Chronicle App for Jira On-Prem v3.0.0

Release Documentation and User Guide

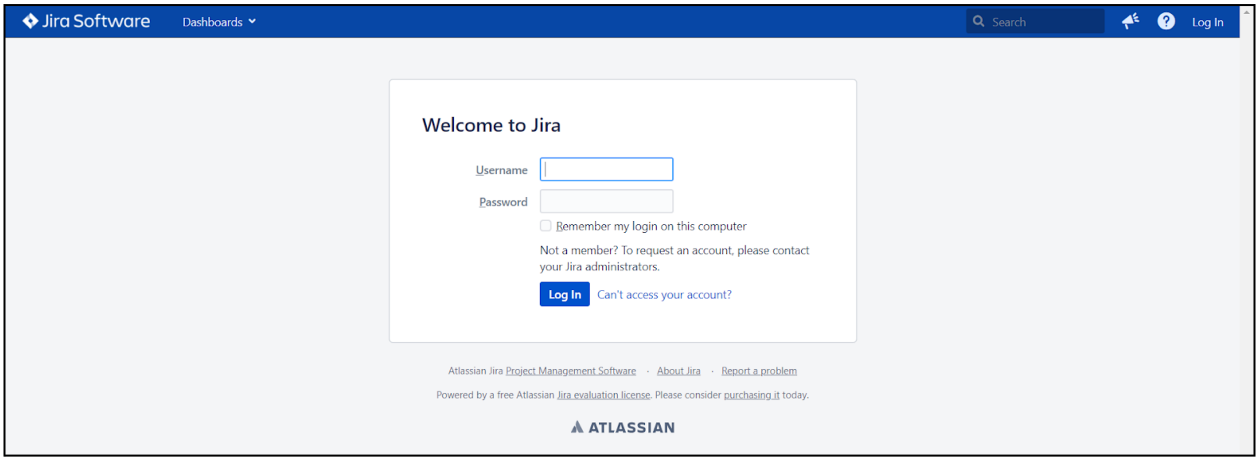
Contents

Installation Instructions

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

Login Page

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



Welcome to Jira

Username

Password

□ Remember my login on this computer

Not a member? To request an account, please contact your Jira administrators.

Log In Can't access your account?

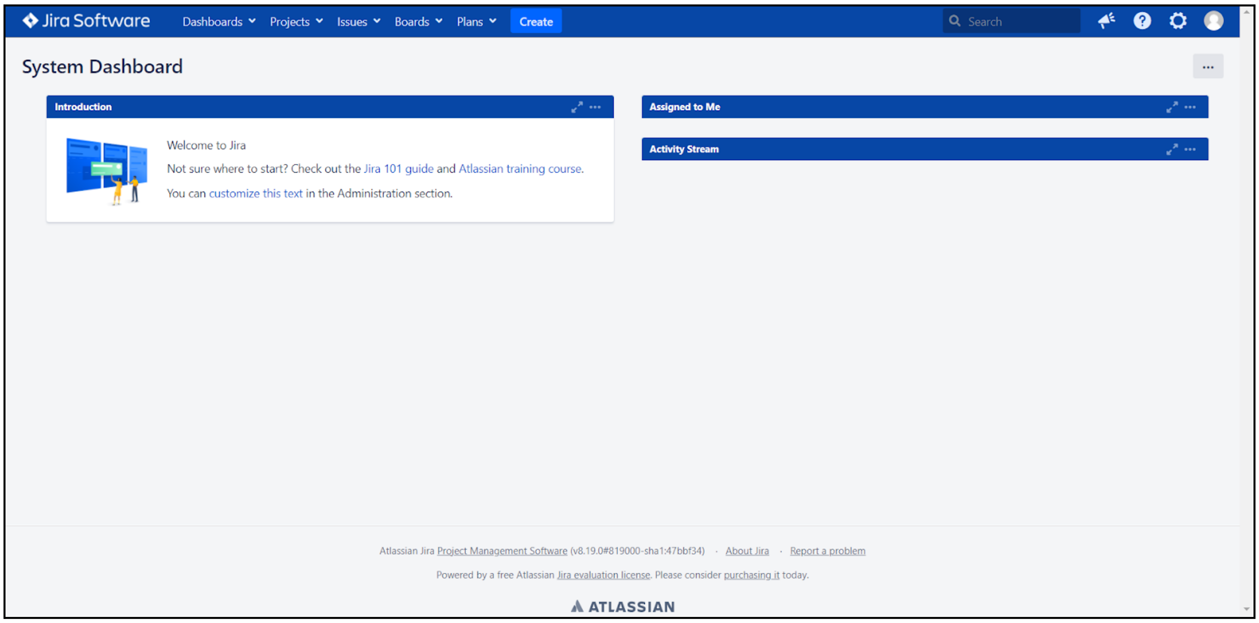
Atlassian Jira Project Management Software · About Jira · Report a problem

Powered by a free Atlassian Jira evaluation license. Please consider purchasing it today.

ATLASSIAN

Landing Page

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



System Dashboard

Introduction

Welcome to Jira

Not sure where to start? Check out the Jira 101 guide and Atlassian training course.

You can customize this text in the Administration section.

Assigned to Me

Activity Stream

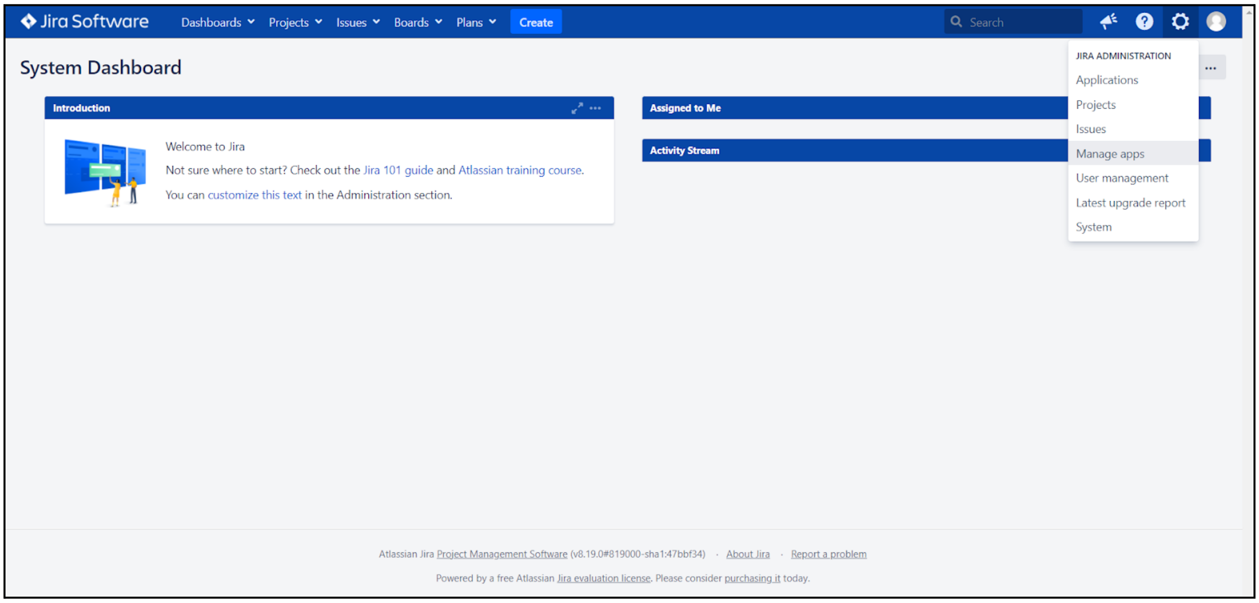
Atlassian Jira Project Management Software (v8.19.0#819000-sha1:47bbf34) · About Jira · Report a problem

Powered by a free Atlassian Jira evaluation license. Please consider purchasing it today.

ATLASSIAN

Goto Manage Apps

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



System Dashboard

Welcome to Jira

Not sure where to start? Check out the Jira 101 guide and Atlassian training course.

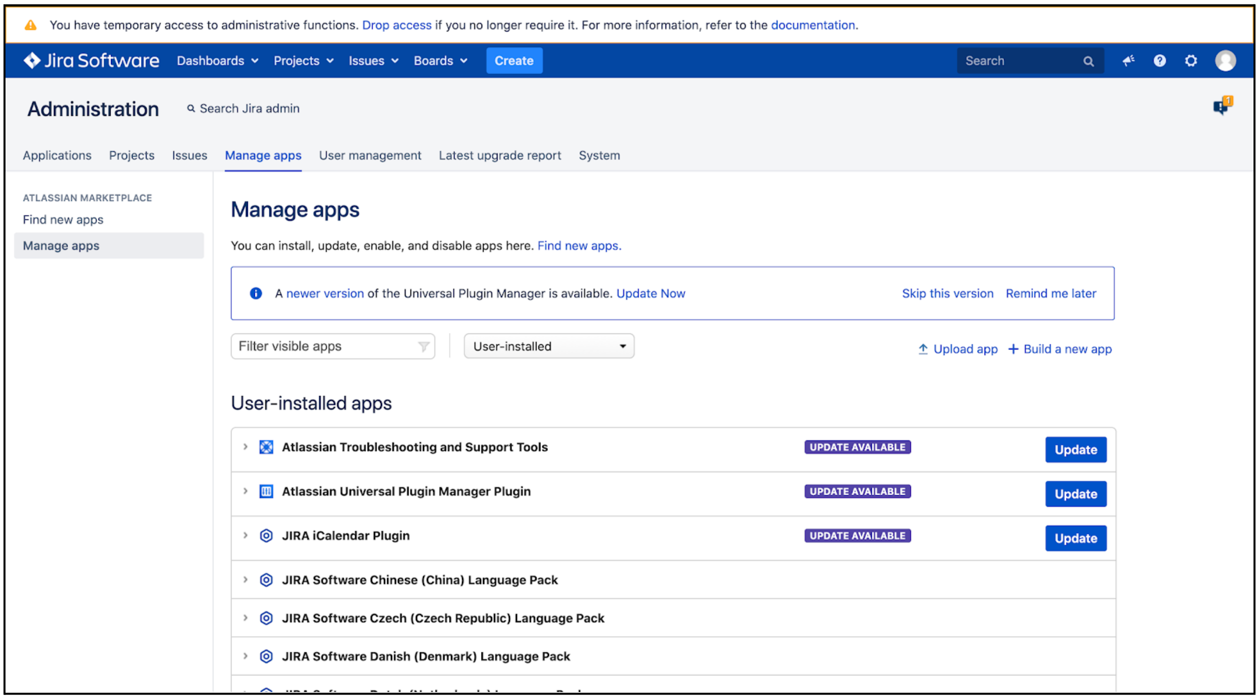
You can customize this text in the Administration section.

Atlassian Jira Project Management Software (v8.19.0#819000-sha1:47bbf34) · About Jira · Report a problem

Powered by a free Atlassian Jira evaluation license. Please consider purchasing it today.

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.



You have temporary access to administrative functions. Drop access if you no longer require it. For more information, refer to the documentation.

Administration

Manage apps

You can install, update, enable, and disable apps here. Find new apps.

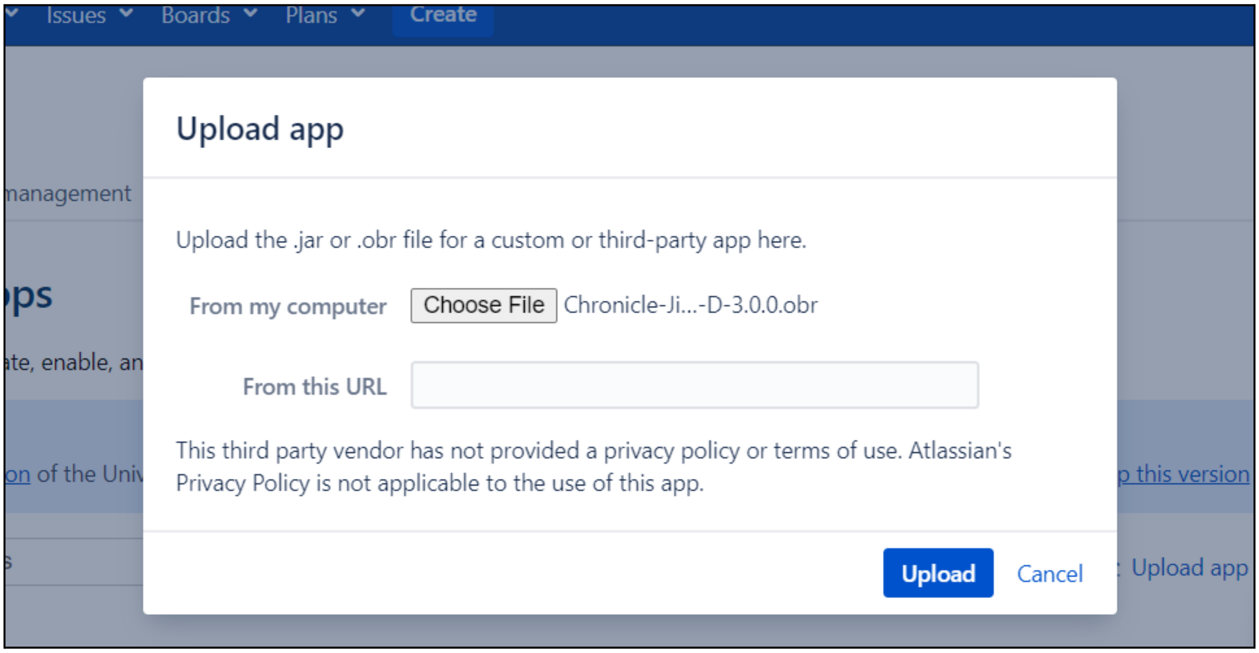
A newer version of the Universal Plugin Manager is available. Update Now

User-installed apps

Atlassian Troubleshooting and Support Tools	UPDATE AVAILABLE	Update
Atlassian Universal Plugin Manager Plugin	UPDATE AVAILABLE	Update
JIRA iCalendar Plugin	UPDATE AVAILABLE	Update
JIRA Software Chinese (China) Language Pack		
JIRA Software Czech (Czech Republic) Language Pack		
JIRA Software Danish (Denmark) Language Pack		

Upload App OBR/JAR file

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



Upload app

Upload the .jar or .obr file for a custom or third-party app here.

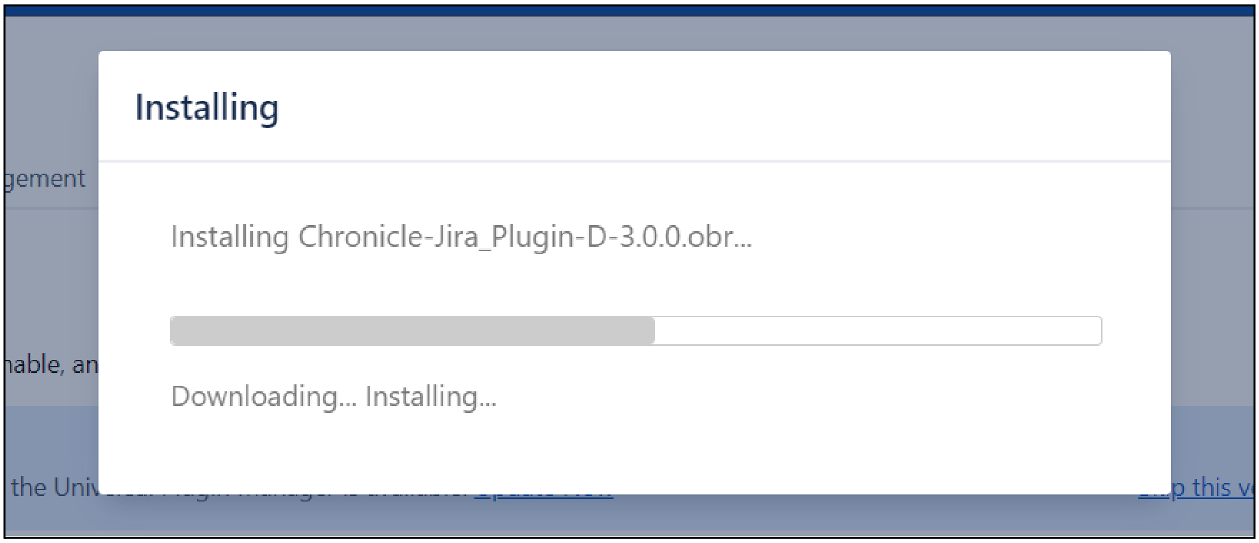
From my computer: Chronicle-Ji...-D-3.0.0.obr

From this URL:

This third party vendor has not provided a privacy policy or terms of use. Atlassian's Privacy Policy is not applicable to the use of this app.

Chronicle App Upload Process

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



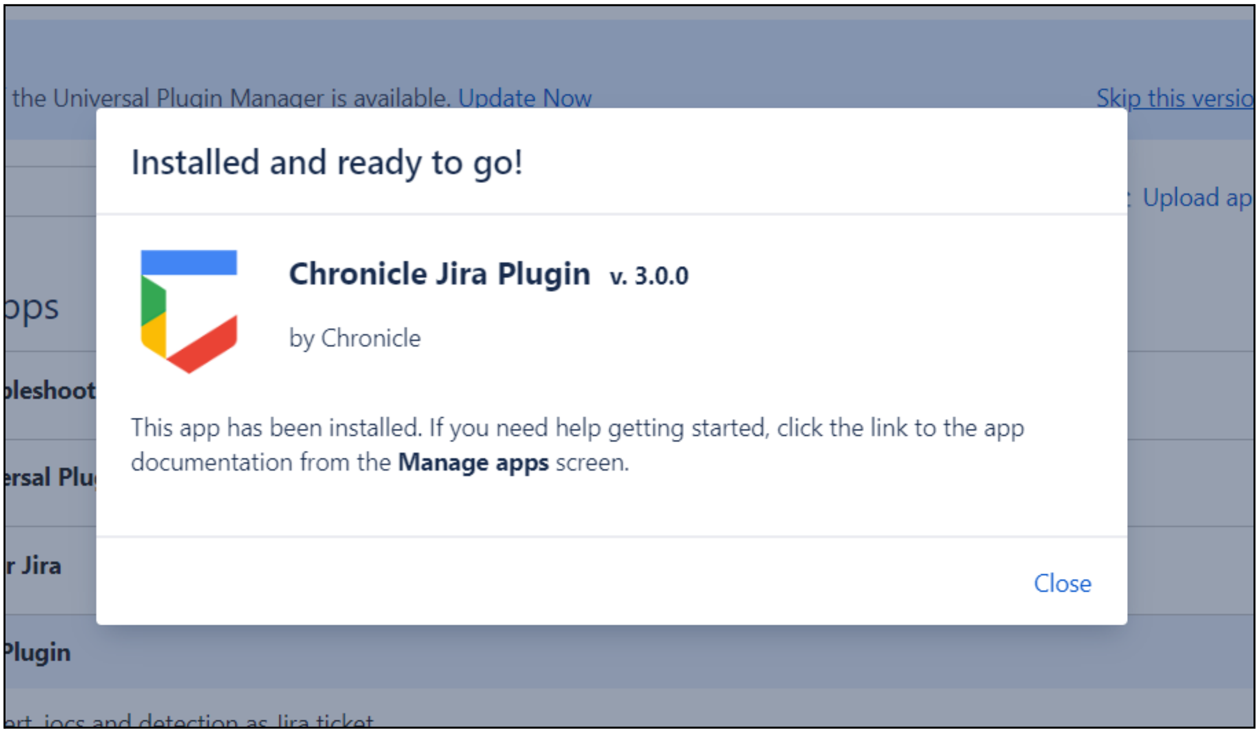
Installing

Installing Chronicle-Jira_Plugin-D-3.0.0.obr...

Downloading... Installing...

Chronicle App Confirmation

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



the Universal Plugin Manager is available. Update Now

Skip this versio

Upload ap

pps

oleshoot

ersal Plu

r Jira

Plugin

ert, iocs and detection as Jira ticket

Installed and ready to go!

Chronicle Jira Plugin v. 3.0.0

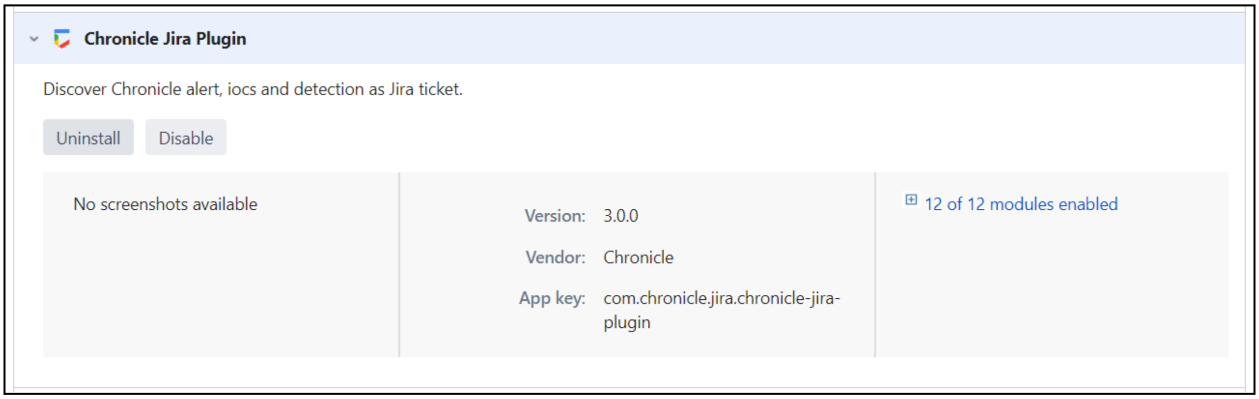
by Chronicle

This app has been installed. If you need help getting started, click the link to the app documentation from the **Manage apps** screen.

