



BeyondTrust

Privileged Remote Access SIEM Tool Plugin Installation and Administration

Table of Contents

BeyondTrust SIEM Tool Plugin Installation and Administration	3
Configure BeyondTrust Privileged Remote Access for Integration	4
Verify That the API is Enabled	4
Create an API Service Account - BeyondTrust 16.1 and Earlier	4
Create an API Service Account - BeyondTrust 17.1 and Later	4
Add an Outbound Event URL	5
Configure the BeyondTrust Privileged Remote Access SIEM Tool Plugin	6
BeyondTrust Appliance	6
SIEM Tool Instance	7
Report Templates	7

BeyondTrust SIEM Tool Plugin Installation and Administration

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 SIEM tool. With additional components and steps required for each, the plugin has built-in support for both HP ArcSight and Splunk as well as the ability to customize the output message format for special needs and/or use cases.

Prerequisite for Installation and Configuration of BeyondTrust SIEM Tool Plugin

To complete this integration, make sure that you have the necessary software installed and configured as indicated in this guide, accounting for any network considerations. Make sure you review and complete all steps in [BeyondTrust Middleware Engine Installation and Configuration](http://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/middleware-engine/) at www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/middleware-engine/.

Network Considerations

In addition to the network considerations listed in [BeyondTrust Middleware Engine Installation and Configuration](http://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/middleware-engine/), check the individual SIEM installation guides, HP ArcSight or Splunk, for connectivity components which are specific to each tool and system.

Configure BeyondTrust Privileged Remote Access for Integration

Several configuration changes are necessary on the BeyondTrust Appliance. You must make the changes for each appliance configured in the application's configuration file.

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

Verify That the API is Enabled

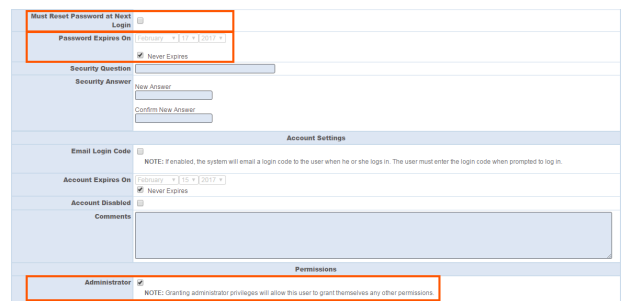
This integration requires the BeyondTrust XML API to be enabled. This feature is used by the BeyondTrust Middleware Engine to communicate with the BeyondTrust APIs.

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

Create an API Service Account - BeyondTrust 16.1 and Earlier

The API user account is used from within the integration to make BeyondTrust Command API calls to BeyondTrust.

1. Go to `/login > Users & Security > Users`.
2. Click **Create New User** and name it **Integration** or something similar.
3. Leave **Must Reset Password at Next Login** unchecked.
4. Set **Password Expires On** to **Never Expires**.
5. Set **Allowed to View Access Session Reports** to **View All Sessions**.
6. Check **Allowed to view access session recordings**.
7. Set **Allowed to View Presentation Session Reports** to **View All Sessions**.
8. Check **Allowed to Use Reporting API** and **Allowed to Use Command API**.
9. Scroll to the bottom and save the account.



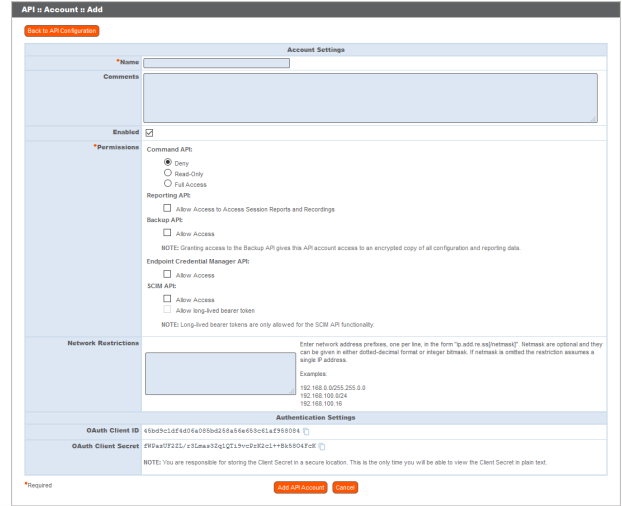
Create an API Service Account - BeyondTrust 17.1 and Later

1. Go to `Management > API Configuration` and create a new API account.



Name	OAuth Client ID	Permissions	Enabled		
Integration Client	edf8b058420b9590e42176284b121f207e	Command API, Read-Only, Reporting API, Access Sessions, Backup API	Yes	Edit	Delete
Middleware Integration	Ra00113ccab7a81e1105a2686e8f5ab3d153	Reporting API, Access Sessions, Backup API	Yes	Edit	Delete

