Google SecOps App for Jira On-Prem v3.2.0

Release Documentation and User Guide

Contents

Release Notes

v3.1.0

- Added support for Curated Detections:
    - Fetch Curated detections and create Jira issues.
    - New issue type for Curated Detections with certain custom fields.
- Added support to fetch Detections via Streaming:
    - Users would have an option to fetch both Detections and Curated Detections via Streaming APIs.
- Added a Reset button on the configuration page, which would allow users to reset the configurations to default.
- Added functionality where the app checks and retries to do project customization for custom issue types, custom fields and schema mappings if they have been updated or do not exist when clicking on the save button.
- Various Minor Bug Fixes and Improvements.

v3.2.0

- Rebranding
    - Google Google SecOps 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.

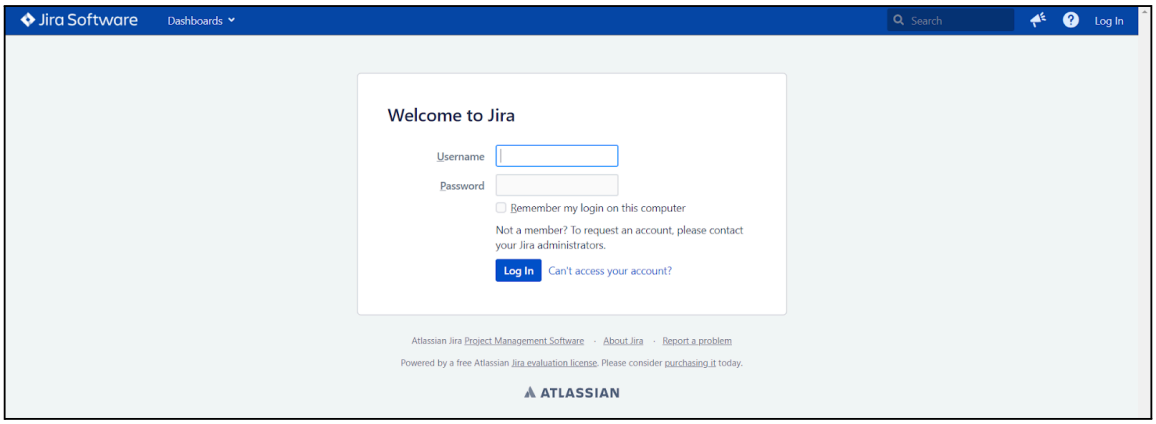
- Added support for Jira Server (Data Center) v10.

Installation Instructions

This section will cover the installation procedure of the Google SecOps App for Jira(On-Prem). For installation of the app, the Jira admin user will need the Google SecOps App(OBR/JAR) file.

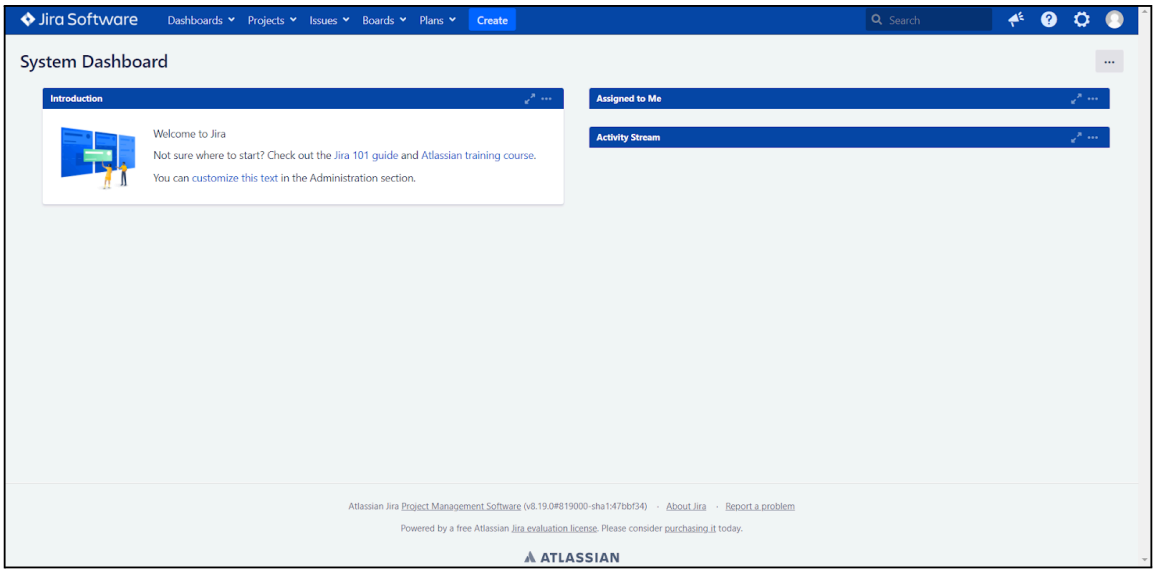
Login Page

Enter the Jira Admin credentials, to start the installation process for the Google SecOps App.



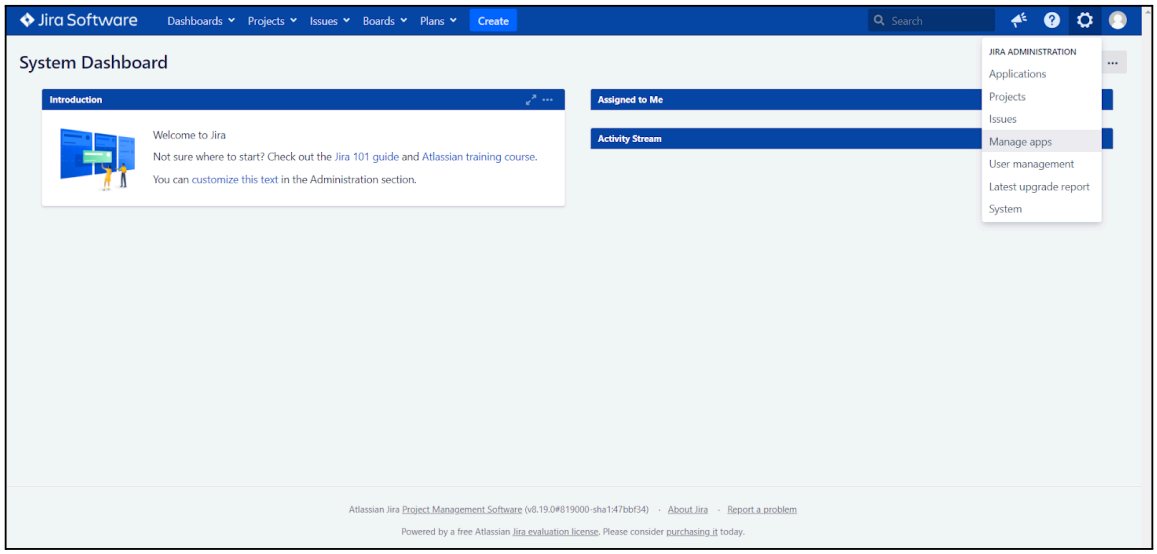
Landing Page

Upon Login with the admin credentials, the below-displayed landing page should be visible.



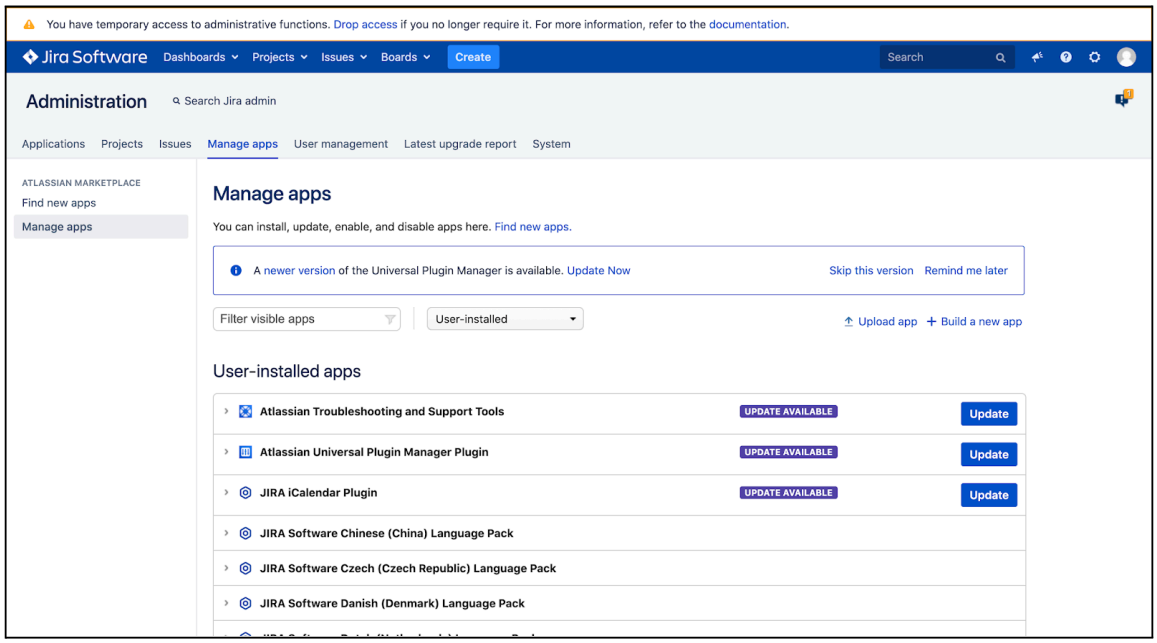
Goto Manage Apps

Click on the **Gear** Icon in the top right corner of the screen and click on the **Manage Apps** option.



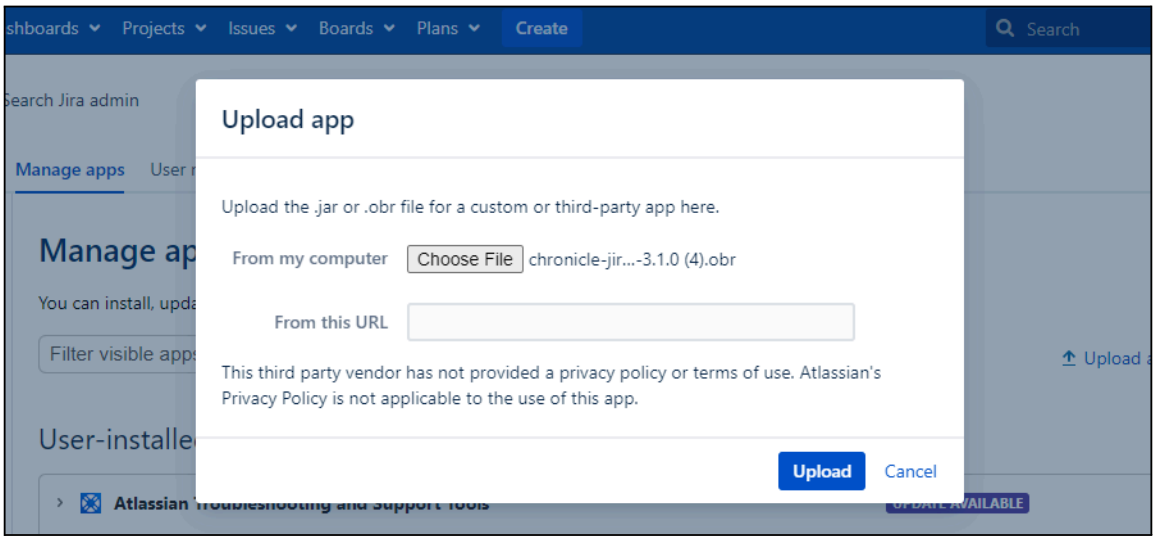
Manage Apps Page

Upon clicking on the **Manage Apps** option, the displayed page below will be visible listing all the apps that have been currently installed.



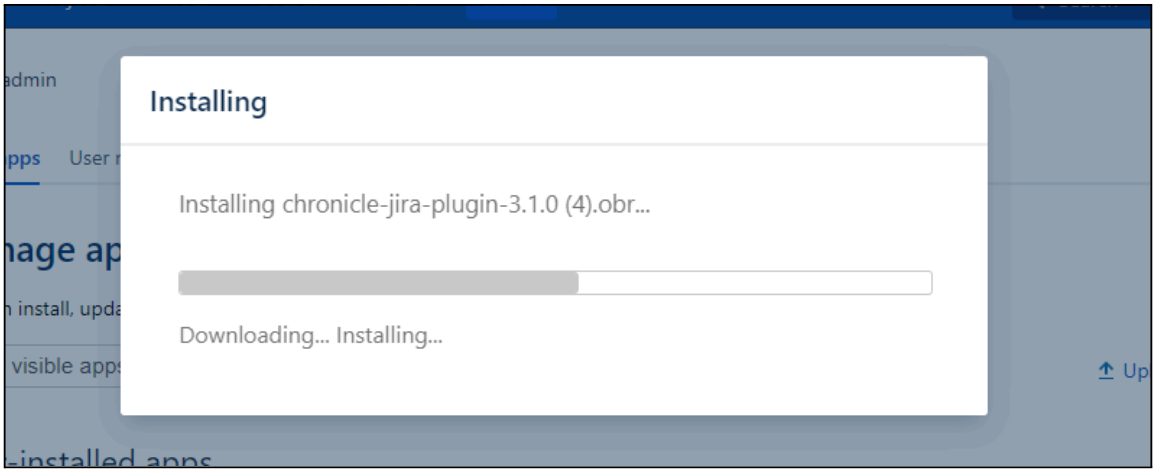
Upload App OBR/JAR file

Click on Upload all options from the previous screen, and a popup will appear as displayed below.



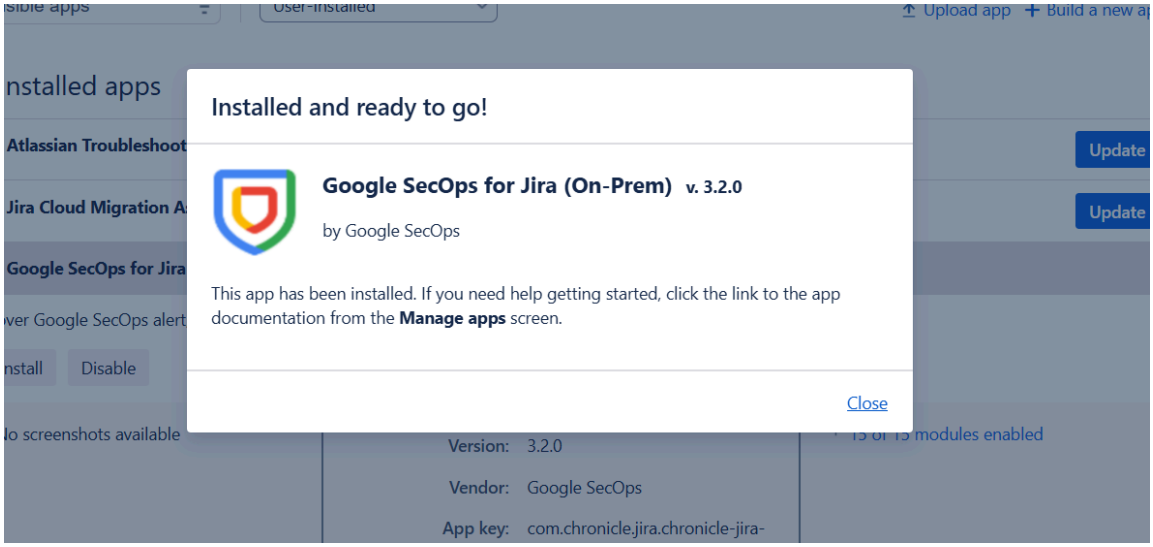
Google SecOps App Upload Process

Upon selection of the OBR/JAR file that will be provided by the customer to the end user, the below-displayed popup will appear showcasing the progress for the installation of the app.



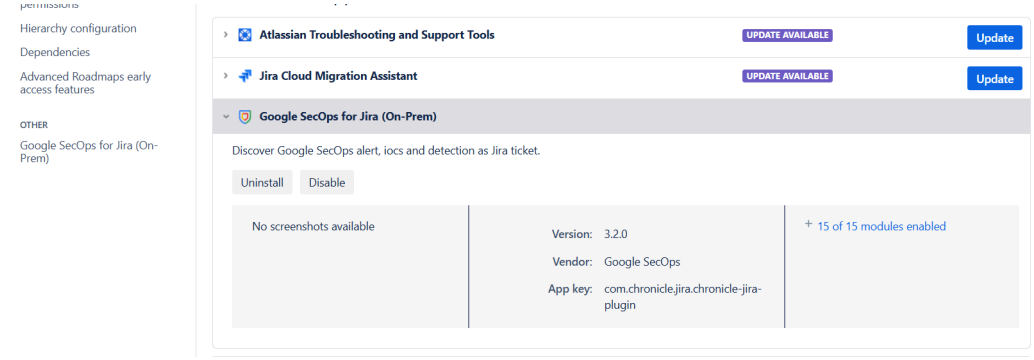
Google SecOps App Confirmation

Upon the successful installation of the Google SecOps app, the below-displayed popup will appear confirming the Installation was successful.



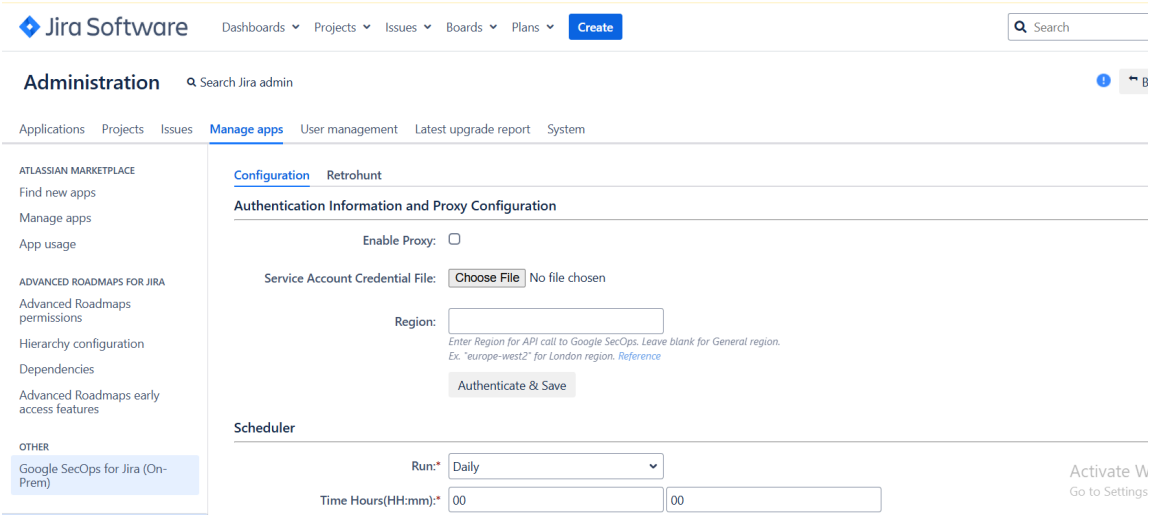
Listing of Google SecOps App

The Google SecOps app will be displayed in the list of apps installed, upon closing the popup from the previous screen.



Google SecOps App Config Page Confirmation

Once the installation process is completed, then the app with the name **Google SecOps App** will be displayed in the **Manage Apps** screen under the **OTHER** segment, which will present on the left side of the screen, as shown in the screenshot below.



This marks the successful completion of the Installation of the Google SecOps App for **Jira(on-prem)**. The same steps need to be followed for the different flavours of Jira(**Software** and **Service Desk**).

Installing the app from the marketplace

- Users will have a provision to install the application from the marketplace. Click on the **Gear** Icon on the top right corner of the screen, and click on the **Manage Apps** option.
- In the **Find New Apps** screen, enter the name of the app **Google SecOps for Jira (On-Prem)** in the Search the Marketplace search bar and click Enter.
- **Google SecOps for Jira (On-Prem)** will be available in the marketplace based on the search from where the user would be able to install the app.

Upgrade

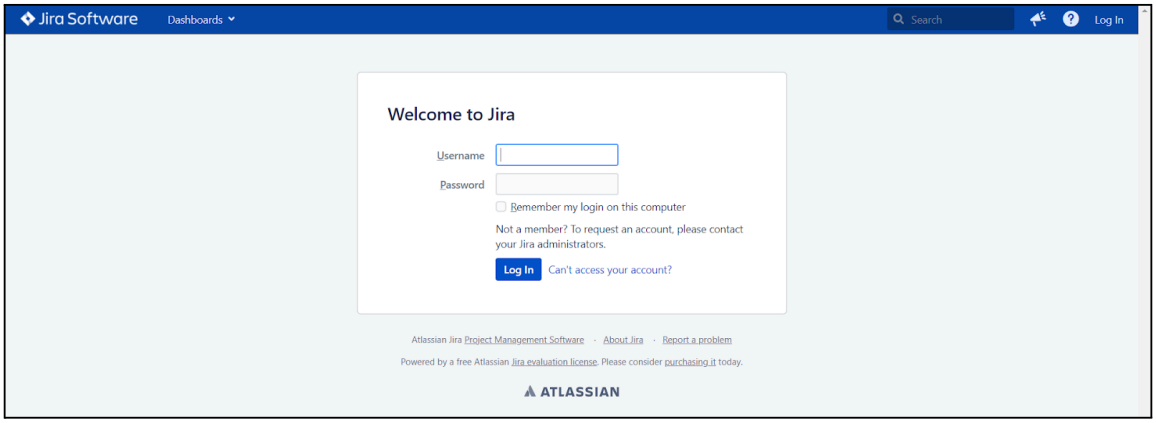
- If the user has already installed the previous version of the app and installed the new version/upgrades it to v3.2.0 from previous versions, they would not need to reconfigure the app.

Un-installation Instructions

Note: If you uninstall v3.2.0 of the app, existing schedulers will be deregistered and the saved app configurations will not be deleted from the Jira instance.