Close

Listing of Chronicle App

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



Chronicle Jira Plugin

Discover Chronicle alert, iocs and detection as Jira ticket.

Uninstall Disable

No screenshots available

Version: 3.0.0

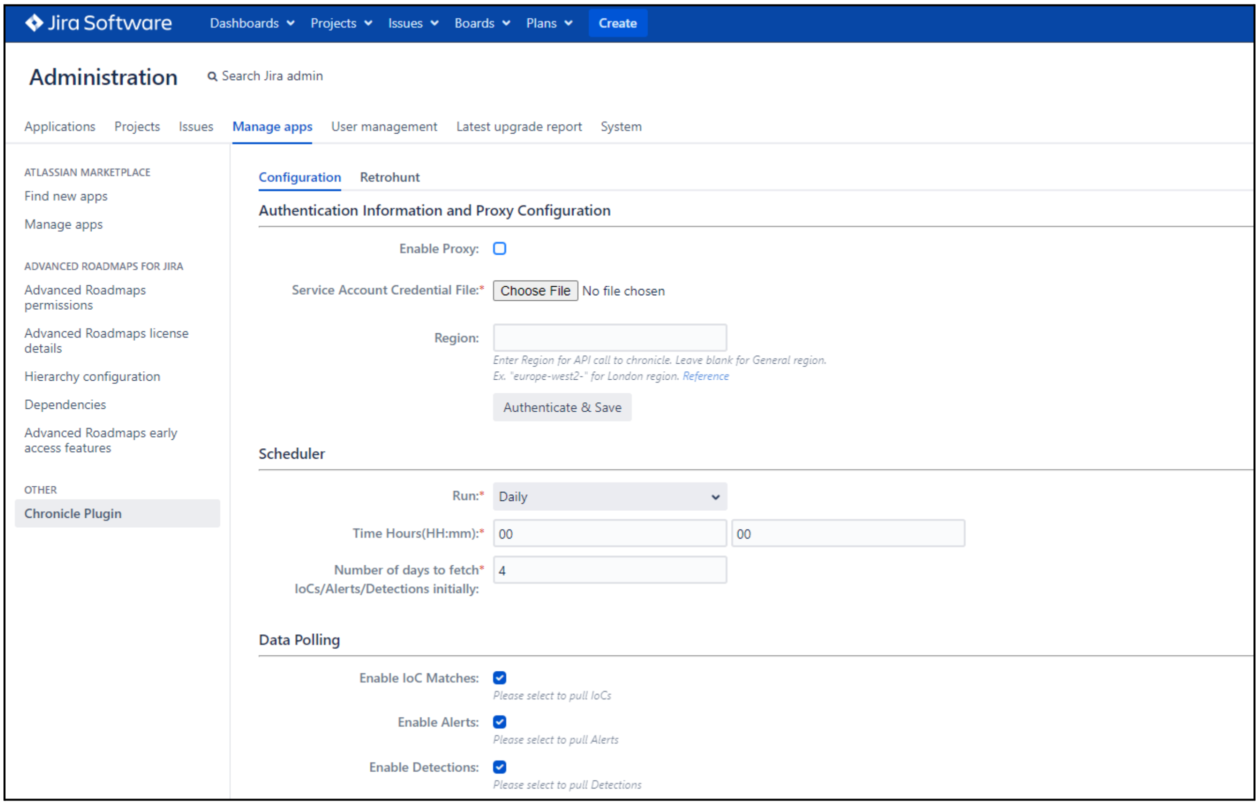
Vendor: Chronicle

App key: com.chronicle.jira.chronicle-jira-plugin

12 of 12 modules enabled

Chronicle App Config Page Confirmation

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



Authentication Information and Proxy Configuration

Enable Proxy: □

Service Account Credential File:* Choose File No file chosen

Region:

Enter Region for API call to chronicle. Leave blank for General region. Ex. "europe-west2-" for London region. Reference

Authenticate & Save

Scheduler

Run:* Daily

Time Hours(HH:mm):* 00 00

Number of days to fetch IoCs/Alerts/Detections initially:* 4

Data Polling

Enable IoC Matches: ☑ *Please select to pull IoCs*

Enable Alerts: ☑ *Please select to pull Alerts*

Enable Detections: ☑ *Please select to pull Detections*

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

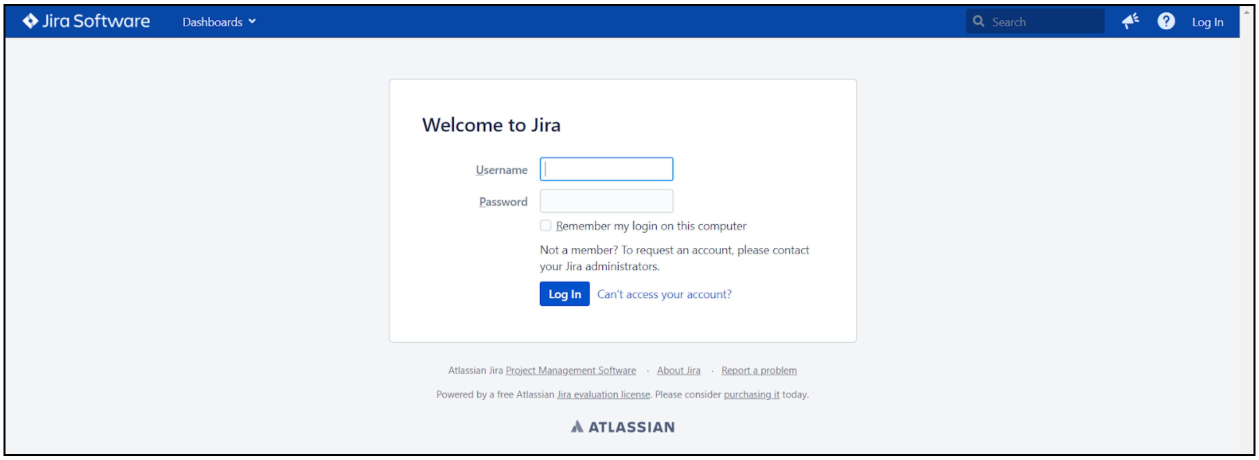
Installing the app from the marketplace

- 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 **Chronicle JIRA App** in the Search the Marketplace search bar and click Enter.
- **Chronicle JIRA App** will be available in the marketplace based on the search from where the user would be able to install the app.

Un-installation Instructions

Login Page

Enter the Jira admin credentials and click on Log In



Welcome to Jira

Username

Password

□ Remember my login on this computer

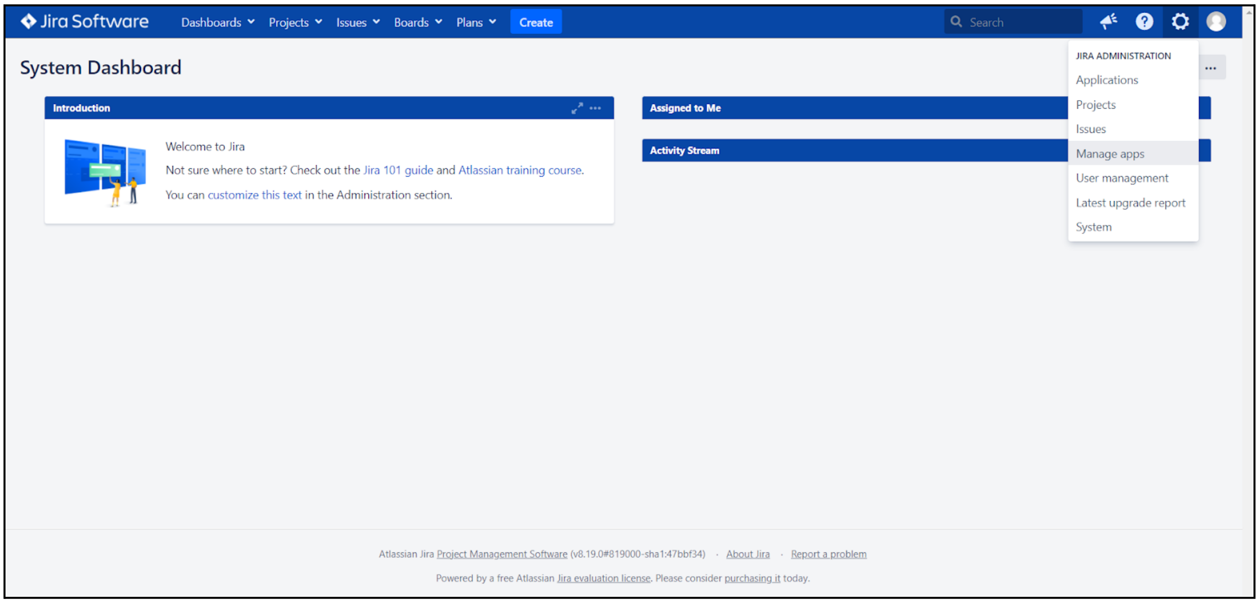
Not a member? To request an account, please contact your Jira administrators.

Atlassian Jira Project Management Software · About Jira · Report a problem

Powered by a free Atlassian Jira evaluation license. Please consider purchasing it today.

Goto Manage Apps

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



System Dashboard

Welcome to Jira

Not sure where to start? Check out the Jira 101 guide and Atlassian training course.

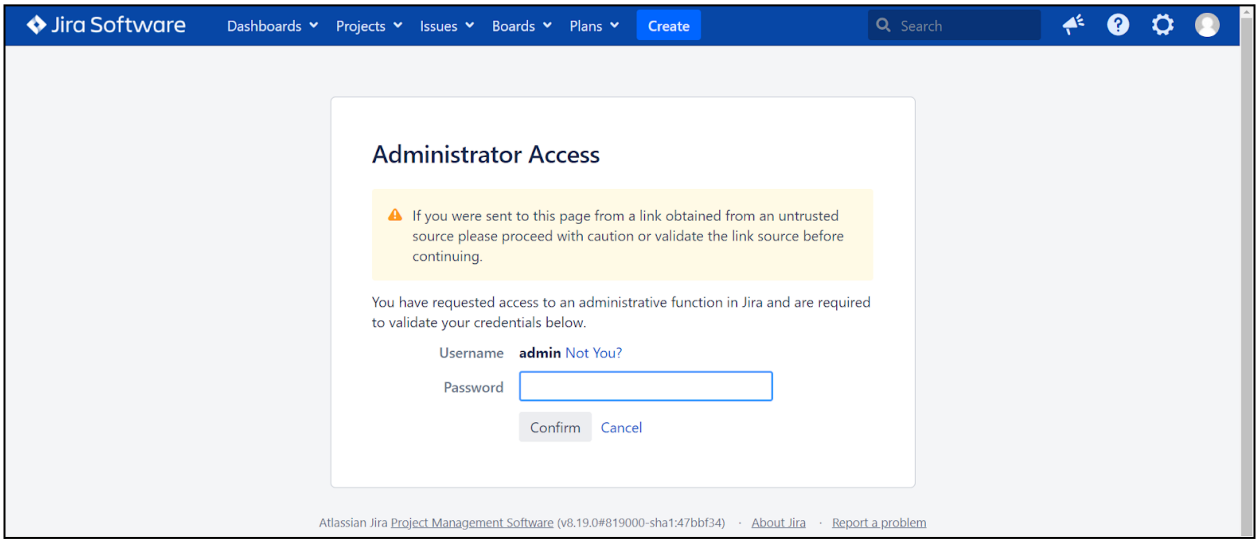
You can customize this text in the Administration section.

Atlassian Jira Project Management Software (v8.19.0#819000-sha1:47bbf34) · About Jira · Report a problem

Powered by a free Atlassian Jira evaluation license. Please consider purchasing it today.

Password for the Administrator Access

Enter the Jira Administrator Access credentials and click on Confirm.



Administrator Access

If you were sent to this page from a link obtained from an untrusted source please proceed with caution or validate the link source before continuing.

You have requested access to an administrative function in Jira and are required to validate your credentials below.

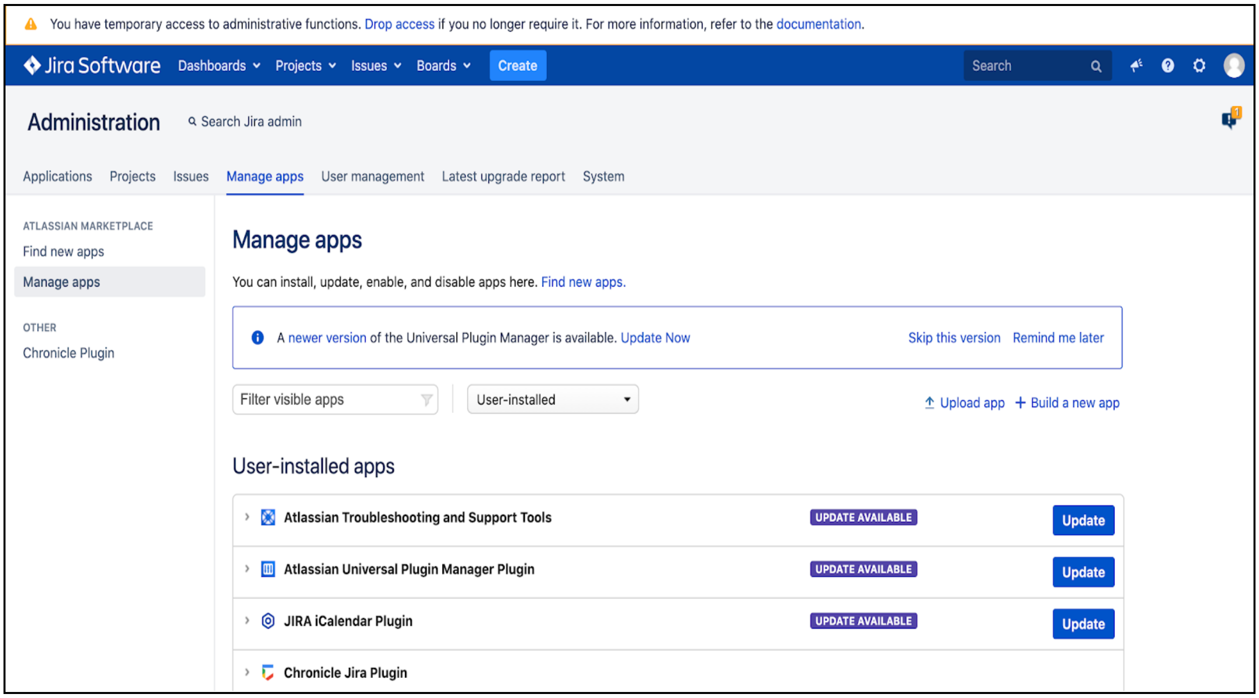
Username admin Not You?

Password

Atlassian Jira Project Management Software (v8.19.0#819000-sha1:47bbf34) · About Jira · Report a problem

Manage Apps Page

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


You have temporary access to administrative functions. Drop access if you no longer require it. For more information, refer to the documentation.

Manage apps

You can install, update, enable, and disable apps here. Find new apps.

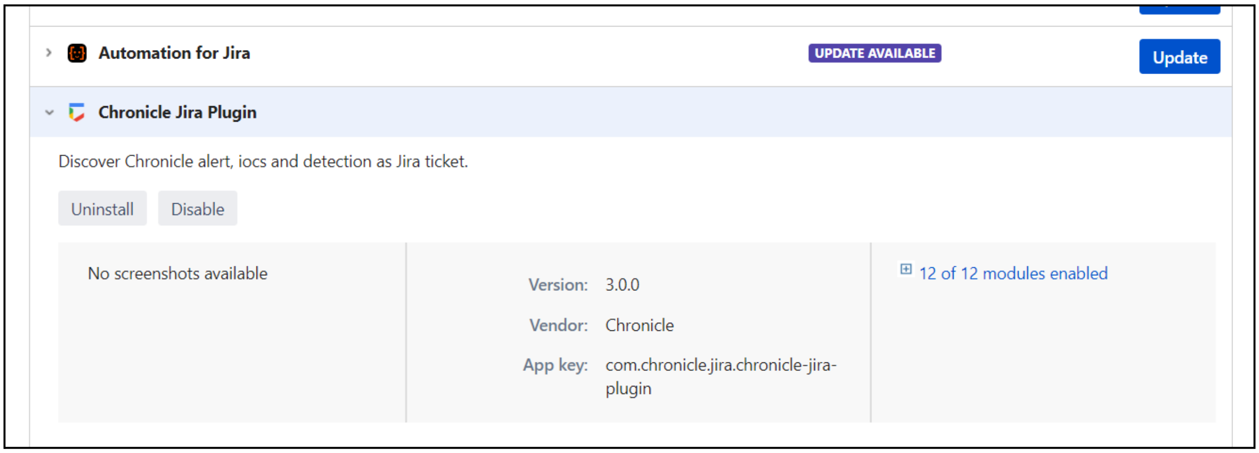
A newer version of the Universal Plugin Manager is available. Update Now Skip this version Remind me later

User-installed apps

Atlassian Troubleshooting and Support Tools	UPDATE AVAILABLE	Update
Atlassian Universal Plugin Manager Plugin	UPDATE AVAILABLE	Update
JIRA iCalendar Plugin	UPDATE AVAILABLE	Update
Chronicle Jira Plugin		

Search Chronicle Jira Plugin

Search and Expand the Chronicle Jira Plugin and click Uninstall.



Discover Chronicle alert, iocs and detection as Jira ticket.

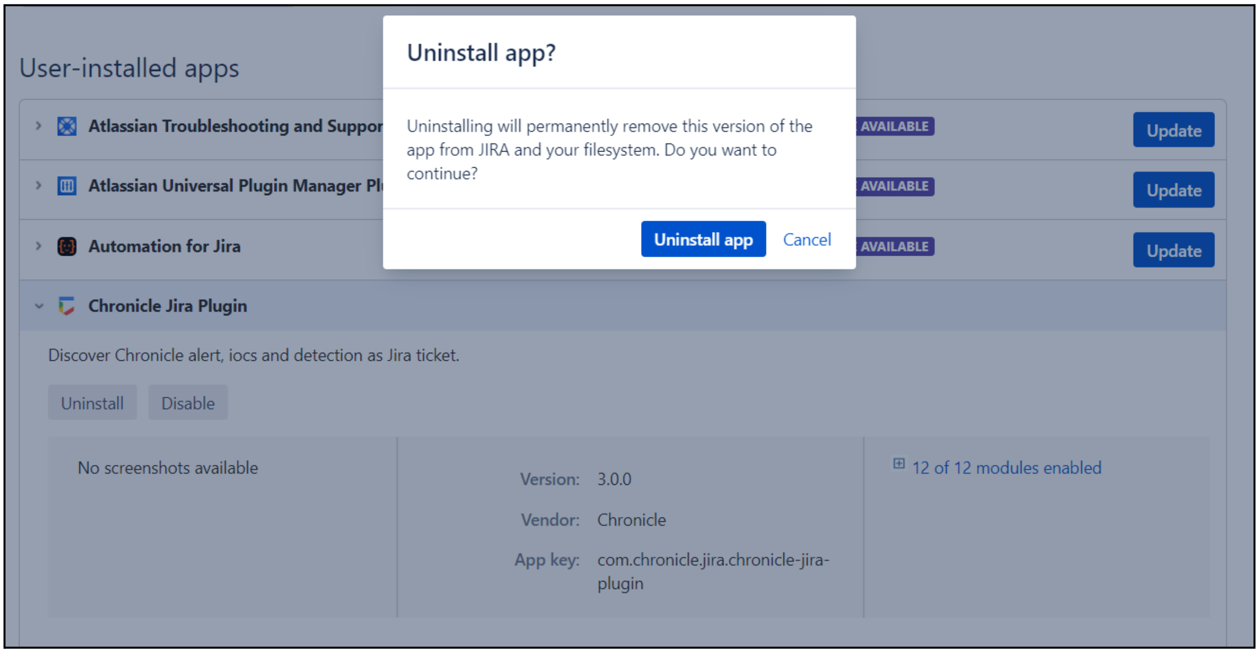
Version: 3.0.0

Vendor: Chronicle

App key: com.chronicle.jira.chronicle-jira-plugin

Uninstallation Confirmation

Click on the Uninstall all button to uninstall the Chronicle Plugin.



Uninstall app?

Uninstalling will permanently remove this version of the app from JIRA and your filesystem. Do you want to continue?

Discover Chronicle alert, iocs and detection as Jira ticket.

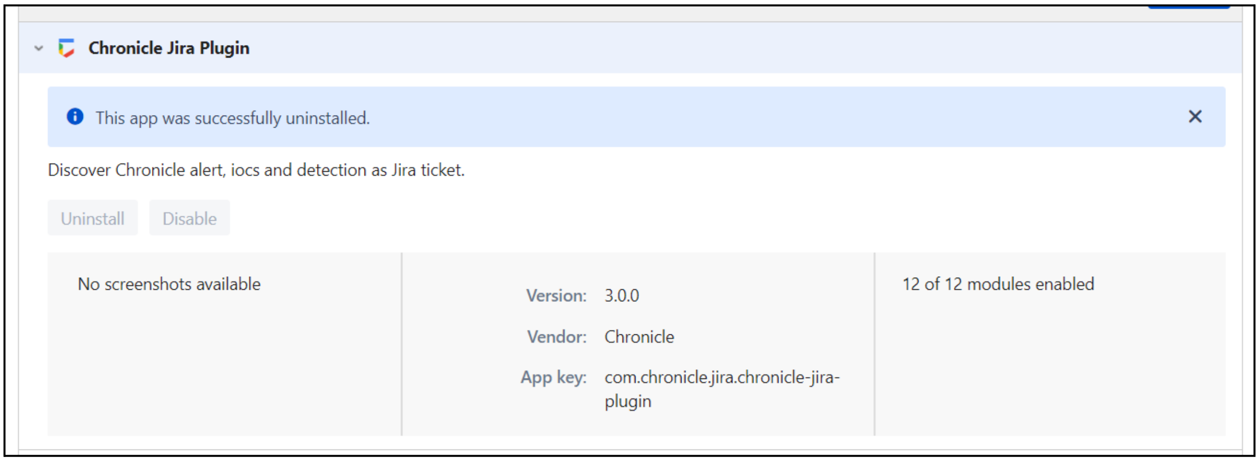
Version: 3.0.0

Vendor: Chronicle

App key: com.chronicle.jira.chronicle-jira-plugin

Uninstallation Successful

Below screenshot will be displayed upon successful uninstallation.



