

# Google SecOps for Jira Cloud

## Release Documentation and User Guide

<b>Overview</b>	<b>2</b>
<b>Compatibility Matrix</b>	<b>2</b>
<b>Prerequisites</b>	<b>3</b>
<b>User Permissions</b>	<b>3</b>
<b>Release History</b>	<b>3</b>
v1.1.0	3
v1.0.0	3
v2.0.0	4
v2.1.0	4
v2.2.0	5
<b>App Usage Instructions</b>	<b>5</b>
Installation	5
Getting User's Service Account JSON	5
Getting User's Service Account JSON for v1 Alpha	6
Configuring Google SecOps	7
Issue Creation	14
Issue Enrichment	15
<b>Third-Party Libraries Used</b>	<b>22</b>
<b>Known Behavior</b>	<b>24</b>
<b>Troubleshooting</b>	<b>24</b>

# Overview

Google SecOps is a global security telemetry platform for investigating incidents and hunting for threats in your enterprise network. Purpose-built on core Google infrastructure, Google SecOps can ingest massive amounts of telemetry data, normalize it, index it, correlate it to known threats, and make it available for analysis in seconds. The intended application will create Jira issues based on alerts, IoCs, detections and curated detections generated by the Google SecOps platform. The app also provides functionality to start, cancel and list retrohunts from the Jira platform.

Google SecOps for Jira Cloud provides functionality to periodically receive alerts, IoCs, detections, and curated detections from Google SecOps into Jira Cloud based on specific filters and configured schedules. The app allows users to configure filters related to alerts, detections, and curated detections. The app would create issues in the configured project in Jira based on the Google SecOps data. The created issues will have custom issue types, custom fields, and the Google SecOps Enrichment feature. The app provides a Google SecOps Enrichment manual action. Users can enrich Jira issues with any of the following that would be added as part of the Issue comment:

1. IoC Details
2. List Events Discovered
3. List Asset Impacted
4. List Asset Aliases
5. List User Aliases
6. UDM Search Query

## Compatibility Matrix

Browser	Google Chrome, Safari
Google SecOps REST API Version	IOCs: v1, Alerts: v1, Detections: v2, Curated Detections: v2, UDM Search: v1
Jira Cloud REST API Version	v3
Forge CLI Version	v10.13.4
Forge NodeJS Runtime Version	v20.x.x
Development Platform	Atlassian Forge

App Hosting Type	Cloud
Supported Atlassian Products	Jira, Jira Service Management

## Prerequisites

- Jira Cloud instance configured properly with Google SecOps installed.

## User Permissions

- Only Jira admin users could configure the App.

## Release History

### v1.1.0

- Updated ruleLabels parsing function with empty values handled.
- Updated Jira priority field mapping to handle malicious IoC severity.

### v1.0.0

- Automated Google SecOps Sync
  - The app will automatically fetch Google SecOps Alerts, Detections, and Indicators of Compromise (IoCs) and create Jira issues corresponding to them
  - The syncing process occurs at the user-configured interval.
  - The app provides flexibility to the user for doing certain configurations for the scheduler, Jira projects, and filters for detections and alerts
  - The app would create custom issue types for Alerts, Detections, and IoCs in Jira and add custom fields to enrich issues with Google SecOps Data
- Manual Google SecOps Enrichment
  - The app provides a manual action in the issues created by the app to enrich them with the Google SecOps information
  - App provides a manual action to bring data related to which Assets were impacted and which Events were discovered related to a particular Domain or IP address in the user-provided time frame and add the information in the Jira comment
  - The app allows users to perform the following enrichments:
    - IoC Details

- List Assets Impacted
- List Events Discovered

## v2.0.0

- Automated Google SecOps Sync
  - Added support for Curated Detections.
  - Added certain configuration parameters like support of dynamic region, limits on tickets created per sync, and some other filter parameters.
- Manual Google SecOps Enrichment
  - Added support to perform the following new enrichments:
    - List Asset Aliases
    - List User Aliases
- Manual Update Rule State
  - The app also provides the ability to activate/deactivate the Alerting Rule State and Live Rule State of a particular detection rule.
  - This action would be available in all detection Jira issues.
- Retrohunt
  - A new tab is added to the app configuration page, which allows the user to start/cancel a Retrohunt.
  - The user can provide RuleID or VersionID along with the date range while starting a new Retrohunt.

## v2.1.0

- Updated Forge Runtime
  - Updated Forge runtime from sandbox to v20.x.x in app manifest.
- Rebranding
  - Google Chronicle is now rebranded to Google SecOps.
  - Updated app configuration title, field descriptions, logs, and logos as per the new name across the app.
- UDM Search
  - The app also provides the ability to search UDM events based on provided query and time interval.
  - This action is provided as issue enrichment in all the Jira issues created by the app and would add the results to the Jira Issue comment.

