



# Cisco Secure Cloud Analytics

Webhooks and Services Configuration Guide



---

# Table of Contents

|   |           |
|---|-----------|
| <b>Introduction</b> .....                   | <b>5</b>  |
| Overview .....                              | 5         |
| Configuration Options .....                 | 5         |
| <b>AWS S3 Service</b> .....                 | <b>6</b>  |
| Overview .....                              | 6         |
| Edit AWS S3 Bucket Policy .....             | 6         |
| Add Service to Secure Cloud Analytics ..... | 7         |
| <b>AWS SNS Service</b> .....                | <b>9</b>  |
| Overview .....                              | 9         |
| Edit AWS SNS Access Policy .....            | 9         |
| Add Service to Secure Cloud Analytics ..... | 9         |
| <b>AWS SQS Service</b> .....                | <b>11</b> |
| Overview .....                              | 11        |
| Edit AWS SQS Permissions .....              | 11        |
| Add Service to Secure Cloud Analytics ..... | 11        |
| <b>Azure Log Analytics</b> .....            | <b>13</b> |
| Overview .....                              | 13        |
| Azure Workspace Credentials .....           | 13        |
| Add Service to Secure Cloud Analytics ..... | 13        |
| <b>DataDog</b> .....                        | <b>15</b> |
| Overview .....                              | 15        |
| Create API Key .....                        | 15        |
| Add Webhook to Secure Cloud Analytics ..... | 15        |
| <b>Email</b> .....                          | <b>17</b> |
| Overview .....                              | 17        |
| Add Service to Secure Cloud Analytics ..... | 17        |
| <b>GCP PubSub</b> .....                     | <b>19</b> |
| Overview .....                              | 19        |

---

|   |           |
|---|-----------|
| GCP Permissions .....                       | 19        |
| Add Service to Secure Cloud Analytics ..... | 19        |
| <b>GCP Storage .....</b>                    | <b>21</b> |
| Overview .....                              | 21        |
| GCP Permissions .....                       | 21        |
| Add Service to Secure Cloud Analytics ..... | 21        |
| <b>PagerDuty .....</b>                      | <b>23</b> |
| Overview .....                              | 23        |
| Create Integration Key .....                | 23        |
| Add Service to Secure Cloud Analytics ..... | 23        |
| <b>Slack .....</b>                          | <b>25</b> |
| Overview .....                              | 25        |
| Slack Configuration .....                   | 25        |
| Add Service to Secure Cloud Analytics ..... | 25        |
| <b>Splunk HEC .....</b>                     | <b>27</b> |
| Overview .....                              | 27        |
| Splunk Configuration .....                  | 27        |
| Enable HEC .....                            | 27        |
| Create HEC token .....                      | 28        |
| Determine your HEC URI .....                | 28        |
| Splunk Enterprise .....                     | 29        |
| Splunk Cloud (Self-Service) .....           | 29        |
| Splunk Cloud (Managed) .....                | 29        |
| Add Service to Secure Cloud Analytics ..... | 29        |
| <b>Webex App .....</b>                      | <b>31</b> |
| Overview .....                              | 31        |
| Configure Webex Space .....                 | 31        |
| Add Service to Secure Cloud Analytics ..... | 32        |
| <b>Webhooks .....</b>                       | <b>33</b> |
| Overview .....                              | 33        |

---

---

|  |           |
|--|-----------|
| Add Webhooks to Secure Cloud Analytics ..... | 33        |
| <b>Additional Resources</b> .....            | <b>35</b> |
| <b>Contacting Support</b> .....              | <b>36</b> |
| <b>Change History</b> .....                  | <b>37</b> |

---

# Introduction

## Overview

This guide explains how to configure webhooks and services in the Secure Cloud Analytics (formerly Stealthwatch Cloud) web portal. Services and webhooks allow us to send notification messages when alerts are published. This can be used to generate service tickets, notify staff, or initiate automatic remediation.

## Configuration Options

To view all configured services and webhooks, select **Settings > Webhooks/Services**.

Click the **⋮ (Ellipsis)** icon to access the following options for each configured service or webhook:

- **Delivery Logs:** Provide more context about the messages sent for each service, including the time sent, HTTP status codes, and the option to resend the message.
- **Edit:** Update the configuration details, including notes or descriptions for the service.
- **Enable/Disable:** Toggle on or off sending messages to a service.
- **Delete:** Remove the service from the Secure Cloud Analytics portal.



The SecureX Incident Manager service can't be deleted since it is automatically created by Secure Cloud Analytics when the SecureX ribbon is activated.

---

# AWS S3 Service

## Overview

This service sends alert notification messages to an Amazon S3 bucket. Each message will be a separate file with a unique name. To configure this service, you will need to edit the AWS S3 bucket policy to allow Secure Cloud Analytics to put objects into the bucket.

## Edit AWS S3 Bucket Policy



This configuration is for the public cloud. If you are on GovCloud, the account ID will change. See the [GovCloud Integration Guide](#) for more information.

1. Log in to your AWS S3 console.
2. In the **Buckets** list, choose the bucket you want to edit.
3. Click **Permissions**.
4. Under **Bucket policy**, click **Edit**.
5. In the **Policy** box, add the following, replacing `<bucket>` with your bucket name:

- If using new permissions:

```
{
  "Version": "2012-10-17",
  "Id": "ObsrvblWebhookPolicy",
  "Statement": [
    {
      "Sid": "ObsrvblWebhookStatement",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::757972810156:root"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::<bucket>/*"
    }
  ]
}
```

- If using existing permissions:

