



# BeyondTrust

## **Identity Security Insights Integration Guide 24.04**

## Table of Contents

---

<b>Identity Security Insights Integrations</b> .....	<b>3</b>
View Available Integrations .....	3
Integrate Identity Security Insights With Elastic Security .....	4
Retrieve the Elastic Security Credentials .....	4
Add an Elastic Integration .....	4
Edit an Elastic Integration .....	4
Elastic Schema Mapping .....	4
Integrate Identity Security Insights With Splunk .....	6
Create a New Splunk HTTP Event Collector .....	6
Add a Splunk Integration .....	6
Edit a Splunk Integration .....	6
Splunk Schema Mapping .....	7
Integrate Identity Security Insights with Application Webhooks .....	8
Overview .....	8
Webhook Configuration .....	8
Trigger an Existing Webhook .....	9
Edit or Delete an Existing Webhook .....	9
Integrate Identity Security Insights Webhooks with Slack .....	10
Integrate Identity Security Insights Webhooks with Microsoft Teams .....	11

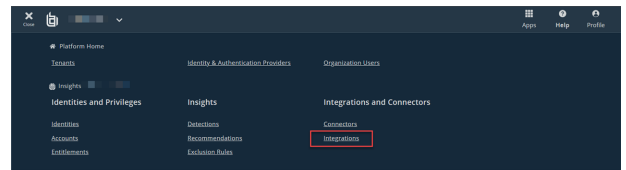
# Identity Security Insights Integrations

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 to the provided endpoint.

Along with custom integrations for SIEM tools like Splunk and Elastic, Identity Security Insights also provides generic Webhooks integrations to automate detection reporting to your security team's preferred platform.

## View Available Integrations

1. Log in to your Insights console.
2. Select your desired tenant from the dropdown at the top of the console.
3. Click **Menu** in the top left corner.
4. Under **Integrations and Connectors**, click **Integrations**.



## Integrate Identity Security Insights With Elastic Security

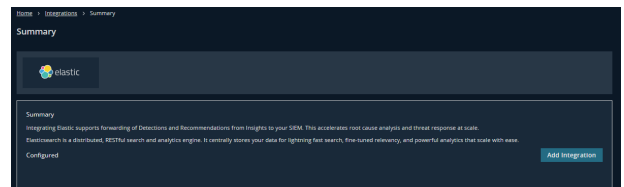
Identity Security Insights integrations allow you to connect third-party security information and event management (SIEM) tools to your BeyondTrust Insights console. Once an integration is configured, Insights automatically sends information regarding new detections and recommendations.

### 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.

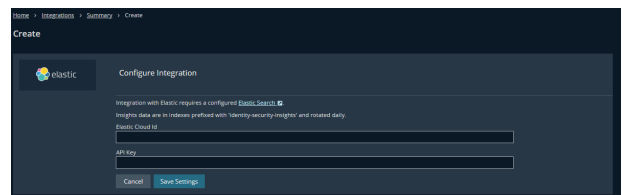


### Edit an Elastic Integration

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.

### Elastic Schema Mapping

Field	Internal Mapping
message	"<incidentDescription>"
tags	["Detection   Recommendation"]

Field	Internal Mapping
labels	{ "current_status": "<Open   Expected   FalsePositive   Resolved   InProgress>" }
event.id	"<incidentId>"
event.url	"https://app.beyondtrust.io/t/<tenantId>/detections/details/<incidentId>"
event.reason	"<incidentDefinitionDetail>"
event.severity	<incidentSeverity>
event.code	"<incidentDefinitionId>"
rule.id	"<incidentDefinitionId>"
rule.description	"<incidentDescription>"
rule.version	"<incidentDefinitionVersion>"
ecs.version	"8.7.0"
impacted_entities[i].entity_id	"<incidentImpactedEntityId>"
impacted_entities[i].entity_type	"<incidentImpactedEntityType>"
impacted_entities[i].tenant_id	"<incidentImpactedEntityTenantId>"
impacted_entities[i].name	"<incidentImpactedEntityName>"
impacted_entities[i].description	"<incidentImpactedEntityDescription>"

## Integrate Identity Security Insights With Splunk

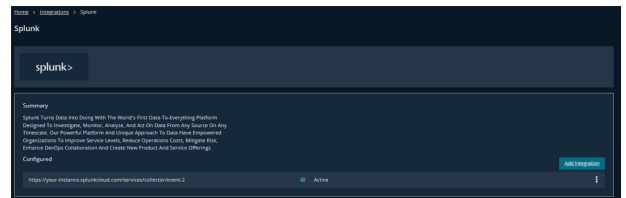
Identity Security Insights integrations allow you to connect third-party security information and event management (SIEM) tools to your BeyondTrust Insights console. Once an integration is configured, Insights automatically sends information regarding new detections and recommendations.