This app was successfully uninstalled.

Discover Chronicle alert, iocs and detection as Jira ticket.

No screenshots available

Version: 3.0.0

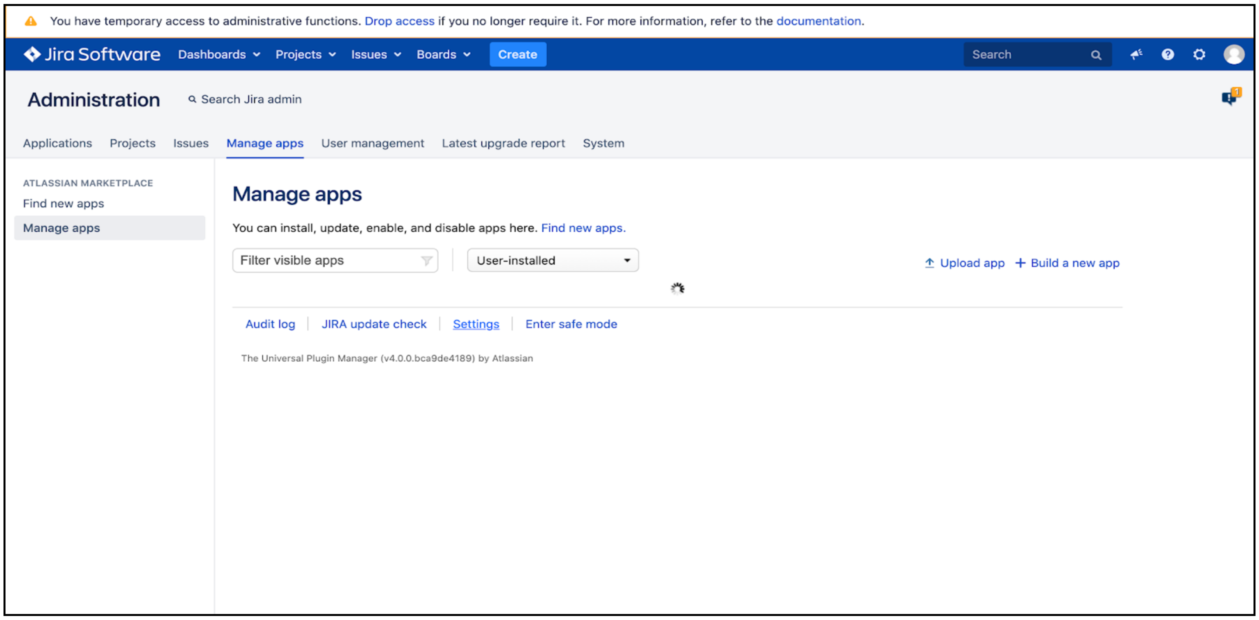
Vendor: Chronicle

App key: com.chronicle.jira.chronicle-jira-plugin

12 of 12 modules enabled

Confirm the Uninstallation

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



You have temporary access to administrative functions. Drop access if you no longer require it. For more information, refer to the documentation.

Manage apps

You can install, update, enable, and disable apps here. Find new apps.

The Universal Plugin Manager (v4.0.0.bca9de4189) by Atlassian

User Manual

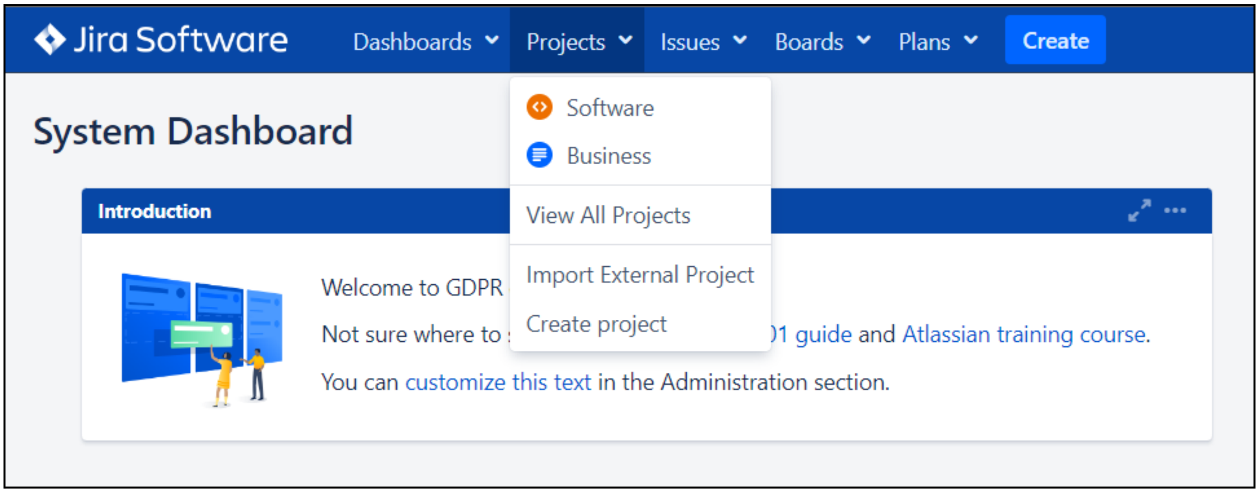
This section will cover the step-by-step process for configuring the Chronicle App. The Chronicle App offers the following functionality:

1. Types of scheduler settings, that enables users to select how frequently the data needs to be collected from the chronicle.
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. Show the last job run date and time, which enables the user to understand when the last successful job was executed.
6. Custom Issue types, through which the tickets can be identified whether the tickets are of IoC, Alerts and Detections.
7. Enrichment, 5 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
8. 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”.
9. 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 Chronicle Template

This section will go through the process of Project Creation with the chronicle template. It is important to do this, even before starting with the configuration of the app. As the Project that is created with the chronicle 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 chronicle to the jira fields

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

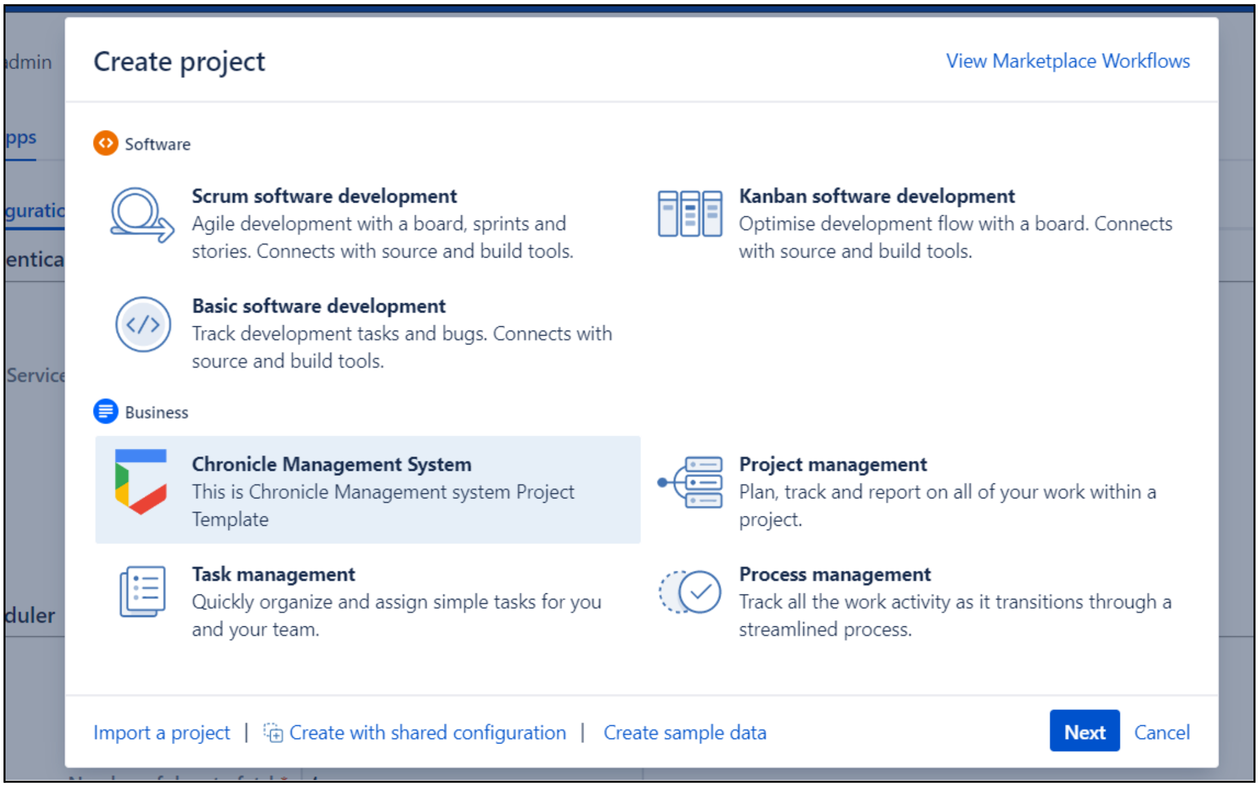


Welcome to GDPR

Not sure where to s 01 guide and Atlassian training course.

You can customize this text in the Administration section.

Select **Chronicle Management System** from the Create project popup to create the customized chronicle project.



Scrum software development
Agile development with a board, sprints and stories. Connects with source and build tools.

Kanban software development
Optimise development flow with a board. Connects with source and build tools.

Basic software development
Track development tasks and bugs. Connects with source and build tools.

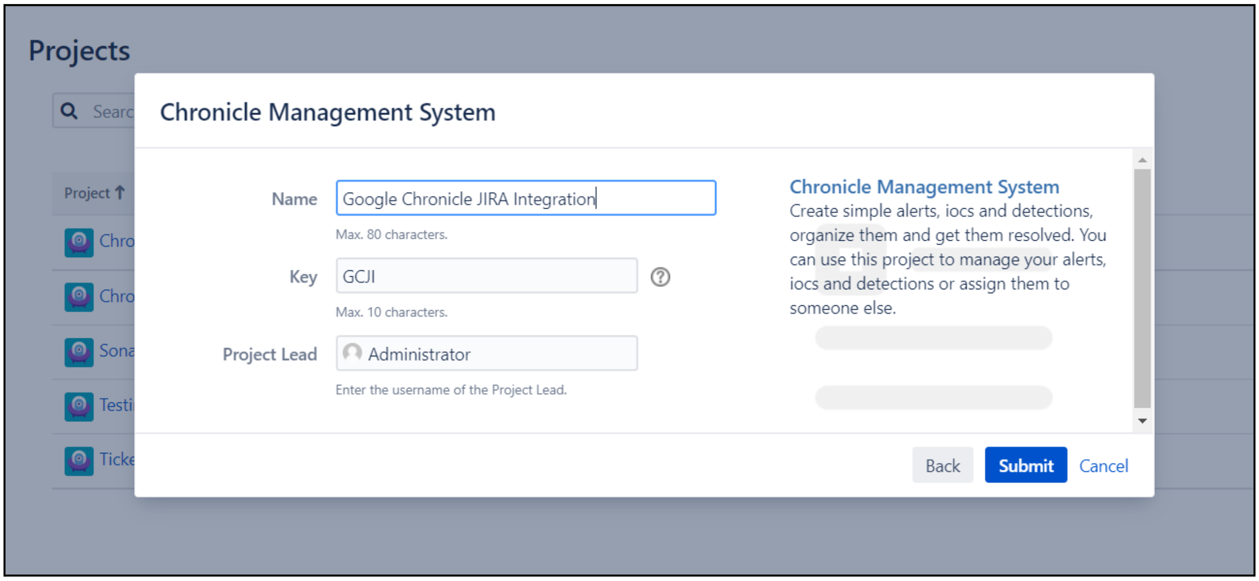
Chronicle Management System
This is Chronicle Management system Project Template

Project management
Plan, track and report on all of your work within a project.

Task management
Quickly organize and assign simple tasks for you and your team.

Process management
Track all the work activity as it transitions through a streamlined process.

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.



Chronicle Management System

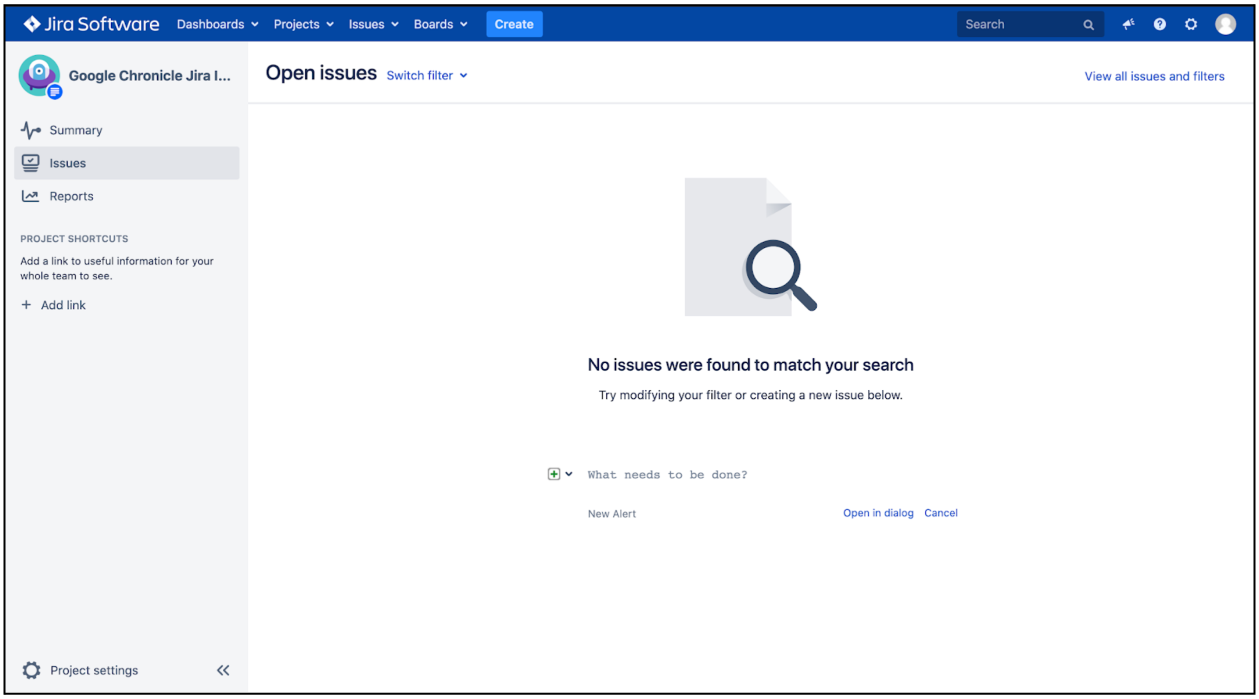
Name: Google Chronicle JIRA Integration
Max. 80 characters.

Key: GCJI
Max. 10 characters.

Project Lead: Administrator
Enter the username of the Project Lead.

Chronicle Management System
Create simple alerts, iocs and detections, organize them and get them resolved. You can use this project to manage your alerts, iocs and detections or assign them to someone else.

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



Open issues

No issues were found to match your search

Try modifying your filter or creating a new issue below.

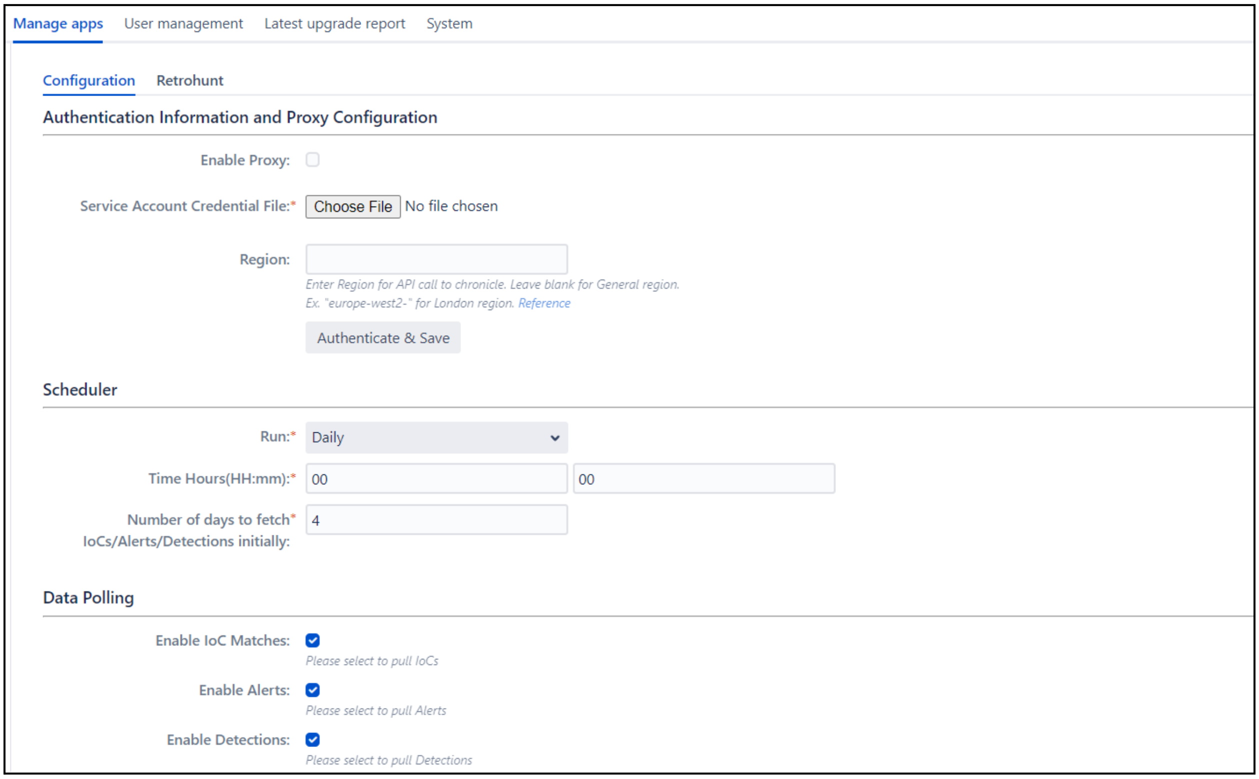
What needs to be done?

New Alert

App Configuration

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

App Configuration Page with Default Values and fields usage



Authentication Information and Proxy Configuration

Enable Proxy: □

Service Account Credential File:* Choose File No file chosen

Region:

Enter Region for API call to chronicle. Leave blank for General region.
Ex. "europe-west2-" for London region. Reference

Scheduler

Run:* Daily

Time Hours(HH:mm):* 00 00

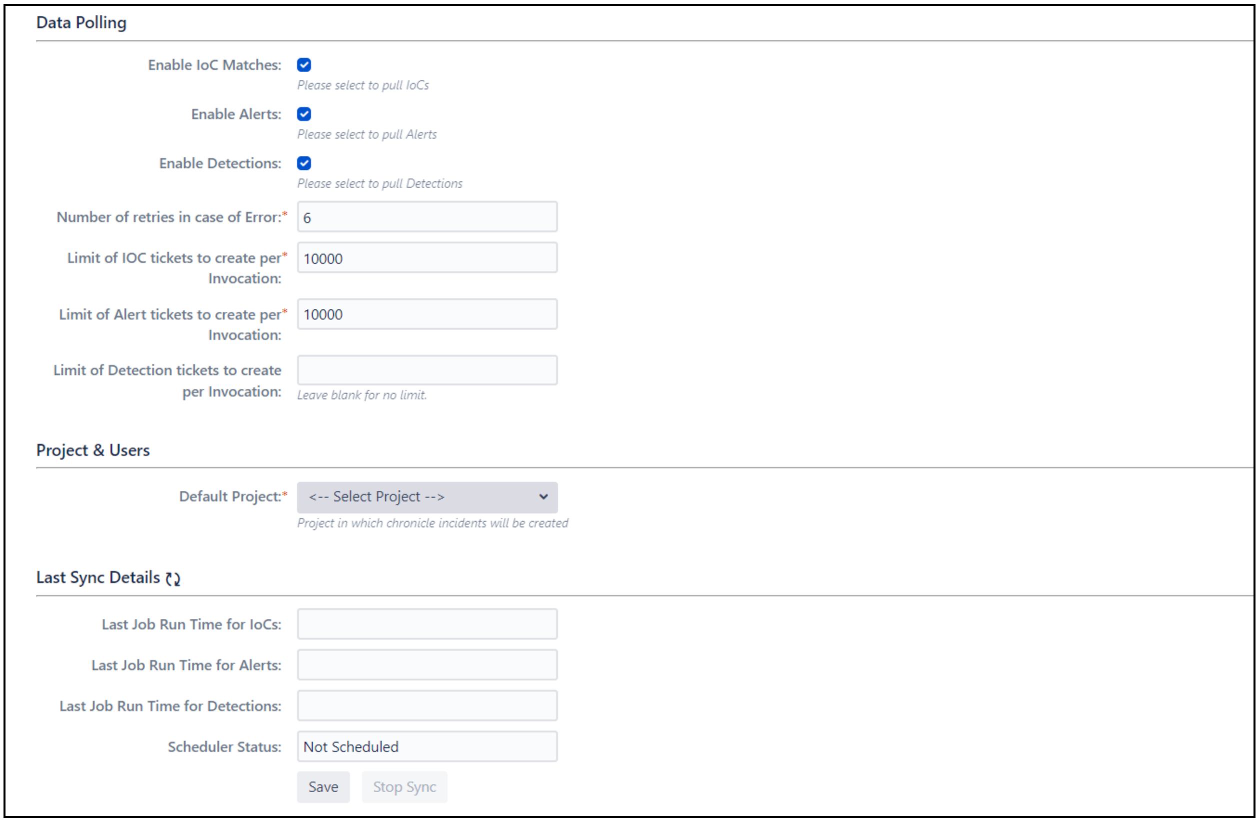
Number of days to fetch* IoCs/Alerts/Detections initially: 4

Data Polling

Enable IoC Matches: ☑
Please select to pull IoCs

Enable Alerts: ☑
Please select to pull Alerts

Enable Detections: ☑
Please select to pull Detections



Data Polling

Enable IoC Matches: ☑
Please select to pull IoCs

Enable Alerts: ☑
Please select to pull Alerts

Enable Detections: ☑
Please select to pull Detections

Number of retries in case of Error:* 6

Limit of IOC tickets to create per Invocation:* 10000

Limit of Alert tickets to create per Invocation:* 10000

Limit of Detection tickets to create per Invocation:
Leave blank for no limit.