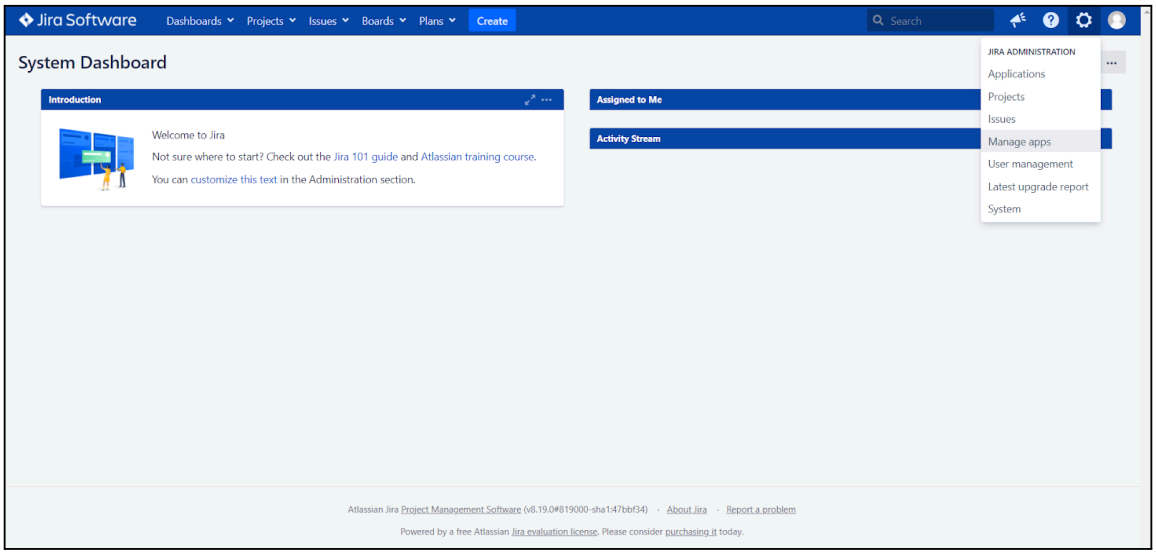
Login Page

Enter the Jira admin credentials and click on Log In



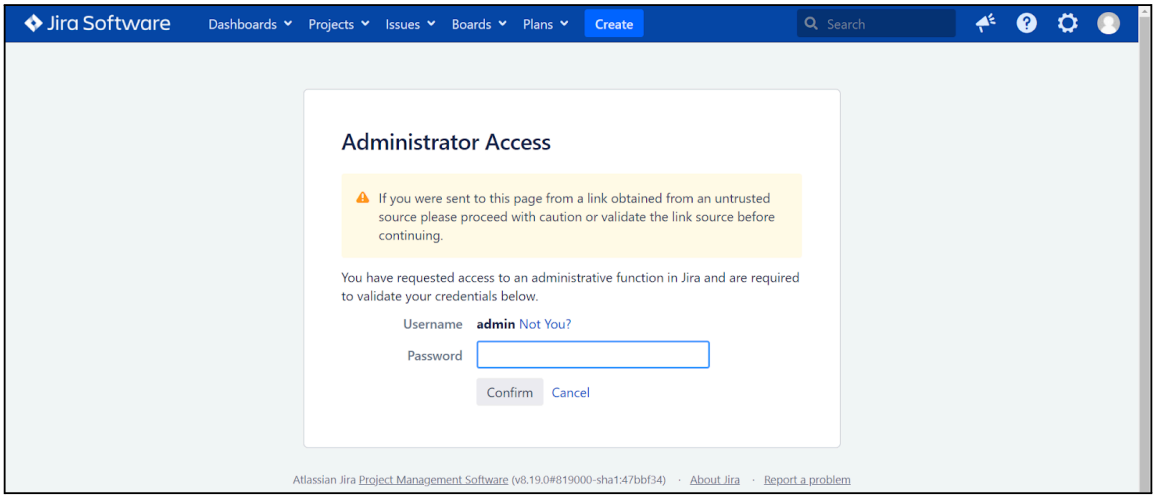
Goto Manage Apps

Click on the **Manage Apps** from the Settings gear that is located in the top right corner.



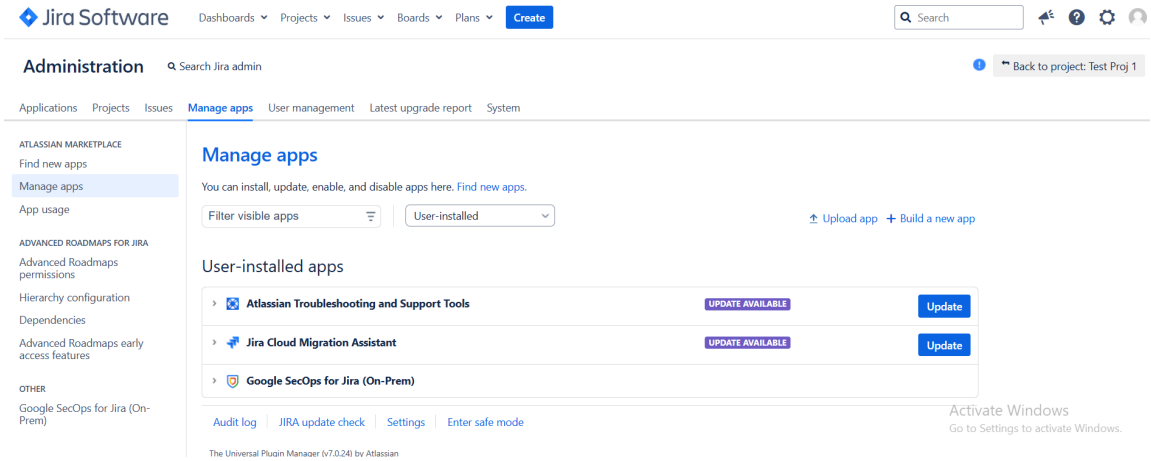
Password for the Administrator Access

Enter the Jira Administrator Access credentials and click on Confirm.



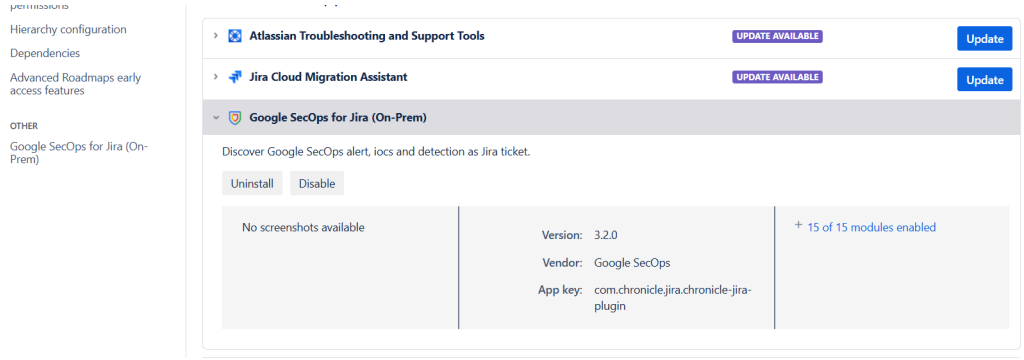
Manage Apps Page

Click on Manage Apps which is located on the left side under the ATLASSIAN MARKETPLACE section.



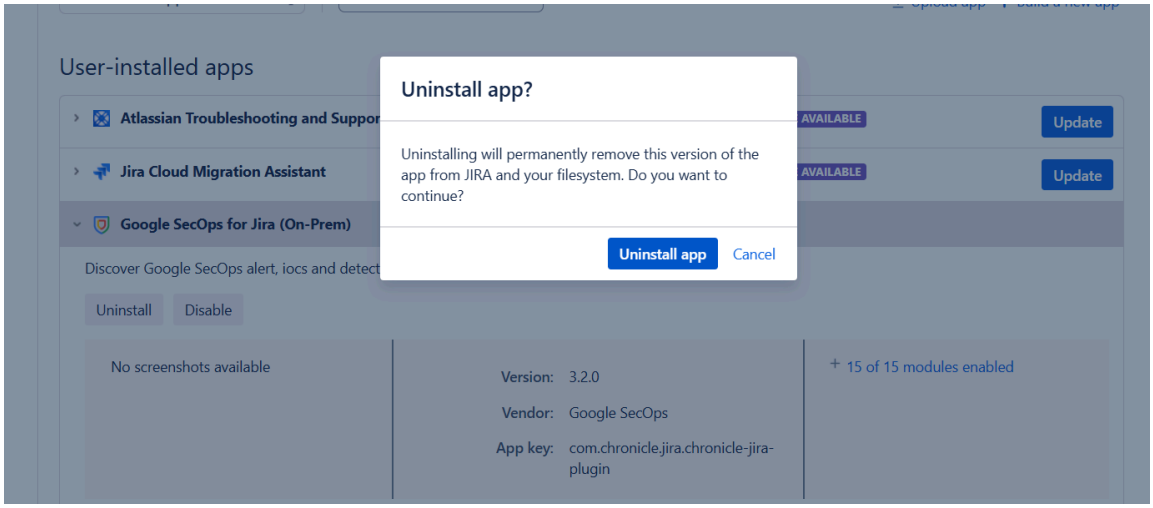
Search Google SecOps for Jira (On-Prem)

Search and Expand the Google SecOps for Jira (On-Prem) and click Uninstall.



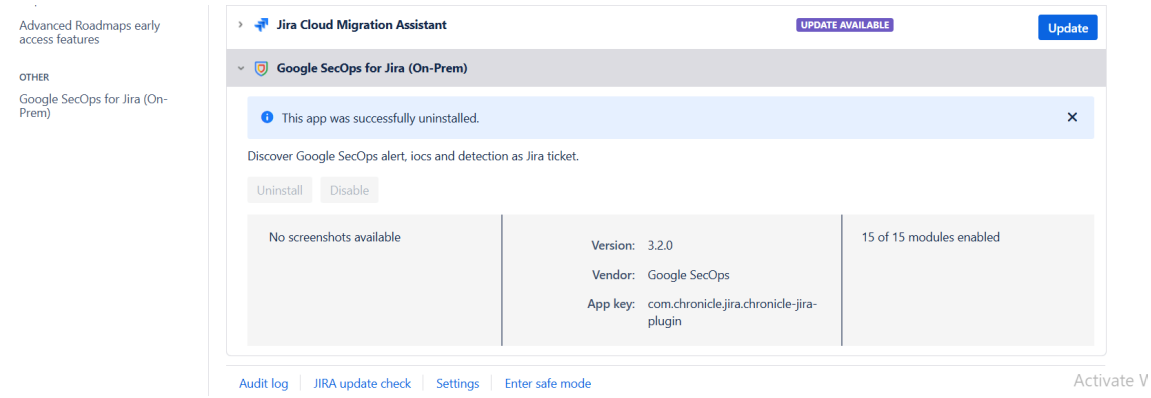
Uninstallation Confirmation

Click on the Uninstall app button to uninstall the Google SecOps Plugin.



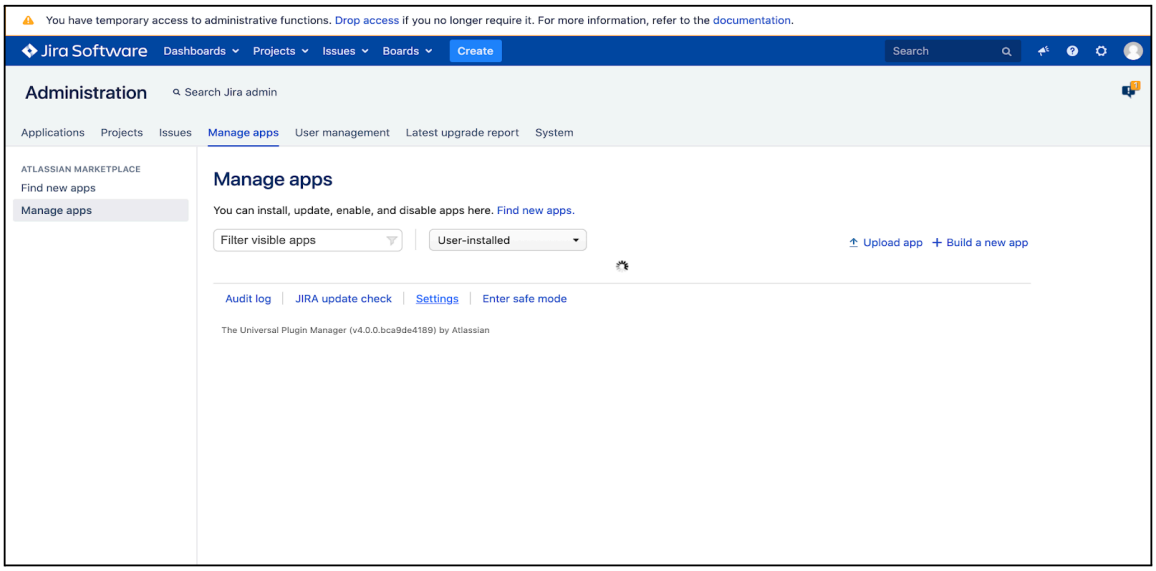
Uninstallation Successful

The below screenshot will be displayed upon successful uninstallation.



Confirm the Uninstallation

Click on Manage Apps and confirm that the Google SecOps App is no longer displayed in the list and also it is not listed in the left section of Atlassian Marketplace.



User Manual

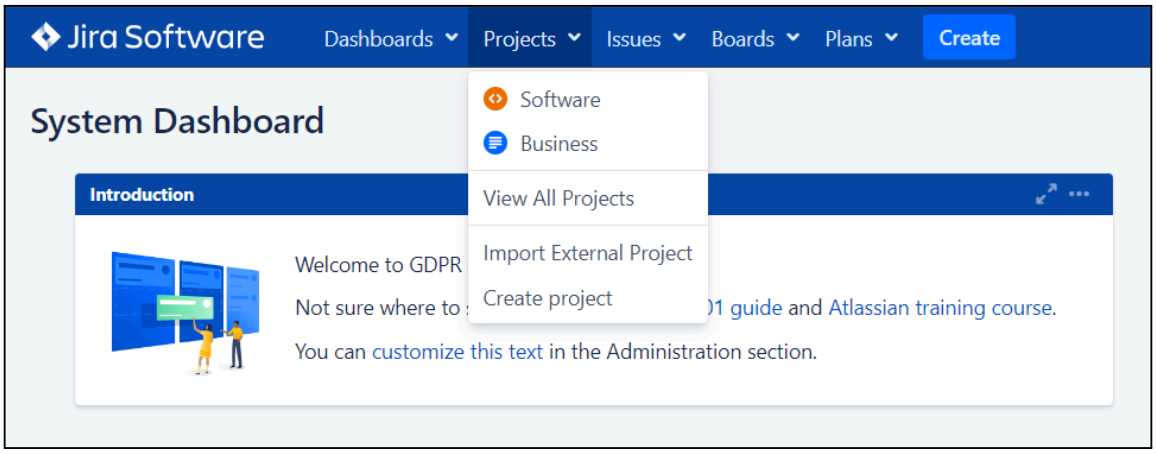
This section will cover the step-by-step process for configuring the Google SecOps App. The Google SecOps App offers the following functionality:

1. Types of scheduler settings, that enables users to select how frequently the data needs to be collected from the SecOps.
2. User Assignment Criteria, wherein the user can create the criteria based upon the filter condition, which scheduled job will assign the tickets directly to the user that has been mentioned in the criteria.
3. Ticket Creation Criteria, wherein the user can create the criteria based upon the filter condition, enabling the user to only create those tickets which match the criteria.
4. Detection Criteria, where the user can create criteria based on the filter condition, and a scheduled job will generate detection tickets as well as assign the tickets directly to the user that has been mentioned in the criteria.
5. Curated Detection Criteria, where the user can create criteria based on the filter condition, and a scheduled job will generate Curated Detection tickets as well as assign the tickets directly to the user that has been mentioned in the criteria.
6. Show the last job run date and time, which enables the user to understand when the last successful job was executed.
7. Custom Issue types, through which the tickets can be identified whether the tickets are of IoC, Alerts, Detections and Curated Detections.
8. Enrichment, 6 types of enrichment a user will be able to perform:
    a. IoC Matches
    b. List Assets Impacted
    c. List Events
    d. List Asset Aliases
    e. List User Aliases
    f. UDM Search
9. Update Rule State, wherein the user will be able to update the Detection Rule state associated with the Detection issue using the custom issue action “Update Detection Rule State”.
10. Retrohunt, wherein the users will be able to see a list of Retrohunts created earlier. Users will also be able to start/cancel the retrohunts.

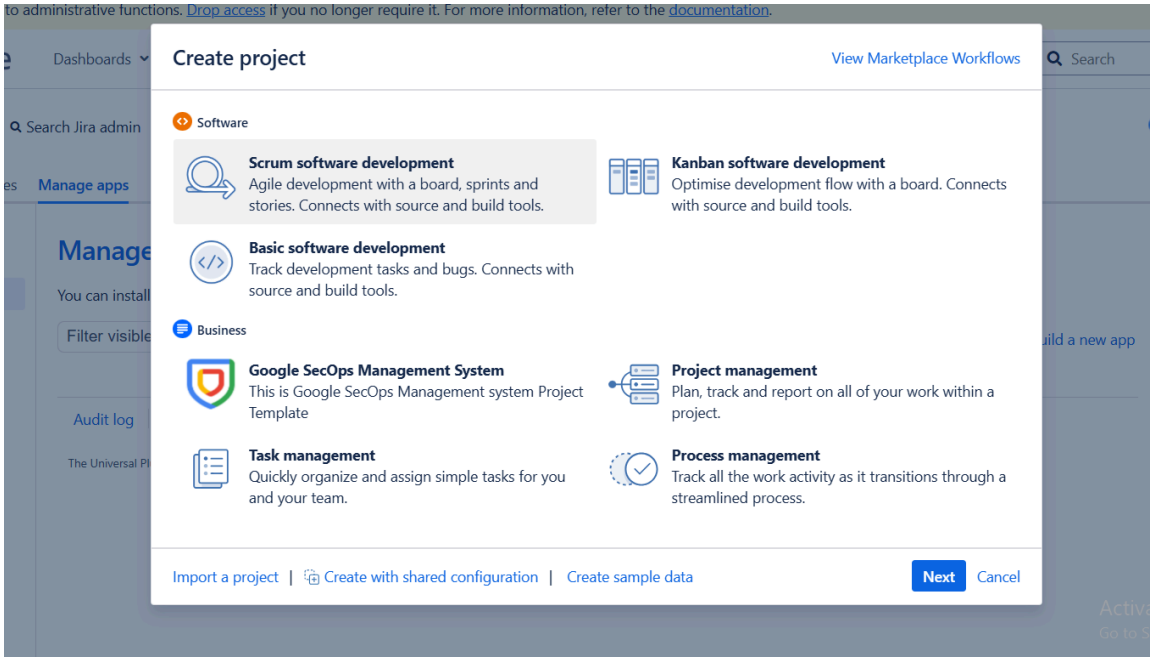
Project Creation from the Google SecOps Template

This section will go through the process of Project Creation with the Google SecOps template. It is important to do this, even before starting with the configuration of the app. As the Project that is created with the Google SecOps template will only be listed in the configuration screen, also this custom project will have all the custom fields, Issue types and labels that will be used when the ticket is created in order to map the response from Google SecOps to the jira fields

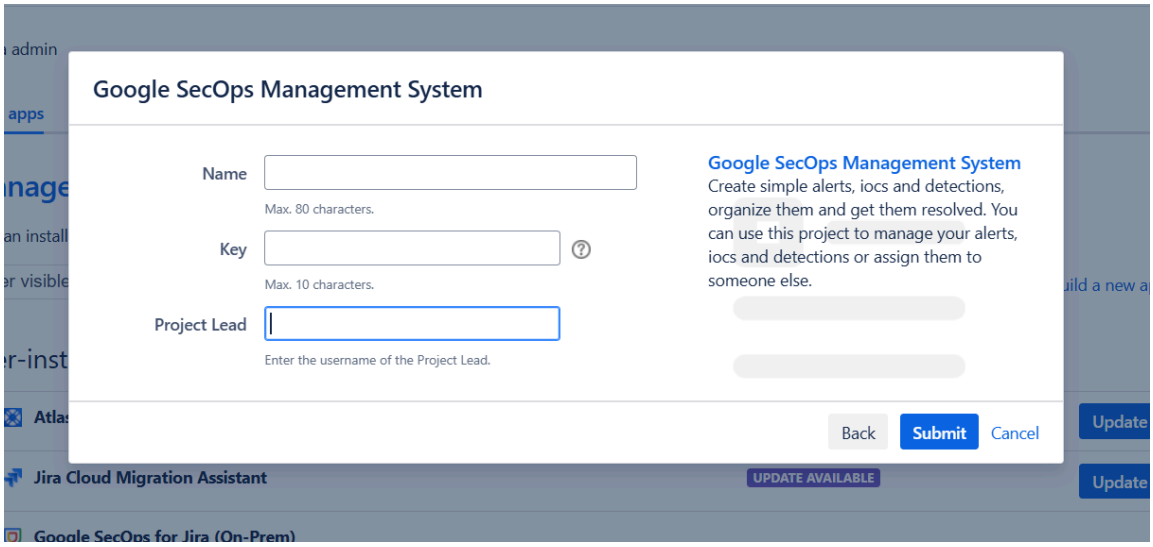
Hover / Click on the Projects section from the menu bar, and select Create Project as displayed below:



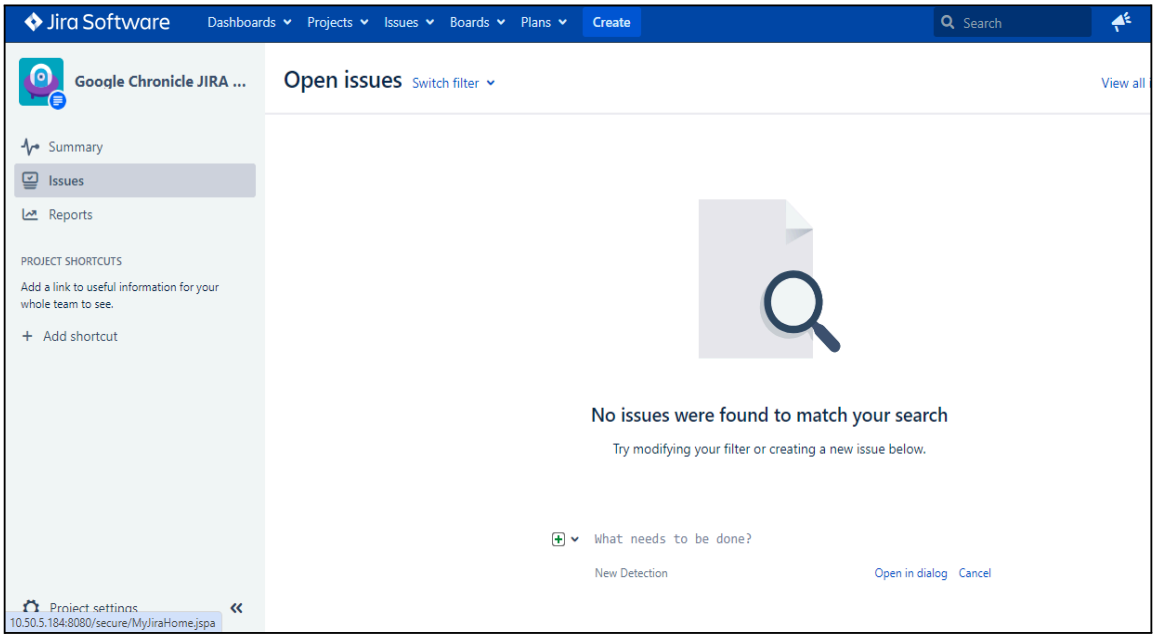
Select the **Google SecOps Management System** from the Create Project popup to create the custom Google SecOps project.