### 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.

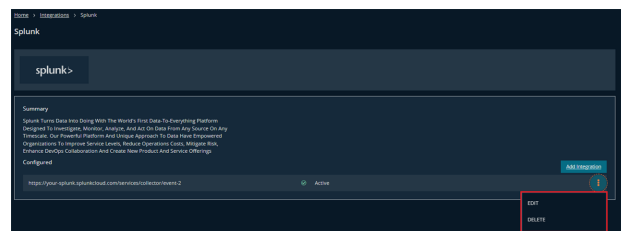


### Edit a Splunk Integration

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.



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

## Splunk Schema Mapping

Field	Internal Mapping
message	"<incidentDescription>"
tags	["Detection   Recommendation"]
labels	{ "current_status": "<Open   Expected   FalsePositive   Resolved   InProgress>" }
event.id	"<incidentId>"
event.url	"https://app.beyondtrust.io/t/<tenantId>/detections/details/<incidentId>"
event.reason	"<incidentDefinitionDetail>"
event.severity	<incidentSeverity>
event.code	"<incidentDefinitionId>"
rule.id	"<incidentDefinitionId>"
rule.description	"<incidentDescription>"
rule.version	"<incidentDefinitionVersion>"
ecs.version	"8.7.0"
impacted_entities[i].entity_id	"<incidentImpactedEntityId>"
impacted_entities[i].entity_type	"<incidentImpactedEntityType>"
impacted_entities[i].tenant_id	"<incidentImpactedEntityTenantId>"
impacted_entities[i].name	"<incidentImpactedEntityName>"
impacted_entities[i].description	"<incidentImpactedEntityDescription>"

# Integrate Identity Security Insights with Application Webhooks

## Overview

Webhooks allow Identity Security Insights to send information and data directly to your third-party applications, automating workflows within your organization. Once configured, webhooks provide a real-time method of notifying external systems about an incident.

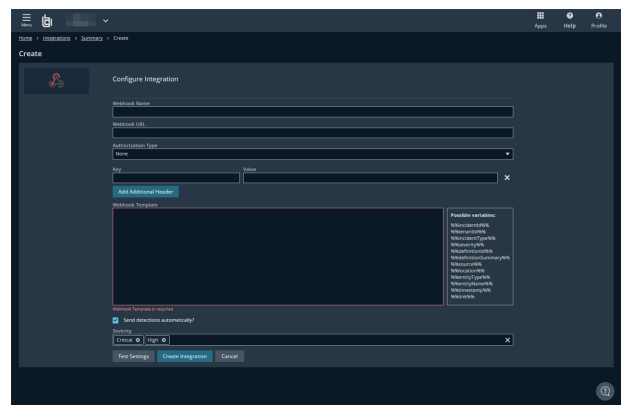
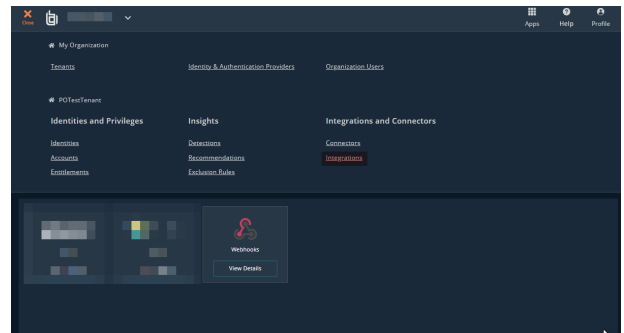
Detection and recommendation information can be sent from your Insights dashboard to applications like Slack, Tines, or Teams, and the webhook messages can be customized for your needs using a suite of built-in variables.