Project & Users

Default Project:* <-- Select Project -->
Project in which chronicle incidents will be created

Last Sync Details

Last Job Run Time for IoCs:

Last Job Run Time for Alerts:

Last Job Run Time for Detections:

Scheduler Status: Not Scheduled

Below are 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 Chronicle account belongs.
Run (Dropdown)	How often the app needs to fetch the data from the Chronicle Instance. The total options that we get are Daily, Weekly, Monthly and Periodically.
Time Hours(HH:mm) (HH field picker) (mm	At what Time of the day that chronicle app

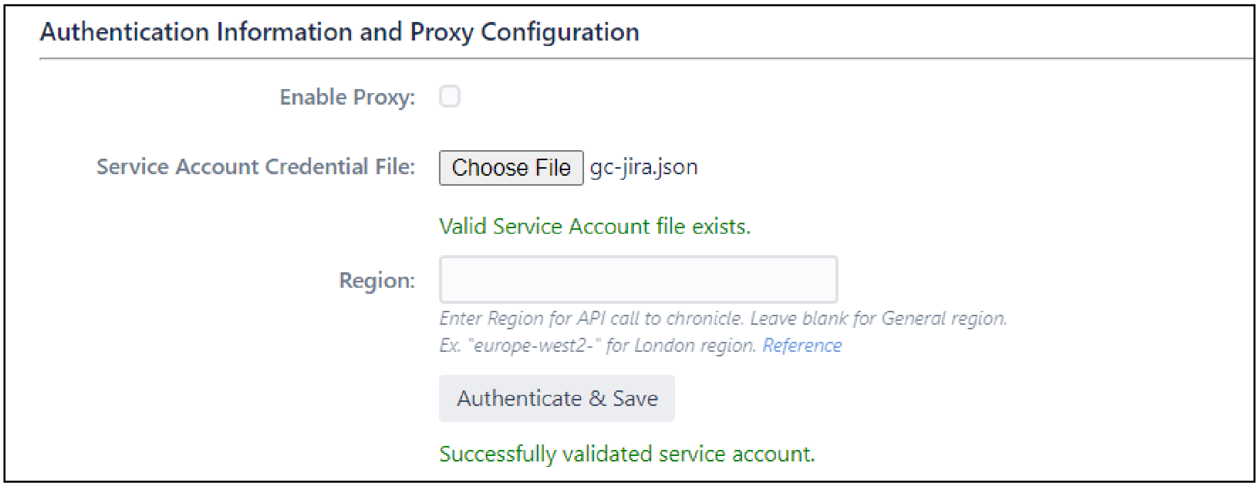
field picker)	should fetch the data from the chronicle instance. Time can be configured in Hours and Minutes. This field will only be visible for Daily, Weekly and Monthly.
Day (Dropdown for Weekly) (Day field picker for Monthly)	For the Weekly Run option, the Day dropdown list will have the day of the 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 chronicle app need to be fetched from the chronicle 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 Chronicle 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.
Enable Detections (Checkbox)	Upon checking, the app will create the Tickets for Detections.
The number of retries in case of Error (Number)	How many times the app should retry Chronicle API call in case of 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
Last Job Run Time for IoCs (Read-only text box)	Last successful job run time for fetching the IoCs from chronicle instance.

Last Job Run Time for Alerts (Read-only text box)	Last successful job run time for fetching the Alerts from chronicle instance.
Last Job Run Time for Detections (Read-only text box)	Last successful job run time for fetching the Detections from chronicle instance
Scheduler Status (Read-only text box)	This field displays the Status of the Job: ● Scheduled: Means the Job is currently scheduled and it will run based upon the configuration saved ● Not Scheduled: Means the Job is currently not scheduled and no API calls will be made to Chronicle
Next Job Run Time (Read-only text box)	When will the next call be made to chronicle.
Save (Button)	Save the configuration, with the confirmation box.
Stop Sync (Button)	Stop pulling the data from the chronicle.
Start Retrohunt (Button)	Open dialog 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)	End time for the time range of retrohunt
Refresh List (Button)	Refresh the list of retrohunts in 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 Chronicle team for the Authentication of the Chronicle API and provide the region to which the Chronicle 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.



Authentication Information and Proxy Configuration

Enable Proxy: □

Service Account Credential File: gc-jira.json

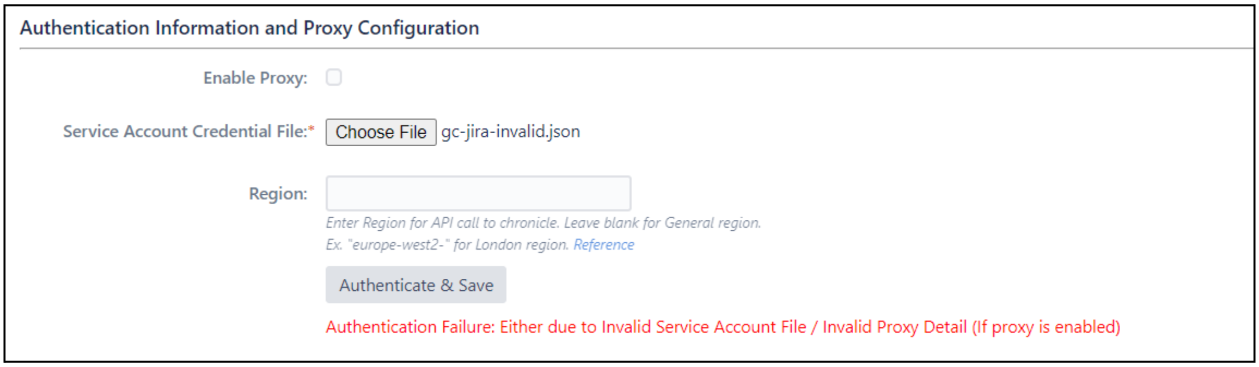
Valid Service Account file exists.

Region:

Enter Region for API call to chronicle. Leave blank for General region. Ex. "europe-west2-" for London region. Reference

Successfully validated service account.

- And on failure, it would show the appropriate failure message.



Authentication Information and Proxy Configuration

Enable Proxy: □

Service Account Credential File:* gc-jira-invalid.json

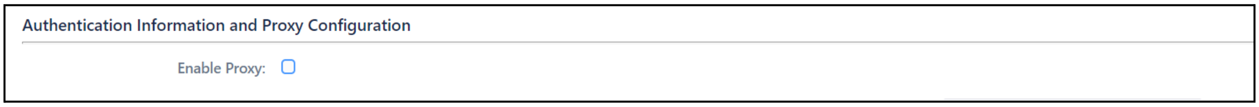
Region:

Enter Region for API call to chronicle. Leave blank for General region. Ex. "europe-west2-" for London region. Reference

Authentication Failure: Either due to Invalid Service Account File / Invalid Proxy Detail (If proxy is enabled)

Proxy Details: Default

- An optional provision will be available to configure the proxy server details in case the user wants the Chronicle 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.



Authentication Information and Proxy Configuration

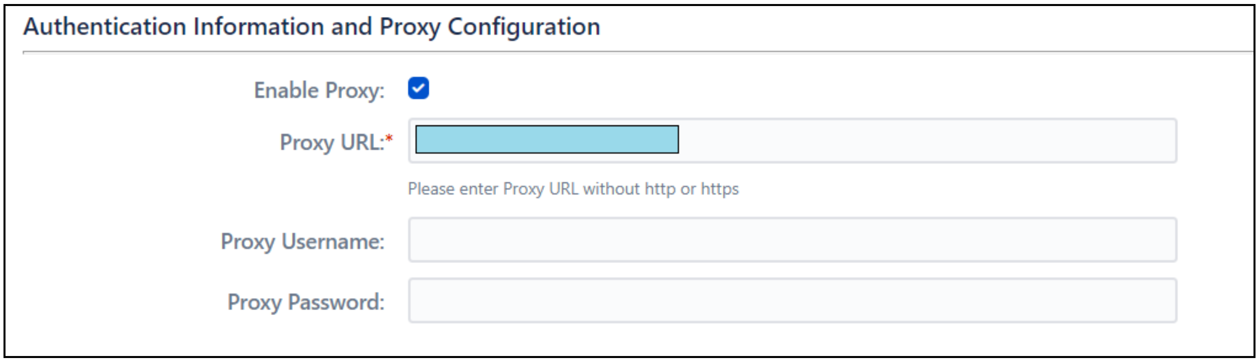
Enable Proxy: □

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 Chronicle 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.



Authentication Information and Proxy Configuration

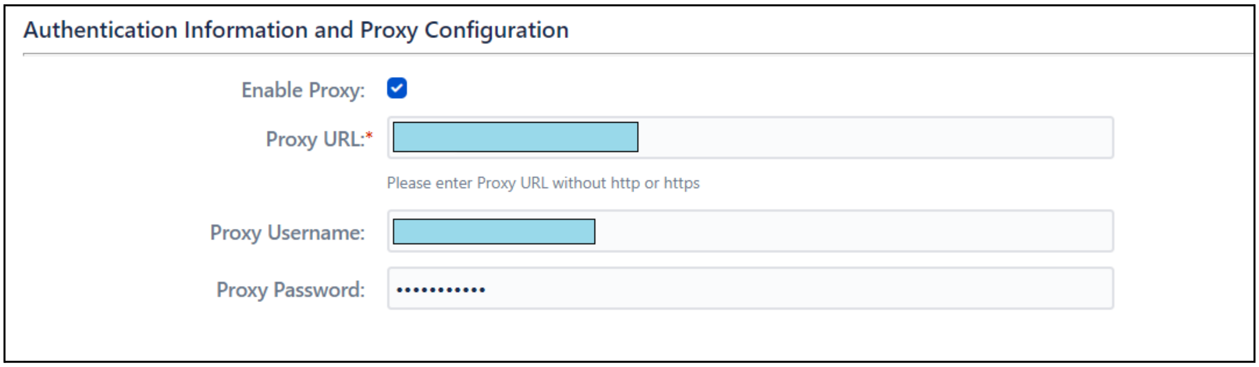
Enable Proxy: ☑

Proxy URL:* [redacted]

Please enter Proxy URL without http or https

Proxy Username:

Proxy Password:



Authentication Information and Proxy Configuration

Enable Proxy: ☑

Proxy URL:* [redacted]

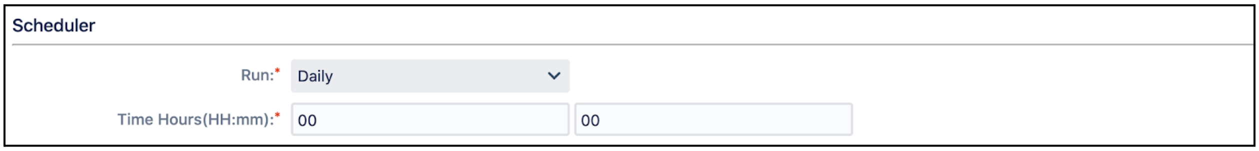
Please enter Proxy URL without http or https

Proxy Username: [redacted]

Proxy Password: ••••••••••••

Scheduler Daily

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



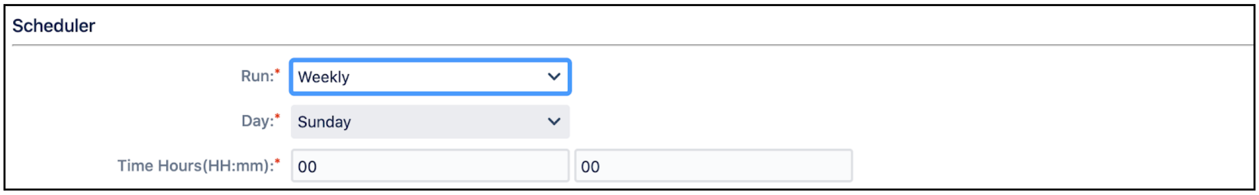
Scheduler

Run:* Daily

Time Hours(HH:mm):* 00 00

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

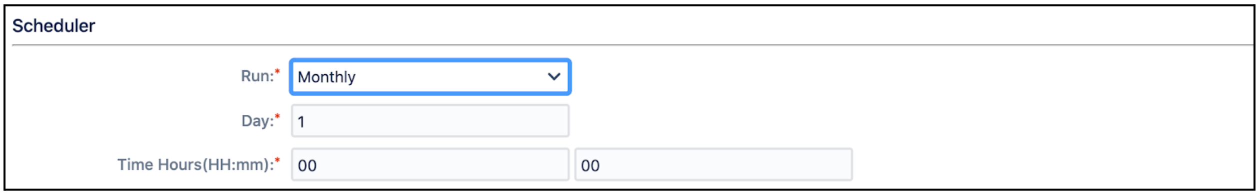
Run:* Weekly

Day:* Sunday

Time Hours(HH:mm):* 00 00

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

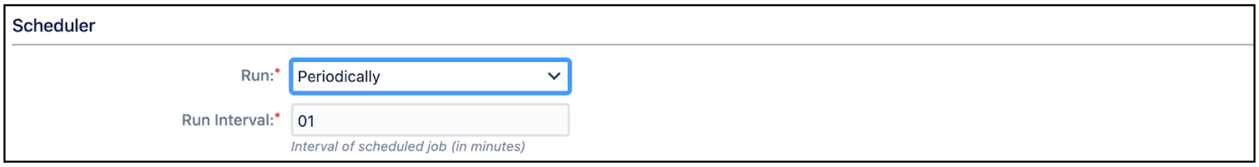
Run:* Monthly

Day:* 1

Time Hours(HH:mm):* 00 00

Scheduler Periodically

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



Scheduler

Run:* Periodically

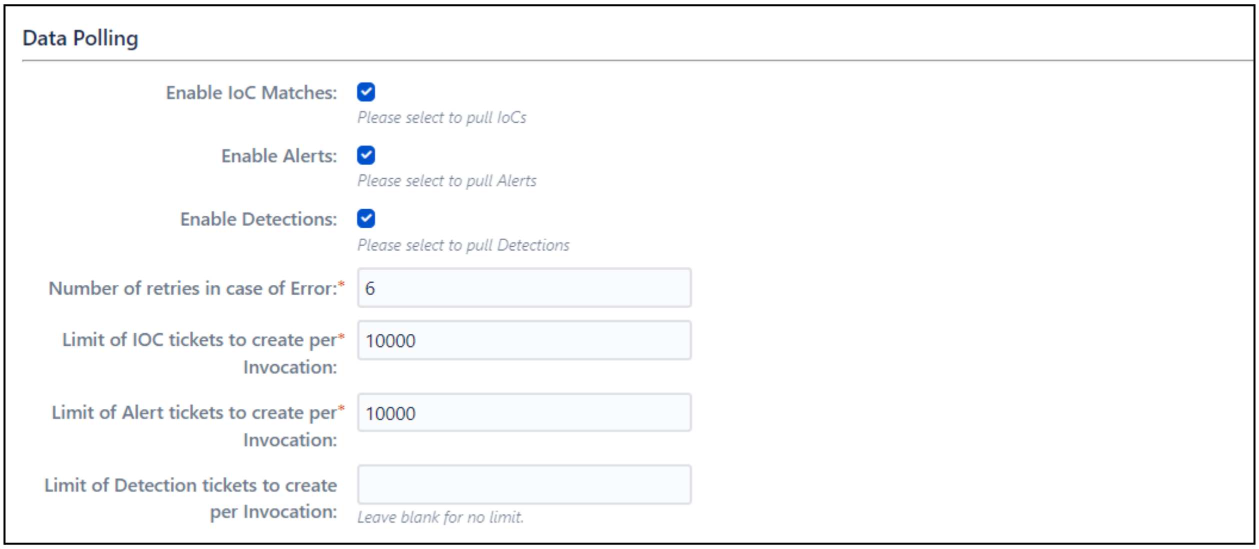
Run Interval:* 01

Interval of scheduled job (in minutes)

Data Polling: Default

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



Data Polling

Enable IoC Matches: ☑
Please select to pull IoCs

Enable Alerts: ☑
Please select to pull Alerts

Enable Detections: ☑
Please select to pull Detections

Number of retries in case of Error:* 6

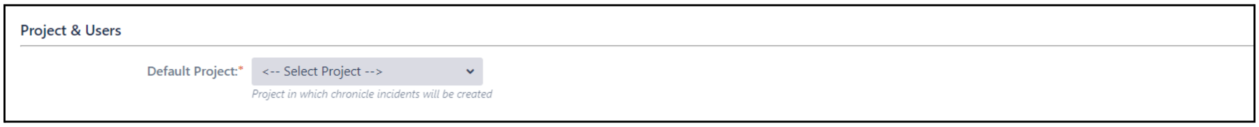
Limit of IOC tickets to create per Invocation:* 10000

Limit of Alert tickets to create per Invocation:* 10000

Limit of Detection tickets to create per Invocation:
Leave blank for no limit.

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 Chronicle Project creation template.

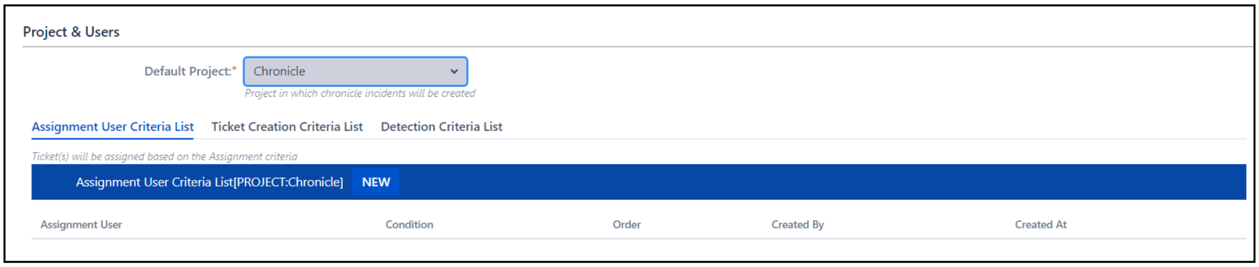


Project & Users

Default Project:* <-- Select Project -->
Project in which chronicle incidents will be created

Project & Users: When the project is selected

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



Project & Users

Default Project:* Chronicle
Project in which chronicle incidents will be created

Ticket(s) will be assigned based on the Assignment criteria

Assignment User Criteria List[PROJECT:Chronicle] NEW

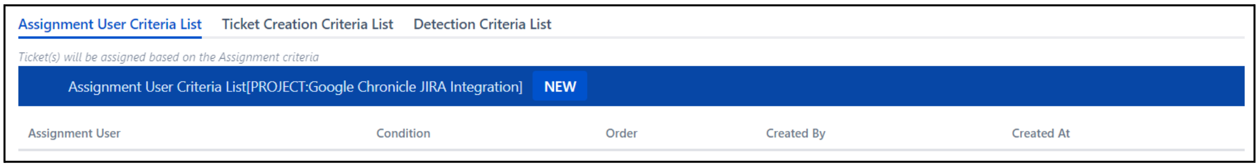
Assignment User	Condition	Order	Created By	Created At

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



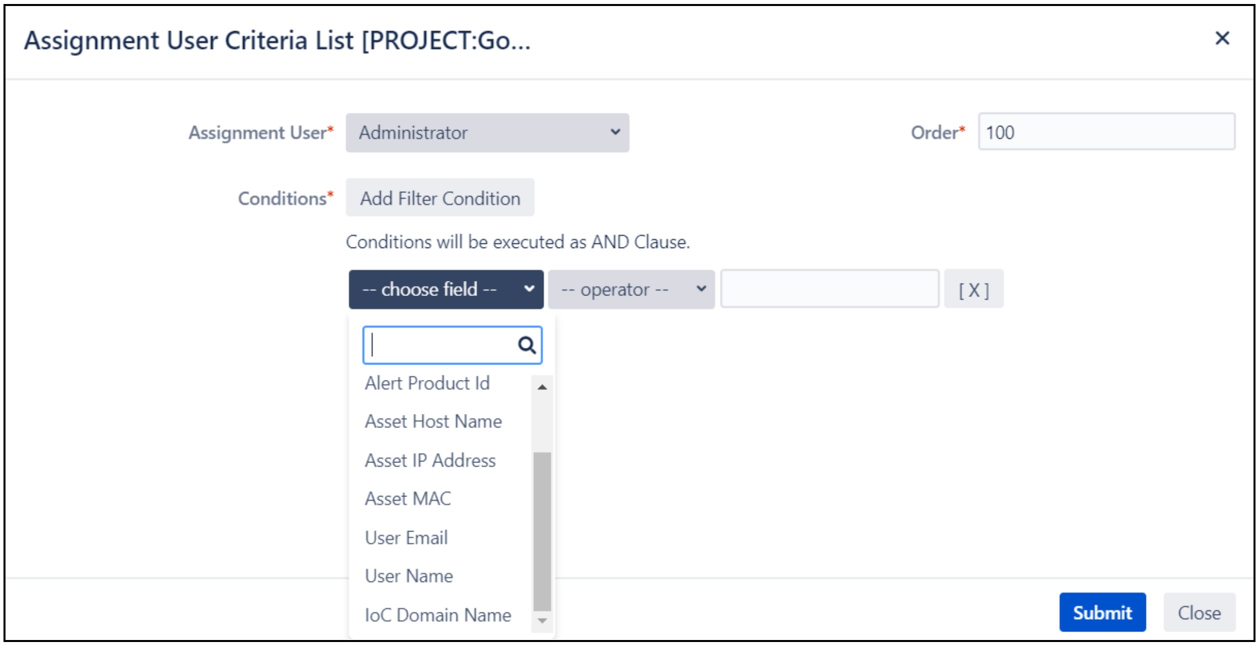
Ticket(s) will be assigned based on the Assignment criteria

Assignment User Criteria List[PROJECT:Google Chronicle JIRA Integration]

Assignment User	Condition	Order	Created By	Created At

User Assignment Criteria: Creation

- Assignment User needs to be part of either of the mentioned User Groups depending upon the Jira(on-prem) flavour is installed, along with the permission for the chronicle project that is created via the chronicle template.
  - Jira-administrators
  - Jira-software-users
  - Jira-service desk-users
- 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.