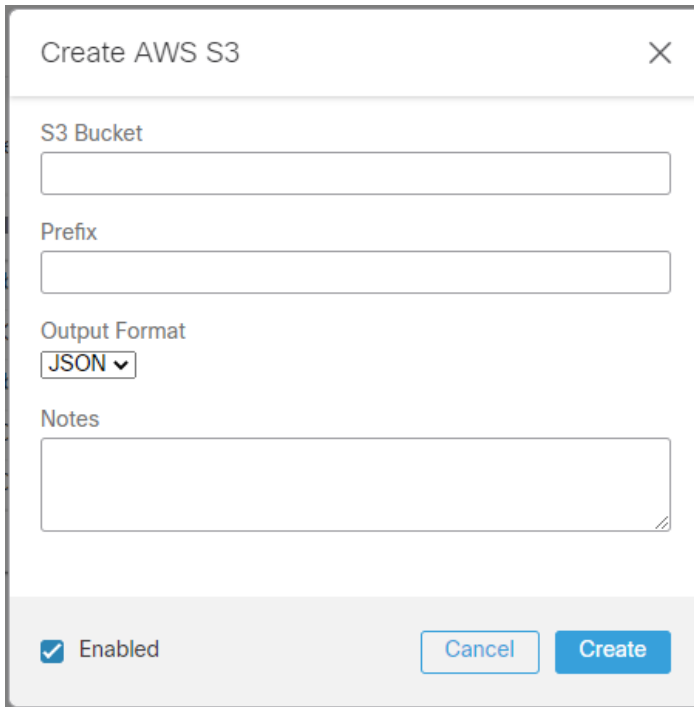
```
{
  "Sid": "ObsrvblWebhookStatement",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::757972810156:root"
  },
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::<bucket>/*"
}
```

6. Click **Save changes**.

## Add Service to Secure Cloud Analytics

1. Log in to your Secure Cloud Analytics web portal.
2. Select **Settings > Webhooks/Services**.

3. Select **Add New Webhooks/Service > AWS S3**. The **Create AWS S3** dialog box opens.



The screenshot shows a dialog box titled "Create AWS S3" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- S3 Bucket**: A text input field.
- Prefix**: A text input field.
- Output Format**: A dropdown menu currently showing "JSON".
- Notes**: A text area for entering notes.
- Enabled**: A checked checkbox.
- Buttons**: "Cancel" and "Create" buttons at the bottom right.

4. Enter your **S3 Bucket** name.
5. Enter a **Prefix** to limit where the notifications are delivered.
6. Select an **Output Format** from the drop-down list.
7. Enter **Notes** if you want to display text in the alert notification service summary.
8. Check the **Enabled** check box to enable the service.
9. Click **Create**.



---

# AWS SNS Service

## Overview

This service sends alert notification messages to an existing Amazon Simple Notification Service (SNS) topic. To configure this service, you will need to edit the SNS topic's Access Policy to allow Secure Cloud Analytics to publish to the topic.

## Edit AWS SNS Access Policy

1. Log in to your AWS SNS console.
2. Select **Topics**, then choose the topic you want to edit.
3. Select the **Access policy** tab, then click **Edit**.
4. Add the following to the existing policy, replacing `<Topic ARN>` with your topic's Amazon Resource Name (ARN):

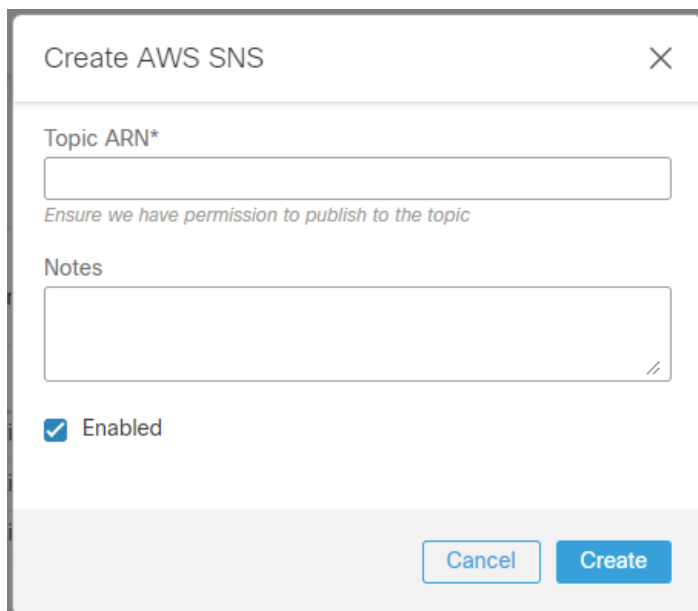
```
{
  "Sid": "swc_publish",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::757972810156:role/site_role"
  },
  "Action": "sns:Publish",
  "Resource": "<Topic ARN>"
}
```

5. On the **Review** page, click **Save changes**.

## Add Service to Secure Cloud Analytics

1. Log in to your Secure Cloud Analytics web portal.
2. Select **Settings > Webhooks/Services**.

3. Select **Add New Webhooks/Service > AWS SNS**. The **Create AWS SNS** dialog box opens.



Create AWS SNS

Topic ARN\*

Ensure we have permission to publish to the topic

Notes

Enabled

Cancel Create

4. Enter the **Topic ARN** used above.
5. Enter **Notes** if you want to display text in the alert notification service summary.
6. Check the **Enabled** check box to enable the service.
7. Click **Create**.

---

# AWS SQS Service

## Overview

This service sends alert notification messages to an Amazon Simple Queue Service (SQS). The message bodies will match the API JSON format. To configure this service, you will need to edit the SQS permissions to allow Secure Cloud Analytics to send messages to the queue.

