Table of Contents

BeyondTrust SIEM Tool Plugin Installation and Administration ........................................... 3

Configure BeyondTrust Remote Support for Integration ......................................................... 4
  Verify the API Is Enabled ........................................................................................................ 4
  Create an OAuth API Account ............................................................................................... 4
  Add an Outbound Event URL ............................................................................................... 5

Configure the BeyondTrust Remote Support SIEM Tool Plugin .......................................... 7
  BeyondTrust Appliance B Series ........................................................................................... 7
  SIEM Tool Instance ............................................................................................................... 8
  Report Templates ................................................................................................................. 8

BeyondTrust Remote Support Integration with Splunk ......................................................... 9

Prerequisites for the BeyondTrust Remote Support Integration with Splunk ...................... 10
  Applicable Versions ............................................................................................................. 10
  Network Considerations ....................................................................................................... 10
  Prerequisite Installation and Configuration .......................................................................... 10

Configure Splunk for Integration with BeyondTrust Remote Support ............................... 11

Configure BeyondTrust Remote Support for Integration with Splunk ............................... 12

Configure the SIEM Tool Plugin for Integration between Splunk and BeyondTrust Remote Support ........................................................................................................... 13
  BeyondTrust Appliance B Series ........................................................................................... 13
  Splunk Instance .................................................................................................................... 13
BeyondTrust SIEM Tool Plugin Installation and Administration

The Security Information and Event Management (SIEM) tool plugin for BeyondTrust Remote Support 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 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 at www.beyondtrust.com/docs/remote-support/how-to/integrations/middleware-engine/index.htm.

Network Considerations

In addition to the network considerations listed in BeyondTrust Middleware Engine Installation and Configuration, check the individual SIEM installation guides, HP ArcSight or Splunk, for connectivity components which are specific to each tool and system.
Configure BeyondTrust Remote Support for Integration

Several configuration changes are necessary on the BeyondTrust Appliance B Series. You must make the changes for each B Series 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 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

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

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

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 Autotask.
6. Under **Permissions**, check **Allow Access** for the **Endpoint Credential Manager API**.
7. Click **Save** at the top of the page to create the account.

**Add an Outbound Event URL**

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 an appliance ID of **default**: `http://<middleware-host>:<port>/ERSPost`. The default port is 8180.
   - If using an appliance ID other than **default**: `http://<middleware-host>:<port>/ERSPost?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.
4. Scroll to **Events to Send** and check the following events:
   - **Support Session End**
   - **Customer Exit Survey is Completed**
   - **Representative Survey is Completed**
   - **Someone Joins a Support Session** (Optional)
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 BeyondTrust Remote Support SIEM Tool Plugin

Once the plugin has been deployed as described in BeyondTrust Remote Support 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 B Series

The first portion of the plugin configuration provides the necessary settings for communication between the plugin and the BeyondTrust Appliance B Series. The 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 elements.
4. **BeyondTrust Integration API OAuth Client ID**: When using API accounts in BeyondTrust Remote Support 16.2.1 or newer, this field should contain the Client ID of the OAuth account.
5. **BeyondTrust Integration API OAuth Client Secret**: When using API Accounts available in BeyondTrust Remote Support 16.2.1 or newer, this field should contain the client Secret of the OAuth account.
6. **BeyondTrust Integration API User Name**: The username of the API service account created on the B Series Appliance.
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.
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**: 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.

- Support Session End

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. At this time, 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.

15. **Retry Attempt Limit:** Enter the number of retries that can be attempted if the plugin fails to process an event.

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.

**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 plugin to format the textual 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 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 more information on Handlebars templates, please see the [Handlebars website](http://handlebarsjs.com).**
BeyondTrust Remote Support Integration with Splunk

IMPORTANT!
You must purchase this integration separately for both your Remote Support software and your Splunk solution. For more information, contact BeyondTrust sales.

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 Remote Support 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.
Prerequisites for the BeyondTrust Remote Support Integration with Splunk

Applicable Versions

- BeyondTrust Remote Support: 14.x and newer
- Splunk On-Premises and Cloud: 6.3.0 and newer

Network Considerations

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

<table>
<thead>
<tr>
<th>Outbound From</th>
<th>Inbound To</th>
<th>TCP Port #</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>BeyondTrust Middleware Engine Server</td>
<td>Splunk Server</td>
<td>1514</td>
<td>Session event data is pushed as specially formatted syslog messages into Splunk</td>
</tr>
<tr>
<td>BeyondTrust Appliance B Series</td>
<td>Splunk Server</td>
<td>514</td>
<td>Syslog event information from the B Series Appliance</td>
</tr>
</tbody>
</table>

Prerequisite Installation and Configuration

The Splunk integration is a BeyondTrust Middleware Engine plugin.

For more information on installing and working with the BeyondTrust Middleware Engine, please see the BeyondTrust Remote Support Middleware Engine Installation and Configuration document at [www.beyondtrust.com/docs/remote-support/how-to/integrations/middleware-engine](http://www.beyondtrust.com/docs/remote-support/how-to/integrations/middleware-engine).
Configure Splunk for Integration with BeyondTrust Remote Support

To install the integration, follow the steps below to import an item into Splunk.

1. Log in to Splunk as a user with administrative rights.

2. From the main home page, /app/launcher/home, click on the gear icon in the upper-left corner and go to Manage Apps.

3. On the Apps page, click Install app from file.

4. Browse to the location of the Splunk_TA_BeyondTrust-1.0.1.tar.gz file to install the Splunk Technology Add-on.

Other Considerations

For manual installation not completed through the web user interface, you must determine your deployment method, standalone or distributed. If distributed, your BeyondTrust technical account manager must go to the Splunk Indexer or Forwarder.
Configure BeyondTrust Remote Support for Integration with Splunk

In addition to the steps outlined in the BeyondTrust SIEM Tool Plugin Installation and Administration at www.beyondtrust.com/docs/remote-support/how-to/integrations/siem-tool/index.htm, the Splunk integration also supports consumption of syslog output directly from the BeyondTrust Appliance B Series.

All of the steps in this section take place in the BeyondTrust /appliance administrative interface.

1. Access your BeyondTrust interface by going to the hostname of your B Series Appliance followed by /appliance (e.g., https://support.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 a message format.
5. Click Submit.
Configure the SIEM Tool Plugin for Integration between Splunk and BeyondTrust Remote Support

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

BeyondTrust Appliance B Series

The first portion of plugin configuration provides the necessary settings for communication between the plugin and the B Series Appliance. These fields are described in the BeyondTrust SIEM Tool Plugin Installation and Administration at www.beyondtrust.com/docs/remote-support/how-to/integrations/siem-tool/index.htm.

Splunk Instance

1. **Target SIEM System:** Select Splunk from the list.
2. **SIEM Syslog Host:** Enter the hostname or IP address of the Splunk instance that should receive messages.
3. **SIEM Syslog Port:** Enter the port used by the Splunk instance to receive syslog messages, usually port 1514.
4. **SIEM Syslog Protocol:** Select the appropriate protocol from the list, usually UDP.
5. **Events to Process:** BeyondTrust session data may contain many different event types. All types are available; however, only a subset may be desired in the SIEM tool. Select only the events you would like sent to Splunk. Events matching unchecked event types are ignored.