Assignment User Criteria List [PROJECT:Go...

Assignment User* Administrator

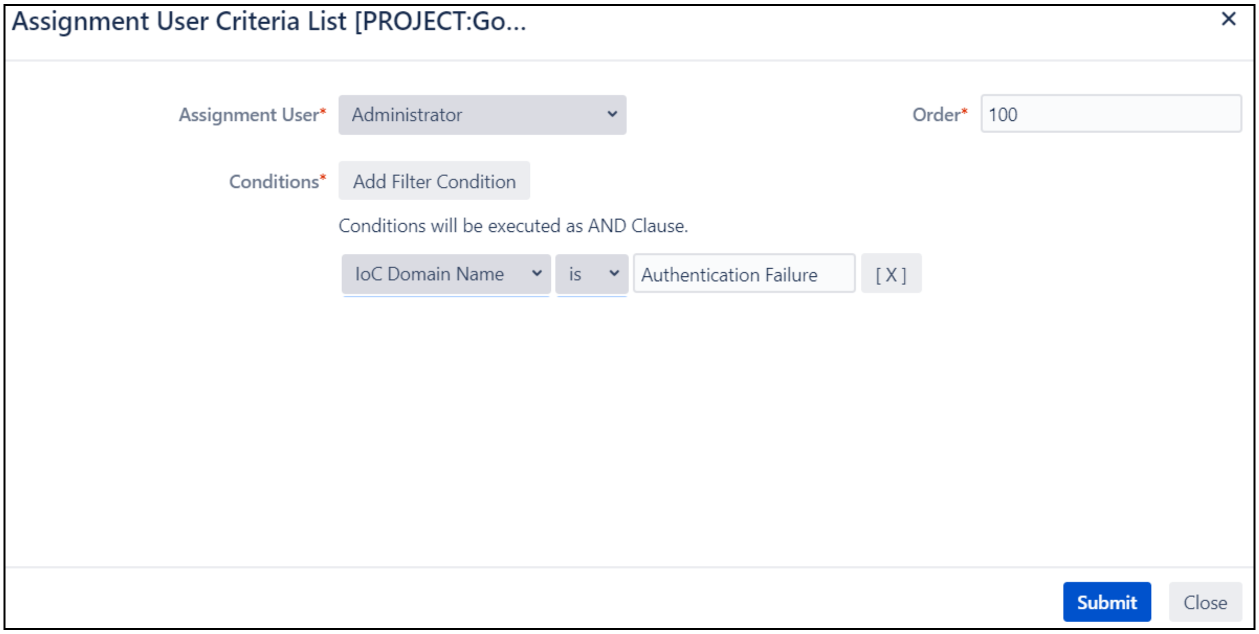
Order* 100

Conditions* Add Filter Condition

Conditions will be executed as AND Clause.

- 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 needs to be assigned to the user
Operator	Which condition that user wants to apply to filter out the data
Values	Enter the value that will satisfy with 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



Assignment User Criteria List [PROJECT:Go...

Assignment User*: Administrator

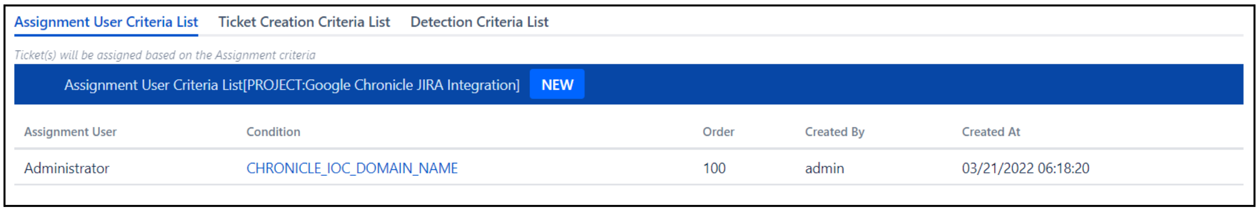
Order*: 100

Conditions*

Conditions will be executed as AND Clause.

IoC Domain Name | is | Authentication Failure

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



Ticket(s) will be assigned based on the Assignment criteria

Assignment User Criteria List[PROJECT:Google Chronicle JIRA Integration]

Assignment User	Condition	Order	Created By	Created At
Administrator	CHRONICLE_IOC_DOMAIN_NAME	100	admin	03/21/2022 06:18:20

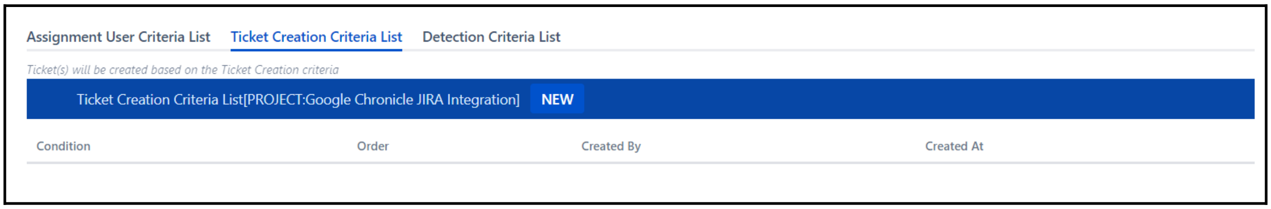
- So, as per this configuration, the user alert or asset alert tickets will have the alert name “Authentication Failure” will be assigned to the admin user.

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



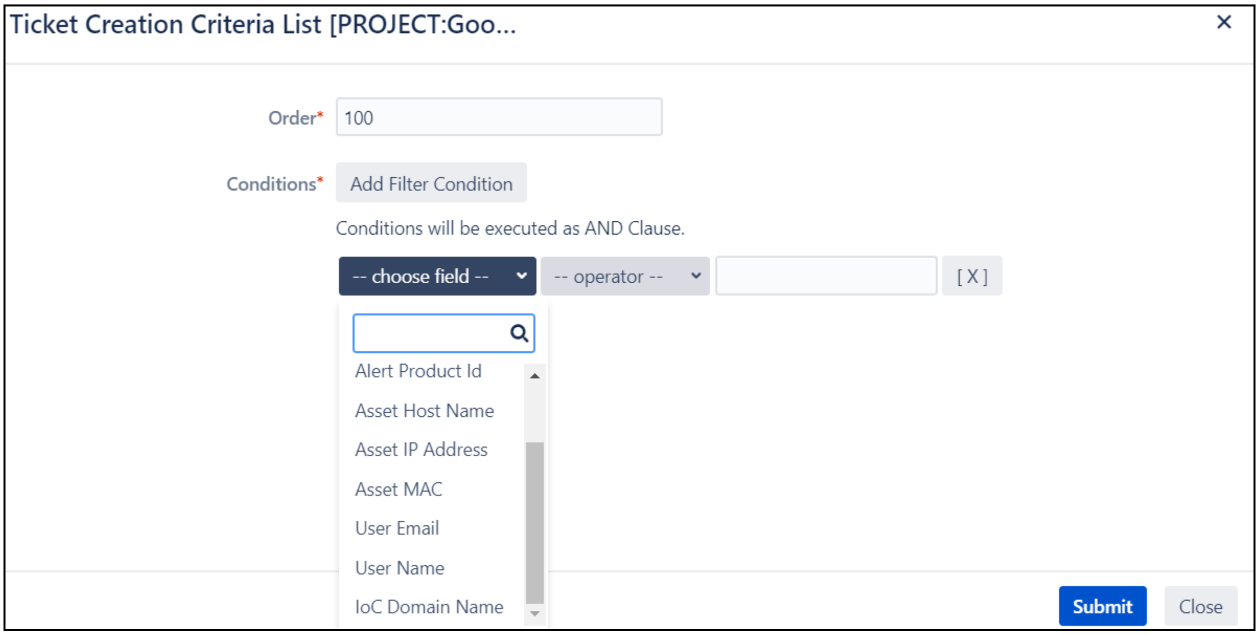
Ticket(s) will be created based on the Ticket Creation criteria

Ticket Creation Criteria List[PROJECT:Google Chronicle JIRA Integration]

Condition	Order	Created By	Created At

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 needs 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.



Ticket Creation Criteria List [PROJECT:Goo...

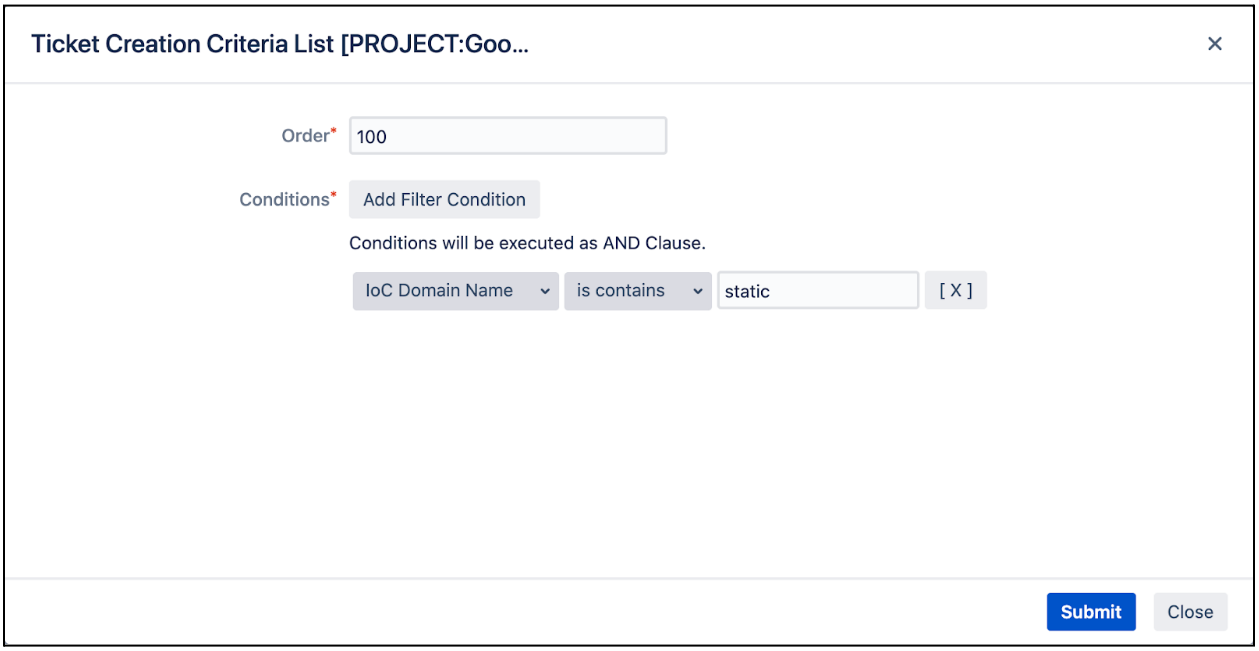
Order* 100

Conditions* Add Filter Condition

Conditions will be executed as AND Clause.

- 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 that user wants to apply to filter out the data
Values	Enter the value that will satisfy with 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



Ticket Creation Criteria List [PROJECT:Goo...

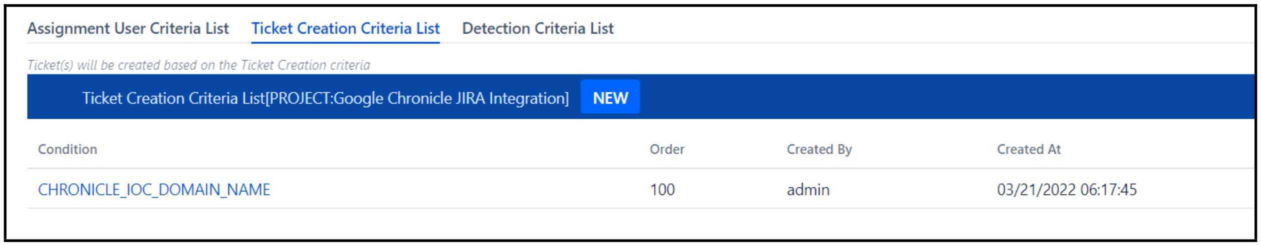
Order* 100

Conditions*

Conditions will be executed as AND Clause.

IoC Domain Name | is contains | static

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



Ticket(s) will be created based on the Ticket Creation criteria

Ticket Creation Criteria List[PROJECT:Google Chronicle JIRA Integration]

Condition	Order	Created By	Created At
CHRONICLE_IOC_DOMAIN_NAME	100	admin	03/21/2022 06:17:45

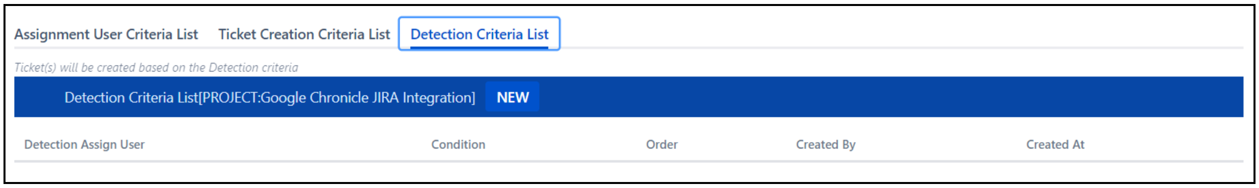
- So, as per this configuration, tickets will be created for IoC Domain matches which contain the phrase “static” in the domain name.

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.



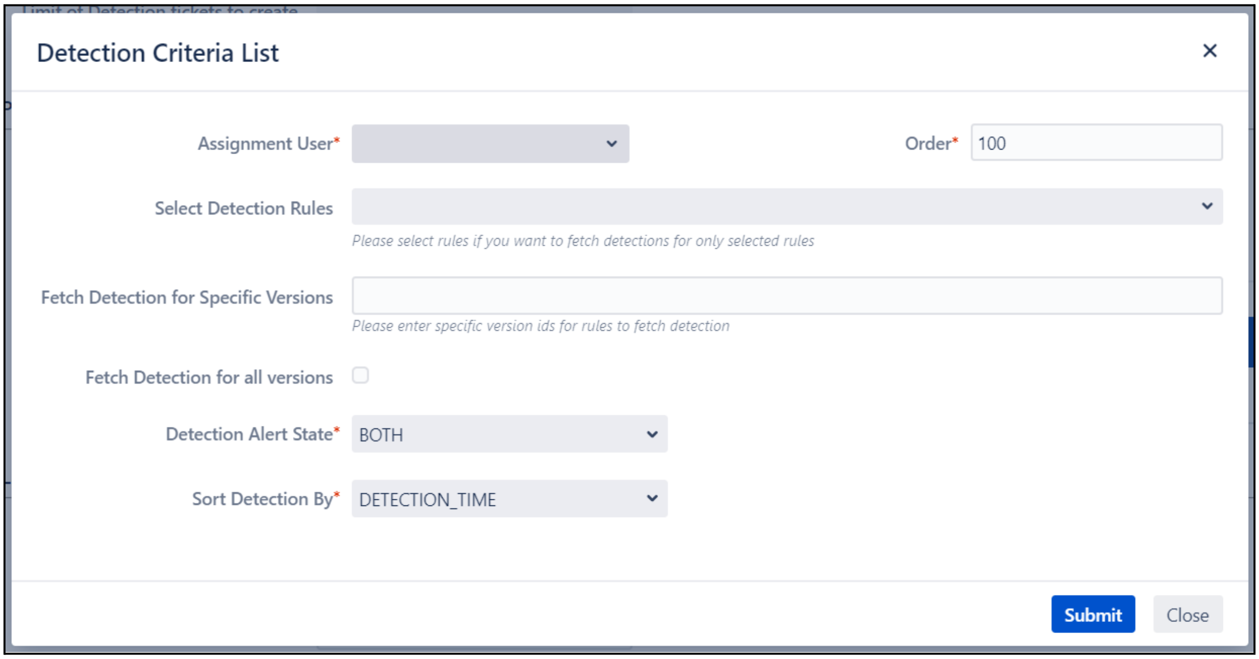
Ticket(s) will be created based on the Detection criteria

Detection Criteria List[PROJECT:Google Chronicle JIRA Integration] NEW

Detection Assign User	Condition	Order	Created By	Created At

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 needs 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.



Detection Criteria List

Assignment User*

Order* 100

Select Detection Rules

Please select rules if you want to fetch detections for only selected rules

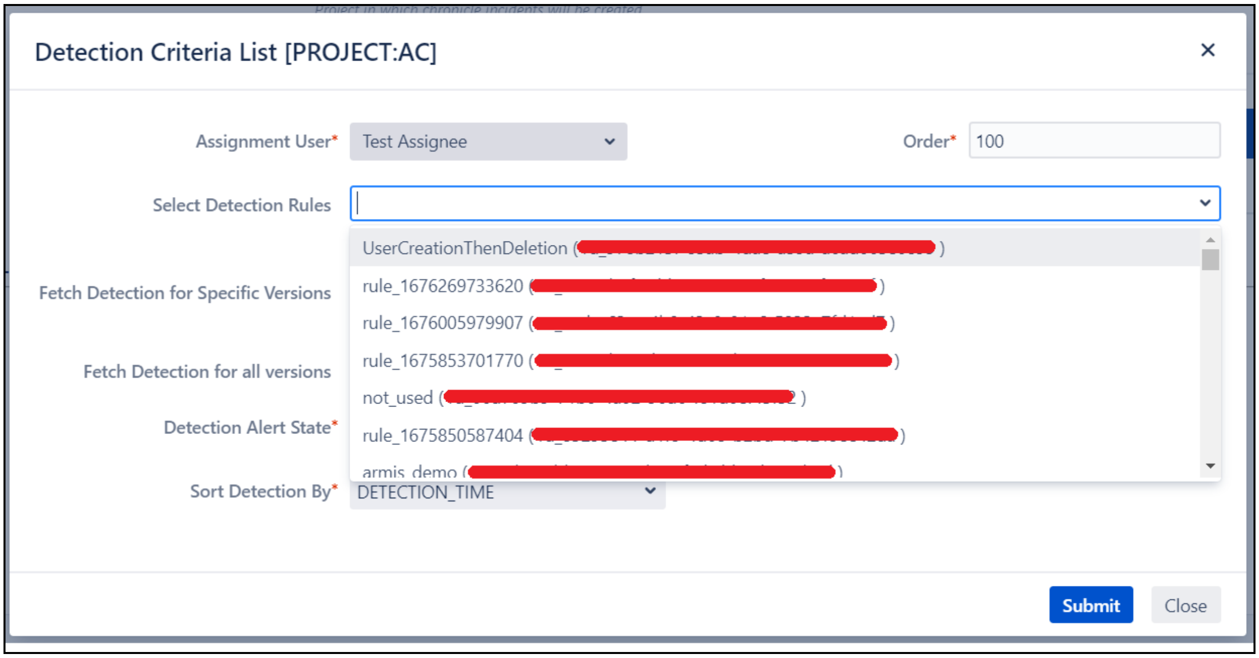
Fetch Detection for Specific Versions

Please enter specific version ids for rules to fetch detection

Fetch Detection for all versions □

Detection Alert State* BOTH

Sort Detection By* DETECTION_TIME



Project in which chronicle incidents will be created

Detection Criteria List [PROJECT:AC]

Assignment User*: Test Assignee

Order*: 100

Select Detection Rules:

- UserCreationThenDeletion ([redacted])
- rule_1676269733620 ([redacted])
- rule_1676005979907 ([redacted])
- rule_1675853701770 ([redacted])
- not_used ([redacted])
- rule_1675850587404 ([redacted])
- armis_demo ([redacted])

