Identity Security Insights Integration Guide 24.04

TC:4/25/2024

Table of Contents

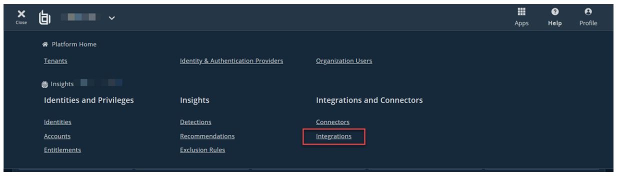
Identity Security Insights Integrations

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. From the dropdown at the top of the **Home** page, select your desired tenant.
3. Under **Integrations and Connectors**, click **Integrations**.



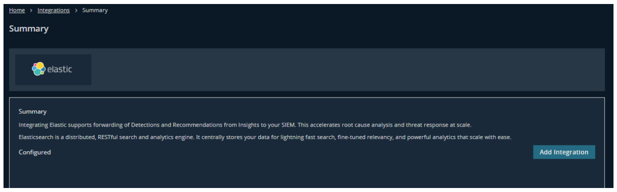
Integrate Identity Security Insights With Elastic Security

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

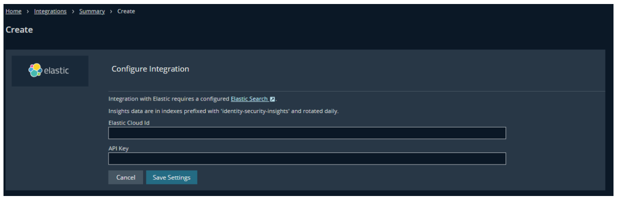


Integrating Elastic supports forwarding of Detections and Recommendations from Insights to your SIEM. This accelerates root cause analysis and threat response at scale.

Elasticsearch is a distributed, RESTful search and analytics engine. It centrally stores your data for lightning fast search, fine-tuned relevancy, and powerful analytics that scale with ease.

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



Integration with Elastic requires a configured Elastic Search.

Insights data are in indexes prefixed with 'identity-security-insights' and rotated daily.

Elastic Cloud Id

API Key

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_entites[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

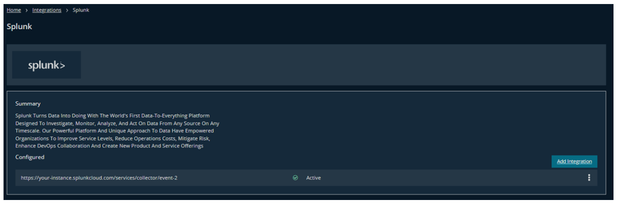
Identity Security Insights integrations allow you to connect third-party security information and event management (SIEM) tools to your BeyondTrust Insights console. Once an integration is configured, Insights automatically sends information regarding new detections and recommendations.

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.



Splunk Turns Data Into Doing With The World's First Data-To-Everything Platform Designed To Investigate, Monitor, Analyze, And Act On Data From Any Source On Any Timescale. Our Powerful Platform And Unique Approach To Data Have Empowered Organizations To Improve Service Levels, Reduce Operations Costs, Mitigate Risk, Enhance DevOps Collaboration And Create New Product And Service Offerings

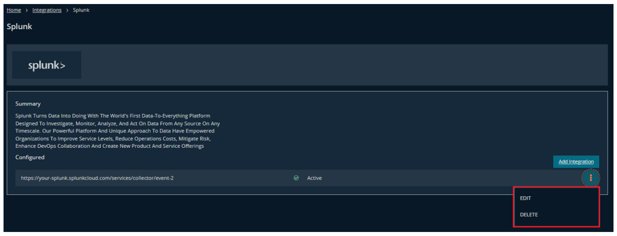
https://your-instance.splunkcloud.com/services/collector/event-2 ✓ Active

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.