## Webhook Configuration

### Requirements

Identity Security Insights can integrate with any third-party application capable of receiving generic incoming webhooks. To integrate Insights via an application webhook, you must provide the following:

- **Webhook URL:** The URL where Insights will send information. This may represent the location of a Teams or Slack channel or other application URL.
- **Authorization Type:** If your webhook requires Basic or Bearer authorization, select it from the dropdown.
  - **Bearer:** Provide a long-lived access token in the **Token** field.
  - **Basic:** Provide a **Username** and **Password** to use for authentication.
- **Add Additional Header:** Click this option to add up to ten **Key-Value** headers in the webhook request.
- **Webhook Template:** A JSON object, which represents the information sent from Insight.



**Note:** The formatting of each JSON object is unique to each application. Consult the documentation for your application for more information.

Implementation examples are provided for the following applications:

- Microsoft Teams
- Slack



## Webhook Variables

The following variables may be added to the webhook template to provide additional information or context around the incident:

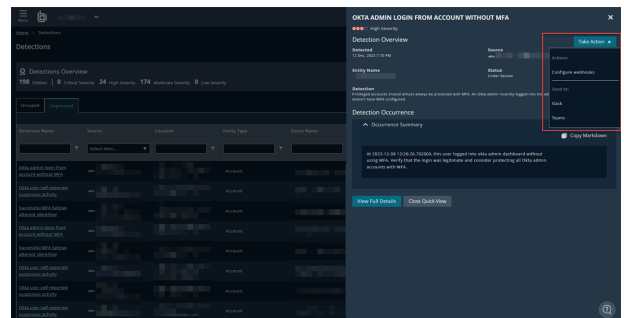
Field	Internal Mapping
%%incidentId%%	The internal ID of the detection or recommendation.
%%tenantId%%	The ID of the tenant that the detection or recommendation was detected in.
%%incidentType%%	Whether the incident was a detection or recommendation.
%%severity%%	The severity of the detection or recommendation, from 1 - 4. The higher the number, the more severe the issue.
%%definitionId%%	The name of the detection or recommendation.
%%definitionSummary%%	A high-level summary of the detection or recommendation.
%%source%%	A comma separated list of all the sources of the impacted entities.
%%location%%	A comma separated list of all the locations of the impacted entities.
%%entityType%%	A comma separated list of all the entity types of the impacted entities (i.e., Identity or Account).
%%entityName%%	A comma separated list of all the entity names of the impacted entities.
%%timestamp%%	The date and time the incident occurred.
%%link%%	A deep link to the details page of the specific detection or recommendation.

## Trigger an Existing Webhook

Once a webhook is configured, it can be manually triggered from any detection or recommendation via the **Take Action** menu. Triggering a webhook will send a message containing the specified detection or recommendation context to the configured application.

The Take Action menu is available in both the Detection or Recommendation Details pages, and the Quick View panel accessible from the Detection and Recommendation lists.

To trigger a webhook, select the configured application from the Take Action menu. The message will be immediately sent, and a notification will appear when the trigger is successful.

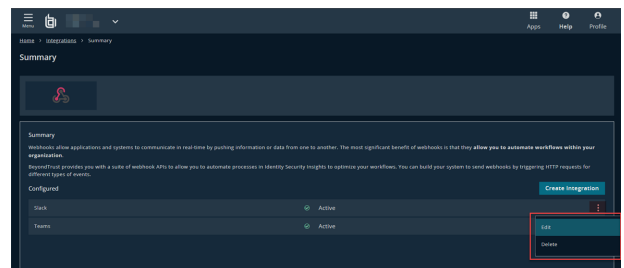


## Edit or Delete an Existing Webhook

Individual webhooks can be edited or removed by clicking the ellipses beside a configured webhook.

Clicking **Edit** directs you to the configuration details page for your webhook. From here you can edit the **Webhook Name**, **Webhook URL**, and update the **Webhook Template**.

Clicking **Delete** removes this integration entirely.

