BeyondTrust

Privileged Remote Access SIEM Tool Plugin Installation and Administration

TC:3/4/2024

Table of Contents

Configure and Administer the BeyondTrust SIEM Tool Plugin

The Security Information and Event Management (SIEM) tool plugin for BeyondTrust Privileged Remote Access (PRA) enables the processing and transmission of session event data to your preferred SIEM tool. This complements tools that gather syslog data, which includes only appliance events. The plugin can customize the output message format for special needs and/or use cases.

Review Prerequisites

Before using this plugin, you must:

- Install and configure the BeyondTrust Middleware Engine, which supports this and other plugins.
- Install this plugin following the instructions in the Middleware Guide.
- Review the network considerations for your preferred SIEM tool.

> *For more information about installing and configuring the BeyondTrust Middleware Engine and installing plugins, please see BeyondTrust Privileged Remote Access Middleware Engine Installation and Configuration at https://www.beyondtrust.com/docs/privileged-remote-access/documents/integrations/pra-middleware-engine.pdf.*

Configure BeyondTrust Privileged Remote Access for Using the SIEM Plugin

All of the steps in this section take place in the BeyondTrust **/login** administrative interface. Access your Privileged Remote Access interface by going to the hostname of your B Series Appliance followed by **/login**, (e.g., https://access.example.com/login).

SIEM plugin configuration is required for each BeyondTrust Appliance B Series configured in the application's configuration file.

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.

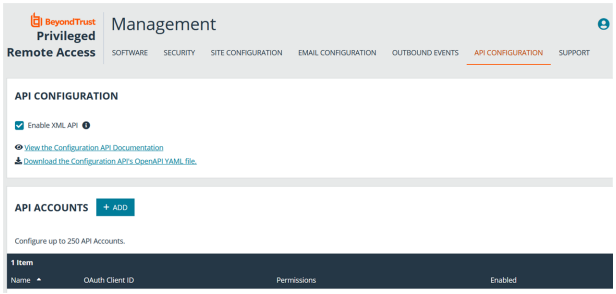
Go to **/login > Management > API Configuration** and verify that **Enable XML API** is checked.

Create an OAuth API Account

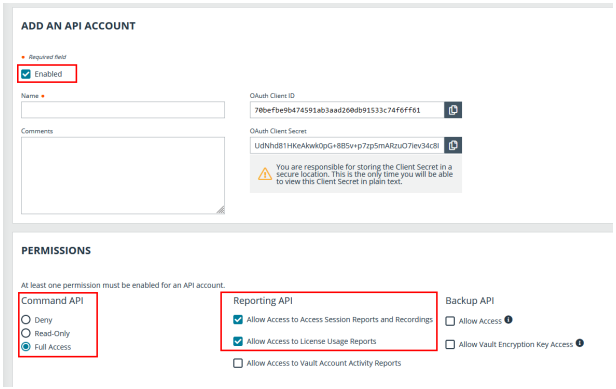
Management > API CONFIGURATION

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

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



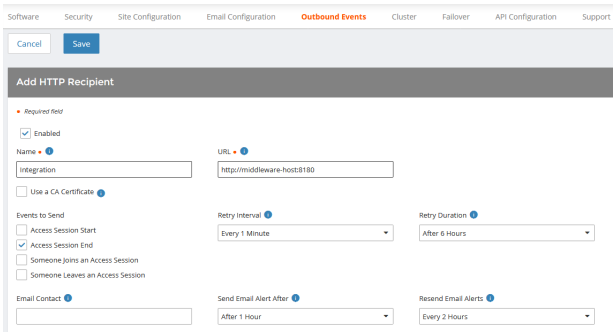
3. Check **Enabled**.
4. Enter a name for the account.
5. **OAuth Client ID** and **OAuth Client Secret** is used during the OAuth configuration step in SIEM Tool.
6. Under **Permissions**, check the following:
    - Command API: **Full Access**.
    - Reporting API: **Allow Access to Support Session 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.