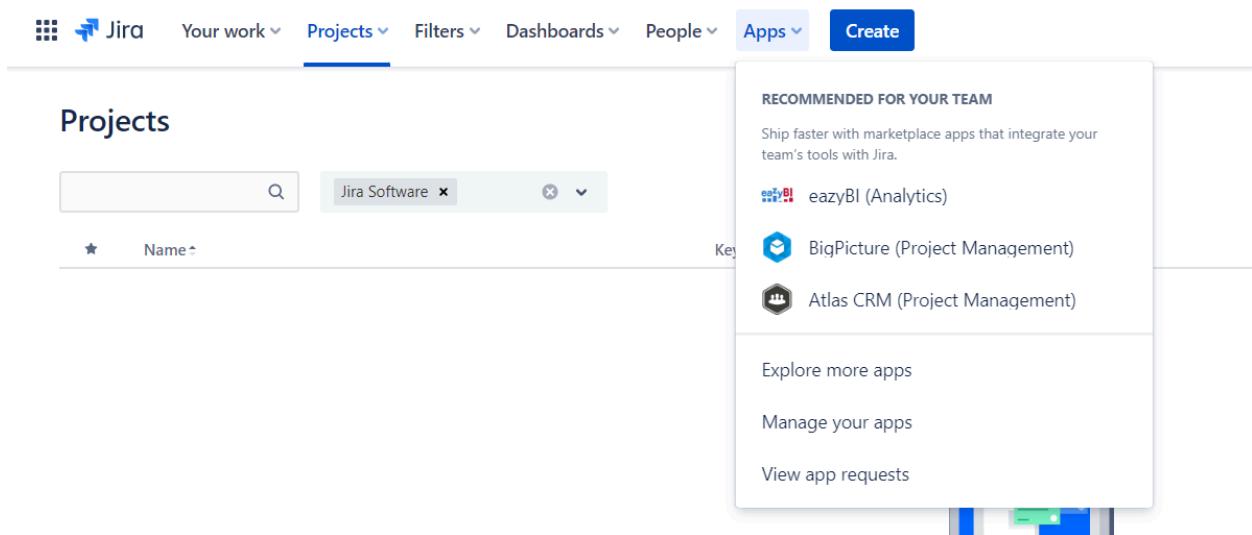
## v2.2.0

- Added support for Jira Work type field. The app would be compatible with both Issue Type and Work Type fields.

# App Usage Instructions

## Installation

1. Log in to your Atlassian Jira account. Click on the Apps tab on the top and then select Explore More Apps. Only Jira administrators have the privilege to access this.



2. In the search bar, search for the Google SecOps for Jira. Click on the app and then press the *Get App* button. A pop-up would appear, then click on the *Get it now* button. Pressing that would begin the installation process. Once installed, a message would appear on the bottom left indicating that installation is successful.
3. Click on the apps tab on the top and navigate to *Manage Apps*. You can see the Google SecOps for Jira in the User-Installed Apps section.

## Getting User's Service Account JSON

1. This app requires User's Service Account JSON from Google SecOps, which is used to make API calls from Jira to Google SecOps.
2. The User's Service Account JSON is required during the configuration of the app post-installation.
3. To generate the User's Service Account JSON, follow these [steps](#).

# Getting User's Service Account JSON for v1 Alpha

1. Log in to Google Cloud Console
  - a. Open Google Cloud Console (<https://console.cloud.google.com/>).
  - b. Make sure you have selected the required project in the top project dropdown.
2. Navigate to Service Account
  - a. In the left-hand menu, go to IAM & Admin > Service Accounts.
  - b. Click '+ CREATE SERVICE ACCOUNT' at the top.
3. Create a Service Account
  - a. Service account name: Enter a descriptive name (e.g., secops-service-account).
  - b. Service account ID: Automatically filled based on the name.
  - c. Description: Optional, e.g., 'Service account for Secops integration.'
  - d. Click CREATE AND CONTINUE.
4. Assign Roles
  - a. Assign the necessary roles based on the use case.
    - i. Viewer (read-only access)
    - ii. Editor (if modification required)
  - b. Or specific API roles like Cloud Storage Object Admin, Pub/Sub Publisher, etc.
  - c. Click CONTINUE > DONE.
5. Create and Download JSON Key
  - a. Go to the Service Accounts page.
  - b. Click on the service account you just created.
  - c. Go to the Keys tab.
  - d. Click ADD KEY > Create new key.
  - e. Choose JSON as the key type.
  - f. Click CREATE > The JSON file will automatically download.
  - g. Important: Keep this file secure.
6. Optional - Using the Service Account Key
  - a. Set the environment variable (Linux/macOS):
    - b. export GOOGLE\_APPLICATION\_CREDENTIALS="/path/to/secops-service-account.json"
  - c. Test authentication:
    - i. gcloud auth activate-service-account --key-file="\$GOOGLE\_APPLICATION\_CREDENTIALS"
    - ii. gcloud auth list
  - d. You should see the service account as active.
7. Optional - Restrict Key Usage
  - a. Consider restricting the service account key usage to specific APIs or IP ranges in the Keys > Key restrictions settings.
  - b. Required Permissions for Service Account JSON
    - i. Viewer Permission: If you only need to get or list resources, the Secops Viewer role is sufficient. [Learn more](#)

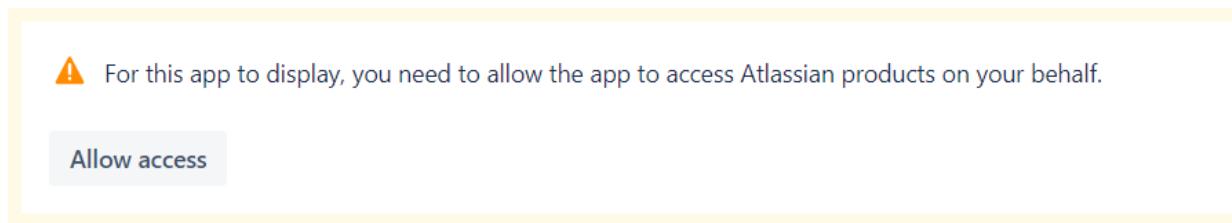
- ii. Editor Permission: If you need to create or update resources (such as creating or editing rules), the Secops Editor role is required. [Learn more](#)

## Configuring Google SecOps

- Post successful installation, under the Apps tab on the top, a Manage your Apps option would be visible. Clicking on it would open the Manage Apps section.

The screenshot shows the Jira interface with the 'Apps' tab selected. On the left, there's a search bar and filters for 'Owner' and 'Project'. Below that, a list of dashboards includes the 'Default dashboard'. To the right, a sidebar titled 'RECOMMENDED FOR YOUR TEAM' lists several apps with their icons: Easy Agile TeamRhythm, eazyBI (Analytics), and BigPicture (Project Management). At the bottom of the sidebar are links to 'Explore more apps', 'Manage your apps', and 'View app requests'.

