Remote Support

Splunk Integration Guide

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Table of Contents

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

BeyondTrust Remote Support Integration with Splunk

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

The BeyondTrust RS 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 RS's rich logging capability is populated into Splunk's platform, and reports are provided for security review.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Prerequisites for the BeyondTrust Remote Support Integration with Splunk

Confirm Software Versions

Using this integration requires the following software and versions:

- A currently supported version of BeyondTrust Remote Support. To confirm your version is supported, contact Support or refer to the BeyondTrust End of Life Policy at https://www.beyondtrust.com/eos-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

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

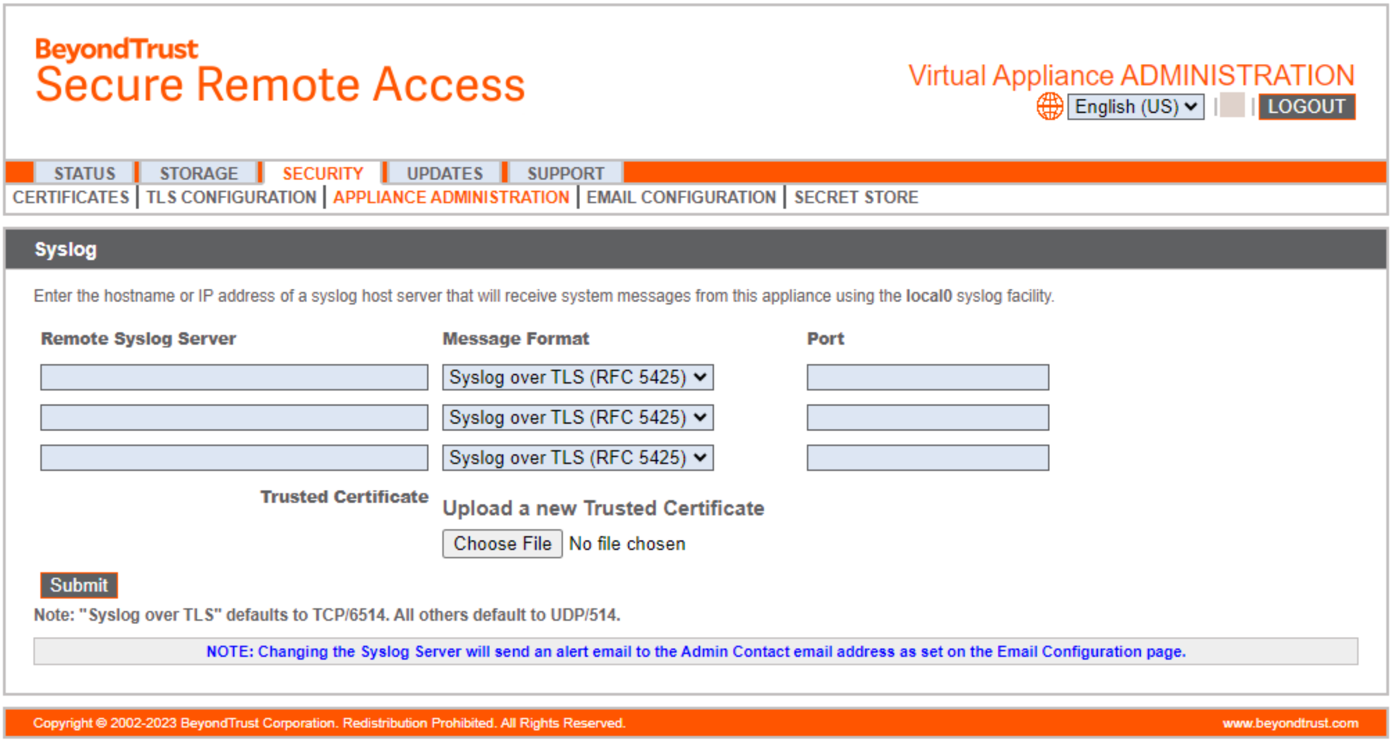
Configure BeyondTrust Remote Support for Integration with Splunk

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

To enable this, follow the steps below to create the syslog feed, verify the API is enabled, and create an OAuth API account.