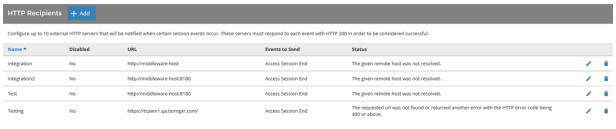
Add an Outbound Event URL

Management > OUTBOUND EVENTS

1. Go to **/login > Management > Outbound Events**.
2. In the HTTP Recipients section, click **Add** and name it **Integration** or something similar.
3. Enter the URL to use:
    - If using the default appliance ID:
        - *http://<middleware-host>:<port>/PAMPost*.
        - The default port is *8180*.
    - If using an appliance ID other than the default:
        - *http://<middleware-host>:<port>/PAMPost?appliance=<appliance-id>* where *<middleware-host>* is the hostname where the BeyondTrust Middleware Engine is installed.
        - The default port is *8180*.
        - The *<appliance-id>* is an arbitrary name, but note the value used, as it is required later in the plugin configuration. This name accepts only alphanumeric values, periods, and underscores.



4. Scroll to **Events to Send** and check the following event: **Support Session End**
5. Click **Save**.
6. The list of outbound events contains the event just added. The **Status** column displays a value of **OK** if communication is working. If communication is not working, the **Status** column displays an error which you can use to repair communication.



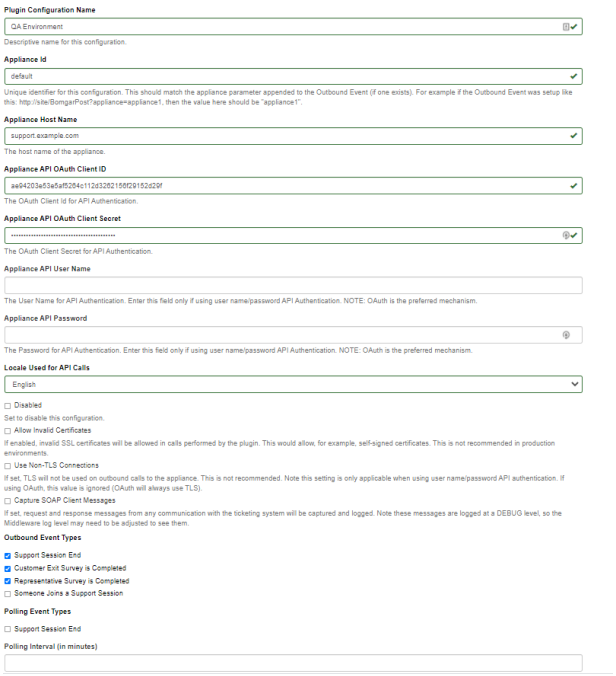
Configure the Privileged Remote Access SIEM Tool Plugin

All of the steps in this section take place in the BeyondTrust Middleware Administration Tool. Access this tool by going to a browser on the server where the Middleware Engine is installed, and entering the address *http://127.0.0.1:53231/*.

To begin configuration, and click the clipboard icon next to the plugin name.

Configure Communication between the SIEM Plugin and the BeyondTrust Appliance B Series

Enter the settings for communication between the plugin and the appliance. Configuration sections include:



1. **Plugin Configuration Name:** Any desired value. Because multiple configurations can be created for a single plugin, allowing different environments to be targeted, provide a descriptive name to indicate how this plugin is to be used.
2. **Appliance Id:** This can be left as **default** or can be given a custom name. This value must match the value configured on the outbound event URL in the BeyondTrust Appliance B Series. If outbound events are not being used, this value is still required, but any value may be used.
3. **B Series Appliance Host Name:** The hostname of the B Series Appliance. Do not include https:// or other URL protocol elements. For example, enter *www.example.com*.
4. **BeyondTrust Integration API OAuth Client ID**: This field must contain the Client ID of the OAuth account.
5. **BeyondTrust Integration API OAuth Client Secret:** This field must contain the client secret of the OAuth account
6. **BeyondTrust Integration API User Name:** The username of the API service account created on the .
7. **BeyondTrust Integration API Password:** The password of the above user.
8. **Locale Used for BeyondTrust API Calls:** This value directs the B Series Appliance to return session data in the specified language.
9. **Disabled:** Enable or disable this plugin configuration. It must be enabled to function.
10. **Allow Invalid Certificates:** Leave unchecked unless there is a specific need to allow. If enabled, invalid SSL certificates are allowed in calls performed by the plugin. This would allow, for example, self-signed certificates. This is not recommended in production environments.
11. **Use Non-TLS Connections:** Leave unchecked unless it is the specific goal to use non-secure connections to the B Series Appliance. If checked, TLS communication is disabled altogether. If non-TLS connections are allowed, HTTP access must be enabled on the BeyondTrust **/login > Management > API Configuration** page. Using non-secure connections is discouraged.