Fill in the Name, Key and Project Lead(will be used as the reporter of the ticket), and Click on the Submit button to create the project.



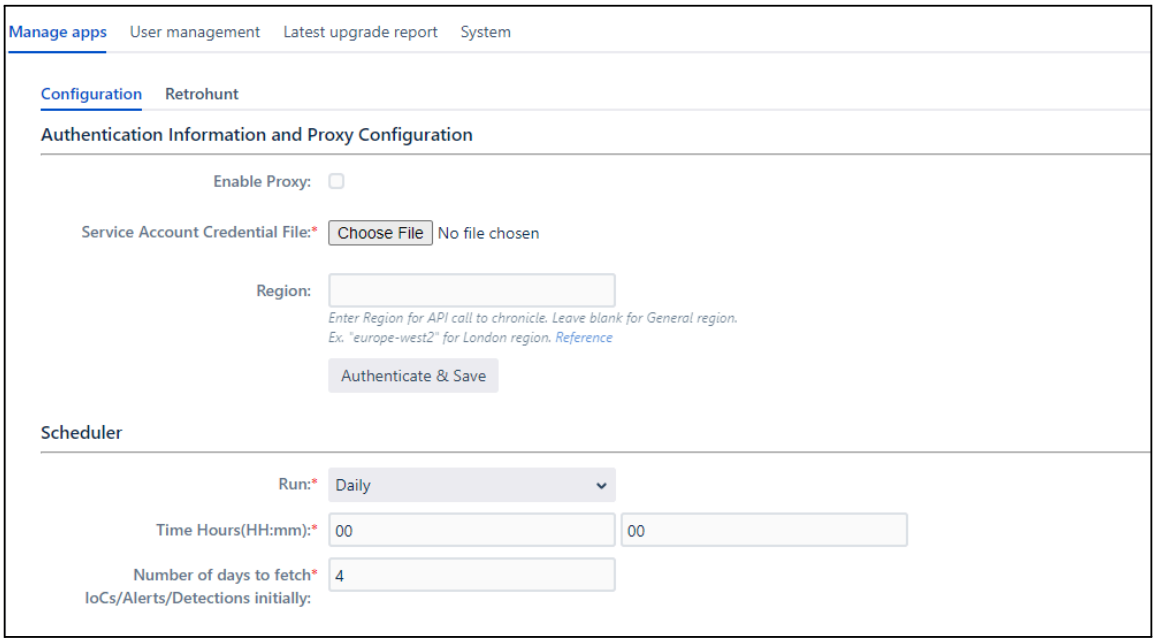
The below screen confirms that the custom Google SecOps Project has been created, and now the user is ready to configure the Google SecOps App.

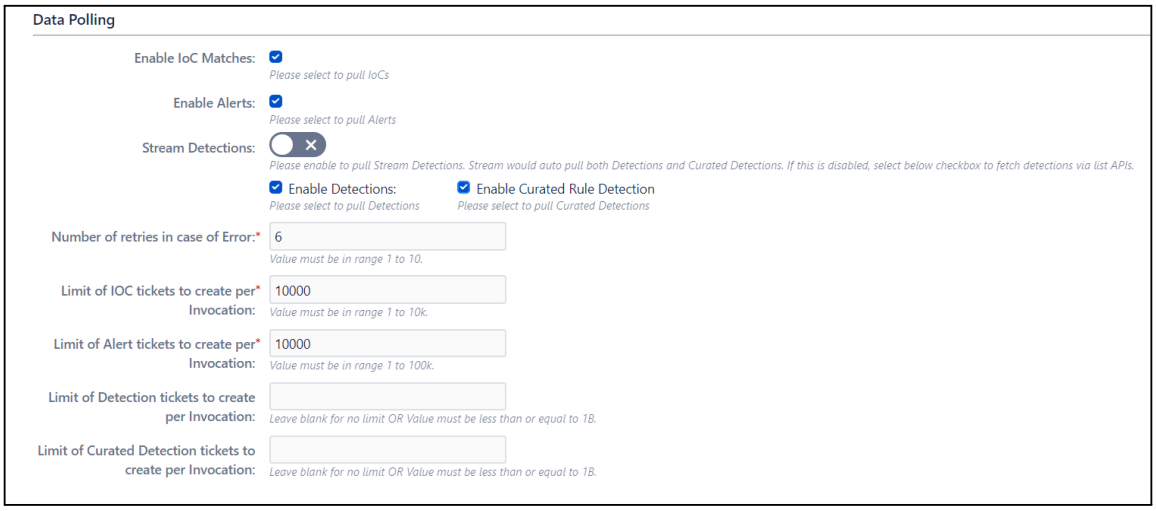


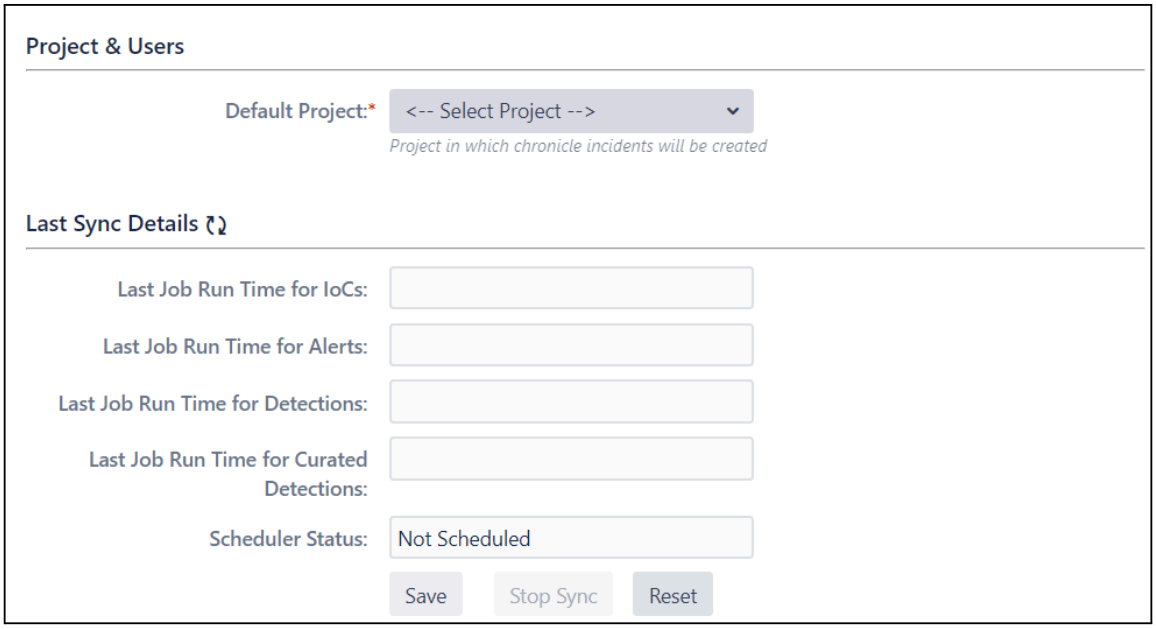
App Configuration

This section will cover the configuration of the Google SecOps App and its detailed usage.

App Configuration Page with Default Values and Fields usage







Below are the fields and their details:

Field Name	**Description**
Enable Proxy (Checkbox)	Upon checking, the proxy details will be visible to the user.
Proxy URL (Textbox)	URL of the proxy server.
Proxy Username (Textbox)	Username to access the proxy service.
Proxy Password (Textbox)	Password to authenticate the proxy service.
Service Account Credential File (File picker)	Service Account file provided by Google for Authorisation of API.
Region (Textbox)	Region to which the Google SecOps account belongs.
Run (Dropdown)	How often does the app need to fetch the data from the Google SecOps Instance? The total options that we get are Daily, Weekly, Monthly and Periodically.
Time Hours(HH:mm) (HH field picker) (mm field picker)	At what Time of the day the Google SecOps app should fetch the data from the Google SecOps instance. Time can be configured in Hours and Minutes. This field will only be visible for Daily, Weekly and Monthly.

Day (Dropdown for Weekly) (Day field picker for Monthly)	For the Weekly Run option, the Day dropdown list will have the day of the week value from Sunday to Saturday. Users can configure any day of the week as per their preference. For the Monthly Run option, the Day picker will have the day of the month values from 1 to 31. Users can configure any day of the month as per their preference.
Run Interval (Minutes field picker)	At what interval of time(in minutes) does the data from the Google SecOps app need to be fetched from the Google SecOps instance.
No of days to fetch IoCs/Alerts/Detections Initially (Day field picker)	Historical data that we need to fetch in days, the value entered in this field will fetch the data for those many days to the current date.
Default Project (Dropdown)	It will display the list of the projects that were created by the Google SecOps Project Creation Template.
Enable IoC Matches (Checkbox)	Upon checking, the app will create the Tickets for IoC Matches.
Enable Alerts (Checkbox)	Upon checking, the app will create the Tickets for User and Asset Alerts.
Stream Detections (Toggle Button)	Enable this toggle button to receive detections continuously. Once enabled, the checkbox for detection and curated detection would get disabled as they would be auto-pulled.
Enable Detections (Checkbox)	Upon checking, the app will create the Tickets for Detection. This checkbox will be deactivated if Stream Detections is enabled.
Enable Curated Detections(Checkbox)	Upon checking, the app will create the Tickets for Curated Detections. This checkbox will be deactivated if Stream Detections is enabled.
The number of retries in case of Error (Number)	How many times should the app retry Google SecOps API call in case of a rate limit error
Limit of IOC tickets to create per Invocation (Number)	How many IOC tickets to create per sync interval
Limit of Alert tickets to create per Invocation (Number)	How many Alert tickets to create per sync interval

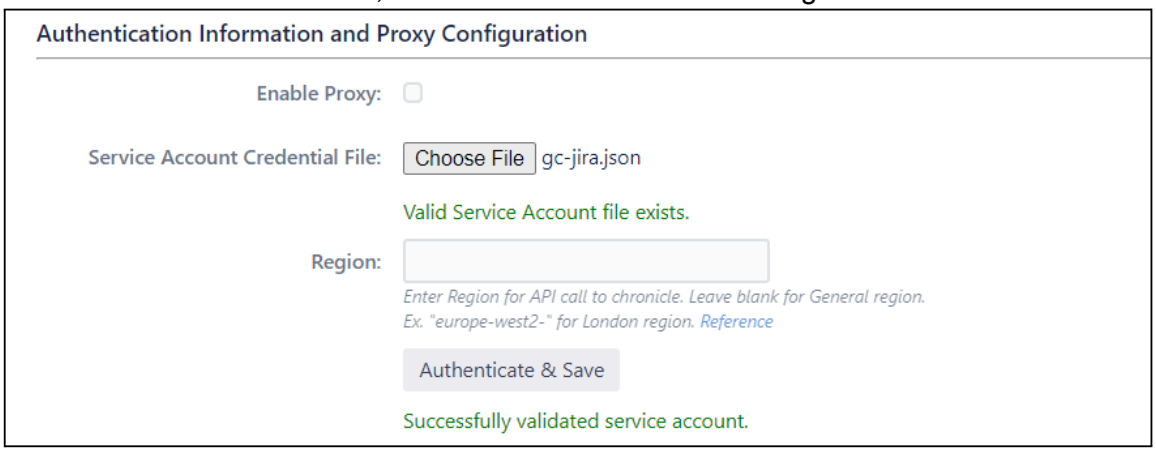
Limit of Detection tickets to create per Invocation (Number)	How many Detection tickets to create per sync interval (This configuration is not applicable for stream detections.)
Limit of Curated Detection tickets to create per Invocation (Number)	How many Curated Detection tickets to create per sync interval (This configuration is not applicable for stream detections.)
Last Job Run Time for IoCs (Read-only text box)	Last successful job run time for fetching the IoCs from the Google SecOps instance.
Last Job Run Time for Alerts (Read-only text box)	Last successful job run time for fetching the Alerts from the Google SecOps instance.
Last Job Run Time for Detections (Read-only text box)	Last successful job run time for fetching the Detections from the Google SecOps instance.
Last Job Run Time for Curated Detections (Read-only text box)	Last successful job run time for fetching the Curated Detections from the Google SecOps instance.
Scheduler Status (Read-only text box)	This field displays the Status of the Job: ● Scheduled: This means the Job is currently scheduled and it will run based on the configuration saved ● Not Scheduled: This means the Job is currently not scheduled and no API calls will be made to SecOps
Next Job Run Time (Read-only text box)	When will the next call be made to SecOps? Note that this status is not applicable for stream detections.
Save (Button)	Save the configuration and Sync will be initiated, with the confirmation box.
Stop Sync (Button)	Stop pulling the data from the SecOps.
Reset (Button)	Reset the configuration to default and stop the existing sync, with the confirmation box.
Start Retrohunt (Button)	Open dialogue box to take user inputs to start retrohunt
Rule ID or Version ID (Textbox)	Rule ID or Version ID for which Retrohunt needs to be started.
Start DateTime (Datetime picker)	Start time for the time range of retrohunt
End DateTime (Datetime picker)	The end time for the time range of retrohunt

Refresh List (Button)	Refresh the list of retrohunts in the table
Cancel (Button)	Cancel the particular “RUNNING” retrohunt

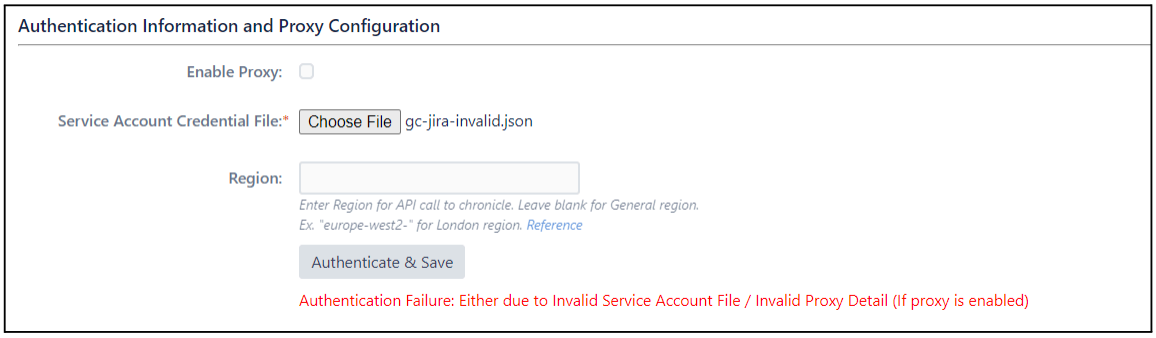
Authentication Information and Proxy Configuration

Users need to upload the valid Service Account file that will be provided by the Google Google SecOps team for the Authentication of the Google SecOps API and provide the region to which the Google SecOps account belongs.
Once the “Authenticate & Save” button is clicked, it validates the provided service account file and region.

- On successful authentication, it would show a success message.

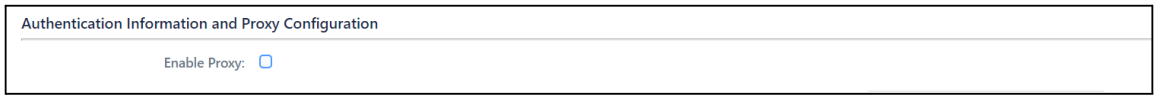


- On failure, it would show the appropriate failure message.



Proxy Details: Default

- An optional provision will be available to configure the proxy server details in case the user wants the Google SecOps API requests used for ticket creation, enrichment and detection to be routed via a proxy server
- There will be an Enable Proxy checkbox in the ‘Authentication Information and Proxy Configuration’ section. By default, it will be unchecked.

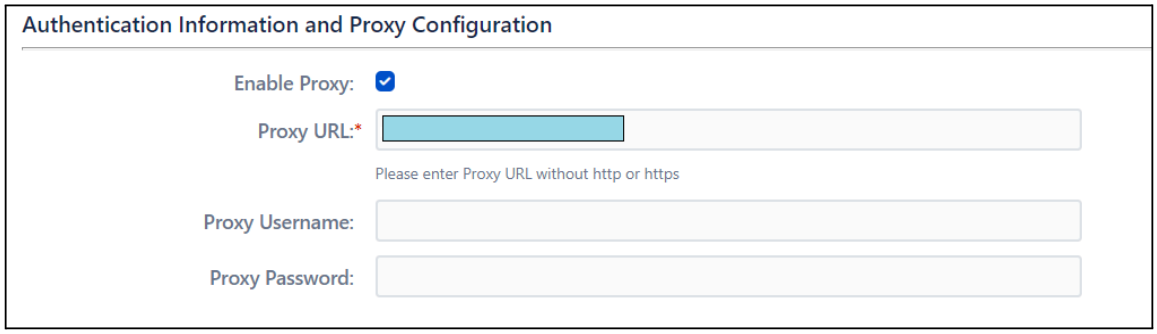


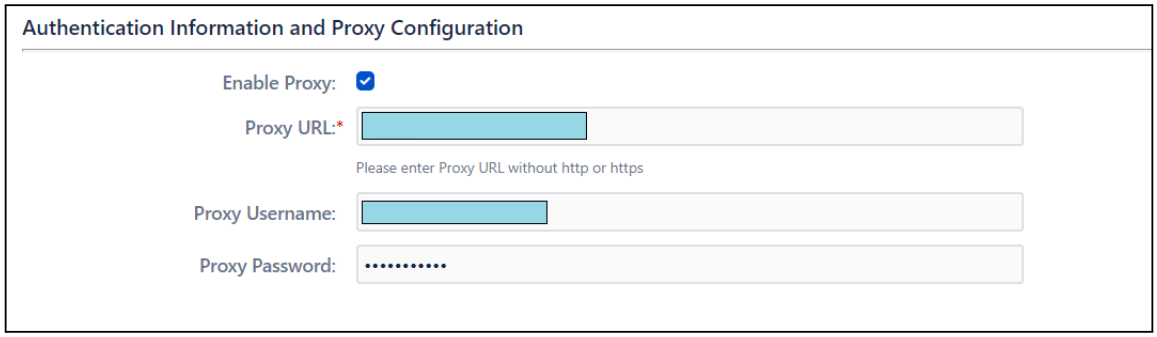
Proxy Details: When the checkbox is checked

If the checkbox is checked, the user will have the provision to configure the details of the proxy server like Proxy URL, Proxy Username and Proxy Password in case the user wants the Google SecOps API requests to be routed via a proxy server.
Note: Please ensure that the proxy URL should be entered as <Hostname/IP-Address>:<Port>. The hostname/IP address where the proxy server is installed and the port at which the proxy server is listening.

Proxy Details: Proxy configuration

Users can configure the proxy server details with proxy credentials and without proxy credentials. However, in both cases the proxy URL value is mandatory.





Scheduler Daily

Upon configuration, the job will run daily on the time(Hours: Minutes) defined by the user

Scheduler Weekly

Upon configuration, the job will be scheduled on the selected day of the week and the time(Hours: Minutes) defined by the user

Scheduler Monthly

Upon configuration, the job will be scheduled on the selected date of the month and the time(Hours: Minutes) defined by the user

Scheduler Periodically

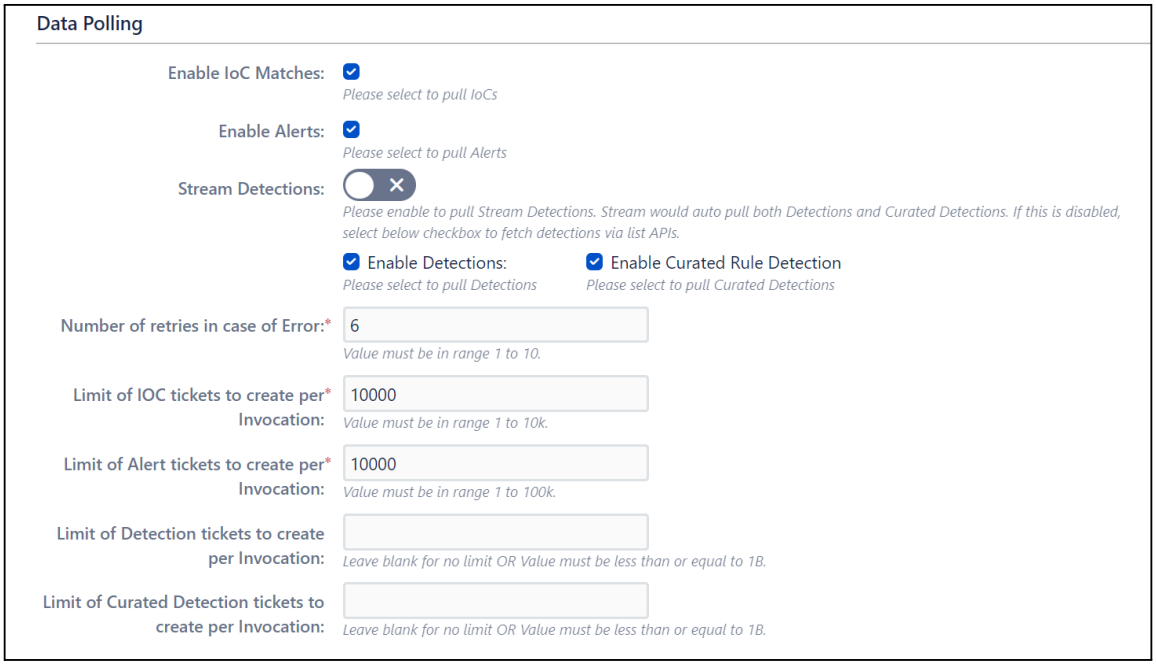
Upon configuration, the job will be scheduled periodically based on the Run Interval(Minutes) defined by the user

Note: In the case of Stream Detections the data is continuous, it will continually collect the detections from the Google SecOps and create JIRA tickets in the Google SecOps without relying on the scheduler configuration.