## Edit AWS SQS Permissions

1. Log in to your AWS SQS console.
2. Select **Queues**.
3. Choose a queue, then click **Edit**.
4. Scroll to the **Access policy** section.
5. Add the following to the existing policy, replacing `<SQS ARN>` with your SQS's Amazon Resource Name (ARN):

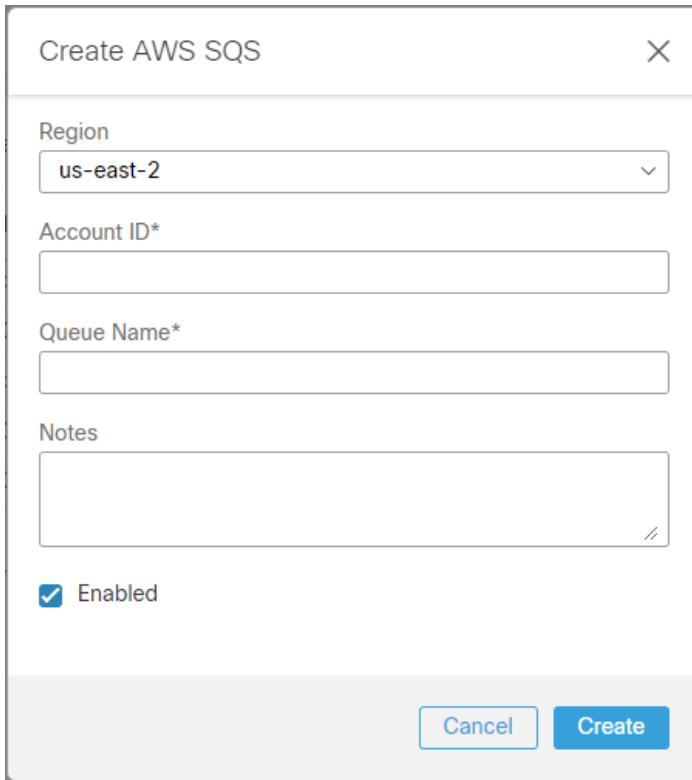
```
{
  "Sid": "SCA_Publish",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::757972810156:root"
  },
  "Action": [
    "sqs:SendMessage",
    "sqs:GetQueueURL"
  ],
  "Resource": "<SQS ARN>"
}
```

6. Click **Save**.

## Add Service to Secure Cloud Analytics

1. Log in to your Secure Cloud Analytics web portal.
2. Select **Settings > Webhooks/Services**.

3. Select **Add New Webhooks/Service > AWS SQS**. The **Create AWS SQS** dialog box opens.



The screenshot shows a dialog box titled "Create AWS SQS" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Region:** A dropdown menu with "us-east-2" selected.
- Account ID\*:** A text input field.
- Queue Name\*:** A text input field.
- Notes:** A text area with a small icon in the bottom right corner.
- Enabled:** A checked checkbox.
- Buttons:** "Cancel" and "Create" buttons at the bottom right.

4. Select your AWS deployment **Region** from the drop-down list.
5. Enter the **Account ID**.
6. Enter the **Queue Name**.
7. Enter **Notes** if you want to display text in the alert notification service summary.
8. Check the **Enabled** check box to enable the service.
9. Click **Create**.

# Azure Log Analytics

## Overview

This service sends alert notification messages to Azure Log Analytics workspaces. To configure this service, you will need the Workspace ID and key.

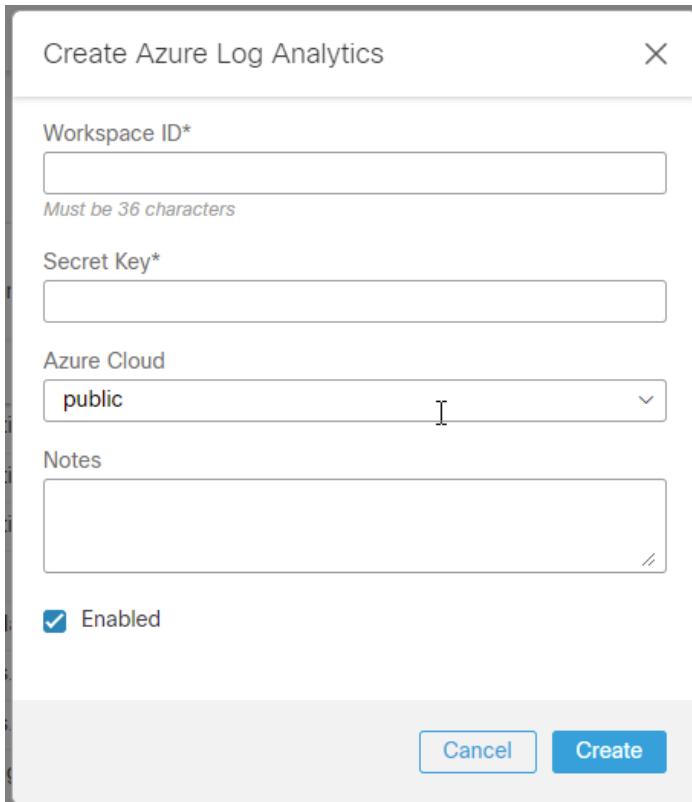
## Azure Workspace Credentials

1. Sign in to your Azure portal.
2. In the Search Bar, type **Log Analytics**.
3. Select **Log Analytics workspaces**.
4. In your list of **Log Analytics workspaces**, choose the workspace you want to send notifications to.
5. Select **Agents management**.
6. Copy the **Workspace ID** and the **Primary key**, or **Secondary key**.

## Add Service to Secure Cloud Analytics

1. Log in to your Secure Cloud Analytics web portal.
2. Select **Settings > Webhooks/Services**.

3. Select **Add New Webhooks/Service > Azure Log Analytics**. The **Create Azure Log Analytics** dialog box opens.



Create Azure Log Analytics

Workspace ID\*

Must be 36 characters

Secret Key\*

Azure Cloud

public

Notes

Enabled

Cancel Create

4. Enter the copied **Workspace ID**.
5. Enter the copied **Secret Key**.
6. Select your **Azure Cloud** deployment type from the drop-down list.
7. Enter **Notes** if you want to display text in the alert notification service summary.
8. Check the **Enabled** check box to enable the service.
9. Click **Create**.

---

# DataDog

## Overview

This webhook sends alert notification messages to DataDog. To configure this service, you will need to create a DataDog API key.

 We recommend creating a new API key instead of using an existing one.