> ***Note:*** *When using OAuth authentication, TLS cannot be disabled.*

12. **Outbound Events Types:** Check which types of events the plugin processes when received by the middleware engine. Event types selected here must also be configured to be sent in BeyondTrust. The middleware engine receives any events configured to be sent in BeyondTrust but passes them off to the plugin only if the corresponding event type is selected in this section.

13. **Polling Event Types:** If network constraints limit connectivity between the B Series Appliance and the middleware engine such that outbound events cannot be used, an alternative is to use polling. The middleware engine regularly polls the B Series Appliance for any sessions that have ended since the last session was processed, however only the **Support Session End** event type is supported.
14. **Polling Interval:** Enter only if polling is used. This determines how often the middleware engine polls the B Series Appliance for sessions that have ended. Too frequent polling may cause performance issues.
15. **Retry Attempt Limit:** Enter the number of retries that can be attempted if the plugin fails to process an event. Too many retries may cause performance issues.
16. **Retry Outbound Event Types:** Specify which outbound events the plugin retries if it fails to process the event.
17. **Retry Polling Event Types:** Specify which polling events the plugin retries if it fails to process the event.

For more information about installing and configuring the BeyondTrust Middleware Engine and installing plugins, please see BeyondTrust Privileged Remote Access Middleware Engine Installation and Configuration at https://www.beyondtrust.com/docs/privileged-remote-access/documents/integrations/pra-middleware-engine.pdf.

SIEM Tool Instance

These are the fields and selections needed to configure the plugin for integration with your SIEM tool. Please see your SIEM installation guide for the values to provide.

1. **Target SIEM System :** Select the target SIEM tool from the list.
2. **SIEM Syslog Host:** Enter the hostname or IP address of the SIEM instance that should receive the messages.
3. **SIEM Syslog Port:** Enter the port used by the SIEM instance to receive syslog messages.
4. **SIEM Syslog Protocol:** Select the appropriate protocol from the list.
5. **Events to Process:** BeyondTrust session data can contain many different event types. All types are available; however, a subset may be desired in the SIEM tool. Select only the events you would like sent to the tool. Events matching unchecked event types are ignored.

For a complete list of available events, please see "BeyondTrust SIEM Tool Message Reference List" on page 8.

Report Templates

On the BeyondTrust Middleware Engine server, in the **<install dir>\Plugins\<integration>\Templates** folder, there are multiple files ending with ***.hbs**. These are Handlebars template files. These files are used by the plugin to format the session report and exit surveys that are added to the corresponding ticket each time a BeyondTrust session ends or each time a survey is submitted. The templates can be edited if desired.

***Note:** If you are editing a template, we recommend copying and saving the original in case the changes need to be reverted.*

For more information on Handlebars templates, please see the Handlebars website at handlebarsjs.com.

BeyondTrust SIEM Tool Message Reference List

Event Name	Event ID
Callback Button Deployed	10
Callback Button Removed	20
Chat Message	30
Command Shell Session Started	40
Conference Member Added	50
Conference Member Departed	60
Conference Member State Changed	70
Conference Owner Changed	80
Credential Injection Attempt Failed	90
Credential Injection Attempt	100
Customer Exit Survey	110
Directory Created	120
External Key	130
File Deleted	140
File Download Failed	150
File Download	160
File Moved	170
File Upload Failed	180
File Upload	190
Files Shared	200
Jump Item Authorization Request Utilized	210
Jump Item Authorization Request	220
Legal Agreement Response	230
Pinned Session Moved Away from Queue	240
Pinned Session Moved to Queue	250
Pinned Session Password Modified	260
Registry Exported	270
Registry Imported	280
Registry Key Added	290
Registry Key Deleted	300
Registry Key Renamed	310
Registry Value Added	320
Registry Value Deleted	330
Registry Value Modified	340

Event Name	Event ID
Registry Value Renamed	350
Representative Exit Survey	360
Representative Monitoring Started	370
Representative Monitoring Stopped	380
Screen Recording	390
Screenshot Captured	400
Service Access Allowed	410
Session Assigned	420
Session Assignment Response	430
Session End	440
Session Foreground Window Changed	450
Session Note Added	460
Session Pinned to Queue	470
Session Start	480
Session Transferred Away from Queue	490
Session Transferred to Queue	500
Session Unpinned from Queue	510
Show My Screen Recording	520
System Information Retrieved	530