BeyondTrust

# Privilege Management Cloud
# Splunk App Integration



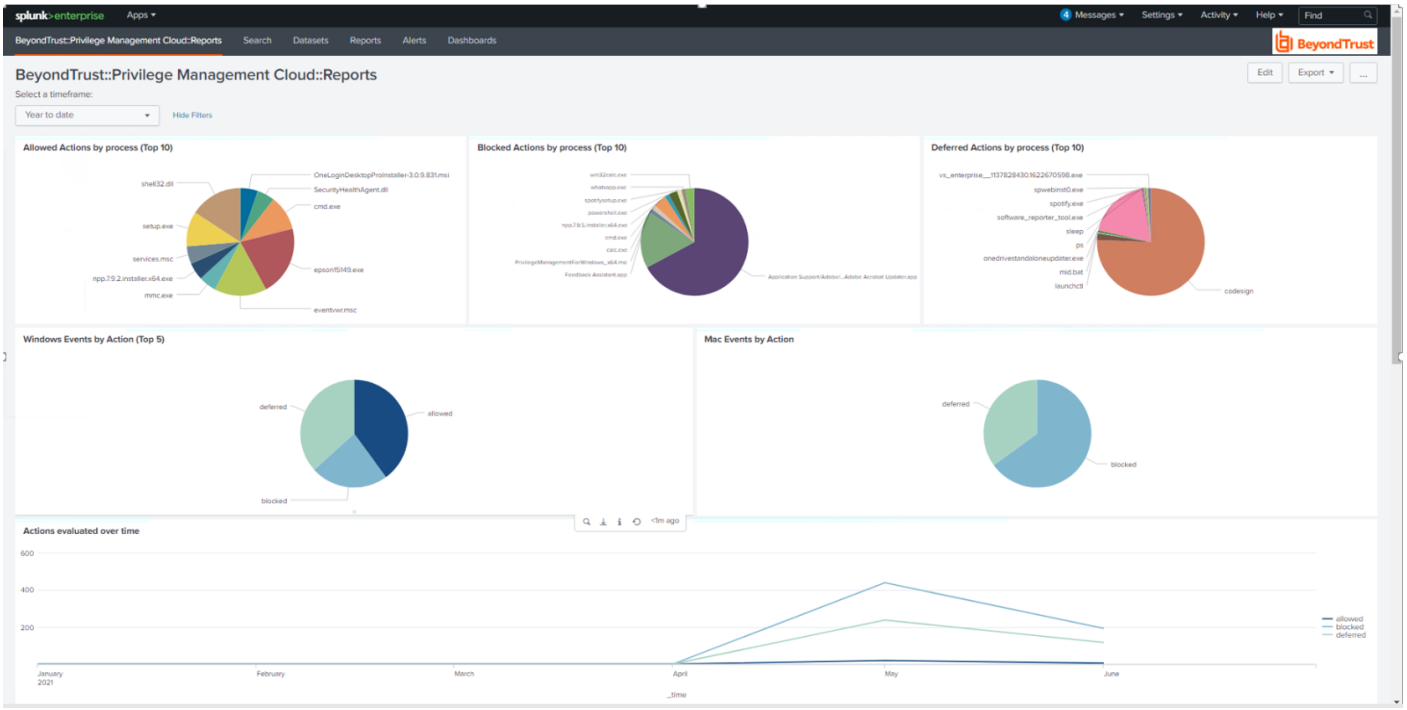
TC:6/3/2024

# Use the Splunk App for Endpoint Privilege Management

This document describes the installation and configuration of the Splunk app and BeyondTrust Endpoint Privilege Management. The integration consists of an application that can be installed in a Splunk instance directly from Splunkbase.

Using the Splunk app, you can:

- Pull client events and activity audit events generated by Endpoint Privilege Management endpoints and EPM into Splunk.
- On the dashboard, visualize and interpret the large number of events forwarded to Splunk by Endpoint Privilege Management. You can more rapidly benefit from the integration between Endpoint Privilege Management and Splunk by leveraging these working reports that can be used as is or as templates for custom reports.




## Prerequisites

Before proceeding with the integration, it's important to ensure a few things are in place.

EPM 23.1 or later is required.

### Network Considerations

Your Splunk instance needs to connect to various REST API endpoints provided by your EPM site. Communication is in the form of secure HTTP traffic on TCP port 443. The purpose of this connectivity is to query the EPM site for event information, which can be ingested by Splunk.

### Create an Endpoint Privilege Management API Account

The API account is used in Splunk to make API calls to EPM. When creating the account, ensure the following permissions are granted:

- **Audit**: Read Only
- **Reporting**: Read Only

> *For more information, see Configure Access to the Management API at https://www.beyondtrust.com/docs/privilege-management/console/pm-cloud/configuration/configure-api-settings.htm.*

## Install and Configure the App

Once the prerequisites are satisfied, you can move on to the installation and configuration of the integration.