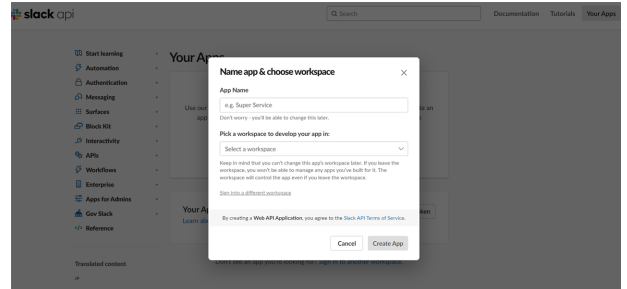


## Integrate Identity Security Insights Webhooks with Slack

Webhooks allow Identity Security Insights to send detection and recommendation information to a configured Slack channel.

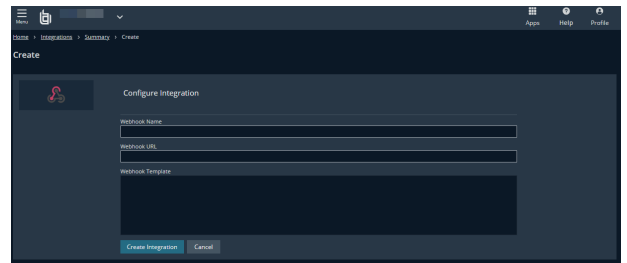
### Configure Incoming Webhooks in Slack

1. Within the Slack API dashboard, navigate to **Your apps > create your first app**.
2. Under **Create an app**, click **From scratch**, and provide an app name and workspace for your app to connect to.
3. Click **Create app**. You are then redirected to the app's setting page automatically.
4. Within the app settings:
  - Enable **Incoming Webhooks**, and select **Activate Incoming Webhooks**. The settings page reloads once this is enabled.
  - Enable **Add New Webhook to Workspace**.
  - Select a channel that the Insights app will post to, and click **Authorize**. The settings page reloads once your app is authorized.
  - Under **Webhook URLs for Your Workspace**, copy the newly generated URL for use in Identity Security Insights.



### Create a New Webhook

1. Within Identity Security Insights, navigate to **Menu > Integrations**.
2. Click **Webhooks**, and select **Create Integration**.
3. Enter the following information:
  - **Name:** a name for the new webhook.
  - **Webhook URL:** The URL generated by Slack for your new Slack app.
  - **Webhook Template:** A JSON object, which will be sent to the Webhook URL. A sample template is provided below.
4. Click **Configure Integration**.



### Sample Webhook Template

The following template creates a new card in Slack for a given detection or recommendation, provides additional information about the report, and includes a link to the incident in Identity Security Insights:

```
{
  "blocks": [
    {
      "type": "section",
      "text": {
        "type": "mrkdwn",
```

```

        "text": "A new %%incidentType%% was found:\n*<%%link%%|Go to %%incidentType%%>*"
    },
    {
        "type": "section",
        "fields": [
            {
                "type": "mrkdwn",
                "text": "Severity:\n%%severity%%"
            },
            {
                "type": "mrkdwn",
                "text": "When:\n%%timestamp%%"
            },
            {
                "type": "mrkdwn",
                "text": "Summary:\n%%definitionSummary%%"
            },
            {
                "type": "mrkdwn",
                "text": "Source:\n%%source%%"
            },
            {
                "type": "mrkdwn",
                "text": "Location:\n%%location%%"
            },
            {
                "type": "mrkdwn",
                "text": "Entity Type:\n%%entityType%%"
            },
            {
                "type": "mrkdwn",
                "text": "Entity Name:\n%%entityName%%"
            }
        ]
    }
]
}

```

## Integrate Identity Security Insights Webhooks with Microsoft Teams

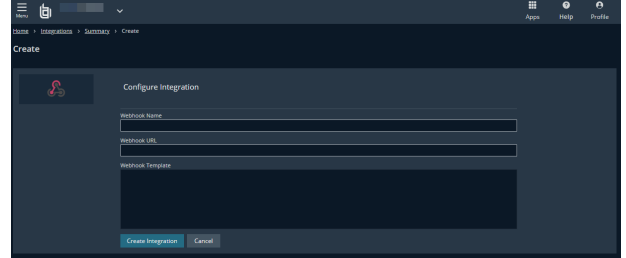
Webhooks allow Identity Security Insights to send detection and recommendation information to a configured Teams channel.