Create Syslog Feed

1. Access your BeyondTrust interface by going to the hostname of your B Series Appliance followed by **/appliance**, for example, https://support.example.com/appliance.
2. Go to **/appliance >Security > Appliance Administration** and locate the **Syslog** section.



Enter the hostname or IP address of a syslog host server that will receive system messages from this appliance using the **local0** syslog facility.

Remote Syslog Server	Message Format	Port
	Syslog over TLS (RFC 5425)	
	Syslog over TLS (RFC 5425)	
	Syslog over TLS (RFC 5425)	

Note: "Syslog over TLS" defaults to TCP/6514. All others default to UDP/514.

NOTE: Changing the Syslog Server will send an alert email to the Admin Contact email address as set on the Email Configuration page.

Copyright © 2002-2023 BeyondTrust Corporation. Redistribution Prohibited. All Rights Reserved.

3. Enter the hostname or IP address for your remote syslog server.
4. Select your preferred message format.
5. Click **Submit**.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

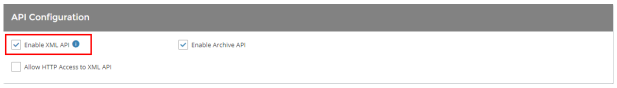
The remaining steps take place in the BeyondTrust **/login** administrative interface. Access your Remote Support interface by going to the hostname of your B Series Appliance followed by **/login** (e.g., https://support.example.com/login).

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 ☑ Enable Archive API

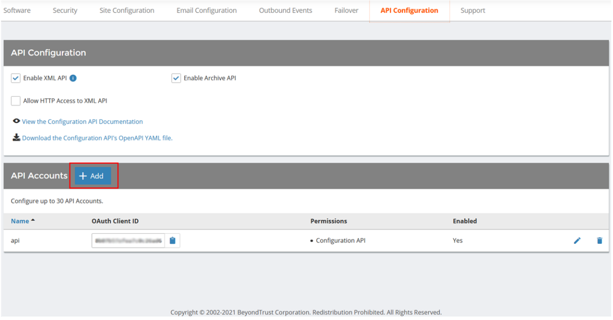
□ Allow HTTP Access to XML API

Create an OAuth API Account

Management | API CONFIGURATION

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

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



API Configuration

☑ Enable XML API ☑ Enable Archive API

□ Allow HTTP Access to XML API

View the Configuration API Documentation

Download the Configuration API's OpenAPI YAML file.

API Accounts + Add

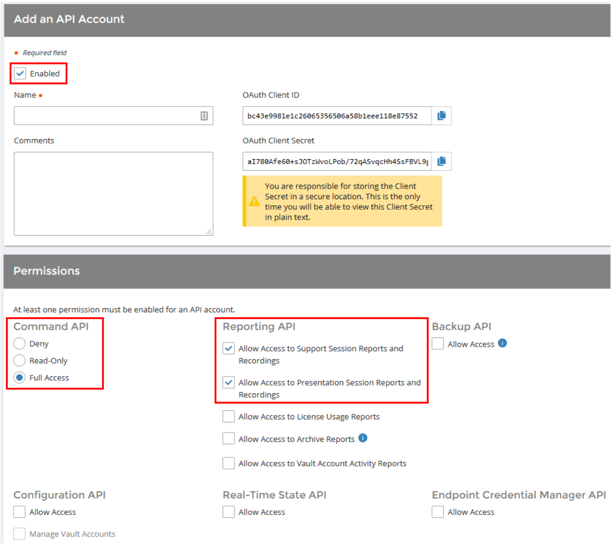
Configure up to 30 API Accounts.

