection

To configure Syslog messages in Privilege Manager

1. Browse to **Admin > Configuration > Foreign Systems**, and click **SysLog**.
2. Click **Add New**.
3. Specify a **Name** and the **Syslog Server Address**. You can specify **tcp** or **udp**.

Note: If you do not see **Syslog** in the **Admin > Configuration> Foreign Systems** tab, navigate to `https://[YourOrganizationURL]/TMS/Setup/ProductOptions/SelectProducts`, select the **Thycotic Syslog Connector**, and click **Install**.



You added a Syslog connection that lets you send logs to your Syslog server manually.

Scheduling how often events are pushed to the Syslog server

Schedule a server task to push events that are received by Privilege Manager to a Syslog server automatically.

1. Go to **Admin > More... > Tasks**.
2. Expand the **Server Tasks** folder, browse to **Foreign Systems**, select **SysLog,** and click **Add New**.
3. From the menu, select **Send SysLog Application Events**.
4. Specify the following items:
    a. A **Name** for this task
    b. An **Event Name**. For example: "`Privilege Manager Application Events`".
    c. The **Event Severity**
5. Click **Select Resource** and select your Syslog server.
6. if you have VirusTotal configured, set the **Security Rating Provider**. If not, skip this step.
7. Click **Create**.
8. In the **Scheduled Tasks** page, specify how often you want events that are received by Privilege Manager (for example, all events that are viewed in **Admin > Event Discovery**) to be pushed to the Syslog server.
   The schedule can be hourly, every 30 minutes, daily, or any period that you want.

After this task runs and successfully completes, verify that **Event Discovery** events appear in your Syslog system.