Data Polling: Default

- Enable Ioc Matches, upon checking it will create the IoC tickets in the selected project.
- Enable Alerts, upon checking it will create the User Alerts and Asset Alerts tickets into the selected project.

- Stream Detections: To receive continuous detection alerts and create JIRA tickets in the selected project, please enable the 'Stream Detections' toggle button. This will activate the 'Stream Detection' feature, which provides both 'Detection' and 'Curated Detections' types of detection alerts. As a result, the 'Enable Detections' and 'Enable Curated Detections' checkboxes will be deactivated, as the 'Stream Detection' option covers both types of detections. Therefore, there is no need to select individual detection options.
    - Enable Detections, upon checking will create the Detection tickets for the selected project.
    - Enable Curated Detections, upon checking will create the Curated Detection tickets into the selected project.
- Provide the value of the field “Number of retries in case of Error” to restrict the maximum retries the app should do in case of Rate Limit error from Google SecOps API. The user can provide a maximum value of 10.
- Provide the value of the field “Limit of IOC tickets to create per Invocation” to restrict the maximum number of IOC tickets the app should create per sync interval. The user can provide a maximum value of 10k(10000).
- Provide the value of the field “Limit of Alert tickets to create per Invocation” to restrict the maximum number of Alert tickets the app should create per sync interval. The user can provide a maximum value of 100k(100000).
- Provide the value of the field “Limit of Detection tickets to create per Invocation” to restrict the maximum number of Detection tickets the app should create per sync interval. Leave this field blank for no limit in detection ticket creation or if the user wants to create a particular number of tickets for Detection criteria then the value must be less than or equal to 1B(1000000000). This configuration is not applicable for stream detections as it provides continuous data.
- Provide the value of the field “Limit of Curated Detection tickets to create per Invocation” to restrict the maximum number of Curated Detection tickets the app should create per sync interval. Leave this field blank for no limit in curated detection ticket creation or if the user wants to create a particular number of tickets for Curated Detection criteria then the value must be less than or equal to 1B(1000000000). This configuration is not applicable for stream detections as it provides continuous data.

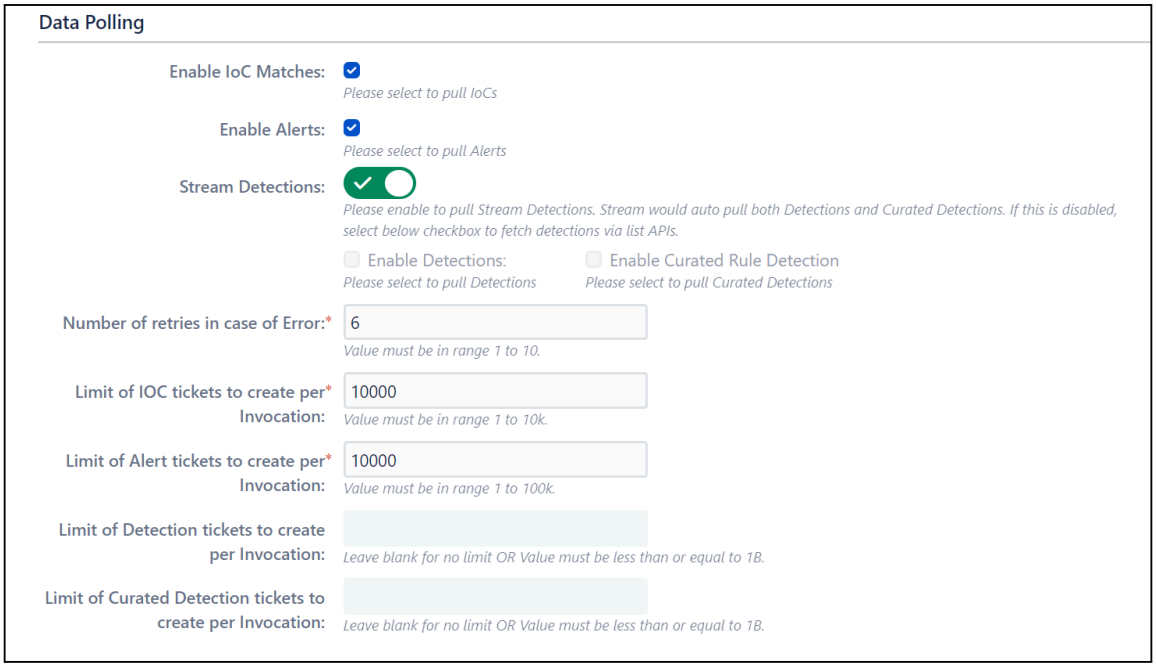


Data Polling: Stream Detections

The Stream Detections provides real-time access to detections generated by both User-defined Rules and Google Security Operations Rules. For each detection fetched from the API, JIRA tickets are created with detection details.

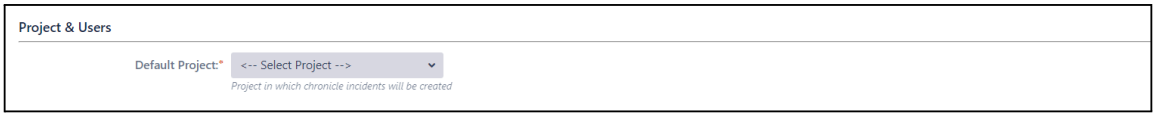
- A single toggle button labelled "Stream Detections" is provided to enable continuous detections.
- Once the "Stream Detections" toggle is enabled, the "Enable Detections" and "Enable Curated Detections" checkboxes will be deactivated because "Stream Detections" provides both types of detections: "Detections" and "Curated Detections", rendering the individual checkboxes is redundant.
- The "Number of days to fetch IoCs/Alerts/Detections initially" determines the continuation time parameter for API calls. However, if the user inputs a value exceeding the last 7 days, the app will automatically set the continuation time to 7 days from the current time.
- The "Limit of Detection tickets to create per Invocation" and "Limit of Curated Detection tickets to create per Invocation" field inputs are deactivated for Stream Detections, as it operates as a continuous stream connection.
- Based on the provided configuration create HTTP stream connection.
- Once the connection is established according to the configured data, it continuously receives Detection Engine results over an HTTP stream as the detections are discovered.
- All the detections created by rules whose alerting status was enabled at the time of detection should parse data according to the JIRA ticket.

- Upon successful parsing of data, the app will generate a JIRA ticket for each detection. These tickets will be created with the "Detection" or "Curated Detection" Issue Type.



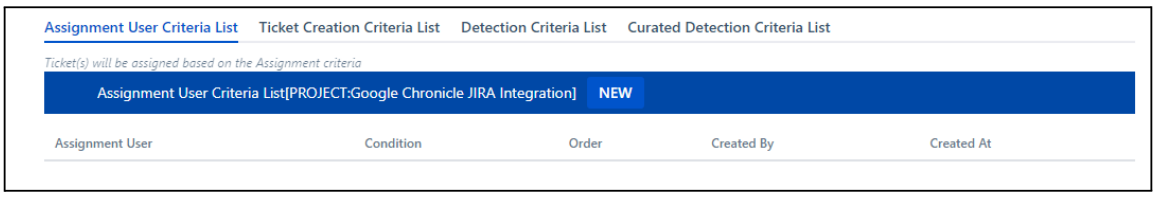
Project & Users: Default

Users can select the project from the drop-down menu and can select a particular project under which the tickets will be created. Only those projects will be listed which are created from the Google SecOps Project creation template.



Project & Users: When the project is selected

Once the project is selected then the User Assignment, Ticket Creation Criteria section, Detection Criteria and Curated Detection CriteriaList section will be displayed.

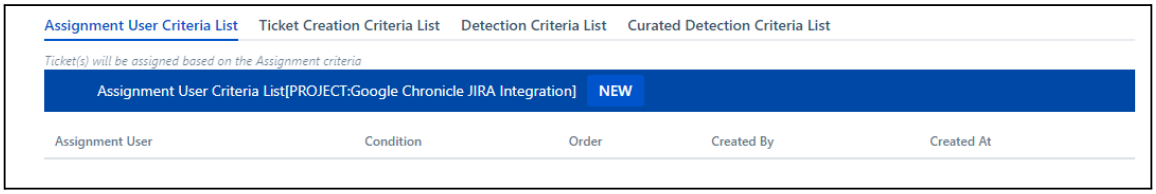


User Assignment Criteria

Over here the criteria can be defined with the filter condition, which will enable the app to directly assign the tickets which will be created by the scheduler to the user as defined in the criteria.

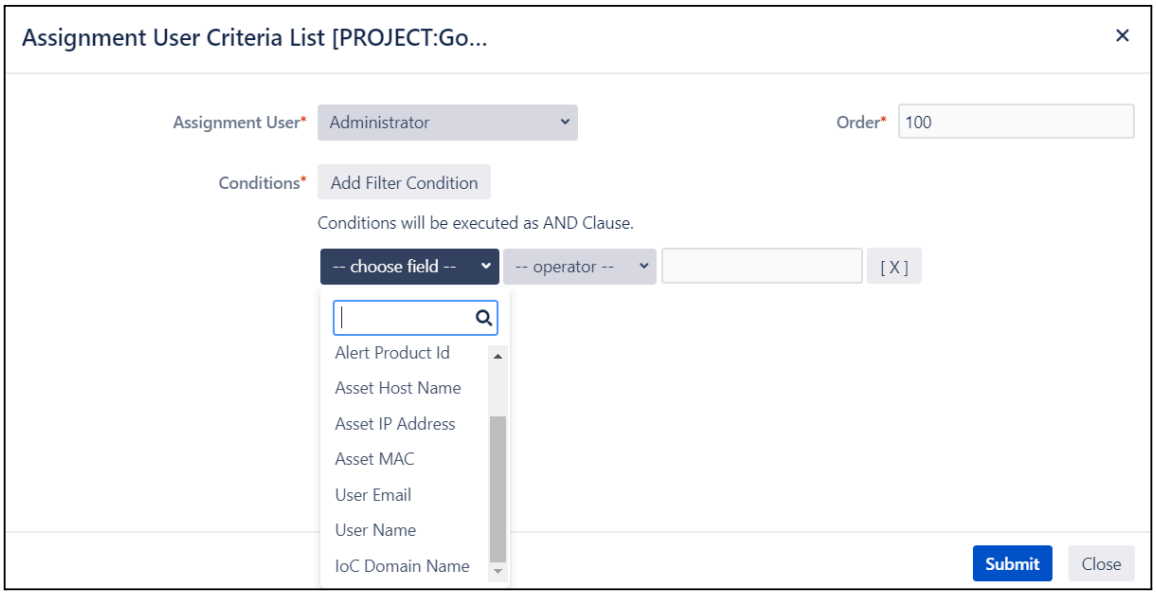
Following are the steps by which a user can create the criteria:

- Click on the **NEW** Button in the Assignment User Criteria List tab



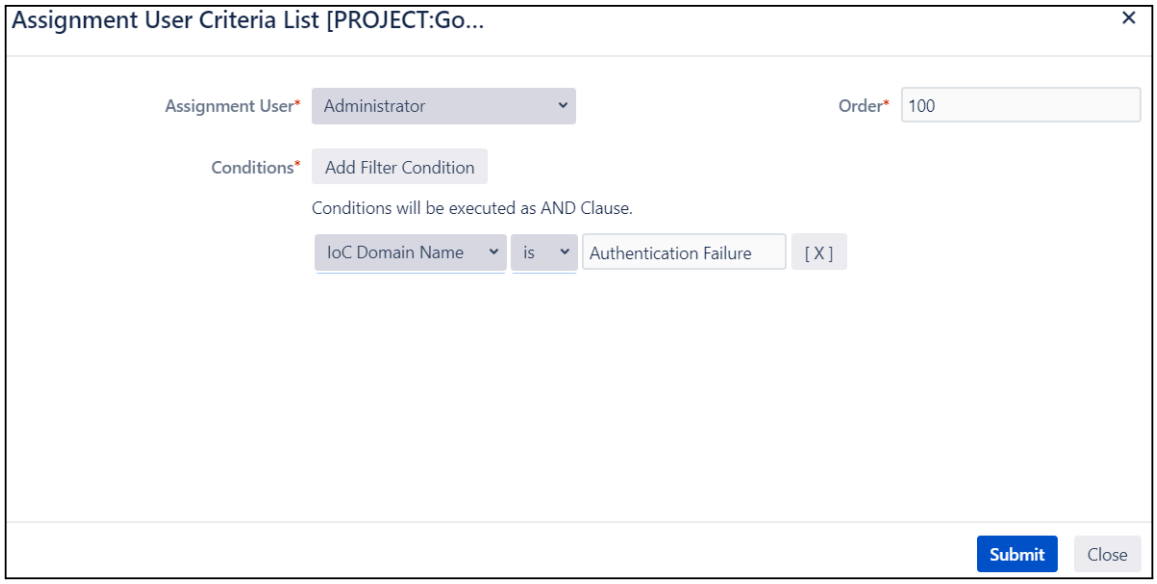
User Assignment Criteria: Creation

- Assignment User needs to be part of either of the mentioned User Groups depending upon the Jira(on-prem) flavour installed, along with the permission for the Google SecOps project that is created via the Google SecOps template.
    - Jira-administrators
    - Jira-software-users
    - Jira-service desk-users
- The assignment User Criteria List window will appear where the user will have the provision to configure the assignment user criteria for the tickets to be assigned to a specific user
- Tickets will be assigned to the selected user from the Assignment User dropdown list, by the scheduled job.
- Click on Add Filter Condition, and a criteria section will appear which will have the below criteria for configuration.

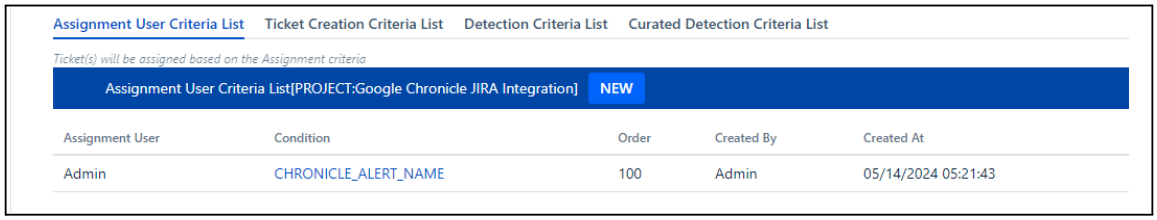


- Prepare the filter condition as desired and then click on the Submit button to save the criteria.

Field Name	**Description**
Assignment User	List of users that are part of the User Groups
Add Filter Condition	Add the new filter condition, and all the filter conditions that the user defines, will work in conjunction with each other
Choose Field	Select the field on which the tickets need to be assigned to the user
Operator	Which condition the user wants to apply to filter out the data
Values	Enter the value that will satisfy the condition criteria
Order	The priority of the criteria, that will be used to filter the response in order to assign the tickets to the user. Lowest to Highest, where lowest will be preferred



- Once the assignment user criteria are saved, it will be displayed in the config screen as a list view as shown below:



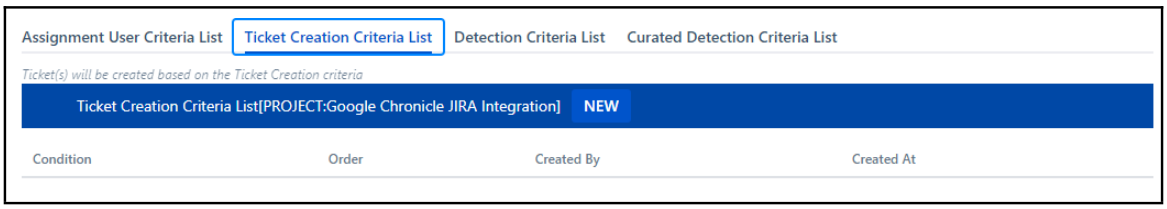
- So, as per this configuration, the user alert or asset alert tickets will have the alert name “Authentication Failure” assigned to the admin user.

Ticket Creation Criteria

Over here the criteria can be defined with the filter condition, which will enable the app to create only those tickets that satisfy the ticket creation criteria as defined by the user.

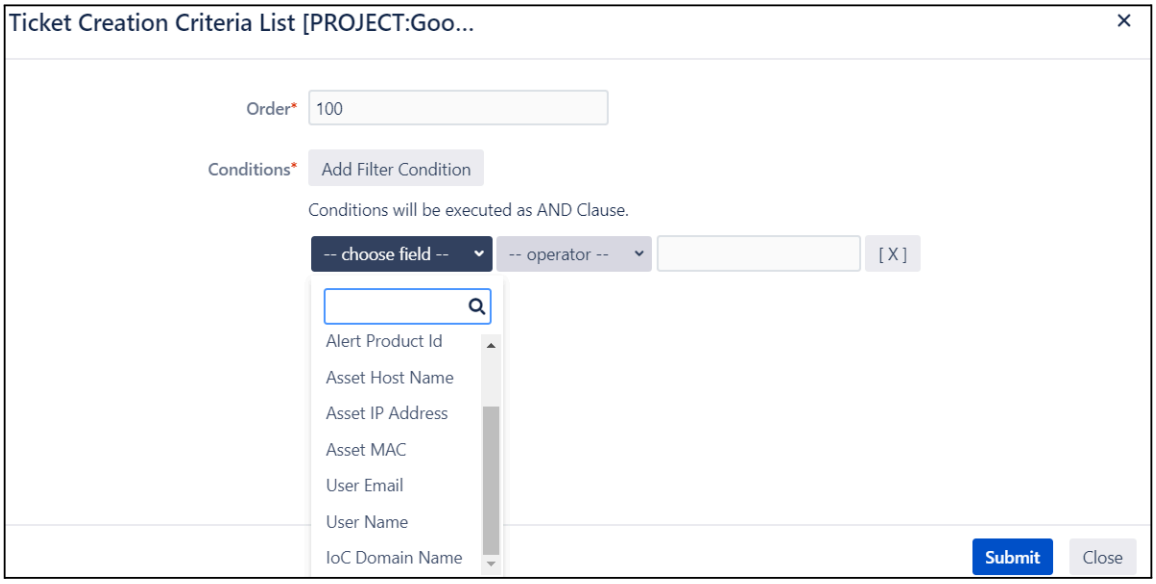
Following are the steps by which a user can create the criteria:

- Click on the **New** button in the Ticket Creation Criteria List tab



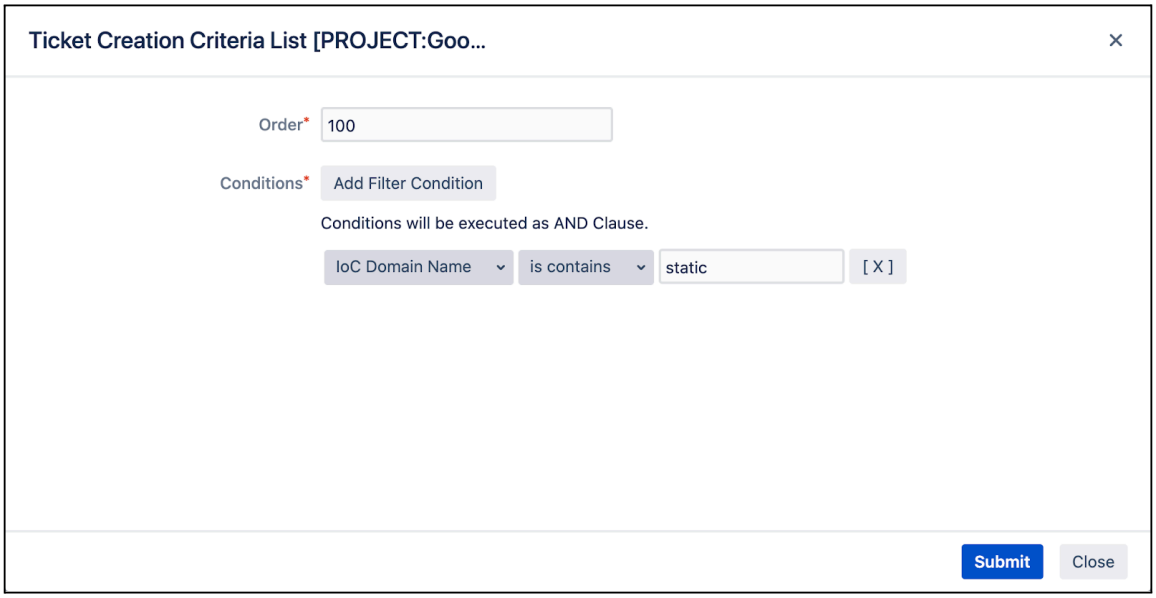
Ticket Creation Criteria: Creation

- Ticket Creation Criteria List window will appear where the user will have the provision to configure the ticket creation criteria in case any specific tickets need to be created in the selected project.
- Click on Add Filter condition, and a criteria section will appear which will have the below criteria for configuration.

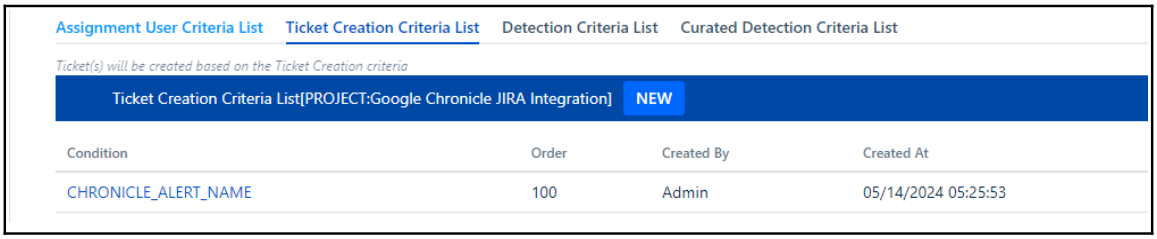


- Prepare the filter condition as desired and then click on the Submit button to save the criteria.