- On the left panel, the Google SecOps for Jira Cloud under the Apps section would be visible. Clicking on it would open the configuration page for the Google SecOps for Jira Cloud.
- For the first time, it might ask for allowing the app to access Atlassian products on your behalf. Clicking on the Allow Access button would open the authorization window. After validating the permission, the Accept button needs to be clicked.



- It would open up the Configuration page for the app.
- The user needs to provide the *Google Service Account JSON* and *Select the region* based on the location of the Google SecOps backstory instance under the

Authentication Information panel.

## Authentication Information

User's Service Account JSON \* 

Region 

Enter Base URL \* 

6. In Scheduler Configurations, a user needs to select the interval at which the syncing process should occur between Google SecOps and Jira. The provided options are Hourly, Daily and Weekly. The app also allows fetching historical data. In the field *Number of days, to fetch IoCs/Alerts/Detections/CuratedDetections initially* users can add the number of days from which they want to collect data from the Google SecOps and create Jira issues.

### Scheduler Configuration

Run \*

Hourly

Number of days to fetch IoCs/Alerts/Detections initially \*

5

7. The user needs to select the project in which Jira issues will be created. If the required project is not visible in the dropdown, type the project name in the project selection field and if the project with the entered name is present it will show up for selection. The project selection field restricts team-managed projects. Users also need to select the *default Assignee*, the default will be unassigned.

### Project & Users

Select Project \* 

Select...

Default Assignee \*

Unassigned

8. The user needs to select the data polling checkbox for which the data needs to be fetched from the Google SecOps and Jira issues need to be created. At least one checkbox selection is required. The user needs to specify the number of the ticket that

needs to be created per invocation. The default limit for IoC and Curated Detection is 10000 and for Alerts is 100000.

8.1 - Two types of detections can be fetched from the Google SecOps, one with alert\_state as ALERTING and another one with NOT\_ALERTING. By default, the app retrieves both detections. However, this can be changed in the filters panel, as explained in the 11th point below.

## Data Polling

Enable IoC Matches

Please select to pull IoCs

Limit of IOC tickets to create per Invocation.\*

10000

Enable Alerts

Please select to pull Alerts

Limit of Alert tickets to create per Invocation.\*

100000

Enable Detections

Please select to pull Detections

Enable Curated Detection

Please select to pull Curated Detection

Limit of curated detection tickets to create per Invocation.\*

10000

9. In the *Detections to fetch by Rule ID or Version ID* field user can provide comma-separated ruleID and versionID and if it is not provided, by default detection of all ruleIDs and versionIDs will be collected.
10. In the *Curated Detections to fetch by Rule ID* field user can provide comma-separated ruleID and if it is not provided, by default detection of all ruleIDs and versionIDs will be collected.
11. By default the Curated Detections would be disabled. The user needs to enable it to start getting Curated Detections.
12. In the *Filter detections by alert state* field, the user can filter detections based on alert state. By default, it will be filtered by both states.

13. In the *List Basis*, the user can select which sort type the detections will be fetched. By default, it will be Created Time.
14. In the *Select the severity of alerts to be fetched* field user can select which severity of alerts issue will be created. Multiple severities can be provided. By default, issues will be created for all alert severities.

## Detection & Alert Configuration

---

Detections to fetch by Rule ID or Version ID [?](#)

Enter Comma Separated Values

Fetch all rules detections

Curated Detections to fetch by Rule ID [?](#)

Enter Comma Separated Values

Fetch all rules detections

Filter detections by alert state [?](#)

BOTH

List Basis [?](#)

CREATED TIME

Select the severity of alerts to be fetched [?](#)

Select...

15. After configuring all these fields, the user needs to click the *Validate and Save* button to save the configuration. On successful authentication, it would show a message as seen in the below image.

[Validate and Save](#) [Reset](#) [Stop Sync](#)

THE CONFIGURATION HAS BEEN DONE SUCCESSFULLY. SYNCING PROCESS WOULD INITIATE IN SOME TIME.

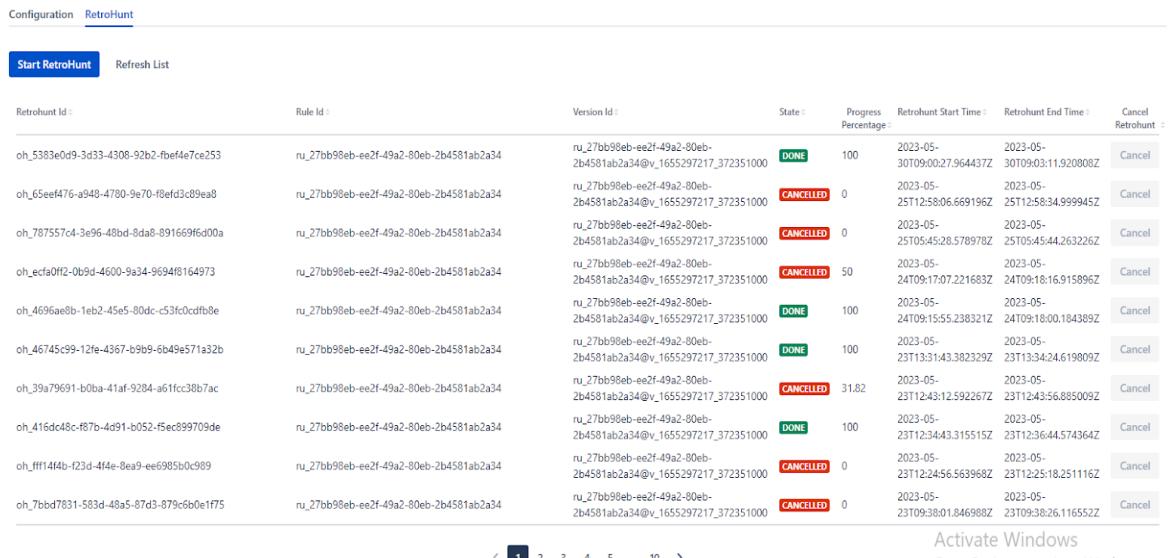
16. In case of a failed authentication, it would show a message as seen in the below image.