Name	OAuth Client ID	Permissions	Enabled
api	[redacted]	• Configuration API	Yes

Copyright © 2002-2021 BeyondTrust Corporation. Redistribution Prohibited. All Rights Reserved.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

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

bc43e9981e1c26065356506a58b1eee118e87552

Comments

OAuth Client Secret

aI780Afe60+sJOTzWvoLPob/72qASvqcHh4SsFBVL9

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 Support Session Reports and Recordings

☑ Allow Access to Presentation Session Reports and Recordings

□ Allow Access to License Usage Reports

□ Allow Access to Archive Reports

□ Allow Access to Vault Account Activity Reports

Backup API

□ Allow Access

Configuration API

□ Allow Access

□ Manage Vault Accounts

Real-Time State API

□ Allow Access

Endpoint Credential Manager API

□ Allow Access

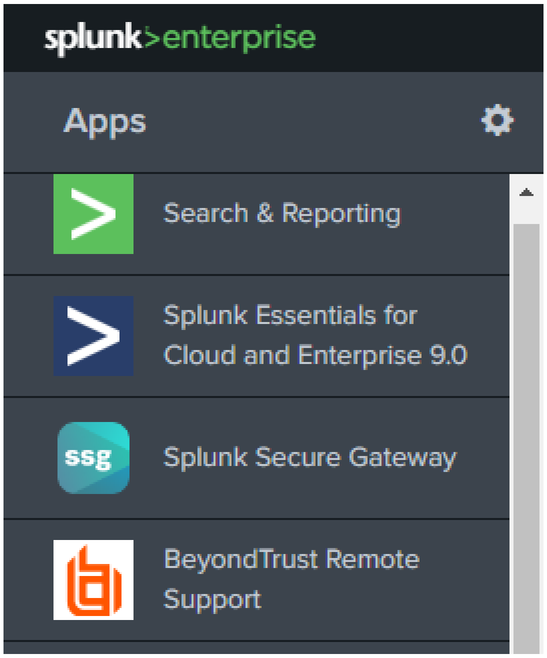
©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Install and Configure the Splunk Integration App

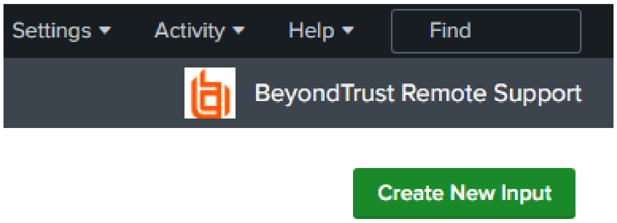
The integration application is available in the Splunkbase at https://splunkbase.splunk.com/app/6968. You must log in to your Splunk account to download the application.

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 Remote Support** option.

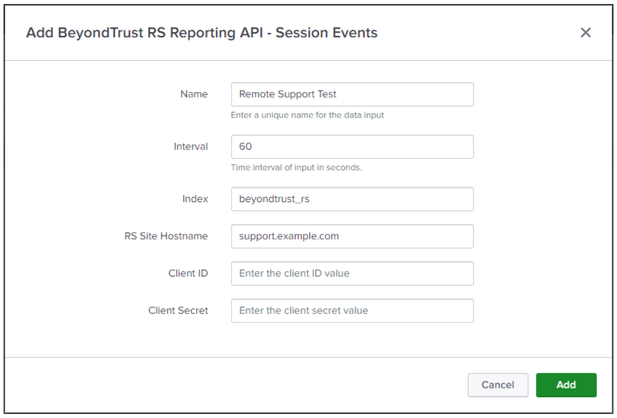

splunk>enterprise
Apps
Search & Reporting
Splunk Essentials for Cloud and Enterprise 9.0
Splunk Secure Gateway
BeyondTrust Remote Support

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



©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

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_rs**. Create this index if it does not already exist.
   - **RS Site hostname**: Your Remote Support 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 RS Reporting API - Session Events

Name: Remote Support Test
Enter a unique name for the data input

Interval: 60
Time interval of input in seconds.

Index: beyondtrust_rs

RS Site Hostname: support.example.com

Client ID: Enter the client ID value

Client Secret: Enter the client secret value

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.