Fetch Detection for Specific Versions

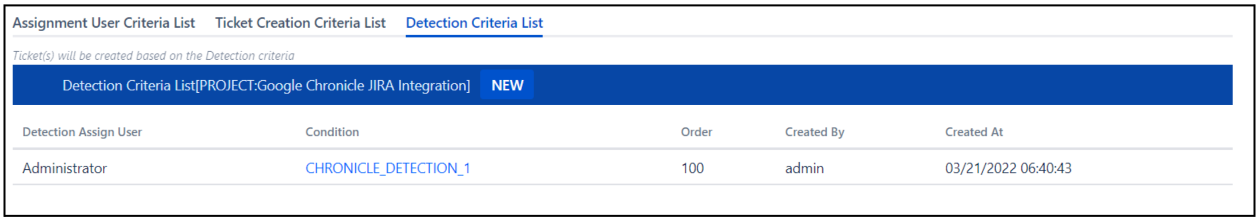
Fetch Detection for all versions

Detection Alert State*

Sort Detection By*: DETECTION_TIME

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 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 it will be displayed in the config screen as list below



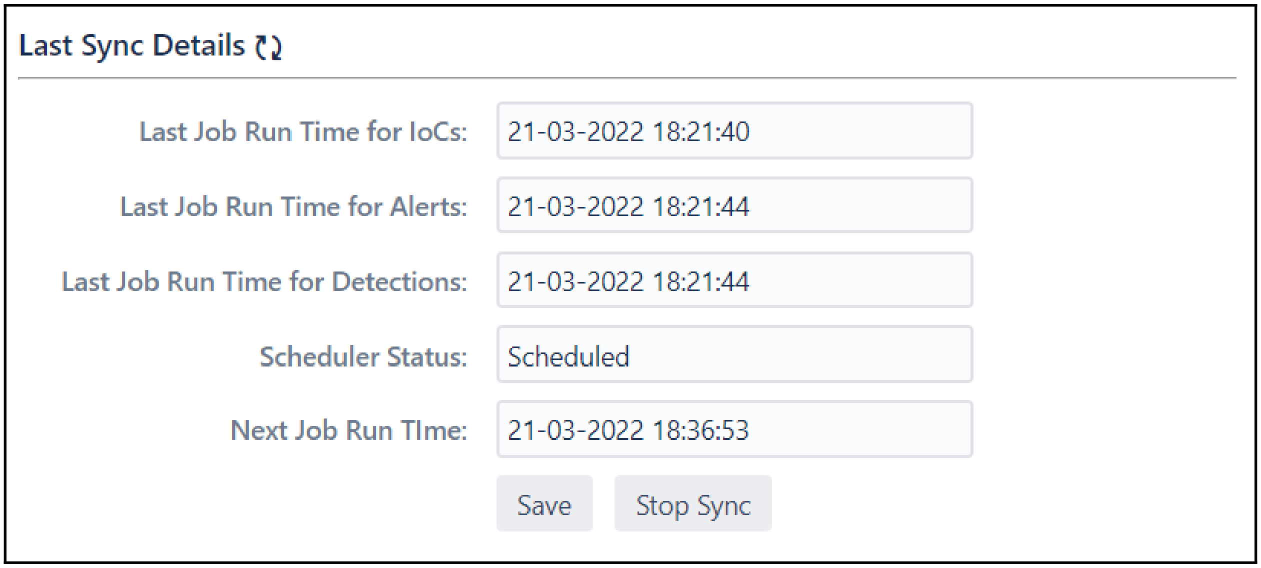
Ticket(s) will be created based on the Detection criteria

Detection Criteria List[PROJECT:Google Chronicle JIRA Integration]

Detection Assign User	Condition	Order	Created By	Created At
Administrator	CHRONICLE_DETECTION_1	100	admin	03/21/2022 06:40:43

Last Sync Details

- Upon Clicking Save, the scheduler will trigger the Job to fetch the data from Chronicle 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 and 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 Chronicle.
- Next Job Run Time: The Date and time for the next scheduled job run.

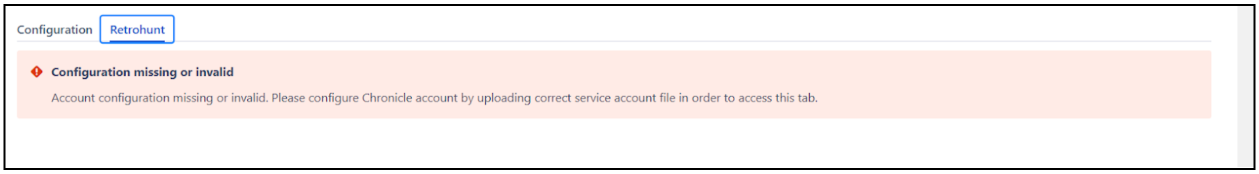


Last Sync Details

Last Job Run Time for IoCs:	21-03-2022 18:21:40
Last Job Run Time for Alerts:	21-03-2022 18:21:44
Last Job Run Time for Detections:	21-03-2022 18:21:44
Scheduler Status:	Scheduled
Next Job Run TIme:	21-03-2022 18:36:53

Retrohunt

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



Configuration missing or invalid

Account configuration missing or invalid. Please configure Chronicle account by uploading correct service account file in order to access this tab.

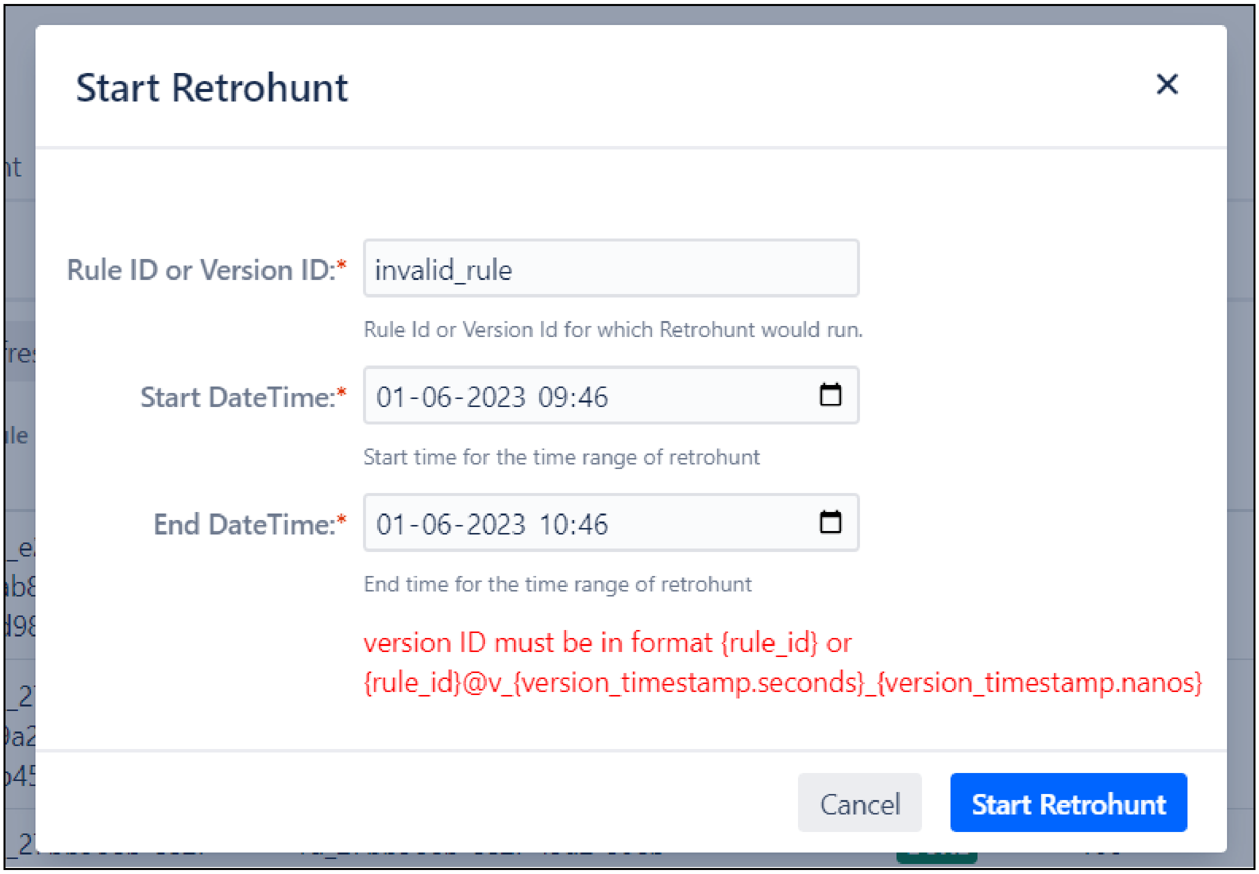
If the user has already done the Chroncile authentication then the below screen would be displayed with options to start/cancel the retrohunt and see a list of retrohunts created earlier as the table view.

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 of any error occurred while starting the new retrohunt, the Error message will be displayed as shown below.



Start Retrohunt

Rule ID or Version ID:* invalid_rule

Rule Id or Version Id for which Retrohunt would run.

Start DateTime:* 01-06-2023 09:46

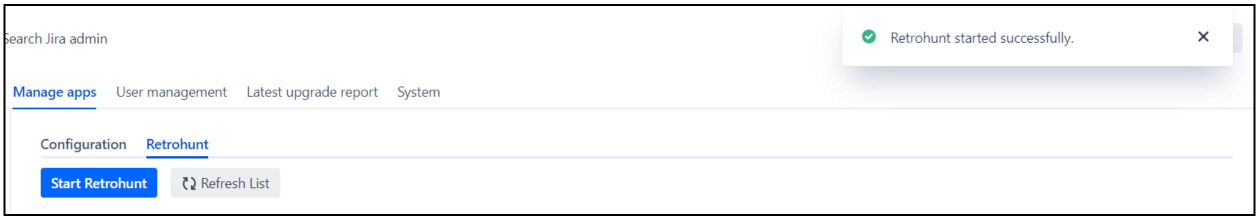
Start time for the time range of retrohunt

End DateTime:* 01-06-2023 10:46

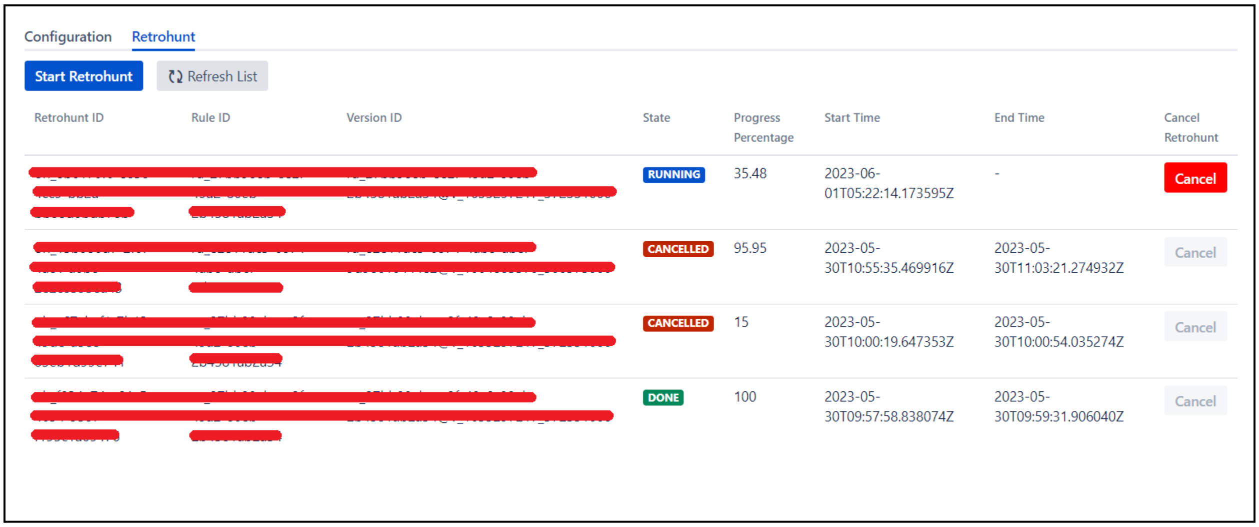
End time for the time range of retrohunt

version ID must be in format {rule_id} or {rule_id}@v_{version_timestamp.seconds}_{version_timestamp.nanos}

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.



Retrohunt started successfully.

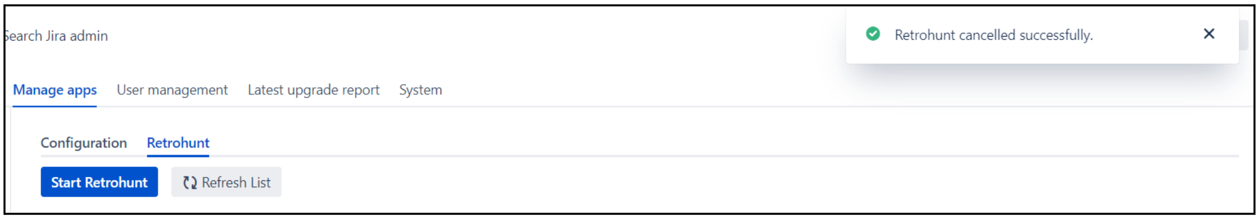


Retrohunt ID	Rule ID	Version ID	State	Progress Percentage	Start Time	End Time	Cancel Retrohunt
[redacted]	[redacted]	[redacted]	RUNNING	35.48	2023-06-01T05:22:14.173595Z	-	Cancel
[redacted]	[redacted]	[redacted]	CANCELLED	95.95	2023-05-30T10:55:35.469916Z	2023-05-30T11:03:21.274932Z	Cancel
[redacted]	[redacted]	[redacted]	CANCELLED	15	2023-05-30T10:00:19.647353Z	2023-05-30T10:00:54.035274Z	Cancel
[redacted]	[redacted]	[redacted]	DONE	100	2023-05-30T09:57:58.838074Z	2023-05-30T09:59:31.906040Z	Cancel

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.



Retrohunt cancelled successfully.

Ticket Created by the App

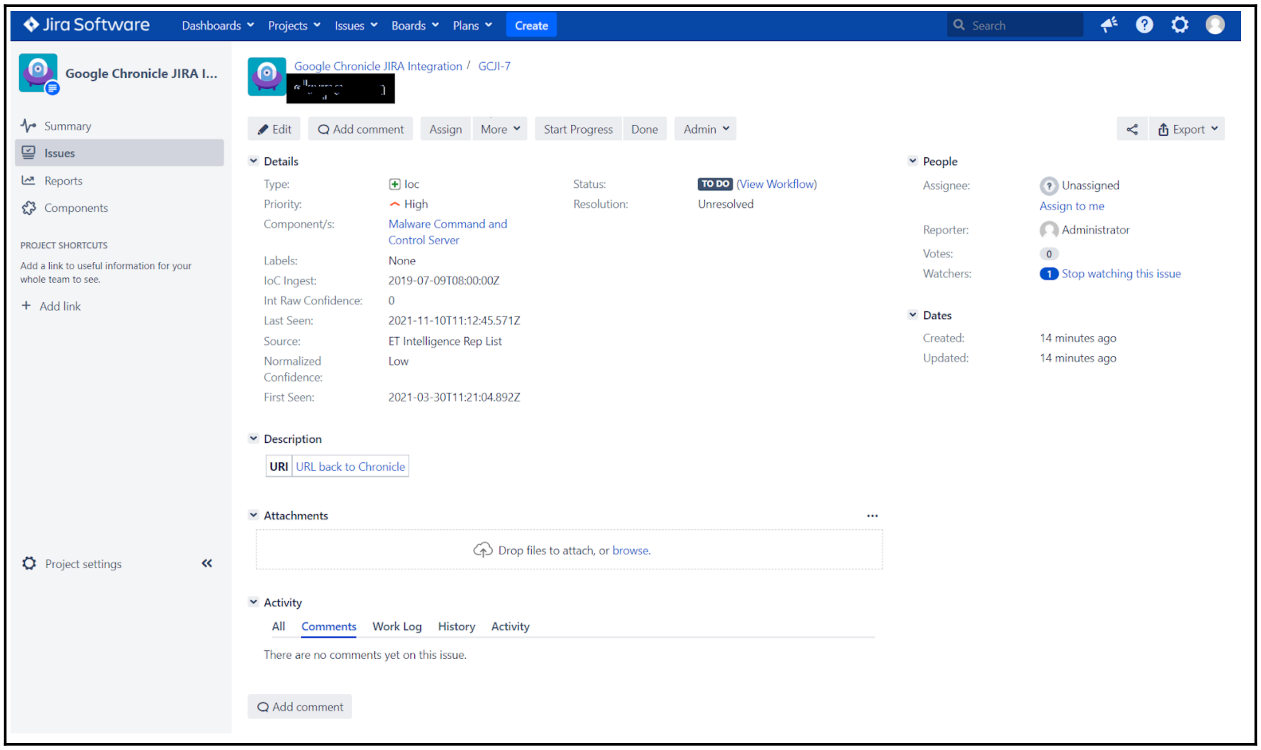
The app can create a total of 4 different types of tickets, based upon the configuration that the user chooses:

1. IoC Match
2. User Alert
3. Asset Alert
4. 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 are Domain Name, which means only a single ticket will be created for the Domain that is compromised until the ticket is in Todo, In-Progress and In-Review stages.



Google Chronicle JIRA Integration / GCJI-7

[redacted]

Details

Type:	Ioc
Priority:	High
Component/s:	Malware Command and Control Server
Labels:	None
IoC Ingest:	2019-07-09T08:00:00Z
Int Raw Confidence:	0
Last Seen:	2021-11-10T11:12:45.571Z
Source:	ET Intelligence Rep List
Normalized Confidence:	Low
First Seen:	2021-03-30T11:21:04.892Z
Status:	TO DO (View Workflow)
Resolution:	Unresolved

People

Assignee:	Unassigned Assign to me
Reporter:	Administrator
Votes:	0
Watchers:	1 Stop watching this issue

Dates

Created:	14 minutes ago
Updated:	14 minutes ago

Description

URI | URL back to Chronicle

Attachments

Drop files to attach, or browse.

Activity

All | Comments | Work Log | History | Activity

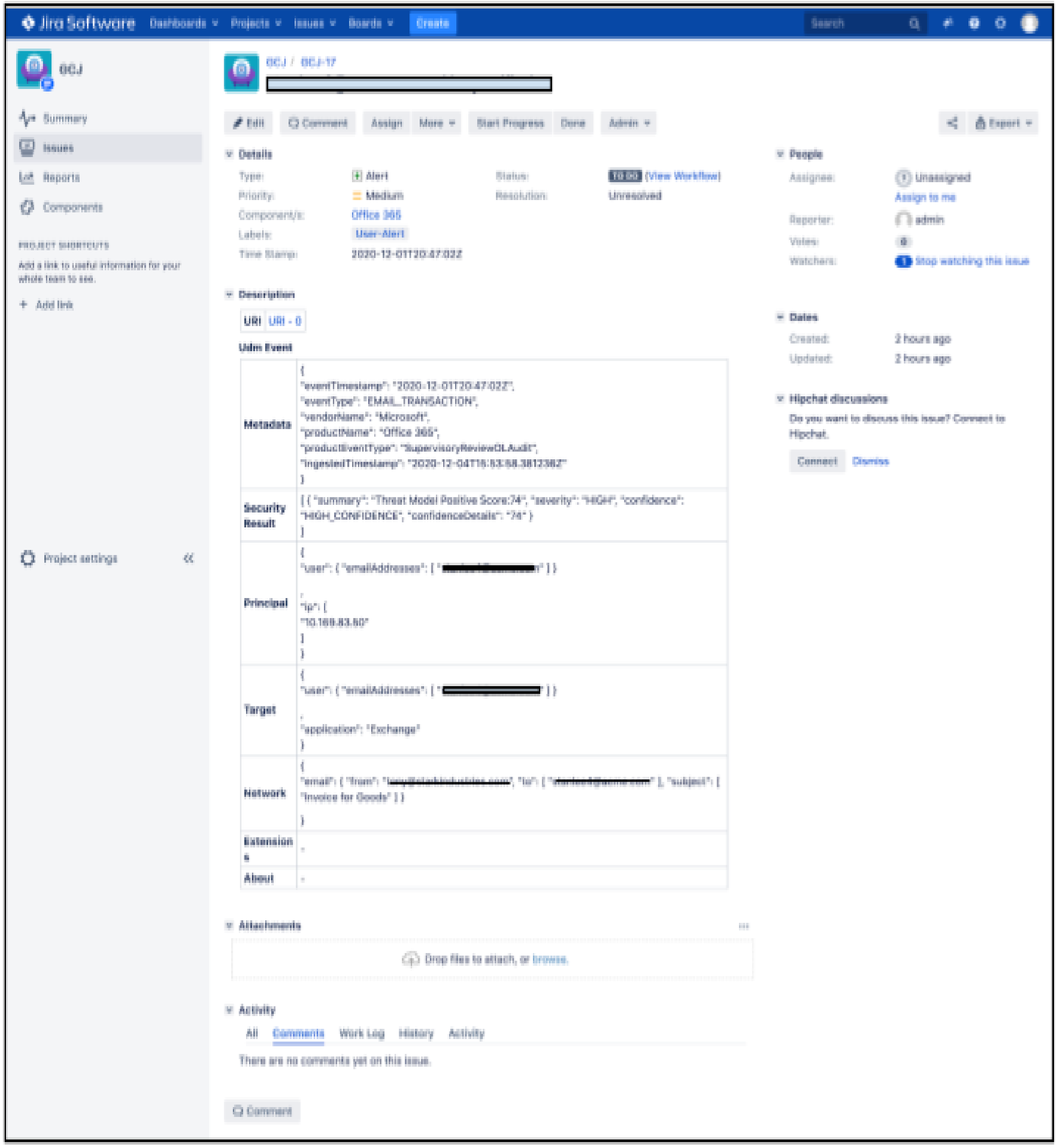
There are no comments yet on this issue.

Add comment

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 Todo, In-Progress and In-Review stage.