Validate and Save    Reset    Stop Sync

AUTHENTICATION FAILED! PLEASE CHECK THE SERVICE ACCOUNT JSON.

17. Reset Button: When the *Reset* button is clicked it will clear all the previously saved configuration parameters and checkpoints.
18. Stop Sync: When the *Stop Sync* button is clicked, further scheduler runs will be stopped.
19. In the Retrohunt tab, all previously started Retrohunts will be listed. There would be a cancel button for each Retrohunt to cancel that particular Retrohunt. The cancel button would be clickable only for Retrohunt those who are in the “RUNNING” state.

#### Chronicle App Configuration



Retrohunt Id :	Rule Id :	Version Id :	State :	Progress Percentage :	Retrohunt Start Time :	Retrohunt End Time :	Cancel Retrohunt :
oh_5383e0d9-3d33-4308-92b2-fbef4e7ce253	ru_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34	ru_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34@v_1655297217_372351000	DONE	100	2023-05-30T09:00:27.964437Z	2023-05-30T09:03:11.920808Z	<a href="#">Cancel</a>
oh_65eeff476-a948-4780-9e70-f8efcd3c9fea8	ru_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34	ru_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34@v_1655297217_372351000	CANCELLED	0	2023-05-25T12:58:06.669196Z	2023-05-25T12:58:34.999945Z	<a href="#">Cancel</a>
oh_787557c4-3e96-48bd-8da8-891669f6d00a	ru_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34	ru_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34@v_1655297217_372351000	CANCELLED	0	2023-05-25T05:45:28.578978Z	2023-05-25T05:45:44.263226Z	<a href="#">Cancel</a>
oh_ecfa0ff2-0b9d-4600-9a34-9694f8164973	ru_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34	ru_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34@v_1655297217_372351000	CANCELLED	50	2023-05-24T09:17:07.221683Z	2023-05-24T09:18:16.915896Z	<a href="#">Cancel</a>
oh_4696ae8b-1eb2-45e5-80dc-c53fc0cdfb8e	ru_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34	ru_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34@v_1655297217_372351000	DONE	100	2023-05-24T09:15:55.238321Z	2023-05-24T09:18:00.184389Z	<a href="#">Cancel</a>
oh_46745c99-12fe-4367-b9b9-6b49e571a32b	ru_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34	ru_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34@v_1655297217_372351000	DONE	100	2023-05-23T13:34:24.619009Z	2023-05-23T13:34:24.619009Z	<a href="#">Cancel</a>
oh_39a79691-b0ba-41af-9284-a61fcc38b7ac	ru_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34	ru_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34@v_1655297217_372351000	CANCELLED	31.82	2023-05-23T12:43:12.592267Z	2023-05-23T12:43:56.885009Z	<a href="#">Cancel</a>
oh_a16dc48c-f87b-4d91-b052-f5ec899709de	ru_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34	ru_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34@v_1655297217_372351000	DONE	100	2023-05-23T12:34:43.315515Z	2023-05-23T12:34:44.574364Z	<a href="#">Cancel</a>
oh_ff1f4f4b-f23d-4f4e-8ea9-e6985b0c989	ru_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34	ru_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34@v_1655297217_372351000	CANCELLED	0	2023-05-23T12:24:56.569568Z	2023-05-23T12:24:56.569568Z	<a href="#">Cancel</a>
oh_7bbd7831-583d-48a5-87d3-879c6b0ef75	ru_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34	ru_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34@v_1655297217_372351000	CANCELLED	0	2023-05-23T09:38:01.846988Z	2023-05-23T09:38:26.116552Z	<a href="#">Cancel</a>

< 1 2 3 4 5 ... 10 >

Activate Windows

Go to Settings to activate Windows.

20. By clicking on Start Retrohunt, a dialogue box will open and the User needs to provide the RuleID/VersionID, StartTime, and EndTime details. After that User needs to click on Start RetroHunt. On the successful start of Retrohunt, the success message would be visible.

## Start RetroHunt

Rule ID or Version ID \*

Rule Id or Version Id for which Retrohunt would run.

Start DateTime \*

1/5/2023 9:00 am x

Start time for the time range of retrohunt.

End DateTime \*

30/5/2023 9:00 am x

End time for the time range of retrohunt.

Cancel Start RetroHunt

ru\_27bb98eb-ee2f-49a2-80eb-CANCELED 0 2023-05-  
ee6985b0c989

✓ RetroHunt successfully started. x

21. The Users can click on the Refresh List button to see the latest List of the Retrohunts.

## Configuration Page Field Information

Field Name	Description
User's Service Account JSON	Enter service account JSON file contents. <a href="#">Steps</a> to get service account JSON file.
Select Region	Select the region based on the location of the Google SecOps backstory instance. Options: General, Europe, Europe West, Asia
Run	Select the interval at which the scheduler should run. Options: Hourly, Daily, Weekly
Number of days to fetch IoCs/Alerts/Detections initially	For how many days of historical data to be fetched. Max: 31 days
Select Project	Select the project in which Jira issues will be created. This field restricts Team-managed projects.
Default Assignee	Select to whom the created issues will be assigned by default. Options: unassigned, administrator, automatically
Enable IoC Matches	Whether to poll IoC Matches data or not
Enable Alerts	Whether to poll Alerts data or not
Enable Detections	Whether to poll Detections data or not
Detections to fetch by Rule ID or Version ID	Fetches detection by either Rule ID (format: ru_{UUID}) or Version ID (format: {ruleId}@v_{int64}_{int64}). Enter in comma-separated format to add multiple. Entered rules have precedence over the 'Fetch all rules detections' checkbox.
Fetch all rules detections	The detections of all rules and versions will be fetched.
Filter detections by alert state	Select the alert state to filter the detections to be fetched using fetch incidents. Available options are 'ALERTING' and 'NOT_ALERTING'. By default 'BOTH' option will be selected.
List Basis	Sort detections by 'DETECTION_TIME' or by 'CREATED_TIME'. If not specified, it defaults to 'CREATED_TIME'. This configuration is applicable to 'Detection alerts' only.

