Privileged Remote Access Splunk Integration

TC:3/4/2024

Table of Contents

BeyondTrust Privileged Remote Access Integration with Splunk

IT administrators using Splunk can now integrate BeyondTrust Privileged Remote Access (PRA) to strengthen access control, identify and prioritize threats seamlessly in real time, and remediate incidents proactively.

The BeyondTrust PRA integration helps safeguard your business by giving you complete visibility into activity across the IT infrastructure, including external threats such as malware hackers, internal threats such as data breaches and fraud, risks from application flaws and configuration changes, and compliance pressures from failed audits.

Through the integration, session event data captured through BeyondTrust PRA's rich logging capability is populated into Splunk's platform, and reports are provided for security review.

Prerequisites for the BeyondTrust Privileged Remote Access Integration with Splunk

Confirm Software Versions

Using this integration requires the following software and versions:

- A currently supported version of BeyondTrust Privileged Remote Access. To confirm your version is supported, contact Support or refer to the BeyondTrust End of Life Policy at https://www.beyondtrust.com/docs/eol/.
- Splunk On-Premises or Cloud: 6.3.0 or newer.

Review Network Considerations

The following network communication channels must be open for the integration to work properly:

Outbound From	Inbound To	TCP Port #	Purpose
Splunk Server	BeyondTrust Appliance B Series	443	Session event data pulled from the Reporting API
BeyondTrust Appliance B Series	Splunk Server	514	Syslog event information from the B Series Appliance

Configure BeyondTrust Privileged Remote Access for Integration with Splunk

The Splunk integration supports consumption of syslog output directly from the B Series Appliance.

To enable this, follow the steps below. These steps are completed in the BeyondTrust**/appliance** administrative interface.

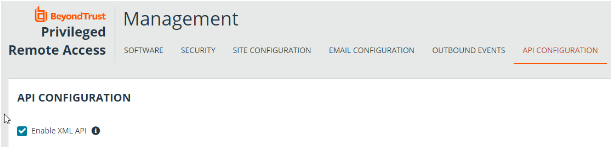
1. Access your BeyondTrust interface by going to the hostname of your B Series Appliance followed by **/appliance**, for example, https://access.example.com/appliance.
2. Go to **/appliance >Security > Appliance Administration** and locate the **Syslog** section.
3. Enter the hostname or IP address for your remote syslog server.
4. Select your preferred message format.
5. Click **Submit**.

Verify the API is Enabled

Management | API CONFIGURATION

This integration requires the BeyondTrust XML API to be enabled. This feature is used by the BeyondTrust Middleware Engine to communicate with the BeyondTrust APIs.

Go to **/login > Management > API Configuration** and verify that **Enable XML API** is checked.



API CONFIGURATION

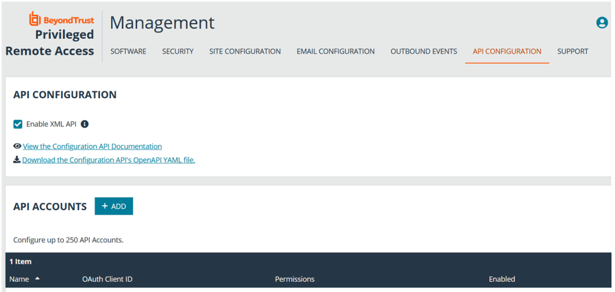
☑ Enable XML API

Create an OAuth API Account

Management | API CONFIGURATION

The Splunk API account is used from within Splunk to make Privileged Remote Access Command API calls to Privileged Remote Access.

1. In **/login**, navigate to **Management > API Configuration**.
2. Click **Add**.


BeyondTrust Privileged Remote Access
Management
SOFTWARE
SECURITY
SITE CONFIGURATION
EMAIL CONFIGURATION
OUTBOUND EVENTS
API CONFIGURATION
SUPPORT
View the Configuration API Documentation
Download the Configuration API's OpenAPI YAML file.
+ ADD

API CONFIGURATION

☑ Enable XML API

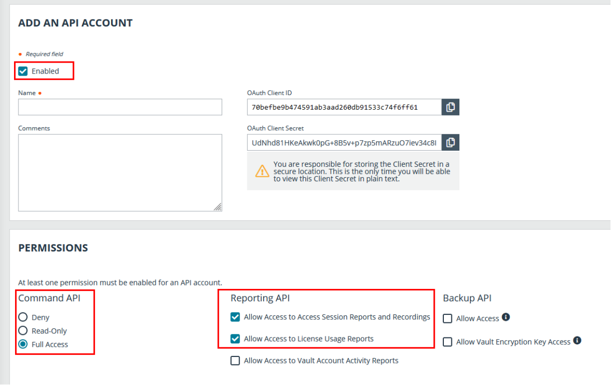
API ACCOUNTS

Configure up to 250 API Accounts.