Splunk Turns Data Into Doing With The World's First Data-To-Everything Platform Designed To Investigate, Monitor, Analyze, And Act On Data From Any Source On Any Timescale. Our Powerful Platform And Unique Approach To Data Have Empowered Organizations To Improve Service Levels, Reduce Operations Costs, Mitigate Risk, Enhance DevOps Collaboration And Create New Product And Service Offerings

https://your-splunk.splunkcloud.com/services/collector/event-2 ✓ Active

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

Splunk Schema Mapping

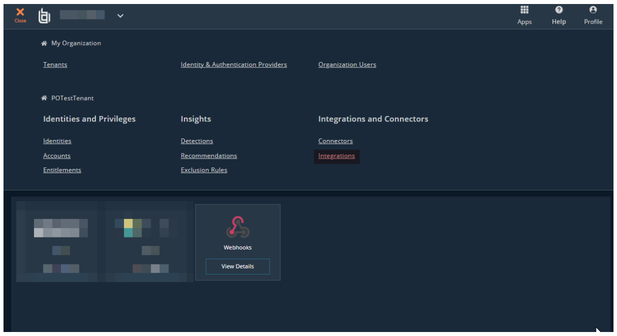
Field	Internal Mapping
message	"<incidentDescription>"
tags	["Detection | Recommendation"]
labels	{ "current_status": "<Open | Expected | FalsePositive | Resolved | InProgress>" }
event.id	"<incidentId>"
event.url	"https://app.beyondtrust.io/t/<tenantId>/detections/details/<incidentId>"
event.reason	"<incidentDefinitionDetail>"
event.severity	<incidentSeverity>
event.code	"<incidentDefinitionId>"
rule.id	"<incidentDefinitionId>"
rule.description	"<incidentDescription>"
rule.version	"<incidentDefinitionVersion>"
ecs.version	"8.7.0"
impacted_entites[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, eliminating manual intervention and delays. Once configured, webhooks provide a real-time method of notifying external systems about an incident, and can improve your organization's overall security posture.

Detection and recommendation information can be sent from your Insights dashboard to applications like Slack, Azure Sentinel, or Teams. Webhook message content can be customized using a suite of built-in variables.



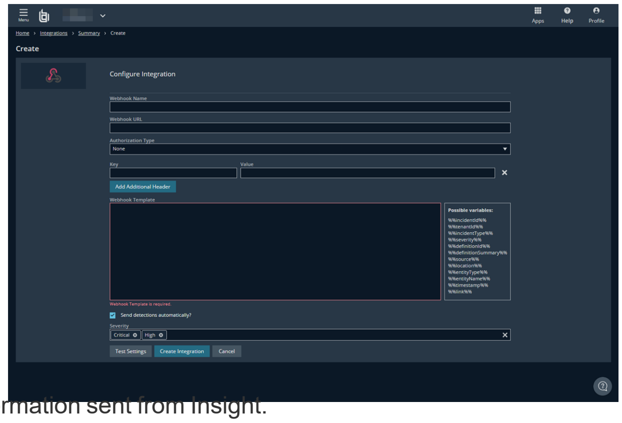
Webhook Configuration

To view existing webhooks or configure a new webhook, navigate to **Menu > Integrations**, and click **Webhooks**.

Create a New Webhook

Identity Security Insights can integrate with any third-party application capable of receiving generic incoming webhooks.

1. To integrate Insights via an application webhook, click **Create Integration** to create a new webhook.
2. Provide the following information:
   - **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.



Authorization Type: None

Possible variables:
%%incidentId%%
%%tenantId%%
%%incidentType%%
%%severity%%
%%definitionId%%
%%definitionSummary%%
%%source%%
%%location%%
%%entityType%%
%%entityName%%
%%timestamp%%
%%link%%

Webhook Template is required.

☑ Send detections automatically?

Severity: Critical, High

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

Implementation Examples

Implementation examples are provided for the following applications:

- Azure Sentinel
- Microsoft Teams
- Slack

Webhook Variables

The following variables may be added to the JSON object used in the webhook template. These variables provide additional information or context around the incident.