Select the severity of alerts to be fetched	Select the severity of alerts to be filtered for Fetch Incidents. Available options are 'High', 'Medium', 'Low', and 'Unspecified' (If not selected, fetches all alerts).
Validate and Save	This button will authenticate and validate all the configurations entered by the user. On successful authentication and validation, the configuration will be stored in the Forge storage.
Reset	This button will reset all the configurations and remove any old checkpoints stored.
Stop Sync	This button will stop any further scheduler runs.

## Issue Creation

- Once the Configurations are validated and saved successfully, the issue creation process will be initiated.
- The issues will get created in the configured project and syncing will occur at user-configured intervals.

The screenshot shows a Jira issue creation page for a project named 'test proj 1' under 'TP1-41025'. The issue title is 'rule\_to\_detect\_status\_update'. The 'Description' field contains a link to 'See this detection in Google SecOps'. The 'Detection Details' section lists various parameters for the rule, such as 'Google SecOps Detection ID' (de\_c83d78c5-8edf-39bf-3cc9-e85d7aae20cf), 'Google SecOps Rule Description' (This rule is to generate alerts when the event\_type is STATUS\_UPDATE), and 'Event Discovered' details like 'Event Timestamp' (2025-02-24T18:31:11Z) and 'Event Type' (STATUS\_UPDATE). The right side of the screen displays the Jira sidebar with sections for Backlog, Actions, Pinned fields, Details, Assignee (Unassigned), Reporter (Google SecOps for Jira Cloud), Development (Create branch, Create commit), Labels (None), Rule ID (ru\_39212a4a-170d-4130-a63d-0325f33ee077), Rule Version (ru\_39212a4a-170d-4130-a63d-0325f33ee077@v\_1732873302\_954607000), Live (After\_second), Rule Author (Shreya Kapadia), Generator (None), Alert State (ALERTING), and Rule Type (SINGLE\_EVENT). At the bottom, there are activity tabs (Show: All, Comments, History, Work log) and a summary bar.

- All the details related to the corresponding Detection/Alert/IOC will be added in the description along with the Event Discovered.

- In the Details panel, the user would be able to see the custom fields which have the Google SecOps information.
- In the Description, a link is provided to see the Detection/Alert/loc/CuratedDetections in Google SecOps. When the user clicks on the provided link, it navigates to the Google SecOps platform where details of the detection can be seen.

Projects / test proj 1 / TP1-41025

## rule\_to\_detect\_status\_update

+ Add @ Apps

Description

[See this detection in Google SecOps](#)

## Issue Enrichment

- If the user opens any of the issues created by the app and navigates to the top right corner, the user will be able to see a Google SecOps Enrichment option.

13 days left

Log work

Add flag

Google SecOps Enrichment

UDM Search

Update Rule State

Connect Slack channel

Convert to Subtask

Move

2. On clicking the Google SecOps Enrichment option, it would open a panel where the user needs to configure the data with which they want to enrich the Jira issue

## Google SecOps Enrichment

Enrich Type \*

List Assets Impacted (Max 5)

For Input \*

Domain name

For Value \* 

Date Range

Start date \*

2/18/1993



End date \*

2/18/1993

**Submit**

Cancel

1.

- Once the details are added and clicked on the submit button, it would add the details in the comment section of the issue.

Projects / Test120 / TST120-7

Show: All Comments History Work log Newest first ↗

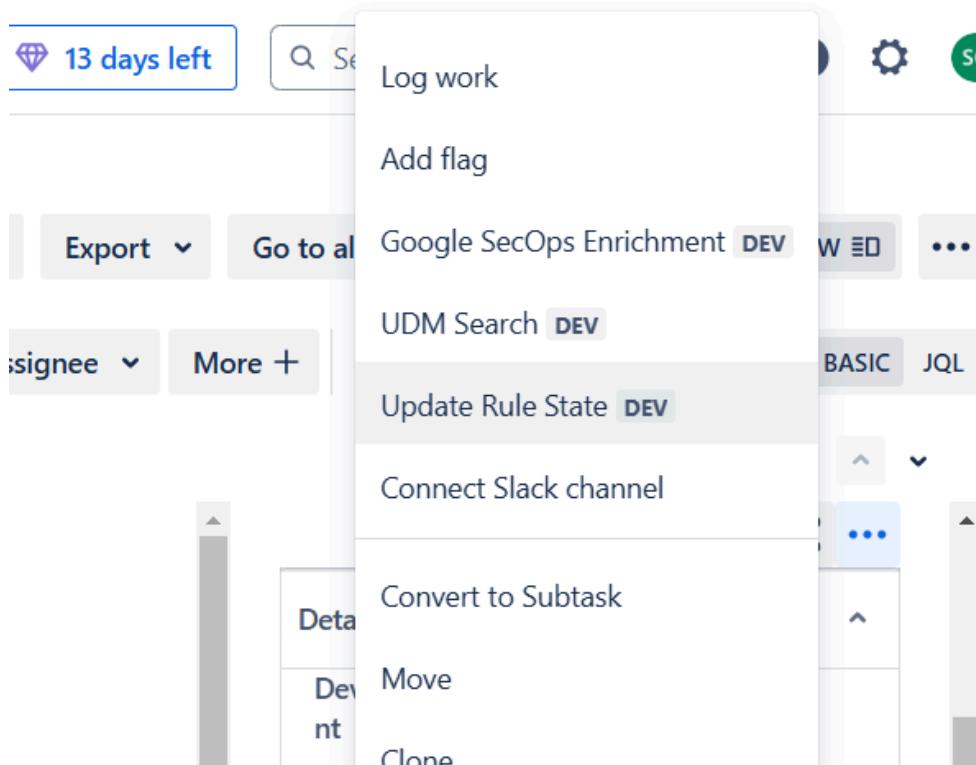
**JD** Add a comment... Pro tip: press **M** to comment