Field Name	**Description**
Add Filter Condition	Add the new filter condition and all the filter conditions that the user defines, all will work in conjunction with each other
Choose Field	Select the field on which the tickets need to be assigned to the user
Operator	Which condition the user wants to apply to filter out the data
Values	Enter the value that will satisfy the condition criteria
Order	The priority of the criteria, that will be used to filter the response in order to assign the tickets to the user. Lowest to Highest, where lowest will be preferred



- Once the ticket creation criteria are saved, it will be displayed in the config screen as a list view as shown below:



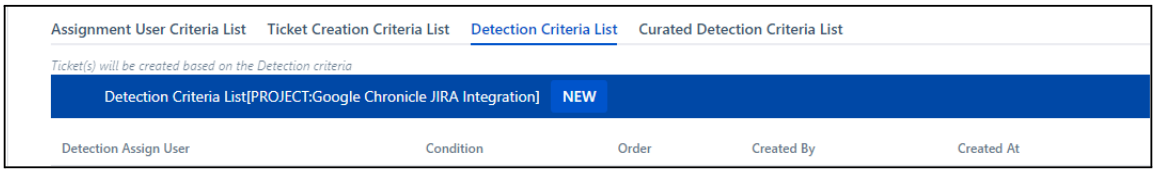
- So, as per this configuration, tickets will be created for IoC Domain matches which contain the phrase “static” in the domain name.

Detection Criteria List

Over here the criteria can be defined with the filter condition, which will enable the app to create only those tickets that satisfy the detection criteria list as defined by the user.

Following are the steps by which a user can create the criteria:

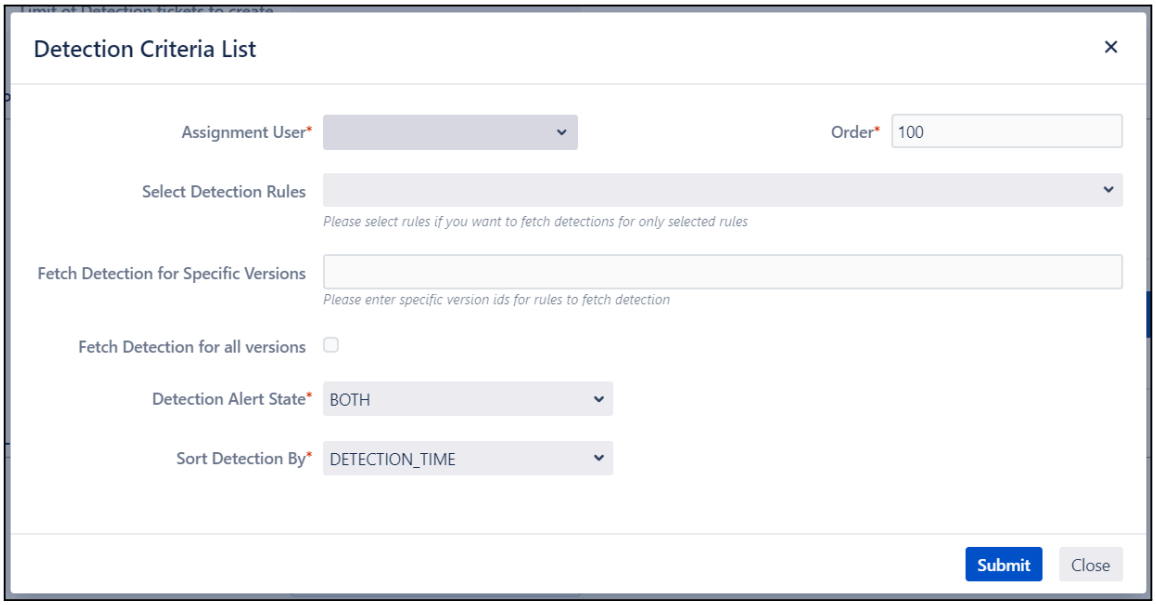
- Click on the **New** button in the Detection Criteria List tab.

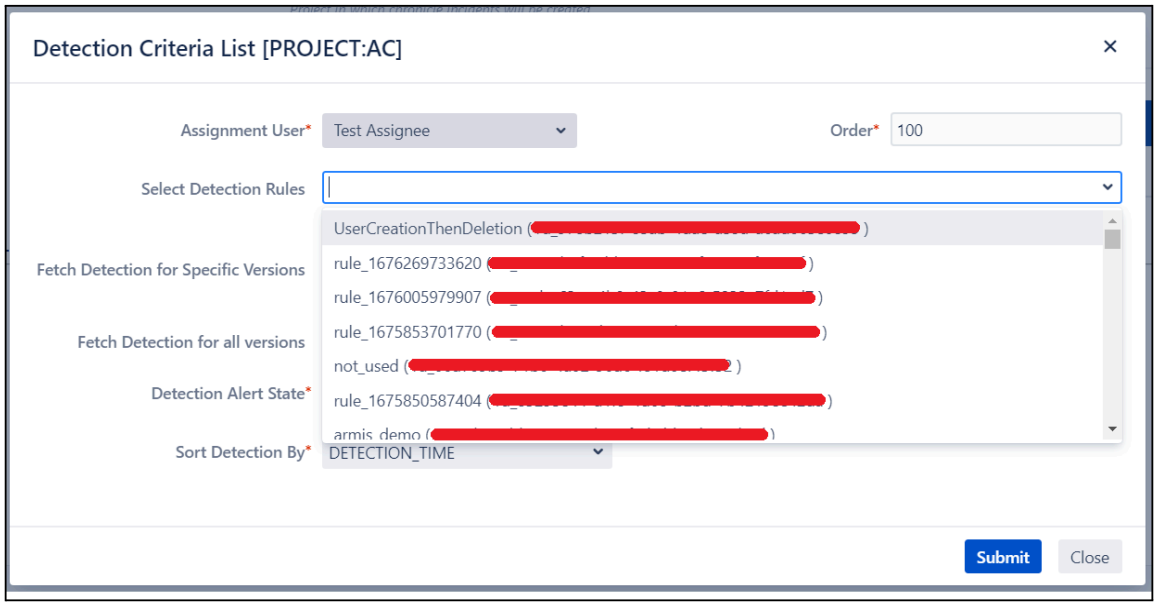


Detection Criteria List: Creation

- Detection Criteria List window will appear where the user will have the provision to configure the detection criteria in case any specific tickets need to be created in the selected project.
- Click on *Select Detection Rules*, and a multi-select dropdown with different rules will be displayed.
- Enter comma-separated version IDs of the selected rule in '*Fetch Detection for Specific Versions*' to create the detection ticket for the specific version of the rule
- Click on the checkbox '*Fetch detections for all versions*' to fetch the detection for all the versions of the selected rules.
- Click on the *Detection Alert State* to filter the detections by alert state.
- Click on the *Sort Detection By* dropdown to filter the detections by time.

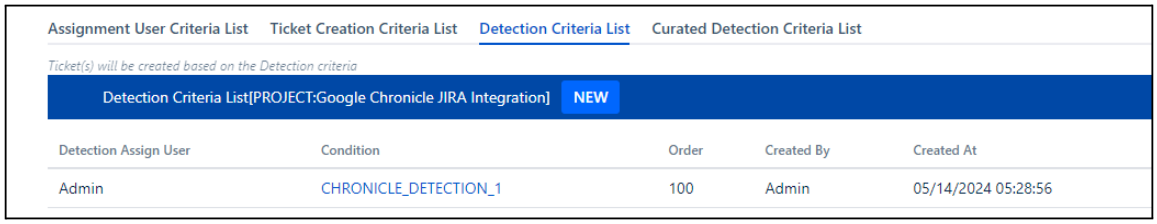
Note: The Detection Criteria and Curated Detection Criteria List will be deactivated for Stream Detections since it does not provide responses based on Criteria.





Field Name	Description
Assignment User	List of users that are part of the User Groups
Order	The priority of the criteria will be used to filter the response in order to assign the tickets to the user. Lowest to Highest, where the Highest will be preferred Default order: 100
Select Detection Rules	Select the rules needed to create the detection ticket
Fetch Detection for Specific Versions	Enter comma-separated version IDs of the selected rule to create the detection ticket for the specific version of the rule
Fetch Detection for all Versions	To fetch the detection for all the versions of the selected rules
Detection Alert State	Select the alert state for fetching the desired detection
Sort Detection By	Select the option to fetch the detection on the basis of time

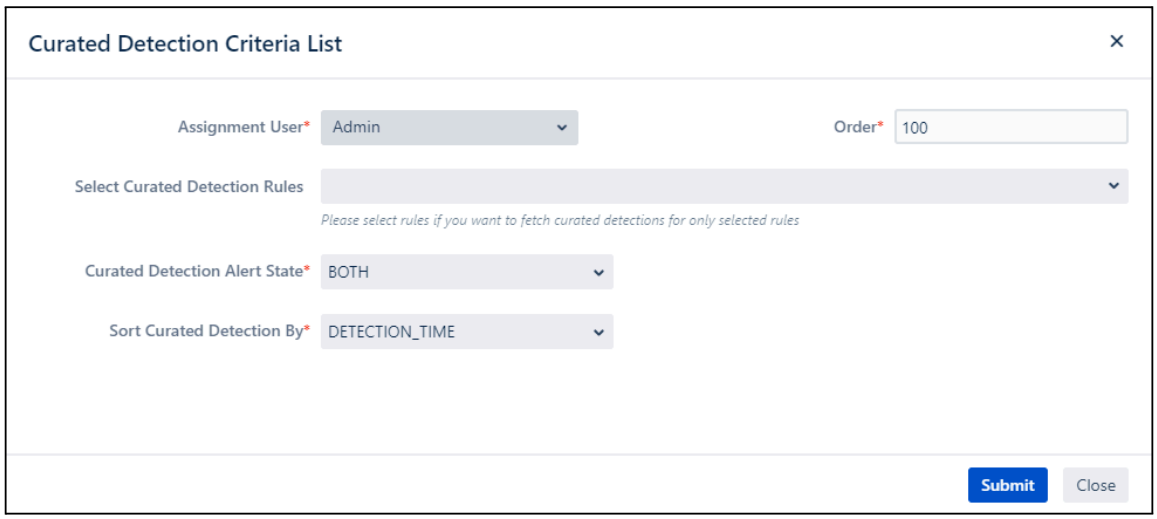
- Once the detection criteria are saved they will be displayed in the config screen as listed below

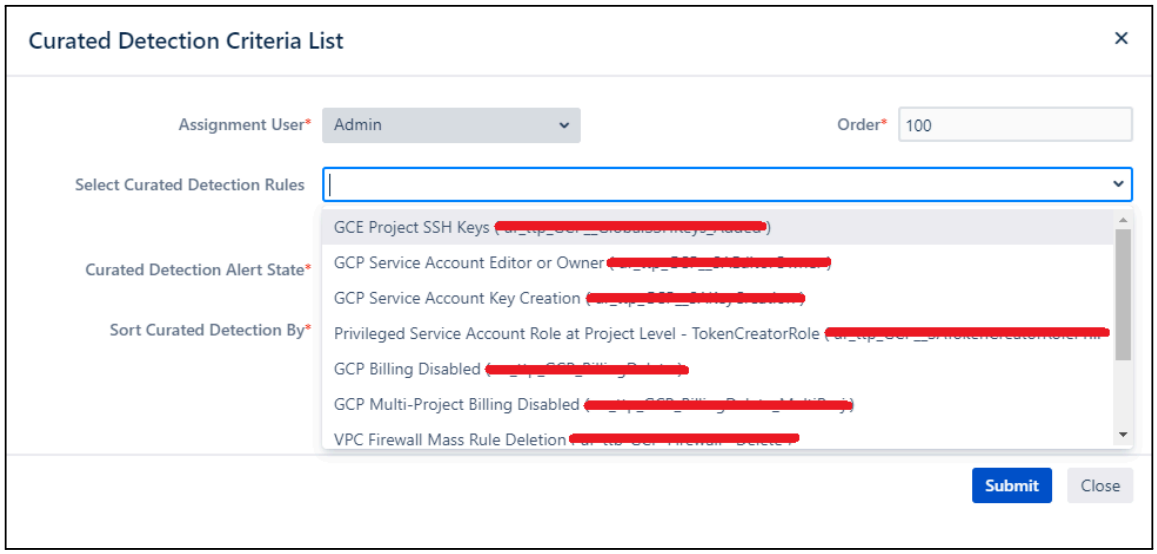


Curated Detection Criteria List: Creation

- A curated Detection Criteria List window will appear where the user will have the provision to configure the curated detection criteria in case any specific tickets need to be created in the selected project.
- Click on *Select Curated Detection Rules*, and a multi-select dropdown with different rules will be displayed.
- Click on the *Curated Detection Alert State* to filter the Curated Detections by alert state, the default value for alert state BOTH(ALERTING, NON_ALERTING)
- Click on the *Sort Curated Detection By* dropdown to filter the Curated Detections by time

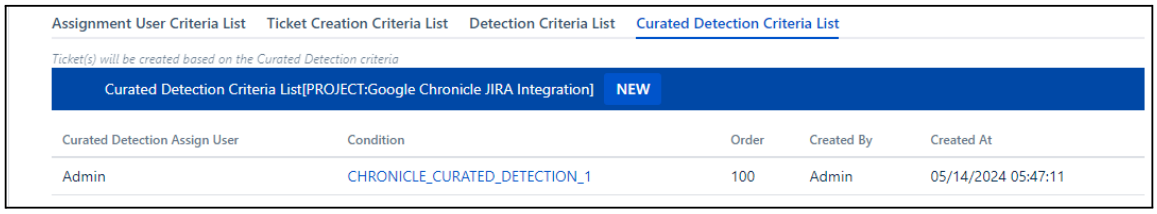
Note: The Detection Criteria and Curated Detection Criteria List will be deactivated for Stream Detections since it does not provide responses based on Criteria.





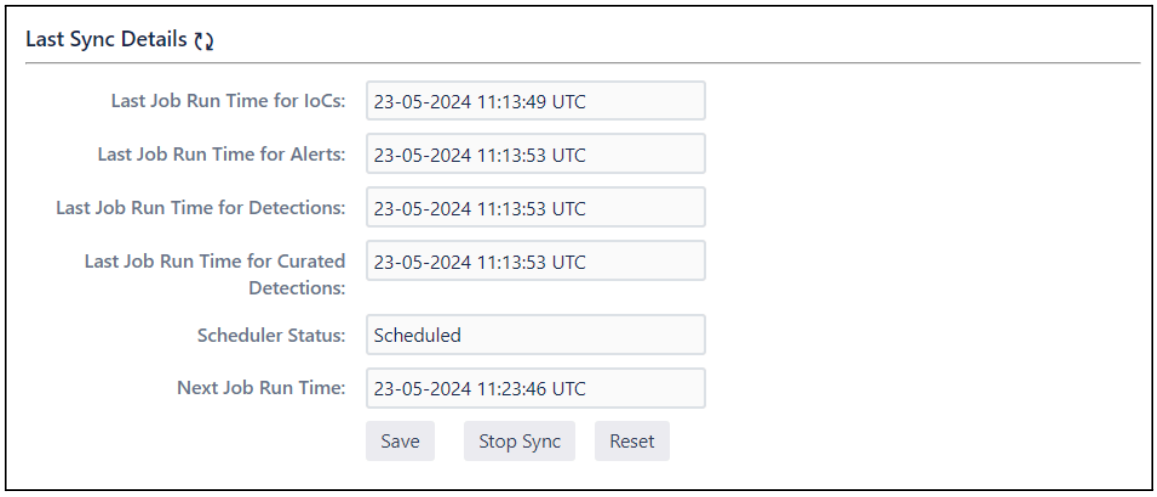
Field Name	Description
Assignment User	List of users that are part of the User Groups
Order	The priority of the criteria will be used to filter the response in order to assign the tickets to the user. Lowest to Highest, where the Highest will be preferred Default order: 100
Select Curated Detection Rules	Select the rules needed to create the Curated Detection ticket
Curated Detection Alert State	Select the alert state for fetching the desired Curated Detection
Sort Curated Detection By	Select the option to fetch the Curated Detection on the basis of time

- Once the Curated Detection criteria are saved they will be displayed in the config screen as listed below



Last Sync Details

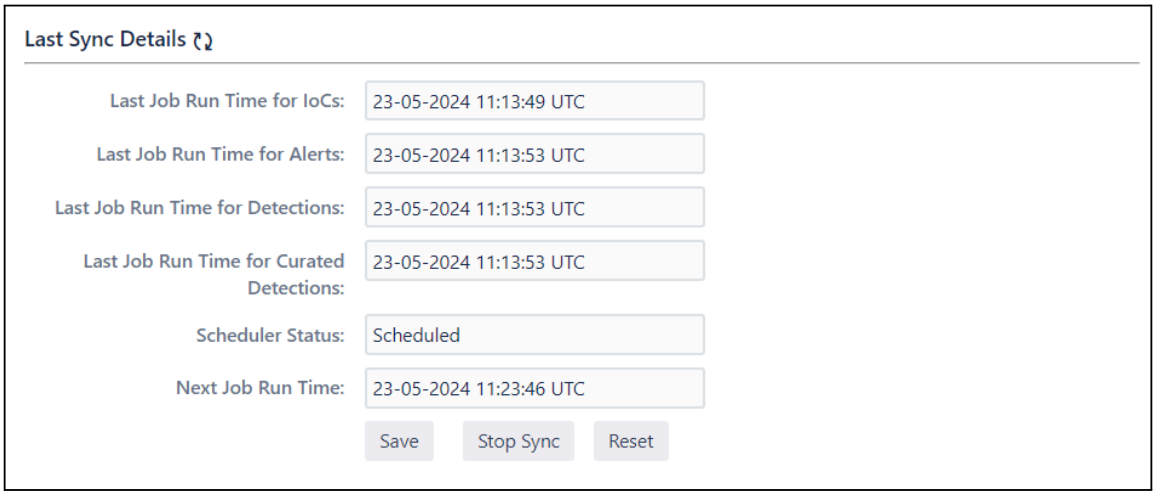
- Upon Clicking Save, the scheduler will trigger the Job to fetch the data from Google SecOps in order to start creating the tickets.
- Once the Job has been executed successfully, wait for a few moments and then click on the Refresh icon beside the Last Sync Details label.
- Upon clicking the Refresh icon, it will update the Last Job Run Time for IoCs, Alerts, Detections and Curated Detections.
- Scheduler Status: Scheduled means that the job has been configured and scheduled successfully.
- Scheduler Status: Not Scheduled means that the Job is currently not scheduled and no API calls will be made to SecOps.
- Next Job Run Time: The Date and time for the next scheduled job run.



Button Event Action

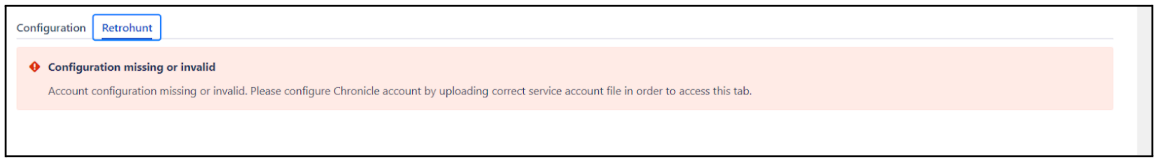
- Save: This action will stop the current sync process and initiate the new sync process as per the new configuration provided.
- Stop Sync: This action will stop the current sync process and deregister the scheduler.
- Reset: This action will stop the current sync process, deregister the scheduler and set the configuration to the default one.

Existing sync would be completed in case of updates and changes would be applicable from the next invocation.



Retrohunt

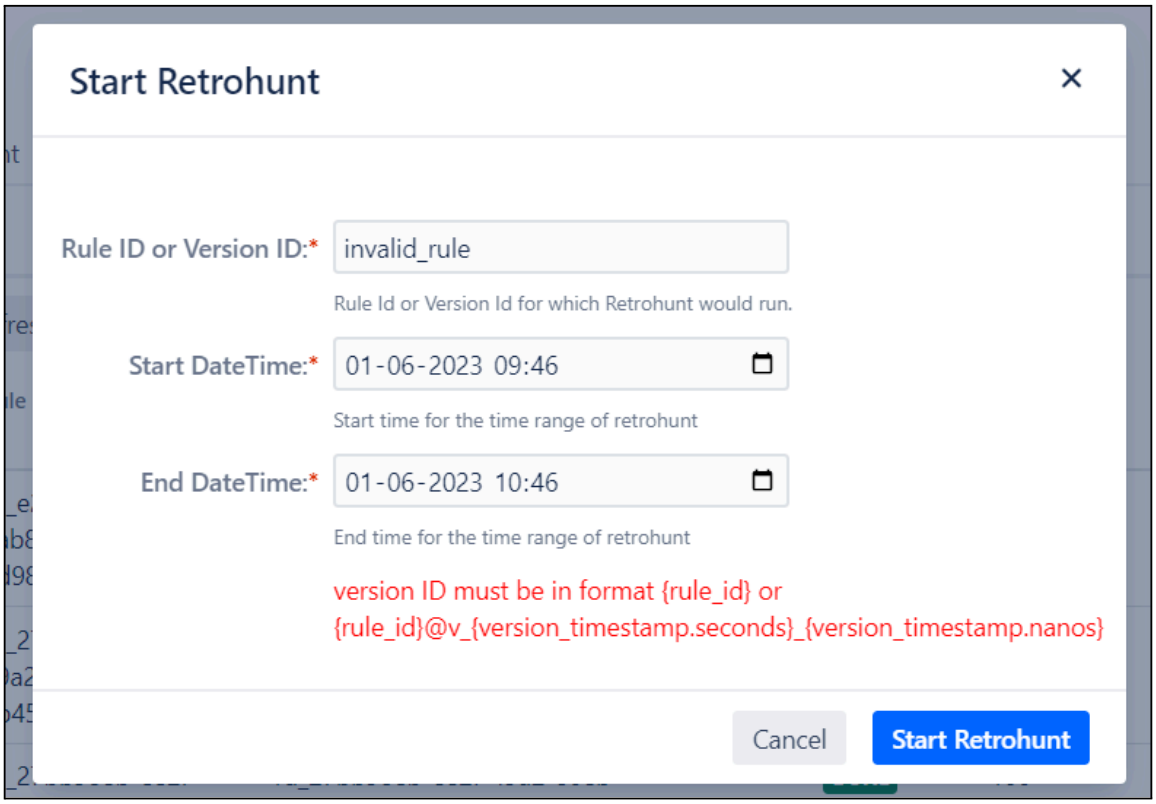
Once the user opens the Retrohunt tab, it will check whether the user has done the Google SecOps authentication configuration or not.
If the user has not already done the Google SecOps authentication then the below message will be displayed



If the user has already done the SecOps authentication then the below screen would be displayed with options to start/cancel the retrohunt and see a list of retrohunts created earlier as the table view.