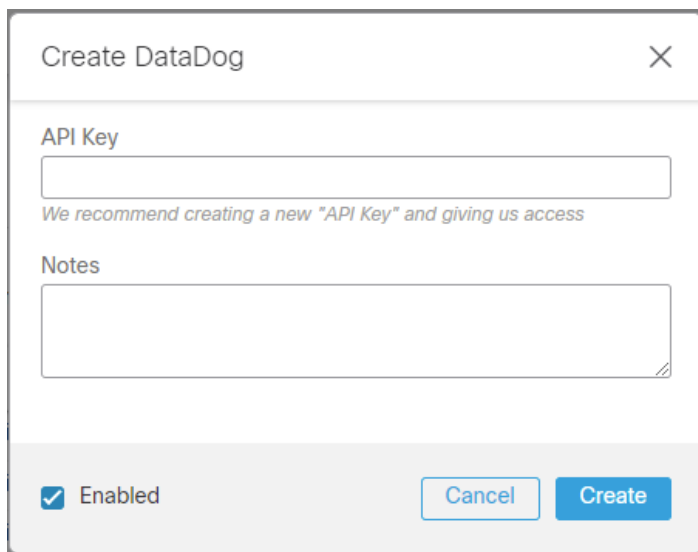
## Create API Key

1. Log in to your DataDog console.
2. Select your **Account Name > Organization settings**.
3. Click **API Keys**.
4. Click **New API key**.
5. Enter a name for your key.
6. Click **Create API key**.
7. Your key will be obscured by default. Hover over the purple box to reveal and copy the **API key**.

## Add Webhook to Secure Cloud Analytics

1. Log in to your Secure Cloud Analytics web portal.
2. Select **Settings > Webhooks/Services**.

3. Select **Add New Webhooks/Service > DataDog**. The **Create DataDog** dialog box opens.



Create DataDog

API Key

*We recommend creating a new "API Key" and giving us access*

Notes

Enabled

Cancel Create

4. Enter the copied **API Key**.
5. Enter **Notes** if you want to display text in the alert notification service summary.
6. Check the **Enabled** check box to enable the service.
7. Click **Create**.



# Email

## Overview

This service sends alert notifications to an email address.

## Add Service to Secure Cloud Analytics

1. Log in to your Secure Cloud Analytics web portal.
2. Select **Settings > Webhooks/Services**.
3. Select **Add New Webhooks/Service > Email**. The **Create Email** dialog box opens.

The screenshot shows a 'Create Email' dialog box with the following fields and controls:

- Email Address:** An empty text input field.
- Subject Format:** A text input field containing the text 'Alert from Cisco'.
- Email Footer:** An empty text input field.
- Notes:** A larger text area for additional information.
- Enabled:** A checkbox that is checked.
- Buttons:** 'Cancel' and 'Create' buttons at the bottom right.

4. Enter a recipient **Email Address**.
5. Update the **Subject Format** and **Email Footer**. You can add parameters to the email for information specific to that alert, as described in the following table:

| Parameter                    | Definition   |
|------------------------------|--|
| <code>\${type}</code>        | The alert type   |
| <code>\${source_name}</code> | The name of the entity that caused the alert to be generated |

---

|                       |                                |
|-----------------------|--------------------------------|
| <code>\${time}</code> | The time of alert generation   |
| <code>\${tags}</code> | Tags associated with the alert |

6. Enter **Notes** if you want to display text in the alert notification service summary.
7. Check the **Enabled** check box to enable the service.
8. Click **Create**.

# GCP PubSub

## Overview

This service sends alert notification messages to a Google Cloud PubSub topic. The messages will match the API JSON format. To configure this service, you will need to authorize Secure Cloud Analytics the right to publish messages to the topic.

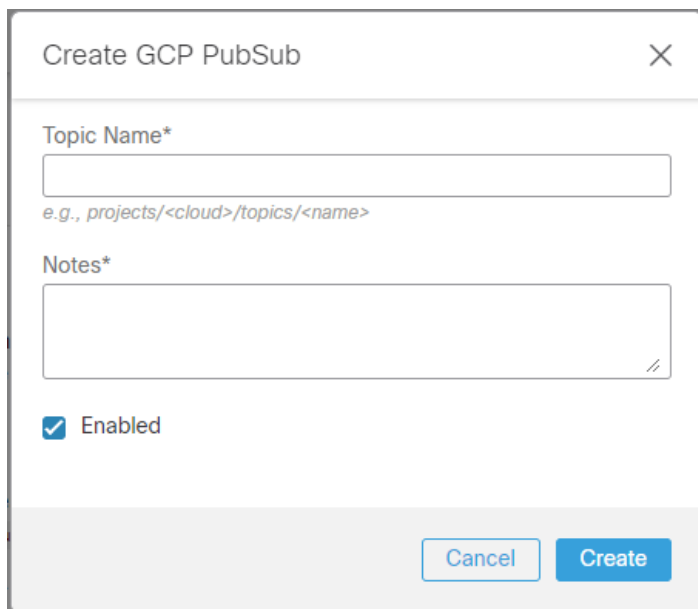
## GCP Permissions

1. Log in to your Google Cloud console.
2. Select **Pub/Sub > Topics**.
3. Choose the topic you want to edit.
4. In the **Permissions** tab, click **Add Principal**.
5. Fill out the **Grant access** form with the following information:
  - **Add principals:** `service@swatch-cloud.iam.gserviceaccount.com`
  - **Assign roles:** `Pub/Sub Publisher`
6. Click **Save**.

## Add Service to Secure Cloud Analytics

1. Log in to your Secure Cloud Analytics web portal.
2. Select **Settings > Webhooks/Services**.

3. Select **Add New Webhooks/Service > GCP PubSub**. The **Create GCP PubSub** dialog box opens.



Create GCP PubSub

Topic Name\*

*e.g., projects/<cloud>/topics/<name>*

Notes\*

Enabled

Cancel Create

4. Enter the **Topic Name**.
5. Enter **Notes** if you want to display text in the alert notification service summary.
6. Check the **Enabled** check box to enable the service.
7. Click **Create**.