**JD** John Doe 18 seconds ago **oP**  
**Action:** List Assets impacted  
**Input Type:** domain\_name  
**Input:** test.com  
**Start Time:** 2018-02-18T10:48:45.038Z  
**End Time:** 2023-01-13T10:48:45.038Z

Asset	First Seen	Last Seen
1 hostname : crest_55	2021-03-17T15:09:00.549Z	2021-03-18T13:36:00.823Z
2 hostname : crest_38	2021-03-18T13:36:00.829Z	2021-03-18T13:36:00.829Z
3 hostname : crest_44	2021-03-17T12:18:01.446Z	2021-03-18T12:57:00.086Z
4 hostname : crest_66	2021-03-17T12:06:01.516Z	2021-03-18T13:27:00.042Z
5 hostname : crest_33	2021-03-17T13:00:01.818Z	2021-03-18T13:18:00.860Z

Edit · Delete · ⚙️

- For Update Rule State User needs to click on the 3 dots shown in the top right of the issue details screen.
- Select the Update Rule State option from the menu.



6. A model will open containing the fields to be entered by the user.

## Update Detection Rule State

Rule Name:

rule\_to\_detect\_status\_update

Rule ID:

ru\_39212a4a-170d-4130-a63d-0325f33ee077

Alerting Rule State

Please select/deselect to activate/deactivate the Alerting Rule State.

Live Rule State

Please select/deselect to activate/deactivate the Live Rule State.

**Submit**

[Cancel](#)

7. User can enable or disable the Alerting Rule State and Live Rule State by checking and unchecking the checkbox. On submission, the App would update the Rule state on the Google SecOps side and the message would be populated in the comment section of the Jira issue for failure or success.

 neil.mcharris 38 seconds ago

Successfully disabled Live Rule State for Detection Rule [ru\_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34].

[Edit](#) · [Delete](#) · 

 neil.mcharris 36 seconds ago

Successfully disabled Alerting for Detection Rule [ru\_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34].

[Edit](#) · [Delete](#) · 

 neil.mcharris 2 minutes ago

Successfully enabled Live Rule State for Detection Rule [ru\_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34].

[Edit](#) · [Delete](#) · 

 neil.mcharris 2 minutes ago

Successfully enabled Alerting for Detection Rule [ru\_27bb98eb-ee2f-49a2-80eb-2b4581ab2a34].

[Edit](#) · [Delete](#) · 

- For searching UDM events, the user needs to click on the 3 dots shown in the top right of the issue details screen.
- Select the UDM Search option from the menu.

The screenshot shows a Jira issue details page for a task titled "Google SecOps Enrichment". The "UDM Search" option is highlighted in the context menu, which also includes other actions like "Log work", "Add flag", and "Convert to Subtask".

<b>Description ID</b>	de_cbbbd902-acd9-8a59-6bd7-09bee0304804
<b>Description</b>	This rule is to generate alerts when the event_type is STATUS_UPDATE
<b>Description Host</b>	-

- A model will open containing the fields to be entered by the user.

## UDM Search

UDM query\*

Start DateTime

2/27/2025
12:41 PM
×

End DateTime

2/27/2025
12:41 PM
×

Limit ?

Submit
Cancel

11. Users need to enter the *UDM query*, select *Start Date/Time* and *End Date/Time*. Set the *Limit* field which represents the number of results fetched from the UDM search API and then click on the Submit button which will start the query execution.
12. The query execution will run in the background after the user clicks on the Submit button. Once the execution is completed, the search results will be added as Jira comments and can be seen in the Jira issue details screen. An appropriate error message will be added in Jira comment in case any error occurs in query execution or while adding Jira comments.
13. The search results will be added in batches of 10 per comment. If there are more than 10 results, additional Jira comments will be created.

The screenshot shows the Jira interface for a project named "test proj 1". The left sidebar shows various project management options like TP1 board, Timeline, Kanban board, Calendar, Reports, Summary, List, Forms, Goals, and Issues. The main area displays an activity feed for issue TP1-41025. A comment from "Google SecOps for Jira Cloud" is visible, timestamped 3 seconds ago. The comment content is:

```

UDM Query: metadata.event_type = "NETWORK_CONNECTION"

Event 1
• Event ID: 0000000d21026caab00fe0b7f11baebe882874700000000060000000000000000
• Event Timestamp: 2025-02-27T10:03:50Z
• Event Type: NETWORK_CONNECTION
• Description: -
• Security Results: -
• Principal Asset Identifier: Host Name: HARBOR-Z4XW33RTDW
IP: [ 0.0.0.0 ]
• Target Asset Identifier: IP: [ 2a01:b740:a16:3000::1f2 ]

```

14. This action can be performed for a maximum of 120 times per hour due to the API limitation on the Google SecOps side.

## UDM Search Field Information

Field Name	Description
UDM Query	Enter the exact query string which will be executed in Google SecOps
Start Date/Time	The start date and time for which the events will be queried.
End Date/Time	The end date and time for which the events will be queried.