[redacted]

Details

Type: Alert
Priority: Medium
Component/s: Office 365
Labels: User-Alert
Time Stamp: 2020-12-01T20:47:02Z
Status: TO DO (View Workflow)
Resolution: Unresolved

People

Assignee: Unassigned
Assign to me
Reporter: admin
Votes: 0
Watchers: 1 Stop watching this issue

Dates

Created: 2 hours ago
Updated: 2 hours ago

Hipchat discussions

Do you want to discuss this issue? Connect to Hipchat.

Connect Dismiss

Description

URI URI - 0

Udm Event

Metadata	{
	"eventTimestamp": "2020-12-01T20:47:02Z",
	"eventType": "EMAIL_TRANSACTION",
	"vendorName": "Microsoft",
	"productName": "Office 365",
	"productEventType": "SupervisoryReviewOLAudit",
	"ingestedTimestamp": "2020-12-04T16:53:58.381238Z"
	}

Security Result	[{ "summary": "Threat Model Positive Score:74", "severity": "HIGH", "confidence": "HIGH_CONFIDENCE", "confidenceDetails": "74" }]

Principal	{
	"user": { "emailAddresses": ["[redacted]"] }
	,
	"ip": [
	"10.169.83.60"
	]
	}

Target	{
	"user": { "emailAddresses": ["[redacted]"] }
	,
	"application": "Exchange"
	}

Network	{
	"email": { "from": "[redacted]", "to": ["[redacted]"], "subject": ["Invoice for Goods"] }
	}

Extensions	-
About	-

Attachments

Drop files to attach, or browse.

Activity

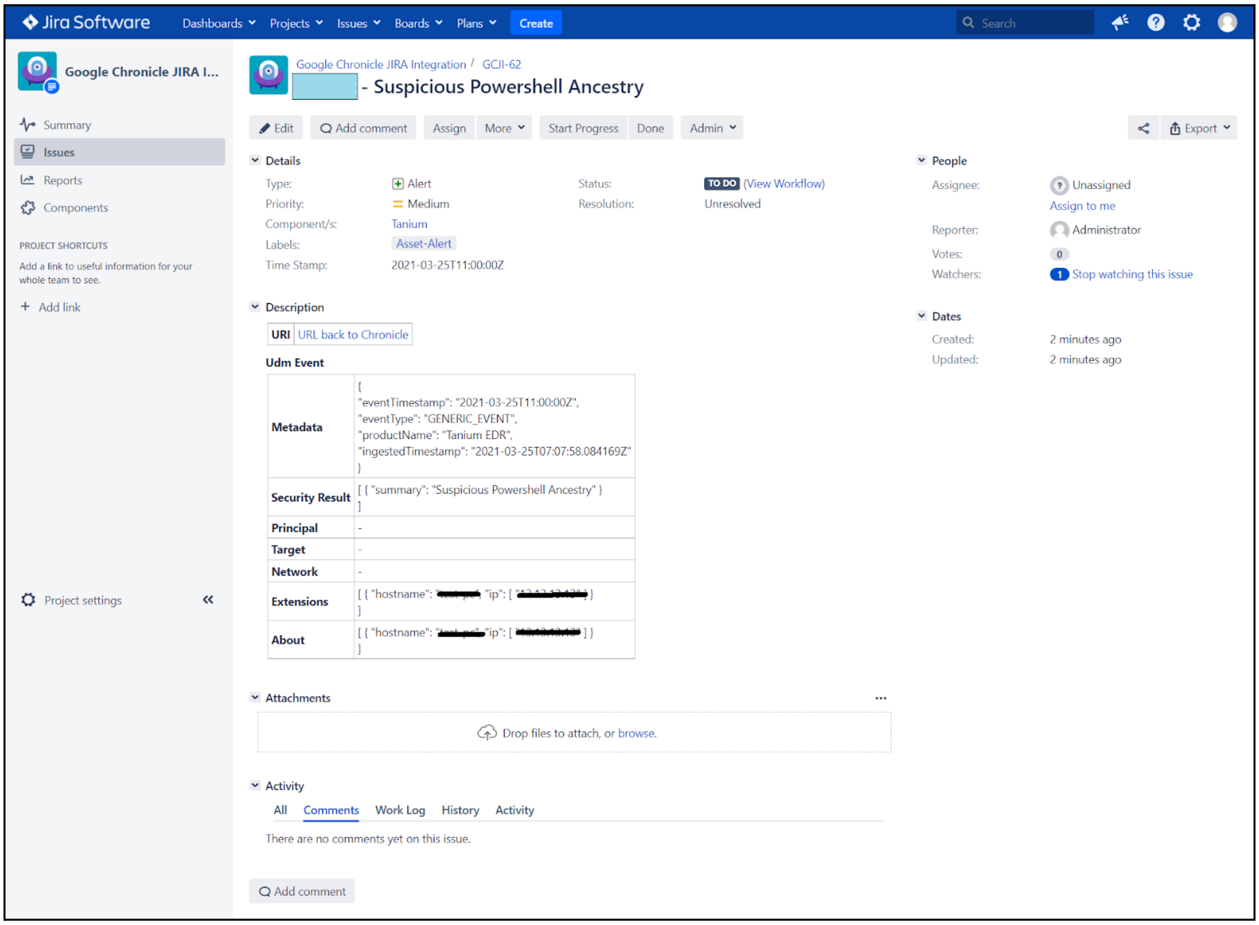
All Comments Work Log History Activity

There are no comments yet on this issue.

Comment

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 Todo, In-Progress and In-Review stage.



[redacted] - Suspicious Powershell Ancestry

Details

Type:	Alert	Status:	TO DO (View Workflow)
Priority:	Medium	Resolution:	Unresolved
Component/s:	Tanium		
Labels:	Asset-Alert		
Time Stamp:	2021-03-25T11:00:00Z		

Description

URI	URL back to Chronicle

Udm Event

Metadata	{
	"eventTimestamp": "2021-03-25T11:00:00Z",
	"eventType": "GENERIC_EVENT",
	"productName": "Tanium EDR",
	"ingestedTimestamp": "2021-03-25T07:07:58.084169Z"
	}

Security Result	[{ "summary": "Suspicious Powershell Ancestry" }]
Principal	-
Target	-
Network	-
Extensions	[{ "hostname": [redacted] "ip": [[redacted] }]
About	[{ "hostname": [redacted] "ip": [[redacted]] }]

Attachments

Drop files to attach, or browse.

Activity

All Comments Work Log History Activity

There are no comments yet on this issue.

Add comment

People

Assignee:	Unassigned Assign to me
Reporter:	Administrator
Votes:	0
Watchers:	1 Stop watching this issue

Dates

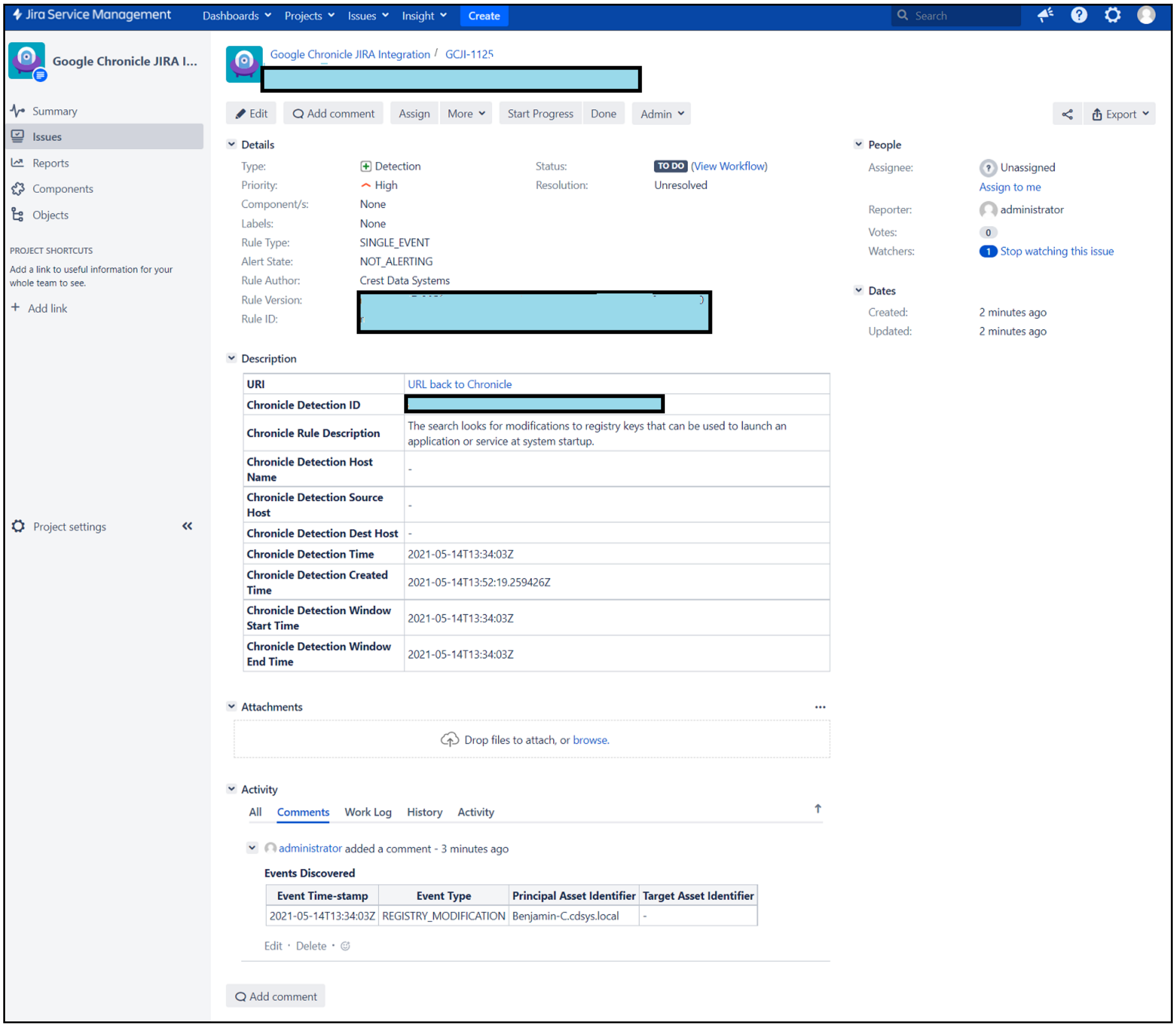
Created:	2 minutes ago
Updated:	2 minutes ago

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 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.



Google Chronicle JIRA Integration / GCJI-1125

[redacted]

Details

Type:	Detection	Status:	TO DO (View Workflow)
Priority:	High	Resolution:	Unresolved
Component/s:	None		
Labels:	None		
Rule Type:	SINGLE_EVENT		
Alert State:	NOT_ALERTING		
Rule Author:	Crest Data Systems		
Rule Version:	[redacted]		
Rule ID:			

People

Assignee:	Unassigned Assign to me
Reporter:	administrator
Votes:	0
Watchers:	1 Stop watching this issue

Dates

Created:	2 minutes ago
Updated:	2 minutes ago

Description

URI	URL back to Chronicle
Chronicle Detection ID	[redacted]
Chronicle Rule Description	The search looks for modifications to registry keys that can be used to launch an application or service at system startup.
Chronicle Detection Host Name	-
Chronicle Detection Source Host	-
Chronicle Detection Dest Host	-
Chronicle Detection Time	2021-05-14T13:34:03Z
Chronicle Detection Created Time	2021-05-14T13:52:19.259426Z
Chronicle Detection Window Start Time	2021-05-14T13:34:03Z
Chronicle Detection Window End Time	2021-05-14T13:34:03Z

Attachments

Drop files to attach, or browse.

Activity

All Comments Work Log History Activity

administrator added a comment - 3 minutes ago

Events Discovered

Event Time-stamp	Event Type	Principal Asset Identifier	Target Asset Identifier
2021-05-14T13:34:03Z	REGISTRY_MODIFICATION	Benjamin-C.cdsys.local	-

Edit · Delete ·

Add comment

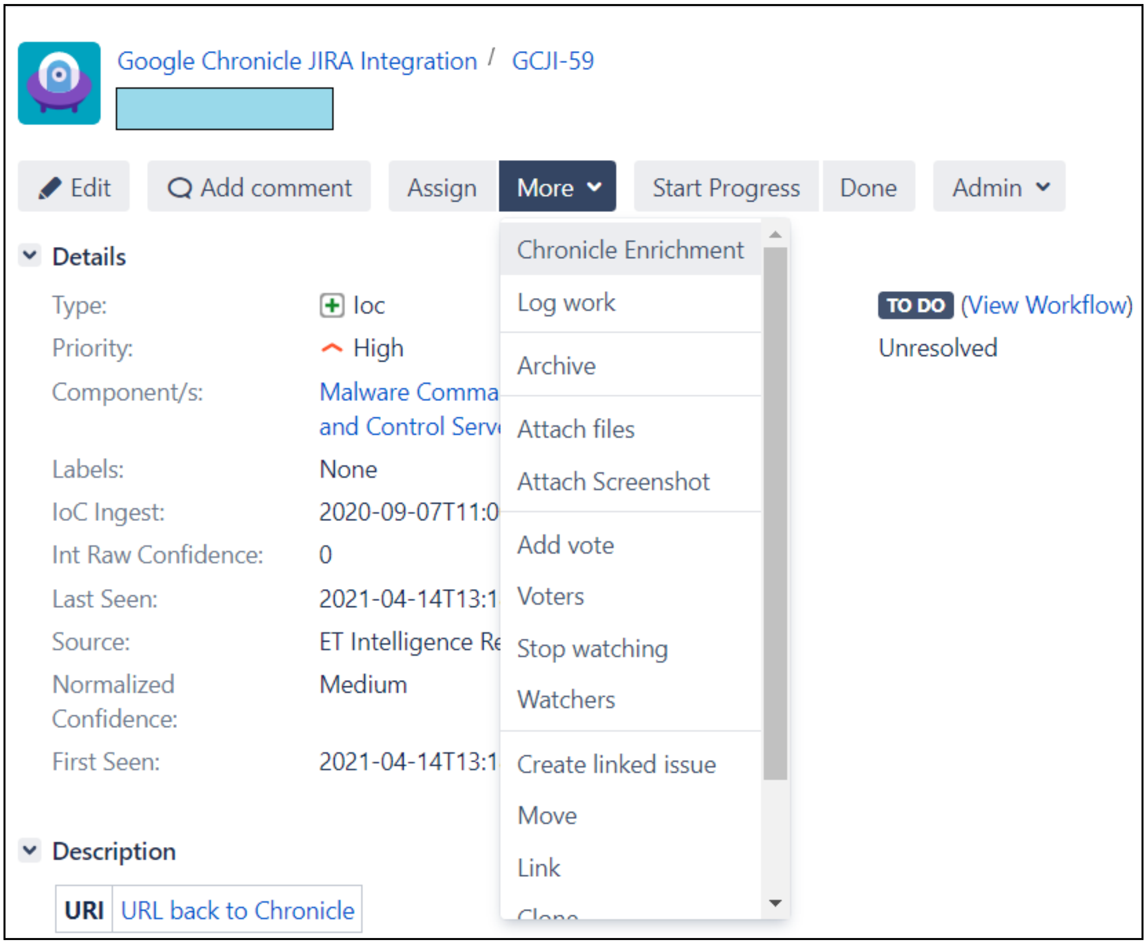
Enrichments

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 five 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

IoC Details

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



Google Chronicle JIRA Integration / GCJI-59

[redacted]

Details

Type: Ioc

Priority: High

Component/s: Malware Comma and Control Serv

Labels: None

IoC Ingest: 2020-09-07T11:0

Int Raw Confidence: 0

Last Seen: 2021-04-14T13:1

Source: ET Intelligence Re

Normalized Confidence: Medium

First Seen: 2021-04-14T13:1

TO DO (View Workflow)

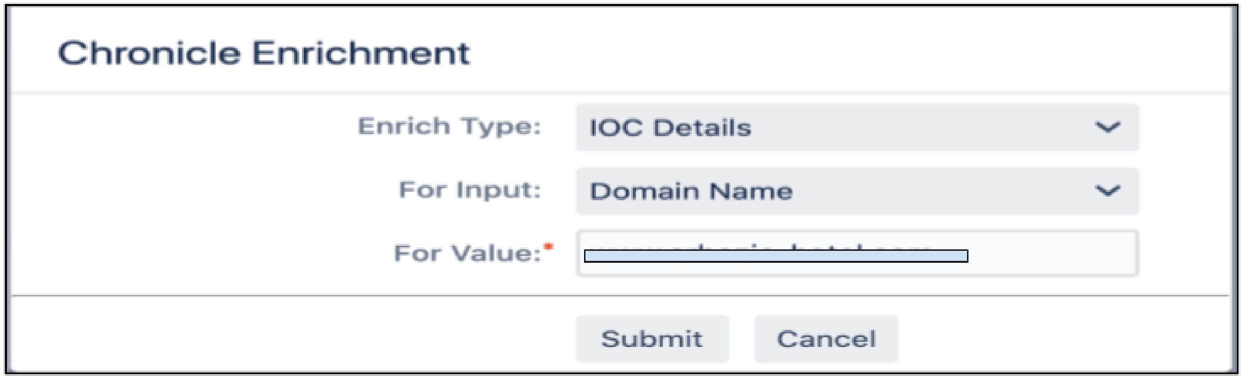
Unresolved

Description

URI URL back to Chronicle

- Upon clicking on the Chronicle 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.



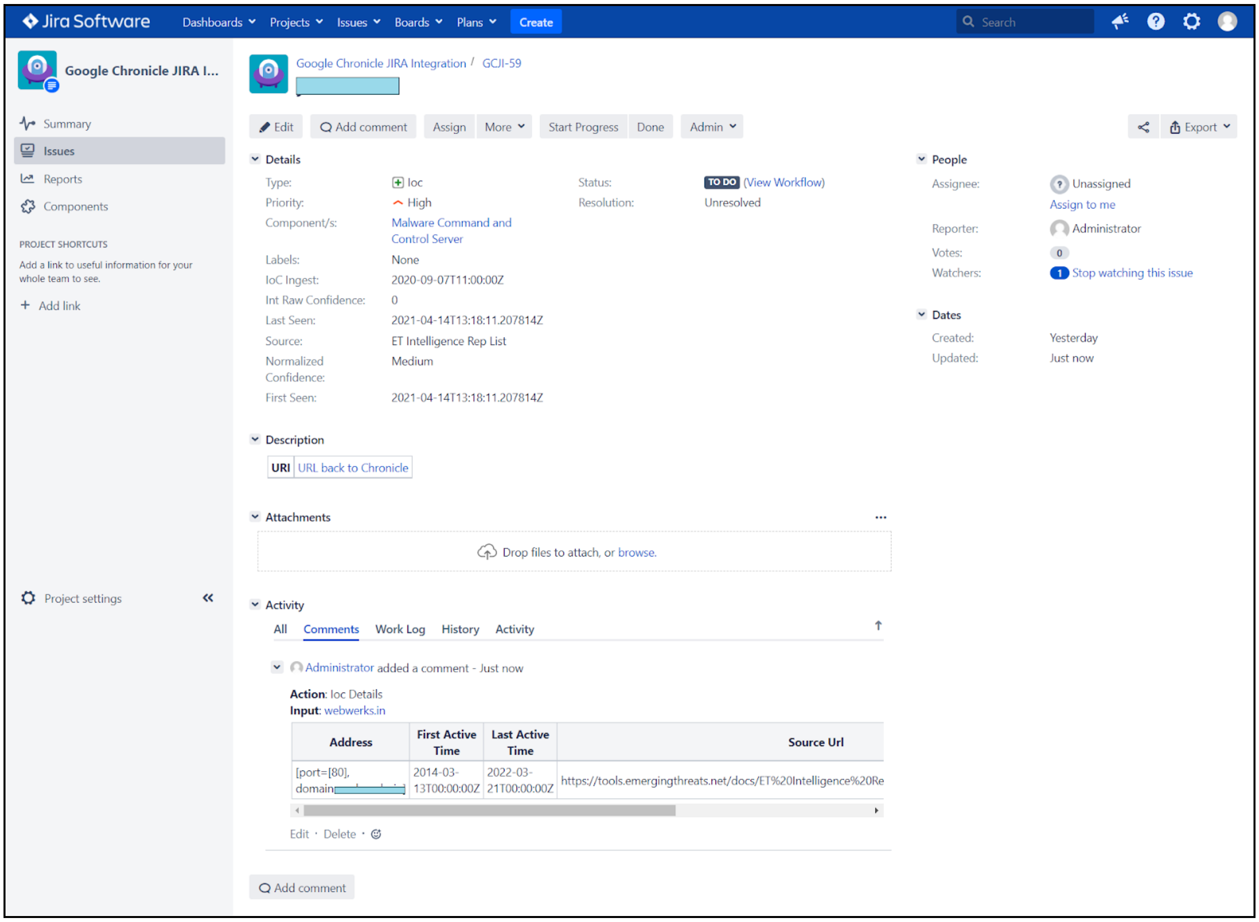
Chronicle Enrichment

Enrich Type: IOC Details

For Input: Domain Name

For Value:* [redacted]

- 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 chronicle API.



[redacted]

Details

Type:	Ioc
Priority:	High
Component/s:	Malware Command and Control Server
Labels:	None
IoC Ingest:	2020-09-07T11:00:00Z
Int Raw Confidence:	0
Last Seen:	2021-04-14T13:18:11.207814Z
Source:	ET Intelligence Rep List
Normalized Confidence:	Medium
First Seen:	2021-04-14T13:18:11.207814Z
Status:	TO DO (View Workflow)
Resolution:	Unresolved

People

Assignee:	Unassigned Assign to me
Reporter:	Administrator
Votes:	0
Watchers:	1 Stop watching this issue

Dates

Created:	Yesterday
Updated:	Just now

Description

URI	URL back to Chronicle

Attachments

Drop files to attach, or browse.