Start Retrohunt

In order to start the new retrohunt, click on the “Start Retrohunt” button, which will open a popup asking for the user input required to start the new retrohunt.
After entering all the required information click on the “Start Retrohunt” button to start the new retrohunt.
In case any error occurs while starting the new retrohunt, the Error message will be displayed as shown below.



On success, the below message will be displayed to the user and the user can click on the “Refresh List” button to refresh the list of the retrohunts displayed in the table to see the details of the latest retrohunt.

Cancel Retrohunt

In order to cancel the running retrohunt click on the “Cancel” button placed in the last column of that particular row of the retrohunt. The users would not be able to cancel the retrohunts which are cancelled or done.

On success, the below message will be displayed to the user.

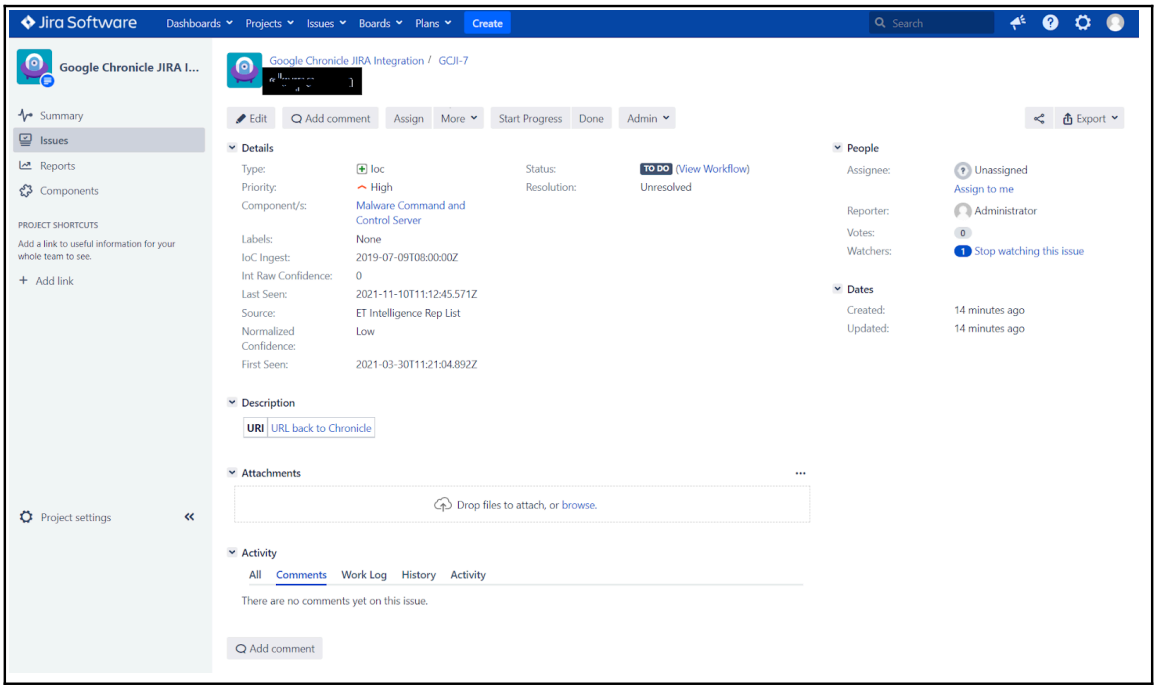
Ticket Created by the App

The app can create a total of 4 different types of tickets, based on the configuration that the user chooses:

1. IoC Match
2. User Alert
3. Asset Alert
4. Detections
5. Curated Detections

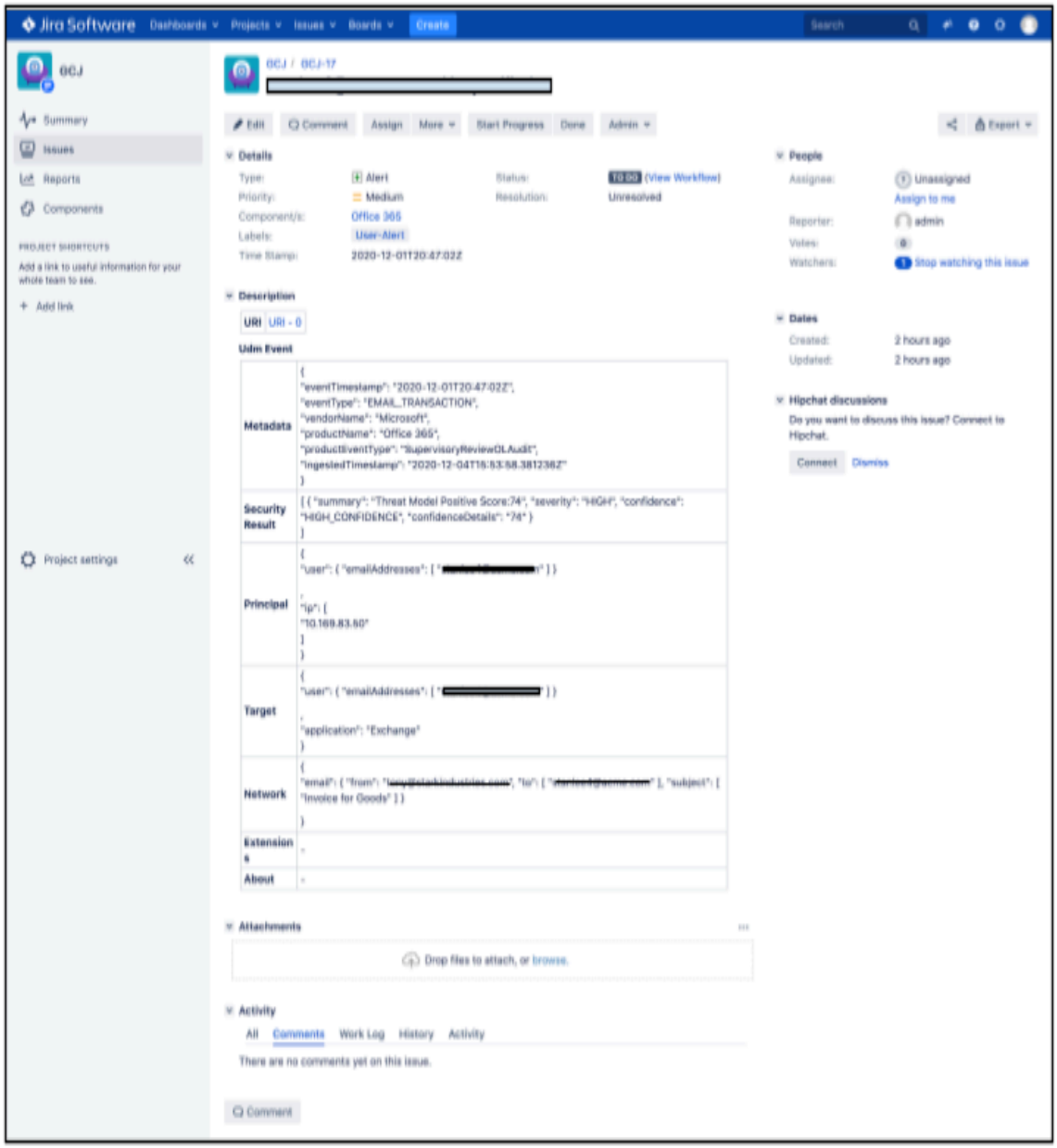
IoC Domain Match

IoC(Indicators of Compromise) ticket, will help users to determine which domain has been compromised, catering all the information for that domain and will display in the ticket form as displayed below.
The deduplication criteria over here is the summary of Jira Issue which is built using Artifact, which means only a single ticket will be created for the artifact that is compromised until the ticket is in the Todo, In-Progress and In-Review stages.



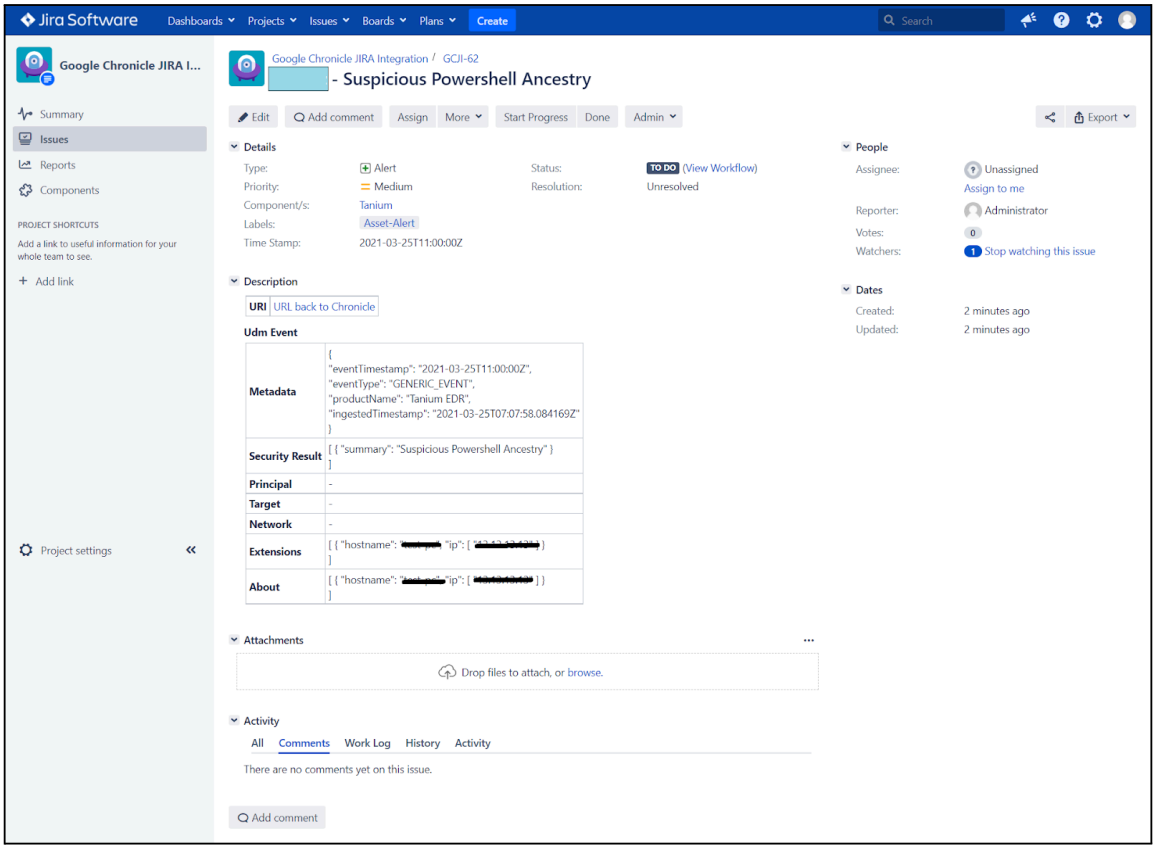
User Alert Ticket

When any alert occurs for a particular user, then those data are captured and displayed in the form of a ticket as displayed below, helping the user to understand what could be the cause of the alert and to take appropriate action.
The deduplication criteria for the User Alert is the combination of the Email Address and Alert Name until the ticket is in the Todo, In-Progress and In-Review stage.
Note that here component names are case insensitive.



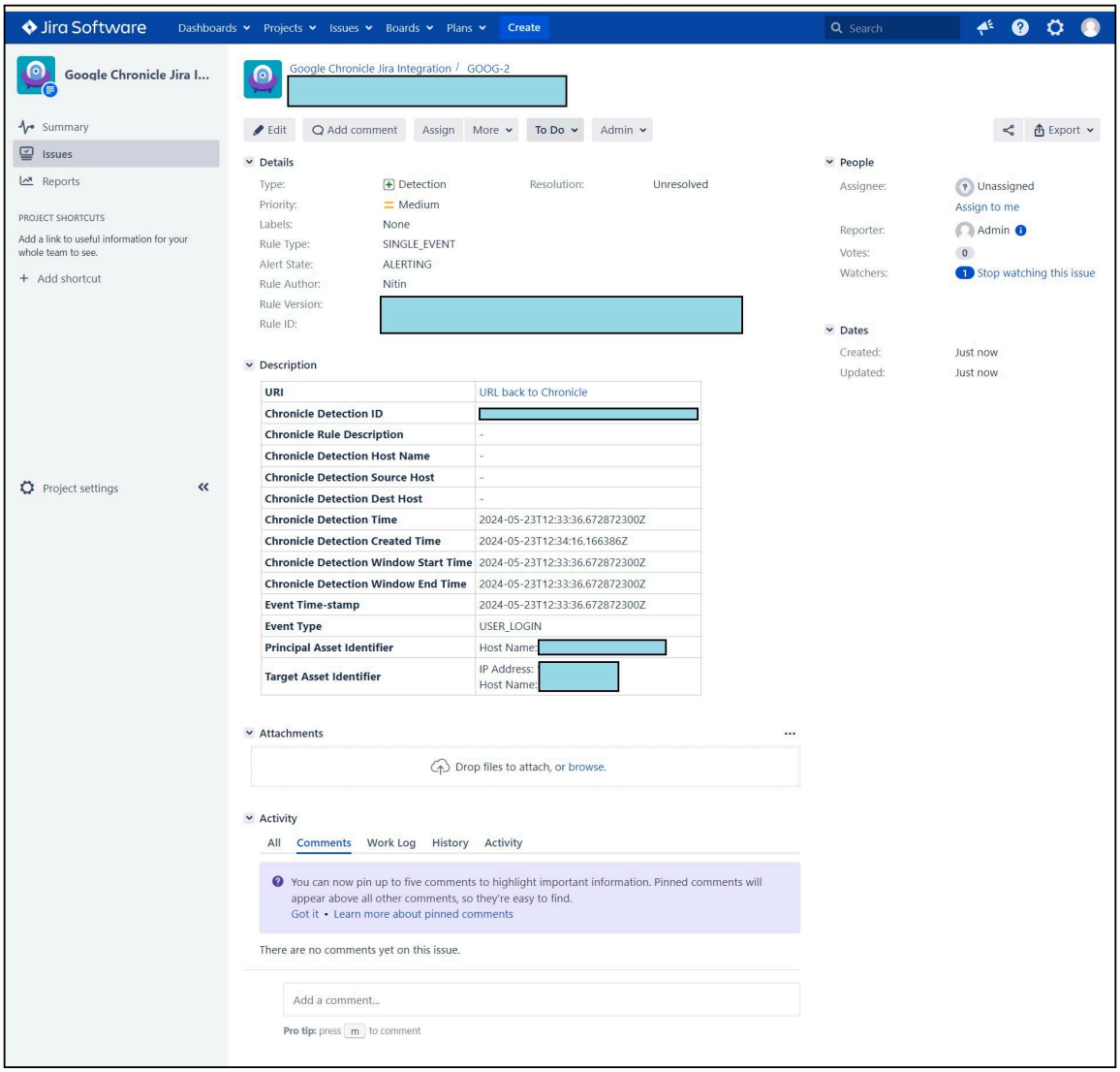
Asset Alert Ticket

When any alert occurs for a particular asset, then those data are captured and displayed in the form of a ticket as displayed below, helping the user to understand what could be the cause that would have impacted the asset and to take appropriate action.
The deduplication criteria for the Asset Alert is the combination of the Asset Name and Alert Name until the ticket is in the Todo, In-Progress and In-Review stage.
Note that here component names are case insensitive.



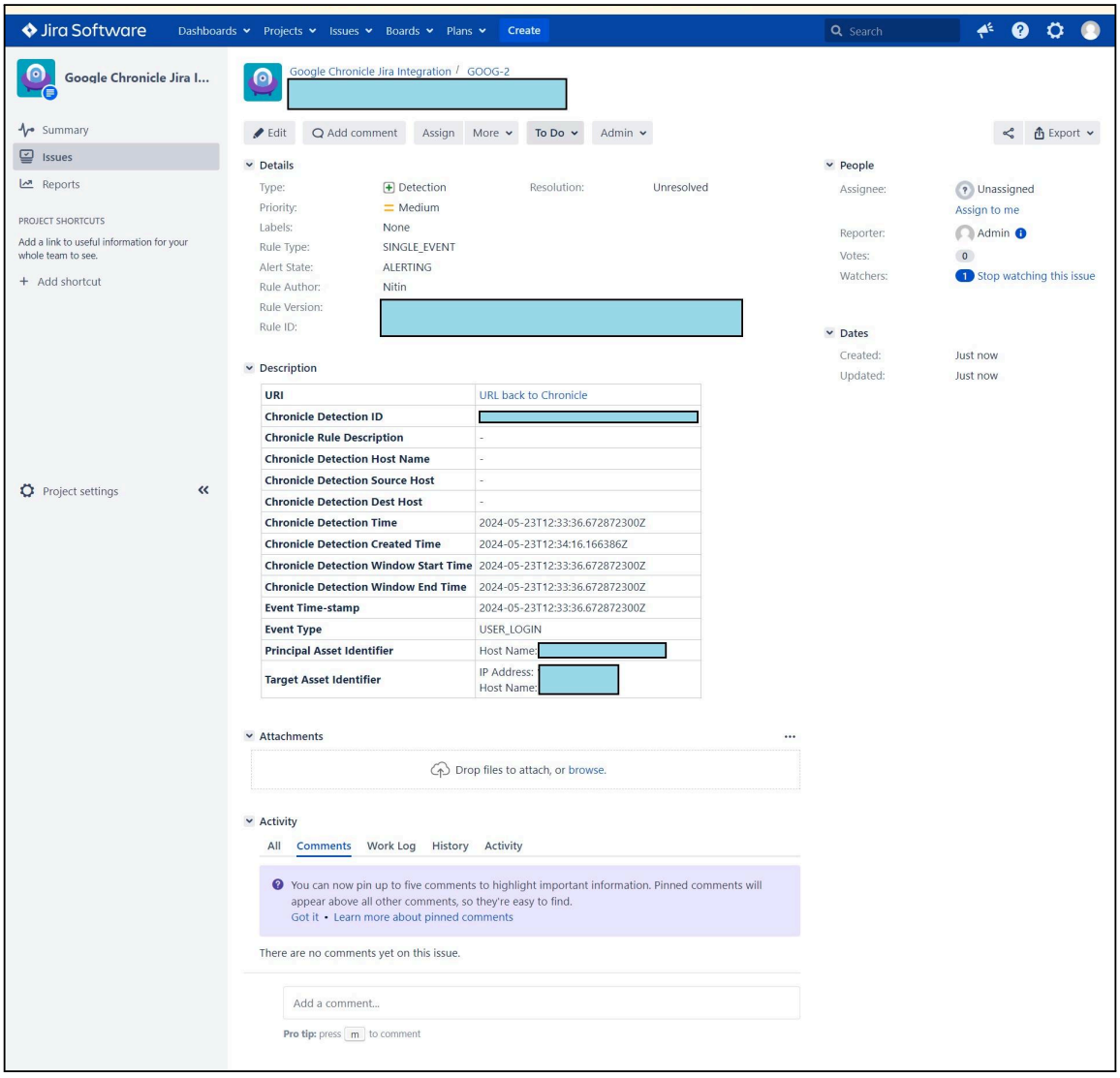
Detection Ticket

When any detection occurs for the particular rule, then those data are captured and are displayed in the form of a ticket as displayed below, helping the user to understand what could be the cause that would have impacted the rule and to take appropriate action.
The deduplication criteria for the Detection is the Detection ID until the ticket is in the Todo, In-Progress and In-Review stages.
There will not be any Enrichment feature for detections, instead, the data will be populated and a comment will be added to the corresponding detection ticket.



Curated Detection Ticket

When any Curated Detection occurs for the particular rule, then those data are captured and displayed in the form of a ticket as displayed below, helping the user to understand what could be the cause that would have impacted the rule and to take appropriate action.
The deduplication criteria for the Curated Detection is the Curated Detection ID until the ticket is in the Todo, In-Progress and In-Review stages.
There will not be any Enrichment feature for Curated Detections, instead, the data will be populated and a comment will be added to the corresponding Curated Detection ticket.