Limit	The maximum no. of results to be fetched. The field will only allow values between 1 to 100.
-------	--

## Google SecOps Enrichment Field Information

Field Name	Description
Enrich Type	Select which type of data to be fetched. Options: List Assets Impacted (Max 5), List Events Discovered (Max 5), IoC Details
For Input	The options of this field are dependent on Enrich type: List Assets Impacted <ul style="list-style-type: none"> <li>• Domain Name</li> <li>• IP Address</li> <li>• HASH MD5</li> <li>• HASH SHA1</li> <li>• HASH SHA256</li> </ul> List Events Discovered <ul style="list-style-type: none"> <li>• Host Name</li> <li>• IP Address</li> <li>• MAC Address</li> <li>• Product ID</li> </ul> IoC Details <ul style="list-style-type: none"> <li>• Domain Name</li> <li>• IP Address</li> </ul>
For Value	Enter value based on selected For Input option. Multiple values are not supported.
Date Range	Select the start date and end date. This is only applicable to List Assets Impacted and List Events Impacted. Future dates are not allowed.

## Third-Party Libraries Used

Library	Version	Github/Bitbucket	License
eslint	7.32.0	<a href="https://github.com/eslint/eslint/blob/v7.32.0/LICENSE">https://github.com/eslint/eslint/blob/v7.32.0/LICENSE</a>	<a href="https://github.com/eslint/eslint/blob/v7.32.0/LICENSE">https://github.com/eslint/eslint/blob/v7.32.0/LICENSE</a>
eslint-plugin-react-hooks	4.2.0	<a href="https://github.com/facebook/react/blob/main/LICENSE">https://github.com/facebook/react/blob/main/LICENSE</a>	<a href="https://github.com/facebook/react/blob/main/LICENSE">https://github.com/facebook/react/blob/main/LICENSE</a>
husky	8.0.3	<a href="https://github.com/typicode/husky/blob/main/LICENSE">https://github.com/typicode/husky/blob/main/LICENSE</a>	<a href="https://github.com/typicode/husky/blob/main/LICENSE">https://github.com/typicode/husky/blob/main/LICENSE</a>
ataskit/button	20.3.12	<a href="https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/">https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/</a>	<a href="https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/">https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/</a>
ataskit/css-reset	6.16.0	<a href="https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/">https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/</a>	<a href="https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/">https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/</a>
ataskit/datetime-picker	15.13.1	<a href="https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/">https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/</a>	<a href="https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/">https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/</a>
ataskit/form	11.2.0	<a href="https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/">https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/</a>	<a href="https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/">https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/</a>
ataskit/icon-object	6.2.7	<a href="https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/">https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/</a>	<a href="https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/">https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/</a>
ataskit/select	18.10.6	<a href="https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/">https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/</a>	<a href="https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/">https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/</a>
ataskit/textfield	7.0.0	<a href="https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/">https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/</a>	<a href="https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/">https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/</a>
ataskit/tooltip	19.2.0	<a href="https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/">https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/</a>	<a href="https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/">https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/</a>
ataskit/checkbox	15.4.0	<a href="https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/">https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/</a>	<a href="https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/">https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/</a>

atlaskit/lozenge	11.14.0	<a href="https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/">https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/</a>	<a href="https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/LICENSE">https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/LICENSE</a>
atlaskit/modal-dialog	12.20.8	<a href="https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/">https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/</a>	<a href="https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/LICENSE">https://bitbucket.org/atlassian/atlassian-frontend-mirror/src/master/LICENSE</a>
react	16.13.1	<a href="https://github.com/facebook/react">github.com/facebook/react</a>	<a href="https://github.com/facebook/react/blob/main/LICENSE">https://github.com/facebook/react/blob/main/LICENSE</a>
react-dom	16.13.1	<a href="https://github.com/facebook/react">github.com/facebook/react</a>	<a href="https://github.com/facebook/react/blob/main/LICENSE">https://github.com/facebook/react/blob/main/LICENSE</a>

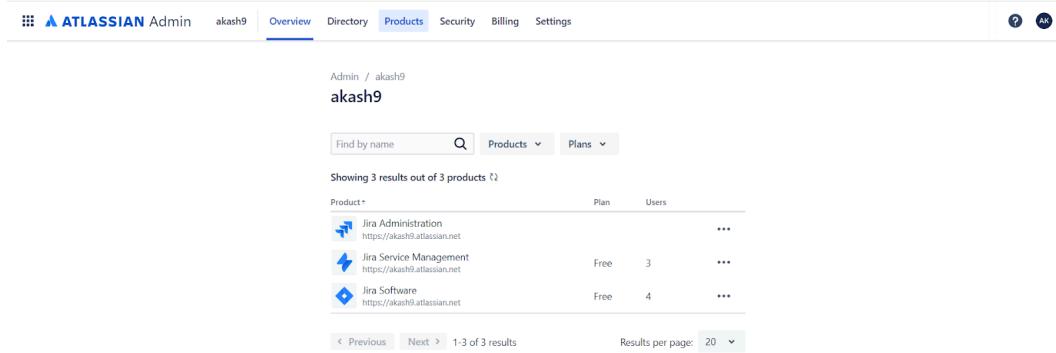
## Known Behavior

1. After the successful configuration, the Atlassian Forge platform may take some time to initiate the scheduler.
2. In case the user resets the app configuration then all the data of the configured interval will be fetched again and respective issues will be created. This will result in the duplication of previously created issues.
3. In case during the scheduler run, a platform unexpected error is faced then the scheduler execution will be stopped and will continue from the next scheduler run based on the checkpoint saved before the error occurrence.
4. In case an error occurred during the issue creation process, the app will retry the issue creation process of the failed records a maximum of 4 times. If after 4 times still the failure occurs then proper logs will be added for those failures.

## Troubleshooting

1. To see the application logs, follow the below steps. It would require the role of a system administrator.

- a. Go to <https://admin.atlassian.com/>.
- b. Click on Products.