Activity

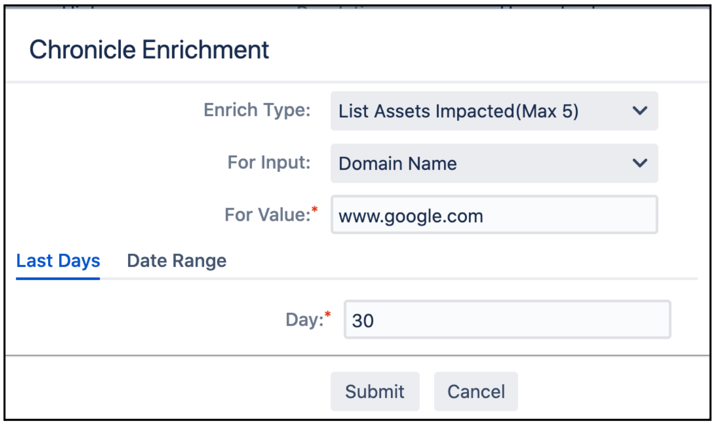
Administrator added a comment - Just now

Action: Ioc Details
Input: webwerks.in

Address	First Active Time	Last Active Time	Source Url
[port=[80], domain[redacted]	2014-03-13T00:00:00Z	2022-03-21T00:00:00Z	https://tools.emergingthreats.net/docs/ET%20Intelligence%20Re

List Assets Impacted

- Upon clicking the More Menu and then Chronicle 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.
- For 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.



Chronicle Enrichment

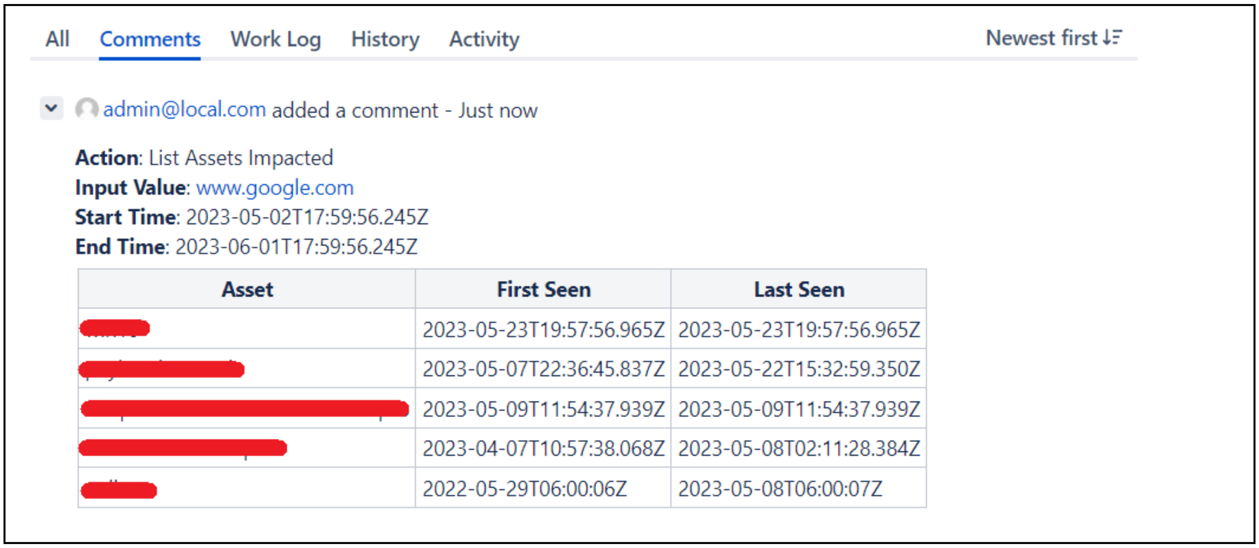
Enrich Type: List Assets Impacted(Max 5)

For Input: Domain Name

For Value:* www.google.com

Day:* 30

- 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 chronicle API.



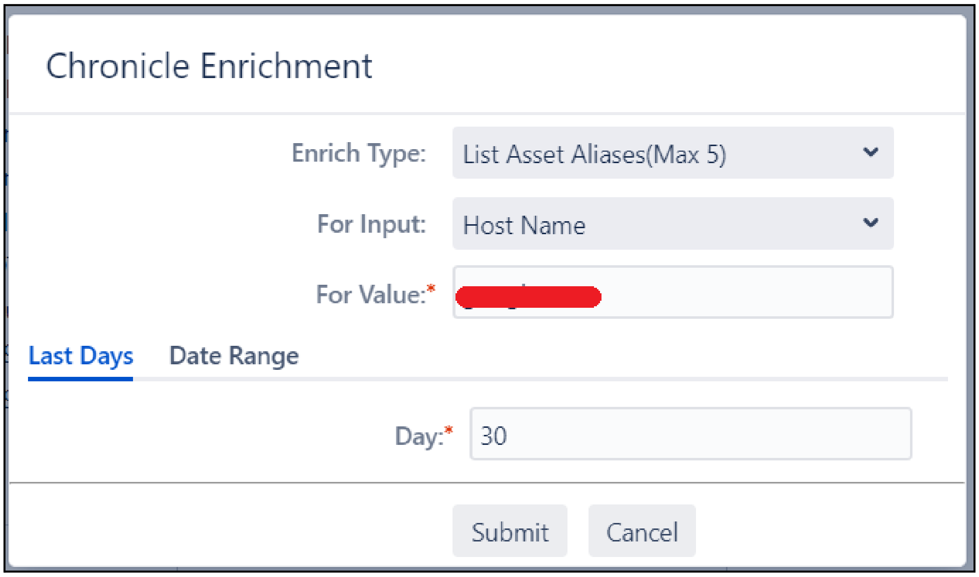
admin@local.com added a comment - Just now

Action: List Assets Impacted
Input Value: www.google.com
Start Time: 2023-05-02T17:59:56.245Z
End Time: 2023-06-01T17:59:56.245Z

Asset	First Seen	Last Seen
[redacted]	2023-05-23T19:57:56.965Z	2023-05-23T19:57:56.965Z
[redacted]	2023-05-07T22:36:45.837Z	2023-05-22T15:32:59.350Z
[redacted]	2023-05-09T11:54:37.939Z	2023-05-09T11:54:37.939Z
[redacted]	2023-04-07T10:57:38.068Z	2023-05-08T02:11:28.384Z
[redacted]	2022-05-29T06:00:06Z	2023-05-08T06:00:07Z

List Asset Aliases

- Upon clicking the More Menu and then Chronicle 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.



Chronicle Enrichment

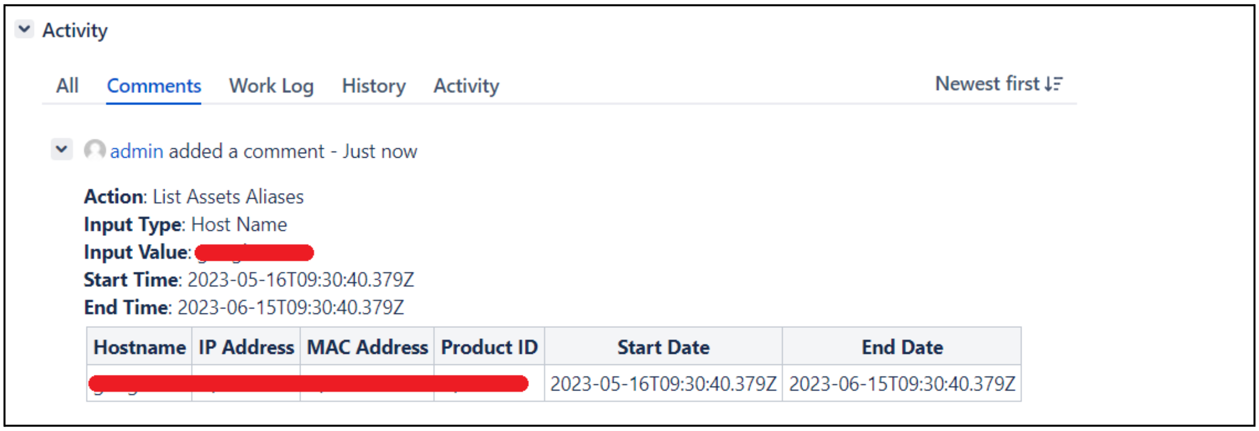
Enrich Type: List Asset Aliases(Max 5)

For Input: Host Name

For Value:* [redacted]

Day:* 30

- 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 chronicle API.



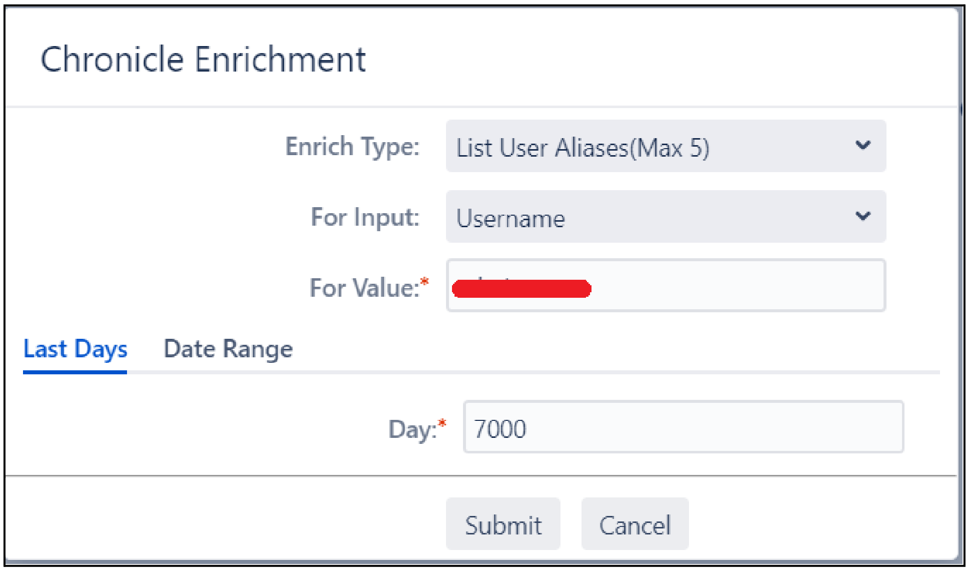
admin added a comment - Just now

Action: List Assets Aliases
Input Type: Host Name
Input Value: [redacted]
Start Time: 2023-05-16T09:30:40.379Z
End Time: 2023-06-15T09:30:40.379Z

Hostname	IP Address	MAC Address	Product ID	Start Date	End Date
[redacted]	[redacted]	[redacted]	[redacted]	2023-05-16T09:30:40.379Z	2023-06-15T09:30:40.379Z

List User Aliases

- Upon clicking the More Menu and then Chronicle 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.



Chronicle Enrichment

Enrich Type: List User Aliases(Max 5)

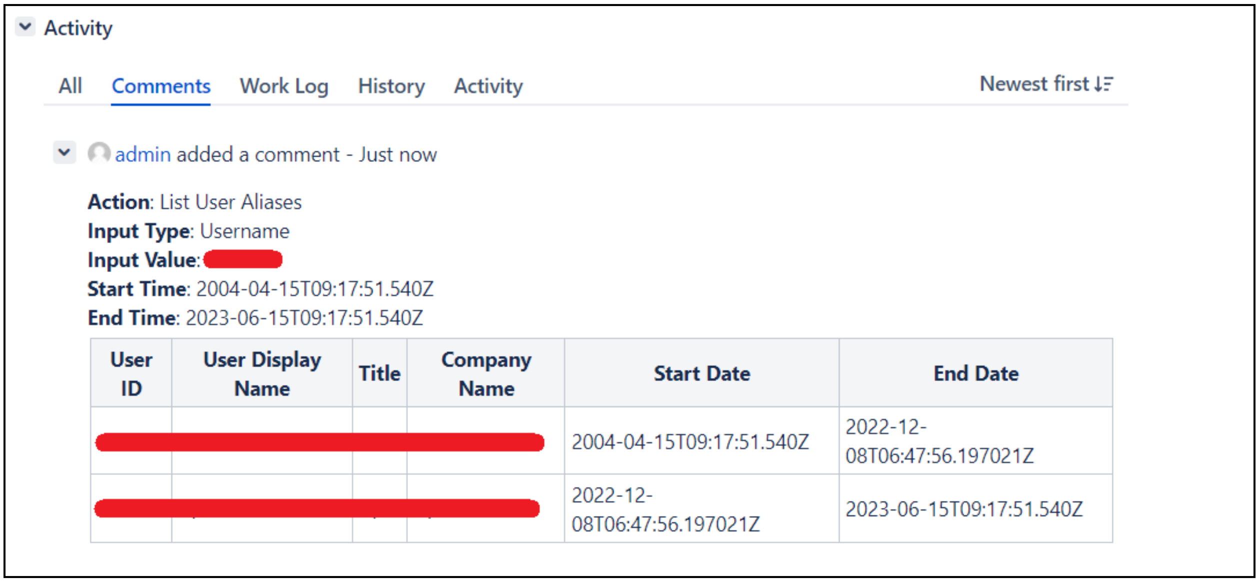
For Input: Username

For Value:* [redacted]

Last Days | Date Range

Day:* 7000

- 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 chronicle API.



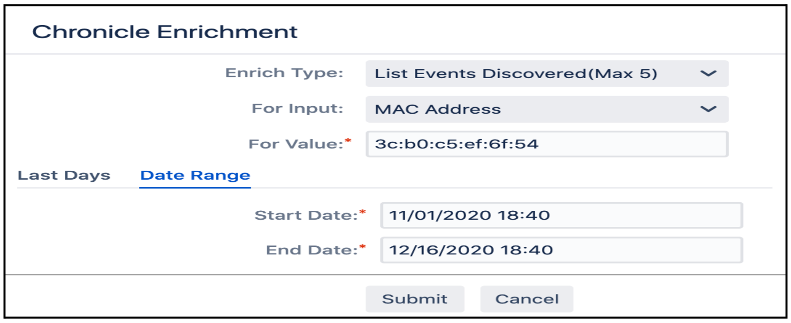
admin added a comment - Just now

Action: List User Aliases
Input Type: Username
Input Value: [redacted]
Start Time: 2004-04-15T09:17:51.540Z
End Time: 2023-06-15T09:17:51.540Z

User ID	User Display Name	Title	Company Name	Start Date	End Date
[redacted]	[redacted]	[redacted]	[redacted]	2004-04-15T09:17:51.540Z	2022-12-08T06:47:56.197021Z
[redacted]	[redacted]	[redacted]	[redacted]	2022-12-08T06:47:56.197021Z	2023-06-15T09:17:51.540Z

List Events Discovered

- Upon clicking the More Menu and then Chronicle 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.



Chronicle Enrichment

Enrich Type: List Events Discovered(Max 5)

For Input: MAC Address

For Value:* 3c:b0:c5:ef:6f:54

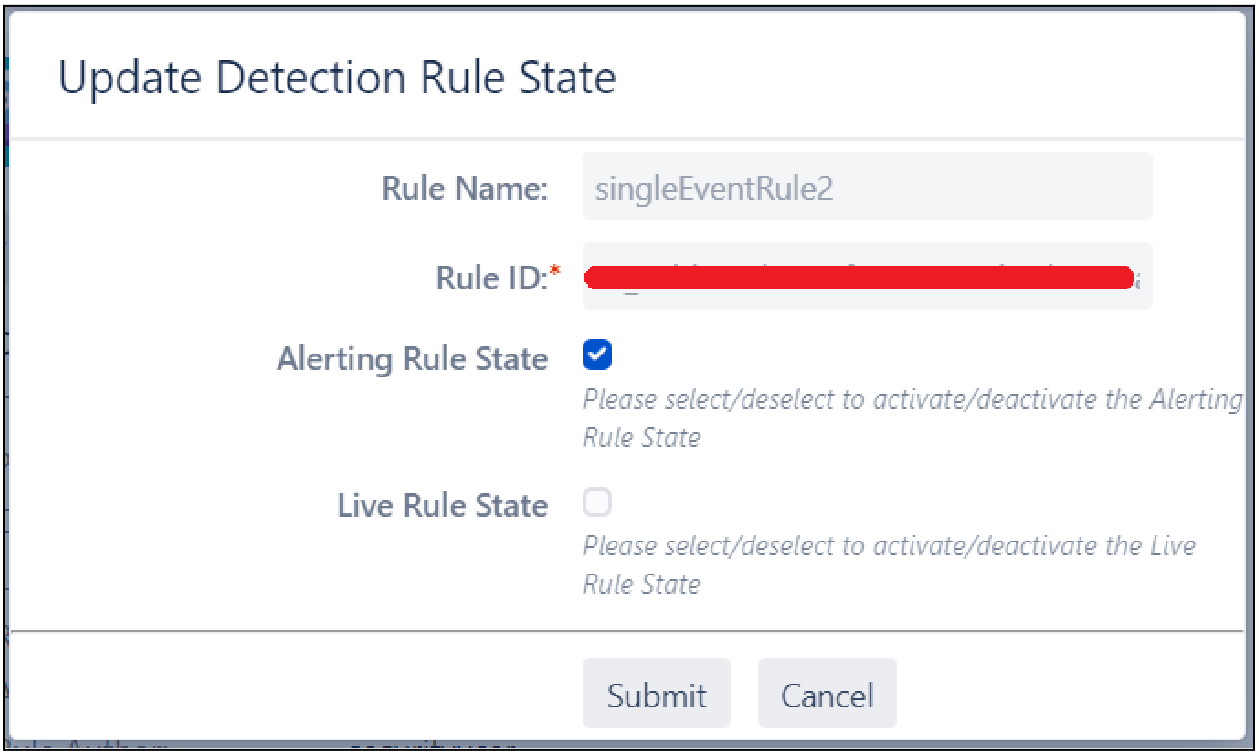
Start Date:* 11/01/2020 18:40

End Date:* 12/16/2020 18:40

- 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 chronicle API.

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.



Update Detection Rule State

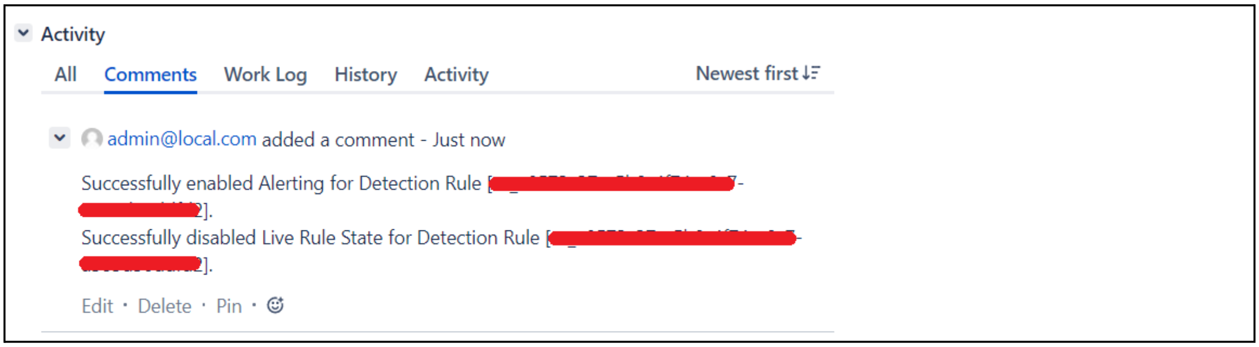
Rule Name: singleEventRule2

Rule ID:* [redacted]

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

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



admin@local.com added a comment - Just now

Successfully enabled Alerting for Detection Rule [[redacted]-
[redacted]].
Successfully disabled Live Rule State for Detection Rule [[redacted]-
[redacted]].

Development Assumptions

1. Only those projects will be listed which would have been created via the Chronicle Project Creation Template
2. For Daily, weekly and monthly the job won't trigger immediately. It will only fetch the data as the user will configure it.
3. The deduplication criteria for the ticket creation are as follows:
    - IoC: Domain Name.
    - Asset Alert: Combination of Asset and Alert Name.
    - User Alert: Combination of Email Address and Alert Name.
    - Detection: Detection Id.
4. If the severity is empty/NA and has not been sent as part of the chronicle 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. 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 and Detections will be reset and the data will be fetched based on the No of days to fetch IoCs/Alerts/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 Initially** for Project B.
8. 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 and detections, and it won’t interrupt the current scheduler
9. 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 and detections and it won’t interrupt the current scheduler.
10. The app sends the entered inputs to Chronicle API and validations are handled by Chronicle 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.
11. For the Asset Aliases option in Chronicle 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.
12. If there is more data available for IOCs, Alerts or 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 chronicle for an

interval of 1 day then only 1000 IOCs will be created in Jira and the remaining 200 will be missed.

13. 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 Chronicle Management System template. The restriction in the customized templates is good, as that doesn't allow any user to make changes stopping to cause issues in the creation of the tickets
14. 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 logs error.

Messages	**Responses**	**Location**
Invalid service account file or Invalid region.	If the Invalid service account file is uploaded or the Invalid region value is entered	Config Screen
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 / Chronicle 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 Chronicle 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
pullRules() Failed	Failed to pull 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
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 Chronicle Enrichment [“User Aliases”] fails	Logs
assetAliases() Failed: {}	When Chronicle 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

Below segment covers some additional information about the Chronicle App

Application Dependencies

Area	Version
Java	8 (1.8.x)
Atlassian SDK	8.2.7
Chronicle API Version	V1, V2

App - Jira Version Compatible Matrix

Jira Software	8.19.x - 9.8.x
Jira Service Desk	4.19.x - 5.8.x

——------——--End of Document—---