---

# GCP Storage

## Overview

This service sends alert notification messages to a Google Cloud Storage bucket. Each message will be a separate file with a unique name. To configure the service, you will need to authorize Secure Cloud Analytics the right to create storage objects in the bucket.

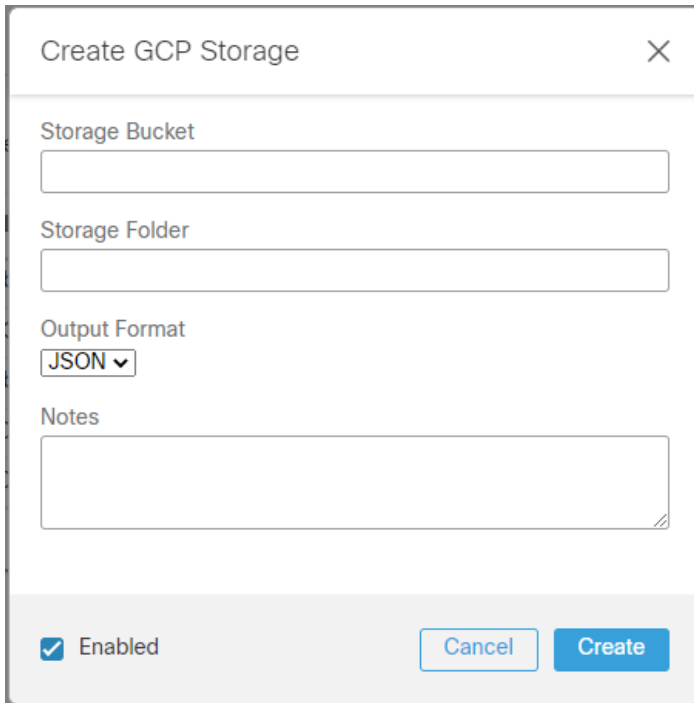
## GCP Permissions

1. Log in to your Google Cloud console.
2. Select **Cloud Storage > Buckets**.
3. Choose the bucket you want to edit.
4. Click **Permissions**, then click **Add Principal**.
5. Fill out the **Grant access** form with the following information:
  - **Add principals:** `service@swatch-cloud.iam.gserviceaccount.com`
  - **Assign roles:** `Storage Object Creator`
6. Click **Save**.

## Add Service to Secure Cloud Analytics

1. Log in to your Secure Cloud Analytics web portal.
2. Select **Settings > Webhooks/Services**.

3. Select **Add New Webhooks/Service > GCP Storage**. The **Create GCP Storage** dialog box opens.



The screenshot shows a dialog box titled "Create GCP Storage" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Storage Bucket**: A text input field.
- Storage Folder**: A text input field.
- Output Format**: A dropdown menu currently showing "JSON".
- Notes**: A text area for entering notes.
- Enabled**: A checked checkbox.
- Buttons**: "Cancel" and "Create" buttons at the bottom right.

4. Enter your **Storage Bucket** name.
5. Enter a **Storage Folder** where the files will be created in the bucket.
6. Select an **Output Format** from the drop-down list.
7. Enter **Notes** if you want to display text in the alert notification service summary.
8. Check the **Enabled** check box to enable the service.
9. Click **Create**.

---

# PagerDuty

## Overview

This service sends alert notification messages to PagerDuty. To configure this service, you will need to add a new API Service that interacts with Secure Cloud Analytics.

 We support the trigger event.

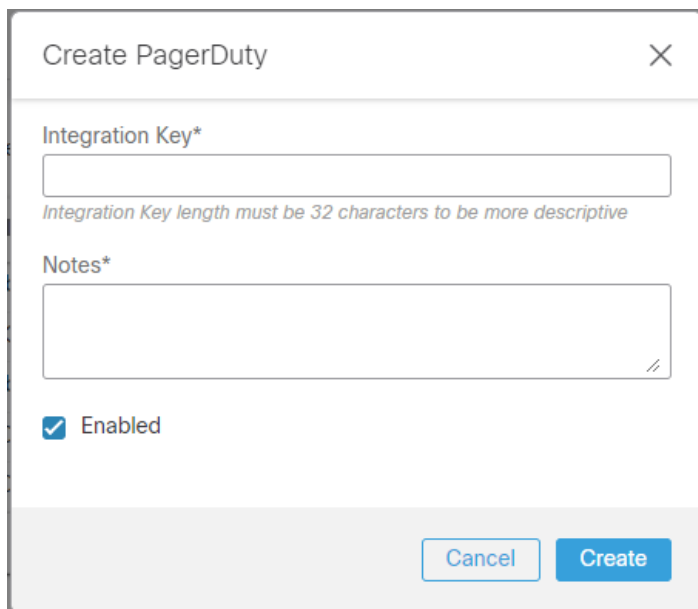
## Create Integration Key

1. Log in to PagerDuty.
2. Select **Configuration > Services**.
3. Click **+Add New Service**.
4. Enter a **Name** and **Description** for the service.
5. Under **Integration Settings**, select **Use our API directly**.
6. Click **Create Service**.
7. You will be redirected to the Integrations page for your service. Copy the **Integration Key**.

## Add Service to Secure Cloud Analytics

1. Log in to your Secure Cloud Analytics web portal.
2. Select **Settings > Webhooks/Services**.

3. Select **Add New Webhooks/Service > PagerDuty**. The **Create PagerDuty** dialog box opens.



Create PagerDuty

Integration Key\*

Integration Key length must be 32 characters to be more descriptive

Notes\*

Enabled

Cancel Create

4. Enter the copied **Integration Key**.
5. Enter **Notes** if you want to display text in the alert notification service summary.
6. Check the **Enabled** check box to enable the service.
7. Click **Create**.