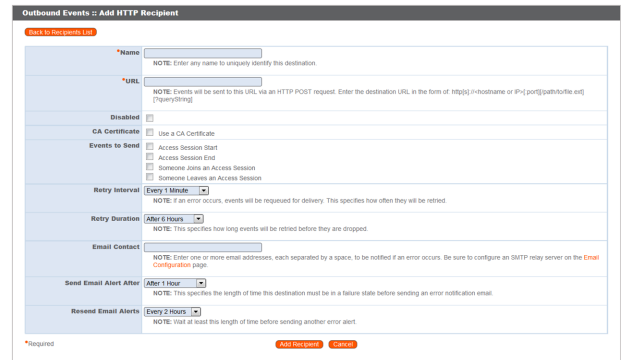
- Under **Permissions**, check **Full Access** to the **Command API**.
- For the **Reporting API**, check **Allow Access to Session Reports and Recordings** and **Allow Access to Presentation Session Reports and Recordings**. Also be sure to copy the values for both the **OAuth Client ID** and **OAuth Client Secret** for use in a later step.



- Click **Add API Account** to create the account.

Add an Outbound Event URL

- Go to **/login > Management > Outbound Events**.
- Click **Add New HTTP Recipient** and name it **Integration** or something similar.
- Enter the URL to use:
 - If using an appliance ID of "default":
`http://<middleware-host>:<port>/PAMPost`. The default port is **8180**.
 - If using an appliance ID other than "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 entered later in the plugin configuration. This name accepts only alphanumeric values, periods, and underscores.



- Scroll to **Events to Send** and check the following events:
 - Access Session Ends**
- Scroll to the bottom and click **Add Recipient**.
- Now, the list of outbound events should contain 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 BeyondTrust Privileged Remote Access SIEM Tool Plugin

Once the plugin has been deployed as described in [BeyondTrust Privileged Remote Access Middleware Engine Installation and Configuration](#), the plugin can then be configured and tested.


To begin configuration, launch the **Middleware Administration Tool** and click the clipboard icon next to the plugin name.

BeyondTrust Appliance

The first portion of the plugin configuration provides the necessary settings for communication between the plugin and the BeyondTrust Appliance. The configuration sections include:

- 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.
- 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. If outbound events are not being used, this value is still required, but any value may be used.
- BeyondTrust Appliance Host Name:** The hostname of the BeyondTrust Appliance. Do not include `https://` or other URL elements.
- BeyondTrust Integration API OAuth Client ID:** When using API accounts in BeyondTrust PRA 17.1 or newer, this field should contain the Client ID of the OAuth account.
- BeyondTrust Integration API OAuth Client Secret:** When using API Accounts available in BeyondTrust PRA 17.1 or newer, this field should contain the client Secret of the OAuth account.
- BeyondTrust Integration API User Name:** The username of the API service account created on the BeyondTrust Appliance.
- BeyondTrust Integration API Password:** The password of the above user.
- Locale Used for BeyondTrust API Calls:** This value directs the BeyondTrust Appliance to return session data in the specified language.
- Disabled:** Enable or disable this plugin configuration.
- 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.
- Use Non-TLS Connections:** Leave unchecked unless it is the specific goal to use non-secure connections to the BeyondTrust 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:** Specify which events the plugin processes when received by the middleware engine. Keep in mind that any 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.
 - a. **Access Session End**
13. **Polling Event Types:** If network constraints limit connectivity between the BeyondTrust Appliance and the middleware engine such that outbound events cannot be used, an alternative is to use polling. The middleware engine regularly polls the BeyondTrust Appliance for any sessions that have ended since the last session was processed. At this time, only the **Access Session End** event type is supported.
14. **Polling Interval:** Enter only if polling is used. This determines how often the middleware engine polls the BeyondTrust Appliance for sessions that have ended.

SIEM Tool Instance

These are the fields and selections needed to configure the plugin for integration with the SIEM tool. Please see the individual SIEM installation guides for guidance on what 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.

Report Templates

On the BeyondTrust Middleware Engine server, in the `<install dir>\Plugins<integration>\Templates` folder, there are multiple files ending with `*.hbs`. These files are used by the application to format the syslog messages transmitted to the SIEM tool each time a BeyondTrust session ends. The templates can be edited if desired.



Note: *If changes need to be made to a template, it is a good idea to first back up the original in case the changes ever need to be reverted.*

For additional information on Handlebars templates, see handlebarsjs.com.