The screenshot shows the Atlassian Admin interface with the 'Products' tab selected. The page displays three products: Jira Administration, Jira Service Management, and Jira Software, each with a status of 'Free' and 3 or 4 users respectively. The interface includes a search bar, navigation links for Overview, Directory, Products, Security, Billing, and Settings, and a bottom footer with pagination controls and a results per page dropdown set to 20.

Product	Plan	Users
Jira Administration https://akash9.atlassian.net		...
Jira Service Management https://akash9.atlassian.net	Free	3
Jira Software https://akash9.atlassian.net	Free	4

- c. Click on your site from the SITES AND PRODUCTS section.

The screenshot shows the Atlassian Admin interface with the 'Products' tab selected. The left sidebar has sections for 'Products' (User access settings, Product URLs, Release tracks, Sandbox) and 'SITES AND PRODUCTS' (akash9 Site). The main area shows a table of products with columns for Product, Plan, Users, and Actions. Three products are listed: Jira Administration (Plan: System, Users: 1), Jira Service Management (Plan: Free, Users: 3), and Jira Software (Plan: Free, Users: 4). Each product row has a 'Manage access' link under the Actions column.

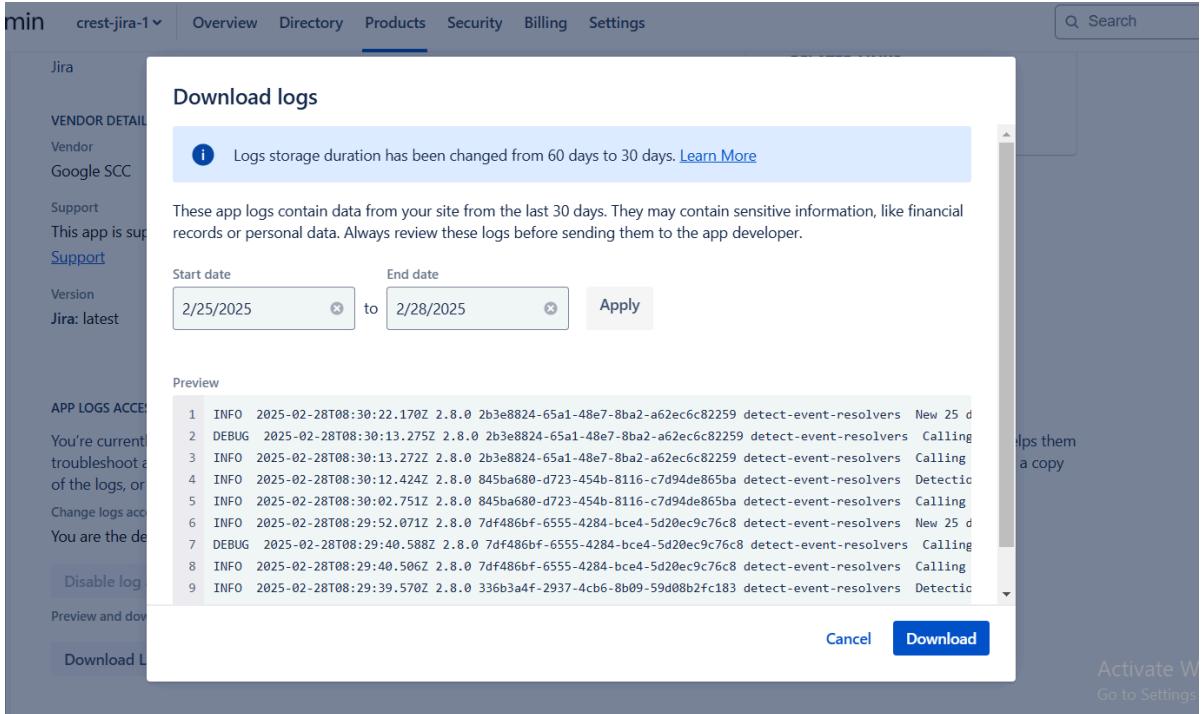
#### d. Navigate to “Connected Apps”.

The screenshot shows the Atlassian Admin interface with the 'Connected apps' section selected in the sidebar. The main area lists several installed apps, each with a 'View app details' link. The apps listed are: Atlassian Assist by Atlassian, Atlassian Home for Jira Cloud by Atlassian, Jira Cloud for Slack by Atlassian, Automation for Jira by Atlassian, Embedded Marketplace for Jira by Atlassian, Google SecOps for Jira Cloud by Atlassian, Jira Cloud for Microsoft Teams by Atlassian, Jira Cloud for Outlook by Atlassian, Jira Service Management Widget by Atlassian, and Jira Cloud for Spreadsheets by Atlassian.

#### e. Find Google SecOps for Jira Cloud from the installed apps list and click on the View app details.

The screenshot shows the 'View app details' page for Google SecOps for Jira Cloud. The page includes the app's name, provider (by Atlassian), plan (Admin), URL (https://crest-jira-1.atlassian.net), and a 'View app details' link. A red box highlights the 'View app details' link.

#### f. From the app details page, click on the Download Logs button present at the bottom which will open a dialog box. The user can apply the time interval and download the logs.



2. Manage users, groups, permissions, and roles in Jira Cloud
  - a. To manage users, groups, permissions, and roles in Jira Cloud review the following link and execute the steps  
<https://support.atlassian.com/jira-cloud-administration/docs/manage-users-groups-permissions-and-roles-in-jira-cloud/>
3. Unable to install/activate the app on Jira Cloud
  - a. If any issue is faced during installation/activation of the app on the Jira Cloud, review the following link and execute the steps.  
<https://confluence.atlassian.com/upm/installing-marketplace-apps-273875715.html>
4. Issue encountered in Jira Issue creation
  - a. If an error occurs during authentication, in the creation of issues based on the user's configured details, or in the creation of new issues after resetting/updating the configured fields, the user can check the error message and reset the data on the Configuration page. Make sure to reset cautiously, as it might result in duplication of issues.