---

# Slack

## Overview

This webhook sends alert notification messages to Slack. To configure this webhook, you will need to create a Slack app and Webhook URL.

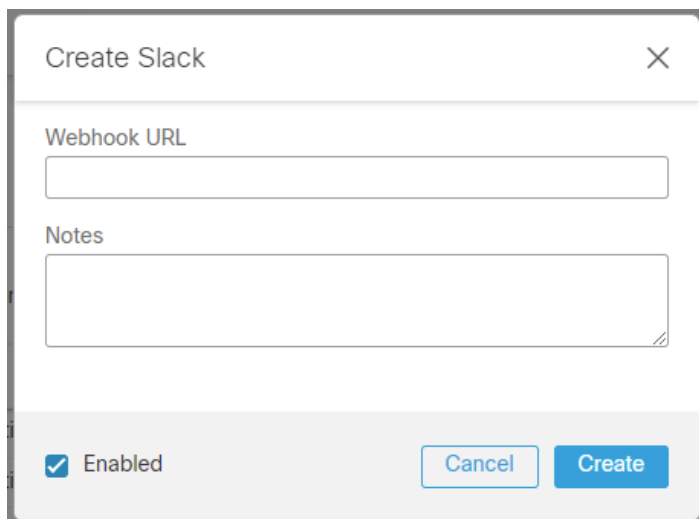
## Slack Configuration

1. Go to [https://api.slack.com/apps?new\\_app](https://api.slack.com/apps?new_app).
2. Click **Create an App**.
3. Enter a name and choose the workspace you want to send messages to.
4. Click **Create App**.
5. After creating, you'll be redirected to the settings page for your new app.  
If you are using an existing app, load settings using your app's management dashboard.
6. Select the **Incoming Webhooks** feature, and click the **Activate Incoming Webhooks** toggle to switch it on. The settings page will refresh.
7. Click **Add New Webhook to Workspace**.
8. Pick a channel that the app will post to, then click **Authorize**.
9. On your app settings page, you should see a new entry under the **Webhook URLs for Your Workspace** section, with a Webhook URL that will look something like this:  
`https://hooks.slack.com/services/NNNNNNN/`
10. Copy the **Webhook URL**.

## Add Service to Secure Cloud Analytics

1. Log in to your web portal.
2. Select **Settings > Webhooks/Services**.

3. Select **Add New Webhooks/Service > Slack**. The **Create Slack** dialog box opens.




The screenshot shows a dialog box titled "Create Slack" with a close button (X) in the top right corner. Below the title bar, there is a "Webhook URL" label followed by a text input field. Underneath that is a "Notes" label followed by a larger text area. At the bottom left, there is a checked checkbox labeled "Enabled". At the bottom right, there are two buttons: "Cancel" and "Create".


4. Enter the copied **Webhook URL**.
5. Enter **Notes** if you want to display text in the alert notification service summary.
6. Check the **Enabled** check box to enable the service.
7. Click **Create**.

# Splunk HEC

## Overview

This service sends alert notification messages to a Splunk HTTP Event Collector (HEC) for monitoring. To configure this service, you will need to create a Splunk HEC, generate an HEC token, then upload the HEC URI.

 Your Splunk Endpoint Certificate must be signed by a public Certificate Authority. For more information, refer to the [Splunk documentation](#).

 Make sure that your HEC is accessible externally, so that Secure Cloud Analytics can send notifications.

## Splunk Configuration

In the Splunk Enterprise console, you will need to enable the HEC, create a HEC token, and determine your HEC URI to send notifications from Secure Cloud Analytics to Splunk.

### Enable HEC

 If you subscribe to Splunk Cloud Platform, HEC is enabled by default.


To enable the Event Collector to receive events through HTTP, complete the following steps:

1. Log in to your Splunk Enterprise console.
2. Select **Settings > Data Inputs**.
3. Click **HTTP Event Collector**.
4. Click **Global Settings**.
5. In the **All Tokens** toggle button, select **Enabled**.
6. (Optional) Choose a **Default Source Type** for all HEC tokens. You can also type in the name of the source type in the text field above the drop-down list box before choosing the source type.
7. (Optional) Choose a **Default Index** for all HEC tokens.
8. (Optional) Choose a **Default Output Group** for all HEC tokens.
9. (Optional) To use a deployment server to handle configurations for HEC tokens, check the **Use Deployment Server** check box.

10. To have HEC listen and communicate over HTTPS, check the **Enable SSL** check box.

 We do not support disabling SSL.

11. Enter a number in the **HTTP Port Number** field for HEC to listen on.

 Confirm that no firewall blocks the port number that you specified in the HTTP Port Number field, either on the clients or the Splunk instance that hosts HEC.

12. Click **Save**.

## Create HEC token

To create a HEC token, complete the following steps:

1. Log in to your Splunk Enterprise console.
2. Select **Settings > Add Data**.
3. Click **monitor**.
4. Click **HTTP Event Collector**.
5. In the **Name** field, enter a name for the token.
6. (Optional) In the **Source name override** field, enter a source name for events that this input generates.
7. (Optional) In the **Description** field, enter a description for the input.
8. (Optional) In the **Output Group** field, select an existing forwarder output group.
9. (Optional) If you want to enable indexer acknowledgment for this token, check the **Enable indexer acknowledgment** check box.
10. Click **Next**.
11. (Optional) Confirm the source type and the index for HEC events.
12. Click **Review**.
13. Confirm that all settings for the endpoint are what you want.
14. If all settings are what you want, click **Submit**. Otherwise, click < to make changes.
15. Copy the token value that Splunk Web displays and paste it into a text editor for reference later.

## Determine your HEC URI

Based on your HEC deployment and Splunk subscription, determine the URI for your HEC.

---

## Splunk Enterprise

If you subscribe to Splunk Enterprise:

1. Copy the following URI and paste it into a plaintext editor:

```
https://<host>:<port>/services/collector
```

2. Replace `<host>` with the hostname in your plaintext editor.
3. Replace `<port>` with the port number in your plaintext editor.