### Install the Application

The app is currently available for installation via Splunkbase.

To install the application:

1. Authenticate to your Splunk instance as an administrator.
2. Click **Apps > Manage Apps**.
3. At the top, click **Browse more apps**.
4. Search for *BeyondTrust Endpoint Privilege Management*.
5. Click **Install** on the app listing.

### Configure Application

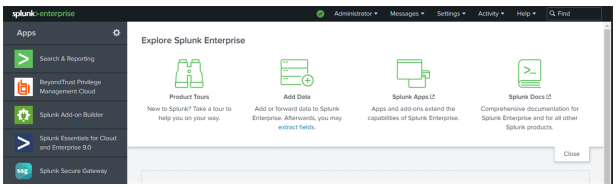
Once the application is installed in your Splunk instance, you can add configuration for one or both data feeds that it is able to consume.

The two categories of events that can be consumed by the application are:

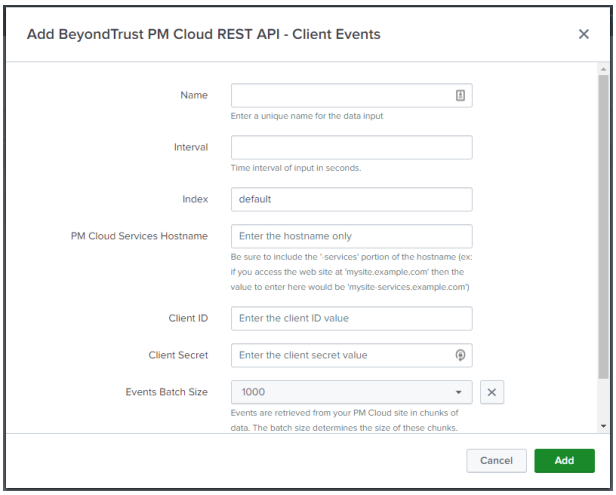
- **Client Events**: These events originate from the individual systems being managed by BeyondTrust Endpoint Endpoint Privilege Management. They flow back to the EPM site, and are retrievable via the API. Examples include: user logon, a process started, a process blocked, etc.
- **Activity Audits**: These events represent activities that occur in the EPM web interface. Examples include: user role changes, editing or committing a policy draft, assigning a computer to a group, etc.

To add an input for either of the data feeds:

1. Authenticate to your Splunk instance as an administrator.
2. Click **Apps > BeyondTrust Privilege Management Cloud**.



3. On the **Inputs** tab, click **Create New Input**.
4. Two options are presented for the type of input to create. Select an input type: **Client Events** or **Audit Activity**.
5. Enter the appropriate values in each of the configuration fields. The screen capture shows the **Client Events** fields.




   - **Name**: Give the input configuration a unique name.
   - **Interval**: The number of seconds between each attempt to retrieve new data.
   - **Index**: The name of the index into which all events from this input are placed. By default, use the index created by the app installation: **idx_beyondtrust_pmc**.
   - **PM Cloud Services Hostname**: The services hostname of your EPM site. For example, if you access your EPM web interface at **mysite.example.com**, then the appropriate value here is *mysiteservices.example.com*
   - **Client ID**: The ID value of the API account created in "Prerequisites" on page 2.
   - **Client Secret**: The secret value of the API account created in "Prerequisites" on page 2.
   - **Events Batch Size (Client Events only)**: If the integration needs to make multiple calls to retrieve available events, this is the number that is returned in one batch or response. **1000** is both the default and the max value.
   - **Audit Activity Page Size (Activity Audits only)**: If the integration needs to make multiple calls to retrieve available events, this is the number that is returned in one page or response. **200** is both the default and the max value.
6. Click **Add** to save the configuration. The input runs immediately.
7. (Optional) If you want the app to ingest event data from both data feeds, repeat steps 4 and 5 for the other input type.

# Troubleshoot and Support

## Log Files

Should you encounter issues with event ingestion, the application writes separate log files for each input type. In an on-premises Splunk Enterprise deployment, the files are located in a location similar to **C:\Program Files\Splunk\var\log\splunk**, using files with the following names:

- Client Events:

  **beyondtrust_pmcloud_integration_beyondtrust_pm_cloud_rest_api_client_events.log**

- Activity Audits:

  **beyondtrust_pmcloud_integration_beyondtrust_pm_cloud_rest_api_audit_data.log**

## Data Mismatch

If the dashboard doesn't show data but manual search queries confirm that data is successfully being ingested, this may indicate a mismatch between the dashboard queries and how the event data is being stored - most likely under a different index than expected.

To correct this, change the filters used by the dashboard to specify an index, source type, and time frame that should match the ingested events. If the filters are not already displayed, click the **Show Filters** link next to the report title to view and edit the filter values.