1 Item

Name	OAuth Client ID	Permissions	Enabled

3. Check **Enabled**.
4. Enter a name for the account.
5. **OAuth Client ID** and **OAuth Client Secret** is used during the OAuth configuration step in Splunk.
6. Under **Permissions**, check the following:
   - Command API: **Full Access**.
   - Reporting API: **Allow Access to Support Session Reports and Recordings**, and **Allow Access to Presentation Session Reports and Recordings**.
7. Click **Save** at the top of the page to create the account.



ADD AN API ACCOUNT

• Required field

☑ Enabled

Name •

OAuth Client ID: 70befbe9b474591ab3aad260db91533c74f6ff61

Comments

OAuth Client Secret: UdNhd81HKeAkwk0pG+8B5v+p7zp5mARzuO7iev34c8l

You are responsible for storing the Client Secret in a secure location. This is the only time you will be able to view this Client Secret in plain text.

PERMISSIONS

At least one permission must be enabled for an API account.

Command API
○ Deny
○ Read-Only
● Full Access

Reporting API
☑ Allow Access to Access Session Reports and Recordings
☑ Allow Access to License Usage Reports
□ Allow Access to Vault Account Activity Reports

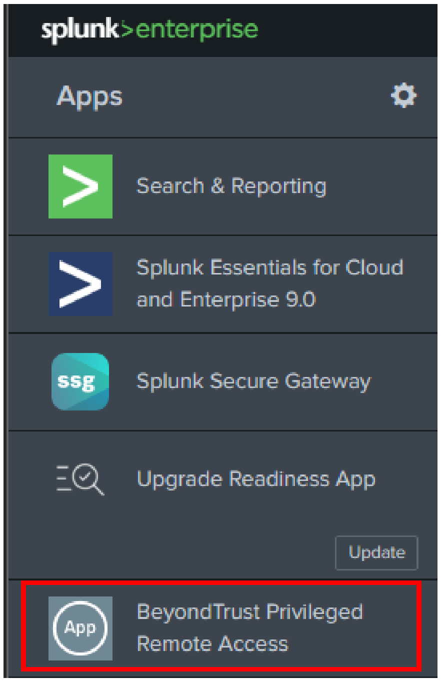
Backup API
□ Allow Access
□ Allow Vault Encryption Key Access

Configure the Splunk Integration App

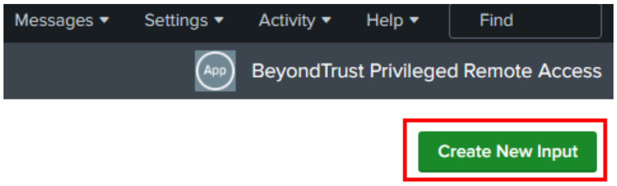
The integration application is available in the Splunkbase at https://splunkbase.splunk.com/app/6913. You must log in to your Splunk account to download the application.

Once the new application is installed, follow these steps in the app to configure it:

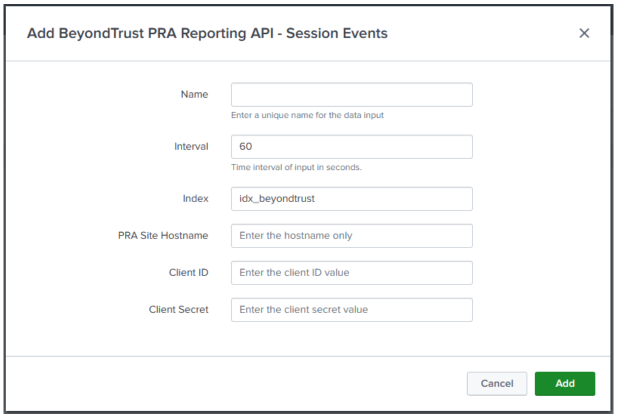
1. In the list of Splunk Apps, click the new **BeyondTrust Privileged Remote Access** option.



2. On the **BeyondTrust Privileged Remote Access** Inputs page, click **Create New Input**.



3. Enter the required input information:
   - **Name:** Desired unique input name.
   - **Interval**: Desired polling interval. A short polling interval can result in poor performance. At least 60 seconds is recommended.
   - **Index**: Must be **beyondtrust_pra**. Create this index if it does not already exist.
   - **PRA Site hostname**: Your Privileged Remote Access hostname. Do not include the protocol (https://) or other URL components. This value must be the hostname only. For example, support.example.com.
   - **Client ID**: Your previously configured Client ID.
   - **Client Secret**: Your previously configured Client Secret.
4. Click **Add**.



Add BeyondTrust PRA Reporting API - Session Events

Name:
Enter a unique name for the data input

Interval: 60
Time interval of input in seconds.

Index: idx_beyondtrust

PRA Site Hostname: Enter the hostname only

Client ID: Enter the client ID value

Client Secret: Enter the client secret value