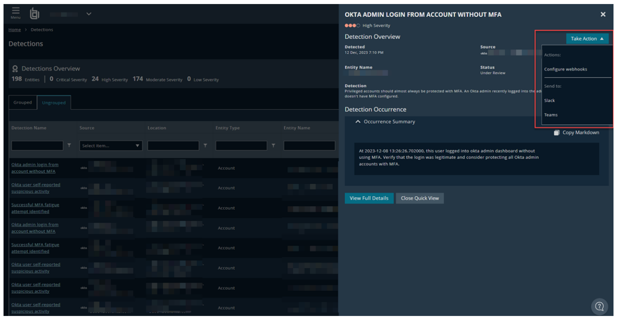
Variable	Description
%%incidentId%%	The internal ID of the detection or recommendation.
%%tenantId%%	The ID of the tenant that the detection or recommendation was detected in.
%%incidentType%%	Whether the incident was a detection or recommendation.
%%severity%%	The severity of the detection or recommendation, 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.



OKTA ADMIN LOGIN FROM ACCOUNT WITHOUT MFA

High Severity

Detection Overview

Detected
12 Dec, 2023 7:10 PM

Source
okta [redacted]

Entity Name
[redacted]

Status
Under Review

Detection
Privileged accounts should almost always be protected with MFA. An Okta admin recently logged into the ad... doesn't have MFA configured.

Detection Occurrence

Occurrence Summary

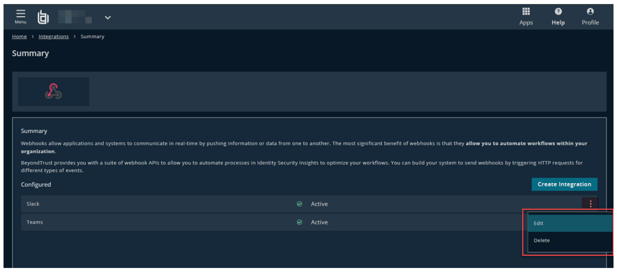
At 2023-12-08 13:26:26.702000, this user logged into okta admin dashboard without using MFA. Verify that the login was legitimate and consider protecting all Okta admin accounts with MFA.

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.



Summary

Summary

Webhooks allow applications and systems to communicate in real-time by pushing information or data from one to another. The most significant benefit of webhooks is that they **allow you to automate workflows within your organization**.

BeyondTrust provides you with a suite of webhook APIs to allow you to automate processes in Identity Security Insights to optimize your workflows. You can build your system to send webhooks by triggering HTTP requests for different types of events.

Configured

Slack	✓ Active
Teams	✓ Active

Integrate Identity Security Insights Webhooks with Microsoft Azure Sentinel

This webhook allows Identity Security Insights to automatically send detections and recommendations to Microsoft Azure Sentinel.

An Identity Security Insights account with Administrator privileges is required to create webhook integrations.

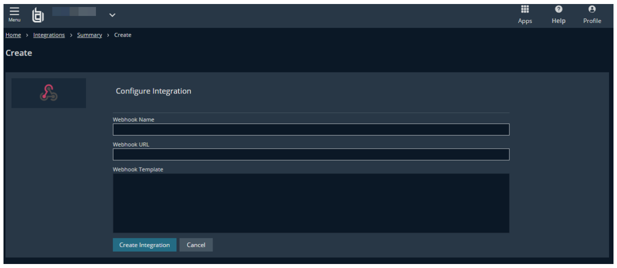
Requirements

To integrate Microsoft Azure Sentinel with Identity Security Insights, an Azure Logic App and Log Analytics Workspace must both be configured.