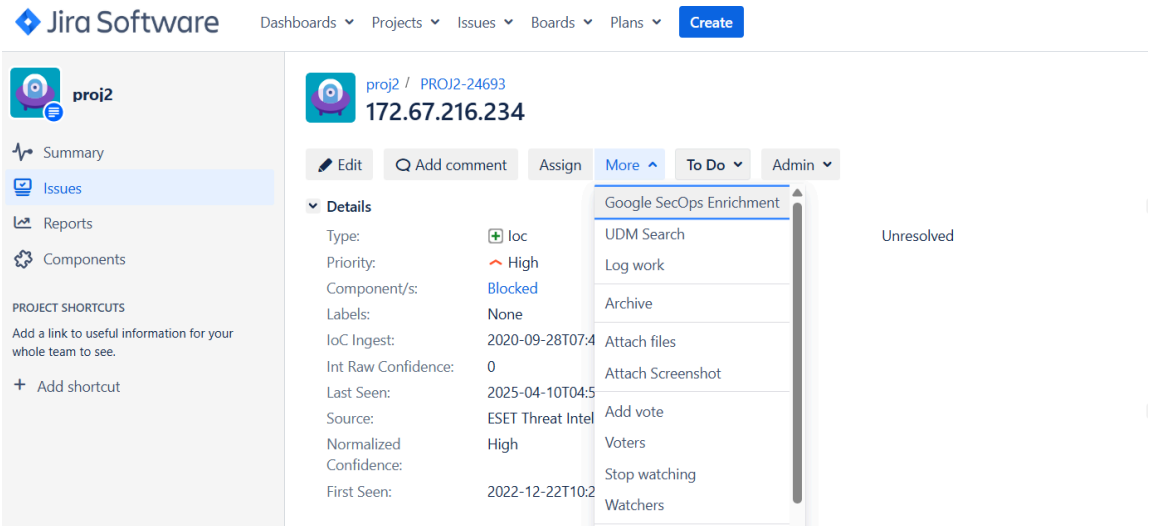
Enrichments

The enrichment process enables the user to select the time frame(number of days/date range) to determine which Assets were impacted and which Events were discovered related to a particular Domain or IP address.
This segment will take through the enrichment process that users can do on the created tickets. There are six different types of enrichment that the users can perform:

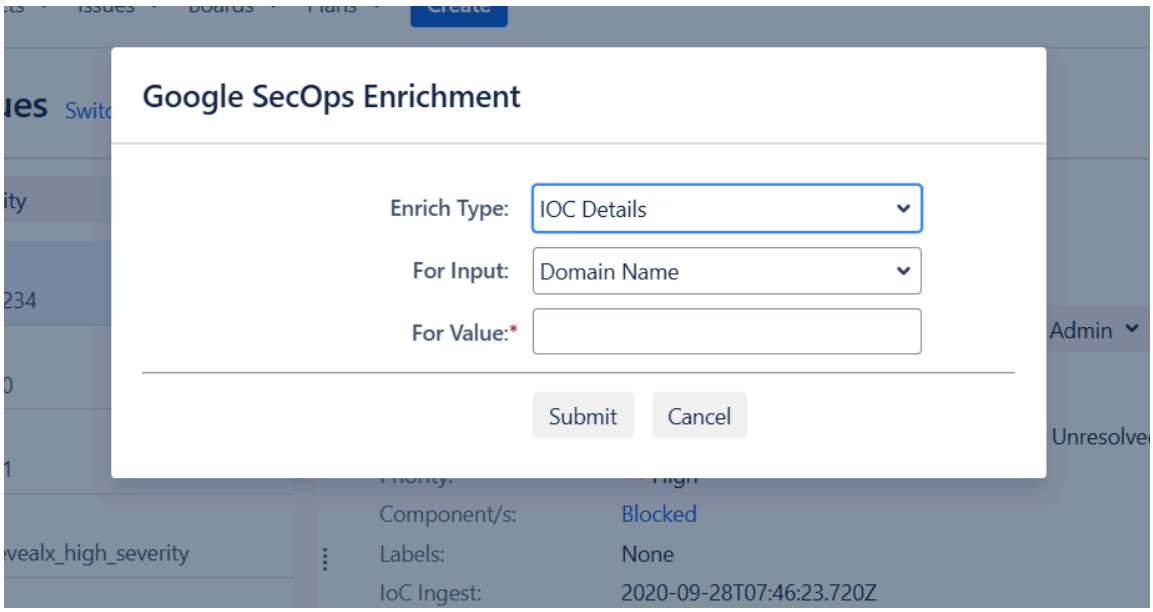
1. IoC Details
2. List Assets Impacted
3. List Events Discovered
4. List Asset Aliases
5. List User Aliases
6. UDM Search

IoC Details

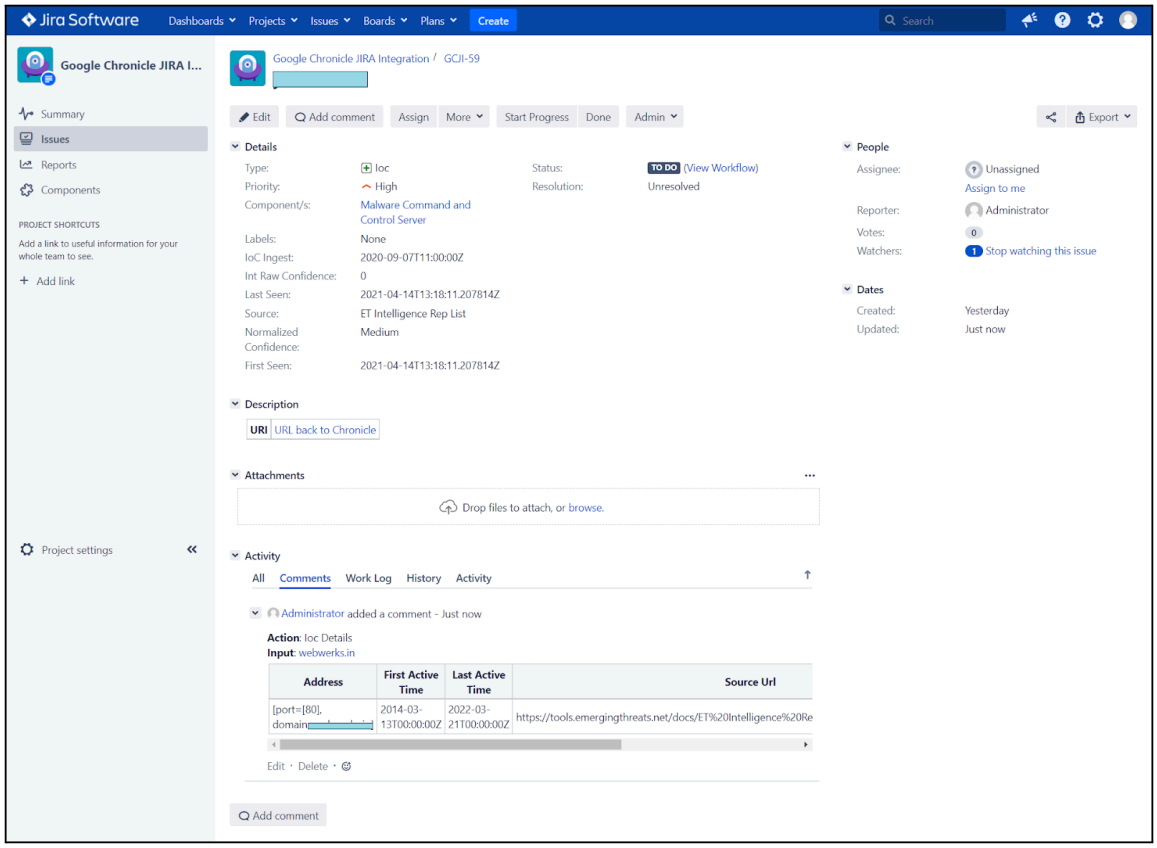
- Click on the More Menu, and then click on the Google SecOps Enrichment option.



- Upon clicking on the Google SecOps Enrichment, the below-displayed popup will be displayed.
- Selected the Enrichment type as IOC Details, as we would like to perform enrichment for IoC.
- The Input dropdown list will have two values Domain Name and IP Address.
- Select For Input as Domain Name, which will determine on which domain we would like to perform the enrichment.
- Enter the Domain Name in For Value, and click on Submit.

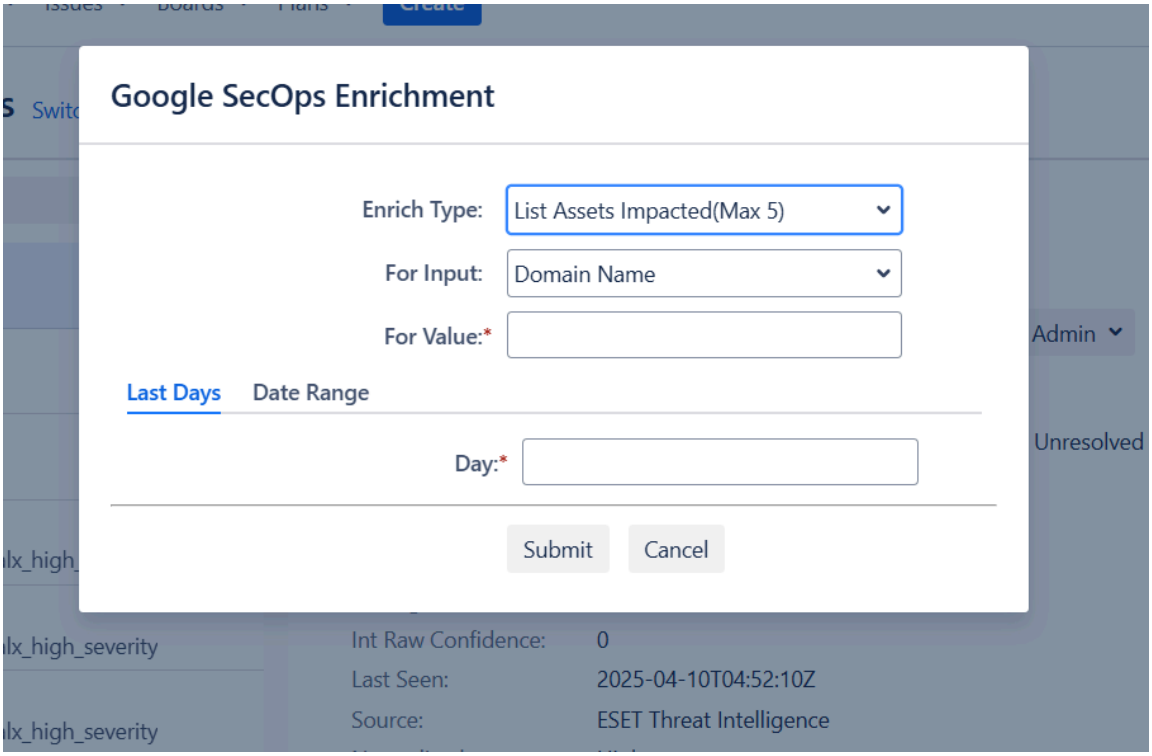


- The Response will be rendered in the comment section in the tabular format. Mentioning the fields chosen by the user and the value entered for the enrichment, and below that it will show the response received from the Google SecOps API.

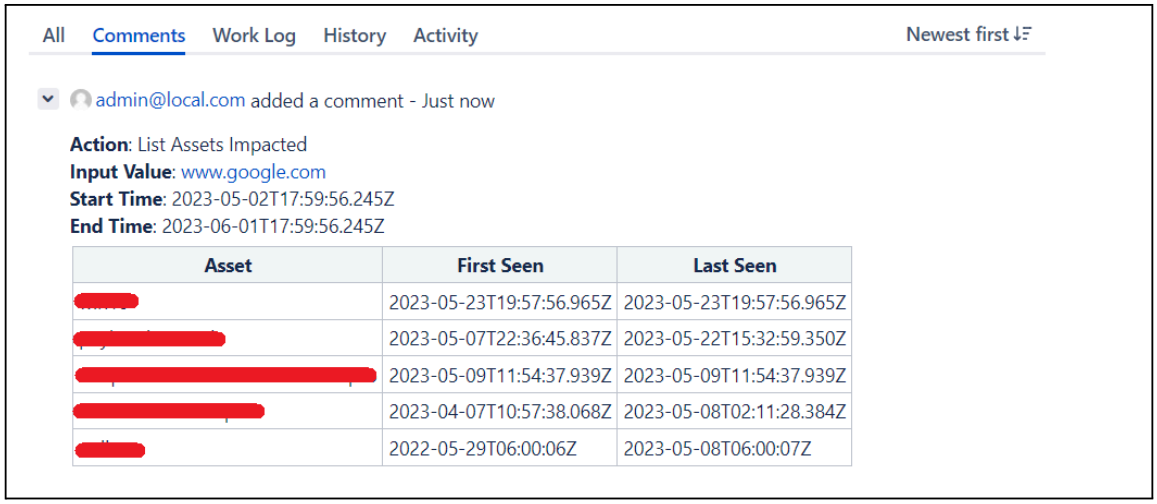


List Assets Impacted

- Upon clicking the More Menu and then Google SecOps Enrichment, the below-displayed popup will be displayed.
- Select the Enrichment type as List Assets Impacted, as we would like to perform enrichment for Asset Impacted.
- The input dropdown list will have multiple values like Domain Name, IP Address, HASH MD5, Hash SHA1 and Hash SHA256
- Select For Input as Domain Name, which will determine on which domain we would like to perform the enrichment.
- Enter the Domain Name in For Value.
- Then either enter the number of days or select the date range, and then click on Submit.

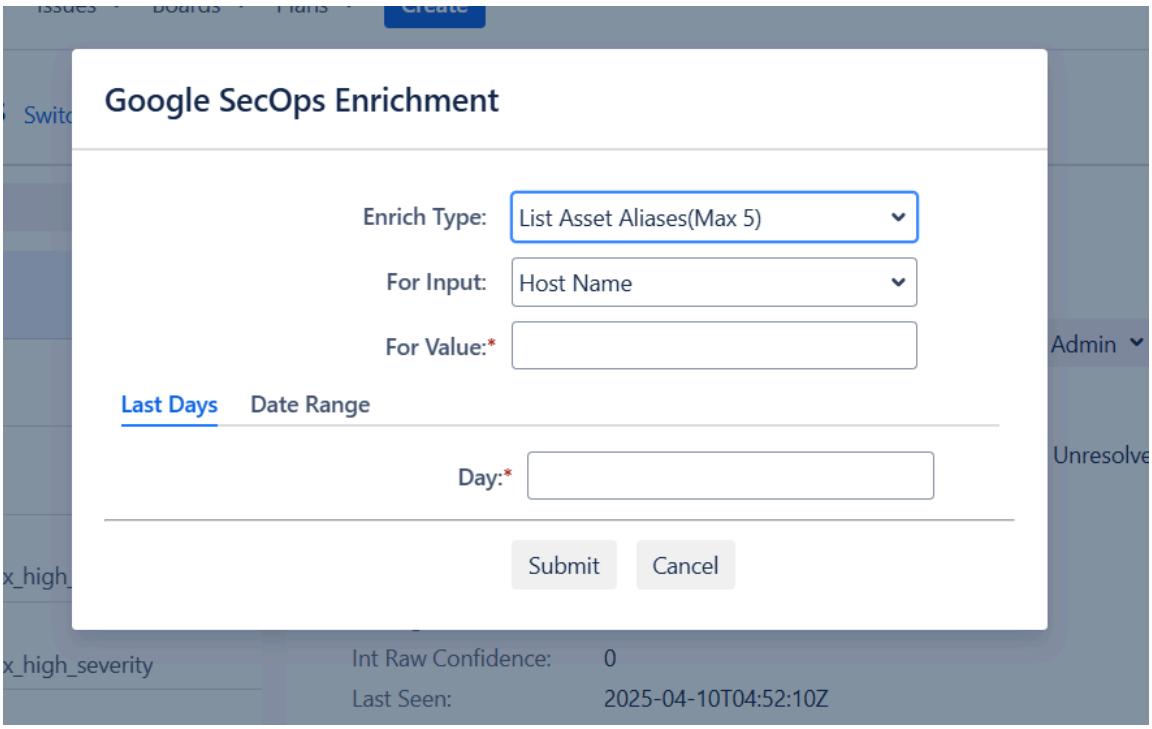


- The Response will be rendered in the comment section in the tabular format. Mentioning the fields chosen by the user and the value entered for the enrichment, and below that it will show the response received from the Google SecOps API.

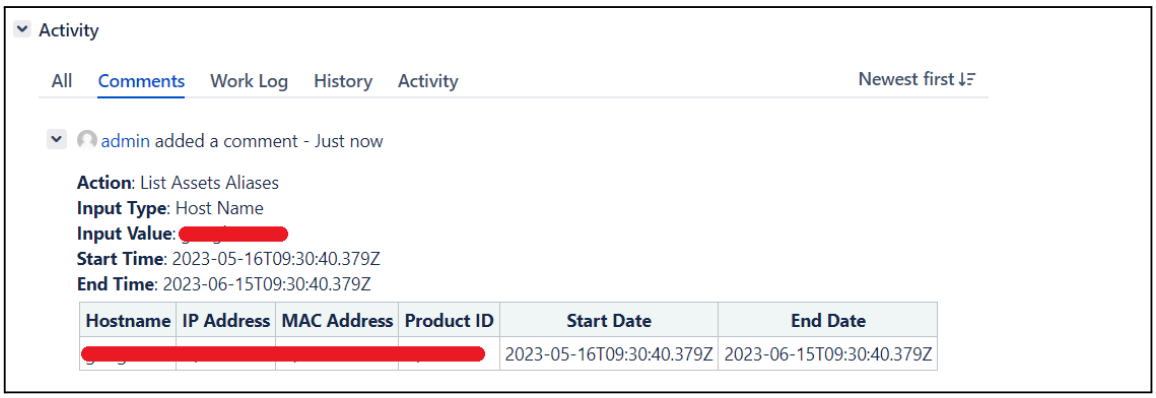


List Asset Aliases

- Upon clicking the More Menu and then Google SecOps Enrichment, a popup will be displayed.
- Select the Enrichment type as List Asset Aliases, as we would like to perform enrichment for Asset Aliases.
- For Input dropdown list will have multiple values like Host Name, IP Address, MAC Address and Product ID.
- Select For Input as Hostname, which will determine on which Hostname we would like to perform the enrichment.
- Enter the Hostname in For Value.
- Then either enter the number of days or select the date range, and then click on Submit.



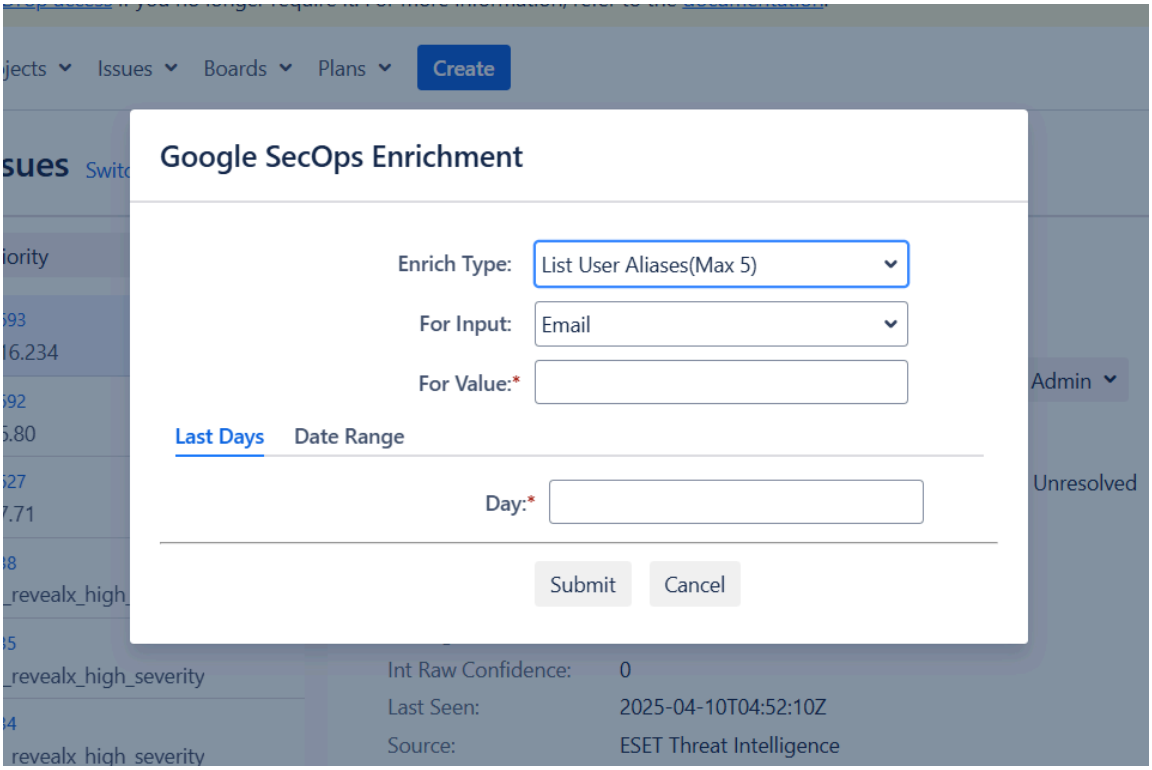
- The Response will be rendered in the comment section in the tabular format. Mentioning the fields chosen by the user and the value entered for the enrichment, and below that it will show the response received from the Google SecOps API.



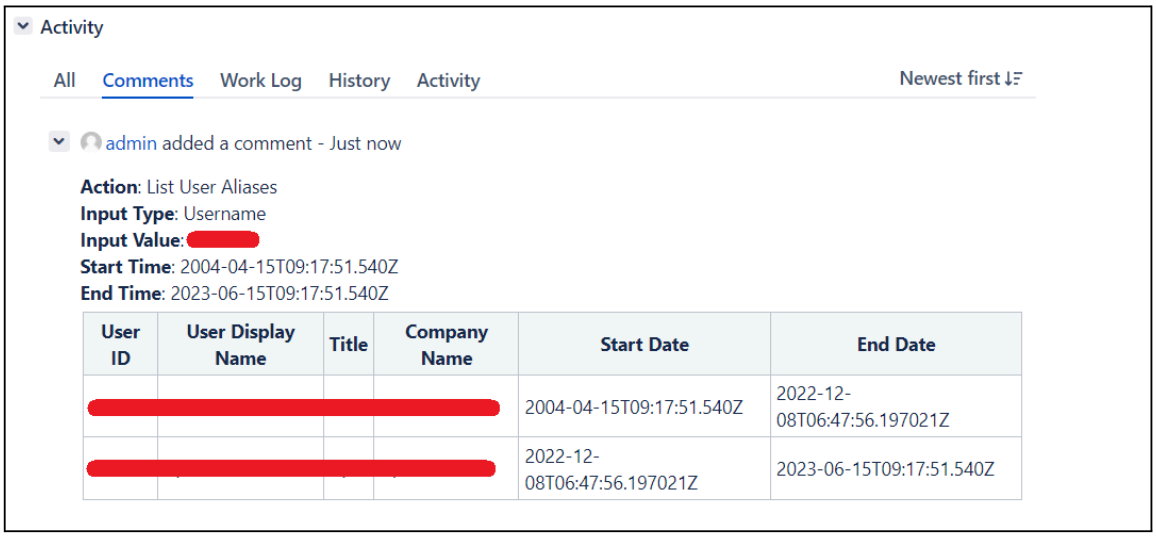
List User Aliases

- Upon clicking the More Menu and then Google SecOps Enrichment, the below-displayed popup will be displayed.
- Select the Enrichment type as List User Aliases, as we would like to perform enrichment for User Aliases.
- For Input dropdown list will have multiple values like Email, Username, Windows SID, Employee ID and Product Object ID.

