Integrate Identity Security Insights With Elastic Security

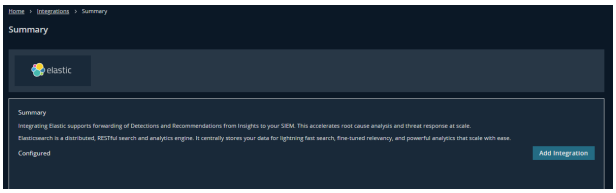
Identity Security Insights integrations allow you to connect third-party security information and event management (SIEM) tools to your BeyondTrust Insights console. Once an integration is configured, Insights automatically sends information regarding new detections and recommendations.

Retrieve the Elastic Security Credentials

1. Log in to your Elastic Cloud account and navigate to your desired deployment.
2. From your deployment's overview page, copy the **Cloud ID**. This ID is required in the next section.
3. Navigate to **Security/API Keys**.
4. Click **Create API Key**, and enter a name for the new key. This key is required in the next section.

Add an Elastic Integration

1. Within your Insights instance, click **Integrations** from the **Menu**, and select **Elastic** on the following page.
2. Click **Add Integration** beside the Elastic summary.
3. Enter the details for your Elastic configuration:
    - **Elastic Cloud ID:** The Cloud ID for your Elastic deployment.
    - **API Key:** The API Key created in Elastic.
4. Click **Save Settings**. You are redirected to your Elastic integration dashboard, with your new integration added.



Edit an Elastic Integration

Individual Elastic integrations can be edited or removed by clicking the ellipses beside a configured integration.

Clicking **Edit** directs you to the configuration details page for your integration. From here, you can edit the **Cloud ID** and **API Key** to assist in troubleshoot failing integrations.

Clicking **Delete** removes this integration entirely.

Note: *Edits to an integration may take up to two minutes to take effect.*

Integrate Identity Security Insights With Splunk

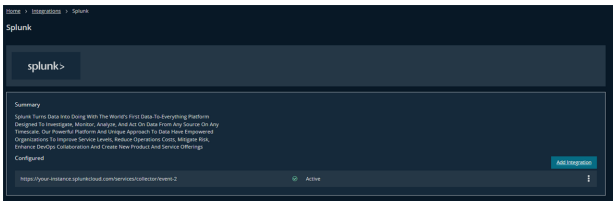
Identity Security Insights integrations allow you to connect third-party security information and event management (SIEM) tools to your BeyondTrust Insights console. Once an integration is configured, Insights automatically sends information regarding new detections and recommendations.

Create a New Splunk HTTP Event Collector

1. From your Splunk dashboard, navigate to **Settings > Add Data**, and click **monitor**.
2. Click **HTTP Event Collector**, and provide the following information:
    - **Name:** a name for the new token.
    - Changes to **Source name override**, **Description**, and **Indexer acknowledgment** are optional.
3. Click **Next**, and confirm where you would like the new events stored. This Index is used in your integration configuration.
4. Click **Review**, and ensure your new settings are correct.
5. Click **Submit**.
6. **Copy the token value** provided by Splunk Web. This is used in your integration configuration.

Add a Splunk Integration

1. Within your Insights instance, click **Integrations** from the **Menu**, and select **Splunk** on the following page.
2. Click **Add Integration** beside the Splunk summary.
3. Enter the details for your Splunk configuration:
    - **Hostname:** The hostname of your HTTP Event Collector endpoint.
    - **Index:** The index of your HTTP Event Collector.
    - **Token:** The token created with your new HTTP Event Collector.
4. Click **Save Settings**. You are redirected to your Splunk integration dashboard, with your new integration added.



Edit a Splunk Integration

Individual Splunk integrations can be edited or removed by clicking the ellipses beside a configured integration.

Clicking **Edit** directs you to the configuration details page for your integration. From here, you can edit the **Hostname**, **Index**, and **Token** to assist in troubleshoot failing integrations.

Clicking **Delete** removes this integration entirely.