1. Create a new Microsoft Azure Log Analytics Workspace. For more information, see the Log Analytics Workspace documentation.
    - Copy the Connection Name, Workspace ID, and Workspace Key to use in the next step.
2. Create a new Logic App to use with Identity Security Insights. For more information, see the Microsoft Logic App documentation.
    - When adding a new action to send data, paste the Connection Name, Workspace ID, and Workspace Key from your Log Analytics Workspace.
3. Once your Logic App is created, click on the HTTP request node and copy the 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 your Logic App for the HTTP request node.
    - **Webhook Template**: A JSON object, which is sent to the Webhook URL.
4. Click **Configure Integration**.



Create

Configure Integration

Webhook Name

Webhook URL

Webhook Template

Integrate Identity Security Insights Webhooks with Microsoft Teams

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

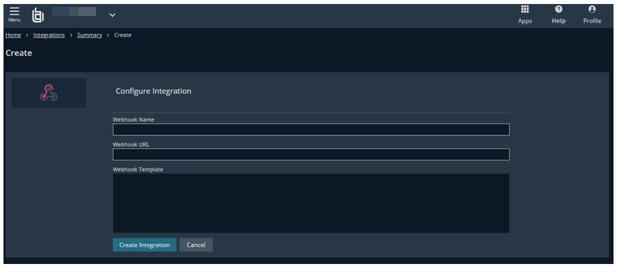
> *An Identity Security Insights account with Administrator privileges is required to create webhook integrations.*

Requirements

1. A Teams channel must be configured to receive incoming webhook events from Identity Security Insights. For more information on creating Incoming Webhooks in Teams, see the Microsoft documentation.
2. Once your Incoming Webhook is created, copy the 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 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**.



Example Card 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. For additional information on card formatting, see the Microsoft documentation.

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
          }
```

```
        ]
      }
    }
  ]
}
```

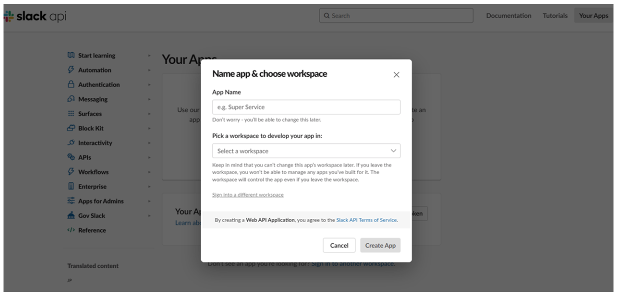
Integrate Identity Security Insights Webhooks with Slack

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

> *An Identity Security Insights account with Administrator privileges is required to create webhook integrations.*

Requirements

1. A Slack app and Bot must be configured in order to receive messages from Identity Security Insights. For more information on creating a Slack app and Bot, see the Slack documentation.
2. Once your Bot is created, copy the **Bot User OAuth Token** for your workspace.
3. Invite the Bot to the Slack channel you would like to receive updates from Insights with */invite @{botname}* (e.g. *invite /@insights*).



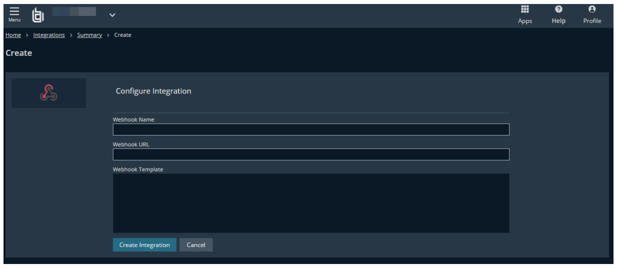
Don't worry - you'll be able to change this later.

Keep in mind that you can't change this app's workspace later. If you leave the workspace, you won't be able to manage any apps you've built for it. The workspace will control the app even if you leave the workspace.

By creating a **Web API Application**, you agree to the Slack API Terms of Service.

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:***https://slack.com/api/chat.postMessage*
   - **Authorization Type:** Select Bearer, and paste your **Bot User OAuth Token** in the value field.
   - **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. For more information on card formatting, see the Slack documentation.

```
{
    "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%%"
                }
            ]
        }
    ]
}
```