- Select For Input as Username, which will determine on which username we would like to perform the enrichment.
- Enter the Username in For Value.
- Then either enter the number of days or select the date range, and then click on Submit.

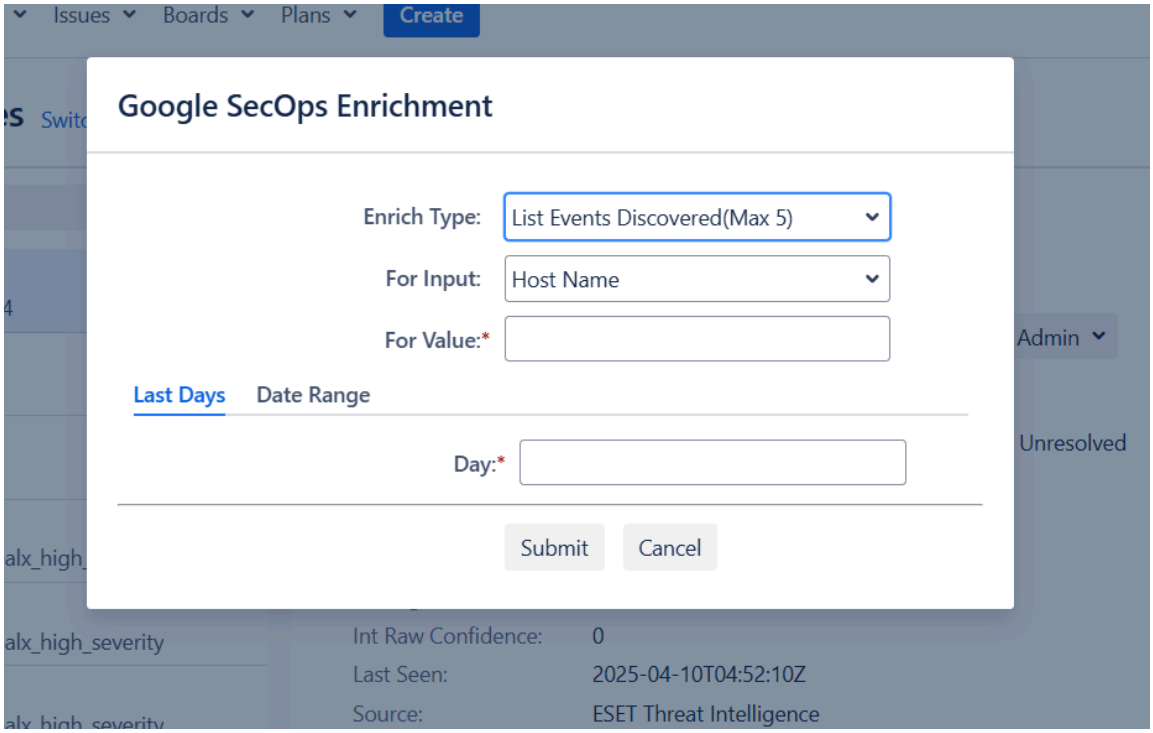


- The Response will be rendered in the comment section in the tabular format. Mentioning the fields chosen by the user and the value entered for the enrichment, and below that it will show the response received from the Google SecOps API.



List Events Discovered

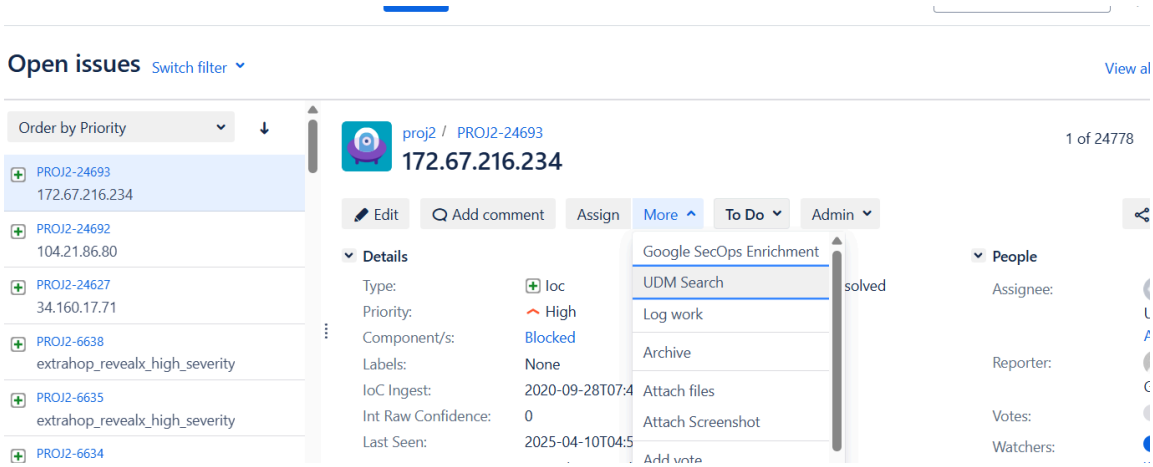
- Upon clicking the More Menu and then Google SecOps Enrichment, the below-displayed popup will be displayed.
- Select the Enrichment type as List Assets Impacted, as we would like to perform enrichment for Events Discovered.
- The Input dropdown list will have multiple values like Host Name, IP Address, MAC Address and Product ID.
- Select For Input as MAC Address, which will determine on which domain we would like to perform the enrichment.
- Enter the MAC Address in For Value.
- Then either enter the number of days or select the data range, and then click on Submit.



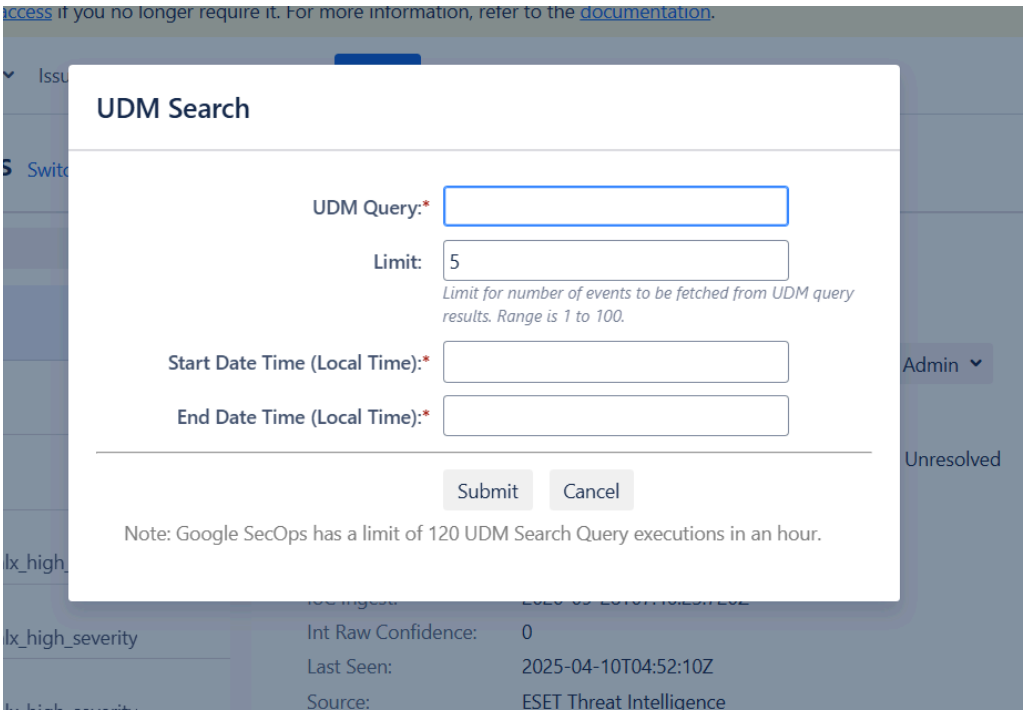
- The Response will be rendered in the comment section in the tabular format. Mentioning the fields chosen by the user and the value entered for the enrichment, and below that it will show the response received from the Google SecOps API.

UDM Search

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



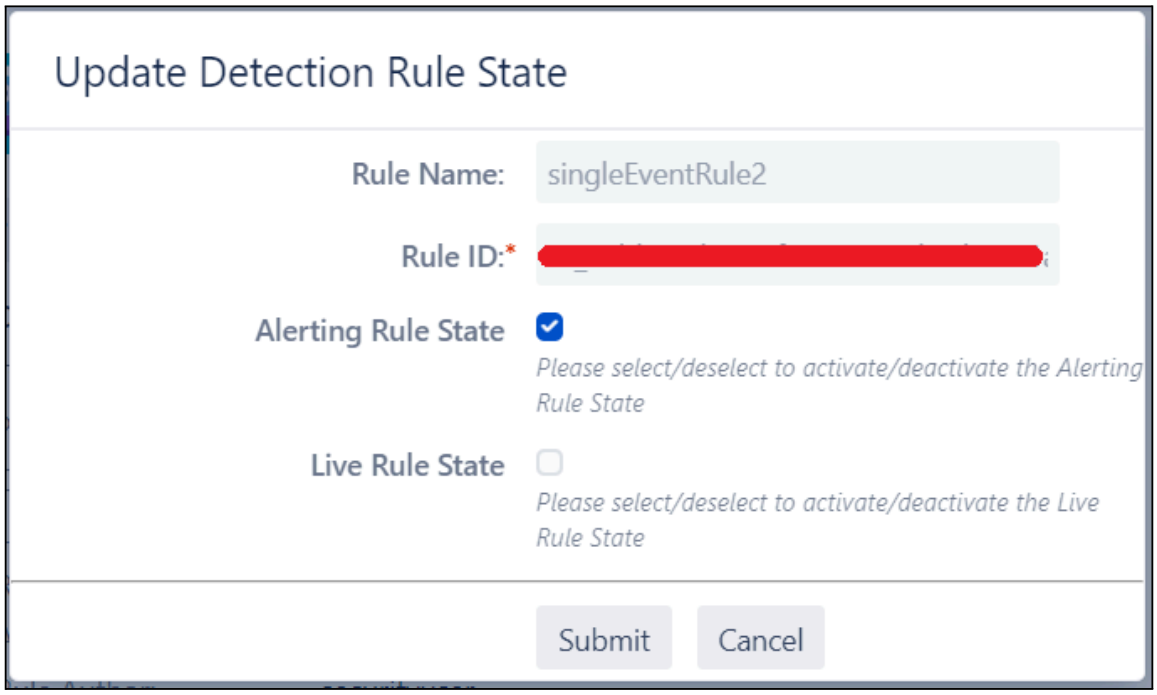
- Users need to enter the UDM query, select Start DateTime and EndTime. Set the Limit field which represents the no. of results fetched from the UDM search API and then click on the Submit button which will start the query execution.
- The query execution will run in the background after the user clicks 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.
- 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.



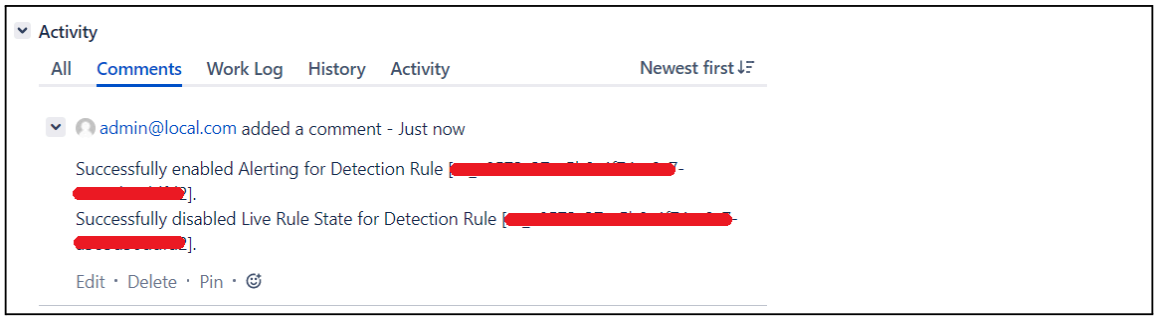
Update Detection Rule State

This option enables the user to enable/disable the Alerting and Live Rule State of the detection rule associated with the detection ticket. Only Jira issues of detection issue type having a value of “Rule ID” custom field will have the option of “Update Detection Rule State”.
Click on the More Menu, and then click on the “Update Detection Rule State” option.

Upon clicking on the “Update Detection Rule State”, a popup will be displayed as below with the prefilled values of the Rule Name and Rule ID according to the Rule ID associated with the Detection ticket. Based on the current state of Alerting and Live for the given Rule ID, checkboxes would be selected/deselected by default.
Select/Deselect the Checkbox to enable/disable the Alerting or Live Rule State and click on “Submit” to update the Rule state.



The comment will be added to the Jira issue indicating whether the Update Rule State was successful or not.



Development Assumptions

1. Only those projects will be listed which would have been created via the Google SecOps Project Creation Template
2. For Daily, weekly and monthly the job won't trigger immediately. It will only fetch the data as the user configures it.

3. The deduplication criteria for the ticket creation are as follows:
    - IoC: Summary of Jira Issue which is built using artifacts (Domain Name, DestinationIP, SHA etc.)
    - Asset Alert: Combination of Asset and Alert Name.
    - User Alert: Combination of Email Address and Alert Name.
    - Detection: Detection Id.
    - Curated Detection: Detection Id.
4. If the severity is empty/NA and has not been sent as part of the Google SecOps API response then, in that case, the ticket severity will be set to the project default.
5. No Updation will take place once the tickets are created based on deduplication criteria.
6. The same tickets will be created based on the deduplication criteria when those tickets are closed by the user.
7. When the project is changed and the configuration is saved, the Last Job runtime for Ioc, Alerts, Detections and Curated Detections will be reset and the data will be fetched based on the No of days to fetch IoCs/Alerts/Detections/Curated Detections Initially.
    - If an app is configured with Project A, and it's currently synching the data, and then a user changes the Project to B and then clicks on Save. Then the Last Job Run time will Reset and the synching will start based on the days that would have been mentioned in **No of days to fetch IoCs/Alerts/Detections/Curated Detections Initially** for Project B.
8. The Stream Detection feature utilizes a separate scheduler that is invoked every 10 minutes. If a scheduled job is currently running, it will skip the new job and continue the ongoing stream collection. However, if the stream fails due to any reason, it will start the new job in the next 10-minute interval.
9. In the Stream Detection feature, when the user configures the new stream detection configuration and saves the new configuration, the stream detection will start using the new configuration after a maximum of 10-minute time range, at the next scheduled job invocation.
10. The "Number of days to fetch IoCs/Alerts/Detections/Curated Detections initially" determines the continuation time parameter for Stream API calls. However, if the user inputs a value exceeding the last 7 days, the app will automatically set the continuation time to 7 days from the current time.
11. On installation, if configurations are present then the scheduler will be registered and sync will start with the existing configuration.
12. When the invalid service account file is selected and authenticated, then it would consider the previously saved valid service account file for fetching the IOCs, alerts, Detections and Curated Detections and it won’t interrupt the current scheduler
13. When the incorrect proxy details are entered and authenticated, then it would consider the previously saved valid data when the configuration is saved, for fetching the IOCs, alerts, Detections, and Curated Detections and it won’t interrupt the current scheduler.
14. The app sends the entered inputs to the Google SecOps API and validations are handled by the Google SecOps itself. Based on the API response, the following message will be displayed in the comment section based on the user input

    - *No Response / Empty Response / Null Response:* Display the User-entered criteria with the message “No Data Found for the above Enrichment Criteria.”
    - *Bad Response / Error Response:* Display the User-entered criteria with the reason for failure.
15. For the Asset Aliases option in Google SecOps Enrichment, if the value of the selected input type parameter in the entity response is the same as the input value then that alias will not be added in the comment.
16. It is suggested that the user must first Reset the config before uninstallation.
17. If there is more data available for IOCs, Alerts, Detection or Curated Detection than the limit set on the configuration page then data beyond that limit will be lost.
    Ex. Suppose the “*Limit of IOC tickets to create per invocation*” is set to 1000 and the Daily scheduler is configured. If there are 1200 IOCs present in the Google SecOps for an interval of 1 day then only 1000 IOCs will be created in Jira and the remaining 200 will be missed.
18. Jira admin users won’t be able to change the workflow(Todo, In-Progress, In-Review and Done), custom fields and the Issue types of the project which are created by the Google SecOps Management System template. The restriction in the customized templates is good, as that doesn't allow any user to make changes stopping causing issues in the creation of the tickets
19. The users should be part of either of the following groups:
    - Jira Software
    - Jira Service Desk
    - Jira Administrator

Troubleshooting

1. For any issues, please refer to the “atlassian-jira.log” log file.
   (Location: $JIRA_HOME/atlassian/application-data/jira/log/atlassian-jira.log)
2. Following are the log errors.

Messages	**Responses**	**Location**
Invalid service account file or Invalid region.	If the Invalid service account file is uploaded or the Invalid region value	Config Screen

	is entered	
Failed to authenticate the service account file.	If the existing service account is no longer valid	Config Screen
Internal Server error.	The Jira server is down	Config Screen
Successfully validated service account.	Valid service account file	Config Screen
Valid Service Account file exists.	The existing service account file is valid	Config Screen
Previously saved valid authentication data will be considered.	The previously saved valid service account file/ proxy detail is considered.	Config Screen
Failure: Either due to invalid region selection / Google SecOps instance is unreachable	When an invalid region is selected for a service account credential file.	Config Screen
Authentication Failure: Either due to Invalid Service Account File / Invalid Proxy Detail (If proxy is enabled)	The uploaded service account file is invalid or the proxy details entered are incorrect.	Config Screen
API call failed on path[%s] status:%s & reason-phrase:%s	For the Google SecOps API error	Logs
authenticate() Failed to authenticate message:	Authentication Failed	Logs
Failed to call API on the path:	API called failed	Logs
Failed to close Http-Client	Cannot establish Http client connection	Logs
pullIoCDetails() Failed	Failed to pull Ioc's Data	Logs
pullAssets() Failed	Failed to pull Asset Data	Logs
pullEvents() Failed	Failed to pull Events Data	Logs
pullDetections() Failed	Failed to pull Detections data	Logs
pullCuratedDetections() Failed	Failed to pull Curated Detections data	Logs
pullStreamDetection() Failed	Stream connection failed.	Logs
pullStreamDetections() Finish	Stream connection closed and data collection was stopped.	Logs
pullRules() Failed	Failed to pull Rules data	Logs
pullCuratedRules() Failed	Failed to pull Curated Rules data	Logs
pullIoc() finish @ {}, IOC Match Count: {} & Ticket Count : {}	Display the counts of Ioc and how many tickets are created	Logs
iOcs() response: {}	Display the list of IoC under comments and in logs	Ticket comments and Logs
iocDetails() response: {}	Display the details of IoC under comments and in logs	Ticket comments and Logs

pullAlerts() finish @ {}, Alerts Count: {} & Ticket Count: {}	Display the counts of Alerts and how many tickets are created	Logs
assets() response: {}	Display the details of Asset under comments and in logs	Ticket comments and Logs
events() response: {}	Display the details of Events under comments and in logs	Ticket comments and Logs
pullDetection.detections() Finish @ {}, Last-Sync-Time {}, Detection Count : {}, Ticket Count : {} & Duplicate Ticket Count : {}	Display the counts of Detections and how many tickets are created	Logs
detections() response: {}	Display the details of Detections under comments and in logs	Ticket comments and Logs
pullCuratedDetection.curatedDetections() Finish @ {}, Last-Sync-Time {}, Curated Detection Count : {}, Ticket Count : {} & Duplicate Ticket Count : {}	Display the counts of Curated Detectors and how many tickets are created	Logs
streamDetection(), Finish @ {}, Last-Sync-Time {},Detection Ticket Count : {} & Curated Detection Ticket Count : {}	Display the counts of Detection and Curated Detectors received and how many tickets are created.	Logs
curatedDetections() response: {}	Display the details of Curated Detections under comments and in logs	Ticket comments and Logs
getAccessToken() Failed: Access-token can not be null or empty.	Access Token not valid	Logs
iocTicket() duplicate ticket[{}]: {}	Duplicates IoC found	Logs
iocTicket() created ticket: {}	IoC Tickets Created	Logs
Can not find %s custom field	If the custom field is not found	Logs
Can not find %s issue type	If the Issue Types is not found	Logs
Failed job runner	If the job is failed	Logs
registerSchedule() with parameter	When the job is registered based on the configuration	Logs
Error waiting until next try for the backoff strategy. Error: {}	When 429 error received for calling API endpoint	Logs
Retry Failed: Total of attempts: {}. Total waited time {} ms.	When the number of retries exceeded the maximum limit	Logs
userAliases() Failed: {}	When Google SecOps Enrichment [“User Aliases”] fails	Logs
assetAliases() Failed: {}	When Google SecOps Enrichment [“Asset Aliases”] fails	Logs
enableAlerting Failed: {}	When “Update Detection Rule State” fails to enable alerting for given rule	Logs

disableAlerting Failed: {}	When “Update Detection Rule State” fails to disable alerting for given rule	Logs
enableLiveRule Failed: {}	When “Update Detection Rule State” fails to enable Live state for given rule	Logs
disableLiveRule Failed: {}	When “Update Detection Rule State” fails to disable Live state for given rule	Logs
runRetrohunt() Failed: {}	When Starting a new retrohunt fails	Logs
cancelRetrohunt() Failed: {}	When cancelling a retrohunt fails	Logs
pullRetrohunts() Failed: {}	When getting retrohunts fails	Logs
getRuleDetails() Failed: {}	When getting rule details for particular detection rule fails	Logs

Additional Information

The below segment covers some additional information about the Google SecOps App

Application Dependencies

Area	**Version**
Java	8 (1.8.x)

Atlassian SDK	8.2.7
Google SecOps API Version	v1, v2

App - Jira Version Compatible Matrix

Jira Software	9.0.x - 9.15.x, 10.0.x - 10.3.x
Jira Service Desk	5.0.x - 5.15.x

——----------End of Document—----------