### Configure Incoming Webhooks in Teams

1. Within Teams, open the channel you would like to receive messages from Identity Security Insights.
2. Click the ellipsis in the upper right corner of the channel, and click **Connectors**.
3. In the Connectors window, search for **Incoming Webhook**, and click **Configure**.
4. Provide a name for your new webhook, and click **Create**.
5. Copy the newly generated unique webhook URL for use in Identity Security Insights.

## Create a New Webhook

1. Within Identity Security Insights, navigate to **Menu > Integrations**.
2. Click **Webhooks**, and select **Create Integration**.
3. Enter the following information:
  - **Name:** a name for the new webhook.
  - **Webhook URL:** The URL generated by Teams for your new webhook.
  - **Webhook Template:** A JSON object, which is sent to the Webhook URL. A sample template is provided below.
4. Click **Configure Integration**.



## Sample Webhook Templates

The following templates each create a new card in Teams for a given detection or recommendation, provide additional information about the report, and include a link to the incident in Identity Security Insights.

### Message Card

```
{
  "@type": "MessageCard",
  "@context": "http://schema.org/extensions",
  "themeColor": "0076D7",
  "summary": "A new %%incidentType%% was found.",
  "sections": [
    {
      "activityTitle": "A new %%incidentType%% was found.",
      "activitySubtitle": "%%tenantId%%",
      "facts": [
        { "name": "Incident Id", "value": "%%incidentId%%" },
        { "name": "Severity", "value": "%%severity%%" },
        { "name": "Definition Id", "value": "%%definitionId%%" },
        { "name": "Definition Summary", "value": "%%definitionSummary%%" },
        { "name": "Source", "value": "%%source%%" },
        { "name": "Location", "value": "%%location%%" },
        { "name": "Entity Type", "value": "%%entityType%%" },
        { "name": "Entity Name", "value": "%%entityName%%" },
        { "name": "Timestamp", "value": "%%timestamp%%" },
        { "name": "Link", "value": "%%link%%" }
      ],
      "markdown": true
    }
  ],
  "potentialAction": [
    {
      "@type": "OpenUri",
      "name": "Go to %%incidentType%%",
      "targets": [{ "os": "default", "uri": "%%link%%" }]
    }
  ]
}
```

```
]
}
```

## Adaptive Card

```
{
  "type": "message",
  "attachments": [
    {
      "contentType": "application/vnd.microsoft.card.adaptive",
      "contentUrl": null,
      "content": {
        "Summary": "A new %%incidentType%% was found.",
        "type": "AdaptiveCard",
        "actions": [
          {
            "type": "Action.OpenUrl",
            "title": "Open %%incidentType%%",
            "url": "%%link%"
          }
        ]
      },
      "$schema": "http://adaptivecards.io/schemas/adaptive-card.json",
      "version": "1.4",
      "body": [
        {
          "type": "TextBlock",
          "size": "Medium",
          "weight": "Bolder",
          "text": "A new %%incidentType%% was found.",
          "spacing": "ExtraLarge",
          "horizontalAlignment": "Center",
          "color": "Warning"
        },
        {
          "type": "ColumnSet",
          "columns": [
            {
              "type": "Column",
              "items": [
                {
                  "type": "TextBlock",
                  "weight": "Bolder",
                  "text": "%%incidentType%%",
                  "wrap": true,
                  "spacing": "Large",
                  "color": "Accent",
                  "horizontalAlignment": "Left"
                }
              ]
            },
            {
              "type": "TextBlock",
              "spacing": "None",
              "text": "Created %%timestamp%",
              "isSubtle": true,
            }
          ]
        }
      ]
    }
  ]
}
```

```
        "wrap": true,  
        "color": "Good",  
        "fontType": "Default"  
    }  
    ],  
    "width": "stretch"  
  }  
  ]  
},  
{  
  "type": "TextBlock",  
  "text": "%%definitionSummary%%",  
  "wrap": true  
},  
{  
  "type": "FactSet",  
  "facts": [  
    {  
      "title": "Incident Type:",  
      "value": "%%incidentType%%"  
    },  
    {  
      "title": "Incident Id:",  
      "value": "%%incidentId%%"  
    },  
    {  
      "title": "Definition Id:",  
      "value": "%%definitionId%%"  
    },  
    {  
      "title": "Severity:",  
      "value": "%%severity%%"  
    }  
  ],  
  "spacing": "Medium",  
  "separator": true  
}  
]  
}  
]  
}
```