## Splunk Cloud (Self-Service)

If you subscribe to self-service Splunk Cloud:

1. Copy the following URI and paste it into a plaintext editor:

```
https://input-<host>:8088/services/collector
```

2. Replace `<host>` with the hostname in your plaintext editor.

## Splunk Cloud (Managed)

If you subscribe to managed Splunk Cloud:

1. Copy the following URI and paste it into a plaintext editor:

```
https://http-inputs-<host>:443/services/collector
```

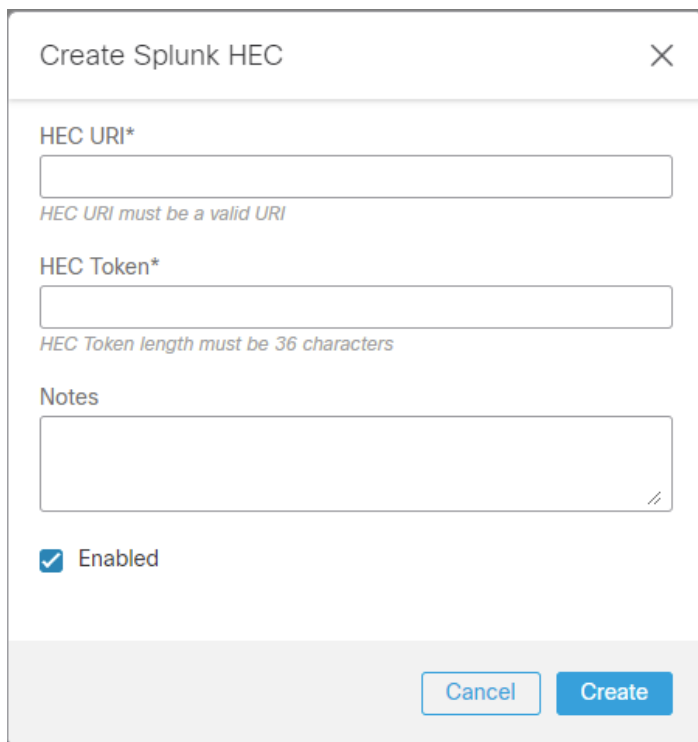
2. Replace `<host>` with the hostname in your plaintext editor.

## Add Service to Secure Cloud Analytics

To add the Splunk service URI to Secure Cloud Analytics, complete the following steps:

1. Log in to your Secure Cloud Analytics web portal.
2. Select **Settings > Webhooks/Services**.

3. Select **Add New Webhooks/Service > Splunk HEC**. The **Create Splunk HEC** dialog box opens.



Create Splunk HEC

HEC URI\*

HEC URI must be a valid URI

HEC Token\*

HEC Token length must be 36 characters

Notes

Enabled

Cancel Create

4. Enter the **HEC URI**.
5. Enter the copied **HEC Token**.
6. Enter **Notes** if you want to display text in the alert notification service summary.
7. Check the **Enabled** check box to enable the service.
8. Click **Create**.

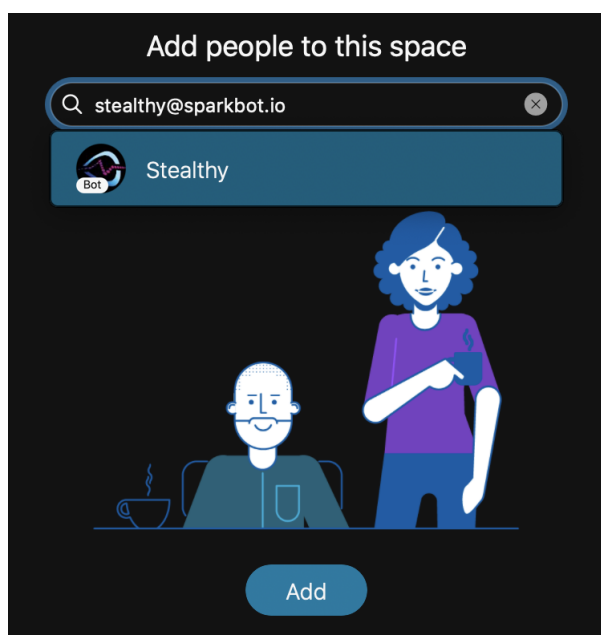
# Webex App

## Overview

This service sends alert notification messages to a Webex App Space. To configure this service, you will need the Space ID and to add the Secure Cloud Analytics bot to the Space.

## Configure Webex Space

1. Choose the space in Webex App to send notifications to and add `stealthy@sparkbot.io` to the Space.



2. Copy the Space ID. This can be found using either of the following ways:
  - In the Webex App space, click the (Gear) icon, then select **Copy space link**. Paste the link into a text editor. It will look something like this:  
`webxteams://im?space= space_id.`
  - In the Webex App space, copy the space information to the clipboard:
    - On Windows use `Ctrl + Shift + K`
    - On Mac use `Option + Command + K`

Paste the space information into a text editor, it will look something like this:

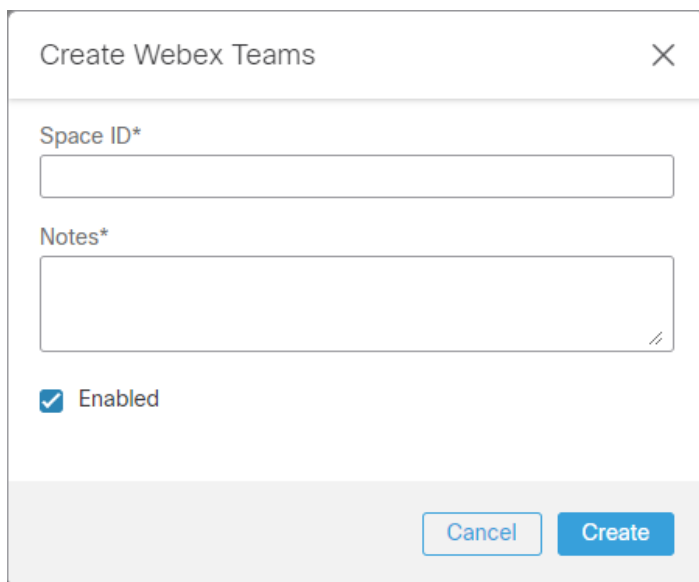
Space name: My Space

Space ID: 397538b0-7497-11ec-9fcb

```
Space URI: webexteams://im?space=397538b0-7497-11ec-9fc
Space URI (markdown): [My Space]
(webexteams://im?space=397538b0-7497-11ec-9fc)
Participant count: 3
External participant count: 0
Conversation type: group
Actor role: Member
```

## Add Service to Secure Cloud Analytics

1. Log in to your Secure Cloud Analytics web portal.
2. Select **Settings > Webhooks/Services**.
3. Select **Add New Webhooks/Service > Webex Teams**. The **Create Webex Teams** dialog box opens.



The screenshot shows a dialog box titled "Create Webex Teams" with a close button (X) in the top right corner. The dialog contains the following elements:

- A text input field labeled "Space ID\*".
- A text input field labeled "Notes\*" with a small double-slash icon (//) in the bottom right corner.
- A checked checkbox labeled "Enabled".
- Two buttons at the bottom right: "Cancel" and "Create".

4. Enter the copied **Space ID**.
5. Enter **Notes** if you want to display text in the alert notification service summary.
6. Check the **Enabled** check box to enable the service.
7. Click **Create**.



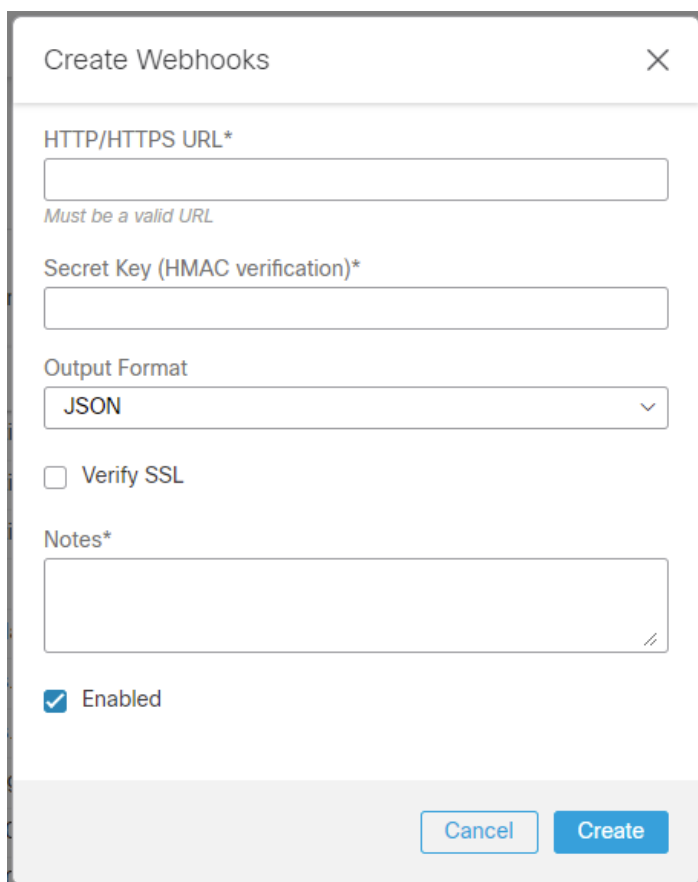
# Webhooks

## Overview

This general purpose webhook delivers alert notifications as a `POST` request to the webhook URL that you provide. The system generates a hash-based message authentication code (HMAC) hash of the `POST` request body using a webhook secret key that you provide. The `POST` request custom `X-OBSERVABLE-SIGNATURE` header contains this HMAC hash.

## Add Webhooks to Secure Cloud Analytics

1. Log in to your Secure Cloud Analytics web portal.
2. Select **Settings > Webhooks/Services**.
3. Select **Add New Webhooks/Service > Webhooks**. The **Create Webhooks** dialog box opens.



The screenshot shows a 'Create Webhooks' dialog box with the following fields and options:

- HTTP/HTTPS URL\***: A text input field with a note below it: *Must be a valid URL*.
- Secret Key (HMAC verification)\***: A text input field.
- Output Format**: A dropdown menu currently set to **JSON**.
- Verify SSL**: An unchecked checkbox.
- Notes\***: A text area for entering notes.
- Enabled**: A checked checkbox.

At the bottom of the dialog are two buttons: **Cancel** and **Create**.

4. Enter your webhook URL into the **HTTP/HTTPS URL** field.

- 
5. Enter your secret key into the **Secret Key (HMAC verification)** field.
  6. Select an **Output Format** from the drop-down list.
  7. If you used an HTTPS webhook URL, select **Verify SSL**.
  8. Enter **Notes** if you want to display text in the alert notification service summary.
  9. Check the **Enabled** check box to enable the service.
  10. Click **Create**.

# Additional Resources

For more information about Secure Cloud Analytics, refer to the following:

- <https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html> for a general overview
- <https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/tsd-products-support-series-home.html> for documentation resources
- <https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html> for installation and configuration guides, including the Secure Cloud Analytics Initial Deployment Guide

# Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: <http://www.cisco.com/c/en/us/support/index.html>
- To open a case by email: [tac@cisco.com](mailto:tac@cisco.com)
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers:  
<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

---

## Change History

| Revision | Revision Date    | Description                     |
|----------|------------------|---------------------------------|
| 1.0      | November 1, 2022 | Initial version.                |
| 1.1      | May 17, 2024     | Updated the Splunk HEC section. |

---

# Copyright Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

